Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)

Darij Grinberg

Monday 11th November, 2019 at 13:01.
Status: finished up to Section 4.2.4.

Contents

1. Introduction

This file contains notes for the Math 4281 class ("Introduction to Modern Algebra") I have taught at the University of Minnesota in Spring 2019. Occasionally, it also includes material that did not appear in the lectures.

The website of the class is `https://www.cip.ifi.lmu.de/~grinberg/t/19s/index.html` ; you will find homework sets and midterms there.

1.1. Status

The first few chapters of these notes are finished. The rest are at various degrees of completion (mostly readable, but sometimes not completely polished).

1.2. Literature

Many books have been written about abstract algebra. I have only a passing familiarity with most of them. Some of the "bibles" of the subject (bulky texts covering lots of material) are Dummit/Foote [DumFoo04], Knapp [Knapp16a] and [Knapp16b] (both freely available), van der Waerden [Waerde91a] and [Waerde91b] (one of the oldest texts on modern algebra, thus rather dated, but still as readable as ever).

Of course, any book longer than 200 pages likely goes further than our course will (unless it is full of details or solved exercises or printed in really large letters, like this one will be once it is finished). Thus, let me recommend some more introductory sources. Siksek's lecture notes [Siksek15] are a readable introduction that is a lot more amusing than I had ever expected an algebra text to be. Goodman's free book [Goodma16] combines introductory material with geometric motivation and applications, such as the classification of regular polyhedra and 2-dimensional crystals. In a sense, it is a great complement to our ungeometric course. Pinter's [Pinter10] often gets used in classes like ours. Armstrong's notes [Armstr18] cover a significant part of what we do. Childs's [Childs00] comes the closest to what we are setting out to do here, that is, give an example-grounded introduction to basic abstract algebra.

Keith Conrad's blurbs [Conrad*] are not a book, as they only cover selected topics. But at pretty much every topic they cover, they are one of the best sources (clear, full of examples, and often going fairly deep). We shall follow one of them particularly closely: the one on Gaussian integers [ConradG].

We will use some basic linear algebra, all of which can be found in Hefferon's book [Heffer17] (but we won't need all of this book). As far as determinants are concerned, we will briefly build up their theory; we refer to [Strick13, Section 12 & Appendix B] for proofs (and to [Grinbe15, Chapter 6] for a really detailed and formal treatment).

This course will begin (after some motivating questions) with a survey of elementary number theory. This is in itself a deep subject (despite the name) with a long history (perhaps as old as mathematics), and of course we will just scratch the surface. Books like [NiZuMo91], [Burton10] and [UspHea39] cover a lot more than we can do. The Gallier/Quaintance survey [GalQua17] covers a good amount of basics and more.

We assume that the reader is familiar with the commonplaces of mathematical argumentation, such as induction (including strong induction), "WLOG" arguments, proof by contradiction, summation signs ($\sum$) and polynomials (a vague notion of polynomials will suffice; we will give a precise definition when it becomes necessary). If not, several texts can be helpful in achieving such familiarity: e.g., [LeLeMe18, particularly Chapters 1–5], [Hammac18], [Day16].

I thank the students of the Math 4281 class for discovering and reporting errors in previous versions of these notes. Some of the discussion of variants of Gaussian integers (and the occasional correction) is due to Keith Conrad; the discussion of Gaussian integers itself owes much to his [ConradG].

These notes include some excerpts from [Grinbe16] and slightly rewritten sections of [Grinbe15].

1.3. The plan

The material I am going to cover is mostly standard. However, the order in which I will go through it is somewhat unusual: I will spend a lot of time studying the basic examples before defining abstract notions such as "group", "monoid", "ring" and "field". This way, once I come to these notions, you'll already have many examples to work with. (Don't be fooled by the word "example": We will prove a lot about them, much of which is neither straightforward nor easy.)

First, I will show some motivating questions that are easy to state yet require abstract algebra to answer. We will hopefully see their answers by the end of this class. (Some of them can also be answered elementarily, without using abstract algebra, but such answers usually take more work and are harder to find.)

1.4. Motivation: $n = x^2 + y^2$

A *perfect square* means the square of an integer. Thus, the perfect squares are

$$0^2 = 0, \qquad 1^2 = 1, \qquad 2^2 = 4, \qquad 3^2 = 9, \qquad 4^2 = 16, \qquad \ldots.$$

Here is an old problem (first solved by Pierre de Fermat in 1640, but apparently already studied by Diophantus in the 3rd Century):

Question 1.4.1. What integers can be written as sums of two perfect squares?

For example, 5 can be written in this way, since $5 = 2^2 + 1^2$.

So can 4, since $4 = 2^2 + 0^2$. (Keep in mind that 0 is a perfect square.)

However, 7 cannot be written in this way. In fact, if we had $7 = a^2 + b^2$ for two integers a and b, then a^2 and b^2 would have to be ≤ 7 (since a^2 and b^2 are always ≥ 0, no matter what sign a and b have); but the only perfect squares that are ≤ 7 are $0, 1, 4$, and there is no way to write 7 as a sum of two of these perfect squares (just check all the possibilities).

For a similar but simpler reason, no negative number can be written as a sum of two perfect squares.

We can of course approach Question 1.4.1 using a computer: It is easy to check, for a given integer n, whether n is a sum of two perfect squares. (Just check all possibilities for a and b for the validity of the equation $n = a^2 + b^2$. You only need to try a and b belonging to $\{0, 1, \ldots, \lfloor \sqrt{n} \rfloor\}$, where $\lfloor y \rfloor$ (for a real number y) denotes the largest integer that is less or equal than y (also known as "y rounded down").) If you do this, you will see that among the first 101 nonnegative integers, the ones that can be written as sums of two perfect squares are precisely

$$\begin{gathered}0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, \\ 32, 34, 36, 37, 40, 41, 45, 49, 50, 52, 53, 58, 61, 64, \\ 65, 68, 72, 73, 74, 80, 81, 82, 85, 89, 90, 97, 98, 100.\end{gathered}$$

Having this data, you can look up the sequence in the Online Encyclopedia of Integer Sequences (short OEIS), and see that the sequence of these integers is known as OEIS Sequence A001481. In the "Comments" field, you can read a lot of what is known about it (albeit in telegraphic style).

For example, one of the comments says "Closed under multiplication". This is short for "if you multiply two entries of the sequence, then the product will again be an entry of the sequence". In other words, if you multiply two integers that are sums of two perfect squares, then you get another sum of two perfect squares. Why is this so?

It turns out that there is a "simple" reason for this: the identity

$$\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ad + bc)^2 + (ac - bd)^2, \tag{1}$$

which holds for arbitrary reals a, b, c, d (and thus, in particular, for integers). This is known as the Brahmagupta-Fibonacci identity, and of course can easily be proven by expanding both sides. But how would you come up with such an identity?

If you stare at the above sequence long enough, you may also discover another pattern: An integer of the form $4k + 3$ with integer k (that is, an integer that is larger by 3 than a multiple of 4) can never be written as a sum of two perfect squares. (Thus, $3, 7, 11, 15, 19, 23, \ldots$ cannot be written in this way.) This does not account for all integers that cannot be written in this way, but it does provide some clues to the answer that we will later see. In order to prove this observation, we shall need basic modular arithmetic (or at least division with remainder); we will see this proof very soon (see Exercise 2.7.2 **(c)**).

We will resolve Question 1.4.1 using the theory of Gaussian integers in Chapter 4. For a survey of different approaches to Question 1.4.1 (including a full answer using finite fields), see [AigZie18, Chapter 4].

Further questions can be asked. One of them is: Given an integer n, how many ways are there to represent n as a sum of two perfect squares? This is actually several questions masquerading as one, since it is not so clear what a "way" is. Do $5 = 1^2 + 2^2$ and $5 = 2^2 + 1^2$ count as two different ways? What about $5 = 1^2 + 2^2$ versus $5 = (-1)^2 + 2^2$ (here, the perfect squares are the same, but do we really want to count the squares or rather the numbers we are squaring?).

Let me formalize the question as follows:

> **Question 1.4.2.** Let n be an integer.
>
> **(a)** How many pairs $(a, b) \in \mathbb{N}^2$ are there that satisfy $n = a^2 + b^2$? Here, and in the following, $\mathbb{N}$ denotes the set $\{0, 1, 2, \ldots\}$ of all nonnegative integers.
>
> **(b)** How many pairs $(a, b) \in \mathbb{Z}^2$ are there that satisfy $n = a^2 + b^2$? Here, and in the following, $\mathbb{Z}$ denotes the set $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ of all integers.
>
> **(c)** How do these counts change if we count **unordered** pairs instead (i.e., count (a, b) and (b, a) as one only)?

Note that when I say "pair", I always mean "ordered pair" by default, unless I explicitly say "unordered pair".

Again, a little bit of programming easily yields answers to all three parts of this question for small values of n, and the resulting data can be plugged into the OEIS and yields lots of information.

First steps toward answering Question 1.4.2. **(a)** I claim that the number of such pairs is even unless n is twice a perfect square (i.e., unless $n = 2m^2$ for some integer m); in the latter case, this number is odd instead.

Why? Let me define a *solution* to be a pair (a, b) such that $n = a^2 + b^2$. So I want to know whether the number of solutions is even or odd. But we have $a^2 + b^2 = b^2 + a^2$ for all a and b. Thus, if (a, b) is a solution, then so is (b, a). Hence, the solutions themselves "come in pairs", with each solution (a, b) being matched to the solution (b, a), unless there is a solution (a, b) with $a = b$ (because such a solution would be matched to itself, and thus not form an actual pair). But solutions (a, b) with $a = b$ are easy to classify: If n is twice a perfect square, then there is exactly one such solution (namely, $\left(\sqrt{n/2}, \sqrt{n/2}\right)$); otherwise there is none (because $n = a^2 + b^2$ with $a = b$ leads to $n = b^2 + b^2 = 2b^2$, which can only happen when n is twice a perfect square). Since we know that all the other solutions "come in pairs", we thus conclude that the number of solutions is odd if n is twice a perfect square and even otherwise. This proves our claim.

Of course, we have not made much headway into Question 1.4.2; knowing whether a number is even or odd is far from knowing the number itself. But I think the argument above was worth showing; similar reasoning is used a lot in algebra.

(b) By reasoning analogous to the one we used in part **(a)**, we can see that the number of such pairs will be divisible by 8 whenever n is neither a perfect square nor twice a perfect square. Indeed, this relies on the fact that

$$\begin{aligned} a^2+b^2 &= b^2+a^2 = (-a)^2+b^2 = b^2+(-a)^2 = a^2+(-b)^2 = (-b)^2+a^2 \\ &= (-a)^2+(-b)^2 = (-b)^2+(-a)^2 \end{aligned}$$

for all a and b. Thus the pairs $(a,b) \in \mathbb{Z}^2$ that satisfy $n = a^2+b^2$ don't just come in pairs; they come in sets of 8 (namely, each (a,b) comes in a set with (b,a), $(-a,b)$, $(b,-a)$, $(a,-b)$, $(-b,a)$, $(-a,-b)$ and $(-b,-a)$). These sets of 8 can "degenerate" to smaller sets when some of their elements coincide, but this can only happen when n is a perfect square (in which case we can have $(a,b) = (-a,b)$ for example) or twice a perfect square (in which case we can have $(a,b) = (b,a)$ or $(a,b) = (-b,-a)$ or other such coincidences). (Check this!)

(c) We can reduce this to parts **(a)** and **(b)**. Indeed:[1]

- When n is not twice a perfect square, the number of unordered pairs will be half the number of ordered pairs, since each unordered pair $(u,v)_{\text{unordered}}$ corresponds to precisely two ordered pairs (u,v) and (v,u).
- When n is twice a perfect square, we have

  $$\begin{aligned} &(\text{the number of unordered pairs}) \\ &= \frac{(\text{the number of ordered pairs}) + (\text{the number of pairs with } a=b)}{2}. \end{aligned}$$

  Indeed, each unordered pair $(u,v)_{\text{unordered}}$ corresponds to precisely two ordered pairs (u,v) and (v,u) unless $u = v$, in which case it corresponds to only one ordered pair. Thus, if we multiply the number of unordered pairs by 2, then we **overcount** the number of ordered pairs, because we are counting the pairs (u,v) with $u = v$ (that is, the pairs with $a = b$) twice. So we get (the number of ordered pairs) + (the number of pairs with $a = b$). This proves our above formula.

  What is the number of pairs with $a = b$? If $n = 0$, then it is 1 (and the only such pair is $(0,0)$). Otherwise, it is 1 if we are counting pairs in $\mathbb{N}^2$ (and the only such pair is $\left(\sqrt{n/2}, \sqrt{n/2}\right)$), and is 2 if we are counting pairs in $\mathbb{Z}^2$ (and the only two such pairs are $\left(\sqrt{n/2}, \sqrt{n/2}\right)$ and $\left(-\sqrt{n/2}, -\sqrt{n/2}\right)$). □

Note that sums of squares have a geometric meaning (going back to Pythagoras): Two real numbers a and b satisfy $a^2+b^2 = n$ (for a given integer $n \geq 0$) if and only if the point with Cartesian coordinates (a,b) lies on the circle with center 0 and

[1] In the rest of this argument, "pair" will always mean "pair (a,b) satisfying $n = a^2+b^2$".

radius $\sqrt{n}$. This will actually prove a valuable insight that will lead us to the answers to the above questions.

Just as a teaser: There are formulas for all three parts of Question 1.4.2, in terms of divisors of n of the forms $4k+1$ and $4k+3$. We will see these formulas after we have properly understood the concept of Gaussian integers.

1.5. Motivation: Algebraic numbers

A real number z is said to be *algebraic* if there exists a nonzero polynomial P with rational coefficients such that $P(z) = 0$. In other words, a real number z is algebraic if and only if it is a root of a nonzero polynomial with rational coefficients.

(If you know the complex numbers, you can replace "real" by "complex" in this definition; but we shall only see real numbers in this little motivational section.)

Here are a few examples:

- Each rational number a is algebraic (being a root of the nonzero polynomial $x-a$ with rational coefficients).

- The number $\sqrt{2}$ is algebraic (being a root of the nonzero polynomial x^2-2).

- The number $\sqrt[3]{5}$ is algebraic (being a root of x^3-5).

- All the roots of the polynomial $f(x) := \dfrac{3}{2}x^4 + 17x^3 - 12x + \dfrac{9}{4}$ (whatever they are) are algebraic.
  Speaking of these roots, what are they? Using a computer, one can show that this polynomial $f(x)$ has 4 real roots $(-11.269\ldots, -0.960\ldots, 0.198\ldots, 0.697\ldots)$, which can be written as complicated expressions with radicals (i.e., $\sqrt[k]{\ }$ signs), though complex numbers appear in these expressions (despite the roots being real!). All this does not matter to the fact that they are algebraic ⌣̈

- All the roots of the polynomial $g(x) := x^7 - x^5 + 1$ are algebraic.
  This polynomial has only one real root. This root cannot be written as an expression with radicals (as can be proven using Galois theory – indeed, the discovery of this theory greatly motivated the development of abstract algebra). Nevertheless, it is algebraic, by definition. (The same holds for the remaining 6 complex roots of g – we are working with real numbers here only for the sake of familiarity.)

- The most famous number that is not algebraic is π. This is a famous result of Lindemann, but it belongs to analysis, not to algebra, because π is not defined algebraically in the first place (it is defined as the length of a curve or as an area of a curved region – but either of these definitions boils down to a limit of a sequence).

- The second most famous number that is not algebraic is Euler's number e (the basis of the natural logarithm). Again, analysis is needed to define e, and thus also to prove its non-algebraicity.

Numbers that are not algebraic are called *transcendental*. We shall not study them much, since most of them do not come from algebra. Instead, we shall try our hands at the following question:

> **Question 1.5.1.** **(a)** Is the sum of two (or, more generally, finitely many) algebraic numbers always algebraic?
>
> **(b)** What if we replace "sum" by "difference" or "product"?

Let me motivate why this is a natural question to ask. The sum of two integers is still an integer; the sum of two rational numbers is still a rational number. These facts are fundamental; without them we could hardly work with integers and rational numbers. If a similar fact would not hold for algebraic numbers, it would mean that the algebraic numbers are not a good "number system" to work in; on a practical level, it would mean that (e.g.) if we defined a function on the set of all algebraic numbers, then we could not plug a sum of algebraic numbers into it.

*Attempts at answering Question 1.5.1 **(a)**.* Let us try a particularly simple example of a sum of two algebraic numbers: Let w be $\sqrt{2}+\sqrt{3}$. Is w algebraic?

To answer this question affirmatively, we need to find a nonzero polynomial $f(x)$ with rational coefficients that has w as a root.

Just looking at the equality $w=\sqrt{2}+\sqrt{3}$, we cannot directly eyeball such an f. The problem, in a sense, is that there are too many (namely, two) square roots in this equality.

However, if we square this equality, then we obtain

$$w^2=\left(\sqrt{2}+\sqrt{3}\right)^2=2+2\sqrt{2}\cdot\sqrt{3}+3=5+2\sqrt{6},$$

which is an equality with only one square root (a sign of progress). Subtracting 5 from this equality (in order to "isolate" this remaining square root), we obtain $w^2-5=2\sqrt{6}$. If we now square this equality, then we obtain $\left(w^2-5\right)^2=\left(2\sqrt{6}\right)^2=24$. At this point all square roots are gone, and we are left with an equality that contains rational numbers and w only! We can further rewrite it as $\left(w^2-5\right)^2-24=0$. Thus, w is a root of the polynomial $f(x):=\left(x^2-5\right)^2-24=x^4-10x^2+1$. This means that w is algebraic (since f is nonzero).

Let us try a more complicated example: Let z be the number $\sqrt{2}+\sqrt[3]{2}$. Is z algebraic? The squaring trick no longer works, since squaring $\sqrt{2}+\sqrt[3]{2}$ does not reduce the number of radicals (= root signs). Let's instead try rewriting $z=\sqrt{2}+\sqrt[3]{2}$ as $z-\sqrt{2}=\sqrt[3]{2}$. Cubing this equality, we obtain $\left(z-\sqrt{2}\right)^3=2$. In view of

$$\left(z-\sqrt{2}\right)^3=z^3-3z^2\sqrt{2}+3z\left(\sqrt{2}\right)^2-\left(\sqrt{2}\right)^3$$

(this is a particular case of the identity $(a-b)^3 = a^3 - 3a^2b + 3ab^2 - b^3$, which is one form of the Binomial Theorem for exponent 3), this rewrites a

$$z^3 - 3z^2\sqrt{2} + 3z\left(\sqrt{2}\right)^2 - \left(\sqrt{2}\right)^3 = 2.$$

This simplifies to

$$z^3 - 3\sqrt{2}z^2 + 6z - 2\sqrt{2} = 2.$$

Let us transform this inequality in such a way that all terms with a $\sqrt{2}$ in them end up on the right hand side while all the remaining terms end up on the left. We thus obtain

$$z^3 + 6z - 2 = \sqrt{2}\left(3z^2 + 2\right).$$

Now, squaring this equality yields

$$\left(z^3 + 6z - 2\right)^2 = 2\left(3z^2 + 2\right)^2.$$

Hence, z is a root of the polynomial

$$g(x) := \left(x^3 + 6x - 2\right)^2 - 2\left(3x^2 + 2\right)^2 = x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4.$$

This is a nonzero polynomial with rational coefficients; hence, z is algebraic.

We thus have verified that the sum of two algebraic numbers is algebraic in two cases. What about more complicated cases, such as

$$\sqrt{2} + \sqrt{3} + \sqrt[7]{11}\ ?$$

This is a sum of two algebraic numbers (since we already know that $\sqrt{2} + \sqrt{3} = w$ is algebraic). Is it algebraic? Neither of our above two methods properly works here; do we have to come up with new ad-hoc tricks? □

1.6. Motivation: Shamir's Secret Sharing Scheme

1.6.1. The problem

Adi Shamir is one of the founders of modern mathematical cryptography (famous in particular for the RSA cryptosystem, which we will discuss in Subsection 3.8.1).

Shamir's Secret Sharing Scheme is a way in which a secret **a** (a piece of data – e.g., nuclear launch codes) can be distributed among n people in such a way that

- any k of them can (if they come together) reconstruct it uniquely, but
- any $k-1$ of them (if they come together) cannot gain **any** insight about it (i.e., not only cannot they reconstruct it, but they cannot even tell that some values are more likely than others to be **a**).

Here n and k are fixed positive integers.

Understanding this scheme completely will require some abstract algebra, but we can already start thinking about the problem and get reasonably far.

So we have n people $1, 2, \ldots, n$, a positive integer $k \in \{1, 2, \ldots, n\}$ and a secret piece of data $\mathbf{a}$. We assume that this data $\mathbf{a}$ is encoded as a *bitstring* – i.e., a finite sequence of bits. A *bit* is an element of the set $\{0, 1\}$. Thus, examples of bitstrings are $(0, 1, 1, 0)$ and $(1, 0)$ and $(1, 1, 0, 1, 0, 0, 0)$ as well as the empty sequence $()$. When writing bitstring, we shall usually omit both the commas and the parentheses; thus, e.g., the bitstring $(1, 1, 0, 1, 0, 0, 0)$ will become 1101000. Make sure you don't mistake it for a number. Our goal is to give each of the n people $1, 2, \ldots, n$ some bitstring in such a way that:

- *Requirement 1:* Any k of the n people can (if they come together) reconstruct $\mathbf{a}$ uniquely.
- *Requirement 2:* Any $k - 1$ of the n people are unable to gain any insight about $\mathbf{a}$ (even if they collaborate).

We denote the bitstrings given to the people $1, 2, \ldots, n$ by $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$, respectively.

We assume that the length of our secret bitstring $\mathbf{a}$ is known in advance to all parties; i.e., it is not a secret. Thus, when we say "$k - 1$ persons cannot gain any insight about $\mathbf{a}$", we do not mean that they don't know the length; and when we say "some values are more likely than others to be $\mathbf{a}$", we only mean values that fit this length.

1.6.2. The $k = 1$ case

One simple special case of our problem is when $k = 1$. In this case, it suffices to give each of the n people the full secret $\mathbf{a}$ (that is, we set $\mathbf{a}_i = \mathbf{a}$ for all i). Then, Requirement 1 is satisfied (since any 1 of the n people already knows $\mathbf{a}$), while Requirement 2 is satisfied as well (0 people know nothing).

1.6.3. The $k = n$ case: what doesn't work

Let us now consider the case when $k = n$. This case will not help us solve the general problem, but it will show some ideas that we will encounter again and again in abstract algebra.

We want to ensure that all n people needed to reconstruct the secret $\mathbf{a}$, while any $n - 1$ of them will be completely clueless.

It sounds reasonable to split $\mathbf{a}$ into n parts, and give each person one of these parts[2] (i.e., we let $\mathbf{a}_i$ be the i-th part of $\mathbf{a}$ for each $i \in \{1, 2, \ldots, n\}$). This method satisfies Requirement 1 (indeed, all n people together can reconstruct $\mathbf{a}$ simply by

[2] assuming that $\mathbf{a}$ is long enough for that

fusing the n parts back together), but fails Requirement 2 (indeed, any $n-1$ people know $n-1$ parts of the secret $\mathbf{a}$, which is a far from being clueless about $\mathbf{a}$). So this method doesn't work. It is not that easy.

1.6.4. The XOR operations

One way to solve the $k=n$ case is using the XOR operation.

Let us first define some basic language. A *binary operation* on a set S is (informally speaking) a function that takes two elements of S and assigns a new element of S to them. More formally:

Definition 1.6.1. A *binary operation* on a set S is a map f from $S \times S$ to S. When f is a binary operation on S and a and b are two elements of S, we shall write afb for the value $f(a,b)$.

Example 1.6.2. Addition, subtraction and multiplication of integers are three binary operations on the set $\mathbb{Q}$ (the set of all rational numbers). For example, addition is the map from $\mathbb{Q} \times \mathbb{Q}$ to $\mathbb{Q}$ that sends each pair $(a,b) \in \mathbb{Q} \times \mathbb{Q}$ to $a+b$.

Division is not a binary operation on the set $\mathbb{Q}$. Indeed, if it was, then it would send the pair $(1,0)$ to some integer called $1/0$; but there is no such integer.

There are myriad more complicated binary operations around waiting for someone to name them. For example, you could define a binary operation ☺ on the set $\mathbb{Q}$ by $a☺b = \dfrac{a-b}{1+a^2+b^2}$. Indeed, you can do this because $1+a^2+b^2$ is always nonzero when $a,b \in \mathbb{Q}$ (after all, squares are nonnegative, so that $1+\underbrace{a^2}_{\geq 0}+\underbrace{b^2}_{\geq 0} \geq 1 > 0$). I am not saying that you should...

Now, we define some specific binary operations on the set $\{0,1\}$ of all bits, and on the set $\{0,1\}^n$ of all length-n bitstrings (for a given n).

Definition 1.6.3. We define a binary operation XOR on the set $\{0,1\}$ by setting

$$0 \operatorname{XOR} 0 = 0,$$
$$0 \operatorname{XOR} 1 = 1,$$
$$1 \operatorname{XOR} 0 = 1,$$
$$1 \operatorname{XOR} 1 = 0.$$

This is a valid definition, because there are only four pairs $(a,b) \in \{0,1\} \times \{0,1\}$, and we have just defined $a \operatorname{XOR} b$ for each of these four options. We can also rewrite this definition as follows:

$$a \operatorname{XOR} b = \begin{cases} 1, & \text{if } a \neq b; \\ 0, & \text{if } a = b \end{cases} = \begin{cases} 1, & \text{if } \textbf{exactly} \text{ one of } a \text{ and } b \text{ is } 1; \\ 0, & \text{otherwise.} \end{cases}$$

For lack of a better name, we refer to $a \operatorname{XOR} b$ as the "XOR of a and b".

The name "XOR" is short for "exclusive or". In fact, if you identify bits with boolean truth values (so the bit 0 stands for "False" and the bit 1 stands for "True"), then $a \operatorname{XOR} b$ is precisely the truth value for "exactly one of a and b is True", which is also known as "a exclusive-or b".

Definition 1.6.4. Let m be a nonnegative integer. We define a binary operation XOR on the set $\{0,1\}^m$ (this is the set of all length-m bitstrings) by

$$(a_1, a_2, \ldots, a_m) \operatorname{XOR} (b_1, b_2, \ldots, b_m) = (a_1 \operatorname{XOR} b_1, a_2 \operatorname{XOR} b_2, \ldots, a_m \operatorname{XOR} b_m).$$

In other words, if $\mathbf{a}$ and $\mathbf{b}$ are two length-m bitstrings, then $\mathbf{a} \operatorname{XOR} \mathbf{b}$ is obtained by taking the XOR of each entry of $\mathbf{a}$ with the corresponding entry of $\mathbf{b}$, and packing these m XORs into a new length-m bitstring.

For example,

$$\begin{aligned}
(1001) \operatorname{XOR} (1100) &= 0101; \\
(11011) \operatorname{XOR} (10101) &= 01110; \\
(11010) \operatorname{XOR} (01011) &= 10001; \\
(1) \operatorname{XOR} (0) &= 1; \\
() \operatorname{XOR} () &= ().
\end{aligned}$$

Note that if $\mathbf{a}$ and $\mathbf{b}$ are two length-m bitstrings, then the 0's in the bitstring $\mathbf{a} \operatorname{XOR} \mathbf{b}$ are at the positions where $\mathbf{a}$ and $\mathbf{b}$ have equal entries, and the 1's in $\mathbf{a} \operatorname{XOR} \mathbf{b}$ are at the positions where $\mathbf{a}$ and $\mathbf{b}$ have different entries. Thus, $\mathbf{a} \operatorname{XOR} \mathbf{b}$ essentially pinpoints the differences between $\mathbf{a}$ and $\mathbf{b}$.

We observe the following simple properties of these operations XOR on bits and on bitstrings[3]:

- We have $a \operatorname{XOR} 0 = a$ for any bit a. (This can be trivially checked by considering both possibilities for a.)
- Thus, $\mathbf{a} \operatorname{XOR} \mathbf{0} = \mathbf{a}$ for any bitstring $\mathbf{a}$, where $\mathbf{0}$ denotes the bitstring $00 \cdots 0 = (0, 0, \ldots, 0)$ (of appropriate length – i.e., of the same length as $\mathbf{a}$).
- We have $a \operatorname{XOR} a = 0$ for any bit a. (This can be trivially checked by considering both possibilities for a.)
- Thus, $\mathbf{a} \operatorname{XOR} \mathbf{a} = \mathbf{0}$ for any bitstring $\mathbf{a}$. We shall refer to this as the *self-cancellation law*.
- We have $a \operatorname{XOR} b = b \operatorname{XOR} a$ for any bits a, b. (Again, this is easy to check by going through all four options for a and b.)

[3] As a mnemonic, we shall try to use boldfaced letters like $\mathbf{a}$ and $\mathbf{b}$ for bitstrings and regular italic letters like a and b for single bits.

- Thus, $\mathbf{a} \operatorname{XOR} \mathbf{b} = \mathbf{b} \operatorname{XOR} \mathbf{a}$ for any bitstrings $\mathbf{a}, \mathbf{b}$.
- We have $a \operatorname{XOR} (b \operatorname{XOR} c) = (a \operatorname{XOR} b) \operatorname{XOR} c$ for any bits a, b, c. (Again, this is easy to check by going through all eight options for a, b, c.)
- Thus, $\mathbf{a} \operatorname{XOR} (\mathbf{b} \operatorname{XOR} \mathbf{c}) = (\mathbf{a} \operatorname{XOR} \mathbf{b}) \operatorname{XOR} \mathbf{c}$ for any bitstrings $\mathbf{a}, \mathbf{b}, \mathbf{c}$.
- Thus, for any bitstrings $\mathbf{a}$ and $\mathbf{b}$, we have

  $$(\mathbf{a} \operatorname{XOR} \mathbf{b}) \operatorname{XOR} \mathbf{b} = \mathbf{a} \operatorname{XOR} \underbrace{(\mathbf{b} \operatorname{XOR} \mathbf{b})}_{\substack{=\mathbf{0} \\ \text{(by the self-cancellation law)}}} = \mathbf{a} \operatorname{XOR} \mathbf{0} = \mathbf{a}.$$

  This observation gives rise to a primitive cryptosystem (known as a *one-time pad*): If you have a secret bitstring $\mathbf{a}$ that you want to encrypt, and another secret bitstring $\mathbf{b}$ that can be used as a key, then you can encrypt $\mathbf{a}$ by XORing it with $\mathbf{b}$ (that is, you transform it into $\mathbf{a} \operatorname{XOR} \mathbf{b}$). Then, you can decrypt it again by XORing it with $\mathbf{b}$ again; indeed, if you do this, you will obtain $(\mathbf{a} \operatorname{XOR} \mathbf{b}) \operatorname{XOR} \mathbf{b} = \mathbf{a}$. This is a highly safe cryptosystem as long as you can safely communicate the key $\mathbf{b}$ to whomever needs to be able to decrypt (or encrypt) your secrets, and as long as you are able to generate uniformly random keys $\mathbf{b}$ of sufficient length. Its only weakness is its impracticality (in many situations): If the secret you want to encrypt is long (say, a whole book), your key will need to be equally long. Even storing such keys can become difficult.

We shall refer to the properties $a \operatorname{XOR} b = b \operatorname{XOR} a$ and $\mathbf{a} \operatorname{XOR} \mathbf{b} = \mathbf{b} \operatorname{XOR} \mathbf{a}$ as *laws of commutativity*, and we shall refer to the properties $a \operatorname{XOR} (b \operatorname{XOR} c) = (a \operatorname{XOR} b) \operatorname{XOR} c$ and $\mathbf{a} \operatorname{XOR} (\mathbf{b} \operatorname{XOR} \mathbf{c}) = (\mathbf{a} \operatorname{XOR} \mathbf{b}) \operatorname{XOR} \mathbf{c}$ as *laws of associativity*. These are, of course, similar to well-known facts like $\alpha + \beta = \beta + \alpha$ and $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for numbers α, β, γ (which is why we are giving them the same names). This similarity is not coincidental. Just as for addition or multiplication of numbers, these laws lead to a notion of "XOR-products":

Proposition 1.6.5. Let m be a positive integer. Let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m$ be m bitstrings. Then, the "XOR-product" expression

$$\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3 \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_m$$

is well-defined, in the sense that it does not depend on the parenthesization.

What do we mean by "parenthesization"? To clarify things, let us set $m = 4$. In this case, we want to make sense of the expression $\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4$. This expression does not make sense a priori, since it is a XOR of **four** bitstrings, whereas we have defined only the XOR of **two** bitstrings. But there are five ways to put parentheses around some of its sub-expressions such that the expression becomes meaningful:

$$\begin{gathered}(\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2) \operatorname{XOR} (\mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4)\,, \\ ((\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2) \operatorname{XOR} \mathbf{a}_3) \operatorname{XOR} \mathbf{a}_4, \\ \mathbf{a}_1 \operatorname{XOR} ((\mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3) \operatorname{XOR} \mathbf{a}_4)\,, \\ \mathbf{a}_1 \operatorname{XOR} (\mathbf{a}_2 \operatorname{XOR} (\mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4))\,, \\ (\mathbf{a}_1 \operatorname{XOR} (\mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3)) \operatorname{XOR} \mathbf{a}_4.\end{gathered}$$

Each of these five parenthesizations (= placements of parentheses) turns our expression $\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4$ into a combination of XOR's of **two** bitstrings each, and thus gives it meaning. The question is: Do these five parenthesizations give it the **same** meaning?

Well, let us calculate:

$$\begin{aligned}&(\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2) \operatorname{XOR} (\mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4) \\ &= \mathbf{a}_1 \operatorname{XOR} \underbrace{(\mathbf{a}_2 \operatorname{XOR} (\mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4))}_{=(\mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3) \operatorname{XOR} \mathbf{a}_4} \\ &= \mathbf{a}_1 \operatorname{XOR} ((\mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3) \operatorname{XOR} \mathbf{a}_4) \\ &= \underbrace{(\mathbf{a}_1 \operatorname{XOR} (\mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3))}_{=(\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2) \operatorname{XOR} \mathbf{a}_3} \operatorname{XOR} \mathbf{a}_4 \\ &= ((\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2) \operatorname{XOR} \mathbf{a}_3) \operatorname{XOR} \mathbf{a}_4,\end{aligned}$$

where we used the law of associativity in each step. This shows that our five parenthesizations yield the same result. Thus, they all give our "XOR-product" expression $\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4$ the same meaning; so we can say that this expression is well-defined. This confirms Proposition 1.6.5 for $m = 4$.

Of course, proving Proposition 1.6.5 is less simple. Such a proof appears in Exercise 4 on homework set #0 (for more general binary operations than XOR).

1.6.5. The $k = n$ case: an answer

Let us now return to our problem. We have n persons $1, 2, \ldots, n$ and a secret $\mathbf{a}$ (encoded as a bitstring). We want to give each person i some bitstring $\mathbf{a}_i$ such that only all n of them can recover $\mathbf{a}$ but any $n-1$ of them cannot gain any insight about $\mathbf{a}$.

We let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{n-1}$ be $n-1$ **uniformly** random bitstrings of the same length as $\mathbf{a}$. (Think of them as random gibberish.) Set

$$\mathbf{a}_n = \mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_{n-1}.$$

(This expression makes sense because of Proposition 1.6.5.)

Then,

$$\begin{aligned}
&\mathbf{a}_n \operatorname{XOR} \mathbf{a}_{n-1} \operatorname{XOR} \mathbf{a}_{n-2} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_1 \\
&= (\mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_{n-1}) \operatorname{XOR} \mathbf{a}_{n-1} \operatorname{XOR} \mathbf{a}_{n-2} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_1 \\
&= \mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \underbrace{\mathbf{a}_{n-1} \operatorname{XOR} \mathbf{a}_{n-1}}_{=\mathbf{0}} \operatorname{XOR} \mathbf{a}_{n-2} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_1 \\
&= \mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \underbrace{\mathbf{a}_{n-2} \operatorname{XOR} \mathbf{0}}_{=\mathbf{a}_{n-2}} \operatorname{XOR} \mathbf{a}_{n-2} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_1 \\
&= \mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \underbrace{\mathbf{a}_{n-2} \operatorname{XOR} \mathbf{a}_{n-2}}_{=\mathbf{0}} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_1 \\
&= \cdots \\
&= \mathbf{a}
\end{aligned}$$

(here, we have been unravelling the big XOR-product from the middle on, by cancelling equal bitstrings using the self-cancellation law and then removing the resulting $\mathbf{0}$ using the $\mathbf{a} \operatorname{XOR} \mathbf{0} = \mathbf{a}$ law). Hence, the n people together can decrypt the secret $\mathbf{a}$.

Can $n-1$ people gain any insight about it? The $n-1$ people $1, 2, \ldots, n-1$ certainly cannot, since all they know are the random bitstrings $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{n-1}$. But the $n-1$ people $2, 3, \ldots, n$ cannot gain any insight about $\mathbf{a}$ either: In fact, all they know are the random bitstrings $\mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_{n-1}$ and the bitstring

$$\mathbf{a}_n = \mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_{n-1};$$

therefore, all the information they have about $\mathbf{a}$ and $\mathbf{a}_1$ comes to them through $\mathbf{a} \operatorname{XOR} \mathbf{a}_1$, which says nothing about $\mathbf{a}$ as long as they know nothing about $\mathbf{a}_1$. (We used a bit of handwaving in this argument, but then again we never formally defined what it means to "gain no insight"; this is done in courses on cryptography and information theory.) Similar arguments show that any other choice of $n-1$ persons remains equally clueless about $\mathbf{a}$. So we have solved the problem in the case $k = n$.

1.6.6. The $k = 2$ case

The next simple case is when $k = 2$. So we want to ensure that any 2 of our n people can together recover the secret, but no 1 person can learn anything about it alone.

A really nice approach was suggested by Nathan (a student in class): We pick n random bitstrings $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{n-1}$ of the same length as $\mathbf{a}$. Set

$$\mathbf{x}_n = \mathbf{a} \operatorname{XOR} \mathbf{x}_1 \operatorname{XOR} \mathbf{x}_2 \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{x}_{n-1};$$

thus, as in the $k = n$ case, we have

$$\mathbf{x}_n \operatorname{XOR} \mathbf{x}_{n-1} \operatorname{XOR} \mathbf{x}_{n-2} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{x}_1 = \mathbf{a}. \tag{2}$$

Each person i now receives the bitstring

$$\mathbf{a}_i = \mathbf{x}_1 \mathbf{x}_2 \cdots \mathbf{x}_{i-1} \mathbf{x}_{i+1} \mathbf{x}_{i+2} \cdots \mathbf{x}_n,$$

where the product stands for *concatenation* (i.e., the bitstring $\mathbf{a}_i$ is formed by writing down all of the bitstrings $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ one after the other but skipping $\mathbf{x}_i$). Thus, each person i can recover all the $n-1$ bitstrings $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, \mathbf{x}_{i+2}, \ldots, \mathbf{x}_n$ (because their lengths are the length of $\mathbf{a}$, which is known), but knows nothing about $\mathbf{x}_i$ (his "blind spot"). Hence, 2 people together can recover all the n bitstrings $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ and therefore recover the secret $\mathbf{a}$ (by (2)). On the other hand, each single person has no insight about $\mathbf{a}$ (this is proven similarly to the $k = n$ case). So again, the problem is solved in this case.

1.6.7. The $k = 3$ case

Now, let us come to the case when $k = 3$. Here, I think, the usefulness of the XOR approach has come to its end: at least, I don't know how to make it work here. Instead, out of the blue, I will invoke something completely different: polynomials (let's say with rational coefficients).

Recall a fact you might have heard in high school:

Proposition 1.6.6. A polynomial $\mathbf{f}(x) = cx^2 + bx + a$ of degree ≤ 2 is uniquely determined by any three of its values. More precisely: If u, v, w are three fixed distinct numbers, then a polynomial $\mathbf{f}(x) = cx^2 + bx + a$ of degree ≤ 2 is uniquely determined by the values $\mathbf{f}(u), \mathbf{f}(v), \mathbf{f}(w)$.

More precisely: If u, v, w are three fixed distinct numbers, and if p, q, r are three arbitrary numbers, then there is a unique polynomial $\mathbf{f}(x) = cx^2 + bx + a$ of degree ≤ 2 satisfying

$$\mathbf{f}(u) = p, \qquad \mathbf{f}(v) = q, \qquad \text{and} \qquad \mathbf{f}(w) = r.$$

Here, the word "number" is deliberately left ambiguous, but you can think of rational or real numbers (Proposition 1.6.6 is definitely true for them).

Also recall that any bitstring of given length N can be encoded as an integer in $\{0, 1, \ldots, 2^N - 1\}$: Just read it as a number in binary. More precisely, any bitstring $a_{N-1} a_{N-2} \cdots a_0$ of length N becomes the integer $a_{N-1} \cdot 2^{N-1} + a_{N-2} \cdot 2^{N-2} + \cdots + a_0 \cdot 2^0 \in \{0, 1, \ldots, 2^N - 1\}$. For example, the bitstring 010110 of length 6 becomes the integer

$$0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 22 \in \left\{0, 1, \ldots, 2^6 - 1\right\}.$$

Choose two **uniformly random** bitstrings $\mathbf{c}$ and $\mathbf{b}$ (of the same length as $\mathbf{a}$) and encode them as numbers c and b (as just explained). Encode the secret $\mathbf{a}$ as a number a as well (in the same way). Define the polynomial $\mathbf{f}(x) = cx^2 + bx + a$.

Reveal to each person $i \in \{1, 2, \ldots, n\}$ the value $\mathbf{f}(i)$ – or, rather, a bitstring that encodes it in binary – as $\mathbf{a}_i$.

Any three of the n values $\mathbf{f}(i)$ uniquely determine the polynomial $\mathbf{f}$ (because of Proposition 1.6.6). Thus, any three people can use their bitstrings $\mathbf{a}_i$ to recover three values $\mathbf{f}(i)$ and therefore $\mathbf{f}$ and therefore a (as the constant term of $\mathbf{f}$) and therefore $\mathbf{a}$ (by decoding a). So our method satisfies Requirement 1.

Now, let us see whether it satisfies Requirement 2. Any 2 people can recover two values $\mathbf{f}(i)$, which generally do not determine $\mathbf{f}$ uniquely. It is not hard to show that they do not even determine a uniquely; thus, they do not determine $\mathbf{a}$ uniquely. What's better: If you know just two values of $\mathbf{f}$, there are infinitely many possible choices for $\mathbf{f}$, and all of them have distinct constant terms (unless one of the two values you know is $\mathbf{f}(0)$, which of course pins down the constant term)[4]. So we get infinitely many possible values for a, and thus infinitely many possible values for $\mathbf{a}$. This means that our 2 people don't gain any insight about $\mathbf{a}$, right?

Not so fast! We cannot really have "infinitely many possible values for $\mathbf{a}$", since $\mathbf{a}$ is bound to be a bitstring of a given length – there are only finitely many of those! You can only get infinitely many possible values for $\mathbf{f}$ if you forget how $\mathbf{f}$ was constructed (from c, b and a) and pretend that $\mathbf{f}$ is just a "uniformly random" polynomial (whatever this means). But no one can force the 2 people to do this; it is certainly not in their interest! Here are some things they might do with this knowledge:

- Let N be the length of $\mathbf{a}$ (which, as we said, is known). Thus, $\mathbf{c}$ and $\mathbf{b}$ are bitstrings of length N, so that c and b are integers in $\{0, 1, \ldots, 2^N - 1\}$. Assume that one of the 2 people is person 2. Now, person 2 knows $\mathbf{f}(2) = c2^2 + b2 + a = 4c + 2b + a$, and thus knows whether a is even or odd (because a is even resp. odd if and only if $4c + 2b + a$ is even resp. odd). This means she knows the last bit of the secret $\mathbf{a}$. This is not "clueless".

- You might try to fix this by picking c and b to be uniformly random rational numbers instead (rather than using uniformly random bitstrings $\mathbf{c}$ and $\mathbf{b}$).

  Unfortunately, there is no such thing as a "uniformly random rational number" (in the sense that, e.g., larger numbers aren't less likely to be picked than smaller numbers). Any probability distribution will make some numbers more likely than others, and this will usually cause information about $\mathbf{a}$ to "leak". For example, if c and b are chosen from the interval $[0, 2^N - 1]$, then person 1's knowledge of $\mathbf{f}(1) = c1^2 + b1 + a = c + b + a$ will sometimes reveal to person 1 that $a \geq 0.5 \cdot (2^N - 1)$ (namely, this will happen when $\mathbf{f}(1) \geq 2.5 \cdot (2^N - 1)$, which occasionally happens). This, again, is nontrivial information about the secret $\mathbf{a}$, which a single person (or even two people) should not be having.

[4] Prove this! (**Hint:** The constant term of a polynomial is just its value at 0. Thus, if you know two values of $\mathbf{f}$ at points other than 0 and also the constant term of $\mathbf{f}$, then you simply know three values of $\mathbf{f}$.)

So we cannot make Requirement 2 hold, and the culprit is that there are too many numbers (namely, infinitely many). What would help is a finite "number system" in which we can add, subtract, multiply and divide (so that we can define polynomials over it, and a polynomial of degree ≤ 2 is still uniquely determined by any 3 values). Assuming that this "number system" is large enough that we can encode bitstrings using "numbers" of this system (instead of integers), we can then play the above game using this "number system" and obtain actually uniformly random numbers.

It turns out that such "number systems" exist. They are called *finite fields*, and we will construct them later in this course.

Assuming that they can be constructed, we thus obtain a method of solving the problem for $k = 3$. A similar method works for arbitrary k, using polynomials of degree $\leq k - 1$. This is called *Shamir's Secret Sharing Scheme*.

2. Elementary number theory

Let us now begin a systematic introduction to algebra. We start with studying integers and their divisibility properties – the beginnings of number theory. Part of these will be used directly in what will follow; part of these will inspire more general results and proofs.

2.1. Notations

Definition 2.1.1. Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ be the set of **nonnegative** integers.

Let $\mathbb{P} = \{1, 2, 3, \ldots\}$ be the set of **positive** integers.

Let $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ be the set of integers.

Let $\mathbb{Q}$ be the set of rational numbers.

Let $\mathbb{R}$ be the set of real numbers.

Be careful with the notation $\mathbb{N}$: While I use it for $\{0, 1, 2, \ldots\}$, various other authors use it for $\{1, 2, 3, \ldots\}$ instead. There is no consensus in sight on what $\mathbb{N}$ should mean.

Same holds for the word "natural number" (which I will avoid): It means "element of $\mathbb{N}$", so again its ultimate meaning depends on the author.

The word "list" shall always mean "ordered finite list" unless declared otherwise. Examples of lists of numbers are $(2, 5, 2)$, $(1, 9)$, the one-entry list (9) (not the same as the number 9 itself) and the empty list $()$. The word "tuple" means the same as "list", but more specifically, the word "k-tuple" (for some $k \in \mathbb{N}$) means "list with exactly k entries". For instance, $(5, 1, 5)$ is a 3-tuple. The word "sequence" means an ordered, but not necessarily finite, list.

2.2. Divisibility

We now go through the basics of divisibility of integers.

Definition 2.2.1. Let a and b be two integers. We say that $a \mid b$ (or "*a divides b*" or "b is *divisible by a*" or "b is a *multiple* of a") if there exists an integer c such that $b = ac$.

We furthermore say that $a \nmid b$ if a does not divide b.

Some authors define the "divisibility" relation a bit differently, in that they forbid $a = 0$. From the viewpoint of abstract algebra, this feels like an unnecessary exception, so we don't follow them.

Example 2.2.2. **(a)** We have $4 \mid 12$, since $12 = 4 \cdot 3$.

(b) We have $a \mid 0$ for any $a \in \mathbb{Z}$, since $0 = a \cdot 0$.

(c) An integer b satisfies $0 \mid b$ only when $b = 0$, since $0 \mid b$ implies $b = 0c = 0$ (for some $c \in \mathbb{Z}$).

(d) We have $a \mid a$ for any $a \in \mathbb{Z}$, since $a = a \cdot 1$.

(e) We have $1 \mid b$ for each $b \in \mathbb{Z}$, since $b = 1 \cdot b$.

I apologize in advance for the next proposition, in which vertical bars stand both for the "divides" relation and for the absolute value of a number. Unfortunately, both of these uses are standard notation. Confusion is possible, but hopefully will not happen often[5].

Proposition 2.2.3. Let a and b be two integers.

(a) We have $a \mid b$ if and only if $|a| \mid |b|$. (Here, "$|a| \mid |b|$" means "$|a|$ divides $|b|$".)

(b) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

(c) Assume that $a \neq 0$. Then, $a \mid b$ if and only if $\frac{b}{a} \in \mathbb{Z}$.

Before we prove this proposition, let us recall a well-known fact: We have

$$|xy| = |x| \cdot |y| \tag{3}$$

for any two integers[6] x and y. (This can be easily proven by case distinction: x is either nonnegative or negative, and so is y.)

Proof of Proposition 2.2.3. **(a)** $\Longrightarrow$:[7] Assume that $a \mid b$. Thus, there exists an integer

[5] Unfortunately, the use of vertical bars for absolute values alone suffices to generate confusion! Just think of the meaning of "$|a|\, b\, |c|$" when a, b and c are three numbers. Does it stand for "$(|a|) \cdot b \cdot (|c|)$" (where I am using parentheses to make the ambiguity disappear) or for "$|(a \cdot |b| \cdot c)|$"? If you see any expressions in my notes that allow for more than one meaningful interpretation, please let me know!

[6] or real numbers

[7] If you are unfamiliar with the shorthand notation "$\Longrightarrow$:", let me explain it. Our goal is to prove that $a \mid b$ if and only if $|a| \mid |b|$. In other words, we need to prove the equivalence $(a \mid b) \Longleftrightarrow (|a| \mid |b|)$. In order to prove this equivalence, it suffices to prove the two implications $(a \mid b) \Longrightarrow (|a| \mid |b|)$ (called the "forward implication" or the "$\Longrightarrow$ direction" of the equivalence) and $(a \mid b) \Longleftarrow (|a| \mid |b|)$ (called the "backward implication" or the "$\Longleftarrow$ direction"). The shorthand "$\Longrightarrow$:" simply marks the beginning of the proof of the forward implication; similarly, the symbol "$\Longleftarrow$:" heralds in the proof of the backward implication.

d such that $b = ad$ (by Definition 2.2.1). Consider[8] this d. We have $b = ad$ and thus $|b| = |ad| = |a| \cdot |d|$ (by (3)). Thus, there exists an integer c such that $|b| = |a| \cdot c$ (namely, $c = |d|$). In other words, $|a| \mid |b|$. This proves the "$\Longrightarrow$" direction of Proposition 2.2.3 **(a)**.

$\Longleftarrow$: Assume that $|a| \mid |b|$. Thus, there exists an integer f such that $|b| = |a| \cdot f$ (by Definition 2.2.1). Consider this f.

The definition of $|b|$ shows that $|b|$ equals either b or $-b$. In other words, $|b|$ equals either $1b$ or $(-1)\,b$ (since $b = 1b$ and $-b = (-1)\,b$). In other words, $|b| = qb$ for some $q \in \{1, -1\}$. Similarly, $|a| = ra$ for some $r \in \{1, -1\}$. Consider these q and r.

From $q \in \{1, -1\}$, we obtain $q^2 \in \left\{ \underbrace{1^2}_{=1}, \underbrace{(-1)^2}_{=1} \right\} = \{1, 1\} = \{1\}$. In other words, $q^2 = 1$.

Now, $q \underbrace{|b|}_{=qb} = \underbrace{qq}_{=q^2=1} b = b$, so that $b = q \underbrace{|b|}_{=|a|\cdot f} = q \underbrace{|a|}_{=ra} \cdot f = qra \cdot f = a \cdot qfr$. Hence, there exists an integer c such that $b = ac$ (namely, $c = qfr$). In other words, $a \mid b$ (by Definition 2.2.1). This proves the "$\Longleftarrow$" direction of Proposition 2.2.3 **(a)**.

Thus, the proof of Proposition 2.2.3 **(a)** is complete.

(b) Assume that $a \mid b$ and $b \neq 0$.

From $a \mid b$, we conclude that there exists an integer c such that $b = ac$. Consider this c. We have $ac = b \neq 0$, thus $c \neq 0$. Hence, $|c| > 0$, and thus $|c| \geq 1$ (since $|c|$ is an integer). We can multiply this inequality by $|a|$ (since $|a| \geq 0$), and obtain $|a| \cdot |c| \geq |a| \cdot 1 = |a|$.

From $b = ac$, we obtain $|b| = |ac| = |a| \cdot |c|$ (by (3)). Hence, $|b| = |a| \cdot |c| \geq |a|$. This proves Proposition 2.2.3 **(b)**.

(c) $\Longrightarrow$: Assume that $a \mid b$. We must prove that $\frac{b}{a} \in \mathbb{Z}$.

We have $a \mid b$. In other words, there exists an integer d such that $b = ad$. Consider this d. We can divide the equality $b = ad$ by a (since $a \neq 0$), and thus obtain $\frac{b}{a} = d \in \mathbb{Z}$. This proves the "$\Longrightarrow$" direction of Proposition 2.2.3 **(c)**.

$\Longleftarrow$: Assume that $\frac{b}{a} \in \mathbb{Z}$. We must prove that $a \mid b$.

We have $\frac{b}{a} \in \mathbb{Z}$ and $b = a \cdot \frac{b}{a}$. Thus, there exists an integer c such that $b = ac$ (namely, $c = \frac{b}{a}$). In other words, $a \mid b$. This proves the "$\Longleftarrow$" direction of Proposition 2.2.3 **(c)**. Hence, the proof of Proposition 2.2.3 **(c)** is complete. □

Proposition 2.2.3 **(a)** shows that both a and b in the statement "$a \mid b$" can be replaced by their absolute values. Thus, when we talk about divisibility of integers,

[8] Me saying "Consider this d" means that I am picking some integer d such that $b = ad$ (this can be done, since we have just proven that such a d exists), and will be referring to it as d from now on.

the sign of the integers does not really matter – it usually suffices to work with nonnegative integers. We will often use this (tacitly, after a while) in proofs.

The next proposition shows some basic properties of the divisibility relation:

> **Proposition 2.2.4.** **(a)** We have $a \mid a$ for every $a \in \mathbb{Z}$. (This is called the *reflexivity of divisibility*.)
>
> **(b)** If $a, b, c \in \mathbb{Z}$ satisfy $a \mid b$ and $b \mid c$, then $a \mid c$. (This is called the *transitivity of divisibility*.)
>
> **(c)** If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$, then $a_1 a_2 \mid b_1 b_2$.

Proof of Proposition 2.2.4. **(a)** Let $a \in \mathbb{Z}$. Then, $a = a \cdot 1$. Hence, there exists an integer c such that $a = ac$ (namely, $c = 1$). In other words, $a \mid a$ (by Definition 2.2.1). This proves Proposition 2.2.4 **(a)**.

(b) Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid b$ and $b \mid c$.

From $a \mid b$, we conclude that there exists an integer d such that $b = ad$ (by Definition 2.2.1). Consider this d.

From $b \mid c$, we conclude that there exists an integer e such that $c = be$ (by Definition 2.2.1). Consider this e.

We have $c = \underbrace{b}_{=ad} e = ade$. Hence, there exists an integer f such that $c = af$ (namely, $f = de$). In other words, $a \mid c$ (by Definition 2.2.1). This proves Proposition 2.2.4 **(b)**.

(c) Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$.

From $a_1 \mid b_1$, we conclude that there exists an integer d such that $b_1 = a_1 d$. Consider this d.

From $a_2 \mid b_2$, we conclude that there exists an integer e such that $b_2 = a_2 e$. Consider this e.

We have $\underbrace{b_1}_{=a_1 d} \underbrace{b_2}_{=a_2 e} = a_1 d a_2 e = a_1 a_2 de$. Hence, there exists an integer f such that $b_1 b_2 = a_1 a_2 f$ (namely, $f = de$). In other words, $a_1 a_2 \mid b_1 b_2$ (by Definition 2.2.1). This proves Proposition 2.2.4 **(c)**. □

> **Exercise 2.2.1.** Let $a \in \mathbb{Z}$.
>
> **(a)** Prove that $a \mid |a|$. (This means "a divides $|a|$".)
>
> **(b)** Prove that $|a| \mid a$. (This means "$|a|$ divides a".)

> **Exercise 2.2.2.** Let a and b be two integers such that $a \mid b$ and $b \mid a$. Prove that $|a| = |b|$.

> **Exercise 2.2.3.** Let a, b, c be three integers such that $c \neq 0$. Prove that $a \mid b$ holds if and only if $ac \mid bc$.

Exercise 2.2.4. Let $n \in \mathbb{Z}$. Let $a, b \in \mathbb{N}$ be such that $a \leq b$. Prove that $n^a \mid n^b$.

Exercise 2.2.5. Let g be a nonnegative integer such that $g \mid 1$. Prove that $g = 1$.

Exercise 2.2.6. Let $a, b \in \mathbb{Z}$ be such that $a \mid b$. Let $k \in \mathbb{N}$. Prove that $a^k \mid b^k$.

2.3. Congruence modulo n

The next definition is simple but crucial:

Definition 2.3.1. Let $n, a, b \in \mathbb{Z}$. We say that *a is congruent to b modulo n* if and only if $n \mid a - b$. We shall use the notation "$a \equiv b \mod n$" for "a is congruent to b modulo n".

We furthermore shall use the notation "$a \not\equiv b \mod n$" for "a is not congruent to b modulo n".

Example 2.3.2. **(a)** Is $3 \equiv 7 \mod 2$? Yes, since $2 \mid 3 - 7 = -4$.

(b) Is $3 \equiv 6 \mod 2$? No, since $2 \nmid 3 - 6 = -3$. So we have $3 \not\equiv 6 \mod 2$.

Now, let a and b be two integers.

(c) We have $a \equiv b \mod 0$ if and only if $a = b$. (Indeed, $a \equiv b \mod 0$ is defined to mean $0 \mid a - b$, but the latter divisibility happens only when $a - b = 0$, which is tantamount to saying $a = b$.)

(d) We have $a \equiv b \mod 1$ always, since $1 \mid a - b$ always holds (remember: 1 divides everything).

Note that being congruent modulo 2 means having the same parity: i.e., two even numbers will be congruent modulo 2, and two odd numbers will be, but an even number will never be congruent to an odd number modulo 2. (To be rigorous: This is not quite obvious at this point yet; but it will be easy once we have properly introduced division with remainder. See Exercise 2.7.1 **(i)** below for the proof.)

The word "modulo" in the phrase "a is congruent to b modulo n" originates with Gauss and means something like "with respect to". You should think of "a is congruent to b modulo n" as a relation between all three of the numbers a, b and n, but a and b are the "main characters" and n sets the scene.

Exercise 2.3.1. Let $a, b \in \mathbb{Z}$. Prove that $a + b \equiv a - b \mod 2$.

We begin with a proposition so fundamental that we will always use it without saying:

Proposition 2.3.3. Let $n \in \mathbb{Z}$ and $a \in \mathbb{Z}$. Then, $a \equiv 0 \mod n$ if and only if $n \mid a$.

Proof of Proposition 2.3.3. We have the following chain of equivalences:

$$\begin{aligned}(a \equiv 0 \mod n) &\iff (n \mid a - 0) \qquad \text{(by Definition 2.3.1)} \\ &\iff (n \mid a) \qquad (\text{since } a - 0 = a).\end{aligned}$$

This proves Proposition 2.3.3. □

Next come some staple properties of congruences:

Proposition 2.3.4. Let $n \in \mathbb{Z}$.

(a) We have $a \equiv a \mod n$ for every $a \in \mathbb{Z}$.

(b) If $a, b, c \in \mathbb{Z}$ satisfy $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.

(c) If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \mod n$, then $b \equiv a \mod n$.

(d) If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \equiv b_1 \mod n$ and $a_2 \equiv b_2 \mod n$, then

$$a_1 + a_2 \equiv b_1 + b_2 \mod n; \tag{4}$$

$$a_1 - a_2 \equiv b_1 - b_2 \mod n; \tag{5}$$

$$a_1 a_2 \equiv b_1 b_2 \mod n. \tag{6}$$

(e) Let $m \in \mathbb{Z}$ be such that $m \mid n$. If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \mod n$, then $a \equiv b \mod m$.

Proof of Proposition 2.3.4. **(a)** Let $a \in \mathbb{Z}$. Recall that $a \equiv a \mod n$ is defined to mean $n \mid a - a$. Since $n \mid a - a$ holds (because $a - a = 0 = n \cdot 0$), we thus see that $a \equiv a \mod n$ holds. This proves Proposition 2.3.4 **(a)**.

(b) Let $a, b, c \in \mathbb{Z}$ satisfy $a \equiv b \mod n$ and $b \equiv c \mod n$.

We have $a \equiv b \mod n$. In other words, $n \mid a - b$ (by Definition 2.3.1). In other words, there exists an integer p such that $a - b = np$ (by Definition 2.2.1). Consider this p.

We have $b \equiv c \mod n$. In other words, $n \mid b - c$ (by Definition 2.3.1). In other words, there exists an integer q such that $b - c = nq$ (by Definition 2.2.1). Consider this q.

Now,

$$a - c = \underbrace{(a - b)}_{=np} + \underbrace{(b - c)}_{=nq} = np + nq = n(p + q).$$

Hence, there exists an integer r such that $a - c = nr$ (namely, $r = p + q$). In other words, $n \mid a - c$ (by Definition 2.2.1). In other words, $a \equiv c \mod n$ (by Definition 2.3.1). This proves Proposition 2.3.4 **(b)**.

(c) Let $a, b \in \mathbb{Z}$ satisfy $a \equiv b \mod n$.

We have $a \equiv b \mod n$. In other words, $n \mid a - b$ (by Definition 2.3.1). In other words, there exists an integer p such that $a - b = np$ (by Definition 2.2.1). Consider this p. Now,

$$b - a = -\underbrace{(a - b)}_{=np} = -np = n(-p).$$

Hence, there exists an integer c such that $b - a = nc$ (namely, $c = -p$). In other words, $n \mid b - a$ (by Definition 2.2.1). In other words, $b \equiv a \mod n$ (by Definition 2.3.1). This proves Proposition 2.3.4 **(c)**.

(d) Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \equiv b_1 \mod n$ and $a_2 \equiv b_2 \mod n$.

We have $a_1 \equiv b_1 \mod n$. In other words, $n \mid a_1 - b_1$ (by Definition 2.3.1). In other words, there exists an integer p such that $a_1 - b_1 = np$ (by Definition 2.2.1). Consider this p.

We have $a_2 \equiv b_2 \operatorname{mod} n$. In other words, $n \mid a_2 - b_2$ (by Definition 2.3.1). In other words, there exists an integer q such that $a_2 - b_2 = nq$ (by Definition 2.2.1). Consider this q.

We have

$$(a_1 + a_2) - (b_1 + b_2) = \underbrace{(a_1 - b_1)}_{=np} + \underbrace{(a_2 - b_2)}_{=nq} = np + nq = n(p+q).$$

Hence, there exists an integer c such that $(a_1 + a_2) - (b_1 + b_2) = nc$ (namely, $c = p + q$). In other words, $n \mid (a_1 + a_2) - (b_1 + b_2)$ (by Definition 2.2.1). In other words, $a_1 + a_2 \equiv b_1 + b_2 \operatorname{mod} n$ (by Definition 2.3.1). A similar argument (using $p - q$ instead of $p + q$) shows that $a_1 - a_2 \equiv b_1 - b_2 \operatorname{mod} n$. It thus remains to show that $a_1 a_2 \equiv b_1 b_2 \operatorname{mod} n$.

Let us first show that $a_1 a_2 \equiv a_1 b_2 \operatorname{mod} n$. Indeed, $a_1 a_2 - a_1 b_2 = a_1 \underbrace{(a_2 - b_2)}_{=nq} = a_1 nq = n(a_1 q)$. Hence, there exists an integer c such that $a_1 a_2 - a_1 b_2 = nc$ (namely, $c = a_1 q$). In other words, $n \mid a_1 a_2 - a_1 b_2$ (by Definition 2.2.1). In other words, $a_1 a_2 \equiv a_1 b_2 \operatorname{mod} n$ (by Definition 2.3.1).

Next, let us show that $a_1 b_2 \equiv b_1 b_2 \operatorname{mod} n$. Indeed, $a_1 b_2 - b_1 b_2 = b_2 \underbrace{(a_1 - b_1)}_{=np} = b_2 np = n(b_2 p)$. Hence, there exists an integer c such that $a_1 b_2 - b_1 b_2 = nc$ (namely, $c = b_2 p$). In other words, $n \mid a_1 b_2 - b_1 b_2$ (by Definition 2.2.1). In other words, $a_1 b_2 \equiv b_1 b_2 \operatorname{mod} n$ (by Definition 2.3.1).

From $a_1 a_2 \equiv a_1 b_2 \operatorname{mod} n$ and $a_1 b_2 \equiv b_1 b_2 \operatorname{mod} n$, we now conclude that $a_1 a_2 \equiv b_1 b_2 \operatorname{mod} n$ (by Proposition 2.3.4 **(b)**, applied to $a = a_1 a_2$, $b = a_1 b_2$ and $c = b_1 b_2$). This completes the proof of Proposition 2.3.4 **(d)**.

(e) Let $a, b \in \mathbb{Z}$ satisfy $a \equiv b \operatorname{mod} n$.

We have $a \equiv b \operatorname{mod} n$. In other words, $n \mid a - b$ (by Definition 2.3.1). From $m \mid n$ and $n \mid a - b$, we obtain $m \mid a - b$ (by Proposition 2.2.4 **(b)**, applied to m, n and $a - b$ instead of a, b and c). In other words, $a \equiv b \operatorname{mod} m$ (by Definition 2.3.1). This proves Proposition 2.3.4 **(e)**. □

In the above proof, we took care to explicitly cite Definition 2.2.1 and Definition 2.3.1 whenever we used them; in the following, we will omit references like this.

Proposition 2.3.4 **(d)** is saying that congruences modulo n (for a fixed integer n) can be added, subtracted and multiplied together. This does not mean that you can do everything with them that you can do with equalities. The next exercise shows that dividing congruences and taking a congruence to the power of another does not generally work:

Exercise 2.3.2. Let $n, a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \equiv b_1 \operatorname{mod} n$ and $a_2 \equiv b_2 \operatorname{mod} n$. Then, **in general**, neither $a_1 / a_2 \equiv b_1 / b_2 \operatorname{mod} n$ nor $a_1^{a_2} \equiv b_1^{b_2} \operatorname{mod} n$ is necessarily true. Of course, this is partly due to the fact that a_1 / a_2, b_1 / b_2 and $a_1^{a_2}$ and $b_1^{b_2}$ are not always integers in the first place (and being congruent modulo n only makes sense for integers, at least for now). But even when a_1/a_2, b_1/b_2 and $a_1^{a_2}$ and $b_1^{b_2}$ are integers, the congruences $a_1/a_2 \equiv b_1/b_2 \mod n$ and $a_1^{a_2} \equiv b_1^{b_2} \mod n$ are often false. Find examples of n, a_1, a_2, b_1, b_2 such that a_1/a_2, b_1/b_2 and $a_1^{a_2}$ and $b_1^{b_2}$ are integers but the congruences $a_1/a_2 \equiv b_1/b_2 \mod n$ and $a_1^{a_2} \equiv b_1^{b_2} \mod n$ are false.

However, we can divide a congruence $a \equiv b \mod n$ by a nonzero integer d when all of a, b, n are divisible by d:

Exercise 2.3.3. Let $n, d, a, b \in \mathbb{Z}$, and assume that $d \neq 0$. Assume that d divides each of a, b, n, and assume that $a \equiv b \mod n$. Prove that $a/d \equiv b/d \mod n/d$.

We can also take a congruence to the k-th power when $k \in \mathbb{N}$:

Exercise 2.3.4. Let $n, a, b \in \mathbb{Z}$ be such that $a \equiv b \mod n$. Prove that $a^k \equiv b^k \mod n$ for each $k \in \mathbb{N}$.

(Note that the "n" is not being taken to the k-th power here.)
We can add not just two, but any finite number of congruences:

Exercise 2.3.5. Let n be an integer. Let S be a finite set. For each $s \in S$, let a_s and b_s be two integers. Assume that

$$a_s \equiv b_s \mod n \qquad \text{for each } s \in S. \tag{7}$$

(a) Prove that

$$\sum_{s \in S} a_s \equiv \sum_{s \in S} b_s \mod n. \tag{8}$$

(b) Prove that

$$\prod_{s \in S} a_s \equiv \prod_{s \in S} b_s \mod n. \tag{9}$$

(Keep in mind that if the set S is empty, then $\sum\limits_{s \in S} a_s = \sum\limits_{s \in S} b_s = 0$ and $\prod\limits_{s \in S} a_s = \prod\limits_{s \in S} b_s = 1$; this holds by the definition of empty sums and of empty products.)

Exercise 2.3.6. Is it true that if $a_1, a_2, b_1, b_2, n_1, n_2 \in \mathbb{Z}$ satisfy $a_1 \equiv b_1 \mod n_1$ and $a_2 \equiv b_2 \mod n_2$, then $a_1 a_2 \equiv b_1 b_2 \mod n_1 n_2$?

Exercise 2.3.7. Let $a, b, n \in \mathbb{Z}$. Prove that $a \equiv b \mod n$ if and only if there exists some $d \in \mathbb{Z}$ such that $b = a + nd$.

Exercise 2.3.8. Let $a, b, c, n \in \mathbb{Z}$. Prove that we have $a - b \equiv c \mod n$ if and only if $a \equiv b + c \mod n$.

Exercise 2.3.9. Let $a, b, n \in \mathbb{Z}$. Prove that $a \equiv b \bmod n$ if and only if $a \equiv b \bmod -n$.

2.4. Chains of congruences

Convention 2.4.1. For this whole Section 2.4, we fix an integer n.

Chains of equalities are a fundamental piece of notation used throughout mathematics. For example, here is a chain of equalities:

$$\begin{aligned}
&(ad+bc)^2 + (ac-bd)^2 \\
&= (ad)^2 + 2ad \cdot bc + (bc)^2 + (ac)^2 - 2ac \cdot bd + (bd)^2 \\
&= a^2d^2 + 2abcd + b^2c^2 + a^2c^2 - 2abcd + b^2d^2 \\
&= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\
&= \left(a^2 + b^2\right)\left(c^2 + d^2\right)
\end{aligned}$$

(where a, b, c, d are arbitrary numbers). This chain proves the equality (1). But why does it really? If we look closely at this chain of equalities, we see that it has the form "$A = B = C = D = E$", where A, B, C, D, E are five numbers (namely, $A = (ad+bc)^2 + (ac-bd)^2$ and $B = (ad)^2 + 2ad \cdot bc + (bc)^2 + (ac)^2 - 2ac \cdot bd + (bd)^2$ and so on). This kind of statement is called a "chain of equalities", and, a priori, it simply means that any two **adjacent** numbers in this chain are equal: $A = B$ and $B = C$ and $C = D$ and $D = E$. Without as much as noticing it, we have concluded that **any** two numbers in this chain are equal; thus, in particular, $A = E$, which is precisely the equality (1) we wanted to prove.

That this kind of "chaining" is possible is one of the most basic facts in mathematics. Let us define a chain of equalities formally:

Definition 2.4.2. If $a_1, a_2, \ldots, a_k$ are k objects[9], then the statement "$a_1 = a_2 = \cdots = a_k$" shall mean that

$$a_i = a_{i+1} \text{ holds for each } i \in \{1, 2, \ldots, k-1\}.$$

(In other words, it shall mean that $a_1 = a_2$ and $a_2 = a_3$ and $a_3 = a_4$ and $\cdots$ and $a_{k-1} = a_k$. This is vacuously true when $k \leq 1$. If $k = 2$, then it simply means that $a_1 = a_2$.)

Such a statement will be called a *chain of equalities*.

Proposition 2.4.3. Let $a_1, a_2, \ldots, a_k$ be k objects such that $a_1 = a_2 = \cdots = a_k$. Let u and v be two elements of $\{1, 2, \ldots, k\}$. Then, $a_u = a_v$.

[9] "Objects" can be numbers, sets, tuples or any other well-defined things in mathematics.

So we have defined a chain of equalities to be true if and only if any two adjacent terms in this chain are equal (i.e., if "each equality sign in the chain is satisfied"). Proposition 2.4.3 shows that in such a chain, **any two** terms are equal. This is intuitively rather clear, but can also be formally proven by induction using the basic properties of equality (transitivity[10], reflexivity[11] and symmetry[12]).

But our goal is to understand basic number theory, not to scrutinize the foundations of mathematics. So let us recall that we have fixed an integer n, and consider congruences modulo n. We claim that these can be chained just as equalities:

Definition 2.4.4. If $a_1, a_2, \ldots, a_k$ are k integers, then the statement "$a_1 \equiv a_2 \equiv \cdots \equiv a_k \mod n$" shall mean that

$$a_i \equiv a_{i+1} \mod n \text{ holds for each } i \in \{1, 2, \ldots, k-1\}.$$

(In other words, it shall mean that $a_1 \equiv a_2 \mod n$ and $a_2 \equiv a_3 \mod n$ and $a_3 \equiv a_4 \mod n$ and $\cdots$ and $a_{k-1} \equiv a_k \mod n$. This is vacuously true when $k \leq 1$. If $k = 2$, then it simply means that $a_1 \equiv a_2 \mod n$.)

Such a statement will be called a *chain of congruences modulo n*.

Proposition 2.4.5. Let $a_1, a_2, \ldots, a_k$ be k integers such that $a_1 \equiv a_2 \equiv \cdots \equiv a_k \mod n$. Let u and v be two elements of $\{1, 2, \ldots, k\}$. Then, $a_u \equiv a_v \mod n$.

Proposition 2.4.5 shows that any two terms in a chain of congruences modulo n must be congruent to each other modulo n. Again, this can be formally proven by induction; see [Grinbe15, proof of Proposition 2.16]. The ingredients of the proof are basic properties of congruence modulo n: transitivity, reflexivity and symmetry. These are fancy names for parts **(b)**, **(a)** and **(c)** of Proposition 2.3.4.

We will use Proposition 2.4.5 tacitly (just as you would use Proposition 2.4.3): i.e., every time we prove a chain of congruences like $a_1 \equiv a_2 \equiv \cdots \equiv a_k \mod n$, we assume that the reader will automatically conclude that any two of its terms are congruent to each other modulo n (and will remember this conclusion). For instance, if we show that $1 \equiv 4 \equiv 34 \equiv 334 \equiv 304 \mod 3$, then we automatically get the congruences $1 \equiv 304 \mod 3$ and $334 \equiv 1 \mod 3$ and $4 \equiv 334 \mod 3$ and several others out of this chain.

Chains of congruences can also include equality signs. For example, if a, b, c, d are integers, then "$a \equiv b = c \equiv d \mod n$" means that $a \equiv b \mod n$ and $b = c$ and $c \equiv d \mod n$. Such a chain is still a chain of congruences, because $b = c$ implies $b \equiv c \mod n$ (by Proposition 2.3.4 **(a)**).

Just as there are chains of equalities and chains of congruences, there are chains of divisibilities:

[10] *Transitivity of equality* says that if a, b, c are three objects satisfying $a = b$ and $b = c$, then $a = c$.

[11] *Reflexivity of equality* says that every object a satisfies $a = a$.

[12] *Symmetry of equality* says that if a, b are two objects satisfying $a = b$, then $b = a$.

Definition 2.4.6. If $a_1, a_2, \ldots, a_k$ are k integers, then the statement "$a_1 \mid a_2 \mid \cdots \mid a_k$" shall mean that

$$a_i \mid a_{i+1} \text{ holds for each } i \in \{1, 2, \ldots, k-1\}.$$

(In other words, it shall mean that $a_1 \mid a_2$ and $a_2 \mid a_3$ and $a_3 \mid a_4$ and $\cdots$ and $a_{k-1} \mid a_k$. This is vacuously true when $k \leq 1$. If $k = 2$, then it simply means that $a_1 \mid a_2$.)

Such a statement will be called a *chain of divisibilities*.

Proposition 2.4.7. Let $a_1, a_2, \ldots, a_k$ be k integers such that $a_1 \mid a_2 \mid \cdots \mid a_k$. Let u and v be two elements of $\{1, 2, \ldots, k\}$ such that $u \leq v$. Then, $a_u \mid a_v$.

Note that we had to require $u \leq v$ in this proposition, unlike the analogous propositions for chains of equalities and chains of congruences, because there is no "symmetry of divisibility" (i.e., if $a \mid b$, then we don't generally have $b \mid a$). The proof of Proposition 2.4.7 relies on the reflexivity of divisibility (Proposition 2.2.4 **(a)**) and on the transitivity of divisibility (Proposition 2.2.4 **(b)**).

Again, chains of divisibilities can include equality signs. For example, $4 \mid 3 \cdot 4 = 12 = 2 \cdot 6 \mid 4 \cdot 6 = 24$.

2.5. Substitutivity for congruences

In Section 2.4, we have learnt that congruences modulo an integer n can be chained together like equalities. A further important feature of congruences is the principle of *substitutivity for congruences*. This is yet another way in which congruences behave like equalities. We are not going to state it fully formally (as it is a metamathematical principle), but will merely explain its meaning. Later on, once we understand what the rings $\mathbb{Z}/n$ (for integer n) are, we will no longer need this principle, since it will just boil down to "equal things can be substituted for one another" (the whole point of $\mathbb{Z}/n$ is to "make congruent numbers equal"); but for now, we cannot treat "congruent modulo n" as "equal", so we have to state it.

You are probably used to making computations like these:

$$\begin{aligned}\underbrace{(a+b)^2}_{=a^2+2ab+b^2} + \underbrace{(a-b)^2}_{=a^2-2ab+b^2} &= \left(a^2 + 2ab + b^2\right) + \left(a^2 - 2ab + b^2\right) \\ &= \underbrace{a^2 + a^2}_{=2a^2} + \underbrace{b^2 + b^2}_{=2b^2} = 2a^2 + 2b^2\end{aligned}$$

(for any two numbers a and b). What is going on in these underbraces (like "$\underbrace{(a+b)^2}_{=a^2+2ab+b^2}$")? Something pretty simple is going on: You are replacing a number (in this case, $(a+b)^2$) by an equal number (in this case, $a^2 + 2ab + b^2$). This relies on a fundamental principle of mathematics (called the *principle of substitutivity for equalities*), which says that an object in an expression can indeed be replaced by any object equal to it (without changing the value of the expression). (This is also known as *Leibniz's equality law*.) To be precise, we are using this principle twice in some of our equality signs above, since we are making several replacements at the same time; but this is fine (we can just do the replacement one by one instead).

We would like to have a similar principle for congruences modulo n: We would like to be able to replace any integer by an integer congruent to it modulo n. For example, we would like to be able to say that if seven integers a, a', b, b', c, c', n satisfy $a \equiv a' \mod n$ and $b \equiv b' \mod n$ and $c \equiv c' \mod n$, then

$$\underbrace{b}_{\equiv b' \mod n} \underbrace{c}_{\equiv c' \mod n} + \underbrace{c}_{\equiv c' \mod n} \underbrace{a}_{\equiv a' \mod n} + \underbrace{a}_{\equiv a' \mod n} \underbrace{b}_{\equiv b' \mod n} \equiv b'c' + c'a' + a'b' \mod n.$$

We have to be careful with this: For example, we run into troubles if division is involved in our expressions. For example, we have $6 \equiv 9 \mod 3$, but we do not have $\underbrace{6}_{\equiv 9 \mod 3} /3 \equiv 9/3 \mod 3$. Similarly, exponentiation can be problematic. So we need to state the principle we are using here in clearer terms, so that we know what we can do.

Convention 2.5.1. For this whole Section 2.5, we fix an integer n.

The *principle of substitutivity for equalities* says the following:

> *Principle of substitutivity for equalities (PSE):* If two objects x and x' are equal, and if we have any expression A that involves the object x, then we can replace this x (or, more precisely, any arbitrary appearance of x in A) in A by x'; the value of the resulting expression A' will equal the value of A.

Here are two examples of how this principle can be used:

- If a, b, c, d, e, c' are numbers such that $c = c'$, then the PSE says that we can replace c by c' in the expression $a(b - (c+d)e)$, and the value of the resulting expression $a(b - (c'+d)e)$ will equal the value of $a(b - (c+d)e)$; that is, we have
$$a(b - (c+d)e) = a\left(b - \left(c'+d\right)e\right). \qquad (10)$$

- If a, b, c, a' are numbers such that $a = a'$, then
$$(a-b)(a+b) = \left(a'-b\right)(a+b), \qquad (11)$$
because the PSE allows us to replace the first a appearing in the expression $(a-b)(a+b)$ by an a'. (We can also replace the second a by a', of course.)

More generally, we can make several such replacements at the same time.

The PSE is one of the headstones of mathematical logic; it is the essence of what it means for two objects to be equal.

The *principle of substitutivity for congruences* is similar, but far less fundamental; it says the following:

> *Principle of substitutivity for congruences (PSC):* If two numbers x and x' are congruent to each other modulo n (that is, $x \equiv x' \bmod n$), and if we have any expression A that involves only integers, addition, subtraction and multiplication, and involves the object x, then we can replace this x (or, more precisely, any arbitrary appearance of x in A) in A by x'; the value of the resulting expression A' will be congruent to the value of A modulo n.

This principle is less general than the PSE, since it only applies to expressions that are built from integers and certain operations (note that division is not one of these operations). But it still lets us prove analogues of our above examples (10) and (11):

- If a, b, c, d, e, c' are integers such that $c \equiv c' \bmod n$, then the PSC says that we can replace c by c' in the expression $a(b-(c+d)e)$, and the value of the resulting expression $a(b-(c'+d)e)$ will be congruent to the value of $a(b-(c+d)e)$ modulo n; that is, we have

$$a(b-(c+d)e) \equiv a\left(b-\left(c'+d\right)e\right) \bmod n. \qquad (12)$$

- If a, b, c, a' are integers such that $a \equiv a' \bmod n$, then

$$(a-b)(a+b) \equiv \left(a'-b\right)(a+b) \bmod n, \qquad (13)$$

  because the PSC allows us to replace the first a appearing in the expression $(a-b)(a+b)$ by an a'. (We can also replace the second a by a', of course.)

We shall not prove the PSC, since we have not formalized it (after all, we have not defined what an "expression" is). But we shall prove the specific congruences (12) and (13) using Proposition 2.3.4; the way in which we prove these congruences is symptomatic: Every congruence obtained from the PSC can be proven in a manner like these. Thus, the proofs of (12) and (13) given below can serve as templates which can easily be adapted to any other situation in which an application of the PSC needs to be justified.

Proof of (12). Let a, b, c, d, e, c' be integers such that $c \equiv c' \bmod n$.

Adding the congruence[13] $c \equiv c' \bmod n$ with the congruence $d \equiv d \bmod n$ (which follows from Proposition 2.3.4 **(a)**), we obtain $c+d \equiv c'+d \bmod n$. Multiplying

[13] Proposition 2.3.4 **(d)** shows that we can add, subtract and multiply congruences modulo n at will. We are using this freedom here and will use it many times below.

this congruence with the congruence $e \equiv e \mod n$ (which follows from Proposition 2.3.4 **(a)**), we obtain $(c+d)\,e \equiv (c'+d)\,e \mod n$. Subtracting this congruence from the congruence $b \equiv b \mod n$ (which, again, follows from Proposition 2.3.4 **(a)**), we obtain $b-(c+d)\,e \equiv b-(c'+d)\,e \mod n$. Multiplying the congruence $a \equiv a \mod n$ (which follows from Proposition 2.3.4 **(a)**) with this congruence, we obtain $a\,(b-(c+d)\,e) \equiv a\,(b-(c'+d)\,e) \mod n$. This proves (12). □

Proof of (13). Let a, b, c, a' be integers such that $a \equiv a' \mod n$.

Subtracting the congruence $b \equiv b \mod n$ (which follows from Proposition 2.3.4 **(a)**) from the congruence $a \equiv a' \mod n$, we obtain $a-b \equiv a'-b \mod n$. Multiplying this congruence with the congruence $a+b \equiv a+b \mod n$ (which follows from Proposition 2.3.4 **(a)**), we obtain $(a-b)\,(a+b) \equiv (a'-b)\,(a+b) \mod n$. This proves (13). □

As we said, these two proofs are exemplary: Any congruence obtained from the PSC can be proven in such a way (starting with the congruence $x \equiv x' \mod n$, and then "wrapping" it up in the expression A by repeatedly adding, multiplying and subtracting congruences that follow from Proposition 2.3.4 **(a)**).

When we apply the PSC, we shall use underbraces to point out which integers we are replacing. For example, when deriving (12) from this principle, we shall write

$$a\left(b-\left(\underbrace{c}_{\equiv c' \mod n}+d\right)e\right) \equiv a\left(b-\left(c'+d\right)e\right) \mod n,$$

in order to stress that we are replacing c by c'. Likewise, when deriving (13) from the PSC, we shall write

$$\left(\underbrace{a}_{\equiv a' \mod n}-b\right)(a+b) \equiv \left(a'-b\right)(a+b) \mod n,$$

in order to stress that we are replacing the first a (but not the second a) by a'.

The PSC allows us to replace a **single** integer x appearing in an expression by another integer x' that is congruent to x modulo n. Applying this principle many times, we thus conclude that we can also replace **several** integers at the same time (because we can get to the same result by performing these replacements one at a time, and Proposition 2.4.5 shows that the value of the final result will be congruent to the value of the original result). For example, if seven integers a, a', b, b', c, c', n satisfy $a \equiv a' \mod n$ and $b \equiv b' \mod n$ and $c \equiv c' \mod n$, then

$$bc+ca+ab \equiv b'c'+c'a'+a'b' \mod n, \qquad (14)$$

because we can replace all the six integers b, c, c, a, a, b in the expression $bc+ca+ab$ (listed in the order of their appearance in this expression) by b', c', c', a', a', b', respectively. If we want to derive this from the PSC, then we must perform the replacements one at a time, e.g., as follows:

$$\begin{aligned}\underbrace{b}_{\equiv b' \bmod n} c + ca + ab &\equiv b' \underbrace{c}_{\equiv c' \bmod n} + ca + ab \equiv b'c' + \underbrace{c}_{\equiv c' \bmod n} a + ab \\ &\equiv b'c' + c' \underbrace{a}_{\equiv a' \bmod n} + ab \equiv b'c' + c'a' + \underbrace{a}_{\equiv a' \bmod n} b \\ &\equiv b'c' + c'a' + a' \underbrace{b}_{\equiv b' \bmod n} \equiv b'c' + c'a' + a'b' \bmod n.\end{aligned}$$

Of course, we shall always just show the replacements as a single step:

$$\underbrace{b}_{\equiv b' \bmod n} \underbrace{c}_{\equiv c' \bmod n} + \underbrace{c}_{\equiv c' \bmod n} \underbrace{a}_{\equiv a' \bmod n} + \underbrace{a}_{\equiv a' \bmod n} \underbrace{b}_{\equiv b' \bmod n} \equiv b'c' + c'a' + a'b' \bmod n.$$

The PSC can be extended: The expression A can be allowed to involve not only integers, addition, subtraction, multiplication and x, but also k-th powers for $k \in \mathbb{N}$ (as long as k remains unchanged in our replacement) as well as finite sums and products (as long as the bounds of the sums and products are unchanged). This follows from Exercise 2.3.4 and Exercise 2.3.5.

Exercise 2.5.1. Let $n \in \mathbb{N}$. Show that $7 \mid 3^{2n+1} + 2^{n+2}$.

2.6. Division with remainder

The following fact you likely remember from high school:

Theorem 2.6.1. Let n be a positive integer. Let $u \in \mathbb{Z}$. Then, there exists a unique pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$.

We shall refer to this as the *"division-with-remainder theorem for integers"*. Before we prove this theorem, let us introduce the notations that it justifies:

Definition 2.6.2. Let n be a positive integer. Let $u \in \mathbb{Z}$. Theorem 2.6.1 shows that there exists a unique pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$. Consider this pair.

(a) We denote the integer q by $u//n$, and refer to it as the *quotient of the division of u by n*.

(b) We denote the integer r by $u\%n$, and refer to it as the *remainder of the division of u by n*.

The words "quotient" and "remainder" are standard, but the notations "$u//n$" and "$u\%n$" are not (I have taken them from the Python programming language); be prepared to see other notations in the literature (e.g., the notations "quo (u, n)" and "rem (u, n)" for $u//n$ and $u\%n$, respectively).

Example 2.6.3. **(a)** We have $14//3 = 4$ and $14\%3 = 2$, because $(4,2)$ is the unique pair $(q,r) \in \mathbb{Z} \times \{0,1,2\}$ satisfying $14 = q \cdot 3 + r$.

(b) We have $18//3 = 6$ and $18\%3 = 0$, because $(6,0)$ is the unique pair $(q,r) \in \mathbb{Z} \times \{0,1,2\}$ satisfying $18 = q \cdot 3 + r$.

(c) We have $(-2)//3 = -1$ and $(-2)\%3 = 1$, because $(-1,1)$ is the unique pair $(q,r) \in \mathbb{Z} \times \{0,1,2\}$ satisfying $-2 = q \cdot 3 + r$.

(d) For each $u \in \mathbb{Z}$, we have $u//1 = u$ and $u\%1 = 0$, because $(u,0)$ is the unique pair $(q,r) \in \mathbb{Z} \times \{0\}$ satisfying $u = q \cdot 1 + r$.

But we have gotten ahead of ourselves: We need to prove Theorem 2.6.1 before we can use the notations "$u//n$" and "$u\%n$".

Let us split Theorem 2.6.1 into two parts: existence and uniqueness:

Lemma 2.6.4. Let n be a positive integer. Let $u \in \mathbb{Z}$. Then, there exists **at least one** pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$.

Lemma 2.6.5. Let n be a positive integer. Let $u \in \mathbb{Z}$. Then, there exists **at most one** pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$.

We begin by proving Lemma 2.6.5 (which is the easier one):

Proof of Lemma 2.6.5. Let (q_1,r_1) and (q_2,r_2) be two pairs $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$. We shall show that $(q_1,r_1) = (q_2,r_2)$.

We know that (q_1,r_1) is a pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$. In other words, $(q_1,r_1) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ and $u = q_1 n + r_1$. Similarly, $(q_2,r_2) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ and $u = q_2 n + r_2$.

From $(q_1,r_1) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$, we obtain $q_1 \in \mathbb{Z}$ and $r_1 \in \{0,1,\ldots,n-1\}$. Similarly, $q_2 \in \mathbb{Z}$ and $r_2 \in \{0,1,\ldots,n-1\}$. Thus, in particular, q_1, q_2, r_1, r_2 are integers.

From $r_1 \in \{0,1,\ldots,n-1\}$ and $r_2 \in \{0,1,\ldots,n-1\}$, we can easily derive

$$|r_2 - r_1| \leq n - 1. \tag{15}$$

[*Proof of (15):* Intuitively, this should be clear: Both r_1 and r_2 belong to the integer interval $\{0,1,\ldots,n-1\}$, and thus the unsigned distance between r_1 and r_2 is at most $n-1$ (with the worst case being when r_1 and r_2 are at opposite ends of this interval).

Here is a formal restatement of this argument: We have $r_1 \in \{0,1,\ldots,n-1\}$, thus $r_1 \geq 0$. Also, $r_2 \in \{0,1,\ldots,n-1\}$, hence $r_2 \leq n-1$. Hence, $\underbrace{r_2}_{\leq n-1} - \underbrace{r_1}_{\geq 0} \leq (n-1) - 0 = n-1$. Similarly, $r_1 - r_2 \leq n - 1$. But recall that $|x| \in \{x, -x\}$ for each $x \in \mathbb{Z}$. Applying this to $x = r_2 - r_1$, we obtain

$$|r_2 - r_1| \in \left\{ r_2 - r_1, \underbrace{-(r_2 - r_1)}_{= r_1 - r_2} \right\} = \{r_2 - r_1, r_1 - r_2\}.$$

In other words, $|r_2 - r_1|$ is one of the two numbers $r_2 - r_1$ and $r_1 - r_2$. Since both of these numbers $r_2 - r_1$ and $r_1 - r_2$ are $\leq n - 1$ (as we have just shown), we thus conclude that $|r_2 - r_1| \leq n - 1$. This proves (15).]

We have $q_1 n + r_1 = u = q_2 n + r_2$, thus $q_1 n - q_2 n = r_2 - r_1$. Hence,

$$r_2 - r_1 = q_1 n - q_2 n = (q_1 - q_2)\, n. \tag{16}$$

Assume (for the sake of contradiction) that $q_1 \neq q_2$. Thus, $q_1 - q_2 \neq 0$, so that $|q_1 - q_2| > 0$ and therefore $|q_1 - q_2| \geq 1$ (since $|q_1 - q_2|$ is an integer). We can multiply this inequality by n (since n is positive) and thus obtain $|q_1 - q_2|\, n \geq 1n = n$. But from (16), we obtain

$$\begin{aligned} |r_2 - r_1| &= |(q_1 - q_2)\, n| = |q_1 - q_2| \cdot \underbrace{|n|}_{\substack{=n \\ \text{(since } n \text{ is positive)}}} \qquad \text{(by (3))} \\ &= |q_1 - q_2|\, n \geq n > n - 1. \end{aligned}$$

This contradicts (15). This contradiction shows that our assumption (that $q_1 \neq q_2$) was false. Hence, we have $q_1 = q_2$. Thus, $q_1 - q_2 = 0$, so that (16) becomes $r_2 - r_1 = \underbrace{(q_1 - q_2)}_{=0} n = 0$ and thus $r_2 = r_1$, so that $r_1 = r_2$. Combining this with $q_1 = q_2$, we obtain $(q_1, r_1) = (q_2, r_2)$.

Now, forget that we have fixed (q_1, r_1) and (q_2, r_2). We thus have proven that if (q_1, r_1) and (q_2, r_2) are two pairs $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$, then $(q_1, r_1) = (q_2, r_2)$. In other words, any two pairs $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$ must be equal. In other words, there exists at most one such pair. This proves Lemma 2.6.5. □

But we also need to prove Lemma 2.6.4. This lemma can be proven by induction on u, but not without some complications: Since it is stated for all integers u (rather than just for nonnegative or positive integers), the classical induction principle (with an induction base and a "u to $u + 1$" step) cannot prove it directly. Instead, we have to either add a "u to $u - 1$" step to our induction (resulting in a "two-sided induction" or "up- and down-induction" argument), or to treat the case of negative u separately. A proof using the first of these two methods can be found in [Grinbe15, proof of Proposition 2.150] (where n and u are denoted by N and n). We shall instead give a proof using the second method; thus, we first state the particular case of Lemma 2.6.4 when u is nonnegative:

Lemma 2.6.6. Let n be a positive integer. Let $u \in \mathbb{N}$. Then, there exists **at least one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$.

This lemma can be proven by induction on u as in [Grinbe15, proof of Proposition 2.150]. Let us instead prove it by **strong** induction on u. See [Grinbe15, §2.8] for an introduction to strong induction; in particular, recall that a strong induction needs no induction base (but often contains a case distinction in its "induction step" that, in some way, does give the first few values a special treatment). The proof of Lemma 2.6.6 that we give below follows a stupid but valid method of finding the pair (q, r): Keep subtracting n from u until u becomes $< n$; then r will be the resulting number, whereas q will be the number of times you have subtracted n.

Proof of Lemma 2.6.6. We proceed by strong induction on u.

Let $U \in \mathbb{N}$. Assume (as the induction hypothesis) that Lemma 2.6.6 holds for every $u \in \mathbb{N}$ satisfying $u < U$. We must prove that Lemma 2.6.6 also holds for $u = U$. In other words, we must prove that there exists **at least one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $U = qn + r$.

We are in one of the following two cases:

Case 1: We have $U < n$.

Case 2: We have $U \geq n$.

Let us first consider Case 1. In this case, we have $U < n$. Thus, $U \leq n - 1$ (since U and n are integers), so that $U \in \{0, 1, \ldots, n-1\}$ (since $U \in \mathbb{N}$). Combining this with $0 \in \mathbb{Z}$, we obtain $(0, U) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$. Hence, $(0, U)$ is a pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $U = qn + r$ (since $U = 0n + U$). Thus, there exists **at least one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $U = qn + r$ (namely, $(q, r) = (0, U)$).

Let us now consider Case 2. In this case, we have $U \geq n$. Hence, $U - n \geq 0$, so that $U - n \in \mathbb{N}$ (remember that $\mathbb{N} = \{0, 1, 2, \ldots\}$). Also, $U - n < U$ (since n is positive). But our induction hypothesis said that Lemma 2.6.6 holds for every $u \in \mathbb{N}$ satisfying $u < U$. Hence, in particular, Lemma 2.6.6 holds for $u = U - n$ (since $U - n \in \mathbb{N}$ and $U - n < U$). In other words, there exists **at least one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $U - n = qn + r$. Fix such a pair and denote it by (q_0, r_0). Thus, $(q_0, r_0) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ and $U - n = q_0 n + r_0$.

From $U - n = q_0 n + r_0$, we obtain $U = n + (q_0 n + r_0) = (q_0 + 1) n + r_0$. Also, from $(q_0, r_0) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$, we obtain $q_0 \in \mathbb{Z}$ and $r_0 \in \{0, 1, \ldots, n-1\}$, and thus $(q_0 + 1, r_0) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$. Thus, the pair $(q_0 + 1, r_0)$ is a pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $U = qn + r$ (since $U = (q_0 + 1) n + r_0$). Therefore, there exists **at least one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $U = qn + r$ (namely, $(q, r) = (q_0 + 1, r_0)$).

Now, in each of the two Cases 1 and 2, we have shown that there exists **at least one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $U = qn + r$. Hence, this holds always. In other words, Lemma 2.6.6 holds for $u = U$. This completes the induction step; thus, Lemma 2.6.6 is proven by strong induction. □

In order to derive Lemma 2.6.4 from Lemma 2.6.6 (that is, to extend Lemma 2.6.6 to the case of negative u), we shall need a simple but important trick: By adding a sufficiently high multiple of the positive integer n to u, we eventually obtain a nonnegative integer v (to which we can then apply Lemma 2.6.6). This trick can be crystallized in the following lemma:

Lemma 2.6.7. Let n be a positive integer. Let $u \in \mathbb{Z}$. Then, there exists a $v \in \mathbb{N}$ such that $u \equiv v \mod n$.

Proof of Lemma 2.6.7. We are in one of the following two cases:

Case 1: We have $u \geq 0$.

Case 2: We have $u < 0$.

Let us first consider Case 1. In this case, we have $u \geq 0$. Thus, $u \in \mathbb{N}$. Also, $u \equiv u \mod n$ (by Proposition 2.3.4 **(a)**). Thus, there exists a $v \in \mathbb{N}$ such that $u \equiv v \mod n$ (namely, $v = u$). This proves Lemma 2.6.7 in Case 1.

Let us now consider Case 2. In this case, we have $u < 0$. Hence, $-u > 0$. Now, $u - (n-1)(-u) = nu$ is divisible by n (since $u \in \mathbb{Z}$). In other words, $n \mid u - (n-1)(-u)$. In other words, $u \equiv (n-1)(-u) \mod n$. Moreover, $n \geq 1$ (since n is a positive integer), so that $n - 1 \geq 0$. We can multiply this inequality with $-u$ (since $-u > 0$), and thus obtain $(n-1)(-u) \geq 0(-u) = 0$. In other words, $(n-1)(-u) \in \mathbb{N}$. Thus, there exists a $v \in \mathbb{N}$ such that $u \equiv v \mod n$ (namely, $v = (n-1)(-u)$). This proves Lemma 2.6.7 in Case 2.

We have now proven Lemma 2.6.7 in both Cases 1 and 2; hence, Lemma 2.6.7 always holds. □

Proof of Lemma 2.6.4. Lemma 2.6.7 shows that there exists a $v \in \mathbb{N}$ such that $u \equiv v \mod n$. Consider this v.

Note that $n \mid u - v$ (since $u \equiv v \mod n$). In other words, there exists an integer c such that $u - v = nc$. Consider this c. From $u - v = nc$, we obtain $u = v + nc$.

Lemma 2.6.6 (applied to v instead of u) yields that there exists **at least one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $v = qn + r$. Fix such a pair, and denote it by (q_0, r_0). Thus, $(q_0, r_0) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ and $v = q_0 n + r_0$. Now,

$$u = \underbrace{v}_{= q_0 n + r_0} + nc = (q_0 n + r_0) + nc = (q_0 + c) n + r_0.$$

Also, from $(q_0, r_0) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$, we obtain $q_0 \in \mathbb{Z}$ and $r_0 \in \{0, 1, \ldots, n-1\}$, and thus $(q_0 + c, r_0) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$. Thus, the pair $(q_0 + c, r_0)$ is a pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$ (since $u = (q_0 + c) n + r_0$). Therefore, there exists **at least one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$ (namely, $(q, r) = (q_0 + c, r_0)$). This proves Lemma 2.6.4. □

Proof of Theorem 2.6.1. Theorem 2.6.1 follows by combining Lemma 2.6.4 with Lemma 2.6.5. □

Remark 2.6.8. We can visualize Theorem 2.6.1 as follows: Mark all the multiples of n on the real line. These multiples are evenly spaced points, with a distance of n between any two neighboring multiples. Thus, they subdivide the real line into infinitely many intervals of length n. More precisely, for each $a \in \mathbb{Z}$, let I_a be the interval $[an, (a+1) n) = \{x \in \mathbb{R} \mid an \leq x < (a+1) n\}$; then, every real belongs to exactly one of these intervals I_a. (This is intuitively clear – I am not saying this is a rigorous proof.) Thus, in particular, u belongs to I_q for some $q \in \mathbb{Z}$.

This q is precisely the q in the unique pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ satisfying $u = qn + r$. Moreover, the r from this pair specifies the relative position of u in the interval I_q.

(Unfortunately, it is not clear to me whether this intuition can be turned into a proper proof of Theorem 2.6.1, since it relies on the fact that every real number belongs to exactly one of the intervals I_a, which fact may well require Theorem 2.6.1 for its proof.)

The following properties of the quotient and the remainder are simple but will be used all the time:

Corollary 2.6.9. Let n be a positive integer. Let $u \in \mathbb{Z}$.

(a) Then, $u\%n \in \{0,1,\ldots,n-1\}$ and $u\%n \equiv u \mod n$.

(b) We have $n \mid u$ if and only if $u\%n = 0$.

(c) If $c \in \{0,1,\ldots,n-1\}$ is such that $c \equiv u \mod n$, then $c = u\%n$.

(d) We have $u = (u//n)\,n + (u\%n)$.

Before we prove this corollary, let us explain its purpose. Corollary 2.6.9 **(a)** says that $u\%n$ is a number in the set $\{0,1,\ldots,n-1\}$ that is congruent to u modulo n. Corollary 2.6.9 **(c)** says that $u\%n$ is the **only** such number (as it says that any further such number c must be equal to $u\%n$). Corollary 2.6.9 **(b)** gives an algorithm to check whether $n \mid u$ holds (namely, compute $u\%n$ and check whether $u\%n = 0$). Corollary 2.6.9 **(d)** is a trivial consequence of the definition of quotient and remainder.

Proof of Corollary 2.6.9. Theorem 2.6.1 says that there is a unique pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$. Consider this pair (q,r). The uniqueness of this pair can be restated as follows: If $(q',r') \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ is any further pair such that $u = q'n + r'$, then

$$(q',r') = (q,r). \tag{17}$$

Recall that $u\%n$ was defined to be r (in Definition 2.6.2 **(b)**). Thus, $u\%n = r$. Now, $n \mid qn = u - r$ (since $u = qn + r$). In other words, $u \equiv r \mod n$. Hence, $r \equiv u \mod n$ (by Proposition 2.3.4 **(c)**). This rewrites as $u\%n \equiv u \mod n$ (since $r = u\%n$).

Furthermore, $u\%n = r \in \{0,1,\ldots,n-1\}$ (since $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$). This completes the proof of Corollary 2.6.9 **(a)**.

Also, $u//n$ was defined to be q (in Definition 2.6.2 **(a)**). Hence, $u//n = q$. Now,

$$u = \underbrace{q}_{=u//n} n + \underbrace{r}_{=u\%n} = (u//n)\,n + (u\%n).$$

This proves Corollary 2.6.9 **(d)**.

(b) $\Longrightarrow$: Assume that $n \mid u$. We must prove that $u\%n = 0$.

We have $n \mid u$. In other words, there exists some integer w such that $u = nw$. Consider this w.

We have $n-1 \in \mathbb{N}$ (since n is a positive integer), thus $0 \in \{0,1,\ldots,n-1\}$. Hence, $(w,0) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ (since $w \in \mathbb{Z}$). Also, $u = nw = wn = wn + 0$. Hence, (17) (applied to $(q',r') = (w,0)$) yields $(w,0) = (q,r)$. In other words, $w = q$ and $0 = r$. Hence, $r = 0$, so that $u\%n = r = 0$. This proves the "$\Longrightarrow$" implication of Corollary 2.6.9 **(b)**.

$\Longleftarrow$: Assume that $u\%n = 0$. We must prove that $n \mid u$.

We have $u = qn + \underbrace{r}_{=u\%n=0} = qn = nq$. Thus, $n \mid u$. This proves the "$\Longleftarrow$" implication of Corollary 2.6.9 **(b)**.

(c) Let $c \in \{0,1,\ldots,n-1\}$ be such that $c \equiv u \mod n$.

We have $c \equiv u \mod n$. In other words, $n \mid c-u$. In other words, there exists some integer w such that $c - u = nw$. Consider this w.

From $-w \in \mathbb{Z}$ and $c \in \{0,1,\ldots,n-1\}$, we obtain $(-w,c) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$. Also, from $c-u = nw$, we obtain $u = c - nw = (-w)\,n + c$. Hence, (17) (applied to $(q',r') = (-w,c)$) yields $(-w,c) = (q,r)$. In other words, $-w = q$ and $c = r$. Hence, $c = r = u\%n$. This proves Corollary 2.6.9 **(c)**. □

Exercise 2.6.1. Let n be a positive integer. Let u and v be integers. Prove that $u \equiv v \mod n$ if and only if $u\%n = v\%n$.

The following exercise provides an analogue of Theorem 2.6.1, in which r is required to be an integer satisfying $|r| \leq n/2$ rather than an element of $\{0,1,\ldots,n-1\}$. Note, however, that r is not always unique in this case.

Exercise 2.6.2. Let n be a positive integer. Let $u \in \mathbb{Z}$.

(a) Prove that there exists a pair $(q,r) \in \mathbb{Z} \times \mathbb{Z}$ such that $u = qn + r$ and $|r| \leq n/2$.

(b) Prove that this pair is not unique in general (i.e., find n and u for which it is not unique).

Remark 2.6.10. There is a simple visualization that makes Exercise 2.6.2 **(a)** intuitively obvious: Mark all the multiples of n on the real line. These multiples are evenly spaced points, with a distance of n between any two neighboring multiples. Hence, every point on the real line is at most a distance of $n/2$ away from the closest multiple of n. Applying this to the point u, we conclude that u is at most a distance of $n/2$ away from the closest multiple of n. In other words, if qn is the closest multiple of n to u (or one of the two closest multiples of n, if u is in the middle between two multiples), then $|u - qn| \leq n/2$. Thus, if we set $r = u - qn$, then $u = qn + r$ and $|r| \leq n/2$. This proves Exercise 2.6.2 **(a)** intuitively.

This point of view also makes Exercise 2.6.2 **(b)** evident: When the point u is exactly in the middle of one of the length-n intervals between multiples of n, then there are two multiples of n equally close to u, and we can pick either of them; hence, the pair (q,r) is not unique.

Convention 2.6.11. The symbols $//$ and $\%$ will be granted higher precedence (in the sense of operator precedence) than addition. This means that an expression of the form "$c + a//n + b$" will always be interpreted as "$c + (a//n) + b$", rather than as "$(c+a)//(n+b)$" (or in any other way). Likewise, an expression of the form "$c + a\%n + b$" will always be interpreted as "$c + (a\%n) + b$", rather than as "$(c+a)\%(n+b)$".

Exercise 2.6.3. Let u and v be two integers. Let n be a positive integer.
(a) Prove that $u\%n + v\%n - (u+v)\%n \in \{0, n\}$.
(b) Prove that $(u+v)//n - u//n - v//n \in \{0, 1\}$.

Exercise 2.6.4. Let n be a positive integer. Prove the following:
(a) The map

$$\begin{aligned} \mathbb{Z} \times \{0, 1, \ldots, n-1\} &\to \mathbb{Z}, \\ (q, r) &\mapsto qn + r \end{aligned}$$

is a bijection.
(b) The map

$$\begin{aligned} \mathbb{N} \times \{0, 1, \ldots, n-1\} &\to \mathbb{N}, \\ (q, r) &\mapsto qn + r \end{aligned}$$

is a bijection.
(c) Any $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$ satisfy $(qn + r)//n = q$.
(d) Any $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$ satisfy $(qn + r)\%n = r$.

2.7. Even and odd numbers

Recall the following:

Definition 2.7.1. Let u be an integer.
(a) We say that u is *even* if u is divisible by 2.
(b) We say that u is *odd* if u is not divisible by 2.

So an integer is either even or odd (but not both at the same time). The following exercise collects various properties of even and odd integers:

Exercise 2.7.1. Let u be an integer.
(a) Prove that u is even if and only if $u\%2 = 0$.
(b) Prove that u is odd if and only if $u\%2 = 1$.
(c) Prove that u is even if and only if $u \equiv 0 \mod 2$.
(d) Prove that u is odd if and only if $u \equiv 1 \mod 2$.
(e) Prove that u is odd if and only if $u + 1$ is even.

(f) Prove that exactly one of the two numbers u and $u+1$ is even.

(g) Prove that $u(u+1) \equiv 0 \mod 2$.

(h) Prove that $u^2 \equiv -u \equiv u \mod 2$.

(i) Let v be a further integer. Prove that $u \equiv v \mod 2$ holds if and only if u and v are either both odd or both even.

Exercise 2.7.2. **(a)** Prove that each even integer u satisfies $u^2 \equiv 0 \mod 4$.

(b) Prove that each odd integer u satisfies $u^2 \equiv 1 \mod 4$.

(c) Prove that no two integers x and y satisfy $x^2 + y^2 \equiv 3 \mod 4$.

(d) Prove that if x and y are two integers satisfying $x^2 + y^2 \equiv 2 \mod 4$, then x and y are both odd.

Exercise 2.7.2 **(c)** establishes our previous experimental observation that an integer of the form $4k+3$ with integer k (that is, an integer that is larger by 3 than a multiple of 4) can never be written as a sum of two perfect squares.

Exercise 2.7.3. **(a)** Prove that the map

$$\{i \in \mathbb{N} \mid i \text{ is even}\} \to \{d \in \mathbb{N} \mid d \equiv 1 \mod 4\},$$
$$i \mapsto 2i+1$$

is well-defined and is a bijection.

(b) Prove that the map

$$\{i \in \mathbb{N} \mid i \text{ is odd}\} \to \{d \in \mathbb{N} \mid d \equiv 3 \mod 4\},$$
$$i \mapsto 2i+1$$

is well-defined and is a bijection.

Note that the map defined in Exercise 2.7.3 **(a)** sends $0, 2, 4, 6, 8, \ldots$ to $1, 5, 9, 13, 17, \ldots$, while the map defined in Exercise 2.7.3 **(b)** sends $1, 3, 5, 7, 9, \ldots$ to $3, 7, 11, 15, 19, \ldots$.

2.8. The floor function

We shall now briefly introduce the floor function (following [Grinbe16]), as it is closely connected to division with remainder.

Definition 2.8.1. Let x be a real number. Then, $\lfloor x \rfloor$ is defined to be the unique integer n satisfying $n \leq x < n+1$. This integer $\lfloor x \rfloor$ is called the *floor* of x, or the *integer part* of x.

Remark 2.8.2. **(a)** Why is $\lfloor x \rfloor$ well-defined? I mean, why does the unique integer n in Definition 2.8.1 exist, and why is it unique? This question is trickier than it sounds and relies on the construction of real numbers. However, in the case when x is rational, the well-definedness of $\lfloor x \rfloor$ follows from Proposition 2.8.3 below.

(b) What we call $\lfloor x \rfloor$ is typically called $[x]$ in older books (such as [NiZuMo91]). I suggest avoiding the notation $[x]$ wherever possible; it has too many different meanings (whereas $\lfloor x \rfloor$ almost always means the floor of x).

(c) The map $\mathbb{R} \to \mathbb{Z}$, $x \mapsto \lfloor x \rfloor$ is called the *floor function* or the *greatest integer function*.

There is also a *ceiling function*, which sends each $x \in \mathbb{R}$ to the unique integer n satisfying $n - 1 < x \leq n$; this latter integer is called $\lceil x \rceil$. The two functions are connected by the rule $\lceil x \rceil = -\lfloor -x \rfloor$ (for all $x \in \mathbb{R}$).

The floor and the ceiling functions are some of the simplest examples of discontinuous functions.

(d) Here are some examples of floors:

$$\begin{array}{lll} \lfloor n \rfloor = n & \text{for every } n \in \mathbb{Z}; & \\ \lfloor 1.32 \rfloor = 1; & \lfloor \pi \rfloor = 3; & \lfloor 0.98 \rfloor = 0; \\ \lfloor -2.3 \rfloor = -3; & \lfloor -0.4 \rfloor = -1. & \end{array}$$

(e) You might have the impression that $\lfloor x \rfloor$ is "what remains from x if the digits behind the comma are removed". This impression is highly imprecise. For one, it is completely broken for negative x (for example, $\lfloor -2.3 \rfloor$ is -3, not -2). But more importantly, the operation of "removing the digits behind the comma" from a number is not well-defined; in fact, the periodic decimal representations $0.999\ldots$ and $1.000\ldots$ belong to the same real number (1), but removing their digits behind the comma leaves us with different integers.

(f) A related map is the map $\mathbb{R} \to \mathbb{Z}$, $x \mapsto \left\lfloor x + \frac{1}{2} \right\rfloor$. It sends each real x to the integer that is closest to x, choosing the larger one in the case of a tie. This is one of the many things that are commonly known as "rounding" a number.

Proposition 2.8.3. Let a and b be integers such that $b > 0$. Then, $\left\lfloor \frac{a}{b} \right\rfloor$ is well-defined and equals $a//b$.

Proof of Proposition 2.8.3. This is a rather easy and neat exercise. A full proof can be found in [Grinbe16, proof of Proposition 1.1.3]. □

See [Grinbe16] and [NiZuMo91, §4.1] for further properties of the floor function.

2.9. Common divisors, the Euclidean algorithm and the Bezout theorem

We are next going to define and study the divisors of an integer, as well as the common divisors of several integers. These concepts form the backbone of most of number theory, and will later be extended to some more complicated notions than integers (e.g., Gaussian integers and polynomials).

2.9.1. Divisors

Definition 2.9.1. Let $b \in \mathbb{Z}$. The *divisors* of b are defined as the integers that divide b.

Be aware that some authors use a mildly different definition of "divisors"; namely, they additionally require them to be positive. We don't make such a requirement.

For example, the divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$. Of course, the negative divisors of an integer b are merely the reflections of the positive divisors through the origin[14] (this follows easily from Proposition 2.2.3 **(a)**); thus, the positive divisors are usually the only ones of interest.

Here are some basic properties of divisors:

Proposition 2.9.2. **(a)** If $b \in \mathbb{Z}$, then 1 and b are divisors of b.

(b) The divisors of 0 are all the integers.

(c) Let $b \in \mathbb{Z}$ be nonzero. Then, all divisors of b belong to the set $\{-|b|, -|b|+1, \ldots, |b|\} \setminus \{0\}$.

Proof of Proposition 2.9.2. **(a)** Clearly, $1 \mid b$ (since $b = 1b$), so that 1 is a divisor of b. Also, $b \mid b$ (since $b = b \cdot 1$), so that b is a divisor of b.

(b) Each integer a divides 0 (since $0 = a \cdot 0$) and thus is a divisor of 0. This proves Proposition 2.9.2 **(b)**.

(c) Let a be a divisor of b. Then, a divides b. In other words, $a \mid b$. Hence, Proposition 2.2.3 **(b)** yields $|a| \leq |b|$ (since $b \neq 0$). But $|a| \geq a$ (since $|x| \geq x$ for each $x \in \mathbb{R}$), so that $a \leq |a| \leq |b|$. Also, $|a| \geq -a$ (since $|x| \geq -x$ for each $x \in \mathbb{R}$) and thus $-a \leq |a| \leq |b|$, so that $a \geq -|b|$. Combining this with $a \leq |b|$, we obtain $-|b| \leq a \leq |b|$ and thus $a \in \{-|b|, -|b|+1, \ldots, |b|\}$ (since a is an integer).

From Example 2.2.2 **(c)**, we know that $0 \mid b$ only when $b = 0$. Thus, we don't have $0 \mid b$ (since $b \neq 0$).

If we had $a = 0$, then we would have $0 = a \mid b$, which would contradict the fact that we don't have $0 \mid b$. Thus, we cannot have $a = 0$. Hence, $a \neq 0$. Combining $a \in \{-|b|, -|b|+1, \ldots, |b|\}$ with $a \neq 0$, we obtain $a \in \{-|b|, -|b|+1, \ldots, |b|\} \setminus \{0\}$.

We have proven this for each divisor a of b. Thus, we conclude that all divisors of b belong to the set $\{-|b|, -|b|+1, \ldots, |b|\} \setminus \{0\}$. This proves Proposition 2.9.2 **(c)**. □

Thanks to Proposition 2.9.2, we have a method to find all divisors of an integer b: If $b = 0$, then Proposition 2.9.2 **(b)** directly yields the result; otherwise, Proposition 2.9.2 **(c)** shows that there is only a finite set of numbers we have to check. When b is large, this is slow, but to some extent that is because the problem is computationally hard (or at least suspected to be hard).

[14] "Reflection through the origin" is just a poetic way to say "negative"; i.e., the reflection of a number a through the origin is $-a$.

2.9.2. Common divisors

It is somewhat more interesting to consider the common divisors of two or more integers:

Definition 2.9.3. Let $b_1, b_2, \ldots, b_k$ be integers. Then, the *common divisors* of $b_1, b_2, \ldots, b_k$ are defined to be the integers a that satisfy

$$(a \mid b_i \text{ for all } i \in \{1, 2, \ldots, k\}) \tag{18}$$

(in other words, that divide all of the integers $b_1, b_2, \ldots, b_k$). We let $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ denote the set of these common divisors.

Note that the concept of common divisors encompasses the concept of divisors: The common divisors of a single integer b are merely the divisors of b. Thus, $\operatorname{Div}(b)$ is the set of all divisors of b whenever $b \in \mathbb{Z}$. (Of course, speaking of "common divisors" of just one integer is like speaking of a conspiracy of just one person. But the definition fits, and we algebraists don't exclude cases just because they are ridiculous.)

(Also, the common divisors of an empty list of integers are all the integers, because the requirement (18) is vacuously true for $k = 0$. In other words, $\operatorname{Div}() = \mathbb{Z}$.)

Here are some more interesting examples of common divisors:

Example 2.9.4. **(a)** The common divisors of 6 and 8 are $-2, -1, 1, 2$. (In order to see this, just observe that the divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$, whereas the divisors of 8 are $-8, -4, -2, -1, 1, 2, 4, 8$; now you can find the common divisors of 6 and 8 by taking the numbers common to these two lists.) Thus,

$$\operatorname{Div}(6, 8) = \{-2, -1, 1, 2\}.$$

(b) The common divisors of 6 and 14 are $-2, -1, 1, 2$ again. (In order to see this, just observe that the divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$, whereas the divisors of 14 are $-14, -7, -2, -1, 1, 2, 7, 14$.)

(c) The common divisors of 6, 10 and 15 are -1 and 1. (In order to see this, note that:

- The divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$.
- The divisors of 10 are $-10, -5, -2, -1, 1, 2, 5, 10$.
- The divisors of 15 are $-15, -5, -3, -1, 1, 3, 5, 15$.

The only numbers common to these three lists are -1 and 1.) However:

- The common divisors of 6 and 10 are $-2, -1, 1, 2$.
- The common divisors of 6 and 15 are $-3, -1, 1, 3$.

- The common divisors of 10 and 15 are $-5, -1, 1, 5$.

This illustrates the fact that three numbers can have pairwise nontrivial common divisors (where "nontrivial" means "distinct from 1 and -1"), but the only common divisors of all three of them may still be just 1 and -1.

Proposition 2.9.5. Let $b_1, b_2, \ldots, b_k$ be finitely many integers that are not all 0. Then, the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ has a largest element, and this largest element is a positive integer.

Proof of Proposition 2.9.5. The integer 1 satisfies $(1 \mid b_i$ for all $i \in \{1, 2, \ldots, k\})$. Thus, 1 is a common divisor of $b_1, b_2, \ldots, b_k$ (by the definition of a "common divisor"). In other words, $1 \in \operatorname{Div}(b_1, b_2, \ldots, b_k)$ (by the definition of $\operatorname{Div}(b_1, b_2, \ldots, b_k)$). Hence, the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ is nonempty.

Moreover, it is easy to see that the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ is finite.

[*Proof:* We have assumed that $b_1, b_2, \ldots, b_k$ are not all 0. In other words, there exists a $j \in \{1, 2, \ldots, k\}$ such that b_j is nonzero. Consider such a j.

Let $d \in \operatorname{Div}(b_1, b_2, \ldots, b_k)$. Thus, d is a common divisor of $b_1, b_2, \ldots, b_k$ (by the definition of $\operatorname{Div}(b_1, b_2, \ldots, b_k)$). In other words, $d \mid b_i$ for all $i \in \{1, 2, \ldots, k\}$ (by the definition of "common divisor"). Applying this to $i = j$, we obtain $d \mid b_j$. Hence, d is a divisor of b_j. But Proposition 2.9.2 **(c)** (applied to $b = b_j$) shows that all divisors of b_j belong to the set $\{-|b_j|, -|b_j|+1, \ldots, |b_j|\} \setminus \{0\}$. Hence, d must belong to this set (since d is a divisor of b_j). In other words, $d \in \{-|b_j|, -|b_j|+1, \ldots, |b_j|\} \setminus \{0\}$.

Now, forget that we fixed d. We thus have shown that $d \in \{-|b_j|, -|b_j|+1, \ldots, |b_j|\} \setminus \{0\}$ for each $d \in \operatorname{Div}(b_1, b_2, \ldots, b_k)$. In other words,

$$\operatorname{Div}(b_1, b_2, \ldots, b_k) \subseteq \{-|b_j|, -|b_j|+1, \ldots, |b_j|\} \setminus \{0\}.$$

Thus, the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ is finite (since the set $\{-|b_j|, -|b_j|+1, \ldots, |b_j|\} \setminus \{0\}$ is finite).]

Now we know that the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ is a nonempty finite set of integers. Thus, this set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ has a largest element (since every nonempty finite set of integers has a largest element). It remains to prove that this largest element is a positive integer.

Let g be this largest element. Thus, we must prove that g is a positive integer. Clearly, g is an integer (since all elements of $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ are integers); it thus remains to show that g is positive.

The element g is the largest element of the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$, and thus is $\geq$ to every element of this set. In other words, $g \geq x$ for each $x \in \operatorname{Div}(b_1, b_2, \ldots, b_k)$. Applying this to $x = 1$, we obtain $g \geq 1$ (since $1 \in \operatorname{Div}(b_1, b_2, \ldots, b_k)$). Hence, g is positive. This completes the proof of Proposition 2.9.5. □

The following exercise shows that the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ depends only on the **set** $\{b_1, b_2, \ldots, b_k\}$, but not on the numbers $b_1, b_2, \ldots, b_k$ themselves. Thus, for example, any integers a, b and c satisfy $\operatorname{Div}(a, b, c, a) = \operatorname{Div}(c, a, b)$ (since $\{a, b, c, a\} = \{c, a, b\}$) and $\operatorname{Div}(a, a, b, a) = \operatorname{Div}(a, b, b)$ (since $\{a, a, b, a\} = \{a, b, b\}$).

Exercise 2.9.1. Let $b_1, b_2, \ldots, b_k$ be finitely many integers. Let $c_1, c_2, \ldots, c_\ell$ be finitely many integers. Prove that if

$$\{b_1, b_2, \ldots, b_k\} = \{c_1, c_2, \ldots, c_\ell\},$$

then

$$\operatorname{Div}(b_1, b_2, \ldots, b_k) = \operatorname{Div}(c_1, c_2, \ldots, c_\ell).$$

2.9.3. Greatest common divisors

Proposition 2.9.5 allows us to make a crucial definition:

Definition 2.9.6. Let $b_1, b_2, \ldots, b_k$ be finitely many integers. The *greatest common divisor* of $b_1, b_2, \ldots, b_k$ is defined as follows:

- If $b_1, b_2, \ldots, b_k$ are not all 0, then it is defined as the largest element of the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$. This largest element is well-defined (by Proposition 2.9.5), and is a positive integer (by Proposition 2.9.5 again).
- If $b_1, b_2, \ldots, b_k$ are all 0, then it is defined to be 0. (This is a slight abuse of the word "greatest common divisor", because 0 is not actually the greatest among the common divisors of $b_1, b_2, \ldots, b_k$ in this case. In fact, when $b_1, b_2, \ldots, b_k$ are all 0, **every** integer is a common divisor of $b_1, b_2, \ldots, b_k$, so that there is no greatest among these common divisors, because there is no "greatest integer". Nevertheless, defining the greatest common divisor of $b_1, b_2, \ldots, b_k$ to be 0 in this case will prove to be a good decision, as it will greatly reduce the number of exceptions in our results.)

Thus, in either case, this greatest common divisor is a nonnegative integer. We denote it by $\gcd(b_1, b_2, \ldots, b_k)$. (Some authors also call it $(b_1, b_2, \ldots, b_k)$, which is rather dangerous as the same notation stands for a k-tuple. We shall avoid this notation at all cost, but you should be aware of it when reading number-theoretical literature.)

We shall also use the word "*gcd*" as shorthand for "greatest common divisor".

The greatest common divisors you will most commonly see are those of two integers. Indeed, any other gcd can be rewritten in terms of these: for example,

$$\gcd(a, b, c, d, e) = \gcd(a, \gcd(b, \gcd(c, \gcd(d, e))))$$

for all $a, b, c, d, e \in \mathbb{Z}$. This is, in fact, a consequence of Proposition 2.9.21 **(d)** (which we will prove later), applied several times.

First, let us observe several properties of greatest common divisors:

Proposition 2.9.7. **(a)** We have $\gcd(a,0) = \gcd(a) = |a|$ for all $a \in \mathbb{Z}$.

(b) We have $\gcd(a,b) = \gcd(b,a)$ for all $a,b \in \mathbb{Z}$.

(c) We have $\gcd(a, ua+b) = \gcd(a,b)$ for all $a,b,u \in \mathbb{Z}$.

(d) If $a,b,c \in \mathbb{Z}$ satisfy $b \equiv c \mod a$, then $\gcd(a,b) = \gcd(a,c)$.

(e) If $a,b \in \mathbb{Z}$ are such that a is positive, then $\gcd(a,b) = \gcd(a, b\%a)$.

(f) We have $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ for all $a,b \in \mathbb{Z}$.

(g) We have $\gcd(-a,b) = \gcd(a,b)$ for all $a,b \in \mathbb{Z}$.

(h) We have $\gcd(a,-b) = \gcd(a,b)$ for all $a,b \in \mathbb{Z}$.

(i) If $a,b \in \mathbb{Z}$ satisfy $a \mid b$, then $\gcd(a,b) = |a|$.

(j) The greatest common divisor of the empty list of integers is $\gcd() = 0$.

Proposition 2.9.7 is not difficult and we could start proving it right away. However, such a proof would require some annoying case distinctions due to the special treatment that the "$b_1, b_2, \ldots, b_k$ are all 0" case required in Definition 2.9.6. Fortunately, we can circumnavigate these annoyances by stating a simple rule for how the gcd of k integers $b_1, b_2, \ldots, b_k$ can be computed from their set of common divisors (including the case when $b_1, b_2, \ldots, b_k$ are all 0):

Lemma 2.9.8. Let $b_1, b_2, \ldots, b_k$ be finitely many integers. Then,

$$\gcd(b_1, b_2, \ldots, b_k) = \begin{cases} \max(\operatorname{Div}(b_1, b_2, \ldots, b_k)), & \text{if } 0 \notin \operatorname{Div}(b_1, b_2, \ldots, b_k); \\ 0, & \text{if } 0 \in \operatorname{Div}(b_1, b_2, \ldots, b_k). \end{cases}$$

(Here, $\max S$ denotes the largest element of a set S of integers, whenever this largest element exists.)

Proof of Lemma 2.9.8. We are in one of the following two cases:

Case 1: The integers $b_1, b_2, \ldots, b_k$ are not all 0.

Case 2: The integers $b_1, b_2, \ldots, b_k$ are all 0.

Let us consider Case 1 first. In this case, the integers $b_1, b_2, \ldots, b_k$ are not all 0. Hence, $\gcd(b_1, b_2, \ldots, b_k)$ is defined as the largest element of the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ (by Definition 2.9.6). In other words,

$$\gcd(b_1, b_2, \ldots, b_k) = \max(\operatorname{Div}(b_1, b_2, \ldots, b_k)). \tag{19}$$

On the other hand, $0 \notin \operatorname{Div}(b_1, b_2, \ldots, b_k)$ [15]. Hence,

$$\begin{cases} \max(\operatorname{Div}(b_1, b_2, \ldots, b_k)), & \text{if } 0 \notin \operatorname{Div}(b_1, b_2, \ldots, b_k); \\ 0, & \text{if } 0 \in \operatorname{Div}(b_1, b_2, \ldots, b_k) \end{cases} = \max(\operatorname{Div}(b_1, b_2, \ldots, b_k)).$$

[15] *Proof.* Assume the contrary. Thus, $0 \in \operatorname{Div}(b_1, b_2, \ldots, b_k)$. In other words, 0 is a common divisor of $b_1, b_2, \ldots, b_k$ (by the definition of $\operatorname{Div}(b_1, b_2, \ldots, b_k)$). In other words, $0 \mid b_i$ for all $i \in \{1, 2, \ldots, k\}$ (by the definition of "common divisor"). Thus, for all $i \in \{1, 2, \ldots, k\}$, we have $b_i = 0$ (since $0 \mid b_i$, so that $b_i = 0c$ for some integer c; but this yields $b_i = 0c = 0$). In other words, $b_1, b_2, \ldots, b_k$ are all 0. But this contradicts the fact that $b_1, b_2, \ldots, b_k$ are not all 0. This contradiction shows that our assumption was false, qed.

Comparing this with (19), we obtain

$$\gcd\left(b_1, b_2, \ldots, b_k\right) = \begin{cases} \max\left(\operatorname{Div}\left(b_1, b_2, \ldots, b_k\right)\right), & \text{if } 0 \notin \operatorname{Div}\left(b_1, b_2, \ldots, b_k\right); \\ 0, & \text{if } 0 \in \operatorname{Div}\left(b_1, b_2, \ldots, b_k\right). \end{cases}$$

Hence, Lemma 2.9.8 is proven in Case 1.

Let us now consider Case 2. In this case, the integers $b_1, b_2, \ldots, b_k$ are all 0. Hence, $\gcd\left(b_1, b_2, \ldots, b_k\right)$ is defined as 0 (by Definition 2.9.6). In other words,

$$\gcd\left(b_1, b_2, \ldots, b_k\right) = 0. \tag{20}$$

On the other hand, $0 \in \operatorname{Div}\left(b_1, b_2, \ldots, b_k\right)$ [16]. Hence,

$$\begin{cases} \max\left(\operatorname{Div}\left(b_1, b_2, \ldots, b_k\right)\right), & \text{if } 0 \notin \operatorname{Div}\left(b_1, b_2, \ldots, b_k\right); \\ 0, & \text{if } 0 \in \operatorname{Div}\left(b_1, b_2, \ldots, b_k\right) \end{cases} = 0.$$

Comparing this with (20), we obtain

$$\gcd\left(b_1, b_2, \ldots, b_k\right) = \begin{cases} \max\left(\operatorname{Div}\left(b_1, b_2, \ldots, b_k\right)\right), & \text{if } 0 \notin \operatorname{Div}\left(b_1, b_2, \ldots, b_k\right); \\ 0, & \text{if } 0 \in \operatorname{Div}\left(b_1, b_2, \ldots, b_k\right). \end{cases}$$

Hence, Lemma 2.9.8 is proven in Case 2.

We have now proven Lemma 2.9.8 in both Cases 1 and 2. Thus, Lemma 2.9.8 always holds. □

A corollary of Lemma 2.9.8 is the following:

> **Lemma 2.9.9.** Let $b_1, b_2, \ldots, b_k$ be finitely many integers. Let $c_1, c_2, \ldots, c_\ell$ be finitely many integers. If
>
> $$\operatorname{Div}\left(b_1, b_2, \ldots, b_k\right) = \operatorname{Div}\left(c_1, c_2, \ldots, c_\ell\right),$$
>
> then
>
> $$\gcd\left(b_1, b_2, \ldots, b_k\right) = \gcd\left(c_1, c_2, \ldots, c_\ell\right).$$

Proof of Lemma 2.9.9. Assume that $\operatorname{Div}\left(b_1, b_2, \ldots, b_k\right) = \operatorname{Div}\left(c_1, c_2, \ldots, c_\ell\right)$. Lemma 2.9.8 yields

$$\begin{aligned} \gcd\left(b_1, b_2, \ldots, b_k\right) &= \begin{cases} \max\left(\operatorname{Div}\left(b_1, b_2, \ldots, b_k\right)\right), & \text{if } 0 \notin \operatorname{Div}\left(b_1, b_2, \ldots, b_k\right); \\ 0, & \text{if } 0 \in \operatorname{Div}\left(b_1, b_2, \ldots, b_k\right) \end{cases} \\ &= \begin{cases} \max\left(\operatorname{Div}\left(c_1, c_2, \ldots, c_\ell\right)\right), & \text{if } 0 \notin \operatorname{Div}\left(c_1, c_2, \ldots, c_\ell\right); \\ 0, & \text{if } 0 \in \operatorname{Div}\left(c_1, c_2, \ldots, c_\ell\right) \end{cases} \end{aligned}$$

[16] *Proof.* The integers $b_1, b_2, \ldots, b_k$ are all 0. In other words, $b_i = 0$ for all $i \in \{1, 2, \ldots, k\}$. Hence, $0 \mid b_i$ for all $i \in \{1, 2, \ldots, k\}$ (since each $i \in \{1, 2, \ldots, k\}$ satisfies $b_i = 0 = 0 \cdot 0$). In other words, 0 is a common divisor of $b_1, b_2, \ldots, b_k$ (by the definition of "common divisor"). In other words, $0 \in \operatorname{Div}\left(b_1, b_2, \ldots, b_k\right)$ (by the definition of $\operatorname{Div}\left(b_1, b_2, \ldots, b_k\right)$).

(since $\operatorname{Div}(b_1, b_2, \ldots, b_k) = \operatorname{Div}(c_1, c_2, \ldots, c_\ell)$). But Lemma 2.9.8 (applied to $c_1, c_2, \ldots, c_\ell$ instead of $b_1, b_2, \ldots, b_k$) yields

$$\gcd(c_1, c_2, \ldots, c_\ell) = \begin{cases} \max(\operatorname{Div}(c_1, c_2, \ldots, c_\ell)), & \text{if } 0 \notin \operatorname{Div}(c_1, c_2, \ldots, c_\ell); \\ 0, & \text{if } 0 \in \operatorname{Div}(c_1, c_2, \ldots, c_\ell). \end{cases}$$

Comparing these two equalities, we obtain $\gcd(b_1, b_2, \ldots, b_k) = \gcd(c_1, c_2, \ldots, c_\ell)$. This proves Lemma 2.9.9. □

Lemma 2.9.9 tells us that in order to prove that two lists of integers have the same gcd, it suffices to check that they have the same set of common divisors. Since many of the claims of Proposition 2.9.7 are equalities between gcds, we can thus reduce them to equalities between sets of common divisors. Let us state these equalities as a lemma, which we will then use as a stepping stone in our proof of Proposition 2.9.7:

Lemma 2.9.10. (a) We have $\operatorname{Div}(a, 0) = \operatorname{Div}(a)$ for all $a \in \mathbb{Z}$.

(b) We have $\operatorname{Div}(a, b) = \operatorname{Div}(b, a)$ for all $a, b \in \mathbb{Z}$.

(c) We have $\operatorname{Div}(a, ua + b) = \operatorname{Div}(a, b)$ for all $a, b, u \in \mathbb{Z}$.

(d) If $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \bmod a$, then $\operatorname{Div}(a, b) = \operatorname{Div}(a, c)$.

(e) If $a, b \in \mathbb{Z}$ are such that a is positive, then $\operatorname{Div}(a, b) = \operatorname{Div}(a, b\%a)$.

(f) We have $\operatorname{Div}(a, b) \subseteq \operatorname{Div}(a)$ and $\operatorname{Div}(a, b) \subseteq \operatorname{Div}(b)$ for all $a, b \in \mathbb{Z}$.

(g) We have $\operatorname{Div}(-a, b) = \operatorname{Div}(a, b)$ for all $a, b \in \mathbb{Z}$.

(h) We have $\operatorname{Div}(a, -b) = \operatorname{Div}(a, b)$ for all $a, b \in \mathbb{Z}$.

(i) If $a, b \in \mathbb{Z}$ satisfy $a \mid b$, then $\operatorname{Div}(a, b) = \operatorname{Div}(a)$.

(j) The set of common divisors of the empty list of integers is $\operatorname{Div}() = \mathbb{Z}$.

Proof of Lemma 2.9.10. **(a)** Here is a sketch of the proof: The number 0 is a "joker" when it comes to common divisors, in the sense that inserting it into a list of integers does not change the common divisors of that list. For example, if $a \in \mathbb{Z}$, then the common divisors of a and 0 are the same as the divisors of a, because every integer divides 0. But this is saying precisely that $\operatorname{Div}(a, 0) = \operatorname{Div}(a)$.

For the sake of completeness, let us give a detailed proof of Lemma 2.9.10 **(a)**:

For any integer x, we have the following chain of equivalences:

$$\begin{aligned} & (x \in \operatorname{Div}(a, 0)) \\ \Longleftrightarrow\ & (x \text{ is a common divisor of } a \text{ and } 0) \qquad (\text{by the definition of } \operatorname{Div}(a, 0)) \\ \Longleftrightarrow\ & (x \mid a \text{ and } x \mid 0) \qquad (\text{by the definition of a ``common divisor''}) \\ \Longleftrightarrow\ & (x \mid a) \qquad (\text{since } x \mid 0 \text{ always holds (since } 0 = x \cdot 0)) \\ \Longleftrightarrow\ & (x \text{ is a common divisor of } a) \qquad (\text{by the definition of a ``common divisor''}) \\ \Longleftrightarrow\ & (x \in \operatorname{Div}(a)) \qquad (\text{by the definition of } \operatorname{Div}(a)). \end{aligned}$$

In other words, an integer belongs to $\operatorname{Div}(a, 0)$ if and only if it belongs to $\operatorname{Div}(a)$. Thus, $\operatorname{Div}(a, 0) = \operatorname{Div}(a)$ (since both $\operatorname{Div}(a, 0)$ and $\operatorname{Div}(a)$ are sets of integers). Thus, Lemma 2.9.10 **(a)** is finally proven.

(b) Let $a, b \in \mathbb{Z}$. For any integer x, we have the following chain of equivalences:

$$\begin{aligned}
& (x \in \operatorname{Div}(a,b)) \\
\Longleftrightarrow\ & (x \text{ is a common divisor of } a \text{ and } b) \qquad (\text{by the definition of } \operatorname{Div}(a,b)) \\
\Longleftrightarrow\ & (x \mid a \text{ and } x \mid b) \qquad (\text{by the definition of a ``common divisor''}) \\
\Longleftrightarrow\ & (x \mid b \text{ and } x \mid a) \\
\Longleftrightarrow\ & (x \text{ is a common divisor of } b \text{ and } a) \\
& \quad (\text{by the definition of a ``common divisor''}) \\
\Longleftrightarrow\ & (x \in \operatorname{Div}(b,a)) \qquad (\text{by the definition of } \operatorname{Div}(b,a)).
\end{aligned}$$

In other words, an integer belongs to $\operatorname{Div}(a,b)$ if and only if it belongs to $\operatorname{Div}(b,a)$. Thus, $\operatorname{Div}(a,b) = \operatorname{Div}(b,a)$ (since both $\operatorname{Div}(a,b)$ and $\operatorname{Div}(b,a)$ are sets of integers). This proves Lemma 2.9.10 **(b)**.

Let us prove part **(d)** now, and then derive part **(c)** from it.

(d) Let $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \mod a$. We must prove that $\operatorname{Div}(a,b) = \operatorname{Div}(a,c)$.

From $b \equiv c \mod a$, we obtain $c \equiv b \mod a$ (by Proposition 2.3.4 **(c)**). Hence, our situation is symmetric with respect to b and c.

We shall now show that $\operatorname{Div}(a,b) \subseteq \operatorname{Div}(a,c)$. Indeed, let $x \in \operatorname{Div}(a,b)$. Then, x is a common divisor of a and b (by the definition of $\operatorname{Div}(a,b)$). In other words, $x \mid a$ and $x \mid b$ (by the definition of a "common divisor"). From $x \mid b$, we obtain $b \equiv 0 \mod x$. But from $x \mid a$ and $c \equiv b \mod a$, we obtain $c \equiv b \mod x$ (by Proposition 2.3.4 **(e)**, applied to a, x, c and b instead of n, m, a and b). Thus, $c \equiv b \equiv 0 \mod x$, so that $x \mid c$. Combining $x \mid a$ and $x \mid c$, we see that x is a common divisor of a and c (by the definition of a "common divisor"). In other words, $x \in \operatorname{Div}(a,c)$ (by the definition of $\operatorname{Div}(a,c)$).

Now, forget that we fixed x. We thus have proven that $x \in \operatorname{Div}(a,c)$ for each $x \in \operatorname{Div}(a,b)$. In other words, $\operatorname{Div}(a,b) \subseteq \operatorname{Div}(a,c)$.

The same argument (but with the roles of b and c swapped) shows that $\operatorname{Div}(a,c) \subseteq \operatorname{Div}(a,b)$ (since our situation is symmetric with respect to b and c). Combining this with $\operatorname{Div}(a,b) \subseteq \operatorname{Div}(a,c)$, we obtain $\operatorname{Div}(a,b) = \operatorname{Div}(a,c)$. This proves Lemma 2.9.10 **(d)**.

(c) Let $a, b, u \in \mathbb{Z}$. Then, $ua + b \equiv b \mod a$ (since $(ua + b) - b = ua$ is clearly divisible by a). Thus, Lemma 2.9.10 **(d)** (applied to $ua + b$ and b instead of b and c) yields $\operatorname{Div}(a, ua + b) = \operatorname{Div}(a,b)$. This proves Lemma 2.9.10 **(c)**.

(e) Let $a, b \in \mathbb{Z}$ be such that a is positive. Then, $b\%a \equiv b \mod a$ (by Corollary 2.6.9 **(a)**, applied to a and b instead of n and u), thus $b \equiv b\%a \mod a$. Hence, $\operatorname{Div}(a,b) = \operatorname{Div}(a, b\%a)$ (by Lemma 2.9.10 **(d)**, applied to $c = b\%a$). This proves Lemma 2.9.10 **(e)**.

(f) Let $a, b \in \mathbb{Z}$. We must prove that $\operatorname{Div}(a,b) \subseteq \operatorname{Div}(a)$ and $\operatorname{Div}(a,b) \subseteq \operatorname{Div}(b)$.

Let $x \in \operatorname{Div}(a,b)$. We shall prove that $x \in \operatorname{Div}(b)$.

Indeed, $x \in \operatorname{Div}(a,b)$; in other words, x is a common divisor of a and b (by the definition of $\operatorname{Div}(a,b)$). In other words, $(x \mid a \text{ and } x \mid b)$ (by the definition of a "common divisor"). Hence, $x \mid a$. In other words, x is a common divisor of a

(by the definition of a "common divisor"). In other words, $x \in \operatorname{Div}(a)$ (by the definition of $\operatorname{Div}(a)$).

Now, forget that we fixed x. We thus have shown that $x \in \operatorname{Div}(a)$ for each $x \in \operatorname{Div}(a,b)$. In other words, $\operatorname{Div}(a,b) \subseteq \operatorname{Div}(a)$. A similar argument shows that $\operatorname{Div}(a,b) \subseteq \operatorname{Div}(b)$. This proves Lemma 2.9.10 **(f)**.

(g) Let $a, b \in \mathbb{Z}$. We must prove that $\operatorname{Div}(-a,b) = \operatorname{Div}(a,b)$.

First, we will show that $\operatorname{Div}(a,b) \subseteq \operatorname{Div}(-a,b)$. Indeed, let $x \in \operatorname{Div}(a,b)$. Then, x is a common divisor of a and b (by the definition of $\operatorname{Div}(a,b)$). In other words, $x \mid a$ and $x \mid b$ (by the definition of a "common divisor"). We have $a \mid -a$ (since $-a = a \cdot (-1)$). Thus, $x \mid a \mid -a$. Combining $x \mid -a$ and $x \mid b$, we see that x is a common divisor of $-a$ and b (by the definition of a "common divisor"). In other words, $x \in \operatorname{Div}(-a,b)$ (by the definition of $\operatorname{Div}(-a,b)$).

Now, forget that we fixed x. We thus have proven that $x \in \operatorname{Div}(-a,b)$ for each $x \in \operatorname{Div}(a,b)$. In other words, $\operatorname{Div}(a,b) \subseteq \operatorname{Div}(-a,b)$.

The same argument (but applied to $-a$ instead of a) shows that $\operatorname{Div}(-a,b) \subseteq \operatorname{Div}(-(-a),b)$. Since $-(-a) = a$, this rewrites as $\operatorname{Div}(-a,b) \subseteq \operatorname{Div}(a,b)$. Combining this with $\operatorname{Div}(a,b) \subseteq \operatorname{Div}(-a,b)$, we obtain $\operatorname{Div}(-a,b) = \operatorname{Div}(a,b)$. This proves Lemma 2.9.10 **(g)**.

(h) We can prove this similarly to how we just proved Lemma 2.9.10 **(g)**, but it is easier to derive it from what was already shown.

Let $a, b \in \mathbb{Z}$. Lemma 2.9.10 **(b)** (applied to $-b$ instead of b) yields

$$\begin{aligned}\operatorname{Div}(a,-b) &= \operatorname{Div}(-b,a) = \operatorname{Div}(b,a) \\ &\qquad\qquad (\text{by Lemma 2.9.10 } \textbf{(g)}\text{, applied to } b \text{ and } a \text{ instead of } a \text{ and } b) \\ &= \operatorname{Div}(a,b) \qquad (\text{by Lemma 2.9.10 } \textbf{(b)}).\end{aligned}$$

This proves Lemma 2.9.10 **(h)**.

(i) Let $a, b \in \mathbb{Z}$ satisfy $a \mid b$. From $a \mid b$, we obtain $b \equiv 0 \mod a$. Hence, Lemma 2.9.10 **(d)** (applied to $c = 0$) yields $\operatorname{Div}(a,b) = \operatorname{Div}(a,0) = \operatorname{Div}(a)$ (by Lemma 2.9.10 **(a)**). This proves Lemma 2.9.10 **(i)**.

(j) The definition of Div shows that $\operatorname{Div}(b_1, b_2, \ldots, b_k) \subseteq \mathbb{Z}$ for any finitely many integers $b_1, b_2, \ldots, b_k$. Thus, in particular, $\operatorname{Div}() \subseteq \mathbb{Z}$. We shall next prove that $\mathbb{Z} \subseteq \operatorname{Div}()$.

Indeed, let $x \in \mathbb{Z}$. Let us denote the empty list $()$ of integers by $(b_1, b_2, \ldots, b_0)$. Then, $(b_1, b_2, \ldots, b_0) = ()$.

But $x \mid b_i$ for all $i \in \{1, 2, \ldots, 0\}$ (indeed, this is vacuously true, since there exists no $i \in \{1, 2, \ldots, 0\}$). In other words, x is a common divisor of $(b_1, b_2, \ldots, b_0)$ (by the definition of "common divisor"). In other words, $x \in \operatorname{Div}(b_1, b_2, \ldots, b_0)$ (by the definition of $(b_1, b_2, \ldots, b_0)$). In other words, $x \in \operatorname{Div}()$ (since $(b_1, b_2, \ldots, b_0) = ()$).

Now, forget that we fixed x. We thus have proven that $x \in \operatorname{Div}()$ for each $x \in \mathbb{Z}$. In other words, $\mathbb{Z} \subseteq \operatorname{Div}()$. Combining this with $\operatorname{Div}() \subseteq \mathbb{Z}$, we obtain $\operatorname{Div}() = \mathbb{Z}$. This proves Lemma 2.9.10 **(j)**. □

Proof of Proposition 2.9.7. **(a)** Let $a \in \mathbb{Z}$. Definition 2.9.6 (specifically, its case when $b_1, b_2, \ldots, b_k$ are all 0) shows that $\gcd(0,0) = 0$ and $\gcd(0) = 0$. Combining this with $|0| = 0$, we obtain $\gcd(0,0) = \gcd(0) = |0|$. In other words, Proposition 2.9.7 **(a)** holds if $a = 0$. Thus, for the rest of this proof, we WLOG assume that $a \neq 0$. Hence, the two integers $a, 0$ are not all zero. Thus, $\gcd(a,0)$ is defined to be the largest element of the set $\operatorname{Div}(a,0)$ (by Definition 2.9.6). Likewise, $\gcd(a)$ is the largest element of the set $\operatorname{Div}(a)$.

Lemma 2.9.10 **(a)** yields $\operatorname{Div}(a,0) = \operatorname{Div}(a)$. Thus, Lemma 2.9.9 (applied to $(a,0)$ and (a) instead of $(b_1, b_2, \ldots, b_k)$ and $(c_1, c_2, \ldots, c_\ell)$) yields $\gcd(a,0) = \gcd(a)$.

For any integer x, we have the following chain of equivalences:

$$\begin{aligned}
&(x \in \operatorname{Div}(a)) \\
&\Longleftrightarrow (x \text{ is a common divisor of } a) \qquad (\text{by the definition of } \operatorname{Div}(a)) \\
&\Longleftrightarrow (x \mid a) \qquad (\text{by the definition of a ``common divisor''}) \\
&\Longleftrightarrow (x \text{ is a divisor of } a).
\end{aligned}$$

Thus, $\operatorname{Div}(a)$ is the set of all divisors of a.

Exercise 2.2.1 **(b)** yields $|a| \mid a$. In other words, $|a|$ is a divisor of a.

Moreover, a is nonzero (since $a \neq 0$). Hence, Proposition 2.9.2 **(c)** (applied to $b = a$) shows that all divisors of a belong to the set $\{-|a|, -|a|+1, \ldots, |a|\} \setminus \{0\}$. Hence, they belong to the set $\{-|a|, -|a|+1, \ldots, |a|\}$, and thus are $\leq |a|$.

Recall that $|a|$ is a divisor of a. Since we also know that all divisors of a are $\leq |a|$, we can thus conclude that $|a|$ is the **largest** divisor of a. In other words, $|a|$ is the largest element of the set $\operatorname{Div}(a)$ (since $\operatorname{Div}(a)$ is the set of all divisors of a). In other words, $|a|$ is $\gcd(a)$ (since $\gcd(a)$ is the largest element of the set $\operatorname{Div}(a)$). Thus, $\gcd(a) = |a|$. Combining this with $\gcd(a,0) = \gcd(a)$, this yields $\gcd(a,0) = \gcd(a) = |a|$. Thus, Proposition 2.9.7 **(a)** is finally proven.

(b) Let $a, b \in \mathbb{Z}$. Lemma 2.9.10 **(b)** yields $\operatorname{Div}(a,b) = \operatorname{Div}(b,a)$. Thus, Lemma 2.9.9 (applied to (a,b) and (b,a) instead of $(b_1, b_2, \ldots, b_k)$ and $(c_1, c_2, \ldots, c_\ell)$) yields $\gcd(a,b) = \gcd(b,a)$. This proves Proposition 2.9.7 **(b)**.

(c) Let $a, b, u \in \mathbb{Z}$. Then, Lemma 2.9.10 **(c)** yields $\operatorname{Div}(a, ua+b) = \operatorname{Div}(a,b)$. Thus, Lemma 2.9.9 (applied to $(a, ua+b)$ and (a,b) instead of $(b_1, b_2, \ldots, b_k)$ and $(c_1, c_2, \ldots, c_\ell)$) yields $\gcd(a, ua+b) = \gcd(a,b)$. This proves Proposition 2.9.7 **(c)**.

(d) Let $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \operatorname{mod} a$. Then, Lemma 2.9.10 **(d)** yields $\operatorname{Div}(a,b) = \operatorname{Div}(a,c)$. Thus, Lemma 2.9.9 (applied to (a,b) and (a,c) instead of $(b_1, b_2, \ldots, b_k)$ and $(c_1, c_2, \ldots, c_\ell)$) yields $\gcd(a,b) = \gcd(a,c)$. This proves Proposition 2.9.7 **(d)**.

(e) Let $a, b \in \mathbb{Z}$ be such that a is positive. Then, Lemma 2.9.10 **(e)** yields $\operatorname{Div}(a,b) = \operatorname{Div}(a, b\%a)$. Thus, Lemma 2.9.9 (applied to (a,b) and $(a, b\%a)$ instead of $(b_1, b_2, \ldots, b_k)$ and $(c_1, c_2, \ldots, c_\ell)$) yields $\gcd(a,b) = \gcd(a, b\%a)$. This proves Proposition 2.9.7 **(e)**.

(f) Let $a, b \in \mathbb{Z}$. We must prove that $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$.

If the two integers a, b are all 0, then this is obvious[17]. Hence, for the rest of this proof, we WLOG assume that a, b are not all 0. Thus, $\gcd(a,b)$ is defined to be

[17] *Proof.* Assume that a, b are all 0. Then, $a = 0 = \gcd(a,b) \cdot 0$, so that $\gcd(a,b) \mid a$; similarly, $\gcd(a,b) \mid b$. Hence, we have proven that $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ if the integers a, b are all 0.

the largest element of the set $\operatorname{Div}(a,b)$ (by Definition 2.9.6). Hence, $\gcd(a,b)$ is an element of this set $\operatorname{Div}(a,b)$. In other words, $\gcd(a,b)$ is a common divisor of a and b (by the definition of $\operatorname{Div}(a,b)$). In other words, $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$. This proves Proposition 2.9.7 **(f)**.

(g) Let $a,b \in \mathbb{Z}$. Then, Lemma 2.9.10 **(g)** yields $\operatorname{Div}(-a,b) = \operatorname{Div}(a,b)$. Thus, Lemma 2.9.9 (applied to $(-a,b)$ and (a,b) instead of $(b_1,b_2,\ldots,b_k)$ and $(c_1,c_2,\ldots,c_\ell)$) yields $\gcd(-a,b) = \gcd(a,b)$. This proves Proposition 2.9.7 **(g)**.

(h) Let $a,b \in \mathbb{Z}$. Then, Lemma 2.9.10 **(h)** yields $\operatorname{Div}(a,-b) = \operatorname{Div}(a,b)$. Thus, Lemma 2.9.9 (applied to $(a,-b)$ and (a,b) instead of $(b_1,b_2,\ldots,b_k)$ and $(c_1,c_2,\ldots,c_\ell)$) yields $\gcd(a,-b) = \gcd(a,b)$. This proves Proposition 2.9.7 **(h)**.

(i) Let $a,b \in \mathbb{Z}$ satisfy $a \mid b$. From $a \mid b$, we obtain $b \equiv 0 \mod a$. Hence, Proposition 2.9.7 **(d)** (applied to $c = 0$) yields $\gcd(a,b) = \gcd(a,0) = |a|$ (by Proposition 2.9.7 **(a)**). This proves Proposition 2.9.7 **(i)**.

(j) The empty list of integers $()$ has the property that all its entries are 0 (indeed, this is vacuously true because it has no entries at all). Thus, its greatest common divisor is defined to be 0 (by the "If $b_1,b_2,\ldots,b_k$ are not all 0" case of Definition 2.9.6). In other words, $\gcd() = 0$. This proves Proposition 2.9.7 **(j)**. □

Remark 2.9.11. Proposition 2.9.7 **(c)** says that if we add a multiple of a to b, then $\gcd(a,b)$ does not change. Similarly, if we add a multiple of b to a, then $\gcd(a,b)$ does not change (i.e., we have $\gcd(vb+a,b) = \gcd(a,b)$ for all $a,b,v \in \mathbb{Z}$).

However, if we **simultaneously** add a multiple of a to b and a multiple of b to a, then $\gcd(a,b)$ may well change: i.e., we may have $\gcd(vb+a, ua+b) \neq \gcd(a,b)$ for all $a,b,u,v \in \mathbb{Z}$. Examples are easy to find (just take $v = 1$ and $u = 1$).

Proposition 2.9.7 gives a quick way to compute $\gcd(a,b)$ for two nonnegative integers a and b, by repeatedly applying division with remainder. For example, let us compute $\gcd(210,45)$ as follows:

$$\begin{aligned}
\gcd(210,45) &= \gcd(45,210) && \text{(by Proposition 2.9.7 } \textbf{(b)}\text{)} \\
&= \gcd\left(45, \underbrace{210\%45}_{=30}\right) && \text{(by Proposition 2.9.7 } \textbf{(e)}\text{)} \\
&= \gcd(45,30) \\
&= \gcd(30,45) && \text{(by Proposition 2.9.7 } \textbf{(b)}\text{)} \\
&= \gcd\left(30, \underbrace{45\%30}_{=15}\right) && \text{(by Proposition 2.9.7 } \textbf{(e)}\text{)} \\
&= \gcd(30,15) \\
&= \gcd(15,30) && \text{(by Proposition 2.9.7 } \textbf{(b)}\text{)} \\
&= \gcd\left(15, \underbrace{30\%15}_{=0}\right) && \text{(by Proposition 2.9.7 } \textbf{(e)}\text{)} \\
&= \gcd(15,0) = |15| && \text{(by Proposition 2.9.7 } \textbf{(a)}\text{)} \\
&= 15.
\end{aligned}$$

This method of computing $\gcd(a,b)$ is called the *Euclidean algorithm*, and is usually much faster than the divisors of a or the divisors of b can be found!

The following exercise shows that the number $\gcd(b_1,b_2,\ldots,b_k)$ depends only on the **set** $\{b_1,b_2,\ldots,b_k\}$, but not on the numbers $b_1,b_2,\ldots,b_k$ themselves. Thus, for example, any integers a, b and c satisfy $\gcd(a,b,c,a) = \gcd(c,a,b)$ (since $\{a,b,c,a\} = \{c,a,b\}$) and $\gcd(a,a,b,a) = \gcd(a,b,b)$ (since $\{a,a,b,a\} = \{a,b,b\}$).

Exercise 2.9.2. Let $b_1,b_2,\ldots,b_k$ be finitely many integers. Let $c_1,c_2,\ldots,c_\ell$ be finitely many integers. Prove that if

$$\{b_1,b_2,\ldots,b_k\} = \{c_1,c_2,\ldots,c_\ell\},$$

then

$$\gcd(b_1,b_2,\ldots,b_k) = \gcd(c_1,c_2,\ldots,c_\ell).$$

2.9.4. Bezout's theorem

The following fact about gcds is one of the most important facts in number theory:

Theorem 2.9.12. Let a and b be two integers. Then, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that

$$\gcd(a,b) = xa + yb.$$

Theorem 2.9.12 is often stated as follows: "If a and b are two integers, then $\gcd(a,b)$ is a $\mathbb{Z}$-linear combination of a and b". The notion "$\mathbb{Z}$-linear combination of a and b" simply means "a number of the form $xa + yb$ with $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$" (this is exactly the notion of a "linear combination" in linear algebra, except that now the scalars must come from $\mathbb{Z}$), so this is just a restatement of Theorem 2.9.12.

Theorem 2.9.12 is known as *Bezout's theorem* (or *Bezout's identity*)[18]. We shall prove it in several steps. The first step is to show it when a and b are nonnegative:

Lemma 2.9.13. Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Then, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that

$$\gcd(a,b) = xa + yb.$$

Proof of Lemma 2.9.13. The following proof uses a strategy similar to the Euclidean algorithm (making one of a and b smaller repeatedly until one of a and b becomes 0), and can in fact be viewed as a "protocol" of the algorithm[19].

We use strong induction on $a + b$. Thus, we fix an $n \in \mathbb{N}$, and assume (as induction hypothesis) that Lemma 2.9.13 holds whenever $a + b < n$. We must now prove that Lemma 2.9.13 holds whenever $a + b = n$.

We have assumed that Lemma 2.9.13 holds whenever $a + b < n$. In other words, the following statement holds:

> *Statement 1:* Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$ be such that $a + b < n$. Then, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$.

Now, we must prove that Lemma 2.9.13 holds whenever $a + b = n$. Let us first prove this in the case when $b \geq a$:

> *Statement 2:* Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$ be such that $a + b = n$ and $b \geq a$. Then, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$.

[*Proof of Statement 2:* We are in one of the following two cases:

Case 1: We have $a = 0$.

Case 2: We have $a \neq 0$.

Let us first consider Case 1. In this case, we have $a = 0$. Now, Proposition 2.9.7 **(a)** (applied to b instead of a) yields $\gcd(b,0) = \gcd(b) = |b| \in \{b, -b\}$. In other words, $\gcd(b,0) = ub$ for some $u \in \{1,-1\}$. Consider this u. Now, Proposition 2.9.7 **(b)** yields

$$\gcd(a,b) = \gcd\left(b, \underbrace{a}_{=0}\right) = \gcd(b,0) = ub = 0a + ub.$$

[18] or *Bezout's theorem for integers* if you want to be more precise (as there are similar theorems for other objects)

[19] or, rather, of a more primitive version of the Euclidean algorithm, in which we apply not the full power of Proposition 2.9.7 **(e)** but only the identity $\gcd(a,b) = \gcd(a, b-a)$

Hence, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$ (namely, $x = 0$ and $y = u$). Thus, Statement 2 is proven in Case 1.

Let us next consider Case 2. In this case, we have $a \neq 0$. Hence, $a > 0$ (since $a \in \mathbb{N}$), so that $a + b > b$. Hence, $b < a + b = n$.

From $b \geq a$, we obtain $b - a \in \mathbb{N}$. Moreover, $a \in \mathbb{N}$ and $b - a \in \mathbb{N}$ satisfy $a + (b - a) = b < n$. Therefore, we can apply Statement 1 **to** $b - a$ **instead of** b. Thus we obtain that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a, b - a) = xa + y(b - a)$. Fix two such integers x and y, and denote them by x_0 and y_0. Thus, x_0 and y_0 are two integers such that $\gcd(a, b - a) = x_0 a + y_0 (b - a)$.

Also, Proposition 2.9.7 **(c)** (applied to $u = -1$) yields $\gcd(a, (-1)a + b) = \gcd(a,b)$. Hence,

$$\gcd(a,b) = \gcd\left(a, \underbrace{(-1)a + b}_{=b-a}\right) = \gcd(a, b - a) = x_0 a + y_0 (b - a)$$
$$= x_0 a + y_0 b - y_0 a = (x_0 - y_0) a + y_0 b.$$

Hence, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$ (namely, $x = x_0 - y_0$ and $y = y_0$). Thus, Statement 2 is proven in Case 2.

We have now proven Statement 2 in both Cases 1 and 2. Hence, Statement 2 is always proven.]

Now, we can prove that Lemma 2.9.13 holds whenever $a + b = n$:

> *Statement 3:* Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$ be such that $a + b = n$. Then, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$.

[*Proof of Statement 3:* We are in one of the following two cases:

Case 1: We have $b \geq a$.

Case 2: We have $b < a$.

Let us first consider Case 1. In this case, we have $b \geq a$. Hence, Statement 2 shows that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$. Thus, Statement 3 is proven in Case 1.

Let us next consider Case 2. In this case, we have $b < a$. Hence, $a > b$, so that $a \geq b$. This shows that we can apply Statement 2 **to** b **and** a **instead of** a **and** b. Thus we obtain that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(b,a) = xb + ya$. Fix two such integers x and y, and denote them by x_0 and y_0. Thus, x_0 and y_0 are two integers such that $\gcd(b,a) = x_0 b + y_0 a$. Now, Proposition 2.9.7 **(b)** yields $\gcd(a,b) = \gcd(b,a) = x_0 b + y_0 a = y_0 a + x_0 b$. Hence, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$ (namely, $x = y_0$ and $y = x_0$). Thus, Statement 3 is proven in Case 2.

We have now proven Statement 3 in both Cases 1 and 2. Hence, Statement 3 is always proven.]

By proving Statement 3, we have shown that Lemma 2.9.13 holds whenever $a + b = n$. This completes the induction step. Thus, Lemma 2.9.13 is proven by strong induction. □

Next, we shall prove Theorem 2.9.12 when $a \in \mathbb{N}$ but b may be negative:

> **Lemma 2.9.14.** Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Then, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that
> $$\gcd(a, b) = xa + yb.$$

Proof of Lemma 2.9.14. We are in one of the following two cases:

Case 1: We have $b \geq 0$.

Case 2: We have $b < 0$.

Let us first consider Case 1. In this case, we have $b \geq 0$. Thus, $b \in \mathbb{N}$ (since $b \in \mathbb{Z}$). Therefore, Lemma 2.9.13 shows that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a, b) = xa + yb$. Thus, Lemma 2.9.14 is proven in Case 1.

Let us now consider Case 2. In this case, we have $b < 0$. Hence, $-b > 0$, so that $-b \in \mathbb{N}$ (since $-b \in \mathbb{Z}$). Therefore, Lemma 2.9.13 (applied to $-b$ instead of b) shows that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a, -b) = xa + y(-b)$. Fix such integers, and denote them by x_0 and y_0. Thus, $x_0 \in \mathbb{Z}$ and $y_0 \in \mathbb{Z}$ are integers such that $\gcd(a, -b) = x_0 a + y_0(-b)$.

Now, Proposition 2.9.7 **(h)** yields $\gcd(a, -b) = \gcd(a, b)$. Hence,

$$\gcd(a, b) = \gcd(a, -b) = x_0 a + y_0(-b) = x_0 a + (-y_0) b.$$

Hence, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a, b) = xa + yb$ (namely, $x = x_0$ and $y = -y_0$). Thus, Lemma 2.9.14 is proven in Case 2.

We have now proven Lemma 2.9.14 in both Cases 1 and 2. Hence, Lemma 2.9.14 is proven. □

Now, we can prove the whole Theorem 2.9.12:

Proof of Theorem 2.9.12. Theorem 2.9.12 can be derived from Lemma 2.9.14 in the same way as Lemma 2.9.14 was derived from Lemma 2.9.13 (except that this time, we have to distinguish between the cases $a \geq 0$ and $a < 0$, and we have to use Proposition 2.9.7 **(g)** instead of Proposition 2.9.7 **(h)**). Again, let us give the detailed argument for the sake of completeness:

We are in one of the following two cases:

Case 1: We have $a \geq 0$.

Case 2: We have $a < 0$.

Let us first consider Case 1. In this case, we have $a \geq 0$. Thus, $a \in \mathbb{N}$ (since $a \in \mathbb{Z}$). Therefore, Lemma 2.9.14 shows that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a, b) = xa + yb$. Thus, Theorem 2.9.12 is proven in Case 1.

Let us now consider Case 2. In this case, we have $a < 0$. Hence, $-a > 0$, so that $-a \in \mathbb{N}$ (since $-a \in \mathbb{Z}$). Therefore, Lemma 2.9.14 (applied to $-a$ instead of a) shows that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(-a, b) = x(-a) + yb$. Fix such integers, and denote them by x_0 and y_0. Thus, $x_0 \in \mathbb{Z}$ and $y_0 \in \mathbb{Z}$ are integers such that $\gcd(-a, b) = x_0(-a) + y_0 b$.

Now, Proposition 2.9.7 **(g)** yields $\gcd(-a, b) = \gcd(a, b)$. Hence,

$$\gcd(a, b) = \gcd(-a, b) = x_0(-a) + y_0 b = (-x_0) a + y_0 b.$$

Hence, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$ (namely, $x = -x_0$ and $y = y_0$). Thus, Theorem 2.9.12 is proven in Case 2.

We have now proven Theorem 2.9.12 in both Cases 1 and 2. Hence, Theorem 2.9.12 is proven. □

Exercise 2.9.3. Let u be an integer.

(a) Prove that $u^b - 1 \equiv u^a - 1 \mod u^{b-a} - 1$ for any $a \in \mathbb{N}$ and $b \in \mathbb{N}$ satisfying $b \geq a$.

(b) Prove that $\gcd\left(u^a - 1, u^b - 1\right) = \left|u^{\gcd(a,b)} - 1\right|$ for all $a \in \mathbb{N}$ and $b \in \mathbb{N}$.

2.9.5. First applications of Bezout's theorem

An important corollary of Theorem 2.9.12 is the following fact:

Theorem 2.9.15. Let $a, b \in \mathbb{Z}$. Then:

(a) For each $m \in \mathbb{Z}$, we have the following logical equivalence:

$$(m \mid a \text{ and } m \mid b) \iff (m \mid \gcd(a,b)). \tag{21}$$

(b) The common divisors of a and b are precisely the divisors of $\gcd(a,b)$.

(c) We have $\operatorname{Div}(a,b) = \operatorname{Div}(\gcd(a,b))$.

The three parts of this theorem are saying the same thing from slightly different perspectives; the importance of the theorem nevertheless justifies this repetition. To prove the theorem, we first show the following:

Lemma 2.9.16. Let $m, a, b \in \mathbb{Z}$ be such that $m \mid a$ and $m \mid b$. Then, $m \mid \gcd(a,b)$.

Proof of Lemma 2.9.16. Theorem 2.9.12 shows that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that

$$\gcd(a,b) = xa + yb. \tag{22}$$

Consider these x and y. Now, $m \mid a \mid xa$, so that $xa \equiv 0 \mod m$. Also, $m \mid b \mid yb$, thus $yb \equiv 0 \mod m$. Adding the congruences $xa \equiv 0 \mod m$ and $yb \equiv 0 \mod m$ together, we find $xa + yb \equiv 0 + 0 = 0 \mod m$; in other words, $m \mid xa + yb$. In view of (22), this rewrites as $m \mid \gcd(a,b)$. This proves Lemma 2.9.16. □

Proof of Theorem 2.9.15. **(a)** Let $m \in \mathbb{Z}$. In order to prove (21), we need to prove the "$\Longrightarrow$" and "$\Longleftarrow$" directions of the equivalence (21). But this is easy: The "$\Longrightarrow$" direction is just the statement of Lemma 2.9.16, whereas the "$\Longleftarrow$" direction is trivial (to wit: if $m \mid \gcd(a,b)$, then

$$m \mid \gcd(a,b) \mid a \qquad \text{(by Proposition 2.9.7 } \textbf{(f)}\text{)}$$

and

$$m \mid \gcd(a,b) \mid b \qquad \text{(by Proposition 2.9.7 } \textbf{(f)}\text{)},$$

and thus $(m \mid a \text{ and } m \mid b)$). Hence, the equivalence (21) is proven. This proves Theorem 2.9.15 **(a)**.

(b) The common divisors of a and b are precisely the integers m that satisfy $(m \mid a \text{ and } m \mid b)$ (by the definition of "common divisor"). In view of the equivalence (21), this rewrites as follows: The common divisors of a and b are precisely the integers m that satisfy $m \mid \gcd(a,b)$. In other words, the common divisors of a and b are precisely the divisors of $\gcd(a,b)$. This proves Theorem 2.9.15 **(b)**.

(c) Recall that each $c \in \mathbb{Z}$ satisfies

$$\begin{aligned}\operatorname{Div}(c) &= \{\text{the common divisors of } c\} \qquad (\text{by the definition of } \operatorname{Div}(c)) \\ &= \{\text{the integers } x \text{ such that } x \mid c\} \\ &\qquad (\text{by the definition of "common divisors"}) \\ &= \{\text{the divisors of } c\}.\end{aligned}$$

Applying this to $c = \gcd(a,b)$, we obtain

$$\operatorname{Div}(\gcd(a,b)) = \{\text{the divisors of } \gcd(a,b)\}. \tag{23}$$

The definition of $\operatorname{Div}(a,b)$ yields

$$\begin{aligned}\operatorname{Div}(a,b) &= \{\text{the common divisors of } a \text{ and } b\} \\ &= \{\text{the divisors of } \gcd(a,b)\} \qquad (\text{by Theorem 2.9.15 } \textbf{(b)}) \\ &= \operatorname{Div}(\gcd(a,b)) \qquad (\text{by (23)}).\end{aligned}$$

This proves Theorem 2.9.15 **(c)**. □

The following corollary of Theorem 2.9.12 let us "combine" two divisibilities $a \mid c$ and $b \mid c$. In fact, Proposition 2.2.4 **(c)** would already allow us to "combine" them to form $ab \mid cc = c^2$; but we can also "combine" them to $ab \mid \gcd(a,b) \cdot c$ using the following fact:

Theorem 2.9.17. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid c$ and $b \mid c$. Then, $ab \mid \gcd(a,b) \cdot c$.

Example 2.9.18. Let $a = 6$ and $b = 10$ and $c = 30$. Then, $a = 6 \mid 30 = c$ and $b = 10 \mid 30 = c$. Thus, Theorem 2.9.17 yields $ab \mid \gcd(a,b) \cdot c$. And indeed, this is true, since $ab = 6 \cdot 10 \mid 2 \cdot 30 = \gcd(a,b) \cdot c$ (because $\gcd(a,b) = \gcd(6,10) = 2$). Note that this latter divisibility is actually an equality: we have $6 \cdot 10 = 2 \cdot 30$. Note also that we do **not** obtain $ab \mid c$ (and indeed, this does not hold).

Proof of Theorem 2.9.17. Theorem 2.9.12 yields that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$. Consider these x and y.

We have $a \mid c$. In other words, there exists an integer u such that $c = au$. Consider this u.

We have $b \mid c$. In other words, there exists an integer v such that $c = bv$. Consider this v.

Now,

$$\underbrace{\gcd(a,b)}_{=xa+yb} \cdot c = (xa+yb)\,c = xa\underbrace{c}_{=bv} + yb\underbrace{c}_{=au} = xabv + ybau = ab\,(xv+yu)\,.$$

Thus, there exists an integer d such that $\gcd(a,b)\cdot c = abd$ (namely, $d = xv+yu$). In other words, $ab \mid \gcd(a,b)\cdot c$. This proves Theorem 2.9.17. □

Here is another corollary of Theorem 2.9.12 whose usefulness will become clearer later on:

Theorem 2.9.19. Let $a,b,c \in \mathbb{Z}$ satisfy $a \mid bc$. Then, $a \mid \gcd(a,b)\cdot c$.

At this point, you should see that Theorem 2.9.19 allows "strengthening" divisibilities: You give it a "weak" divisibility $a \mid bc$, and obtain a "stronger" divisibility $a \mid \gcd(a,b)\cdot c$ from it (stronger because $\gcd(a,b)$ is usually smaller than b).

Proof of Theorem 2.9.19. Theorem 2.9.12 yields that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa+yb$. Consider these x and y.

We have $a \mid bc \mid ybc$; in other words, $ybc \equiv 0 \bmod a$. Also, $a \mid axc$, so that $axc \equiv 0 \bmod a$. Adding the two congruences $axc \equiv 0 \bmod a$ and $ybc \equiv 0 \bmod a$ together, we obtain $axc + ybc \equiv 0+0 = 0 \bmod a$. In view of $axc+ybc = \underbrace{(xa+yb)}_{=\gcd(a,b)}c = \gcd(a,b)\cdot c$, this rewrites as $\gcd(a,b)\cdot c \equiv 0 \bmod a$. In other words, $a \mid \gcd(a,b)\cdot c$. This proves Theorem 2.9.19. □

Theorem 2.9.20. Let $s,a,b \in \mathbb{Z}$. Then,

$$\gcd(sa,sb) = |s|\gcd(a,b)\,.$$

Proof of Theorem 2.9.20. We shall prove that the two integers $\gcd(sa,sb)$ and $s\gcd(a,b)$ mutually divide each other (i.e., they satisfy $\gcd(sa,sb) \mid s\gcd(a,b)$ and $s\gcd(a,b) \mid \gcd(sa,sb)$). Then, Exercise 2.2.2 will let us conclude that $|\gcd(sa,sb)| = |s\gcd(a,b)|$. This will then rewrite as $\gcd(sa,sb) = |s|\gcd(a,b)$, and we will be done. (This trick is actually a common strategy for proving equalities between gcds.)

Here is the argument in detail. For the sake of brevity, let us set $g = \gcd(sa,sb)$ and $h = s\gcd(a,b)$. So our first goal is to prove that $g \mid h$ and $h \mid g$.

Proof of $g \mid h$: Theorem 2.9.12 yields that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa+yb$. Consider these x and y.

Proposition 2.9.7 **(f)** (applied to sa and sb instead of a and b) yields that $\gcd(sa,sb) \mid sa$ and $\gcd(sa,sb) \mid sb$. From $g = \gcd(sa,sb) \mid sa$, we obtain $g \mid sa \mid xsa$, thus $xsa \equiv 0 \bmod g$. Similarly, $ysb \equiv 0 \bmod g$. Adding these two congruences together, we find $xsa + ysb \equiv 0 \bmod g$. Now,

$$h = s\underbrace{\gcd(a,b)}_{=xa+yb} = s\,(xa+yb) = xsa+ysb \equiv 0 \bmod g.$$

In other words, $g \mid h$. Thus, we have proven $g \mid h$.

Proof of $h \mid g$: Proposition 2.9.7 **(f)** yields $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$. Also, $s \mid s$. Hence, Proposition 2.2.4 **(c)** (applied to $s, \gcd(a,b), s, a$ instead of a_1, a_2, b_1, b_2) yields $s\gcd(a,b) \mid sa$. Similarly, $s\gcd(a,b) \mid sb$. Hence, Lemma 2.9.16 (applied to $s\gcd(a,b)$, sa and sb instead of m, a and b) yields $s\gcd(a,b) \mid \gcd(sa,sb)$. In view of $g = \gcd(sa,sb)$ and $h = s\gcd(a,b)$, this rewrites as $h \mid g$. So we have proven $h \mid g$.

Now, Exercise 2.2.2 (applied to g and h instead of a and b) yields $|g| = |h|$.

But recall that a gcd of any finitely many integers is nonnegative (by Definition 2.9.6). Hence, in particular, $\gcd(a,b)$ and $\gcd(sa,sb)$ are nonnegative. From $g = \gcd(sa,sb)$, we obtain

$$|g| = |\gcd(sa,sb)| = \gcd(sa,sb)$$

(since $\gcd(sa,sb)$ is nonnegative). Also, from $h = s\gcd(a,b)$, we obtain

$$|h| = |s\gcd(a,b)| = |s| \cdot \underbrace{|\gcd(a,b)|}_{\substack{=\gcd(a,b) \\ \text{(since } \gcd(a,b) \\ \text{is nonnegative)}}} \qquad \text{(by (3))}$$
$$= |s| \gcd(a,b).$$

Hence,

$$\gcd(sa,sb) = |g| = |h| = |s| \gcd(a,b).$$

This proves Theorem 2.9.20. □

Exercise 2.9.4. Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$. Prove that

$$\gcd(a_1,a_2) \mid \gcd(b_1,b_2).$$

Exercise 2.9.5. Let $a, b \in \mathbb{Z}$.

(a) Prove that $\gcd(a, |b|) = \gcd(a,b)$.

(b) Prove that $\gcd(|a|, b) = \gcd(a,b)$.

(c) Prove that $\gcd(|a|, |b|) = \gcd(a,b)$.

2.9.6. gcds of multiple numbers

The following theorem generalizes some of the previous facts to gcds of multiple integers:

Theorem 2.9.21. Let $b_1, b_2, \ldots, b_k$ be integers.

(a) For each $m \in \mathbb{Z}$, we have the following logical equivalence:

$$(m \mid b_i \text{ for all } i \in \{1,2,\ldots,k\}) \iff (m \mid \gcd(b_1,b_2,\ldots,b_k)).$$

(b) The common divisors of $b_1, b_2, \ldots, b_k$ are precisely the divisors of $\gcd(b_1, b_2, \ldots, b_k)$.

(c) We have $\operatorname{Div}(b_1, b_2, \ldots, b_k) = \operatorname{Div}(\gcd(b_1, b_2, \ldots, b_k))$.

(d) If $k > 0$, then

$$\gcd(b_1, b_2, \ldots, b_k) = \gcd(\gcd(b_1, b_2, \ldots, b_{k-1}), b_k).$$

Proof of Theorem 2.9.21. Forget that we fixed $b_1, b_2, \ldots, b_k$. Rather than prove the four parts of Theorem 2.9.21 separately, we shall prove them together as a package.

We shall proceed by induction on k:

Induction base: Theorem 2.9.21 holds for $k = 0$.

[*Proof:* This is a straightforward exercise in dealing with empty sets, 0-tuples and vacuous truths. For the sake of completeness, here is the full argument:

Assume that $k = 0$. We must prove that Theorem 2.9.21 holds.

Let $b_1, b_2, \ldots, b_k$ be integers. Of course, these are 0 integers, since $k = 0$.

We don't have $k > 0$ (since $k = 0$). Hence, Theorem 2.9.21 **(d)** is vacuously true.

All of $b_1, b_2, \ldots, b_k$ are 0 (indeed, this is vacuously true). Thus, $\gcd(b_1, b_2, \ldots, b_k) = 0$ (by Definition 2.9.6).

For each $m \in \mathbb{Z}$, we have the logical equivalence

$$\begin{aligned}
&(m \mid b_i \text{ for all } i \in \{1, 2, \ldots, k\}) \\
\iff &(\text{truth}) \qquad (\text{since there exists no } i \in \{1, 2, \ldots, k\}) \\
\iff &(m \mid 0) \qquad (\text{since } m \mid 0 \text{ is always true}) \\
\iff &(m \mid \gcd(b_1, b_2, \ldots, b_k)) \qquad (\text{since } 0 = \gcd(b_1, b_2, \ldots, b_k)).
\end{aligned}$$

This proves Theorem 2.9.21 **(a)** (in the case $k = 0$, that is). Parts **(b)** and **(c)** of Theorem 2.9.21 are restatements of Theorem 2.9.21 **(a)** and can be derived from it in the same way as we derived parts **(b)** and **(c)** of Theorem 2.9.15 from Theorem 2.9.15 **(a)**.

Thus, all four parts of Theorem 2.9.21 are proven for $k = 0$. This completes the induction base.]

Induction step: Let ℓ be a positive integer. Assume that Theorem 2.9.21 holds for $k = \ell - 1$. We must prove that Theorem 2.9.21 holds for $k = \ell$.

We have assumed that Theorem 2.9.21 holds for $k = \ell - 1$. In other words, the following statement holds:

> *Statement 1:* Let $b_1, b_2, \ldots, b_{\ell-1}$ be integers.
>
> **(a)** For each $m \in \mathbb{Z}$, we have the following logical equivalence:
>
> $$(m \mid b_i \text{ for all } i \in \{1, 2, \ldots, \ell - 1\}) \iff (m \mid \gcd(b_1, b_2, \ldots, b_{\ell-1})).$$
>
> **(b)** The common divisors of $b_1, b_2, \ldots, b_{\ell-1}$ are precisely the divisors of $\gcd(b_1, b_2, \ldots, b_{\ell-1})$.
>
> **(c)** We have $\operatorname{Div}(b_1, b_2, \ldots, b_{\ell-1}) = \operatorname{Div}(\gcd(b_1, b_2, \ldots, b_{\ell-1}))$.
>
> **(d)** If $\ell - 1 > 0$, then
>
> $$\gcd(b_1, b_2, \ldots, b_{\ell-1}) = \gcd\left(\gcd\left(b_1, b_2, \ldots, b_{(\ell-1)-1}\right), b_{\ell-1}\right).$$

Recall that we must prove that Theorem 2.9.21 holds for $k = \ell$. In other words, we must prove the following statement:

> *Statement 2:* Let $b_1, b_2, \ldots, b_\ell$ be integers.
>
> **(a)** For each $m \in \mathbb{Z}$, we have the following logical equivalence:
>
> $$(m \mid b_i \text{ for all } i \in \{1, 2, \ldots, \ell\}) \iff (m \mid \gcd(b_1, b_2, \ldots, b_\ell)).$$
>
> **(b)** The common divisors of $b_1, b_2, \ldots, b_\ell$ are precisely the divisors of $\gcd(b_1, b_2, \ldots, b_\ell)$.
>
> **(c)** We have $\operatorname{Div}(b_1, b_2, \ldots, b_\ell) = \operatorname{Div}(\gcd(b_1, b_2, \ldots, b_\ell))$.
>
> **(d)** If $\ell > 0$, then
>
> $$\gcd(b_1, b_2, \ldots, b_\ell) = \gcd(\gcd(b_1, b_2, \ldots, b_{\ell-1}), b_\ell).$$

[*Proof of Statement 2:* **(d)** Let us begin with part **(d)**. Assume that $\ell > 0$ (though we already know that this is true).

Let $c = \gcd(b_1, b_2, \ldots, b_{\ell-1})$.

Let $g = \gcd(b_1, b_2, \ldots, b_\ell)$ and $h = \gcd(c, b_\ell)$.

If the integers $b_1, b_2, \ldots, b_\ell$ are all 0, then Statement 2 **(d)** holds[20]. Hence, for the rest of this proof, we WLOG assume that the integers $b_1, b_2, \ldots, b_\ell$ are not all 0. Therefore, $\gcd(b_1, b_2, \ldots, b_\ell)$ is the largest element of the set $\operatorname{Div}(b_1, b_2, \ldots, b_\ell)$ (by Definition 2.9.6). In other words, g is the largest element of the set $\operatorname{Div}(b_1, b_2, \ldots, b_\ell)$ (since $g = \gcd(b_1, b_2, \ldots, b_\ell)$).

Furthermore, the two integers c and b_ℓ are not all 0 [21]. Hence, $\gcd(c, b_\ell)$ is the largest element of the set $\operatorname{Div}(c, b_\ell)$ (by Definition 2.9.6). In other words, h is the largest element of the set $\operatorname{Div}(c, b_\ell)$ (since $h = \gcd(c, b_\ell)$).

We intend to show that $g = h$. For that, it suffices to prove $g \leq h$ and $h \leq g$.

Proof of $g \leq h$: Recall that g is the largest element of the set $\operatorname{Div}(b_1, b_2, \ldots, b_\ell)$. Therefore, $g \in \operatorname{Div}(b_1, b_2, \ldots, b_\ell)$. In other words, g is a common divisor of $b_1, b_2, \ldots, b_\ell$. Hence, $g \mid b_i$ for each $i \in \{1, 2, \ldots, \ell\}$. Thus, in particular, $g \mid b_i$

[20] *Proof.* Assume that $b_1, b_2, \ldots, b_\ell$ are all 0. Then, $\gcd(b_1, b_2, \ldots, b_\ell) = 0$ (by Definition 2.9.6). Moreover, $b_1, b_2, \ldots, b_{\ell-1}$ are all 0 (since $b_1, b_2, \ldots, b_\ell$ are all 0), and thus $\gcd(b_1, b_2, \ldots, b_{\ell-1}) = 0$. Finally, $b_\ell = 0$ (since $b_1, b_2, \ldots, b_\ell$ are all 0). Comparing $\gcd(b_1, b_2, \ldots, b_\ell) = 0$ with $\gcd\left(\underbrace{\gcd(b_1, b_2, \ldots, b_{\ell-1})}_{=0}, \underbrace{b_\ell}_{=0}\right) = \gcd(0, 0) = 0$, we obtain $\gcd(b_1, b_2, \ldots, b_\ell) = \gcd(\gcd(b_1, b_2, \ldots, b_{\ell-1}), b_\ell)$. In other words, Statement 2 **(d)** holds.

[21] *Proof.* Assume the contrary. Thus, both c and b_ℓ are 0. Thus, in particular, $b_\ell = 0$. If the $\ell - 1$ integers $b_1, b_2, \ldots, b_{\ell-1}$ were all 0, then the ℓ integers $b_1, b_2, \ldots, b_\ell$ would be all 0 (since $b_\ell = 0$), which would contradict the fact that the integers $b_1, b_2, \ldots, b_\ell$ are not all 0. Hence, the $\ell - 1$ integers $b_1, b_2, \ldots, b_{\ell-1}$ are not all 0. Thus, $\gcd(b_1, b_2, \ldots, b_{\ell-1})$ is a positive integer (by Definition 2.9.6). Thus, $\gcd(b_1, b_2, \ldots, b_{\ell-1}) > 0$, so that $c = \gcd(b_1, b_2, \ldots, b_{\ell-1}) > 0$. But this contradicts the fact that c is 0. This contradiction shows that our assumption was false, qed.

for each $i \in \{1, 2, \ldots, \ell - 1\}$. But Statement 1 **(a)** (applied to $m = g$) shows that we have the equivalence

$$(g \mid b_i \text{ for all } i \in \{1, 2, \ldots, \ell - 1\}) \iff (g \mid \gcd(b_1, b_2, \ldots, b_{\ell-1})).$$

Hence, we have $g \mid \gcd(b_1, b_2, \ldots, b_{\ell-1})$ (since we know that $g \mid b_i$ for all $i \in \{1, 2, \ldots, \ell - 1\}$). In other words, $g \mid c$ (since $c = \gcd(b_1, b_2, \ldots, b_{\ell-1})$). Combining this with $g \mid b_\ell$, we conclude that g is a common divisor of c and b_ℓ. In other words, $g \in \operatorname{Div}(c, b_\ell)$. Therefore, $g \leq h$ (since h is the largest element of the set $\operatorname{Div}(c, b_\ell)$).

Proof of $h \leq g$: Proposition 2.9.7 **(f)** (applied to $a = c$ and $b = b_\ell$) shows that $\gcd(c, b_\ell) \mid c$ and $\gcd(c, b_\ell) \mid b_\ell$. Thus,

$$h = \gcd(c, b_\ell) \mid c = \gcd(b_1, b_2, \ldots, b_{\ell-1}) \qquad \text{and}$$
$$h = \gcd(c, b_\ell) \mid b_\ell.$$

But Statement 1 **(a)** (applied to $m = h$) shows that we have the equivalence

$$(h \mid b_i \text{ for all } i \in \{1, 2, \ldots, \ell - 1\}) \iff (h \mid \gcd(b_1, b_2, \ldots, b_{\ell-1})).$$

Thus, we have ($h \mid b_i$ for all $i \in \{1, 2, \ldots, \ell - 1\}$) (since we have $h \mid \gcd(b_1, b_2, \ldots, b_{\ell-1})$).

This divisibility $h \mid b_i$ holds not only for all $i \in \{1, 2, \ldots, \ell - 1\}$, but also for $i = \ell$ (because $h \mid b_\ell$). Thus, we conclude that $h \mid b_i$ for all $i \in \{1, 2, \ldots, \ell\}$. In other words, h is a common divisor of $b_1, b_2, \ldots, b_\ell$. In other words, $h \in \operatorname{Div}(b_1, b_2, \ldots, b_\ell)$. Thus, $h \leq g$ (since g is the largest element of the set $\operatorname{Div}(b_1, b_2, \ldots, b_\ell)$).

Combining $h \leq g$ with $g \leq h$, we obtain $g = h$. Comparing this with $g = \gcd(b_1, b_2, \ldots, b_\ell)$, we obtain

$$\gcd(b_1, b_2, \ldots, b_\ell) = h = \gcd(c, b_\ell) = \gcd(\gcd(b_1, b_2, \ldots, b_{\ell-1}), b_\ell)$$

(since $c = \gcd(b_1, b_2, \ldots, b_{\ell-1})$). Hence, Statement 2 **(d)** is proven.

(a) Let $m \in \mathbb{Z}$. Then, we have the equivalence

$$\begin{aligned}
&(m \mid b_i \text{ for all } i \in \{1, 2, \ldots, \ell\}) \\
\iff &\left(\underbrace{(m \mid b_i \text{ for all } i \in \{1, 2, \ldots, \ell - 1\})}_{\substack{\iff (m \mid \gcd(b_1, b_2, \ldots, b_{\ell-1})) \\ \text{(by Statement 1 (a))}}} \text{ and } m \mid b_\ell \right) \\
\iff &(m \mid \gcd(b_1, b_2, \ldots, b_{\ell-1}) \text{ and } m \mid b_\ell) \\
\iff &\left(m \mid \underbrace{\gcd(\gcd(b_1, b_2, \ldots, b_{\ell-1}), b_\ell)}_{\substack{= \gcd(b_1, b_2, \ldots, b_\ell) \\ \text{(by Statement 2 (d), which we have just proved)}}} \right) \\
&\qquad \text{(by Theorem 2.9.15 (a), applied to } a = \gcd(b_1, b_2, \ldots, b_{\ell-1}) \text{ and } b = b_\ell) \\
\iff &(m \mid \gcd(b_1, b_2, \ldots, b_\ell)).
\end{aligned}$$

Thus, Statement 2 **(a)** follows.

Statement 2 **(b)** is a restatement of Statement 2 **(a)** (in the same way that Theorem 2.9.15 **(b)** is a restatement of Theorem 2.9.15 **(a)**).

Statement 2 **(c)** is a restatement of Statement 2 **(b)** (in the same way that Theorem 2.9.15 **(c)** is a restatement of Theorem 2.9.15 **(b)**).]

We are thus done proving Statement 2.

In other words, we have proven that Theorem 2.9.21 holds for $k = \ell$. This completes the induction step. Thus, Theorem 2.9.21 is proven by induction. □

Theorem 2.9.21 **(d)** is the reason why most properties of gcds of multiple numbers can be derived from corresponding properties of gcds of two numbers. For example, we can easily prove the following analogue of Theorem 2.9.20 for gcds of three numbers:

Exercise 2.9.6. Let $s, a, b, c \in \mathbb{Z}$. Prove that $\gcd(sa, sb, sc) = |s| \gcd(a, b, c)$.

More generally, Theorem 2.9.20 can be generalized to any finite number of integers:

Exercise 2.9.7. Let $s \in \mathbb{Z}$, and let $a_1, a_2, \ldots, a_k$ be integers. Prove that $\gcd(sa_1, sa_2, \ldots, sa_k) = |s| \gcd(a_1, a_2, \ldots, a_k)$.

Bezout's theorem (Theorem 2.9.12) also holds for any finite number of integers:

Theorem 2.9.22. Let $b_1, b_2, \ldots, b_k$ be integers. Then, there exist integers $x_1, x_2, \ldots, x_k$ such that

$$\gcd(b_1, b_2, \ldots, b_k) = x_1 b_1 + x_2 b_2 + \cdots + x_k b_k.$$

Once again, we can restate Theorem 2.9.22 by using the concept of a $\mathbb{Z}$-linear combination. Let us define this concept finally:

Definition 2.9.23. Let $b_1, b_2, \ldots, b_k$ be numbers. A *$\mathbb{Z}$-linear combination* of $b_1, b_2, \ldots, b_k$ shall mean a number of the form $x_1 b_1 + x_2 b_2 + \cdots + x_k b_k$, where $x_1, x_2, \ldots, x_k$ are integers.

Thus, Theorem 2.9.22 can be restated as follows:

Theorem 2.9.24. Let $b_1, b_2, \ldots, b_k$ be integers. Then, $\gcd(b_1, b_2, \ldots, b_k)$ is a $\mathbb{Z}$-linear combination of $b_1, b_2, \ldots, b_k$.

Proof of Theorem 2.9.24. We shall prove this by induction on k:

Induction base: The empty list $()$ satisfies $\gcd() = 0$ (by Definition 2.9.6, since all entries of the empty list are 0). But 0 is a $\mathbb{Z}$-linear combination of an empty list of numbers, because $0 = (\text{empty sum})$. In other words, $\gcd()$ is a $\mathbb{Z}$-linear combination of an empty list of numbers (since $\gcd() = 0$). But this is precisely the claim of Theorem 2.9.24 for $k = 0$. Thus, Theorem 2.9.24 holds for $k = 0$. This completes the induction base.

Induction step: Let ℓ be a positive integer. Assume that Theorem 2.9.24 holds for $k = \ell - 1$. We must prove that Theorem 2.9.24 holds for $k = \ell$.

We have assumed that Theorem 2.9.24 holds for $k = \ell - 1$. In other words, the following statement holds:

> *Statement 1:* Let $b_1, b_2, \ldots, b_{\ell-1}$ be integers. Then, $\gcd(b_1, b_2, \ldots, b_{\ell-1})$ is a $\mathbb{Z}$-linear combination of $b_1, b_2, \ldots, b_{\ell-1}$.

Our goal is to prove that Theorem 2.9.24 holds for $k = \ell$. In other words, we must prove the following statement:

> *Statement 2:* Let $b_1, b_2, \ldots, b_\ell$ be integers. Then, $\gcd(b_1, b_2, \ldots, b_\ell)$ is a $\mathbb{Z}$-linear combination of $b_1, b_2, \ldots, b_\ell$.

Proof of Statement 2: Statement 1 shows that $\gcd(b_1, b_2, \ldots, b_{\ell-1})$ is a $\mathbb{Z}$-linear combination of $b_1, b_2, \ldots, b_{\ell-1}$. In other words, there exist $\ell - 1$ integers $y_1, y_2, \ldots, y_{\ell-1}$ such that

$$\gcd(b_1, b_2, \ldots, b_{\ell-1}) = y_1 b_1 + y_2 b_2 + \cdots + y_{\ell-1} b_{\ell-1}.$$

Consider these $y_1, y_2, \ldots, y_{\ell-1}$.

Furthermore, Theorem 2.9.12 (applied to $a = \gcd(b_1, b_2, \ldots, b_{\ell-1})$ and $b = b_\ell$) yields that there exist two integers x and y such that

$$\gcd(\gcd(b_1, b_2, \ldots, b_{\ell-1}), b_\ell) = x \gcd(b_1, b_2, \ldots, b_{\ell-1}) + y b_\ell.$$

Consider these x and y.

Now, $\ell > 0$; thus, Theorem 2.9.21 **(d)** (applied to $k = \ell$) yields

$$\begin{aligned}
\gcd(b_1, b_2, \ldots, b_\ell) &= \gcd(\gcd(b_1, b_2, \ldots, b_{\ell-1}), b_\ell) \\
&= x \underbrace{\gcd(b_1, b_2, \ldots, b_{\ell-1})}_{= y_1 b_1 + y_2 b_2 + \cdots + y_{\ell-1} b_{\ell-1}} + y b_\ell \\
&= x (y_1 b_1 + y_2 b_2 + \cdots + y_{\ell-1} b_{\ell-1}) + y b_\ell \\
&= x y_1 b_1 + x y_2 b_2 + \cdots + x y_{\ell-1} b_{\ell-1} + y b_\ell.
\end{aligned}$$

This is clearly a $\mathbb{Z}$-linear combination of the $b_1, b_2, \ldots, b_\ell$. Thus, $\gcd(b_1, b_2, \ldots, b_\ell)$ is a $\mathbb{Z}$-linear combination of $b_1, b_2, \ldots, b_\ell$. So Statement 2 is proven.

In other words, we have proven that Theorem 2.9.24 holds for $k = \ell$. This completes the induction step. Thus, Theorem 2.9.24 is proven by induction. □

Proof of Theorem 2.9.22. We have just proven Theorem 2.9.24, which is a restatement of Theorem 2.9.22. Thus, Theorem 2.9.22 is also proven. □

For future reference, let us restate Theorem 2.9.21 **(a)** as follows:

Corollary 2.9.25. Let $b_1, b_2, \ldots, b_k$ be integers. For each $m \in \mathbb{Z}$, we have the following logical equivalence:

$$(m \mid b_1 \text{ and } m \mid b_2 \text{ and } \cdots \text{ and } m \mid b_k) \iff (m \mid \gcd(b_1, b_2, \ldots, b_k)).$$

Proof of Corollary 2.9.25. Let $m \in \mathbb{Z}$. Then, we have the following chain of equivalences:

$$\begin{aligned}
&(m \mid b_1 \text{ and } m \mid b_2 \text{ and } \cdots \text{ and } m \mid b_k) \\
&\iff (m \mid b_i \text{ for all } i \in \{1, 2, \ldots, k\}) \\
&\iff (m \mid \gcd(b_1, b_2, \ldots, b_k)) \qquad (\text{by Theorem 2.9.21 } \textbf{(a)}).
\end{aligned}$$

This proves Corollary 2.9.25. □

Theorem 2.9.26. Let $b_1, b_2, \ldots, b_k$ be integers, and let $c_1, c_2, \ldots, c_\ell$ be integers. Then,

$$\begin{aligned}
&\gcd(b_1, b_2, \ldots, b_k, c_1, c_2, \ldots, c_\ell) \\
&= \gcd(\gcd(b_1, b_2, \ldots, b_k), \gcd(c_1, c_2, \ldots, c_\ell)).
\end{aligned}$$

Our proof of this theorem will rely on a simple trick, which we state as a lemma:

Lemma 2.9.27. Let a and b be two integers.

(a) If each $m \in \mathbb{Z}$ satisfies the implication $(m \mid a) \Longrightarrow (m \mid b)$, then $a \mid b$.

(b) If each $m \in \mathbb{Z}$ satisfies the equivalence $(m \mid a) \iff (m \mid b)$, then $|a| = |b|$.

Lemma 2.9.27 **(b)** says that the divisors of an integer a uniquely determine $|a|$ (that is, they uniquely determine a up to sign). Thus, when you want to prove that two integers have the same absolute values, it suffices to prove that they have the same divisors. If you know that your two integers are nonnegative, then you can prove this way that they are equal (since their absolute values are just themselves). This is exactly how we will prove that the left and right hand sides in Theorem 2.9.26 are equal.

Proof of Lemma 2.9.27. **(a)** Assume that each $m \in \mathbb{Z}$ satisfies the implication $(m \mid a) \Longrightarrow (m \mid b)$. Then, applying this to $m = a$, we obtain the implication $(a \mid a) \Longrightarrow (a \mid b)$. Since $a \mid a$ holds, we thus obtain $a \mid b$. This proves Lemma 2.9.27 **(a)**.

(b) Assume that each $m \in \mathbb{Z}$ satisfies the equivalence $(m \mid a) \iff (m \mid b)$. Thus, each $m \in \mathbb{Z}$ satisfies the implication $(m \mid a) \Longrightarrow (m \mid b)$ (since this implication is part of the equivalence we just assumed). Thus, Lemma 2.9.27 **(a)** yields $a \mid b$.

Recall again that each $m \in \mathbb{Z}$ satisfies the equivalence $(m \mid a) \iff (m \mid b)$. Thus, each $m \in \mathbb{Z}$ satisfies the implication $(m \mid b) \Longrightarrow (m \mid a)$ (since this implication is also part of the equivalence). Hence, Lemma 2.9.27 **(a)** (applied to b and a instead of a and b) yields $b \mid a$.

Hence, Exercise 2.2.2 yields $|a| = |b|$. This proves Lemma 2.9.27 **(b)**. □

Lemma 2.9.27 is a simple case of what is known in category theory as the *Yoneda lemma*.

Proof of Theorem 2.9.26. Let $m \in \mathbb{Z}$. Corollary 2.9.25 (applied to $k+\ell$ and $(b_1, b_2, \ldots, b_k, c_1, c_2, \ldots, c_\ell)$ instead of k and $(b_1, b_2, \ldots, b_k)$) shows that we have the following equivalence:

$$\begin{aligned}&(m \mid b_1 \text{ and } m \mid b_2 \text{ and } \cdots \text{ and } m \mid b_k \text{ and } m \mid c_1 \text{ and } m \mid c_2 \text{ and } \cdots \text{ and } m \mid c_\ell)\\ &\iff (m \mid \gcd(b_1, b_2, \ldots, b_k, c_1, c_2, \ldots, c_\ell)).\end{aligned}$$

Hence, we have the following chain of equivalences:

$$\begin{aligned}&(m \mid \gcd(b_1, b_2, \ldots, b_k, c_1, c_2, \ldots, c_\ell))\\ \iff &(m \mid b_1 \text{ and } m \mid b_2 \text{ and } \cdots \text{ and } m \mid b_k \text{ and } m \mid c_1 \text{ and } m \mid c_2 \text{ and } \cdots \text{ and } m \mid c_\ell)\\ \iff &\left(\underbrace{(m \mid b_i \text{ for all } i \in \{1, 2, \ldots, k\})}_{\substack{\iff (m \mid \gcd(b_1, b_2, \ldots, b_k))\\ \text{(by Theorem 2.9.21 \textbf{(a)})}}} \text{ and } \underbrace{(m \mid c_i \text{ for all } i \in \{1, 2, \ldots, \ell\})}_{\substack{\iff (m \mid \gcd(c_1, c_2, \ldots, c_\ell))\\ \text{(by Theorem 2.9.21 \textbf{(a)},}\\ \text{applied to } \ell \text{ and } (c_1, c_2, \ldots, c_\ell)\\ \text{instead of } k \text{ and } (b_1, b_2, \ldots, b_k))}}\right)\\ \iff &(m \mid \gcd(b_1, b_2, \ldots, b_k) \text{ and } m \mid \gcd(c_1, c_2, \ldots, c_\ell))\\ \iff &(m \mid \gcd(\gcd(b_1, b_2, \ldots, b_k), \gcd(c_1, c_2, \ldots, c_\ell)))\\ &\left(\begin{array}{c}\text{by Theorem 2.9.15 \textbf{(a)},}\\ \text{applied to } a = \gcd(b_1, b_2, \ldots, b_k) \text{ and } b = \gcd(c_1, c_2, \ldots, c_\ell)\end{array}\right).\end{aligned}$$

Now, forget that we fixed m. We thus have shown that each $m \in \mathbb{Z}$ satisfies the equivalence

$$\begin{aligned}&(m \mid \gcd(b_1, b_2, \ldots, b_k, c_1, c_2, \ldots, c_\ell))\\ &\iff (m \mid \gcd(\gcd(b_1, b_2, \ldots, b_k), \gcd(c_1, c_2, \ldots, c_\ell))).\end{aligned}$$

Hence, Lemma 2.9.27 **(b)** (applied to $a = \gcd(b_1, b_2, \ldots, b_k, c_1, c_2, \ldots, c_\ell)$ and $b = \gcd(\gcd(b_1, b_2, \ldots, b_k), \gcd(c_1, c_2, \ldots, c_\ell))$) yields

$$\begin{aligned}&|\gcd(b_1, b_2, \ldots, b_k, c_1, c_2, \ldots, c_\ell)|\\ &= |\gcd(\gcd(b_1, b_2, \ldots, b_k), \gcd(c_1, c_2, \ldots, c_\ell))|.\end{aligned} \tag{24}$$

But a gcd of integers is always nonnegative (by Definition 2.9.6); thus, the absolute value of a gcd is always this gcd itself. Therefore, we can remove the absolute value signs on both sides of (24). We thus obtain

$$\gcd(b_1, b_2, \ldots, b_k, c_1, c_2, \ldots, c_\ell) = \gcd(\gcd(b_1, b_2, \ldots, b_k), \gcd(c_1, c_2, \ldots, c_\ell)).$$

This proves Theorem 2.9.26. □

2.9.7. On converses of Bezout's theorem

Some words of warning are in order. Theorem 2.9.12 says that if a and b are two integers, then $\gcd(a,b)$ is a $\mathbb{Z}$-linear combination of a and b. Note the indefinite article "a" here: There are (usually) many $\mathbb{Z}$-linear combinations of a and b, but only one gcd. It is definitely not true that every $\mathbb{Z}$-linear combination of a and b must be $\gcd(a,b)$. However, all these $\mathbb{Z}$-linear combinations are **multiples** of the gcd, as the following (simple) proposition says:

Proposition 2.9.28. Let a and b be two integers. Then, any integers x and y satisfy $\gcd(a,b) \mid xa + yb$.

Proof of Proposition 2.9.28. Let x and y be integers. Let $g = \gcd(a,b)$. Thus, $g = \gcd(a,b) \mid a$ (by Proposition 2.9.7 **(f)**). Hence, $g \mid a \mid xa$ (since $xa = ax$). In other words, $xa \equiv 0 \mod g$. Similarly, $yb \equiv 0 \mod g$. Adding these two congruences together, we obtain $xa + yb \equiv 0 + 0 = 0 \mod g$. In other words, $g \mid xa + yb$. In other words, $\gcd(a,b) \mid xa + yb$ (since $g = \gcd(a,b)$). This proves Proposition 2.9.28. □

A similar proposition holds for $\mathbb{Z}$-linear combinations of any number of integers $b_1, b_2, \ldots, b_k$.

2.10. Coprime integers

2.10.1. Definition

The concept of a gcd leads to one of the most important notions of number theory:

Definition 2.10.1. Let a and b be two integers. We say that a is *coprime* to b if and only if $\gcd(a,b) = 1$.

Instead of "coprime", some authors say "relatively prime" or even "prime" (but the latter language risks confusion with a more standard notion of "prime" that we will see later on.)

Example 2.10.2. (a) The number 2 is coprime to 3, since $\gcd(2,3) = 1$.

(b) The number 6 is not coprime to 15, since $\gcd(6,15) = 3 \neq 1$.

(c) Let a be an integer. We claim (as a generalization of part **(a)**) that the number a is coprime to $a+1$. To prove this, we note that

$$\begin{aligned}\gcd\left(a, \underbrace{a}_{=1a} + 1\right) &= \gcd(a, 1a+1) = \gcd(a,1) \\ &\qquad \text{(by Proposition 2.9.7 } \textbf{(c)}\text{, applied to } u = 1 \text{ and } b = 1\text{)} \\ &\mid 1 \qquad \text{(by Proposition 2.9.7 } \textbf{(f)}\text{, applied to } b = 1\text{)},\end{aligned}$$

and thus $\gcd(a, a+1) = 1$ (by Exercise 2.2.5, since $\gcd(a, a+1)$ is a nonnegative integer), which means that a is coprime to $a+1$.

(d) Let a be an integer. When is a coprime to $a+2$? If we try to compute $\gcd(a, a+2)$, we find

$$\gcd\left(a, \underbrace{a}_{=1a} + 2\right) = \gcd(a, 1a+2) = \gcd(a, 2)$$
$$\text{(by Proposition 2.9.7 \textbf{(c)}, applied to } u = 1 \text{ and } b = 2) .$$

It remains to find $\gcd(a, 2)$. Proposition 2.9.7 **(f)** (applied to $b = 2$) yields $\gcd(a, 2) \mid a$ and $\gcd(a, 2) \mid 2$. Since $\gcd(a, 2)$ is a nonnegative integer and is a divisor of 2 (because $\gcd(a, 2) \mid 2$), we see that $\gcd(a, 2)$ must be either 1 or 2 (since the only nonnegative divisors of 2 are 1 and 2). If a is even, then 2 is a common divisor of a and 2, and thus must be the greatest common divisor of a and 2 (because a common divisor of a and 2 cannot be greater than 2); in other words, we have $\gcd(a, 2) = 2$ in this case. On the other hand, if a is odd, then 2 is not a common divisor of a and 2 (since 2 does not divide a), and thus cannot be the greatest common divisor of a and 2; hence, in this case, we have $\gcd(a, 2) \neq 2$ and thus $\gcd(a, 2) = 1$. Summarizing, we conclude that

$$\gcd(a, 2) = \begin{cases} 2, & \text{if } a \text{ is even;} \\ 1, & \text{if } a \text{ is odd.} \end{cases}$$

Now, recall that $\gcd(a, a+2) = \gcd(a, 2) = \begin{cases} 2, & \text{if } a \text{ is even;} \\ 1, & \text{if } a \text{ is odd.} \end{cases}$ Hence, a is coprime to $a+2$ if and only if a is odd.

Following the book [GrKnPa94], we introduce a slightly quaint notation:

Definition 2.10.3. Let a and b be two integers. We write "$a \perp b$" to signify that a is coprime to b.

Note that the "$\perp$" relation is symmetric:

Proposition 2.10.4. Let a and b be two integers. Then, $a \perp b$ if and only if $b \perp a$.

Proof of Proposition 2.10.4. We have the following chain of equivalences:

$$\begin{aligned}
(a \perp b) &\iff (a \text{ is coprime to } b) \qquad (\text{by the definition of " } \perp \text{ "}) \\
&\iff (\gcd(a, b) = 1) \qquad (\text{by the definition of "coprime"}) \\
&\iff (\gcd(b, a) = 1) \qquad \left(\begin{array}{c} \text{since Proposition 2.9.7 \textbf{(b)}} \\ \text{yields } \gcd(a, b) = \gcd(b, a) \end{array}\right) \\
&\iff (b \text{ is coprime to } a) \qquad (\text{by the definition of "coprime"}) \\
&\iff (b \perp a) \qquad (\text{by the definition of " } \perp \text{ "}) .
\end{aligned}$$

This proves Proposition 2.10.4. □

Definition 2.10.5. Let a and b be two integers. Proposition 2.10.4 shows that a is coprime to b if and only if b is coprime to a. Hence, we shall sometimes use a more symmetric terminology for this situation: We shall say that "*a and b are coprime*" to mean that a is coprime to b (or, equivalently, that b is coprime to a).

Exercise 2.10.1. Let $a \in \mathbb{Z}$. Prove the following:
(a) We have $1 \perp a$.
(b) We have $0 \perp a$ if and only if $|a| = 1$.

2.10.2. Properties of coprime integers

We can now state multiple theorems about coprime numbers. The first one states that we can "cancel" a factor b from a divisibility $a \mid bc$ as long as this factor is coprime to a:

Theorem 2.10.6. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid bc$ and $a \perp b$. Then, $a \mid c$.

Proof of Theorem 2.10.6. We have $a \perp b$; in other words, a is coprime to b (by Definition 2.10.3). In other words, $\gcd(a, b) = 1$ (by the definition of "coprime"). Now, Theorem 2.9.19 yields $a \mid \underbrace{\gcd(a, b)}_{=1} \cdot c = c$. This proves Theorem 2.10.6. □

I like to think of Theorem 2.10.7 as a way of removing "unsolicited guests" from divisibilities. Indeed, it says that we can remove the factor b from $a \mid bc$ if we know that b is "unrelated" (i.e., coprime) to a.

The next theorem lets us "combine" two divisibilities $a \mid c$ and $b \mid c$ to $ab \mid c$ as long as a and b are coprime:

Theorem 2.10.7. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid c$ and $b \mid c$ and $a \perp b$. Then, $ab \mid c$.

Proof of Theorem 2.10.7. We have $a \perp b$; in other words, a is coprime to b (by Definition 2.10.3). In other words, $\gcd(a, b) = 1$ (by the definition of "coprime"). Now, Theorem 2.9.17 yields $ab \mid \underbrace{\gcd(a, b)}_{=1} \cdot c = c$. This proves Theorem 2.10.7. □

Theorem 2.10.7 can be restated as follows: If a and b are two coprime divisors of an integer c, then ab is also a divisor of c. This is often helpful when proving divisibilities where the left hand side (i.e., the number in front of the "$|$" sign) can be split into a product of two mutually coprime factors. Similar reasoning works with several coprime factors (see Exercise 2.10.3 below).

The next theorem (still part of the fallout of Bezout's theorem) is important, but we will not truly appreciate it until later:

Theorem 2.10.8. Let $a, n \in \mathbb{Z}$.

(a) There exists a $b \in \mathbb{Z}$ such that $ab \equiv \gcd(a, n) \bmod n$.

(b) If $a \perp n$, then there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \bmod n$.

(c) If there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \bmod n$, then $a \perp n$.

If $a, n \in \mathbb{Z}$, then an integer $a' \in \mathbb{Z}$ satisfying $aa' \equiv 1 \bmod n$ is called a *modular inverse* of a modulo n. The word "modular inverse" is chosen in analogy to the usual concept of an "inverse" in $\mathbb{Z}$ (which stands for an integer $a' \in \mathbb{Z}$ satisfying $aa' = 1$; this exists if and only if a equals 1 or -1). Theorem 2.10.8 **(b)** shows that such a modular inverse always exists when $a \perp n$; Theorem 2.10.8 **(c)** is the converse of this statement (i.e., it says that if a modular inverse of a modulo n exists, then $a \perp n$).

Proof of Theorem 2.10.8. **(a)** Theorem 2.9.12 (applied to $b = n$) yields that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a, n) = xa + yn$. Consider these x and y. We have $ax = xa \equiv xa + yn \bmod n$ (since $xa - (xa + yn) = -yn = n(-y)$ is clearly divisible by n). Thus, $ax \equiv xa + yn = \gcd(a, n) \bmod n$. Thus, there exists a $a' \in \mathbb{Z}$ such that $aa' \equiv (a, n) \bmod n$ (namely, $a' = x$). This proves Theorem 2.10.8 **(a)**.

(b) Assume that $a \perp n$. In other words, a is coprime to n (by Definition 2.10.3). In other words, $\gcd(a, n) = 1$ (by the definition of "coprime"). Now, Theorem 2.10.8 **(a)** yields that there exists a $a' \in \mathbb{Z}$ such that $aa' \equiv \gcd(a, n) \bmod n$. In view of $\gcd(a, n) = 1$, this rewrites as follows: There exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \bmod n$. This proves Theorem 2.10.8 **(b)**.

(c) Assume that there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \bmod n$. Consider this a'.

Proposition 2.9.7 **(f)** yields $\gcd(a, n) \mid a$ and $\gcd(a, n) \mid n$. Set $g = \gcd(a, n)$. Then, g is a nonnegative integer.

Now, $g = \gcd(a, n) \mid a \mid aa'$, so that $aa' \equiv 0 \bmod g$. But also $g = \gcd(a, n) \mid n$. Hence, from $aa' \equiv 1 \bmod n$, we obtain $aa' \equiv 1 \bmod g$ (by Proposition 2.3.4 **(e)**, applied to g, aa' and 1 instead of m, a and b). Hence, $1 \equiv aa' \equiv 0 \bmod g$. Equivalently, $g \mid 1 - 0 = 1$. Hence, $g = 1$ (by Exercise 2.2.5, since g is a nonnegative integer). Thus, $\gcd(a, n) = g = 1$. In other words, a is coprime to n. In other words, $a \perp n$. This proves Theorem 2.10.8 **(c)**. □

Theorem 2.10.9. Let $a, b, c \in \mathbb{Z}$ such that $a \perp c$ and $b \perp c$. Then, $ab \perp c$.

Proof of Theorem 2.10.9. Theorem 2.10.8 **(b)** (applied to $n = c$) yields that there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \bmod c$. Consider this a'.

Theorem 2.10.8 **(b)** (applied to b and c instead of a and n) yields that there exists a $b' \in \mathbb{Z}$ such that $bb' \equiv 1 \bmod c$. Consider this b'.

Multiplying the two congruences $aa' \equiv 1 \bmod c$ and $bb' \equiv 1 \bmod c$, we obtain $(aa')(bb') \equiv 1 \cdot 1 = 1 \bmod c$.

Now, define the integers $r = ab$ and $s = a'b'$. Then, $\underbrace{r}_{=ab} \underbrace{s}_{=a'b'} = (ab)(a'b') = (aa')(bb') \equiv 1 \bmod c$. Hence, there exists an $r' \in \mathbb{Z}$ such that $rr' \equiv 1 \bmod c$ (namely, $r' = s$). Thus, Theorem 2.10.8 **(c)** (applied to r and c instead of a and n) yields that $r \perp c$. In view of $r = ab$, this rewrites as $ab \perp c$. This proves Theorem 2.10.9. □

Let us generalize Theorem 2.10.9 to products of several numbers instead of just the two numbers a and b:

Exercise 2.10.2. Let $c \in \mathbb{Z}$. Let $a_1, a_2, \ldots, a_k$ be integers such that each $i \in \{1, 2, \ldots, k\}$ satisfies $a_i \perp c$. Prove that $a_1 a_2 \cdots a_k \perp c$.

We can similarly generalize Theorem 2.10.7 to show that the product of several mutually coprime divisors of an integer c must again be a divisor of c:

Exercise 2.10.3. Let $c \in \mathbb{Z}$. Let $b_1, b_2, \ldots, b_k$ be integers that are mutually coprime (i.e., they satisfy $b_i \perp b_j$ for all $i \neq j$). Assume that $b_i \mid c$ for each $i \in \{1, 2, \ldots, k\}$. Prove that $b_1 b_2 \cdots b_k \mid c$.

Exercise 2.10.4. Let $a, b \in \mathbb{Z}$ be such that $a \perp b$. Let $n, m \in \mathbb{N}$. Prove that $a^n \perp b^m$.

The above results have one important application to congruences. Recall that if a, b, c are integers satisfying $ab = ac$, then we can "cancel" a from the equality $ab = ac$ to obtain $b = c$ as long as a is nonzero. Something similar is true for congruences modulo n, but the condition "a is nonzero" has to be replaced by "a is coprime to n":

Lemma 2.10.10. Let a, b, c, n be integers such that $a \perp n$ and $ab \equiv ac \mod n$. Then, $b \equiv c \mod n$.

Lemma 2.10.10 says that we can cancel an integer a from a congruence $ab \equiv ac \mod n$ as long as a is coprime to n. Let us give two proofs of this lemma, to illustrate the uses of some of the previous results:

First proof of Lemma 2.10.10. We have $ab \equiv ac \mod n$. In other words, $n \mid ab - ac = a(b - c)$. But Proposition 2.10.4 (applied to n instead of b) shows that $a \perp n$ if and only if $n \perp a$. Thus, we have $n \perp a$ (since $a \perp n$).

Thus, we know that $n \mid a(b - c)$ and $n \perp a$. Hence, Theorem 2.10.6 (applied to n, a and $b - c$ instead of a, b and c) yields $n \mid b - c$. In other words, $b \equiv c \mod n$. This proves Lemma 2.10.10. □

Second proof of Lemma 2.10.10. Theorem 2.10.8 **(b)** yields that there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \mod n$ (since $a \perp n$). Consider this a'. Now, let us multiply the (trivial) congruence $a' \equiv a' \mod n$ with the congruence $ab \equiv ac \mod n$. We thus find

$$a'ab \equiv \underbrace{a'a}_{\equiv 1 \mod n} c \equiv 1c = c \mod n.$$

Hence,

$$c \equiv \underbrace{a'a}_{\equiv 1 \mod n} b \equiv 1b = b \mod n.$$

In other words, $b \equiv c \mod n$. This proves Lemma 2.10.10. □

For future use, let us restate Exercise 2.10.2 in a form that uses "unordered" finite products $\prod\limits_{i \in I} b_i$ instead of $a_1 a_2 \cdots a_k$:

Exercise 2.10.5. Let $c \in \mathbb{Z}$. Let I be a finite set. For each $i \in I$, let b_i be an integer such that $b_i \perp c$. Prove that $\prod\limits_{i \in I} b_i \perp c$.

Exercise 2.10.6. Let a, b, c be three integers such that $a \equiv b \mod c$. Prove that if $a \perp c$, then $b \perp c$.

Exercise 2.10.7. Let $a, b \in \mathbb{Z}$. Prove that $b - a \perp b$ holds if and only if $a \perp b$.

2.10.3. An application to sums of powers

Let us show an application of Theorem 2.10.7. First, we shall prove a simple lemma:

Lemma 2.10.11. Let $d \in \mathbb{N}$. Let x and y be integers.
(a) We have $x - y \mid x^d - y^d$.
(b) We have $x + y \mid x^d + y^d$ if d is odd.

Proof of Lemma 2.10.11. **(a)** Here are two ways of proving this:

*First proof of Lemma 2.10.11 **(a)**:* We have $x \equiv y \mod x - y$ (since $x - y \mid x - y$). Thus, Exercise 2.3.4 (applied to $n = x - y$, $a = x$, $b = y$ and $k = d$) yields $x^d \equiv y^d \mod x - y$. In other words, $x - y \mid x^d - y^d$. This proves Lemma 2.10.11 **(a)**.

*Second proof of Lemma 2.10.11 **(a)**:* Recall that

$$(a-b)\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}\right) = a^k - b^k \tag{25}$$

for every $a, b \in \mathbb{Q}$ and $k \in \mathbb{N}$. (This is a well-known identity, and it appears (with k renamed as n) as the first half of Exercise 1 on homework set #0.) Applying this identity to $a = x$, $b = y$ and $k = d$, we obtain

$$(x-y)\left(x^{d-1} + x^{d-2}y + x^{d-3}y^2 + \cdots + xy^{d-2} + y^{d-1}\right) = x^d - y^d.$$

Thus, $x - y \mid x^d - y^d$ (since $x^{d-1} + x^{d-2}y + x^{d-3}y^2 + \cdots + xy^{d-2} + y^{d-1}$ is an integer). This proves Lemma 2.10.11 **(a)**.

(b) Assume that d is odd. Thus, $(-1)^d = -1$. Now, Lemma 2.10.11 **(a)** (applied to $-y$ instead of y) yields $x - (-y) \mid x^d - (-y)^d$. Since $x - (-y) = x + y$ and $x^d - \underbrace{(-y)^d}_{=(-1)^d y^d} = x^d - \underbrace{(-1)^d}_{=-1} y^d = x^d - (-1) y^d = x^d + y^d$, this rewrites as $x + y \mid x^d + y^d$. This proves Lemma 2.10.11 **(b)**. □

Next, let us recall a basic fact from combinatorics (the "Little Gauss" sum):

Proposition 2.10.12. Let $n \in \mathbb{N}$. Then,

$$1+2+\cdots+n=\frac{n(n+1)}{2}.$$

Proof of Proposition 2.10.12. Here is one of several equally valid arguments:

$$\begin{aligned}2\cdot(1+2+\cdots+n) &= (1+2+\cdots+n)+\underbrace{(1+2+\cdots+n)}_{\substack{=n+(n-1)+\cdots+1\\ \text{(here, we have reversed}\\ \text{the order of the addends)}}}\\ &= \underbrace{(1+2+\cdots+n)}_{=\sum\limits_{k=1}^{n}k}+\underbrace{(n+(n-1)+\cdots+1)}_{=\sum\limits_{k=1}^{n}(n+1-k)}\\ &= \sum_{k=1}^{n}k+\sum_{k=1}^{n}(n+1-k)=\sum_{k=1}^{n}\underbrace{(k+(n+1-k))}_{=n+1}\\ &= \sum_{k=1}^{n}(n+1)=n(n+1).\end{aligned}$$

Thus, $1+2+\cdots+n=\dfrac{n(n+1)}{2}$, so that Proposition 2.10.12 is proven. □

Proposition 2.10.12 tells us what the sum $1+2+\cdots+n$ of the first n positive integers is. One might also ask what the sum $1^2+2^2+\cdots+n^2$ of their squares is, and similarly for higher powers. While this is tangential to our course, let us collect some formulas for this:

Proposition 2.10.13. Let $n \in \mathbb{N}$. Then:

(a) We have $1+2+\cdots+n=\dfrac{1}{2}n(n+1)$.

(b) We have $1^2+2^2+\cdots+n^2=\dfrac{1}{6}n(n+1)(2n+1)$.

(c) We have $1^3+2^3+\cdots+n^3=\dfrac{1}{4}n^2(n+1)^2$.

(d) We have $1^4+2^4+\cdots+n^4=\dfrac{1}{30}n(2n+1)(n+1)\left(3n+3n^2-1\right)$.

(e) We have $1^5+2^5+\cdots+n^5=\dfrac{1}{12}n^2(n+1)^2\left(2n+2n^2-1\right)$.

Each part of Proposition 2.10.13 can be straightforwardly proven by induction on n; we don't need ingenious arguments like the one we gave above for Proposition 2.10.12 (and in fact, such arguments cannot always be found).

You probably see a pattern in Proposition 2.10.13: It appears that for each positive integer d, there exists some polynomial $p_d(x)$ of degree $d+1$ with rational coefficients such that each $n \in \mathbb{N}$ satisfies $1^d+2^d+\cdots+n^d=p_d(n)$. This is indeed the case. Indeed, this is proven (e.g.) in [Galvin17, Proposition 23.2] and in [Grinbe17, Theorem 3.7]. The polynomial $p_d(x)$ is uniquely determined for each d, and can be explicitly computed via the formula

$$p_d(x) = \sum_{k=1}^{d} k! \left\{ \begin{matrix} d \\ k \end{matrix} \right\} \binom{x+1}{k+1},$$

where $\dbinom{x+1}{k+1} = \dfrac{(x+1)\,x\,(x-1)\cdots(x-k+1)}{(k+1)!}$ and where $\left\{ \begin{matrix} d \\ k \end{matrix} \right\}$ is a *Stirling number of the 2nd kind*. Without going into the details of what Stirling numbers of the 2nd kind are, let me say that $k! \left\{ \begin{matrix} d \\ k \end{matrix} \right\}$ is the number of surjective maps from $\{1,2,\ldots,d\}$ to $\{1,2,\ldots,k\}$. For example,

$$\begin{aligned} p_2(x) &= \sum_{k=1}^{2} k! \left\{ \begin{matrix} 2 \\ k \end{matrix} \right\} \binom{x+1}{k+1} = \underbrace{1! \left\{ \begin{matrix} 2 \\ 1 \end{matrix} \right\}}_{=1} \binom{x+1}{2} + \underbrace{2! \left\{ \begin{matrix} 2 \\ 2 \end{matrix} \right\}}_{=2} \binom{x+1}{3} \\ &= \binom{x+1}{2} + 2\binom{x+1}{3} = \frac{(x+1)\,x}{2} + 2 \cdot \frac{(x+1)\,x\,(x-1)}{6} \\ &= \frac{1}{6} x\,(x+1)\,(2x+1), \end{aligned}$$

and thus

$$1^2 + 2^2 + \cdots + n^2 = p_2(n) = \frac{1}{6} n\,(n+1)\,(2n+1) \qquad \text{for each } n \in \mathbb{N}.$$

This recovers the claim of Proposition 2.10.13 **(b)**. The combinatorial proof presented in [Galvin17, Proposition 23.2] is highly recommended reading for anyone interested in this kind of formulas.

Let us note that the polynomials $p_d(x)$ do **not** have integer coefficients, but nevertheless all their values $p_d(n)$ for $n \in \mathbb{N}$ are integers.

Let us now show the power of Theorem 2.10.7 on the following exercise:

Exercise 2.10.8. Let $n \in \mathbb{N}$. Let d be an odd positive integer. Prove that

$$1 + 2 + \cdots + n \mid 1^d + 2^d + \cdots + n^d.$$

[Hint: Use Proposition 2.10.12 to reduce the claim to proving that $n(n+1) \mid 2\left(1^d + 2^d + \cdots + n^d\right)$. But Theorem 2.10.7 shows that in order to prove this, it suffices to prove $n \mid 2\left(1^d + 2^d + \cdots + n^d\right)$ and $n+1 \mid 2\left(1^d + 2^d + \cdots + n^d\right)$, because $n \perp n+1$.]

2.10.4. More properties of gcds and coprimality

The following is a random collection of further exercises on gcds.

Exercise 2.10.9. Let a, b, x, y be integers such that $xa + yb = 1$. Prove that $a \perp b$.

Exercise 2.10.10. Let $u, v, x, y \in \mathbb{Z}$. Prove that $\gcd(u, v) \cdot \gcd(x, y) = \gcd(ux, uy, vx, vy)$.

Exercise 2.10.11. Let $a, b, c \in \mathbb{Z}$.

(a) Prove that $\gcd(a, b) \cdot \gcd(a, c) = \gcd(ag, bc)$, where $g = \gcd(a, b, c)$.

(b) Prove that $\gcd(a, b) \cdot \gcd(a, c) = \gcd(a, bc)$ if $b \perp c$.

Exercise 2.10.12. Let a and b be two integers that are not both zero. Let $g = \gcd(a, b)$. Prove that $\frac{a}{g}$ and $\frac{b}{g}$ are integers satisfying $\frac{a}{g} \perp \frac{b}{g}$.

Exercise 2.10.13. Let a and b be two integers. Let $k \in \mathbb{N}$. Prove that $\gcd\left(a^k, b^k\right) = (\gcd(a, b))^k$.

The next exercise is simply claiming the well-known fact that any rational number can be written as a reduced fraction:

Exercise 2.10.14. Let $r \in \mathbb{Q}$. Prove that there exist two **coprime** integers a and b satisfying $r = a/b$.

As an application of some of the preceding results, we can prove that certain numbers are irrational:

Exercise 2.10.15. Prove the following:

(a) If a positive integer u is not a perfect square[22], then $\sqrt{u}$ is irrational.

(b) If u and v are two positive integers, then $\sqrt{u} + \sqrt{v}$ is irrational unless both u and v are perfect squares.

Exercise 2.10.15 invites a rather natural generalization: If $u_1, u_2, \ldots, u_k$ are several positive integers that are not all perfect squares, then must $\sqrt{u_1} + \sqrt{u_2} + \cdots + \sqrt{u_k}$ always be irrational? It turns out that the answer is "yes", but this is not as easy to prove anymore as the two cases $k = 1$ and $k = 2$ that we handled in Exercise 2.10.15. Proofs of the general version can be found in [Boreic08] (actually, a stronger statement is proven there, although it takes some work to derive ours from it).

Let us generalize Exercise 2.10.10 a bit:

Exercise 2.10.16. Let $x, y \in \mathbb{Z}$, and let $a_1, a_2, \ldots, a_k$ be finitely many integers. Prove that

$$\gcd(a_1, a_2, \ldots, a_k) \cdot \gcd(x, y) = \gcd(a_1x, a_2x, \ldots, a_kx, a_1y, a_2y, \ldots, a_ky).$$

[22] A *perfect square* means the square of an integer.

We can extend this exercise further to several integers instead of x and y, but this extension would be notationally awkward, so we only state it for the case of three integers:

Exercise 2.10.17. Let $x, y, z \in \mathbb{Z}$, and let $a_1, a_2, \ldots, a_k$ be finitely many integers. Prove that

$$\begin{aligned} & \gcd\left(a_1, a_2, \ldots, a_k\right) \cdot \gcd\left(x, y, z\right) \\ & = \gcd\left(a_1 x, a_2 x, \ldots, a_k x, a_1 y, a_2 y, \ldots, a_k y, a_1 z, a_2 z, \ldots, a_k z\right). \end{aligned}$$

We leave it to the reader to state and solve an exercise generalizing Exercise 2.10.16 and Exercise 2.10.17.

Exercise 2.10.18. Let $a, b, c \in \mathbb{Z}$. Prove that

$$\gcd\left(b, c\right) \cdot \gcd\left(c, a\right) \cdot \gcd\left(a, b\right) = \gcd\left(a, b, c\right) \cdot \gcd\left(bc, ca, ab\right).$$

2.11. Lowest common multiples

Common multiples are, in a sense, a "mirror version" of common divisors. Here is their definition:

Definition 2.11.1. Let $b_1, b_2, \ldots, b_k$ be integers. Then, the *common multiples* of $b_1, b_2, \ldots, b_k$ are defined to be the integers a that satisfy

$$\left(b_i \mid a \text{ for all } i \in \left\{1, 2, \ldots, k\right\}\right).$$

(In other words, a *common multiple* of $b_1, b_2, \ldots, b_k$ is an integer that is a multiple of each of $b_1, b_2, \ldots, b_k$.) We let $\operatorname{Mul}\left(b_1, b_2, \ldots, b_k\right)$ denote the set of these common multiples.

Example 2.11.2. The common multiples of $4, 6$ are $\ldots, -36, -24, -12, 0, 12, 24, 36, \ldots$, that is, all multiples of 12.

The common multiples of $1, 2, 3$ are all multiples of 6.

Note that the common multiples of a single integer b are simply the multiples of b. (Also, the common multiples of an empty list of integers are all the integers; in other words, $\operatorname{Mul}\left(\right) = \mathbb{Z}$.)

Note that the definition of common multiples of $b_1, b_2, \ldots, b_k$ (Definition 2.11.1) is the same as the definition of common divisors of $b_1, b_2, \ldots, b_k$ except that the divisibility has been flipped (i.e., it says "$b_i \mid a$" instead of "$a \mid b_i$"). This is why common multiples are a "mirror version" of common divisors. This analogy is not perfect – in particular, (for example) two nonzero integers have infinitely many common multiples but only finitely many common divisors. We shall now introduce lowest common multiples, which correspond to greatest common divisors in this analogy. However, we have to prove a simple proposition first:

Proposition 2.11.3. Let $b_1, b_2, \ldots, b_k$ be finitely many nonzero integers. Then, the set $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$ has a smallest positive element.

Proposition 2.11.3 is similar to Proposition 2.9.5 (and will play a similar role), but note the differences: It requires **all** of $b_1, b_2, \ldots, b_k$ to be nonzero (unlike Proposition 2.9.5, which needed only one of them to be nonzero), and it does not claim finiteness of any set.

Proof of Proposition 2.11.3. We claim that

$$|b_1 b_2 \cdots b_k| \in \operatorname{Mul}(b_1, b_2, \ldots, b_k). \tag{26}$$

[*Proof of (26):* Let $i \in \{1, 2, \ldots, k\}$. Then, the product $b_1 b_2 \cdots b_k$ can be written as

$$b_1 b_2 \cdots b_k = b_i \cdot (b_1 b_2 \cdots b_{i-1} b_{i+1} b_{i+2} \cdots b_k),$$

and thus is divisible by b_i. In other words, $b_i \mid b_1 b_2 \cdots b_k$. But Exercise 2.2.1 **(a)** (applied to $a = b_1 b_2 \cdots b_k$) yields $b_1 b_2 \cdots b_k \mid |b_1 b_2 \cdots b_k|$. Altogether, $b_i \mid b_1 b_2 \cdots b_k \mid |b_1 b_2 \cdots b_k|$.

Now forget that we fixed i. We thus have proven that $b_i \mid |b_1 b_2 \cdots b_k|$ for all $i \in \{1, 2, \ldots, k\}$. In other words, $|b_1 b_2 \cdots b_k|$ is a common multiple of $b_1, b_2, \ldots, b_k$ (by the definition of a "common multiple"). In other words, $|b_1 b_2 \cdots b_k| \in \operatorname{Mul}(b_1, b_2, \ldots, b_k)$. This proves (26).]

We know that $b_1, b_2, \ldots, b_k$ are nonzero integers. Hence, their product $b_1 b_2 \cdots b_k$ is a nonzero integer as well. Thus, its absolute value $|b_1 b_2 \cdots b_k|$ is a positive integer. Hence, $|b_1 b_2 \cdots b_k|$ is a positive element of $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$ (since (26) shows that it is an element of $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$). Thus, the set $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$ has a positive element. Therefore, this set $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$ has a **smallest** positive element as well[23]. This proves Proposition 2.11.3. □

Definition 2.11.4. Let $b_1, b_2, \ldots, b_k$ be finitely many integers. The *lowest common multiple* of $b_1, b_2, \ldots, b_k$ is defined as follows:

- If $b_1, b_2, \ldots, b_k$ are all nonzero, then it is defined as the smallest positive element of the set $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$. This smallest positive element is well-defined (by Proposition 2.11.3), and is a positive integer (obviously).

[23] Here we are using the following basic fact: If a set of integers S has a positive element, then it has a **smallest** positive element as well. (To prove this fact, you can fix a positive element $s \in S$, which exists by assumption; then, the set $\{1, 2, \ldots, s\} \cap S$ is finite and nonempty (since it contains s), and thus clearly has a smallest element; now you can easily check that its smallest element must also be the smallest positive element of S.)

- If $b_1, b_2, \ldots, b_k$ are not all nonzero (i.e., at least one of $b_1, b_2, \ldots, b_k$ is zero), then it is defined to be 0.

Thus, in either case, this lowest common multiple is a nonnegative integer. We denote it by $\operatorname{lcm}(b_1, b_2, \ldots, b_k)$. (Some authors also call it $[b_1, b_2, \ldots, b_k]$.)

We shall also use the word "*lcm*" as shorthand for "lowest common multiple".

Some authors say "*least common multiple*" instead of "lowest common multiple".

We are slightly abusing the word "lowest common multiple", of course; it would be more precise to say "lowest **positive** common multiple", and even this would only hold for the case when $b_1, b_2, \ldots, b_k$ are all nonzero. Taken literally, a "lowest common multiple" of 2 and 3 would not exist, since 2 and 3 have infinitely many negative common multiples.

Note that the lcm of a single number is the absolute value of this number: i.e., we have $\operatorname{lcm}(a) = |a|$ for each $a \in \mathbb{Z}$. (This is easy to prove.) Also, the lcm of an empty list of numbers is 1: that is, $\operatorname{lcm}() = 1$.

We observe a trivial property of lcms, which (for the sake of brevity) we only state for two integers a and b despite it holding for any number of integers (with the same proof):

Proposition 2.11.5. Let $a, b \in \mathbb{Z}$.

(a) We have $0 \in \operatorname{Mul}(a, b)$.

(b) We have $\operatorname{lcm}(a, b) \in \operatorname{Mul}(a, b)$.

(c) We have $a \mid \operatorname{lcm}(a, b)$ and $b \mid \operatorname{lcm}(a, b)$.

Proof of Proposition 2.11.5. **(a)** The integer 0 clearly satisfies $(a \mid 0 \text{ and } b \mid 0)$. In other words, 0 is a common multiple of a and b (by the definition of a "common multiple"). In other words, $0 \in \operatorname{Mul}(a, b)$ (by the definition of $\operatorname{Mul}(a, b)$). This proves Proposition 2.11.5 **(a)**.

(b) If the two integers a and b are not all nonzero, then Proposition 2.11.5 **(b)** holds[24]. Hence, for the rest of this proof, we WLOG assume that the two integers a and b are all nonzero. Thus, Definition 2.11.4 yields that $\operatorname{lcm}(a, b)$ is the smallest positive element of the set $\operatorname{Mul}(a, b)$. Hence, $\operatorname{lcm}(a, b) \in \operatorname{Mul}(a, b)$. This proves Proposition 2.11.5 **(b)**.

(c) Proposition 2.11.5 **(b)** yields $\operatorname{lcm}(a, b) \in \operatorname{Mul}(a, b)$. In other words, $\operatorname{lcm}(a, b)$ is a common multiple of a and b (by the definition of $\operatorname{Mul}(a, b)$). In other words, we have $(a \mid \operatorname{lcm}(a, b) \text{ and } b \mid \operatorname{lcm}(a, b))$ (by the definition of "common multiple"). This proves Proposition 2.11.5 **(c)**. □

The following theorem yields a good way of computing lcms of two numbers (since we already know how to compute gcds via the Euclidean algorithm):

[24] *Proof.* Assume that the two integers a and b are not all nonzero. Hence, Definition 2.11.4 shows that $\operatorname{lcm}(a, b) = 0 \in \operatorname{Mul}(a, b)$ (by Proposition 2.11.5 **(a)**). Thus, Proposition 2.11.5 **(b)** holds.

Theorem 2.11.6. Let $a, b \in \mathbb{Z}$. Then, $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|$.

Proof of Theorem 2.11.6. If at least one of the two numbers a and b is 0, then Theorem 2.11.6 holds[25]. Hence, for the rest of this proof, we WLOG assume that none of the two numbers a and b is 0. In other words, a and b are nonzero. Thus, Definition 2.11.4 yields that $\operatorname{lcm}(a,b)$ is the smallest positive element of the set $\operatorname{Mul}(a,b)$. Also, $\gcd(a,b)$ is a positive integer (since a and b are nonzero) and thus nonzero. Hence, we can define $c \in \mathbb{Q}$ by $c = \dfrac{ab}{\gcd(a,b)}$. Consider this c. From $c = \dfrac{ab}{\gcd(a,b)}$, we obtain $ab = \gcd(a,b) \cdot c$.

Let $d = |c|$. The number $c = \dfrac{ab}{\gcd(a,b)}$ is nonzero (since a and b are nonzero). Hence, its absolute value $|c|$ is positive. In other words, d is positive (since $d = |c|$). From $ab = \gcd(a,b) \cdot c$, we obtain

$$\begin{aligned} |ab| = |\gcd(a,b) \cdot c| &= \underbrace{|\gcd(a,b)|}_{\substack{=\gcd(a,b) \\ \text{(since } \gcd(a,b) \text{ is positive)}}} \cdot \underbrace{|c|}_{=d} \\ &\qquad \left(\text{by (3), applied to } \gcd(a,b) \text{ and } c \text{ instead of } x \text{ and } y\right) \\ &= \gcd(a,b) \cdot d. \end{aligned} \tag{27}$$

Solving this for d, we find $d = \dfrac{|ab|}{\gcd(a,b)}$ (since $\gcd(a,b)$ is nonzero).

We have $\gcd(a,b) \mid b$ (by Proposition 2.9.7 **(f)**). Thus, $\dfrac{b}{\gcd(a,b)}$ is an integer. Now, $c = \dfrac{ab}{\gcd(a,b)} = a \cdot \dfrac{b}{\gcd(a,b)}$ is the product of two integers (since a and $\dfrac{b}{\gcd(a,b)}$ are integers). Therefore, c itself is an integer. Thus, d is an integer as well (since $d = |c|$). Moreover, $c = a \cdot \dfrac{b}{\gcd(a,b)}$ shows that $a \mid c$ (since $\dfrac{b}{\gcd(a,b)}$ is an integer). But Exercise 2.2.1 **(a)** (applied to c instead of a) yields $c \mid |c|$ (this means "c divides $|c|$"). In other words, $c \mid d$ (since $d = |c|$). Hence, $a \mid c \mid d$.

So we have proven that $a \mid d$. Similarly, $b \mid d$. Thus, we know that ($a \mid d$ and $b \mid d$). In other words, d is a common multiple of a and b (by the definition of a "common multiple"). In other words, $d \in \operatorname{Mul}(a,b)$ (by the definition of $\operatorname{Mul}(a,b)$). Thus, d is a positive element of the set $\operatorname{Mul}(a,b)$ (since d is positive).

[25] *Proof.* Assume that at least one of the two numbers a and b is 0. Thus, the product ab is 0. Hence, $ab = 0$, so that $|ab| = 0$.

On the other hand, the two numbers a, b are not all nonzero (since at least one of the two numbers a and b is 0). Hence, Definition 2.11.4 shows that $\operatorname{lcm}(a,b) = 0$. Comparing $\gcd(a,b) \cdot \underbrace{\operatorname{lcm}(a,b)}_{=0} = 0$ with $|ab| = 0$, we obtain $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|$. In other words, Theorem 2.11.6 holds.

We shall now show that d is the smallest positive element of this set. Indeed, let x be any positive element of $\operatorname{Mul}(a,b)$. We are going to prove that $x \geq d$.

In fact, $x \in \operatorname{Mul}(a,b)$. In other words, x is a common multiple of a and b. In other words, we have $(a \mid x$ and $b \mid x)$. Hence, Theorem 2.9.17 (applied to x instead of c) yields $ab \mid \gcd(a,b) \cdot x$. Both numbers $\gcd(a,b)$ and x are positive; hence, their product $\gcd(a,b) \cdot x$ is positive as well, and thus we have $\gcd(a,b) \cdot x \neq 0$. Hence, Proposition 2.2.3 **(b)** (applied to ab and $\gcd(a,b) \cdot x$ instead of a and b) yields $|ab| \leq |\gcd(a,b) \cdot x| = \gcd(a,b) \cdot x$ (since $\gcd(a,b) \cdot x$ is positive). Thus,

$$\gcd(a,b) \cdot x \geq |ab| = \gcd(a,b) \cdot d \qquad \text{(by (27))}.$$

We can divide this inequality by $\gcd(a,b)$ (since $\gcd(a,b)$ is positive), and thus obtain $x \geq d$.

Now, forget that we fixed x. We thus have proven that each positive element x of the set $\operatorname{Mul}(a,b)$ satisfies $x \geq d$. Hence, d is the **smallest** positive element of the set $\operatorname{Mul}(a,b)$ (since we already know that d is a positive element of the set $\operatorname{Mul}(a,b)$). In other words, d is $\operatorname{lcm}(a,b)$ (since $\operatorname{lcm}(a,b)$ is the smallest positive element of the set $\operatorname{Mul}(a,b)$). In other words, $d = \operatorname{lcm}(a,b)$. Hence, (27) becomes $|ab| = \gcd(a,b) \cdot \underbrace{d}_{=\operatorname{lcm}(a,b)} = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$. This proves Theorem 2.11.6. □

Next, we state an analogue of Theorem 2.9.15 (with all divisibilities flipped):

Theorem 2.11.7. Let $a, b \in \mathbb{Z}$. Then:
(a) For each $m \in \mathbb{Z}$, we have the following logical equivalence:

$$(a \mid m \text{ and } b \mid m) \iff (\operatorname{lcm}(a,b) \mid m). \tag{28}$$

(b) The common multiples of a and b are precisely the multiples of $\operatorname{lcm}(a,b)$.
(c) We have $\operatorname{Mul}(a,b) = \operatorname{Mul}(\operatorname{lcm}(a,b))$.

Again, the three parts of this theorem are saying the same thing from slightly different perspectives. Our proof of Theorem 2.11.7 will rely on the following lemma:

Lemma 2.11.8. Let $m, a, b \in \mathbb{Z}$ be such that $a \mid m$ and $b \mid m$. Then, $\operatorname{lcm}(a,b) \mid m$.

Lemma 2.11.8 is similar to Lemma 2.9.16, but its proof is not:

Proof of Lemma 2.11.8. If at least one of the two numbers a and b is 0, then Lemma 2.11.8 holds[26]. Hence, for the rest of this proof, we WLOG assume that none of the

[26] *Proof.* Assume that at least one of the two numbers a and b is 0. In other words, $a = 0$ or $b = 0$. Let us WLOG assume that $a = 0$ (since the proof in the case $b = 0$ is analogous). We have $a \mid m$, thus $0 = a \mid m$.

On the other hand, the two numbers a, b are not all nonzero (since at least one of the two numbers a and b is 0). Hence, Definition 2.11.4 shows that $\operatorname{lcm}(a,b) = 0 = a \mid m$. In other words, Lemma 2.11.8 holds.

two numbers a and b is 0. In other words, a and b are nonzero. Thus, Definition 2.11.4 yields that $\operatorname{lcm}(a,b)$ is the smallest positive element of the set $\operatorname{Mul}(a,b)$. Set $n = \operatorname{lcm}(a,b)$. Thus, n is the smallest positive element of the set $\operatorname{Mul}(a,b)$ (since $\operatorname{lcm}(a,b)$ is the smallest positive element of the set $\operatorname{Mul}(a,b)$). Therefore, n is a positive integer and belongs to $\operatorname{Mul}(a,b)$.

Now, n is a common multiple of a and b (since n belongs to $\operatorname{Mul}(a,b)$). In other words, we have $(a \mid n \text{ and } b \mid n)$.

Our goal is to prove that $\operatorname{lcm}(a,b) \mid m$. In other words, our goal is to prove that $n \mid m$ (since $n = \operatorname{lcm}(a,b)$). Assume the contrary. Thus, we don't have $n \mid m$. Hence, we don't have $m\%n = 0$ (because Corollary 2.6.9 **(b)** (applied to $u = m$) shows that we have $n \mid m$ if and only if $m\%n = 0$). In other words, we have $m\%n \neq 0$.

Corollary 2.6.9 **(a)** (applied to $u = m$) yields that $m\%n \in \{0,1,\ldots,n-1\}$ and $m\%n \equiv m \mod n$. Combining $m\%n \in \{0,1,\ldots,n-1\}$ with $m\%n \neq 0$, we obtain $m\%n \in \{0,1,\ldots,n-1\} \setminus \{0\} = \{1,2,\ldots,n-1\}$. Hence, $m\%n$ is a positive integer and satisfies $m\%n \leq n-1 < n$.

From $m\%n \equiv m \mod n$ and $a \mid n$, we obtain $m\%n \equiv m \mod a$ (by Proposition 2.3.4 **(e)**, applied to a, $m\%n$ and m instead of m, a and b). But $m \equiv 0 \mod a$ (since $a \mid m$). Thus, $m\%n \equiv m \equiv 0 \mod a$. In other words, $a \mid m\%n$. Similarly, $b \mid m\%n$.

So we have proven that $(a \mid m\%n \text{ and } b \mid m\%n)$. In other words, $m\%n$ is a common multiple of a and b. In other words, $m\%n \in \operatorname{Mul}(a,b)$. Therefore, $m\%n$ is a positive element of $\operatorname{Mul}(a,b)$ (since $m\%n$ is positive). Thus, $m\%n \geq n$ (since n is the **smallest** positive element of $\operatorname{Mul}(a,b)$). This contradicts the fact that $m\%n < n$. This contradiction shows that our assumption was false. Hence, Lemma 2.11.8 is proven. □

Proof of Theorem 2.11.7. **(a)** Let $m \in \mathbb{Z}$. In order to prove (28), we need to prove the "$\Longrightarrow$" and "$\Longleftarrow$" directions of the equivalence (28). But this is easy: The "$\Longrightarrow$" direction is just the statement of Lemma 2.11.8, whereas the "$\Longleftarrow$" direction is trivial (to wit: if $\operatorname{lcm}(a,b) \mid m$, then

$$\begin{aligned} a &\mid \operatorname{lcm}(a,b) && \text{(by Proposition 2.11.5 \textbf{(c)})} \\ &\mid m \end{aligned}$$

and

$$\begin{aligned} b &\mid \operatorname{lcm}(a,b) && \text{(by Proposition 2.11.5 \textbf{(c)})} \\ &\mid m \end{aligned}$$

and thus $(a \mid m \text{ and } b \mid m)$). Hence, the equivalence (28) is proven. This proves Theorem 2.11.7 **(a)**.

(b) Theorem 2.11.7 **(b)** can be derived from Theorem 2.11.7 **(a)** in the same way as Theorem 2.9.15 **(b)** was derived from Theorem 2.9.15 **(a)** (after the necessary changes are made – such as flipping all divisibility relations and replacing "divisor" by "multiple").

(c) Theorem 2.11.7 **(c)** can be derived from Theorem 2.11.7 **(b)** in the same way as Theorem 2.9.15 **(c)** was derived from Theorem 2.9.15 **(b)** (after the necessary changes are made – such as flipping all divisibility relations and replacing "divisor" by "multiple"). □

Our next claim is an analogue of Theorem 2.9.21:

Theorem 2.11.9. Let $b_1, b_2, \ldots, b_k$ be integers.

(a) For each $m \in \mathbb{Z}$, we have the following logical equivalence:

$$(b_i \mid m \text{ for all } i \in \{1, 2, \ldots, k\}) \iff (\operatorname{lcm}(b_1, b_2, \ldots, b_k) \mid m).$$

(b) The common multiples of $b_1, b_2, \ldots, b_k$ are precisely the multiples of $\operatorname{lcm}(b_1, b_2, \ldots, b_k)$.

(c) We have $\operatorname{Mul}(b_1, b_2, \ldots, b_k) = \operatorname{Mul}(\operatorname{lcm}(b_1, b_2, \ldots, b_k))$.

(d) If $k > 0$, then

$$\operatorname{lcm}(b_1, b_2, \ldots, b_k) = \operatorname{lcm}(\operatorname{lcm}(b_1, b_2, \ldots, b_{k-1}), b_k).$$

Proof of Theorem 2.11.9 (sketched). It is not hard to transform our above proof of Theorem 2.9.21 into a proof of Theorem 2.11.9. To do so, we need (of course) to flip the divisibility relations and replace "divisor" by "multiple" and "gcd" by "lcm". (Some more changes need to be made as well – for example, the induction base needs to be handled differently, and the WLOG assumption that "the integers $b_1, b_2, \ldots, b_\ell$ are not all 0" needs to be replaced by a WLOG assumption that "the integers $b_1, b_2, \ldots, b_\ell$ are all nonzero". Also, "largest element" needs to be replaced by "smallest positive element". But these are fairly straightforward changes; the main thrust of the argument remains unchanged.) □

Exercise 2.11.1. Let $a, b \in \mathbb{Z}$.

(a) Prove that $\operatorname{lcm}(a, b) = \operatorname{lcm}(b, a)$.

(b) Prove that $\operatorname{lcm}(-a, b) = \operatorname{lcm}(a, b)$.

(c) Prove that $\operatorname{lcm}(a, -b) = \operatorname{lcm}(a, b)$.

(d) If $a \mid b$, then $\operatorname{lcm}(a, b) = |b|$.

(e) Let $s \in \mathbb{Z}$. Prove that $\operatorname{lcm}(sa, sb) = |s| \operatorname{lcm}(a, b)$.

Exercise 2.11.2. Let a, b, c be three integers.

(a) Prove that $\gcd(a, b, c) \cdot \operatorname{lcm}(bc, ca, ab) = |abc|$.

(b) Prove that $\operatorname{lcm}(a, b, c) \cdot \gcd(bc, ca, ab) = |abc|$.

2.12. The Chinese remainder theorem (elementary form)

Theorem 2.12.1. Let m and n be two coprime integers. Let $a, b \in \mathbb{Z}$.

(a) There exists an integer $x \in \mathbb{Z}$ such that

$$(x \equiv a \bmod m \text{ and } x \equiv b \bmod n).$$

(b) If x_1 and x_2 are two such integers x, then $x_1 \equiv x_2 \bmod mn$.

Theorem 2.12.1 is known as the *Chinese remainder theorem*. More precisely, there is a sizeable cloud of results that share this name; Theorem 2.12.1 is one of the most elementary and basic of these results. A more general result is Theorem 2.12.4 further below. However, the strongest and most general "Chinese remainder theorems" rely on concepts from abstract algebra such as rings and ideals; it will take us a while to get to them.

Theorem 2.12.1 has gotten its name from the fact that a first glimpse of it appears in "Master Sun's Mathematical Manual" from the 3rd century AD; it took centuries until it become a theorem with proof and precise statement.

The claim of Theorem 2.12.1 **(b)** is often restated as "This integer x (i.e., the integer x satisfying $(x \equiv a \bmod m \text{ and } x \equiv b \bmod n)$) is unique modulo mn". The "modulo mn" here signifies that what we are not claiming literal uniqueness (which would mean that if x_1 and x_2 are two such integers x, then $x_1 = x_2$), but merely claiming a weaker form (namely, that if x_1 and x_2 are two such integers x, then $x_1 \equiv x_2 \bmod mn$).

Example 2.12.2. Theorem 2.12.1 **(a)** (applied to $m = 5$, $n = 6$ and $a = 3$ and $b = 2$) shows that there exists an integer $x \in \mathbb{Z}$ such that

$$(x \equiv 3 \bmod 5 \text{ and } x \equiv 2 \bmod 6).$$

We will soon find such an integer, after we have proved Theorem 2.12.1.

Proof of Theorem 2.12.1. The integers m and n are coprime. In other words, $m \perp n$, so that $n \perp m$ (by Proposition 2.10.4).

(a) Theorem 2.10.8 **(b)** (applied to m instead of a) shows that there exists an $m' \in \mathbb{Z}$ such that $mm' \equiv 1 \bmod n$.

Similarly, there exists an $n' \in \mathbb{Z}$ such that $nn' \equiv 1 \bmod m$ (since m and n play symmetric roles in Theorem 2.12.1).

Now, set $x_0 = nn'a + mm'b$. Then,

$$x_0 = \underbrace{nn'}_{\equiv 1 \bmod m} a + \underbrace{mm'b}_{\equiv 0 \bmod m} \equiv 1a + 0 = a \bmod m$$

(here, we have used the Principle of substitutivity for congruences, which we described in Section 2.5) and similarly $x_0 \equiv b \bmod n$. Thus, there exists an integer $x \in \mathbb{Z}$ such that $(x \equiv a \bmod m \text{ and } x \equiv b \bmod n)$ (namely, $x = x_0$). This proves Theorem 2.12.1 **(a)**.

(b) Let x_1 and x_2 be two such integers x. We want to prove that $x_1 \equiv x_2 \bmod mn$.

We know that x_1 is an integer x such that $(x \equiv a \operatorname{mod} m$ and $x \equiv b \operatorname{mod} n)$. Thus, $x_1 \equiv a \operatorname{mod} m$ and $x_1 \equiv b \operatorname{mod} n$.

In particular, $x_1 \equiv a \operatorname{mod} m$, and similarly $x_2 \equiv a \operatorname{mod} m$. Thus, $x_1 \equiv a \equiv x_2 \operatorname{mod} m$, so that $m \mid x_1 - x_2$. Similarly, $n \mid x_1 - x_2$. Since $m \perp n$, we thus obtain $mn \mid x_1 - x_2$ (by Theorem 2.10.7, applied to m, n and $x_1 - x_2$ instead of a, b and c). In other words, $x_1 \equiv x_2 \operatorname{mod} mn$. This proves Theorem 2.12.1. □

Example 2.12.3. Assume that we want to find an $x \in \mathbb{Z}$ such that

$$(x \equiv 3 \operatorname{mod} 5 \text{ and } x \equiv 2 \operatorname{mod} 6).$$

To compute such an x, let us follow the proof of Theorem 2.12.1 **(a)** above.

We need a modular inverse $5'$ of 5 modulo 6. Such an inverse is 5, since $5 \cdot 5 \equiv 1 \operatorname{mod} 6$. (In this particular case, finding this modular inverse was easy, because all we had to do is to test the 6 numbers $0, 1, 2, 3, 4, 5$; it is clear that a modular inverse of a modulo m, if it exists, can be found within the set $\{0, 1, \ldots, m-1\}$. In general, there is a quick way to find a modular inverse of an integer a modulo an integer m using the "Extended Euclidean algorithm".)

We need a modular inverse $6'$ of 6 modulo 5. Such an inverse is 1, since $6 \cdot 1 \equiv 1 \operatorname{mod} 5$.

Now, the proof of Theorem 2.12.1 **(a)** tells us that $x_0 = 6 \cdot 6' \cdot 3 + 5 \cdot 5' \cdot 2$ is an integer $x \in \mathbb{Z}$ such that $(x \equiv 3 \operatorname{mod} 5$ and $x \equiv 2 \operatorname{mod} 6)$. This x_0 is

$$6 \cdot 6' \cdot 3 + 5 \cdot 5' \cdot 2 = 6 \cdot 1 \cdot 3 + 5 \cdot 5 \cdot 2 = 68.$$

So we have found an $x \in \mathbb{Z}$ such that $(x \equiv 3 \operatorname{mod} 5$ and $x \equiv 2 \operatorname{mod} 6)$, namely $x = 68$. (We can easily check this: $68 \equiv 3 \operatorname{mod} 5$ since $68 - 3 = 5 \cdot 13$; and $68 \equiv 2 \operatorname{mod} 6$ since $68 - 2 = 6 \cdot 11$.)

There is also a version of Theorem 2.12.1 for multiple integers:

Theorem 2.12.4. Let $m_1, m_2, \ldots, m_k$ be k mutually coprime integers. Let $a_1, a_2, \ldots, a_k \in \mathbb{Z}$.

(a) There exists an integer x such that

$$(x \equiv a_i \operatorname{mod} m_i \text{ for all } i \in \{1, 2, \ldots, k\}). \tag{29}$$

(b) If x_1 and x_2 are two such integers x, then $x_1 \equiv x_2 \operatorname{mod} m_1 m_2 \cdots m_k$.

Again, Theorem 2.12.4 **(b)** is often stated in the form "This integer x is unique modulo $m_1 m_2 \cdots m_k$".

Clearly, Theorem 2.12.1 is the particular case of Theorem 2.12.4 obtained for $k = 2$.

Proof of Theorem 2.12.4. Forget that we fixed k and $m_1, m_2, \ldots, m_k$ and $a_1, a_2, \ldots, a_k$.

(a) We shall prove Theorem 2.12.4 **(a)** by induction on k:

Induction base: Let us check that Theorem 2.12.4 **(a)** holds for $k = 0$. Indeed, if $k = 0$, then Theorem 2.12.4 **(a)** states the following:

> *Claim 0:* Let $m_1, m_2, \ldots, m_0$ be 0 mutually coprime integers. Let $a_1, a_2, \ldots, a_0 \in \mathbb{Z}$. There exists an integer x such that
>
> $$\left(x \equiv a_i \operatorname{mod} m_i \text{ for all } i \in \{1, 2, \ldots, 0\}\right). \tag{30}$$

But Claim 0 is true, because (30) is vacuously true[27] for **any** integer x (so we can take, for example, $x = 0$). In other words, Theorem 2.12.4 **(a)** holds for $k = 0$; thus, the induction base is complete.

Needless to say, Claim 0 is not an interesting statement, but it is a perfectly valid induction base! (But you are free to check the case $k = 1$ by hand – its proof is almost as easy as that for $k = 0$.)

Induction step: Let ℓ be a positive integer. Assume that Theorem 2.12.4 **(a)** holds for $k = \ell - 1$. We must now prove that Theorem 2.12.4 **(a)** holds for $k = \ell$.

We have assumed that Theorem 2.12.4 **(a)** holds for $k = \ell - 1$. In other words, the following claim holds:

> *Claim 1:* Let $m_1, m_2, \ldots, m_{\ell-1}$ be $\ell - 1$ mutually coprime integers. Let $a_1, a_2, \ldots, a_{\ell-1} \in \mathbb{Z}$. There exists an integer x such that
>
> $$\left(x \equiv a_i \operatorname{mod} m_i \text{ for all } i \in \{1, 2, \ldots, \ell - 1\}\right). \tag{31}$$

We must prove that Theorem 2.12.4 **(a)** holds for $k = \ell$. In other words, we must prove the following claim:

> *Claim 2:* Let $m_1, m_2, \ldots, m_\ell$ be ℓ mutually coprime integers. Let $a_1, a_2, \ldots, a_\ell \in \mathbb{Z}$. There exists an integer x such that
>
> $$\left(x \equiv a_i \operatorname{mod} m_i \text{ for all } i \in \{1, 2, \ldots, \ell\}\right). \tag{32}$$

[*Proof of Claim 2:* The main idea of this proof is to combine Claim 1 (applied to $m_1, m_2, \ldots, m_{\ell-1}$) with Theorem 2.12.1 (applied to the coprime integers $m_1 m_2 \cdots m_{\ell-1}$ and m_ℓ). In details:

The ℓ integers $m_1, m_2, \ldots, m_\ell$ are mutually coprime. Thus, the $\ell - 1$ integers $m_1, m_2, \ldots, m_{\ell-1}$ are mutually coprime. Hence, Claim 1 shows that there exists an integer x such that

$$\left(x \equiv a_i \operatorname{mod} m_i \text{ for all } i \in \{1, 2, \ldots, \ell - 1\}\right).$$

Consider this x, and denote it by u. Thus, u is an integer such that

$$\left(u \equiv a_i \operatorname{mod} m_i \text{ for all } i \in \{1, 2, \ldots, \ell - 1\}\right). \tag{33}$$

[27] since there exists no $i \in \{1, 2, \ldots, 0\}$

Define an integer $m = m_1 m_2 \cdots m_{\ell-1}$.

The integers m and m_ℓ are coprime[28]. Hence, Theorem 2.12.1 **(a)** (applied to $n = m_\ell$, $a = u$ and $b = a_\ell$) yields that there exists an integer $x \in \mathbb{Z}$ such that

$$(x \equiv u \operatorname{mod} m \text{ and } x \equiv a_\ell \operatorname{mod} m_\ell).$$

Consider this x, and denote it by v. Thus, v is an integer such that

$$(v \equiv u \operatorname{mod} m \text{ and } v \equiv a_\ell \operatorname{mod} m_\ell).$$

Now, let $i \in \{1, 2, \ldots, \ell - 1\}$. Then,

$$m = m_1 m_2 \cdots m_{\ell-1} = m_i \cdot (m_1 m_2 \cdots m_{i-1} m_{i+1} m_{i+2} \cdots m_{\ell-1});$$

thus, $m_i \mid m$ (since $m_1 m_2 \cdots m_{i-1} m_{i+1} m_{i+2} \cdots m_{\ell-1}$ is an integer). But as we just have shown, we have $v \equiv u \operatorname{mod} m$. Hence, Proposition 2.3.4 **(e)** (applied to v, u, m and m_i instead of a, b, n and m) yields $v \equiv u \operatorname{mod} m_i$ (since $m_i \mid m$). Hence,

$$v \equiv u \equiv a_i \operatorname{mod} m_i \qquad (\text{by } (33)).$$

Now, forget that we fixed i. We thus have proven the congruence $v \equiv a_i \operatorname{mod} m_i$ for each $i \in \{1, 2, \ldots, \ell - 1\}$. But this congruence also holds for $i = \ell$ (since $v \equiv a_\ell \operatorname{mod} m_\ell$). Hence, this congruence holds for all $i \in \{1, 2, \ldots, \ell\}$. In other words, we have

$$v \equiv a_i \operatorname{mod} m_i \text{ for all } i \in \{1, 2, \ldots, \ell\}.$$

Thus, there exists an integer x such that

$$(x \equiv a_i \operatorname{mod} m_i \text{ for all } i \in \{1, 2, \ldots, \ell\})$$

(namely, $x = v$). This proves Claim 2.]

We have now proven Claim 2. In other words, Theorem 2.12.4 **(a)** is true for $k = \ell$. Thus, the induction step is complete, so we have proven Theorem 2.12.4 **(a)** by induction.

(b) Let k and $m_1, m_2, \ldots, m_k$ and $a_1, a_2, \ldots, a_k$ be as in Theorem 2.12.4. Let x_1 and x_2 be two integers x such that (29). We must prove that $x_1 \equiv x_2 \operatorname{mod} m_1 m_2 \cdots m_k$.

We know that x_1 is an integer x such that (29). In other words, x_1 is an integer and has the property that

$$(x_1 \equiv a_i \operatorname{mod} m_i \text{ for all } i \in \{1, 2, \ldots, k\}). \tag{34}$$

[28] *Proof.* Recall that the ℓ integers $m_1, m_2, \ldots, m_\ell$ are mutually coprime. In other words, $m_i \perp m_j$ for any $i, j \in \{1, 2, \ldots, \ell\}$ satisfying $i \neq j$. Applying this to $j = \ell$, we conclude that $m_i \perp m_\ell$ for any $i \in \{1, 2, \ldots, \ell\}$ satisfying $i \neq \ell$. In other words, $m_i \perp m_\ell$ for any $i \in \{1, 2, \ldots, \ell - 1\}$ (since the numbers $i \in \{1, 2, \ldots, \ell\}$ satisfying $i \neq \ell$ are precisely the numbers $i \in \{1, 2, \ldots, \ell - 1\}$). In other words, each $i \in \{1, 2, \ldots, \ell - 1\}$ satisfies $m_i \perp m_\ell$. Hence, Exercise 2.10.2 (applied to $c = m_\ell$, $k = \ell - 1$ and $a_i = m_i$) yields that $m_1 m_2 \cdots m_{\ell-1} \perp m_\ell$. This rewrites as $m \perp m_\ell$ (since $m = m_1 m_2 \cdots m_{\ell-1}$). In other words, the integers m and m_ℓ are coprime.

Now, let $i \in \{1, 2, \ldots, k\}$. Then, (34) yields $x_1 \equiv a_i \operatorname{mod} m_i$. Similarly, $x_2 \equiv a_i \operatorname{mod} m_i$. Hence, $x_1 \equiv a_i \equiv x_2 \operatorname{mod} m_i$. In other words, $m_i \mid x_1 - x_2$.

Now, forget that we fixed i. We thus have shown that $m_i \mid x_1 - x_2$ for each $i \in \{1, 2, \ldots, k\}$. Hence, Exercise 2.10.3 (applied to $c = x_1 - x_2$ and $b_i = m_i$) shows that $m_1 m_2 \cdots m_k \mid x_1 - x_2$ (since $m_1, m_2, \ldots, m_k$ are mutually coprime). In other words, $x_1 \equiv x_2 \operatorname{mod} m_1 m_2 \cdots m_k$. This proves Theorem 2.12.4 **(b)**. □

2.13. Primes

2.13.1. Definition and the Sieve of Eratosthenes

Definition 2.13.1. Let p be an integer greater than 1. We say that p is *prime* if the only positive divisors of p are 1 and p. A prime integer is often just called *a prime*.

Note that we required p to be greater than 1 here. Thus, 1 does not count as prime even though its only positive divisor is 1 itself.

Example 2.13.2. **(a)** The only positive divisors of 7 are 1 and 7. Thus, 7 is a prime.

(b) The positive divisors of 14 are 1, 2, 7 and 14. These are more than just 1 and 14. Thus, 14 is not a prime.

(c) None of the numbers $4, 6, 8, 10, 12, 14, 16, \ldots$ (that is, the multiples of 2 that are larger than 2) is a prime. Indeed, if p is any of these numbers, then p has a positive divisor other than 1 and p (namely, 2), and therefore does not meet the definition of "prime".

(d) None of the numbers $6, 9, 12, 15, 18, \ldots$ (that is, the multiples of 3 that are larger than 3) is a prime. Indeed, if p is any of these numbers, then p has a positive divisor other than 1 and p (namely, 3), and therefore does not meet the definition of "prime".

Parts **(c)** and **(d)** of Example 2.13.2 suggest a method for finding all primes up to a given integer:

Example 2.13.3. Let us say we want to find all primes that are ≤ 30.

Step 1: All such primes must lie in $\{2, 3, \ldots, 30\}$ (since a prime is always an integer greater than 1); thus, let us first write down all elements of $\{2, 3, \ldots, 30\}$:

$$\begin{array}{cccccccccc} & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \end{array}.$$

(We are using a table just in order to fit these elements on a page.)

We now plan to remove non-prime numbers from this table until only primes are left.

Step 2: First, let us remove all multiples of 2 that are larger than 2 from our table, because none of them is a prime (see Example 2.13.2 **(c)**). We thus are left with

$$\begin{array}{cccccc} & 2 & 3 & 5 & 7 & 9 \\ 11 & & 13 & 15 & 17 & 19 \\ 21 & & 23 & 25 & 27 & 29 \end{array}.$$

Step 3: Next, let us remove all multiples of 3 that are larger than 3 from our table, because none of them is a prime (see Example 2.13.2 **(d)**). We thus are left with

$$\begin{array}{cccccc} & 2 & 3 & 5 & 7 & \\ 11 & & 13 & & 17 & 19 \\ & & 23 & 25 & & 29 \end{array}.$$

(Note that some of these multiples have already been removed in Step 2.)

Step 4: Next, let us remove all multiples of 4 that are larger than 4 from our table, because none of them is a prime (for similar reasons). It turns out that this does not change the table at all, because all such multiples have already been removed in Step 2. This is not a coincidence: Since 4 itself has been removed, we know that 4 was a multiple of some number $d < 4$ (in this case, $d = 2$) whose multiples have been removed; therefore, all multiples of 4 are also multiples of d and thus have been removed along with 4.

Step 5: Next, let us remove all multiples of 5 that are larger than 5 from our table, because none of them is a prime (for similar reasons). We thus are left with

$$\begin{array}{cccccc} & 2 & 3 & 5 & 7 & \\ 11 & & 13 & & 17 & 19 \\ & & 23 & & & 29 \end{array}.$$

Step 6: Next, let us remove all multiples of 6 that are larger than 6 from our table, because none of them is a prime. Just as Step 4, this does not change the table, since all such multiples have already been removed in Step 2.

Step 7: Next, let us remove all multiples of 7 that are larger than 7 from our table, because none of them is a prime. Again, this does not change the table, since all such multiples have already been removed.

Proceed likewise until Step 30, at which point the table has become

$$\begin{array}{cccccc} & 2 & 3 & 5 & 7 & \\ 11 & & 13 & & 17 & 19 \\ & & 23 & & & 29 \end{array}.$$

(You are reading it right: None of the steps from Step 6 to Step 30 causes any changes to the table, since all multiples that these steps attempt to remove have already been removed beforehand.)

The resulting table has the following property: If p is an element of this table, then p cannot be a multiple of any $d \in \{2, 3, \ldots, p-1\}$ (because if it was such a multiple, then it would have been removed from the table in Step d or earlier).

In other words, if p is an element of this table, then p cannot have any divisor $d \in \{2, 3, \ldots, p-1\}$. In other words, if p is an element of this table, then the only positive divisors of p are 1 and p. In other words, if p is an element of this table, then p is prime. Conversely, any prime ≤ 30 is in our table, since the only numbers we have removed from the table were guaranteed to be non-prime. Thus, the table now contains all the primes ≤ 30 and only them. So we conclude that the primes ≤ 30 are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

This method of finding primes is known as the **sieve of Eratosthenes**. We could have made it more efficient using the following two tricks:

- If a number $d \in \{2, 3, \ldots, 30\}$ has been removed from the table before Step d, then we know immediately that Step d will not change the table (because all multiples of d have already been removed before this step). Thus, we do not need to make this step.
- If $d \in \{2, 3, \ldots, 30\}$ satisfies $d^2 > 30$, then Step d will not change the table[29]. Thus, we only need to take the Steps d with $d^2 \leq 30$.

Together, these tricks tell us that the only steps we need to take are the Steps 2, 3 and 5.

2.13.2. Basic properties of primes

Proposition 2.13.4. Let p be a prime. Then, each $i \in \{1, 2, \ldots, p-1\}$ is coprime to p.

Proof of Proposition 2.13.4. Let $i \in \{1, 2, \ldots, p-1\}$. We must prove that i is coprime to p.

[29] *Proof.* Let $d \in \{2, 3, \ldots, 30\}$ be such that $d^2 > 30$. We must show that Step d will not change the table.

Indeed, at Step d, we remove all multiples of d that are larger than d from our table. But all these multiples (at least the ones that appear in our table) have already been removed from this table before Step d.

Here is why: Let $m \in \{2, 3, \ldots, 30\}$ be a multiple of d that is larger than d. Then, $d \mid m$ (since m is a multiple of d) and thus $m/d \in \mathbb{Z}$. Hence, m/d is a positive integer (since m/d is clearly positive) and $m/d > 1$ (since m is larger than d). Furthermore, $m/d \mid m$ (since $m = (m/d)\, d$), so that m is a multiple of m/d. But $d > 1$ (since $d \in \{2, 3, \ldots, 30\}$) and thus $m/d < m$. In other words, $m > m/d$. Hence, m is a multiple of m/d that is larger than m/d.

Furthermore, $d^2 > 30 \geq m$ (since $m \in \{2, 3, \ldots, 30\}$). Dividing both sides of this inequality by d, we obtain $d > m/d$. Hence, $m/d < d$, so that $m/d \in \{2, 3, \ldots, d-1\}$ (since $m/d > 1$). Thus, before Step d begins, Step m/d has already happened. Of course, Step m/d has removed m from the table (since m is a multiple of m/d that is larger than m/d). Therefore, the number m has already been removed from the table before Step d.

Now, forget that we fixed m. We thus have shown that if $m \in \{2, 3, \ldots, 30\}$ is a multiple of d that is larger than d, then m m has already been removed from the table before Step d. In other words, all multiples of d that we try to remove at Step d have already been removed before Step d. Therefore, Step d does not change our table.

From $i \in \{1, 2, \ldots, p-1\}$, we obtain $1 \leq i \leq p-1$ and thus $i \geq 1 > 0$, so that $i \neq 0$. Hence, i and p are not all zero. Also, $|i| = i$ (since $i > 0$).

Also, $\gcd(i, p)$ is a positive integer (since i and p are not all zero). Thus, $|\gcd(i, p)| = \gcd(i, p)$.

Proposition 2.9.7 **(f)** (applied to $a = i$ and $b = p$) shows that $\gcd(i, p) \mid i$ and $\gcd(i, p) \mid p$. From $\gcd(i, p) \mid i$ and $i \neq 0$, we obtain $|\gcd(i, p)| \leq |i|$ (by Exercise 2.2.3 **(b)**, applied to $a = \gcd(i, p)$ and $b = i$). In view of $|\gcd(i, p)| = \gcd(i, p)$ and $|i| = i$, this rewrites as $\gcd(i, p) \leq i$. Hence, $\gcd(i, p) \leq i \leq p-1 < p$ and therefore $\gcd(i, p) \neq p$.

We know that p is prime. In other words, the only positive divisors of p are 1 and p (by the definition of "prime").

The integer $\gcd(i, p)$ is a positive divisor of p (since $\gcd(i, p)$ is positive and satisfies $\gcd(i, p) \mid p$), and thus must be either 1 or p (since the only positive divisors of p are 1 and p). Since we know that $\gcd(i, p) \neq p$, we thus conclude that $\gcd(i, p) = 1$. In other words, i is coprime to p (by the definition of "coprime"). This proves Proposition 2.13.4. □

Note that this proposition characterizes primes: If $p > 1$ is an integer such that each $i \in \{1, 2, \ldots, p-1\}$ is coprime to p, then p is prime. (The proof of this is left as an easy exercise.)

Proposition 2.13.5. Let p be a prime. Let $a \in \mathbb{Z}$. Then, either $p \mid a$ or $p \perp a$.

Proof of Proposition 2.13.5. Assume the contrary. Thus, neither $p \mid a$ nor $p \perp a$.

We know that p is prime. In other words, p is an integer greater than 1 such that the only positive divisors of p are 1 and p (by the definition of "prime").

In particular, p is greater than 1. Hence, $p > 1 > 0$, so that $p \neq 0$. Hence, a and p are not all zero. Thus, $\gcd(a, p)$ is a positive integer.

Proposition 2.9.7 **(f)** (applied to $b = p$) shows that $\gcd(a, p) \mid a$ and $\gcd(a, p) \mid p$. If we had $\gcd(a, p) = p$, then we would obtain $p = \gcd(a, p) \mid a$, which would contradict the fact that we do not have $p \mid a$. Hence, we cannot have $\gcd(a, p) = p$. In other words, we have $\gcd(a, p) \neq p$.

The integer $\gcd(a, p)$ is a positive divisor of p (since $\gcd(a, p)$ is positive and satisfies $\gcd(a, p) \mid p$), and thus must be either 1 or p (since the only positive divisors of p are 1 and p). Since we know that $\gcd(a, p) \neq p$, we thus conclude that $\gcd(a, p) = 1$. But Proposition 2.9.7 **(b)** (applied to $b = p$) yields $\gcd(a, p) = \gcd(p, a)$. Thus, $\gcd(p, a) = \gcd(a, p) = 1$. In other words, p is coprime to a (by the definition of "coprime"). In other words, $p \perp a$. This contradicts the fact that we don't have $p \perp a$.

This contradiction shows that our assumption was false. Hence, Proposition 2.13.5 is proven. □

We note that a converse of Proposition 2.13.5 holds as well: If $p > 1$ is an integer such that each $a \in \mathbb{Z}$ satisfies either $p \mid a$ or $p \perp a$, then p is a prime. This is easy to prove and left to the reader.

Exercise 2.13.1. Let p and q be two distinct primes. Prove that $p \perp q$.

Theorem 2.13.6. Let p be a prime. Let $a, b \in \mathbb{Z}$ such that $p \mid ab$. Then, $p \mid a$ or $p \mid b$.

Proof of Theorem 2.13.6. Assume the contrary. Thus, neither $p \mid a$ nor $p \mid b$.

Proposition 2.13.5 yields that either $p \mid a$ or $p \perp a$. Hence, $p \perp a$ (since $p \mid a$ does not hold). But $p \mid ab$. Hence, Theorem 2.10.6 (applied to p, a and b instead of a, b and c) yields $p \mid b$. This contradicts the fact that we don't have $p \mid b$.

This contradiction shows that our assumption was false. Hence, Theorem 2.13.6 is proven. □

Again, Theorem 2.13.6 has a converse:

Exercise 2.13.2. Let $p > 1$ be an integer. Assume that for every $a, b \in \mathbb{Z}$ satisfying $p \mid ab$, we must have $p \mid a$ or $p \mid b$. Prove that p is prime.

There is also a version of Theorem 2.13.6 for products of multiple integers:

Proposition 2.13.7. Let p be a prime. Let $a_1, a_2, \ldots, a_k$ be integers such that $p \mid a_1 a_2 \cdots a_k$. Then, $p \mid a_i$ for some $i \in \{1, 2, \ldots, k\}$.

We could prove Proposition 2.13.7 by induction on k. But here is a more direct argument:

Proof of Proposition 2.13.7. Assume the contrary. Thus, there exists no $i \in \{1, 2, \ldots, k\}$ such that $p \mid a_i$. In other words, for each $i \in \{1, 2, \ldots, k\}$, we have

$$(\text{not } p \mid a_i). \tag{35}$$

Now, let $i \in \{1, 2, \ldots, k\}$. Then, we don't have $p \mid a_i$ (by (35)). But Proposition 2.13.5 (applied to $a = a_i$) shows that either $p \mid a_i$ or $p \perp a_i$. Hence, we have $p \perp a_i$ (since we don't have $p \mid a_i$). In other words, $a_i \perp p$ (by Proposition 2.10.4).

Now, forget that we fixed i. We thus have proven that each $i \in \{1, 2, \ldots, k\}$ satisfies $a_i \perp p$. Hence, Exercise 2.10.2 (applied to $c = p$) yields $a_1 a_2 \cdots a_k \perp p$. In other words, $a_1 a_2 \cdots a_k$ is coprime to p. In other words, $\gcd(a_1 a_2 \cdots a_k, p) = 1$. Hence, Proposition 2.9.7 **(b)** yields $\gcd(p, a_1 a_2 \cdots a_k) = \gcd(a_1 a_2 \cdots a_k, p) = 1$.

But p is prime; thus, $p > 1$. Hence, p is positive. Recall that $p \mid a_1 a_2 \cdots a_k$; thus, Proposition 2.9.7 **(i)** (applied to $a = p$ and $b = a_1 a_2 \cdots a_k$) yields $\gcd(p, a_1 a_2 \cdots a_k) = |p| = p$ (since p is positive). Comparing this with $\gcd(p, a_1 a_2 \cdots a_k) = 1$, we obtain $p = 1$. This contradicts $p > 1$. This contradiction shows that our assumption was wrong. This proves Proposition 2.13.7. □

Exercise 2.13.3. Let p be a prime. Let k be a positive integer. Let $a \in \mathbb{Z}$. Prove that $a \perp p^k$ holds if and only if $p \nmid a$.

2.13.3. Prime factorization I

The next simple proposition says that every integer $n > 1$ is divisible by at least one prime:

Proposition 2.13.8. Let $n > 1$ be an integer. Then, there exists at least one prime p such that $p \mid n$.

Proof of Proposition 2.13.8. Clearly, n is a divisor of n such that $n > 1$. Thus, there exists a divisor q of n such that $q > 1$ (namely, $q = n$). Let d be the **smallest** such divisor[30]. Thus, d is a divisor of n and satisfies $d > 1$. The integer d is positive (since $d > 1 > 0$) and satisfies $d \mid n$ (since d is a divisor of n).

We claim that d is a prime.

[*Proof:* Let e be any positive divisor of d. Assume (for the sake of contradiction) that $e \notin \{1, d\}$. Thus, $e \neq 1$ and $e \neq d$. Now, e is a divisor of d; thus, $e \mid d \mid n$. In other words, e is a divisor of n. Also, $e > 1$ (because e is positive and $e \neq 1$). Hence, e is a divisor q of n such that $q > 1$.

But d was defined as the **smallest** divisor q of n such that $q > 1$. Hence, any such divisor is $\geq d$. In other words, any divisor q of n such that $q > 1$ must satisfy $q \geq d$. Applying this to $q = e$, we conclude that $e \geq d$ (since e is a divisor q of n such that $q > 1$). Combined with $e \neq d$, this yields $e > d$.

But $e \mid d$ and $d \neq 0$ (since $d > 1 > 0$). Hence, $|e| \leq |d|$ (by Exercise 2.2.3 **(b)**, applied to $a = e$ and $b = d$). Since e is positive, we have $|e| = e$, so that $e = |e| \leq |d| = d$ (since d is positive). This contradicts $e > d$. This contradiction shows that our assumption (that $e \notin \{1, d\}$) was false. Thus, we have proven that $e \in \{1, d\}$. In other words, e is either 1 or d.

Now, forget that we fixed e. We thus have proven that if e is any positive divisor of d, then $e \in \{1, d\}$. In other words, any positive divisor of d is either 1 or d. Thus, the only positive divisors of d are 1 and d (since 1 and d clearly **are** positive divisors of d). In other words, d is prime (by the definition of "prime").]

So we know that $d \mid n$, and that d is prime. Hence, there exists at least one prime p such that $p \mid n$ (namely, $p = d$). This proves Proposition 2.13.8. □

Definition 2.13.9. Let n be an integer. A *prime factor* of n means a prime p such that $p \mid n$. Some say "prime divisor" instead of "prime factor".

Thus, Proposition 2.13.8 says that each integer $n > 1$ has at least one prime divisor.

Proposition 2.13.10. Let n be a positive integer. Then, n can be written as a product of finitely many primes.

[30] This exists, because the set of possible candidates is nonempty (by the previous sentence) and finite.

Example 2.13.11. **(a)** The integer 60 can be written as a product of four primes: namely, $60 = 2 \cdot 2 \cdot 3 \cdot 5$.

(b) The integer 1 is the product of 0 many primes (because a product of 0 many primes is the empty product, which is defined to be 1).

Proof of Proposition 2.13.10. We shall prove Proposition 2.13.10 by strong induction on n. Thus, we fix a positive integer N, and we assume (as the induction hypothesis) that Proposition 2.13.10 holds whenever $n < N$. We must now prove that Proposition 2.13.10 holds for $n = N$. In other words, we must prove that N can be written as a product of finitely many primes.

If $N = 1$, then this is obvious (because 1 is a product of 0 many primes[31]). Thus, for the rest of this proof, we WLOG assume that $N \neq 1$. Hence, $N > 1$ (since N is a positive integer). Therefore, Proposition 2.13.8 (applied to $n = N$) shows that there exists at least one prime p such that $p \mid N$. Consider this p.

We have $p \mid N$. In other words, there exists an integer c such that $N = pc$. Consider this c. We have $p > 1$ (since p is prime); thus, p is positive. Hence, $p \neq 0$. Thus, solving the equality $N = pc$ for c, we find $c = N / \underbrace{p}_{>1} < N/1$ (since N is positive), so that $c < N/1 = N$. But our induction hypothesis says that Proposition 2.13.10 holds whenever $n < N$. Hence, we can apply Proposition 2.13.10 to $n = c$ (since $c < N$). We thus conclude that c can be written as a product of finitely many primes. In other words, there exist primes $q_1, q_2, \ldots, q_k$ such that $c = q_1 q_2 \cdots q_k$. Consider these $q_1, q_2, \ldots, q_k$.

But

$$N = p \underbrace{c}_{=q_1 q_2 \cdots q_k} = p q_1 q_2 \cdots q_k.$$

Hence, N can be written as a product of finitely many primes (namely, of the primes $p, q_1, q_2, \ldots, q_k$). In other words, Proposition 2.13.10 holds for $n = N$. This completes the induction step. Hence, Proposition 2.13.10 is proven by strong induction. □

Proposition 2.13.10 shows that every positive integer n can be represented as a product of finitely many primes. Such a representation – or, more precisely, the list of the primes it contains – will be called the *prime factorization* of n. Rigorously speaking, this means that we make the following definition:

Definition 2.13.12. Let n be a positive integer. A *prime factorization* of n means a tuple $(p_1, p_2, \ldots, p_k)$ of primes such that $n = p_1 p_2 \cdots p_k$.

Keep in mind that "tuple" always means "ordered tuple" unless we say otherwise.

[31] See Example 2.13.11 **(b)**.

Example 2.13.13. **(a)** The prime factorizations of 12 are

$$(2,2,3), \qquad (2,3,2), \qquad (3,2,2).$$

Indeed, these three 3-tuples are prime factorizations of 12 because $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$. It is not hard to check that they are the only prime factorizations of 12.

(b) If p is a prime, then the only prime factorization of p is the 1-tuple (p).

(c) If p is a prime and $i \in \mathbb{N}$, then the only prime factorization of p^i is the i-tuple $\left(\underbrace{p, p, \ldots, p}_{i \text{ times}}\right)$. This is not quite obvious at this point (though it is not hard to derive from Proposition 2.13.7).

(d) The only prime factorization of 1 is the 0-tuple $()$.

This example suggests that all prime factorizations of a given positive integer n are equal to each other up to the order of their entries (i.e., are permutations of each other). This is indeed true, and we are going to prove this soon (in Theorem 2.13.31 below).

2.13.4. Permutations

First of all: what is a "permutation", and what exactly does "equal to each other up to the order of their entries" mean?

Informally speaking, a permutation of a tuple[32] $(a_1, a_2, \ldots, a_k)$ is a tuple obtained from $(a_1, a_2, \ldots, a_k)$ by rearranging its entries (without inserting new entries, or removing or duplicating existing entries). To be rigorous, we need to encode this rearrangement via a bijective map $\sigma : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$ which will tell us which entry of our original tuple will go to which position in the rearranged tuple. Such bijective maps, too, are called permutations – but permutations of sets, not of tuples. So let us first define permutations of a set, and then use this to define permutations of a tuple:

Definition 2.13.14. Let A be a set. A *permutation* of A means a bijective map $A \to A$.

Example 2.13.15. **(a)** The map $\{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ that sends $1, 2, 3, 4$ to $3, 1, 4, 2$ (respectively) is a permutation of $\{1, 2, 3, 4\}$.

(b) The map $\{1, 2, 3\} \to \{1, 2, 3\}$ that sends $1, 2, 3$ to $2, 3, 1$ (respectively) is a permutation of $\{1, 2, 3\}$.

(c) For each set A, the identity map $\mathrm{id} : A \to A$ is a permutation of A.

Thus, we have defined permutations of a set. We shall later study such permutations in more detail, at least for finite sets A.

[32] Recall: a prime factorization is a tuple.

Now we can define permutations of a tuple:

Definition 2.13.16. Let $(p_1, p_2, \ldots, p_k)$ be a k-tuple. A *permutation* of $(p_1, p_2, \ldots, p_k)$ means a k-tuple of the form $\left(p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(k)}\right)$ where σ is a permutation of the set $\{1, 2, \ldots, k\}$. A *permutation* of $(p_1, p_2, \ldots, p_k)$ is also known as a *rearrangement* of $(p_1, p_2, \ldots, p_k)$.

Example 2.13.17. (a) The 4-tuple $(1, 3, 1, 2)$ is a permutation of the 4-tuple $(3, 2, 1, 1)$. In fact, if we denote the 4-tuple $(3, 2, 1, 1)$ by (p_1, p_2, p_3, p_4), then there exists a permutation σ of the set $\{1, 2, 3, 4\}$ such that $(1, 3, 1, 2) = \left(p_{\sigma(1)}, p_{\sigma(2)}, p_{\sigma(3)}, p_{\sigma(4)}\right)$. (Actually, there exist two such permutations σ: One of them sends $1, 2, 3, 4$ to $3, 1, 4, 2$, while the other sends $1, 2, 3, 4$ to $4, 1, 3, 2$.)

(b) Any k-tuple is a permutation of itself. Indeed, if $(p_1, p_2, \ldots, p_k)$ is any k-tuple, then $(p_1, p_2, \ldots, p_k) = \left(p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(k)}\right)$ if we let σ be the identity map $\operatorname{id} : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$.

The following fact is easy and fundamental:

Proposition 2.13.18. Let $(p_1, p_2, \ldots, p_k)$ be a k-tuple. If $(q_1, q_2, \ldots, q_k)$ is a permutation of $(p_1, p_2, \ldots, p_k)$, then $(p_1, p_2, \ldots, p_k)$ is a permutation of $(q_1, q_2, \ldots, q_k)$.

Proof of Proposition 2.13.18. If you don't insist on formalization, this is obvious: Any rearrangement of the entries of a k-tuple can be undone by another rearrangement (which places the entries back in their old positions). Thus, $(p_1, p_2, \ldots, p_k)$ can be obtained from $(q_1, q_2, \ldots, q_k)$ by rearranging the entries.

Here is a formal proof:

Assume that $(q_1, q_2, \ldots, q_k)$ is a permutation of $(p_1, p_2, \ldots, p_k)$. In other words, the k-tuple $(q_1, q_2, \ldots, q_k)$ has the form $\left(p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(k)}\right)$ for some permutation σ of the set $\{1, 2, \ldots, k\}$ (by Definition 2.13.16). Consider this σ, and denote it by τ. Thus, τ is a permutation of the set $\{1, 2, \ldots, k\}$ and has the property that $(q_1, q_2, \ldots, q_k) = \left(p_{\tau(1)}, p_{\tau(2)}, \ldots, p_{\tau(k)}\right)$.

Now, τ is a permutation of the set $\{1, 2, \ldots, k\}$. In other words, τ is a bijective map $\{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$ (by Definition 2.13.14). So the map τ is bijective, hence invertible. Thus, its inverse τ^{-1} is well-defined and is also invertible[33], hence bijective. So we know that τ^{-1} is a bijective map $\{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$. In other words, τ^{-1} is a permutation of the set $\{1, 2, \ldots, k\}$ (by Definition 2.13.14).

We have $(q_1, q_2, \ldots, q_k) = \left(p_{\tau(1)}, p_{\tau(2)}, \ldots, p_{\tau(k)}\right)$. In other words,

$$q_i = p_{\tau(i)} \qquad \text{for each } i \in \{1, 2, \ldots, k\}. \tag{36}$$

Hence, for each $j \in \{1, 2, \ldots, k\}$, we have

$$\begin{aligned} q_{\tau^{-1}(j)} &= p_{\tau(\tau^{-1}(j))} && \left(\text{by (36), applied to } i = \tau^{-1}(j)\right) \\ &= p_j && \left(\text{since } \tau\left(\tau^{-1}(j)\right) = j\right). \end{aligned}$$

[33] And its inverse is $\left(\tau^{-1}\right)^{-1} = \tau$.

In other words, $\left(q_{\tau^{-1}(1)}, q_{\tau^{-1}(2)}, \ldots, q_{\tau^{-1}(k)}\right) = (p_1, p_2, \ldots, p_k)$. Hence, the k-tuple $(p_1, p_2, \ldots, p_k)$ has the form $\left(q_{\sigma(1)}, q_{\sigma(2)}, \ldots, q_{\sigma(k)}\right)$ for some permutation σ of the set $\{1, 2, \ldots, k\}$ (namely, $\sigma = \tau^{-1}$). In other words, the k-tuple $(p_1, p_2, \ldots, p_k)$ is a permutation of the k-tuple $(q_1, q_2, \ldots, q_k)$ (by Definition 2.13.16). This proves Proposition 2.13.18. □

Now, we can say what we mean when we say that two tuples differ only in the order of their entries:

Definition 2.13.19. We say that two tuples *differ only in the order of their entries* if they are permutations of each other.

The next lemma that we shall use is a basic fact from elementary combinatorics:

Lemma 2.13.20. Let P be a set. Let $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ be two tuples of elements of P. Assume that for each $p \in P$, we have

$$\begin{aligned} &(\text{the number of times } p \text{ appears in } (a_1, a_2, \ldots, a_k)) \\ &= (\text{the number of times } p \text{ appears in } (b_1, b_2, \ldots, b_\ell)) . \end{aligned} \tag{37}$$

Then, the two tuples $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ differ only in the order of their entries (i.e., are permutations of each other). (In other words, we have $k = \ell$, and there exists a permutation σ of the set $\{1, 2, \ldots, \ell\}$ such that $(a_1, a_2, \ldots, a_k) = \left(b_{\sigma(1)}, b_{\sigma(2)}, \ldots, b_{\sigma(\ell)}\right)$.)

Lemma 2.13.20 is an intuitively obvious fact: It says that if two tuples (of any objects – e.g., numbers) have the property that any object occurs as often in the first tuple as it does in the second tuple, then the two tuples differ only in the order of their entries. From the formal point of view, though, it is a statement that needs proof. Let us merely sketch how such a proof can be obtained, without going into the details:

Proof of Lemma 2.13.20 (sketched). We can WLOG assume that the set P is finite (since otherwise, we can replace P by the finite subset $\{a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell\}$, without breaking the assumption that $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ are two tuples of elements of P). Assume this (at least if you don't want to use the Axiom of Choice[34]).

For each $p \in P$, define two sets

$$\begin{aligned} A_p &= \{i \in \{1, 2, \ldots, k\} \mid a_i = p\} ; \\ B_p &= \{j \in \{1, 2, \ldots, \ell\} \mid b_j = p\} . \end{aligned}$$

The equation (37) then says that $|A_p| = |B_p|$ for each $p \in P$. Hence, for each $p \in P$, there exists a bijection $\phi_p : A_p \to B_p$ (because if two sets have the same size, then there exists a bijection between them). Pick such a bijection ϕ_p for each $p \in P$. (This does not require the Axiom of Choice, since P is finite.)

[34] I don't.

Now, define a map $\sigma : \{1,2,\ldots,k\} \to \{1,2,\ldots,\ell\}$ as follows: For each $i \in \{1,2,\ldots,k\}$, set $\sigma(i) = \phi_p(i)$, where $p = a_i$. Thus, for each $p \in P$, the map σ sends each $i \in A_p$ to an element of B_p (because if $i \in A_p$, then $a_i = p$, and thus the definition of σ yields $\sigma(i) = \phi_p(i) \in B_p$.)

It is not hard to see that this map σ is a bijection. (Its inverse map sends each $j \in \{1,2,\ldots,\ell\}$ to $\phi_p^{-1}(j)$, where $p = b_j$.) Thus, we have found a bijection from $\{1,2,\ldots,k\}$ to $\{1,2,\ldots,\ell\}$. This shows that the sets $\{1,2,\ldots,k\}$ and $\{1,2,\ldots,\ell\}$ have the same size; in other words, $k = \ell$. Thus, the bijection σ is actually a bijection from $\{1,2,\ldots,\ell\}$ to $\{1,2,\ldots,\ell\}$. In other words, σ is a permutation of the set $\{1,2,\ldots,\ell\}$.

Finally, it is easy to see that $(a_1,a_2,\ldots,a_k) = \left(b_{\sigma(1)},b_{\sigma(2)},\ldots,b_{\sigma(\ell)}\right)$. (Indeed, let $i \in \{1,2,\ldots,k\}$, and set $p = a_i$; then, the definition of σ yields $\sigma(i) = \phi_p(i) \in B_p$ and therefore $b_{\sigma(i)} = a_i$. Since this holds for each i, we thus conclude that $\left(b_{\sigma(1)},b_{\sigma(2)},\ldots,b_{\sigma(k)}\right) = (a_1,a_2,\ldots,a_k)$. Thus, $(a_1,a_2,\ldots,a_k) = \left(b_{\sigma(1)},b_{\sigma(2)},\ldots,b_{\sigma(k)}\right) = \left(b_{\sigma(1)},b_{\sigma(2)},\ldots,b_{\sigma(\ell)}\right)$ (since $k = \ell$).) Thus, we have found a permutation σ of the set $\{1,2,\ldots,\ell\}$ such that $(a_1,a_2,\ldots,a_k) = \left(b_{\sigma(1)},b_{\sigma(2)},\ldots,b_{\sigma(\ell)}\right)$. In other words, the two tuples $(a_1,a_2,\ldots,a_k)$ and $(b_1,b_2,\ldots,b_\ell)$ are permutations of each other. This proves Lemma 2.13.20. □

Lemma 2.13.20 has a converse that is much simpler:

Lemma 2.13.21. Let P be a set. Let $(a_1,a_2,\ldots,a_k)$ and $(b_1,b_2,\ldots,b_\ell)$ be two tuples of elements of P. Assume that these two tuples $(a_1,a_2,\ldots,a_k)$ and $(b_1,b_2,\ldots,b_\ell)$ differ only in the order of their entries (i.e., are permutations of each other). Then, for each $p \in P$, we have

$$\begin{aligned}&(\text{the number of times } p \text{ appears in } (a_1,a_2,\ldots,a_k))\\ &= (\text{the number of times } p \text{ appears in } (b_1,b_2,\ldots,b_\ell)).\end{aligned}$$

We leave the proof of this lemma to the reader.

2.13.5. p-valuations

Now, let us come back to number theory. We first claim that a nonzero integer n can only be divisible by finitely many powers of a given prime p. More precisely:

Lemma 2.13.22. Let p be a prime. Let n be a nonzero integer. Then, there exists a largest $m \in \mathbb{N}$ such that $p^m \mid n$.

The proof of this lemma will rely on a simple inequality, which we leave as an exercise:

Exercise 2.13.4. Let p be an integer such that $p > 1$. Prove that $p^k > k$ for each $k \in \mathbb{N}$.

Proof of Lemma 2.13.22. We know that p is a prime. Thus, p is an integer and $p > 1$ (by the definition of a "prime"). This is all we shall need from our assumption that p is prime.

Let W be the set of all $m \in \mathbb{N}$ satisfying $p^m \mid n$. Then, W is a set of integers. Moreover, 0 is an $m \in \mathbb{N}$ satisfying $p^m \mid n$ (since $p^0 = 1 \mid n$); in other words, $0 \in W$ (by the definition of W). Hence, the set W is nonempty.

Let $u = |n|$. Thus, $u \in \mathbb{N}$.

Exercise 2.13.4 yields that $p^k > k$ for each $k \in \mathbb{N}$. Thus, each $g \in W$ satisfies $g \in \{0, 1, \ldots, u-1\}$ [35]. In other words, $W \subseteq \{0, 1, \ldots, u-1\}$. Hence, the set W is finite (since the set $\{0, 1, \ldots, u-1\}$ is finite). Thus, W is a finite nonempty set of integers. Therefore, the set W has a largest element. In view of how W was defined, this can be restated as follows: There exists a largest $m \in \mathbb{N}$ such that $p^m \mid n$. This proves Lemma 2.13.22. □

Definition 2.13.23. Let p be a prime.

(a) Let n be a nonzero integer. Then, $v_p(n)$ shall denote the largest $m \in \mathbb{N}$ such that $p^m \mid n$. This is well-defined (by Lemma 2.13.22). This nonnegative integer $v_p(n)$ will be called the *p-valuation* (or the *p-adic valuation*) of n.

(b) We extend this definition of $v_p(n)$ to the case of $n = 0$ as follows: Set $v_p(0) = \infty$, where ∞ is a new symbol. This symbol ∞ is supposed to model "positive infinity"; in particular, we take it to satisfy the following rules:

- We have $k + \infty = \infty + k = \infty$ for all integers k.
- We have $\infty + \infty = \infty$.
- Each integer k satisfies $k < \infty$ and $\infty > k$ (and thus $k \leq \infty$ and $\infty \geq k$).
- No integer k satisfies $k \geq \infty$ or $\infty \leq k$ (or $k > \infty$ or $\infty < k$).
- If S is a nonempty set of integers, then $\min(S \cup \{\infty\}) = \min S$ (provided that $\min S$ exists).
- If S is any set of integers, then $\max(S \cup \{\infty\}) = \infty$.

(Note, however, that ∞ is not supposed to be a "first class citizen" of the number system. In particular, $\infty - \infty$ is not defined. More generally, $k - \infty$ is never defined, whatever k is. Indeed, any definition of $k - \infty$ would break some of the familiar rules of arithmetic. The only operations that we shall subject ∞ to are addition, minimum and maximum.)

[35] *Proof.* Let $g \in W$. Thus, g is an $m \in \mathbb{N}$ satisfying $p^m \mid n$ (by the definition of W). In other words, $g \in \mathbb{N}$ and $p^g \mid n$. Also, $n \neq 0$ (since n is nonzero). Hence, Proposition 2.2.3 **(b)** (applied to $a = p^g$ and $b = n$) yields $|p^g| \leq |n| = u$. But p is positive (since $p > 1 > 0$); thus, p^g is positive. Hence, $|p^g| = p^g$. Thus, $p^g = |p^g| \leq u$. But recall that $p^k > k$ for each $k \in \mathbb{N}$. Applying this to $k = g$, we find $p^g > g$. Hence, $g < p^g \leq u$, so that $g \in \{0, 1, \ldots, u-1\}$ (since $g \in \mathbb{N}$). Qed.

Note that the rules for the symbol ∞ yield that

$$k + \infty = \infty + k = \max\{k, \infty\} = \infty$$

and

$$\min\{k, \infty\} = k$$

for each $k \in \mathbb{Z} \cup \{\infty\}$. It is not hard to see that basic properties of inequalities (such as "if $a \leq b$ and $b \leq c$, then $a \leq c$") and of addition (such as "$(a+b)+c = a+(b+c)$") and of the interplay between inequalities and addition (such as "if $a \leq b$, then $a+c \leq b+c$") are still valid in $\mathbb{Z} \cup \{\infty\}$ (that is, they still hold if we plug ∞ for one or more of the variables). However, of course, we cannot "cancel" ∞ from equalities (i.e., we cannot cancel ∞ from $a+\infty = b+\infty$ to obtain $a = b$) or inequalities.

Example 2.13.24. **(a)** We have $v_5(50) = 2$. Indeed, 2 is the largest $m \in \mathbb{N}$ such that $5^m \mid 50$ (because $5^2 = 25 \mid 50$ but $5^3 = 125 \nmid 50$).

(b) We have $v_5(51) = 0$. Indeed, 0 is the largest $m \in \mathbb{N}$ such that $5^m \mid 51$ (because $5^0 = 1 \mid 51$ but $5^1 = 5 \nmid 51$).

(c) We have $v_5(55) = 1$. Indeed, 1 is the largest $m \in \mathbb{N}$ such that $5^m \mid 55$ (because $5^1 = 5 \mid 55$ but $5^2 = 25 \nmid 55$).

(d) We have $v_5(0) = \infty$ (by Definition 2.13.23 **(b)**).

Definition 2.13.23 **(a)** can be restated in the following more intuitive way: Given a prime p and a nonzero integer n, we let $v_p(n)$ be the number of times we can divide n by p without leaving $\mathbb{Z}$. Definition 2.13.23 **(b)** is consistent with this picture, because we can clearly divide 0 by p infinitely often without leaving $\mathbb{Z}$. From this point of view, the following lemma should be obvious:

Lemma 2.13.25. *Let p be a prime. Let $i \in \mathbb{N}$. Let $n \in \mathbb{Z}$. Then, $p^i \mid n$ if and only if $v_p(n) \geq i$.*

Proof of Lemma 2.13.25. First, let us notice that $p^i \mid 0$. Also, Definition 2.13.23 **(b)** yields $v_p(0) = \infty \geq i$ (according to our rules for the symbol ∞). Hence, both statements $\left(p^i \mid 0\right)$ and $\left(v_p(0) \geq i\right)$ hold. Thus, $p^i \mid 0$ if and only if $v_p(0) \geq i$. In other words, Lemma 2.13.25 holds if $n = 0$. Thus, for the rest of this proof, we WLOG assume that $n \neq 0$. Hence, n is nonzero. Thus, $v_p(n)$ is the largest $m \in \mathbb{N}$ such that $p^m \mid n$ (by Definition 2.13.23 **(a)**). Hence, $v_p(n)$ itself is an $m \in \mathbb{N}$ such that $p^m \mid n$. In other words, $v_p(n) \in \mathbb{N}$ and $p^{v_p(n)} \mid n$.

We must prove that $p^i \mid n$ if and only if $v_p(n) \geq i$. Let us prove the "$\Longrightarrow$" and "$\Longleftarrow$" directions of this "if and only if" statement separately:

$\Longrightarrow$: Assume that $p^i \mid n$. We must prove that $v_p(n) \geq i$.

The integer i is an $m \in \mathbb{N}$ such that $p^m \mid n$ (since $p^i \mid n$). But $v_p(n)$ is the **largest** such m (by Definition 2.13.23 **(a)**). Hence, $v_p(n) \geq i$. This proves the "$\Longrightarrow$" direction of Lemma 2.13.25.

$\Longleftarrow$: Assume that $v_p(n) \geq i$. We must prove that $p^i \mid n$.

We have $v_p(n) \geq i$, thus $i \leq v_p(n)$. Hence, Exercise 2.2.4 (applied to p, i and $v_p(n)$ instead of n, a and b) yields $p^i \mid p^{v_p(n)}$. Thus, $p^i \mid p^{v_p(n)} \mid n$.

Hence, we have proven $p^i \mid n$. This proves the "$\Longleftarrow$" direction of Lemma 2.13.25. □

Corollary 2.13.26. Let p be a prime. Let $n \in \mathbb{Z}$. Then, $v_p(n) = 0$ if and only if $p \nmid n$.

Proof of Corollary 2.13.26. $\Longrightarrow$: Assume that $v_p(n) = 0$. We must prove that $p \nmid n$.

We don't have $v_p(n) \geq 1$ (since $v_p(n) = 0 < 1$). But Lemma 2.13.25 (applied to $i = 1$) shows that $p^1 \mid n$ if and only if $v_p(n) \geq 1$. Hence, we don't have $p^1 \mid n$ (since we don't have $v_p(n) \geq 1$). In other words, we have $p^1 \nmid n$. In other words, $p \nmid n$ (since $p = p^1$). This proves the "$\Longrightarrow$" direction of Corollary 2.13.26.

$\Longleftarrow$: Assume that $p \nmid n$. We must prove that $v_p(n) = 0$.

We don't have $p \mid n$ (since $p \nmid n$). In other words, we don't have $p^1 \mid n$ (since $p^1 = p$). But Lemma 2.13.25 (applied to $i = 1$) shows that $p^1 \mid n$ if and only if $v_p(n) \geq 1$. Hence, we don't have $v_p(n) \geq 1$ (since we don't have $p^1 \mid n$). In other words, $v_p(n) < 1$.

If we had $n = 0$, then we would have $p \mid 0 = n$, which would contradict $p \nmid n$. Hence, we don't have $n = 0$. Thus, p is nonzero. Hence, Definition 2.13.23 **(a)** shows that $v_p(n) \in \mathbb{N}$. In light of this, we can conclude $v_p(n) = 0$ from $v_p(n) < 1$. This proves the "$\Longleftarrow$" direction of Corollary 2.13.26. □

Here is another property of p-valuations that is useful in their study:

Lemma 2.13.27. Let p be a prime. Let $n \in \mathbb{Z}$ be nonzero. Then:

(a) There exists a nonzero integer u such that $u \perp p$ and $n = up^{v_p(n)}$.

(b) If $i \in \mathbb{N}$ and $w \in \mathbb{Z}$ are such that $w \perp p$ and $n = wp^i$, then $v_p(n) = i$.

Before we prove this formally, let us show the idea behind this lemma. Recall that, given a prime p and a nonzero integer n, the number $v_p(n)$ counts how often we can divide n by p without leaving $\mathbb{Z}$. What happens after we have divided n by p this many times? We get a number u that is still an integer, but is no longer divisible by p, and thus must be coprime to p (by Proposition 2.13.5). This is what Lemma 2.13.27 **(a)** says. Lemma 2.13.27 **(b)** is a converse statement: It says that if we divide n by p some number of times (say, i times) and obtain an integer coprime to p, then i must be $v_p(n)$.

Proof of Lemma 2.13.27. Definition 2.13.23 **(a)** shows that $v_p(n)$ is the largest $m \in \mathbb{N}$ such that $p^m \mid n$. Hence, $v_p(n)$ itself is an $m \in \mathbb{N}$ such that $p^m \mid n$. In other words, $v_p(n) \in \mathbb{N}$ and $p^{v_p(n)} \mid n$.

Thus, in particular, $p^{v_p(n)} \mid n$. In other words, there exists an integer c such that $n = p^{v_p(n)}c$. Consider this c. We have $n = p^{v_p(n)}c = cp^{v_p(n)}$.

Assume (for the sake of contradiction) that $p \mid c$. Thus, there exists an integer d such that $c = pd$. Consider this d. Now,

$$n = p^{v_p(n)} \underbrace{c}_{=pd} = \underbrace{p^{v_p(n)} p}_{=p^{v_p(n)+1}} d = p^{v_p(n)+1} d.$$

Hence, $p^{v_p(n)+1} \mid n$ (since d is an integer). In other words, $v_p(n) + 1$ is an $m \in \mathbb{N}$ such that $p^m \mid n$. But we know that $v_p(n)$ is the **largest** such m (by Definition 2.13.23 **(a)**). Hence, we conclude that $v_p(n) \geq v_p(n) + 1$. But this is clearly absurd. This contradiction shows that our assumption (that $p \mid c$) was wrong. Hence, we do not have $p \mid c$.

But Proposition 2.13.5 (applied to $a = c$) shows that either $p \mid c$ or $p \perp c$. Hence, $p \perp c$ (since we do not have $p \mid c$). In other words, $c \perp p$ (because of Proposition 2.10.4).

If we had $c = 0$, then we would have $n = p^{v_p(n)} \underbrace{c}_{=0} = 0$, which would contradict the fact that n is nonzero. Hence, we cannot have $c = 0$. Thus, c is nonzero.

Now, we know that c is a nonzero integer satisfying $c \perp p$ and $n = cp^{v_p(n)}$. Hence, there exists a nonzero integer u such that $u \perp p$ and $n = up^{v_p(n)}$ (namely, $u = c$). This proves Lemma 2.13.27 **(a)**.

(b) Let $i \in \mathbb{N}$ and $w \in \mathbb{Z}$ be such that $w \perp p$ and $n = wp^i$. We must prove that $v_p(n) = i$.

From $w \perp p$, we obtain $p \perp w$ (by Proposition 2.10.4). In other words, $\gcd(p, w) = 1$.

We have $n = wp^i = p^i w$ and thus $p^i \mid n$ (since w is an integer). But Lemma 2.13.25 yields that $p^i \mid n$ if and only if $v_p(n) \geq i$. Hence, we have $v_p(n) \geq i$ (since we have $p^i \mid n$).

Now, we shall prove that $v_p(n) \leq i$. Indeed, assume the contrary. Thus, $v_p(n) > i$, so that $v_p(n) \geq i + 1$ (since $v_p(n)$ and i are integers). But Lemma 2.13.25 (applied to $i + 1$ instead of i) shows that $p^{i+1} \mid n$ if and only if $v_p(n) \geq i + 1$. Thus, we have $p^{i+1} \mid n$ (since we have $v_p(n) \geq i + 1$). In other words, $pp^i \mid wp^i$ (since $p^{i+1} = pp^i$ and $n = wp^i$). But p is a prime; thus, $p > 1 > 0$ and therefore $p \neq 0$. Hence, $p^i \neq 0$. Thus, Exercise 2.2.3 (applied to p, w and p^i instead of a, b and c) shows that $p \mid w$ holds if and only if $pp^i \mid wp^i$. Hence, $p \mid w$ holds (since $pp^i \mid wp^i$ holds). Thus, Proposition 2.9.7 **(i)** (applied to p and w instead of a and b) yields $\gcd(p, w) = |p| = p$ (since $p > 0$). Comparing this with $\gcd(p, w) = 1$, we find $p = 1$. This contradicts $p > 1$.

This contradiction shows that our assumption was false. Hence, $v_p(n) \leq i$ is proven. Combining this with $v_p(n) \geq i$, we obtain $v_p(n) = i$. This proves Lemma 2.13.27 **(b)**. □

The next property of p-adic valuations is crucial, as it reveals how they can be computed and bounded:

Theorem 2.13.28. Let p be a prime.

(a) We have $v_p(ab) = v_p(a) + v_p(b)$ for any two integers a and b.

(b) We have $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$ for any two integers a and b.

(c) We have $v_p(1) = 0$.

(d) We have $v_p(q) = \begin{cases} 1, & \text{if } q = p; \\ 0, & \text{if } q \neq p \end{cases}$ for any prime q.

Note that Theorem 2.13.28 **(a)** gives a formula for $v_p(ab)$ in terms of $v_p(a)$ and $v_p(b)$, but there is no such formula for $v_p(a+b)$ (since $v_p(a)$ and $v_p(b)$ do not uniquely determine $v_p(a+b)$). Thus, Theorem 2.13.28 **(b)** only gives a bound.

Proof of Theorem 2.13.28. **(a)** Let a and b be two integers. We must prove that $v_p(ab) = v_p(a) + v_p(b)$.

If $a = 0$, then this is true[36]. Thus, for the rest of the proof of Theorem 2.13.28 **(a)**, we WLOG assume that $a \neq 0$. For similar reasons, we WLOG assume that $b \neq 0$.

The integer a is nonzero (since $a \neq 0$). Thus, Lemma 2.13.27 **(a)** (applied to $n = a$) shows that there exists a nonzero integer u such that $u \perp p$ and $a = up^{v_p(a)}$. Consider this u, and denote it by x. Thus, x is a nonzero integer such that $x \perp p$ and $a = xp^{v_p(a)}$.

The integer b is nonzero (since $b \neq 0$). Thus, Lemma 2.13.27 **(a)** (applied to $n = b$) shows that there exists a nonzero integer u such that $u \perp p$ and $b = up^{v_p(b)}$. Consider this u, and denote it by y. Thus, y is a nonzero integer such that $y \perp p$ and $b = yp^{v_p(b)}$.

We have $x \perp p$ and $y \perp p$. Thus, Theorem 2.10.9 (applied to x, y and p instead of a, b and c) shows that $xy \perp p$.

The integer ab is nonzero (since $a \neq 0$ and $b \neq 0$).

Furthermore, multiplying the equalities $a = xp^{v_p(a)}$ and $b = yp^{v_p(b)}$, we obtain

$$ab = \left(xp^{v_p(a)}\right)\left(yp^{v_p(b)}\right) = (xy)\underbrace{\left(p^{v_p(a)}p^{v_p(b)}\right)}_{=p^{v_p(a)+v_p(b)}} = (xy)\,p^{v_p(a)+v_p(b)}.$$

Thus, Lemma 2.13.27 **(b)** (applied to $n = ab$, $i = v_p(a) + v_p(b)$ and $w = xy$) shows that $v_p(ab) = v_p(a) + v_p(b)$ (since $v_p(a) + v_p(b) \in \mathbb{N}$ and $xy \in \mathbb{Z}$ and $xy \perp p$). This proves Theorem 2.13.28 **(a)**.

(b) Let a and b be two integers. We must prove that $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$.

[36] *Proof.* Assume that $a = 0$. Then, $\underbrace{a}_{=0} b = 0$ and thus $v_p(ab) = v_p(0) = \infty$ (by Definition 2.13.23 **(b)**). Also, from $a = 0$, we obtain $v_p(a) = v_p(0) = \infty$. Hence, $\underbrace{v_p(a)}_{=\infty} + v_p(b) = \infty + v_p(b) = \infty$ (since $\infty + k = \infty$ for each $k \in \mathbb{Z} \cup \{\infty\}$). Comparing this with $v_p(ab) = \infty$, we obtain $v_p(ab) = v_p(a) + v_p(b)$. This is exactly what we wanted to prove.

If $a = 0$, then this is true[37]. Thus, for the rest of the proof of Theorem 2.13.28 **(b)**, we WLOG assume that $a \neq 0$. For similar reasons, we WLOG assume that $b \neq 0$.

The integer a is nonzero (since $a \neq 0$). Thus, $v_p(a) \in \mathbb{N}$ (by Definition 2.13.23 **(a)**). Similarly, $v_p(b) \in \mathbb{N}$.

Let $m = \min\{v_p(a), v_p(b)\}$. Thus, $m \in \mathbb{N}$ (since $v_p(a) \in \mathbb{N}$ and $v_p(b) \in \mathbb{N}$).

We have $m = \min\{v_p(a), v_p(b)\} \leq v_p(a)$; in other words, $v_p(a) \geq m$. But Lemma 2.13.25 (applied to $n = a$ and $i = m$) shows that $p^m \mid a$ if and only if $v_p(a) \geq m$. Hence, we have $p^m \mid a$ (since $v_p(a) \geq m$). In other words, $a \equiv 0 \mod p^m$. Similarly, $b \equiv 0 \mod p^m$. Adding these two congruences together, we obtain $a + b \equiv 0 + 0 = 0 \mod p^m$. In other words, $p^m \mid a + b$.

But Lemma 2.13.25 (applied to $n = a + b$ and $i = m$) shows that $p^m \mid a + b$ if and only if $v_p(a+b) \geq m$. Hence, we have $v_p(a+b) \geq m$ (since $p^m \mid a + b$). Thus, $v_p(a+b) \geq m = \min\{v_p(a), v_p(b)\}$. This proves Theorem 2.13.28 **(b)**.

(c) Exercise 2.10.1 **(a)** (applied to $a = p$) yields $1 \perp p$. Also, $1 = 1 \cdot p^0$. Thus, Lemma 2.13.27 **(b)** (applied to $n = 1$, $i = 0$ and $w = 1$) yields $v_p(1) = 0$. This proves Theorem 2.13.28 **(c)**.

(d) Let q be a prime. We must prove that $v_p(q) = \begin{cases} 1, & \text{if } q = p; \\ 0, & \text{if } q \neq p \end{cases}$.

We are in one of the following two cases:

Case 1: We have $q = p$.

Case 2: We have $q \neq p$.

Let us first consider Case 1. In this case, we have $q = p$. But Exercise 2.10.1 **(a)** (applied to $a = p$) yields $1 \perp p$. Also, $p = 1 \cdot p^1$. Thus, Lemma 2.13.27 **(b)** (applied to $n = p$, $i = 1$ and $w = 1$) yields $v_p(p) = 1$. From $q = p$, we obtain $v_p(q) = v_p(p) = 1$. Comparing this with

$$\begin{cases} 1, & \text{if } q = p; \\ 0, & \text{if } q \neq p \end{cases} = 1 \qquad (\text{since } q = p),$$

we obtain $v_p(q) = \begin{cases} 1, & \text{if } q = p; \\ 0, & \text{if } q \neq p \end{cases}$. Hence, Theorem 2.13.28 **(d)** is proven in Case 1.

Let us now consider Case 2. In this case, we have $q \neq p$. Thus, the primes q and p are distinct. Hence, Exercise 2.13.1 (applied to q and p instead of p and q) yields $q \perp p$. Also, $q = q \cdot p^0$ (since $p^0 = 1$). Thus, Lemma 2.13.27 **(b)** (applied to $n = q$, $i = 0$ and $w = q$) yields $v_p(q) = 0$. Comparing this with

$$\begin{cases} 1, & \text{if } q = p; \\ 0, & \text{if } q \neq p \end{cases} = 0 \qquad (\text{since } q \neq p),$$

[37] *Proof.* Assume that $a = 0$. Then, $v_p\left(\underbrace{a}_{=0} + b\right) = v_p(b) \geq \min\{v_p(a), v_p(b)\}$ (since any element of a set is $\geq$ to the minimum of this set). This is exactly what we wanted to prove.

we obtain $v_p(q) = \begin{cases} 1, & \text{if } q = p; \\ 0, & \text{if } q \neq p \end{cases}$. Hence, Theorem 2.13.28 **(d)** is proven in Case 2.

We have now proven Theorem 2.13.28 **(d)** in each of the two Cases 1 and 2. Thus, Theorem 2.13.28 **(d)** is always proven. □

Corollary 2.13.29. Let p be a prime. Let $a_1, a_2, \ldots, a_k$ be k integers. Then, $v_p(a_1 a_2 \cdots a_k) = v_p(a_1) + v_p(a_2) + \cdots + v_p(a_k)$.

Proof of Corollary 2.13.29. This follows straightforwardly by induction on k, using Theorem 2.13.28 **(a)** (as well as Theorem 2.13.28 **(c)** for the induction base). We leave the details to the reader, who has seen this sort of proof several times already. □

Exercise 2.13.5. Let p be a prime. Let $n \in \mathbb{Z}$. Prove that $v_p(|n|) = v_p(n)$.

Exercise 2.13.6. Let p be a prime. Let $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. Prove that $v_p\left(a^k\right) = kv_p(a)$.

Exercise 2.13.7. Let $p_1, p_2, \ldots, p_u$ be finitely many distinct primes. Let $a_1, a_2, \ldots, a_u$ be nonnegative integers.

(a) Prove that $v_{p_i}\left(p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}\right) = a_i$ for each $i \in \{1, 2, \ldots, u\}$.

(b) Prove that $v_p\left(p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}\right) = 0$ for each prime p satisfying $p \notin \{p_1, p_2, \ldots, p_u\}$.

2.13.6. Prime factorization II

Proposition 2.13.30. Let n be a positive integer. Let $(a_1, a_2, \ldots, a_k)$ be a prime factorization of n. Let p be a prime. Then,

$$\begin{aligned}
&(\text{the number of times } p \text{ appears in the tuple } (a_1, a_2, \ldots, a_k)) \\
&= (\text{the number of } i \in \{1, 2, \ldots, k\} \text{ such that } a_i = p) \\
&= v_p(n).
\end{aligned}$$

Proof of Proposition 2.13.30. We have assumed that $(a_1, a_2, \ldots, a_k)$ is a prime factorization of n. Thus, $a_1, a_2, \ldots, a_k$ are primes satisfying $n = a_1 a_2 \cdots a_k$. Hence, for each $i \in \{1, 2, \ldots, k\}$, the integer a_i is prime and thus satisfies

$$v_p(a_i) = \begin{cases} 1, & \text{if } a_i = p; \\ 0, & \text{if } a_i \neq p \end{cases} \tag{38}$$

(by Theorem 2.13.28 **(d)**, applied to $q = a_i$).

From $n = a_1 a_2 \cdots a_k$, we obtain

$$\begin{aligned}
v_p(n) &= v_p(a_1 a_2 \cdots a_k)\\
&= v_p(a_1) + v_p(a_2) + \cdots + v_p(a_k) \qquad (\text{by Corollary 2.13.29})\\
&= \underbrace{\sum_{i=1}^{k}}_{=\sum_{i\in\{1,2,\ldots,k\}}} \underbrace{v_p(a_i)}_{\substack{=\begin{cases}1, & \text{if } a_i = p;\\ 0, & \text{if } a_i \neq p\end{cases}\\ \text{(by (38))}}} = \sum_{i\in\{1,2,\ldots,k\}} \begin{cases}1, & \text{if } a_i = p;\\ 0, & \text{if } a_i \neq p\end{cases}\\
&= \sum_{\substack{i\in\{1,2,\ldots,k\};\\ a_i = p}} \underbrace{\begin{cases}1, & \text{if } a_i = p;\\ 0, & \text{if } a_i \neq p\end{cases}}_{\substack{=1\\ (\text{since } a_i = p)}} + \sum_{\substack{i\in\{1,2,\ldots,k\};\\ a_i \neq p}} \underbrace{\begin{cases}1, & \text{if } a_i = p;\\ 0, & \text{if } a_i \neq p\end{cases}}_{\substack{=0\\ (\text{since } a_i \neq p)}}\\
&\qquad \left(\begin{array}{c}\text{since each } i \in \{1,2,\ldots,k\} \text{ satisfies either } a_i = p \text{ or } a_i \neq p\\ \text{(but not both)}\end{array}\right)\\
&= \sum_{\substack{i\in\{1,2,\ldots,k\};\\ a_i = p}} 1 + \underbrace{\sum_{\substack{i\in\{1,2,\ldots,k\};\\ a_i \neq p}} 0}_{=0} = \sum_{\substack{i\in\{1,2,\ldots,k\};\\ a_i = p}} 1\\
&= (\text{the number of } i \in \{1,2,\ldots,k\} \text{ such that } a_i = p) \cdot 1\\
&= (\text{the number of } i \in \{1,2,\ldots,k\} \text{ such that } a_i = p)\\
&= (\text{the number of times } p \text{ appears in } (a_1, a_2, \ldots, a_k)).
\end{aligned}$$

This proves Proposition 2.13.30. □

We are finally ready to prove the so-called *Fundamental Theorem of Arithmetic*:

Theorem 2.13.31. Let n be a positive integer.

(a) There exists a prime factorization of n.

(b) Any two such factorizations differ only in the order of their entries (i.e., are permutations of each other).

Proof of Theorem 2.13.31. **(a)** Proposition 2.13.10 shows that n can be written as a product of finitely many primes. In other words, there exist finitely many primes $p_1, p_2, \ldots, p_k$ such that $n = p_1 p_2 \cdots p_k$. Consider these primes. Thus, $(p_1, p_2, \ldots, p_k)$ is a prime factorization of n (by the definition of "prime factorization"). Hence, there exists a prime factorization of n. This proves Theorem 2.13.31 **(a)**.

(b) Let $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ be two prime factorizations of n. We must prove that $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ differ only in the order of their entries (i.e., are permutations of each other).

Let P be the set of all primes. Note that $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ are prime factorizations of n. Hence, $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ are tuples of primes, i.e., tuples of elements of P.

Let $p \in P$. Thus, p is a prime (by the definition of P). Hence, Proposition 2.13.30 shows that

$$\begin{aligned}
&(\text{the number of times } p \text{ appears in the tuple } (a_1, a_2, \ldots, a_k)) \\
&= (\text{the number of } i \in \{1, 2, \ldots, k\} \text{ such that } a_i = p) \\
&= v_p(n).
\end{aligned}$$

Similarly,

$$\begin{aligned}
&(\text{the number of times } p \text{ appears in the tuple } (b_1, b_2, \ldots, b_\ell)) \\
&= (\text{the number of } i \in \{1, 2, \ldots, \ell\} \text{ such that } b_i = p) \\
&= v_p(n).
\end{aligned}$$

Comparing these two equalities, we conclude that

$$\begin{aligned}
&(\text{the number of times } p \text{ appears in } (a_1, a_2, \ldots, a_k)) \\
&= (\text{the number of times } p \text{ appears in } (b_1, b_2, \ldots, b_\ell)). \qquad (39)
\end{aligned}$$

Now, forget that we fixed p. We thus have proven (39) for each $p \in P$. Hence, Lemma 2.13.20 shows that the tuples $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ differ only in the order of their entries (i.e., are permutations of each other). This completes our proof of Theorem 2.13.31 **(b)**. □

2.13.7. The canonical factorization

You have seen finite products such as[38]

$$\prod_{i \in \{1,2,3,4,5\}} i = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5! = 120 \qquad \text{and}$$

$$\prod_{i \in \{3,5,7\}} \left(i^2 + 1\right) = \left(3^2 + 1\right) \cdot \left(5^2 + 1\right) \cdot \left(7^2 + 1\right) = 13000.$$

Sometimes, infinite products (i.e., products ranging over infinite sets) also make sense. Many examples of well-defined infinite products arise from analysis and have to do with convergence. Here, we are doing algebra and thus shall only consider a very elementary, non-analytic meaning of convergence. Namely, we will consider infinite products that have only finitely many factors different from 1. For example, the product $2 \cdot 7 \cdot 4 \cdot \underbrace{1 \cdot 1 \cdot 1 \cdot 1 \cdot \cdots}_{\text{infinitely many 1's}}$ is of such form. It is easy to give

[38] Here and in the following, $n!$ denotes the product $1 \cdot 2 \cdot \cdots \cdot n$ whenever $n \in \mathbb{N}$. Thus, in particular,

$$0! = (\text{empty product}) = 1, \qquad 1! = 1, \qquad 2! = 1 \cdot 2 = 2,$$
$$3! = 1 \cdot 2 \cdot 3 = 6, \qquad 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24, \qquad 5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120.$$

a meaning to such products: Just throw away all the 1's (since multiplying by 1 does not change a number) and take the product of the remaining (finitely many) numbers. So, for example, our product $2 \cdot 7 \cdot 4 \cdot \underbrace{1 \cdot 1 \cdot 1 \cdot 1 \cdot \cdots}_{\text{infinitely many 1's}}$ should evaluate to $2 \cdot 7 \cdot 4 = 56$.

This is indeed a meaningful and useful definition. For example, the set of all prime numbers is infinite (by Theorem 2.13.43 below), but nevertheless, for each nonzero integer n, the product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ (where the "$\prod\limits_{p \text{ prime}}$" symbol means a product ranging over all primes p) is well-defined due to having only finitely many factors different from 1:

Lemma 2.13.32. Let n be a nonzero integer.

(a) We have $v_p(n) = 0$ for every prime $p > |n|$. (Note that "for every prime $p > |n|$" is shorthand for "for every prime p satisfying $p > |n|$".)

(b) The product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ has only finitely many factors different from 1.

(Here and in the following, the "$\prod\limits_{p \text{ prime}}$" symbol means a product ranging over all primes p.)

Proof of Lemma 2.13.32. **(a)** Let p be a prime such that $p > |n|$. We must prove that $v_p(n) = 0$.

We have $p > 1$ (since p is prime); thus, $p > 1 > 0$ and therefore $|p| = p > |n|$.

We have $n \neq 0$ (since n is nonzero). Thus, if we had $p \mid n$, then we would have $|p| \leq |n|$ (by Proposition 2.2.3 **(b)**, applied to $a = p$ and $b = n$), which would contradict $|p| > |n|$. Thus, we cannot have $p \mid n$. In other words, we have $p \nmid n$.

But Corollary 2.13.26 yields that $v_p(n) = 0$ if and only if $p \nmid n$. Hence, $v_p(n) = 0$ (since $p \nmid n$). This proves Lemma 2.13.32 **(a)**.

(b) For every prime $p > |n|$, we have $v_p(n) = 0$ (by Lemma 2.13.32 **(a)**) and thus $p^{v_p(n)} = p^0 = 1$. Thus, all but finitely many primes p satisfy $p^{v_p(n)} = 1$ (since all but finitely many primes p satisfy $p > |n|$). Therefore, all but finitely many factors of the product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ are 1. In other words, the product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ has only finitely many factors different from 1. This proves Lemma 2.13.32 **(b)**. □

Corollary 2.13.33. Let n be a positive integer. Then,

$$n = \prod_{p \text{ prime}} p^{v_p(n)}.$$

Here, the infinite product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ is well-defined (according to Lemma 2.13.32 **(b)**).

This expression $n = \prod\limits_{p \text{ prime}} p^{v_p(n)}$ is called the *canonical factorization* of n.

Proof of Corollary 2.13.33. Theorem 2.13.31 **(a)** shows that there exists a prime factorization of n. Consider such a factorization, and denote it by $(a_1, a_2, \ldots, a_k)$. Thus, $(a_1, a_2, \ldots, a_k)$ is a prime factorization of n; in other words, $a_1, a_2, \ldots, a_k$ are primes satisfying $n = a_1 a_2 \cdots a_k$. For each prime p, we have

$$(\text{the number of } i \in \{1, 2, \ldots, k\} \text{ such that } a_i = p) = v_p(n) \tag{40}$$

(by Proposition 2.13.30). Now,

$$\begin{aligned}
n &= a_1 a_2 \cdots a_k = \prod_{i \in \{1,2,\ldots,k\}} a_i \\
&= \prod_{p \text{ prime}} \prod_{\substack{i \in \{1,2,\ldots,k\};\\ a_i = p}} \underbrace{a_i}_{=p} \\
&\qquad \left(\begin{array}{c}\text{here, we have split our product into smaller}\\ \text{products, according to the value of } a_i;\\ \text{this is allowed, since each } a_i \text{ is a prime}\end{array}\right) \\
&= \prod_{p \text{ prime}} \underbrace{\prod_{\substack{i \in \{1,2,\ldots,k\};\\ a_i = p}} p}_{= p^{(\text{the number of } i \in \{1,2,\ldots,k\} \text{ such that } a_i = p)}} \\
&= \prod_{p \text{ prime}} \underbrace{p^{(\text{the number of } i \in \{1,2,\ldots,k\} \text{ such that } a_i = p)}}_{\substack{= p^{v_p(n)}\\ (\text{by } (40))}} \\
&= \prod_{p \text{ prime}} p^{v_p(n)}.
\end{aligned}$$

This proves Corollary 2.13.33. □

The next exercise says that a nonnegative integer n is uniquely determined by the family $(v_p(n))_{p \text{ prime}}$ of its p-valuations for all primes p:

Exercise 2.13.8. Let n and m be two nonnegative integers. Assume that

$$v_p(n) = v_p(m) \qquad \text{for every prime } p. \tag{41}$$

Prove that $n = m$.

Corollary 2.13.34. Let n be a nonzero integer. Then,

$$|n| = \prod_{p \text{ prime}} p^{v_p(n)}.$$

Here, the infinite product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ is well-defined (according to Lemma 2.13.32 **(b)**).

Proof of Corollary 2.13.34. The integer $|n|$ is positive (since n is nonzero). Hence, Corollary 2.13.33 (applied to $|n|$ instead of n) yields

$$|n| = \prod_{p \text{ prime}} \underbrace{p^{v_p(|n|)}}_{\substack{=p^{v_p(n)} \\ \text{(since Exercise 2.13.5} \\ \text{yields } v_p(|n|)=v_p(n))}} = \prod_{p \text{ prime}} p^{v_p(n)}.$$

This proves Corollary 2.13.34. □

We can furthermore use p-adic valuations to check divisibility of integers:

Proposition 2.13.35. Let n and m be integers. Then, $n \mid m$ if and only if each prime p satisfies $v_p(n) \leq v_p(m)$.

Proof of Proposition 2.13.35. If $m = 0$, then Proposition 2.13.35 is true[39]. Hence, for the rest of this proof, we WLOG assume that $m \neq 0$. Therefore, m is nonzero. Hence, $v_p(m) \in \mathbb{N}$ (by Definition 2.13.23 **(a)**), so that $v_p(m) < \infty$.

If $n = 0$, then Proposition 2.13.35 is true[40]. Hence, for the rest of this proof, we WLOG assume that $n \neq 0$. Therefore, n is nonzero.

The statement of Proposition 2.13.35 does not change if we replace n and m by $|n|$ and $|m|$, respectively[41]. Hence, we can WLOG assume that n and m are nonnegative. Assume this. Then, $n \geq 0$, so that $n > 0$ (since n is nonzero). Hence, n is a positive integer. Thus, Corollary 2.13.33 yields

$$n = \prod_{p \text{ prime}} p^{v_p(n)}. \tag{42}$$

[39] *Proof.* Assume that $m = 0$. Thus, each prime p satisfies $v_p\left(\underbrace{m}_{=0}\right) = v_p(0) = \infty$ (by Definition 2.13.23 **(b)**) and thus $v_p(m) = \infty \geq v_p(n)$, so that $v_p(n) \leq v_p(m)$. Also, $n \mid 0 = m$. Thus, the statements "$n \mid m$" and "each prime p satisfies $v_p(n) \leq v_p(m)$" are both true. Hence, $n \mid m$ if and only if each prime p satisfies $v_p(n) \leq v_p(m)$. In other words, Proposition 2.13.35 is true. Qed.

[40] *Proof.* Assume that $n = 0$. Thus, each prime p satisfies $v_p\left(\underbrace{n}_{=0}\right) = v_p(0) = \infty$ (by Definition 2.13.23 **(b)**) and thus $v_p(m) < \infty = v_p(n)$. Applying this to $p = 2$, we obtain $v_2(m) < v_2(n)$ (since 2 is a prime). Hence, we don't have $v_2(n) \leq v_2(m)$. Thus, the statement "each prime p satisfies $v_p(n) \leq v_p(m)$" is false (since $p = 2$ is a counterexample).

If we had $n \mid m$, then there would be an integer c such that $m = nc$. This would then lead to $m = \underbrace{n}_{=0} c = 0$, which would contradict $m \neq 0$. Hence, we cannot have $n \mid m$. Thus, the statements "$n \mid m$" and "each prime p satisfies $v_p(n) \leq v_p(m)$" are both false. Hence, $n \mid m$ if and only if each prime p satisfies $v_p(n) \leq v_p(m)$. In other words, Proposition 2.13.35 is true. Qed.

[41] Indeed, the statement "$n \mid m$" does not change (since Proposition 2.2.3 **(a)** yields that we have $n \mid m$ if and only if $|n| \mid |m|$), and the statement "each prime p satisfies $v_p(n) \leq v_p(m)$" does not change either (because Exercise 2.13.5 shows that $v_p(|n|) = v_p(n)$ and $v_p(|m|) = v_p(m)$).

Similarly,

$$m = \prod_{p \text{ prime}} p^{v_p(m)}. \tag{43}$$

Our goal is to prove that $n \mid m$ if and only if each prime p satisfies $v_p(n) \leq v_p(m)$. We shall now prove the "$\Longleftarrow$" and "$\Longrightarrow$" directions of this "if and only if" statement separately.

$\Longleftarrow$: Assume that each prime p satisfies $v_p(n) \leq v_p(m)$. We must prove that $n \mid m$.

The product $\prod_{p \text{ prime}} p^{v_p(m)-v_p(n)}$ is well-defined[42].

We have assumed that each prime p satisfies $v_p(n) \leq v_p(m)$. In other words, each prime p satisfies $v_p(m) - v_p(n) \geq 0$ and therefore $p^{v_p(m)-v_p(n)} \in \mathbb{Z}$. Hence, the product $\prod_{p \text{ prime}} p^{v_p(m)-v_p(n)}$ is a product of integers, and thus itself an integer. Let us denote this product by c. Thus,

$$c = \prod_{p \text{ prime}} p^{v_p(m)-v_p(n)}. \tag{44}$$

Thus, c is an integer (since we have just shown that $\prod_{p \text{ prime}} p^{v_p(m)-v_p(n)}$ is an integer). Multiplying the equalities (42) and (44), we obtain

$$nc = \left(\prod_{p \text{ prime}} p^{v_p(n)}\right)\left(\prod_{p \text{ prime}} p^{v_p(m)-v_p(n)}\right) = \prod_{p \text{ prime}} \underbrace{\left(p^{v_p(n)} p^{v_p(m)-v_p(n)}\right)}_{\substack{=p^{v_p(n)+\left(v_p(m)-v_p(n)\right)}=p^{v_p(m)} \\ (\text{since } v_p(n)+\left(v_p(m)-v_p(n)\right)=v_p(m))}}$$
$$= \prod_{p \text{ prime}} p^{v_p(m)} = m \qquad (\text{by (43)}).$$

In other words, $m = nc$. Hence, $n \mid m$. This completes the proof of the "$\Longleftarrow$" direction of Proposition 2.13.35.

$\Longrightarrow$: Assume that $n \mid m$. We must prove that each prime p satisfies $v_p(n) \leq v_p(m)$.

[42] *Proof.* Let p be a prime such that $p > |m|$. Then, $v_p(m) = 0$ (by Lemma 2.13.32 **(a)**, applied to m instead of n), so that $v_p(m) - \underbrace{v_p(n)}_{\geq 0} \leq v_p(m) = 0$. On the other hand, $v_p(n) \leq v_p(m)$ (since we assumed that each prime p satisfies $v_p(n) \leq v_p(m)$); thus, $v_p(m) - v_p(n) \geq 0$. Combining this with $v_p(m) - v_p(n) \leq 0$, we obtain $v_p(m) - v_p(n) = 0$. Hence, $p^{v_p(m)-v_p(n)} = p^0 = 1$.

Now, forget that we fixed p. We thus have proven that every prime $p > |m|$ satisfies $p^{v_p(m)-v_p(n)} = 1$. Hence, all but finitely many primes p satisfy $p^{v_p(m)-v_p(n)} = 1$ (since all but finitely many primes p satisfy $p > |m|$). In other words, the product $\prod_{p \text{ prime}} p^{v_p(m)-v_p(n)}$ has only finitely many factors different from 1. Hence, this product is well-defined.

So let p be a prime. Recall that $n \mid m$. In other words, there exists some integer b such that $m = nb$. Consider this b. Now,

$$\begin{aligned} v_p \left(\underbrace{m}_{=nb} \right) &= v_p (nb) \\ &= v_p (n) + \underbrace{v_p (b)}_{\geq 0} \qquad \text{(by Theorem 2.13.28 **(a)**, applied to } a = n\text{)} \\ &\geq v_p (n), \end{aligned}$$

so that $v_p (n) \leq v_p (m)$. Now, forget that we fixed p. We thus have proven that each prime p satisfies $v_p (n) \leq v_p (m)$. This completes the proof of the "$\Longrightarrow$" direction of Proposition 2.13.35. □

Let us extract one of the steps of our above proof into a separate lemma, since we shall use the same reasoning later on:

Lemma 2.13.36. For each prime p, let a_p and b_p be nonnegative integers such that

$$a_p \leq b_p. \tag{45}$$

Assume that all but finitely many primes p satisfy $b_p = 0$. Then, the products $\prod_{p \text{ prime}} p^{a_p}$ and $\prod_{p \text{ prime}} p^{b_p}$ are both well-defined and satisfy

$$\prod_{p \text{ prime}} p^{a_p} \mid \prod_{p \text{ prime}} p^{b_p}. \tag{46}$$

Proof of Lemma 2.13.36. This is going to be really boring: The well-definedness part is all about bookkeeping finiteness information, whereas the $\prod_{p \text{ prime}} p^{a_p} \mid \prod_{p \text{ prime}} p^{b_p}$ claim is proven just as we proved the "$\Longleftarrow$" direction of Proposition 2.13.35. For the sake of completeness, let us nevertheless give the complete proof:

All but finitely many primes p satisfy $b_p = 0$. In other words, there exists some finite set S of primes such that every prime $p \notin S$ satisfies

$$b_p = 0. \tag{47}$$

Consider this S. Clearly, all but finitely many primes p satisfy $p \notin S$ (since S is finite).

Now, every prime $p \notin S$ satisfies

$$a_p = 0 \tag{48}$$

[43]. Hence, all but finitely many primes p satisfy $a_p = 0$ (since all but finitely many primes p satisfy $p \notin S$). Thus, all but finitely many primes p satisfy $p^{a_p} = p^0 = 1$. In other words,

[43] *Proof.* Let $p \notin S$ be a prime. Then, (45) yields $a_p \leq b_p = 0$ (by (47)). Thus, $a_p = 0$ (since a_p is a nonnegative integer), qed.

only finitely many primes p satisfy $p^{a_p} \neq 1$. In other words, only finitely many factors of the product $\prod\limits_{p \text{ prime}} p^{a_p}$ are different from 1. Hence, this product $\prod\limits_{p \text{ prime}} p^{a_p}$ is well-defined.

Also, all but finitely many primes p satisfy $b_p = 0$. Therefore, all but finitely many primes p satisfy $p^{b_p} = p^0 = 1$. In other words, only finitely many primes p satisfy $p^{b_p} \neq 1$. In other words, only finitely many factors of the product $\prod\limits_{p \text{ prime}} p^{b_p}$ are different from 1. Hence, this product $\prod\limits_{p \text{ prime}} p^{b_p}$ is well-defined.

The product $\prod\limits_{p \text{ prime}} p^{b_p - a_p}$ is well-defined[44]. Denote this product by c.

For each prime p, we have $b_p - a_p \geq 0$ (by (45)) and thus $b_p - a_p \in \mathbb{N}$. Hence, for each prime p, the number $p^{b_p - a_p}$ is an integer. Therefore, $\prod\limits_{p \text{ prime}} p^{b_p - a_p}$ is a product of integers, and thus itself an integer. In other words, c is an integer (since $c = \prod\limits_{p \text{ prime}} p^{b_p - a_p}$).

But from $c = \prod\limits_{p \text{ prime}} p^{b_p - a_p}$, we obtain

$$\left(\prod_{p \text{ prime}} p^{a_p}\right) c = \left(\prod_{p \text{ prime}} p^{a_p}\right)\left(\prod_{p \text{ prime}} p^{b_p - a_p}\right) = \prod_{p \text{ prime}} \underbrace{\left(p^{a_p} p^{b_p - a_p}\right)}_{= p^{a_p + (b_p - a_p)} = p^{b_p}} = \prod_{p \text{ prime}} p^{b_p}.$$

Thus, $\prod\limits_{p \text{ prime}} p^{a_p} \mid \prod\limits_{p \text{ prime}} p^{b_p}$ (since c is an integer). This completes the proof of Lemma 2.13.36. □

Corollary 2.13.37. For each prime p, let b_p be a nonnegative integer. Assume that all but finitely many primes p satisfy $b_p = 0$. Let $n = \prod\limits_{p \text{ prime}} p^{b_p}$. Then,

$$v_q(n) = b_q \qquad \text{for each prime } q.$$

Proof of Corollary 2.13.37. The product $\prod\limits_{p \text{ prime}} p^{b_p}$ is well-defined. (This can be shown just as in the proof of Lemma 2.13.36.) Now, choose a list $(a_1, a_2, \ldots, a_k)$ of primes that contains each prime p exactly b_p times. (Such a list clearly exists: For example, we can pick

$$\left(\underbrace{2, 2, \ldots, 2}_{b_2 \text{ times}}, \underbrace{3, 3, \ldots, 3}_{b_3 \text{ times}}, \underbrace{5, 5, \ldots, 5}_{b_5 \text{ times}}, \ldots\right).$$

[44] *Proof.* Every prime $p \notin S$ satisfies $\underbrace{b_p}_{\substack{=0 \\ \text{(by (47))}}} - \underbrace{a_p}_{\substack{=0 \\ \text{(by (48))}}} = 0 - 0 = 0$ and therefore $p^{b_p - a_p} = p^0 = 1$.

Thus, all but finitely many primes p satisfy $p^{b_p - a_p} = 1$ (since all but finitely many primes p satisfy $p \notin S$). In other words, only finitely many primes p satisfy $p^{b_p - a_p} \neq 1$. In other words, only finitely many factors of the product $\prod\limits_{p \text{ prime}} p^{b_p - a_p}$ are different from 1. Hence, this product $\prod\limits_{p \text{ prime}} p^{b_p - a_p}$ is well-defined.

This is indeed a finite list, since all but finitely many primes p satisfy $b_p = 0$.)

Now, the list $(a_1, a_2, \ldots, a_k)$ contains each prime p exactly b_p times (and no other entries). Hence, the product $a_1 a_2 \cdots a_k$ of the entries of this list contains each prime p exactly b_p times as a factor (and no other factors). Thus, this product equals $\prod\limits_{p \text{ prime}} p^{b_p}$. In other words, $a_1 a_2 \cdots a_k = \prod\limits_{p \text{ prime}} p^{b_p}$. Hence,

$$n = \prod_{p \text{ prime}} p^{b_p} = a_1 a_2 \cdots a_k.$$

Thus, $(a_1, a_2, \ldots, a_k)$ is a prime factorization of n (since $(a_1, a_2, \ldots, a_k)$ is a tuple of primes).

Let q be a prime. Proposition 2.13.30 (applied to $p = q$) yields

$$\begin{aligned} & (\text{the number of times } q \text{ appears in the tuple } (a_1, a_2, \ldots, a_k)) \\ & = (\text{the number of } i \in \{1, 2, \ldots, k\} \text{ such that } a_i = q) \\ & = v_q(n). \end{aligned}$$

Thus,

$$v_q(n) = (\text{the number of times } q \text{ appears in the tuple } (a_1, a_2, \ldots, a_k)) = b_q$$

(since the list $(a_1, a_2, \ldots, a_k)$ contains each prime p exactly b_p times, and thus contains the prime q exactly b_q times). This proves Corollary 2.13.37. □

Exercise 2.13.9. Let n be a nonzero integer. Let a and b be two integers. Assume that

$$a \equiv b \mod p^{v_p(n)} \qquad \text{for every prime } p. \tag{49}$$

Prove that $a \equiv b \mod n$.

Canonical factorizations can also be used to describe gcds and lcms:

Proposition 2.13.38. Let n and m be two nonzero integers. Then,

$$\gcd(n, m) = \prod_{p \text{ prime}} p^{\min\{v_p(n), v_p(m)\}} \tag{50}$$

and

$$\operatorname{lcm}(n, m) = \prod_{p \text{ prime}} p^{\max\{v_p(n), v_p(m)\}}. \tag{51}$$

Proof of Proposition 2.13.38. If p is any prime, then $v_p(n)$ and $v_p(m)$ are nonnegative integers (since n and m are nonzero), and thus so are $\min\{v_p(n), v_p(m)\}$ and $\max\{v_p(n), v_p(m)\}$.

It is easy to see that the infinite products $\prod\limits_{p \text{ prime}} p^{\min\left\{v_p(n), v_p(m)\right\}}$ and $\prod\limits_{p \text{ prime}} p^{\max\left\{v_p(n), v_p(m)\right\}}$ are well-defined[45].

Define two nonnegative integers

$$g = \prod_{p \text{ prime}} p^{\min\left\{v_p(n), v_p(m)\right\}} \qquad \text{and} \qquad h = \gcd(n, m). \tag{52}$$

Note that $h = \gcd(n, m)$ is a positive integer (since n and m are nonzero) and thus nonzero. Thus, $v_p(h)$ is a nonnegative integer for each prime p.

Corollary 2.13.34 yields $|n| = \prod\limits_{p \text{ prime}} p^{v_p(n)}$. But each prime p satisfies $\min\left\{v_p(n), v_p(m)\right\} \leq v_p(n)$ (since the minimum of a set is $\leq$ to any element of the set). Hence, (46) (applied to $a_p = \min\left\{v_p(n), v_p(m)\right\}$ and $b_p = v_p(n)$) yields $\prod\limits_{p \text{ prime}} p^{\min\left\{v_p(n), v_p(m)\right\}} \mid \prod\limits_{p \text{ prime}} p^{v_p(n)}$. This rewrites as $g \mid |n|$ (since $g = \prod\limits_{p \text{ prime}} p^{\min\left\{v_p(n), v_p(m)\right\}}$ and $|n| = \prod\limits_{p \text{ prime}} p^{v_p(n)}$). Hence, $g \mid |n| \mid n$ (by Exercise 2.2.1 **(b)**). Similarly, $g \mid m$. Thus, ($g \mid n$ and $g \mid m$). Hence, Lemma 2.9.16 (applied to g, n and m instead of m, a and b) yields $g \mid \gcd(n, m) = h$.

Proposition 2.9.7 **(f)** (applied to n and m instead of a and b) yields $\gcd(n, m) \mid n$ and $\gcd(n, m) \mid m$. Thus, $h = \gcd(n, m) \mid n$ and $h = \gcd(n, m) \mid m$.

On the other hand, Proposition 2.13.35 (applied to h and n instead of n and m) shows that $h \mid n$ if and only if each prime p satisfies $v_p(h) \leq v_p(n)$. Thus, each prime p satisfies $v_p(h) \leq v_p(n)$ (since $h \mid n$).

Now, fix any prime p. Then, $v_p(h) \leq v_p(n)$ (as we have just seen) and $v_p(h) \leq v_p(m)$ (similarly). Combining these two inequalities, we obtain

$$v_p(h) \leq \min\left\{v_p(n), v_p(m)\right\}$$

(since $\min\left\{v_p(n), v_p(m)\right\}$ must be one of the two numbers $v_p(n)$ and $v_p(m)$, but we have just seen that $v_p(h)$ is $\leq$ to each of these two numbers).

[45] *Proof.* Let p be a prime such that $p > \max\left\{|m|, |n|\right\}$. Thus, $p > \max\left\{|m|, |n|\right\} \geq |m|$ and therefore $v_p(m) = 0$ (by Lemma 2.13.32 **(a)**, applied to m instead of n). Similarly, $v_p(n) = 0$. Hence, $\max\left\{\underbrace{v_p(n)}_{=0}, \underbrace{v_p(m)}_{=0}\right\} = \max\left\{0, 0\right\} = 0$ and therefore $p^{\max\left\{v_p(n), v_p(m)\right\}} = p^0 = 1$.

Now, forget that we fixed p. We thus have proven that every prime $p > \max\left\{|m|, |n|\right\}$ satisfies $p^{\max\left\{v_p(n), v_p(m)\right\}} = 1$. Hence, all but finitely many primes p satisfy $p^{\max\left\{v_p(n), v_p(m)\right\}} = 1$ (since all but finitely many primes p satisfy $p > \max\left\{|m|, |n|\right\}$). In other words, the product $\prod\limits_{p \text{ prime}} p^{\max\left\{v_p(n), v_p(m)\right\}}$ has only finitely many factors different from 1. Hence, this product is well-defined. Similarly, we can show that the product $\prod\limits_{p \text{ prime}} p^{\min\left\{v_p(n), v_p(m)\right\}}$ is well-defined.

Now, forget that we fixed p. We thus have show that each prime p satisfies $v_p(h) \leq \min\{v_p(n), v_p(m)\}$. Hence, (46) (applied to $a_p = v_p(h)$ and $b_p = \min\{v_p(n), v_p(m)\}$) yields $\prod\limits_{p \text{ prime}} p^{v_p(h)} \mid \prod\limits_{p \text{ prime}} p^{\min\{v_p(n),v_p(m)\}}$. But h is positive; hence, Corollary 2.13.33 (applied to h instead of n) yields

$$h = \prod_{p \text{ prime}} p^{v_p(h)} \mid \prod_{p \text{ prime}} p^{\min\{v_p(n),v_p(m)\}} = g.$$

Thus, we know that $g \mid h$ and $h \mid g$. Hence, Exercise 2.2.2 (applied to $a = g$ and $b = h$) yields $|g| = |h|$. But g is nonnegative; thus, $|g| = g$. Hence, $g = |g| = |h| = h$ (since h is positive). In view of (52), this rewrites as $\prod\limits_{p \text{ prime}} p^{\min\{v_p(n),v_p(m)\}} = \gcd(n, m)$. This proves (50).

The proof of (51) is entirely analogous to the proof of (50) we just gave: We merely need to

- flip all divisibilities and inequalities and replace "min" by "max" everywhere;
- use Proposition 2.11.5 **(c)** instead of Proposition 2.9.7 **(f)**;
- use Lemma 2.11.8 instead of Lemma 2.9.16.

□

Example 2.13.39. For this example, set $n = 3^2 \cdot 5 \cdot 7^8$ and $m = 2 \cdot 3^3 \cdot 7^2$. Let us compute $\gcd(n, m)$ and $\operatorname{lcm}(n, m)$ using Proposition 2.13.38.

From $n = 3^2 \cdot 5 \cdot 7^8$, we obtain (using Corollary 2.13.37) that

$$v_3(n) = 2, \qquad v_5(n) = 1, \qquad v_7(n) = 8, \qquad \text{and}$$
$$v_p(n) = 0 \text{ for each prime } p \notin \{3, 5, 7\}.$$

Similarly, from $m = 2 \cdot 3^3 \cdot 7^2$, we obtain

$$v_2(m) = 1, \qquad v_3(m) = 3, \qquad v_7(m) = 2, \qquad \text{and}$$
$$v_p(n) = 0 \text{ for each prime } p \notin \{2, 3, 7\}.$$

Now, (50) yields

$$\begin{aligned}
&\gcd\left(n,m\right)\\
&=\prod_{p\text{ prime}} p^{\min\left\{v_p(n),v_p(m)\right\}}\\
&=\underbrace{2^{\min\{v_2(n),v_2(m)\}}}_{=2^{\min\{0,1\}}=2^0}\cdot\underbrace{3^{\min\{v_3(n),v_3(m)\}}}_{=3^{\min\{2,3\}}=3^2}\cdot\underbrace{5^{\min\{v_5(n),v_5(m)\}}}_{=5^{\min\{1,0\}}=5^0}\\
&\qquad\cdot\underbrace{7^{\min\{v_7(n),v_7(m)\}}}_{=7^{\min\{8,2\}}=7^2}\cdot\prod_{\substack{p\text{ prime;}\\ p\notin\{2,3,5,7\}}}\underbrace{p^{\min\left\{v_p(n),v_p(m)\right\}}}_{\substack{=1\\ \text{(since } v_p(n)=0 \text{ and } v_p(m)=0\\ \text{and thus } \min\left\{v_p(n),v_p(m)\right\}=\min\{0,0\}=0)}}\\
&=2^0\cdot 3^2\cdot 5^0\cdot 7^2=3^2\cdot 7^2.
\end{aligned}$$

Likewise, (51) yields

$$\begin{aligned}
&\operatorname{lcm}\left(n,m\right)\\
&=\prod_{p\text{ prime}} p^{\max\left\{v_p(n),v_p(m)\right\}}\\
&=\underbrace{2^{\max\{v_2(n),v_2(m)\}}}_{=2^{\max\{0,1\}}=2^1}\cdot\underbrace{3^{\max\{v_3(n),v_3(m)\}}}_{=3^{\max\{2,3\}}=3^3}\cdot\underbrace{5^{\max\{v_5(n),v_5(m)\}}}_{=5^{\max\{1,0\}}=5^1}\\
&\qquad\cdot\underbrace{7^{\max\{v_7(n),v_7(m)\}}}_{=7^{\max\{8,2\}}=7^8}\cdot\prod_{\substack{p\text{ prime;}\\ p\notin\{2,3,5,7\}}}\underbrace{p^{\max\left\{v_p(n),v_p(m)\right\}}}_{\substack{=1\\ \text{(since } v_p(n)=0 \text{ and } v_p(m)=0\\ \text{and thus } \max\left\{v_p(n),v_p(m)\right\}=\max\{0,0\}=0)}}\\
&=2^1\cdot 3^3\cdot 5^1\cdot 7^8.
\end{aligned}$$

Proposition 2.13.38 can be generalized to the case of k integers $b_1,b_2,\ldots,b_k$ instead of two integers n,m:

Proposition 2.13.40. Let $b_1,b_2,\ldots,b_k$ be finitely many nonzero integers, with $k>0$. Then,

$$\gcd\left(b_1,b_2,\ldots,b_k\right)=\prod_{p\text{ prime}} p^{\min\left\{v_p(b_1),v_p(b_2),\ldots,v_p(b_k)\right\}}\tag{53}$$

an

$$\operatorname{lcm}\left(b_1,b_2,\ldots,b_k\right)=\prod_{p\text{ prime}} p^{\max\left\{v_p(b_1),v_p(b_2),\ldots,v_p(b_k)\right\}}.\tag{54}$$

Proof of Proposition 2.13.40. The proof of Proposition 2.13.40 is analogous to the proof of Proposition 2.13.38, with two minor exceptions:

- Instead of applying Lemma 2.9.16 (in the proof of (53)), we now have to apply the analogous claim for k integers[46]. The latter claim follows from Theorem 2.9.21 **(a)**.

- Instead of applying Lemma 2.11.8 (in the proof of (54)), we now have to apply the analogous claim for k integers[47]. The latter claim follows from Theorem 2.11.9 **(a)**.

  Alternatively, instead of applying this claim, we can argue as follows: Setting $g = \prod_{p \text{ prime}} p^{\max\{v_p(b_1), v_p(b_2), \ldots, v_p(b_k)\}}$ and $h = \operatorname{lcm}(b_1, b_2, \ldots, b_k)$, we see that $(b_i \mid g \text{ for all } i \in \{1, 2, \ldots, k\})$ (by an argument analogous to the one we used to show $(g \mid n \text{ and } g \mid m)$ in the original proof of (50)). Thus, g is a common multiple of $b_1, b_2, \ldots, b_k$. In other words, $g \in \operatorname{Mul}(b_1, b_2, \ldots, b_k)$. Hence, g is a positive element of $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$ (since g is positive). Hence, $g \geq \operatorname{lcm}(b_1, b_2, \ldots, b_k)$ (since $\operatorname{lcm}(b_1, b_2, \ldots, b_k)$ is the **smallest** positive element of $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$). In other words, $g \geq h$ (since $h = \operatorname{lcm}(b_1, b_2, \ldots, b_k)$). On the other hand, we prove $g \mid h$ (similarly to how we proved $h \mid g$ in the original proof of (50)). Thus, Proposition 2.2.3 **(b)** (applied to g and h instead of a and b) yields $|g| \leq |h|$ (since $h \neq 0$). Since g is positive, we have $|g| = g$ and thus $g = |g| \leq |h| = h$ (since h is positive). Combining this with $g \geq h$, we obtain $g = h$. As before, this completes the proof of (54).

□

We can use Propositions 2.13.38 and 2.13.40 to reprove certain facts about lcms and gcds. For example, let us prove Theorem 2.11.6 and solve Exercise 2.11.2:

Second proof of Theorem 2.11.6 (sketched). WLOG assume that a and b are nonzero (since otherwise, the claim of Theorem 2.11.6 easily reduces to $0 = 0$). Then, ab is nonzero as well. Hence, Corollary 2.13.34 (applied to $n = ab$) yields

$$|ab| = \prod_{p \text{ prime}} p^{v_p(ab)}.$$

Now, Proposition 2.13.38 yields

$$\gcd(a, b) = \prod_{p \text{ prime}} p^{\min\{v_p(a), v_p(b)\}} \qquad \text{and}$$
$$\operatorname{lcm}(a, b) = \prod_{p \text{ prime}} p^{\max\{v_p(a), v_p(b)\}}.$$

[46] Namely: Let $m \in \mathbb{Z}$ and let $b_1, b_2, \ldots, b_k$ be integers such that $(m \mid b_i \text{ for all } i \in \{1, 2, \ldots, k\})$. Then, $m \mid \gcd(b_1, b_2, \ldots, b_k)$.

[47] Namely: Let $m \in \mathbb{Z}$ and let $b_1, b_2, \ldots, b_k$ be integers such that $(b_i \mid m \text{ for all } i \in \{1, 2, \ldots, k\})$. Then, $\operatorname{lcm}(b_1, b_2, \ldots, b_k) \mid m$.

Multiplying these two equalities, we get

$$\begin{aligned}
\gcd(a,b)\cdot\operatorname{lcm}(a,b) &= \left(\prod_{p\text{ prime}} p^{\min\left\{v_p(a),v_p(b)\right\}}\right)\cdot\left(\prod_{p\text{ prime}} p^{\max\left\{v_p(a),v_p(b)\right\}}\right) \\
&= \prod_{p\text{ prime}} \underbrace{\left(p^{\min\left\{v_p(a),v_p(b)\right\}}p^{\max\left\{v_p(a),v_p(b)\right\}}\right)}_{\substack{=p^{\min\left\{v_p(a),v_p(b)\right\}+\max\left\{v_p(a),v_p(b)\right\}} \\ =p^{v_p(a)+v_p(b)} \\ \text{(since }\min\{u,v\}+\max\{u,v\}=u+v\text{ for any reals }u,v)}} \\
&= \prod_{p\text{ prime}} \underbrace{p^{v_p(a)+v_p(b)}}_{\substack{=p^{v_p(ab)} \\ \text{(since }v_p(a)+v_p(b)=v_p(ab) \\ \text{(by Theorem 2.13.28 }\textbf{(a)}\text{))}}} = \prod_{p\text{ prime}} p^{v_p(ab)} = |ab|\,.
\end{aligned}$$

Hence, Theorem 2.11.6 is proven again.

See Section 10.59 for a second solution to Exercise 2.11.2 using Propositions 2.13.38 and 2.13.40 (and a slightly more general result that can be proven in the same way). □

Exercise 2.13.10. Let n and m be two integers. Let p be a prime.
(a) Prove that $v_p(\gcd(n,m)) = \min\left\{v_p(n), v_p(m)\right\}$.
(b) Prove that $v_p(\operatorname{lcm}(n,m)) = \max\left\{v_p(n), v_p(m)\right\}$.

Exercise 2.13.11. Let a, b, c be three integers.
(a) Prove that $\gcd(a, \operatorname{lcm}(b,c)) = \operatorname{lcm}(\gcd(a,b), \gcd(a,c))$.
(b) Prove that $\operatorname{lcm}(a, \gcd(b,c)) = \gcd(\operatorname{lcm}(a,b), \operatorname{lcm}(a,c))$.

The two parts of Exercise 2.13.11 can be regarded as "distributivity laws", but for the binary operations gcd and lcm (or lcm and gcd, respectively) instead of $+$ and $\cdot$.

2.13.8. Coprimality through prime factors

Proposition 2.13.41. Let n and m be two integers. Then, $n \perp m$ if and only if there exists no prime p that divides both n and m.

Proof of Proposition 2.13.41. $\Longrightarrow$: Assume that $n \perp m$. We must prove that there exists no prime p that divides both n and m.

Let p be a prime that divides both n and m. Thus, $p \mid n$ and $p \mid m$. Hence, $p \mid \gcd(n,m)$ (by Lemma 2.9.16, applied to p, n and m instead of m, a and b). But $\gcd(n,m) = 1$ (since $n \perp m$). Hence, $p \mid \gcd(n,m) = 1$. Hence, Proposition 2.2.3 **(b)** (applied to $a = p$ and $b = 1$) yields $|p| \leq |1| = 1$.

But p is a prime; thus, $p > 1 > 0$, so that $|p| = p$ and thus $p = |p| \leq 1$. This contradicts $p > 1$.

Now, forget that we fixed p. We thus have obtained a contradiction for each prime p that divides both n and m. Hence, there exists no prime p that divides both n and m. This proves the "$\Longrightarrow$" direction of Proposition 2.13.41.

$\Longleftarrow$: Assume that there exists no prime p that divides both n and m. We must prove that $n \perp m$.

Assume the contrary. Thus, we don't have $n \perp m$. In other words, we don't have $\gcd(n,m) = 1$. In other words, $\gcd(n,m) \neq 1$. Hence, there exists at least one prime p such that $p \mid \gcd(n,m)$ [48]. Consider this p.

We have $p \mid \gcd(n,m) \mid n$ and $p \mid \gcd(n,m) \mid m$. Thus, the prime p divides both n and m. This contradicts the assumption that there exists no prime p that divides both n and m.

This contradiction shows that our assumption was false. Hence, $n \perp m$ is proven. This proves the "$\Longleftarrow$" direction of Proposition 2.13.41. □

Corollary 2.13.42. Let n and m be two nonzero integers. Then:

(a) The infinite sum $\sum\limits_{p \text{ prime}} v_p(n) v_p(m)$ is well-defined (i.e., all but finitely many primes p satisfy $v_p(n) v_p(m) = 0$).

(b) We have $n \perp m$ if and only if

$$\sum_{p \text{ prime}} v_p(n) v_p(m) = 0.$$

Proof of Corollary 2.13.42 (sketched). **(a)** For every prime $p > |n|$, we have $v_p(n) = 0$ (by Lemma 2.13.32 **(a)**) and thus $\underbrace{v_p(n)}_{=0} v_p(m) = 0$. Now, Corollary 2.13.42 **(a)** follows easily.

(b) A sum of nonnegative reals is 0 if and only if each of its addends is 0. Thus, the sum $\sum\limits_{p \text{ prime}} v_p(n) v_p(m)$ is 0 if and only if we have

$$\left(v_p(n) v_p(m) = 0 \text{ for all primes } p\right)$$

(because all the addends $v_p(n) v_p(m)$ of our sum are nonnegative reals). Hence,

[48] *Proof.* This is obvious if $\gcd(n,m) = 0$ (because in that case, we can take $p = 2$, or any other prime). Thus, for the rest of this proof, we WLOG assume that $\gcd(n,m) \neq 0$. Thus, $\gcd(n,m) > 1$ (since $\gcd(n,m)$ is a nonnegative integer satisfying $\gcd(n,m) \neq 0$ and $\gcd(n,m) \neq 1$). Hence, Proposition 2.13.8 (applied to $\gcd(n,m)$ instead of n) yields that there exists at least one prime p such that $p \mid \gcd(n,m)$. Qed.

we have the following chain of equivalences:

$$\begin{aligned}
&\left(\sum_{p \text{ prime}} v_p\left(n\right) v_p\left(m\right) = 0\right) \\
&\Longleftrightarrow \left(v_p\left(n\right) v_p\left(m\right) = 0 \text{ for all primes } p\right) \\
&\Longleftrightarrow \left(\left(v_p\left(n\right) = 0 \text{ or } v_p\left(m\right) = 0\right) \text{ for all primes } p\right) \\
&\Longleftrightarrow \left(\left(p \nmid n \text{ or } p \nmid m\right) \text{ for all primes } p\right) \\
&\qquad \left(\begin{array}{c}\text{since Corollary 2.13.26 yields the} \\ \text{equivalences } \left(v_p\left(n\right) = 0\right) \Longleftrightarrow \left(p \nmid n\right) \text{ and } \left(v_p\left(m\right) = 0\right) \Longleftrightarrow \left(p \nmid m\right) \\ \text{for each prime } p\end{array}\right) \\
&\Longleftrightarrow \left(\text{there exists no prime } p \text{ such that } \left(p \mid n \text{ and } p \mid m\right)\right) \\
&\Longleftrightarrow \left(\text{there exists no prime } p \text{ that divides both } n \text{ and } m\right) \\
&\Longleftrightarrow \left(n \perp m\right) \qquad \left(\text{by Proposition 2.13.41}\right).
\end{aligned}$$

This proves Corollary 2.13.42 **(b)**. □

Corollary 2.13.42 **(b)** is the reason for the notation "$\perp$" that we are using for coprimality. In fact, when n is a positive integer, we can regard the p-valuations $v_p\left(n\right)$ as the "coordinates" of n in an (infinite-dimensional) Cartesian coordinate system. Then, the sum $\sum\limits_{p \text{ prime}} v_p\left(n\right) v_p\left(m\right)$ in Corollary 2.13.42 is something like a "dot product" between n and m. Thus, Corollary 2.13.42 **(b)** shows that two integers n and m are coprime if and only if their "dot product" is 0. But for vectors in a Euclidean space, the dot product is 0 if and only if the vectors are orthogonal. Thus, coprime integers are like orthogonal vectors. Of course, this analogy should be taken with a grain of salt; in particular, our "dot product" is far from being bilinear[49].

2.13.9. There are infinitely many primes

Theorem 2.13.43. There are infinitely many primes.

Proof of Theorem 2.13.43. The following proof is a classic, appearing in Euclid's *Elements*:

Let $\left(p_1, p_2, \ldots, p_k\right)$ be any finite list of primes. We shall find a new prime distinct from each of $p_1, p_2, \ldots, p_k$.

[49] Or, rather, it is bilinear **with respect to multiplication**: If we denote $\sum\limits_{p \text{ prime}} v_p\left(n\right) v_p\left(m\right)$ by $\langle n, m\rangle$, then we have

$$\langle n_1 n_2, m\rangle = \langle n_1, m\rangle + \langle n_2, m\rangle \qquad \text{and} \qquad \langle n, m_1 m_2\rangle = \langle n, m_1\rangle + \langle n, m_2\rangle$$

for arbitrary integers n_1, n_2, m, n, m_1, m_2.

Indeed, $p_1, p_2, \ldots, p_k$ are primes, and thus are integers > 1 (by the definition of a "prime"). Hence, they are positive integers; thus, their product $p_1 p_2 \cdots p_k$ is a positive integer as well. Thus, $p_1 p_2 \cdots p_k > 0$.

Now, let $n = p_1 p_2 \cdots p_k + 1$. Then, $n = \underbrace{p_1 p_2 \cdots p_k}_{>0} + 1 > 1$. Hence, Proposition 2.13.8 shows that there exists at least one prime p such that $p \mid n$. Consider this p.

We claim that p is distinct from each of $p_1, p_2, \ldots, p_k$.

[*Proof:* Assume the contrary. Thus, $p = p_i$ for some $i \in \{1, 2, \ldots, k\}$. Consider this i.

We have $p_1 p_2 \cdots p_k = p_i \cdot (p_1 p_2 \cdots p_{i-1} p_{i+1} p_{i+2} \cdots p_k)$. Thus, $p_i \mid p_1 p_2 \cdots p_k$ (since $p_1 p_2 \cdots p_{i-1} p_{i+1} p_{i+2} \cdots p_k$ is an integer). Hence, $p = p_i \mid p_1 p_2 \cdots p_k$. In other words, $p_1 p_2 \cdots p_k \equiv 0 \bmod p$. Now,

$$n = \underbrace{p_1 p_2 \cdots p_k}_{\equiv 0 \bmod p} + 1 \equiv 0 + 1 = 1 \bmod p.$$

Hence, $1 \equiv n \bmod p$. But $p \mid n$ and thus $n \equiv 0 \bmod p$. Hence, $1 \equiv n \equiv 0 \bmod p$; in other words, $p \mid 1 - 0 = 1$. Thus, Proposition 2.2.3 **(b)** (applied to $a = p$ and $b = 1$) yields $|p| \leq |1| = 1$. But p is a prime; thus, $p > 1 > 0$, so that $|p| = p > 1$. This contradicts $|p| \leq 1$. This contradiction shows that our assumption was wrong, qed.]

Thus, we have proven that p is distinct from each of $p_1, p_2, \ldots, p_k$. Hence, there exists a prime distinct from each of $p_1, p_2, \ldots, p_k$ (namely, p).

Now, forget that we fixed $p_1, p_2, \ldots, p_k$. We thus have proven that if $(p_1, p_2, \ldots, p_k)$ is any finite list of primes, then there exists a prime distinct from each of $p_1, p_2, \ldots, p_k$. In other words, given any finite list of primes, there exists at least one prime that is not in this list. In other words, no finite list of primes can cover all the primes. In other words, there are infinitely many primes. This proves Theorem 2.13.43. □

Note that our proof of Theorem 2.13.43 is constructive: It gives an algorithm to construct arbitrarily many distinct primes. This algorithm is not very efficient, since $p_1 p_2 \cdots p_k + 1$ can be very large even if $p_1, p_2, \ldots, p_k$ are fairly small. In practice, the sieve of Eratosthenes is much better for generating primes. Much faster algorithms are known.

Exercise 2.13.12. Let p be a prime. Let $a \in \mathbb{Z}$ be such that $a^2 \equiv 1 \bmod p$. Prove that $a \equiv 1 \bmod p$ or $a \equiv -1 \bmod p$.

Exercise 2.13.13. Let p be a prime. Let $k \in \mathbb{N}$. Prove that the nonnegative divisors of p^k are $p^0, p^1, \ldots, p^k$.

2.14. Euler's totient function (ϕ-function)

2.14.1. Definition and some formulas

Recall that $\mathbb{P}$ stands for the set of all positive integers.

Definition 2.14.1. We define a function $\phi : \mathbb{P} \to \mathbb{N}$ as follows: For each $n \in \mathbb{P}$, we let $\phi(n)$ be the number of all $i \in \{1, 2, \ldots, n\}$ that are coprime to n. In other words,

$$\phi(n) = |\{i \in \{1, 2, \ldots, n\} \mid i \perp n\}|. \tag{55}$$

This function ϕ is called *Euler's totient function* or just *ϕ-function*.

Example 2.14.2. (a) We have $\phi(12) = 4$, since the number of all $i \in \{1, 2, \ldots, 12\}$ that are coprime to 12 is 4 (indeed, these i are 1, 5, 7 and 11).

(b) We have $\phi(13) = 12$, since the number of all $i \in \{1, 2, \ldots, 13\}$ that are coprime to 13 is 12 (indeed, these i are $1, 2, \ldots, 12$).

(c) We have $\phi(14) = 6$, since the number of all $i \in \{1, 2, \ldots, 14\}$ that are coprime to 14 is 6 (indeed, these i are $1, 3, 5, 9, 11, 13$).

(d) We have $\phi(1) = 1$, since the number of all $i \in \{1, 2, \ldots, 1\}$ that are coprime to 1 is 1 (indeed, the only such i is 1).

The ϕ-function ϕ is denoted by φ by some authors.

Proposition 2.14.3. Let p be a prime. Then, $\phi(p) = p - 1$.

Proof of Proposition 2.14.3. Here is the idea: The definition of ϕ shows that $\phi(p)$ is the number of all $i \in \{1, 2, \ldots, p\}$ that are coprime to p. But we know exactly what these i are: They are just the first $p - 1$ positive integers $1, 2, \ldots, p - 1$. (In fact, Proposition 2.13.4 shows that each of the integers $1, 2, \ldots, p - 1$ is coprime to p, whereas $\gcd(p, p) = p > 1$ shows that p is **not** coprime to p.) Thus, $\phi(p)$ is the number of these $p - 1$ integers; in other words, $\phi(p) = p - 1$.

For one last time, here is the proof in detail:

We have $p > 1$ (since p is a prime), thus $p \neq 1$. Also, $p \mid p$; hence, Proposition 2.9.7 **(i)** (applied to $a = p$ and $b = p$) yields $\gcd(p, p) = |p| = p$ (since $p > 1 > 0$).

Now, we claim that

$$\{i \in \{1, 2, \ldots, p\} \mid i \perp p\} \subseteq \{1, 2, \ldots, p - 1\}. \tag{56}$$

[*Proof of (56):* Let $i \in \{1, 2, \ldots, p\}$ be such that $i \perp p$. From $i \perp p$, we obtain $\gcd(i, p) = 1$. If we had $i = p$, then we would have $\gcd\left(\underbrace{i}_{=p}, p\right) = \gcd(p, p) = p \neq 1$, which would contradict $\gcd(i, p) = 1$. Thus, we cannot have $i = p$. Hence, we have $i \neq p$. Combining this with $i \in \{1, 2, \ldots, p\}$, we obtain $i \in \{1, 2, \ldots, p\} \setminus \{p\} = \{1, 2, \ldots, p - 1\}$.

Now, forget that we fixed i. We thus have proven that every $i \in \{1, 2, \ldots, p\}$ satisfying $i \perp p$ must belong to $\{1, 2, \ldots, p - 1\}$. In other words, $\{i \in \{1, 2, \ldots, p\} \mid i \perp p\} \subseteq \{1, 2, \ldots, p - 1\}$. This proves (56).]

Conversely, we have

$$\{1, 2, \ldots, p - 1\} \subseteq \{i \in \{1, 2, \ldots, p\} \mid i \perp p\}. \tag{57}$$

[*Proof of (57):* Let $j \in \{1, 2, \ldots, p - 1\}$. Thus, j is coprime to p (by Proposition 2.13.4, applied to $i = j$). In other words, $j \perp p$. Also, $j \in \{1, 2, \ldots, p - 1\} \subseteq \{1, 2, \ldots, p\}$. Hence, j is an $i \in \{1, 2, \ldots, p\}$ satisfying $i \perp p$. In other words, $j \in \{i \in \{1, 2, \ldots, p\} \mid i \perp p\}$.

Now, forget that we fixed j. We thus have shown that $j \in \{i \in \{1,2,\ldots,p\} \mid i \perp p\}$ for each $j \in \{1,2,\ldots,p-1\}$. In other words, $\{1,2,\ldots,p-1\} \subseteq \{i \in \{1,2,\ldots,p\} \mid i \perp p\}$. This proves (57).]

Combining (56) with (57), we obtain

$$\{i \in \{1,2,\ldots,p\} \mid i \perp p\} = \{1,2,\ldots,p-1\}.$$

Now, (55) (applied to $n = p$) yields

$$\phi(p) = \left| \underbrace{\{i \in \{1,2,\ldots,p\} \mid i \perp p\}}_{=\{1,2,\ldots,p-1\}} \right| = |\{1,2,\ldots,p-1\}| = p-1.$$

This proves Proposition 2.14.3. □

Proposition 2.14.3 can be generalized as follows:

Exercise 2.14.1. Let p be a prime. Let k be a positive integer. Prove that $\phi\left(p^k\right) = (p-1)\,p^{k-1}$.

Theorem 2.14.4. Let m and n be two coprime positive integers. Then, $\phi(mn) = \phi(m) \cdot \phi(n)$.

We will prove Theorem 2.14.4 later (in Section 2.16.3).

Theorem 2.14.5. Let n be a positive integer. Then,

$$\phi(n) = \prod_{\substack{p \text{ prime;} \\ p \mid n}} \left((p-1)\, p^{v_p(n)-1} \right) = n \cdot \prod_{\substack{p \text{ prime;} \\ p \mid n}} \left(1 - \frac{1}{p} \right).$$

Theorem 2.14.5 will be proven in Section 2.16.3.

Exercise 2.14.2. Let n be a positive integer.

(a) Prove that

$$n - \phi(n) = |\{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\}|.$$

(b) We have $n - \phi(n) \geq 0$.

(c) Let d be a positive divisor of n. Prove that $d - \phi(d) \leq n - \phi(n)$.

(d) Let d be a positive divisor of n such that $d \neq n$. Prove that $d - \phi(d) < n - \phi(n)$.

2.14.2. The totient sum theorem

Theorem 2.14.6. Let n be a positive integer. Then,

$$\sum_{d|n} \phi(d) = n.$$

Here and in the following, the symbol "$\sum\limits_{d|n}$" stands for "sum over all **positive** divisors d of n".

For example, for $n = 12$, Theorem 2.14.6 states that

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 12.$$

Before we prove Theorem 2.14.6, let us motivate an argument via a classical puzzle:

Exercise 2.14.3. You have a corridor with 1000 lamps, which are initially all off. Each lamp has a lightswitch controlling its state.

Every night, a ghost glides through the corridor (always in the same direction) and flips some of the switches:

On the 1st night, the ghost flips every switch.

On the 2nd night, the ghost flips switches $2, 4, 6, 8, 10, \ldots$.

On the 3rd night, the ghost flips switches $3, 6, 9, 12, 15, \ldots$.

etc.

(That is: For each $k \in \{1, 2, \ldots, 1000\}$, the ghost spends the k-th night flipping switches $k, 2k, 3k, \ldots$.)

Which lamps will be on after 1000 nights?

In more rigorous terms, Exercise 2.14.3 is simply asking which of the numbers $1, 2, \ldots, 1000$ have an odd number of positive divisors. (Indeed, the situation after 1000 nights looks as follows: For each $n \in \{1, 2, \ldots, 1000\}$, the n-th switch has been flipped exactly once for each positive divisor of n; thus, the n-th lamp is on if and only if n has an odd number of positive divisors.)

Experiments reveal that among the first 10 positive integers, only three have an odd number of positive divisors: namely, 1, 4 and 9. (For example, 9 has the 3 positive divisors 1, 3 and 9.) This suggests the following:

Proposition 2.14.7. A positive integer n has an odd number of positive divisors if and only if n is a perfect square.

Proof of Proposition 2.14.7. Fix a positive integer n. If d is a positive divisor of n, then n/d is a positive divisor of n as well[50]. This allows us to define a map

$$F : \{\text{positive divisors of } n\} \to \{\text{positive divisors of } n\}, \\ d \mapsto n/d.$$

This map F has the property that $F \circ F = \operatorname{id}$, because each $d \in \{\text{positive divisors of } n\}$ satisfies

$$\begin{aligned}(F \circ F)(d) &= F\left(\underbrace{\underbrace{F(d)}_{=n/d}}_{\text{(by the definition of } F)}\right) = F(n/d) \\ &= n/(n/d) \qquad \text{(by the definition of } F) \\ &= d = \operatorname{id}(d).\end{aligned}$$

Hence, the map F is inverse to itself. Thus, the map F is invertible, i.e., is a bijection.

For the rest of this proof, the word "divisor" shall mean "positive divisor of n". Thus, F is a map from $\{\text{divisors}\}$ to $\{\text{divisors}\}$.

The rough idea from here on is the following:[51] The map F "pairs up" each divisor d with the divisor $F(d) = n/d$. Thus, the divisors are "grouped into pairs", except for those that satisfy $d = n/d$ (because these would have to be paired up with themselves). When n is not a perfect square, there are no such "exceptional" divisors, since $d = n/d$ means $n = d^2$. When n is a perfect square, there is exactly one such "exceptional" divisor, namely $\sqrt{n}$. So the number of divisors is even if n is not a perfect square, and odd otherwise (because clearly, all the pairs have no effect on the parity of the total number of divisors, and thus can be forgotten). In other words, n has an odd number of positive divisors if and only if n is a perfect square.

There are several ways to make this argument rigorous; here is the easiest (though perhaps the least instructive one): A divisor d shall be called

- *small* if $d < n/d$;
- *medium* if $d = n/d$;
- *large* if $d > n/d$.

[50] *Proof.* Let d be a positive divisor of n. Thus, d is a positive integer satisfying $d \mid n$. But Proposition 2.2.3 **(c)** (applied to $a = d$ and $b = n$) yields that $d \mid n$ if and only if $\frac{n}{d} \in \mathbb{Z}$ (since $d \neq 0$). Hence, $\frac{n}{d} \in \mathbb{Z}$ (since $d \mid n$). In other words, $n/d \in \mathbb{Z}$. Moreover, n/d is positive (since n and d are positive).

So n/d is a positive integer (since $n/d \in \mathbb{Z}$) and is a divisor of n (since $n = (n/d) \cdot d$). Hence, n/d is a positive divisor of n. Qed.

[51] We shall give a more rigorous proof shortly.

It is easy to see that if d is a small divisor, then $F(d)$ is a large divisor[52]. Hence, the map

$$F^{+} : \{\text{small divisors}\} \to \{\text{large divisors}\},$$
$$d \mapsto F(d)$$

is well-defined. Similarly, the map

$$F^{-} : \{\text{large divisors}\} \to \{\text{small divisors}\},$$
$$d \mapsto F(d)$$

is well-defined. These two maps F^{+} and F^{-} are both restrictions of the map F, and thus are mutually inverse (since the map F is inverse to itself). Hence, the map F^{+} is invertible, i.e., is a bijection. Thus, we have found a bijection from $\{\text{small divisors}\}$ to $\{\text{large divisors}\}$ (namely, F^{+}). Therefore,

$$|\{\text{small divisors}\}| = |\{\text{large divisors}\}|. \tag{58}$$

On the other hand, let us take a look at medium divisors. If d is a medium divisor, then $d = n/d$ (by the definition of "medium"), so that $d^2 = n$ and thus n must be a perfect square. Thus, if n is **not** a perfect square, then there are no medium divisors. In other words, if n is **not** a perfect square, then

$$|\{\text{medium divisors}\}| = 0. \tag{59}$$

But if n **is** a perfect square, then n has exactly one medium divisor[53]. In other words, if n **is** a perfect square, then

$$|\{\text{medium divisors}\}| = 1. \tag{60}$$

But each divisor is either small or medium or large, and there are no overlaps between these three classes (i.e., a divisor cannot be small and medium at the same time, or small and large, or medium and large). Thus, in order to count the number of all divisors, we can add the number of small divisors, the number of medium divisors and the number of

[52] *Proof.* Let d be a small divisor. Thus, $d < n/d$. Hence, $n/d > d = n/(n/d)$. In view of $F(d) = n/d$, this rewrites as $F(d) > n/(F(d))$. In other words, $F(d)$ is a large divisor (by the definition of "large divisor"). Qed.

[53] *Proof.* Assume that n is a perfect square. Thus, $n = w^2$ for some $w \in \mathbb{Z}$. Consider this w. Clearly, $w \neq 0$ (since $ww = w^2 = n \neq 0$), so that $|w| > 0$.

Let $u = |w|$. Thus, $u \in \mathbb{Z}$ (since $w \in \mathbb{Z}$). Hence, u is a positive integer (since $u = |w| > 0$). Moreover, from $u = |w|$, we obtain $u^2 = |w|^2 = w^2 = n$. Hence, $u = n/u$.

This positive integer u satisfies $uu = u^2 = n$ and thus $u \mid n$. Hence, u is a positive divisor of n (that is, a divisor, as we call it). This divisor u is medium, since it satisfies $u = n/u$.

Moreover, if d is any medium divisor, then $d = n/d$ (by the definition of "medium"), thus $d^2 = n = u^2$, thus $\sqrt{d^2} = \sqrt{u^2} = |u| = u$ (since u is positive), thus $u = \sqrt{d^2} = |d| = d$ (since d is positive) and therefore $d = u$. In other words, any medium divisor must equal u. This shows that u is the **only** medium divisor (since we already know that u is a medium divisor). Hence, n has exactly one medium divisor.

large divisors. In other words:

$$\begin{aligned}
\left|\{\text{divisors}\}\right| &= \underbrace{\left|\{\text{small divisors}\}\right|}_{\substack{=\left|\{\text{large divisors}\}\right| \\ \text{(by (58))}}} + \left|\{\text{medium divisors}\}\right| + \left|\{\text{large divisors}\}\right| \\
&= \left|\{\text{large divisors}\}\right| + \left|\{\text{medium divisors}\}\right| + \left|\{\text{large divisors}\}\right| \\
&= \underbrace{2 \cdot \left|\{\text{large divisors}\}\right|}_{\equiv 0 \operatorname{mod} 2} + \left|\{\text{medium divisors}\}\right| \\
&\equiv \left|\{\text{medium divisors}\}\right| \operatorname{mod} 2.
\end{aligned}$$

Hence, if n is **not** a perfect square, then

$$\left|\{\text{divisors}\}\right| \equiv \left|\{\text{medium divisors}\}\right| = 0 \operatorname{mod} 2$$

(by (59)). In other words, if n is **not** a perfect square, then the number of divisors is even.

On the other hand, if n **is** a perfect square, then

$$\left|\{\text{divisors}\}\right| \equiv \left|\{\text{medium divisors}\}\right| = 1 \operatorname{mod} 2$$

(by (60)). In other words, if n **is** a perfect square, then the number of divisors is odd.

Combining the results of the previous two paragraphs, we conclude that the number of divisors is odd if n is a perfect square, and is even otherwise. In other words, n has an odd number of positive divisors if and only if n is a perfect square. This proves Proposition 2.14.7. □

Having proven Proposition 2.14.7, we now can answer Exercise 2.14.3: The 31 lamps $1^2, 2^2, \ldots, 31^2$ (and no others) will be on after the 1000 nights. (Indeed, these 31 lamps correspond to the 31 perfect squares in the set $\{1, 2, \ldots, 1000\}$.)

The bijection F from the proof of Proposition 2.14.7 will serve us well in our proof of Theorem 2.14.6. Beside that, we need the following lemma:

Lemma 2.14.8. Let n be a positive integer. Let d be a positive divisor of n. Then,

$$(\text{the number of } i \in \{1, 2, \ldots, n\} \text{ such that } \gcd(i, n) = d) = \phi(n/d).$$

Proof of Lemma 2.14.8. We have $d \mid n$ (since d is a divisor of n) and $d \neq 0$ (since d is positive). Thus, Proposition 2.2.3 **(c)** (applied to d and n instead of a and b) yields that $d \mid n$ if and only if $\frac{n}{d} \in \mathbb{Z}$. Thus, $\frac{n}{d} \in \mathbb{Z}$ (since $d \mid n$). In other words, $n/d \in \mathbb{Z}$. Thus, n/d is an integer. This integer n/d is positive (since n and d are positive). Hence, $\phi(n/d)$ is well-defined.

Define two sets I and J by

$$I = \{i \in \{1, 2, \ldots, n\} \mid \gcd(i, n) = d\} \qquad (61)$$

and

$$J = \{i \in \{1, 2, \ldots, n/d\} \mid i \perp n/d\}. \qquad (62)$$

But (55) (applied to n/d instead of n) yields

$$\phi\left(n/d\right) = \left|\left\{i \in \left\{1,2,\ldots,n/d\right\} \ \mid \ i \perp n/d\right\}\right| = \left|J\right| \tag{63}$$

(since $\left\{i \in \left\{1,2,\ldots,n/d\right\} \ \mid \ i \perp n/d\right\} = J$).

We shall next construct a bijection from I to J (which will show that $|I| = |J|$).

For each $a \in I$, we have $a/d \in J$ [54]. Hence, we can define a map

$$f : I \to J, \qquad a \mapsto a/d.$$

For each $b \in J$, we have $bd \in I$ [55]. Thus, we can define a map

$$g : J \to I, \qquad b \mapsto bd.$$

[54] *Proof.* Let $a \in I$. Thus, $a \in I = \left\{i \in \left\{1,2,\ldots,n\right\} \ \mid \ \gcd\left(i,n\right) = d\right\}$. In other words, a is an element of $\left\{1,2,\ldots,n\right\}$ satisfying $\gcd\left(a,n\right) = d$.

Thus, $d = \gcd\left(a,n\right) \mid a$. But Proposition 2.2.3 **(c)** (applied to d and a instead of a and b) yields that $d \mid a$ if and only if $\dfrac{a}{d} \in \mathbb{Z}$. Thus, $\dfrac{a}{d} \in \mathbb{Z}$ (since $d \mid a$). In other words, $a/d \in \mathbb{Z}$. Also, $a \in \left\{1,2,\ldots,n\right\}$, so that $0 < a \leq n$. We can divide this chain of inequalities by d (since d is positive), and thus obtain $0 < a/d \leq n/d$. Hence, $a/d \in \left\{1,2,\ldots,n/d\right\}$ (since $a/d \in \mathbb{Z}$). Furthermore, Theorem 2.9.20 (applied to d, a/d and n/d instead of s, a and b) yields

$$\gcd\left(d\left(a/d\right), d\left(n/d\right)\right) = \underbrace{|d|}_{\substack{=d \\ \text{(since } d \text{ is positive)}}} \gcd\left(a/d, n/d\right) = d\gcd\left(a/d, n/d\right).$$

Solving this for $\gcd\left(a/d, n/d\right)$, we obtain

$$\gcd\left(a/d, n/d\right) = \frac{1}{d}\gcd\left(\underbrace{d\left(a/d\right)}_{=a}, \underbrace{d\left(n/d\right)}_{=n}\right) = \frac{1}{d}\underbrace{\gcd\left(a,n\right)}_{=d} = \frac{1}{d}d = 1.$$

In other words, $a/d \perp n/d$.

So we know that a/d is an element of $\left\{1,2,\ldots,n/d\right\}$ satisfying $a/d \perp n/d$. In other words, $a/d \in \left\{i \in \left\{1,2,\ldots,n/d\right\} \ \mid \ i \perp n/d\right\} = J$. Qed.

[55] *Proof.* Let $b \in J$. Thus, $b \in J = \left\{i \in \left\{1,2,\ldots,n/d\right\} \ \mid \ i \perp n/d\right\}$. In other words, b is an element of $\left\{1,2,\ldots,n/d\right\}$ satisfying $b \perp n/d$.

From $b \in \left\{1,2,\ldots,n/d\right\} \subseteq \mathbb{Z}$ and $d \in \mathbb{Z}$, we obtain $bd \in \mathbb{Z}$. From $b \in \left\{1,2,\ldots,n/d\right\}$, we obtain $0 < b \leq n/d$. We can multiply this chain of inequalities by d (since d is positive), and thus obtain $0 < bd \leq n$. Thus, $bd \in \left\{1,2,\ldots,n\right\}$ (since $bd \in \mathbb{Z}$). Theorem 2.9.20 (applied to d, b and n/d instead of s, a and b) yields

$$\gcd\left(db, d\left(n/d\right)\right) = \underbrace{|d|}_{\substack{=d \\ \text{(since } d \text{ is positive)}}} \underbrace{\gcd\left(b, n/d\right)}_{\substack{=1 \\ \text{(since } b \perp n/d\text{)}}} = d.$$

Thus, $d = \gcd\left(\underbrace{db}_{=bd}, \underbrace{d\left(n/d\right)}_{=n}\right) = \gcd\left(bd, n\right)$, so that $\gcd\left(bd,n\right) = d$.

So we know that bd is an element of $\left\{1,2,\ldots,n\right\}$ satisfying $\gcd\left(bd,n\right) = d$. In other words, $bd \in \left\{i \in \left\{1,2,\ldots,n\right\} \ \mid \ \gcd\left(i,n\right) = d\right\} = I$, qed.

The two maps f and g are mutually inverse (since the map f divides its input by d, while the map g multiplies its input by d). Hence, f is invertible, i.e., is a bijection. Thus, there exists a bijection from I to J (namely, f). Hence, $|I| = |J| = \phi(n/d)$ (by (63)). Thus,

$$\begin{aligned} \phi(n/d) &= |I| = |\{i \in \{1,2,\ldots,n\} \mid \gcd(i,n) = d\}| \qquad \text{(by (61))} \\ &= (\text{the number of } i \in \{1,2,\ldots,n\} \text{ such that } \gcd(i,n) = d). \end{aligned}$$

This proves Lemma 2.14.8. □

Proof of Theorem 2.14.6. Consider the map F we defined in the proof of Proposition 2.14.7. This map F is a bijection (as we have seen back in that proof). In other words, the map

$$\{\text{positive divisors of } n\} \to \{\text{positive divisors of } n\}, \quad d \mapsto n/d$$

is a bijection (since this is precisely the map F). Thus, we can substitute n/d for d in the sum $\sum_{d|n} \phi(d)$ (and, more generally, in any sum that ranges over all positive divisors d of n). We thus obtain

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi(n/d). \tag{64}$$

But

$$\begin{aligned} n &= |\{1,2,\ldots,n\}| = (\text{the number of } i \in \{1,2,\ldots,n\}) \\ &= \sum_{d|n} \underbrace{(\text{the number of } i \in \{1,2,\ldots,n\} \text{ such that } \gcd(i,n) = d)}_{\substack{=\phi(n/d) \\ \text{(by Lemma 2.14.8)}}} \\ &\qquad (\text{because if } i \in \{1,2,\ldots,n\}, \text{ then } \gcd(i,n) \text{ is a positive divisor of } n) \\ &= \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d) \qquad \text{(by (64))}. \end{aligned}$$

This proves Theorem 2.14.6. □

Exercise 2.14.4. Let $n \in \mathbb{N}$ satisfy $n > 2$. Prove that $\phi(n)$ is even.

Exercise 2.14.5. Let $n \in \mathbb{N}$ satisfy $n > 1$. Prove that

$$\sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i \perp n}} i = n\phi(n)/2.$$

2.15. Fermat, Euler, Wilson

2.15.1. Fermat and Euler: statements

The following theorem is known as *Fermat's Little Theorem* (often abbreviated as "FLT"):

Theorem 2.15.1. Let p be a prime. Let $a \in \mathbb{Z}$.
(a) If $p \nmid a$, then $a^{p-1} \equiv 1 \operatorname{mod} p$.
(b) We always have $a^p \equiv a \operatorname{mod} p$.

The word "little" in the name of Theorem 2.15.1 is meant to distinguish the theorem from "Fermat's Last Theorem", a much more difficult result only proven in the 1990s. (Unfortunately, the latter result is also abbreviated as "FLT".)

We will prove Theorem 2.15.1 soon, by showing a more general result (Theorem 2.15.3). But before we do so, let us convince ourselves that the parts **(a)** and **(b)** of Theorem 2.15.1 are equivalent:

Remark 2.15.2. Theorem 2.15.1 **(b)** follows from Theorem 2.15.1 **(a)**, because (using the notations of Theorem 2.15.1):

- If $p \nmid a$, then Theorem 2.15.1 **(a)** yields $a^{p-1} \equiv 1 \operatorname{mod} p$, thus $a^p = a \underbrace{a^{p-1}}_{\equiv 1 \operatorname{mod} p} \equiv a1 = a \operatorname{mod} p$.
- If $p \mid a$, then both a^p and a are $\equiv 0 \operatorname{mod} p$ (because $p \mid a$ entails $a \equiv 0 \operatorname{mod} p$ and thus $a^p \equiv 0^p = 0 \operatorname{mod} p$ (since $p > 0$)), and therefore $a^p \equiv 0 \equiv a \operatorname{mod} p$.

Conversely, Theorem 2.15.1 **(a)** follows from Theorem 2.15.1 **(b)** by the following argument: Let p and a be as in Theorem 2.15.1. Assume that $p \nmid a$. Then, $p \perp a$ (by Proposition 2.13.5), so that $a \perp p$. Thus, we can "cancel" a from any congruence modulo p (by Lemma 2.10.10). Doing this to the congruence $a^p \equiv a \operatorname{mod} p$ (which follows from Theorem 2.15.1 **(b)**), we obtain $a^{p-1} \equiv 1 \operatorname{mod} p$.

The next result is known as *Euler's theorem*:

Theorem 2.15.3. Let n be a positive integer. Let $a \in \mathbb{Z}$ be coprime to n.
Then, $a^{\phi(n)} \equiv 1 \operatorname{mod} n$.

Theorem 2.15.3 yields Theorem 2.15.1 **(a)**, since $\phi(p) = p - 1$ when p is prime[56]. Since we also know that Theorem 2.15.1 **(b)** follows from Theorem 2.15.1 **(a)**, we see that a proof of Theorem 2.15.3 will immediately yield the whole Theorem 2.15.1. Before we give said proof, let us show an example of how Theorem 2.15.3 can be used:

[56] See below for details of this argument.

> **Exercise 2.15.1.** What is the last digit of 3^{4^5}?
>
> *Notational remark:* An expression of the form "a^{b^c}" always means $a^{\left(b^c\right)}$, not $\left(a^b\right)^c$. (Actually, there is no need for an extra notation for $\left(a^b\right)^c$, because $\left(a^b\right)^c = a^{bc}$.)

Solution to Exercise 2.15.1 (sketched). The last digit of a positive integer n is $n\%10$ (that is, the remainder of n upon division by 10). So we need to work modulo 10.

Since 3 is coprime to 10, we can apply Theorem 2.15.3 to $n = 10$ and $a = 3$. We thus get $3^{\phi(10)} \equiv 1 \operatorname{mod} 10$. Since $\phi(10) = 4$, this rewrites as $3^4 \equiv 1 \operatorname{mod} 10$. Now, $4^5 = 4 \cdot 4^4$, so that

$$3^{4^5} = 3^{4 \cdot 4^4} = \left(\underbrace{3^4}_{\equiv 1 \operatorname{mod} 10}\right)^{4^4} \equiv 1^{4^4} = 1 \operatorname{mod} 10.$$

So the last digit of 3^{4^5} is 1. □

Theorem 2.15.3 is also the reason why certain rational numbers (such as $\dfrac{2}{7} = 0.\overline{285714}$ [57]) have purely periodic decimal expansions, while others (such as $\dfrac{1}{12} = 0.08\overline{3} = 0.0833333\ldots$ or $\dfrac{1}{2} = 0.5\overline{0} = 0.50000\ldots$) have their periods start only after some initial nonrepeating block. We refer [ConradE, §4] to the details of this.[58]

2.15.2. Proving Euler and Fermat

Our proof of Theorem 2.15.3 will rely on the following lemma:

> **Lemma 2.15.4.** Let n be a positive integer. Then,
>
> $$\phi(n) = \left|\left\{i \in \{0, 1, \ldots, n-1\} \mid i \perp n\right\}\right|.$$

First proof of Lemma 2.15.4 (sketched). If $n = 1$, then this lemma can easily be proven by hand. Thus, WLOG assume that $n \neq 1$. Hence, $n > 1$ (since n is a positive

[57] The bar ($\overline{}$) over the "285714" means that we are repeating 285714 over and over. So $0.\overline{285714} = 0.285714285714285714\ldots$.

[58] In brief, the rule is as follows: Any fraction $\dfrac{a}{b}$ with $a, b \in \mathbb{Z}$ (and $b \neq 0$) has such a decimal representation with a period. (A *period* means a part that gets repeated over and over.) A fraction $\dfrac{a}{b}$ is called *purely periodic* if its period (in decimal notation) begins straight after the decimal point. So $\dfrac{2}{7}$ is purely periodic but $\dfrac{1}{12}$ and $\dfrac{1}{2}$ are not. Now, the answer is that a fraction $\dfrac{a}{b}$ (with $a \perp b$) is purely periodic if and only if $b \perp 10$ (in other words, $2 \nmid b$ and $5 \nmid b$). This can be proven using Theorem 2.15.3.

integer). Thus, neither 0 nor n is coprime to n (since $\gcd(0,n) = n > 1$ and $\gcd(n,n) = n > 1$). Hence,

$$\{i \in \{0,1,\ldots,n-1\} \mid i \perp n\} = \{i \in \{1,2,\ldots,n\} \mid i \perp n\}$$

(because these sets could only differ in the elements 0 and n, but none of these two elements belongs to any of these two sets[59]), and therefore

$$|\{i \in \{0,1,\ldots,n-1\} \mid i \perp n\}| = |\{i \in \{1,2,\ldots,n\} \mid i \perp n\}| = \phi(n)$$

(by (55)). This proves Lemma 2.15.4. □

Second proof of Lemma 2.15.4. We have $n \mid n$ and thus $n \equiv 0 \mod n$. Hence, Proposition 2.9.7 **(d)** (applied to $a = n$, $b = n$ and $c = 0$) yields that $\gcd(n,n) = \gcd(n,0) = \gcd(0,n)$ (by Proposition 2.9.7 **(b)**). Hence, $\gcd(0,n) = 1$ holds if and only if $\gcd(n,n) = 1$. In other words, the number 0 is coprime to n if and only if n is coprime to n. Hence, if we remove n from the set $\{1,2,\ldots,n\}$ and add 0 instead (so that our set becomes $\{0,1,\ldots,n-1\}$), then the number of elements coprime to n in that set does not change. In other words,

$$\begin{aligned}
&(\text{the number of all } i \in \{0,1,\ldots,n-1\} \text{ that are coprime to } n) \\
&= (\text{the number of all } i \in \{1,2,\ldots,n\} \text{ that are coprime to } n) \\
&= |\{i \in \{1,2,\ldots,n\} \mid i \perp n\}| = \phi(n) \qquad (\text{by (55)}).
\end{aligned}$$

In other words,

$$\begin{aligned}
\phi(n) &= (\text{the number of all } i \in \{0,1,\ldots,n-1\} \text{ that are coprime to } n) \\
&= |\{i \in \{0,1,\ldots,n-1\} \mid i \perp n\}|.
\end{aligned}$$

This proves Lemma 2.15.4 again. □

Proof of Theorem 2.15.3. Let

$$C = \{i \in \{0,1,\ldots,n-1\} \mid i \perp n\}.$$

Then, Lemma 2.15.4 says that $\phi(n) = |C|$.

Now, set

$$z = \prod_{i \in C} i. \tag{65}$$

Exercise 2.10.5 (applied to $I = C$, $c = n$ and $b_i = i$) yields $\prod_{i \in C} i \perp n$ (since each $i \in C$ satisfies $i \perp n$). In other words, $z \perp n$ (since $z = \prod_{i \in C} i$).

We have $(ai)\,\%n \in C$ for each $i \in C$.

[*Proof:* Let $i \in C$. Corollary 2.6.9 **(a)** (applied to $u = ai$) yields that $(ai)\,\%n \in \{0,1,\ldots,n-1\}$ and $(ai)\,\%n \equiv ai \mod n$. Thus, $ai \equiv (ai)\,\%n \mod n$.

[59] since neither 0 nor n is coprime to n

From $a \perp n$ and $i \perp n$, we obtain $ai \perp n$ (by Theorem 2.10.9, applied to i and n instead of b and c). Hence, Exercise 2.10.6 (applied to ai, $(ai) \% n$ and n instead of a, b and c) yields $(ai) \% n \perp n$ (since $ai \equiv (ai) \% n \mod n$). Combining this with $(ai) \% n \in \{0, 1, \ldots, n-1\}$, we obtain $(ai) \% n \in C$ (by the definition of C), qed.]

Thus, we can define a map

$$f : C \to C,$$
$$i \mapsto (ai) \% n.$$

The map f is injective.

[*Proof:* Let i and j be two elements of C such that $f(i) = f(j)$. We must prove that $i = j$.

We have $f(i) = f(j)$. In view of $f(i) = (ai) \% n$ (by the definition of f) and $f(j) = (aj) \% n$, this rewrites as $(ai) \% n = (aj) \% n$. But Exercise 2.6.1 (applied to $u = ai$ and $v = aj$) shows that $ai \equiv aj \mod n$ if and only if $(ai) \% n = (aj) \% n$. Hence, we have $ai \equiv aj \mod n$ (since $(ai) \% n = (aj) \% n$). By Lemma 2.10.10, we can "cancel" a from this congruence (since $a \perp n$), and obtain $i \equiv j \mod n$. But both i and j belong to C and thus belong to $\{0, 1, \ldots, n-1\}$ (by the definition of C). Hence, from $i \equiv j \mod n$, we can easily obtain that $i = j$ [60].

Now, forget that we fixed i and j. We thus have proven that if i and j and two elements of C such that $f(i) = f(j)$, then $i = j$. In other words, f is injective.]

The map f is surjective.

[*Proof:* Let $i \in C$. We shall prove that $i \in f(C)$.

Indeed, $i \in C$. By the definition of C, this means that $i \in \{0, 1, \ldots, n-1\}$ and $i \perp n$.

But Proposition 2.10.8 **(b)** shows that there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \mod n$ (since $a \perp n$). Consider this a', and denote it by u. Thus, u is an element of $\mathbb{Z}$ and satisfies $au \equiv 1 \mod n$. From $ua = au \equiv 1 \mod n$, we conclude that there exists an $u' \in \mathbb{Z}$ such that $uu' \equiv 1 \mod n$ (namely, $u' = a$). Hence, Theorem 2.10.8 **(c)** (applied to u and u' instead of a and a') shows that $u \perp n$.

Now, Corollary 2.6.9 **(a)** (applied to ui instead of u) shows that $(ui) \% n \in \{0, 1, \ldots, n-1\}$ and $(ui) \% n \equiv ui \mod n$. Set $j = (ui) \% n$. Thus, $j = (ui) \% n \in \{0, 1, \ldots, n-1\}$ and $j = (ui) \% n \equiv ui \mod n$. Multiplying the congruences $a \equiv a \mod n$ and $j \equiv ui \mod n$, we obtain

$$aj \equiv \underbrace{au}_{\equiv 1 \mod n} i \equiv 1i = i \mod n.$$

In other words, $i \equiv aj \mod n$. Therefore, Corollary 2.6.9 **(c)** (applied to aj and i instead of u and c) yields $i = (aj) \% n$ (since $i \in \{0, 1, \ldots, n-1\}$).

Combining $u \perp n$ with $i \perp n$, we obtain $ui \perp n$ (by Theorem 2.10.9, applied to u, i and n instead of a, b and c). Also, $ui \equiv j \mod n$ (since $j \equiv ui \mod n$). Hence,

[60] *Proof.* Corollary 2.6.9 **(c)** (applied to $u = j$ and $c = i$) yields $i = j\%n$ (since $i \equiv j \mod n$ and $i \in \{0, 1, \ldots, n-1\}$). But Corollary 2.6.9 **(c)** (applied to $u = j$ and $c = j$) yields $j = j\%n$ (since $j \equiv j \mod n$ and $j \in \{0, 1, \ldots, n-1\}$). Hence, $i = j\%n = j$.

Exercise 2.10.6 (applied to ui, j and n instead of a, b and c) yields $j \perp n$. From $j \in \{0, 1, \ldots, n-1\}$ and $j \perp n$, we obtain $j \in C$ (by the definition of C). Thus, $f(j)$ is well-defined. The definition of f yields $f(j) = (aj)\,\%n = i$ (since $i = (aj)\,\%n$). Hence, $i = f\left(\underbrace{j}_{\in C}\right) \in f(C)$.

Now, forget that we fixed i. We thus have proven that $i \in f(C)$ for each $i \in C$. In other words, $C \subseteq f(C)$. In other words, the map f is surjective.]

Now we know that the map f is injective and surjective. Hence, this map f is bijective. In other words, f is a bijection from C to C. Thus, we can substitute $f(s)$ for i in the product $\prod\limits_{i \in C} i$. So we obtain

$$\prod_{i \in C} i = \prod_{s \in C} f(s). \tag{66}$$

But for each $s \in C$, we have

$$\begin{aligned} f(s) &= (as)\,\%n && \text{(by the definition of } f\text{)} \\ &\equiv as \mod n && \text{(by Corollary 2.6.9 \textbf{(a)}, applied to } u = as\text{)}. \end{aligned}$$

Hence, (9) (applied to $S = C$, $a_s = f(s)$ and $b_s = as$) yields

$$\prod_{s \in C} f(s) \equiv \prod_{s \in C} (as) = a^{|C|} \underbrace{\prod_{s \in C} s}_{\substack{= \prod\limits_{i \in C} i = z \\ \text{(by (65))}}} = a^{|C|} z = a^{\phi(n)} z \mod n$$

(since $|C| = \phi(n)$). Now, (65) becomes

$$\begin{aligned} z = \prod_{i \in C} i &= \prod_{s \in C} f(s) && \text{(by (66))} \\ &\equiv a^{\phi(n)} z = z a^{\phi(n)} \mod n. \end{aligned}$$

Thus, $z \cdot 1 = z \equiv z a^{\phi(n)} \mod n$. Lemma 2.10.10 lets us "cancel" z from this congruence (since $z \perp n$). We thus obtain $1 \equiv a^{\phi(n)} \mod n$. This proves Theorem 2.15.3. □

Proof of Theorem 2.15.1. As we have explained above, Theorem 2.15.1 follows from Theorem 2.15.3.

Here is the argument in more detail:

(a) Assume that $p \nmid a$. Proposition 2.14.3 yields $\phi(p) = p - 1$. But Proposition 2.13.5 yields that either $p \mid a$ or $p \perp a$. Hence, $p \perp a$ (since $p \nmid a$). In other words, $a \perp p$. In other words, a is coprime to p. Hence, Theorem 2.15.3 (applied to $n = p$) yields $a^{\phi(p)} \equiv 1 \mod p$. This rewrites as $a^{p-1} \equiv 1 \mod p$ (since $\phi(p) = p - 1$). This proves Theorem 2.15.1 **(a)**.

(b) We are in one of the following two cases:

Case 1: We have $p \nmid a$.

Case 2: We have $p \mid a$.

Let us first consider Case 1. In this case, we have $p \nmid a$. Hence, Theorem 2.15.1 **(a)** yields $a^{p-1} \equiv 1 \mod p$. Multiplying this congruence with the congruence $a \equiv a \mod p$, we obtain $a^{p-1}a \equiv 1a = a \mod p$. In view of $a^{p-1}a = a^p$, this rewrites as $a^p \equiv a \mod p$. Hence, Theorem 2.15.1 **(b)** is proven in Case 1.

Let us now consider Case 2. In this case, we have $p \mid a$. In other words, $a \equiv 0 \mod p$. Taking this congruence to the p-th power, we obtain $a^p \equiv 0^p = 0 \mod p$ (since $p > 0$). Thus, $a^p \equiv 0 \equiv a \mod p$ (since $a \equiv 0 \mod p$). Hence, Theorem 2.15.1 **(b)** is proven in Case 2.

We have now proven Theorem 2.15.1 **(b)** in both Cases 1 and 2. Hence, Theorem 2.15.1 **(b)** always holds. □

The next exercise shows an amusing (and useful) corollary of Fermat's Little Theorem: a situation in which congruent exponents lead to congruent powers (albeit under rather specific conditions, and with the congruent powers being congruent modulo a different number than the exponents):

Exercise 2.15.2. Let p be a prime. Let $a \in \mathbb{Z}$ be such that $p \nmid a$. Let $u, v \in \mathbb{N}$ satisfy $u \equiv v \mod p - 1$. Then, $a^u \equiv a^v \mod p$.

2.15.3. The Pigeonhole Principles

In our above proof of Theorem 2.15.3, we have proven that the map $f : C \to C$ (that we constructed) is injective and surjective. It turns out that this was, to some extent, wasteful: It would have been enough to prove one of the two properties only (i.e., injectivity **or** surjectivity). The reason for this are the following two basic facts about finite sets:

Theorem 2.15.5 (Pigeonhole Principle for Injections)**.** Let A and B be two finite sets such that $|A| \geq |B|$. Let $f : A \to B$ be an injective map. Then, f is bijective.

Theorem 2.15.6 (Pigeonhole Principle for Surjections)**.** Let A and B be two finite sets such that $|A| \leq |B|$. Let $f : A \to B$ be an surjective map. Then, f is bijective.

Theorem 2.15.5 is called the *Pigeonhole Principle for Injections*, due to the following interpretation: If a pigeons sit in b pigeonholes with $a \geq b$ (that is, there are at least as many pigeons as there are pigeonholes), and if no two pigeons are sharing the same hole, then every hole must have at least one pigeon in it. (This corresponds to the statement of Theorem 2.15.5 if you let A be the set of pigeons, B be the set of holes, and f be the map that sends each pigeon to the hole it is sitting in. The injectivity of f is then precisely the statement that no two pigeons are sharing the same hole.)

Likewise, Theorem 2.15.6 is called the *Pigeonhole Principle for Surjections*, due to the following interpretation: If a pigeons sit in b pigeonholes with $a \leq b$ (that is, there are at most as many pigeons as there are pigeonholes), and if each hole contains at least one pigeon, then no two pigeons are sharing the same hole.

Theorem 2.15.5 and Theorem 2.15.6 are both basic facts of set theory; how to prove them depends on how you define the size of a finite set in the first place. See [Grinbe15, solution to Exercise 1.1] for one way of proving them (more precisely, Theorem 2.15.5 is the "$\Longrightarrow$" direction of [Grinbe15, Lemma 1.5], while Theorem 2.15.6 is the "$\Longrightarrow$" direction of [Grinbe15, Lemma 1.4]).

Now, Theorem 2.15.5 can be used to simplify our above proof of Theorem 2.15.3. Indeed, in the latter proof, once we have shown that f is injective, we can immediately apply Theorem 2.15.5 (to $A = C$ and $B = C$) in order to conclude that f is bijective (since C is a finite set and satisfies $|C| \geq |C|$). The proof of surjectivity of f is thus unnecessary. Alternatively, we could have omitted the proof of injectivity of f, and instead used the surjectivity of f to apply Theorem 2.15.6 (to $A = C$ and $B = C$) in order to conclude that f is bijective (since C is a finite set and satisfies $|C| \leq |C|$). Either way, we would have obtained a shorter proof.

2.15.4. Wilson

The next theorem is known as *Wilson's theorem*:

Theorem 2.15.7. Let p be a prime. Then, $(p-1)! \equiv -1 \mod p$.

We shall prove Theorem 2.15.7 using modular inverses modulo p. The main idea is that we can "pair up" each factor in the product $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ with its modular inverse modulo p, where of course we take the unique modular inverse that belongs to the set $\{1, 2, \ldots, p-1\}$. This relies on the following lemma:

Lemma 2.15.8. Let p be a prime. Set $A = \{1, 2, \ldots, p-1\}$.

(a) If a_1 and a_2 are two elements of A satisfying $a_1 \equiv a_2 \mod p$, then $a_1 = a_2$.

(b) For each $a \in A$, there exists a unique $a' \in A$ satisfying $aa' \equiv 1 \mod p$.

(c) Define a map $J : A \to A$ as follows: For each $a \in A$, we let $J(a)$ denote the unique $a' \in A$ satisfying $aa' \equiv 1 \mod p$. (This unique a' indeed exists, by Lemma 2.15.8 **(b)**.)

Then, this map J is a bijection satisfying $J \circ J = \mathrm{id}$.

Proof of Lemma 2.15.8. **(a)** Let a_1 and a_2 be two elements of A satisfying $a_1 \equiv a_2 \mod p$. We must prove that $a_1 = a_2$.

We have $a_1 \equiv a_2 \mod p$. Hence, Corollary 2.6.9 **(c)** (applied to p, a_2 and a_1 instead of n, u and c) yields $a_1 = a_2 \% p$ (since $a_1 \in A = \{1, 2, \ldots, p-1\} \subseteq \{0, 1, \ldots, p-1\}$). Also, $a_2 \equiv a_2 \mod p$. Thus, Corollary 2.6.9 **(c)** (applied to p, a_2 and a_2 instead of n, u and c) yields $a_2 = a_2 \% p$ (since $a_2 \in A = \{1, 2, \ldots, p-1\} \subseteq \{0, 1, \ldots, p-1\}$). Comparing this with $a_1 = a_2 \% p$, we obtain $a_1 = a_2$. This proves Lemma 2.15.8 **(a)**.

(b) Let $a \in A$. Thus, $a \in A = \{1, 2, \ldots, p-1\}$. Hence, Proposition 2.13.4 (applied to $i = a$) shows that a is coprime to p. In other words, $a \perp p$. Hence, Theorem 2.10.8 **(a)** shows that there exists a $b \in \mathbb{Z}$ such that $ab \equiv \gcd(a, p) \mod p$. Consider this b.

We have $ab \equiv \gcd(a,p) = 1 \mod p$ (since $a \perp p$). Let $c = b\%p$. Corollary 2.6.9 **(a)** (applied to $n = p$ and $u = b$) yields $b\%p \in \{0,1,\ldots,p-1\}$ and $b\%p \equiv b \mod p$. Now, $c = b\%p \in \{0,1,\ldots,p-1\}$ and $a \underbrace{c}_{=b\%p\equiv b \mod p} \equiv ab \equiv 1 \mod p$.

Assume (for the sake of contradiction) that $c = 0$. Thus, $a \underbrace{c}_{=0} = 0$ and thus $0 = ac \equiv 1 \mod p$. Hence, $1 \equiv 0 \mod p$. In other words, $p \mid 1 - 0 = 1$. Hence, Exercise 2.2.5 (applied to $g = p$) yields $p = 1$. But $p > 1$ (since p is prime). This contradicts $p = 1$. This contradiction shows that our assumption (that $c = 0$) is false.

Hence, $c \neq 0$. Combining this with $c \in \{0,1,\ldots,p-1\}$, we obtain $c \in \{0,1,\ldots,p-1\} \setminus \{0\} = \{1,2,\ldots,p-1\} = A$. Recall that $ac \equiv 1 \mod p$.

Thus, there exists **at least one** $a' \in A$ satisfying $aa' \equiv 1 \mod p$ (namely, $a' = c$). It remains to prove that there is only one such a'.

Indeed, let a'_1 and a'_2 be two elements $a' \in A$ satisfying $aa' \equiv 1 \mod p$. We shall prove that $a'_1 = a'_2$.

We know that a'_1 is an element $a' \in A$ satisfying $aa' \equiv 1 \mod p$. In other words, a'_1 is an element of A and satisfies $aa'_1 \equiv 1 \mod p$. Similarly, a'_2 is an element of A and satisfies $aa'_2 \equiv 1 \mod p$. Hence, $1 \equiv aa'_2 \mod p$, so that $aa'_1 \equiv 1 \equiv aa'_2 \mod p$. Thus, Lemma 2.10.10 (applied to a'_1, a'_2 and p instead of b, c and n) yields $a'_1 \equiv a'_2 \mod p$ (since $a \perp p$). Hence, Lemma 2.15.8 **(a)** (applied to $a_1 = a'_1$ and $a_2 = a'_2$) yields $a'_1 = a'_2$.

Now, forget that we fixed a'_1 and a'_2. We thus have shown that if a'_1 and a'_2 are two elements $a' \in A$ satisfying $aa' \equiv 1 \mod p$, then $a'_1 = a'_2$. In other words, there exists **at most one** $a' \in A$ satisfying $aa' \equiv 1 \mod p$. Thus, there exists **a unique** such a' (because we have already shown that there exists **at least one** such a'). In other words, there exists a unique $a' \in A$ satisfying $aa' \equiv 1 \mod p$. This proves Lemma 2.15.8 **(b)**.

(c) Let $a \in A$. Then, $J(a)$ is the unique $a' \in A$ satisfying $aa' \equiv 1 \mod p$ (by the definition of J). Hence, $J(a)$ is an $a' \in A$ satisfying $aa' \equiv 1 \mod p$. In other words, $J(a)$ is an element of A and satisfies

$$aJ(a) \equiv 1 \mod p. \qquad (67)$$

Now, forget that we fixed a. We thus have proven (67) for each $a \in A$.

Now, let $a \in A$ be arbitrary. Then, $J(a) \in A$ (since J is a map from A to A). Thus, (67) (applied to $J(a)$ instead of a) yields $J(a)J(J(a)) \equiv 1 \mod p$. Also, from $J(a) \in A$, we obtain $J(J(a)) \in A$ (since J is a map from A to A). On the other hand, (67) yields $aJ(a) \equiv 1 \mod p$. Thus, $1 \equiv aJ(a) \mod p$. Now,

$$J(a)J(J(a)) \equiv 1 \equiv aJ(a) = J(a)a \mod p.$$

But $J(a) \in A = \{1,2,\ldots,p-1\}$. Hence, Proposition 2.13.4 (applied to $i = J(a)$) shows that $J(a)$ is coprime to p. In other words, $J(a) \perp p$. Hence, Lemma 2.10.10 (applied to $J(a)$, $J(J(a))$, a and p instead of a, b, c and n) yields $J(J(a)) \equiv a \mod p$

(since $J(a)J(J(a)) \equiv J(a)a \mod p$). Therefore, Lemma 2.15.8 **(a)** (applied to $a_1 = J(J(a))$ and $a_2 = a$) yields $J(J(a)) = a$. Thus, $(J \circ J)(a) = J(J(a)) = a = \operatorname{id}(a)$.

Now, forget that we fixed a. We thus have proven that $(J \circ J)(a) = \operatorname{id}(a)$ for each $a \in A$. In other words, $J \circ J = \operatorname{id}$. Hence, the maps J and J are mutually inverse. Thus, the map J is invertible, i.e., is a bijection. Thus, Lemma 2.15.8 **(c)** is proven. □

Remark 2.15.9. Let S be a set. An *involution* on S means a map $f : S \to S$ satisfying $f \circ f = \operatorname{id}$. Thus, Lemma 2.15.8 **(c)** says that the map $J : A \to A$ defined in this lemma is an involution on A.

We are now ready to prove Theorem 2.15.7:

First proof of Theorem 2.15.7. We have $(2-1)! = 1! = 1 \equiv -1 \mod 2$ (since $1 - (-1) = 2$ is divisible by 2). In other words, Theorem 2.15.7 holds when $p = 2$. Hence, for the rest of this proof, we WLOG assume that we don't have $p = 2$. Hence, $p \neq 2$. Thus, $1 \neq p - 1$.

But p is a prime; thus, $p > 1$, so that $p \geq 2$ (since p is an integer). Combining this with $p \neq 2$, we obtain $p > 2$, so that $p \geq 3$ (since p is an integer).

Define the set A and the map $J : A \to A$ as in Lemma 2.15.8. Hence, Lemma 2.15.8 **(c)** shows that this map J is a bijection satisfying $J \circ J = \operatorname{id}$. The equality $J \circ J = \operatorname{id}$ shows that the map J is inverse to itself. For each $a \in A$, we have

$$aJ(a) \equiv 1 \mod p. \tag{68}$$

(This congruence is proven in the same way as it was proven in our above proof of Lemma 2.15.8 **(c)**.)

Now, the rest of our proof shall follow the following plan (using the same "pairing" idea that we have seen in our proof of Proposition 2.14.7 and in the solution to Exercise 2.14.4): We will use the map J to establish a pairing between the factors of the product $1 \cdot 2 \cdot \cdots \cdot (p-1)$ (pairing up each factor a with the factor $J(a)$), which will pair up almost all of them – more precisely, all of them except for the very first and very last factors (since these two factors would have to pair up with themselves)[61]. For example, if $p = 11$, then we have the following table of values of J:

a	1	2	3	4	5	6	7	8	9	10
$J(a)$	1	6	4	3	9	2	8	7	5	10

(indeed, for example, $J(2) = 6$, since 6 is the unique $a' \in A$ satisfying $2 \cdot a' \equiv 1 \mod 11$), and thus we pair up the factors of the product $1 \cdot 2 \cdot \cdots \cdot (p-1)$ as follows:

$$\begin{aligned} 1 \cdot 2 \cdot \cdots \cdot (p-1) &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &= 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10. \end{aligned}$$

[61] The reason **why** it is precisely these two factors that will not be paired up is not completely trivial. It follows from Exercise 2.13.12.

By the definition of the map J, each pair has the form $(a, J(a))$ for some $a \in A$, and thus the product of any two different factors paired up with each other is $\equiv 1 \operatorname{mod} p$ (by (68)). For example, if $p = 11$, then we have

$$\begin{aligned} 1 \cdot 2 \cdot \cdots \cdot (p-1) &= 1 \cdot \underbrace{(2 \cdot 6)}_{\equiv 1 \operatorname{mod} 11} \cdot \underbrace{(3 \cdot 4)}_{\equiv 1 \operatorname{mod} 11} \cdot \underbrace{(5 \cdot 9)}_{\equiv 1 \operatorname{mod} 11} \cdot \underbrace{(7 \cdot 8)}_{\equiv 1 \operatorname{mod} 11} \cdot 10 \\ &\equiv 1 \cdot 10 \operatorname{mod} 11. \end{aligned}$$

Thus, any two different factors paired up with each other "neutralize" each other when being multiplied (as long as we are computing modulo p). Hence, the product of all the $p-1$ factors will reduce (when working modulo p) to the product of the two factors that have not been paired up, which will be $1 \cdot (p-1) = p - 1 \equiv -1 \operatorname{mod} p$.

Here are the details of this argument:

An element a of A will be called

- *small* if $a < J(a)$;
- *medium* if $a = J(a)$;
- *large* if $a > J(a)$.

Now, we claim that the medium elements of A are precisely 1 and $p-1$.

[*Proof:* We have $1 \leq p - 1$ (since $p \geq 2$). Thus, $1 \in \{1, 2, \ldots, p-1\} = A$ and $p - 1 \in \{1, 2, \ldots, p-1\} = A$. The element 1 of A is medium[62]. The element $p-1$ of A is medium[63]. Hence, the two numbers 1 and $p-1$ are medium elements of A. It remains to prove that these two numbers are the only medium elements of A.

Indeed, let a be a medium element of A. We shall show that $a = 1$ or $a = p - 1$.

Indeed, assume the contrary. Thus, neither $a = 1$ nor $a = p - 1$ holds.

[62] *Proof.* We have $1 \in A$. Hence, $J(1) \in A$ (since J is a map from A to A). Furthermore, (68) (applied to $a = 1$) yields $1J(1) \equiv 1 \operatorname{mod} p$. Thus, $1 \equiv 1J(1) = J(1) \operatorname{mod} p$. Thus, Lemma 2.15.8 **(a)** (applied to $a_1 = 1$ and $a_2 = J(1)$) yields $1 = J(1)$. In other words, the element 1 of A is medium.

[63] *Proof.* We have $p - 1 \in A$. Hence, $J(p-1) \in A$ (since J is a map from A to A). Furthermore, (68) (applied to $a = p - 1$) yields $(p-1) J(p-1) \equiv 1 \operatorname{mod} p$. Multiplying this congruence with the obvious congruence $p - 1 \equiv p - 1 \operatorname{mod} p$, we obtain

$$(p-1)(p-1) J(p-1) \equiv (p-1) 1 = p - 1 \operatorname{mod} p.$$

Hence,

$$\begin{aligned} p - 1 &\equiv (p-1)(p-1) J(p-1) = \left(\underbrace{p-1}_{\equiv -1 \operatorname{mod} p} \right)^2 J(p-1) \equiv \underbrace{(-1)^2}_{=1} J(p-1) \\ &= J(p-1) \operatorname{mod} p. \end{aligned}$$

Thus, Lemma 2.15.8 **(a)** (applied to $a_1 = p - 1$ and $a_2 = J(p-1)$) yields $p - 1 = J(p-1)$. In other words, the element $p-1$ of A is medium.

If we had $a \equiv 1 \mod p$, then Lemma 2.15.8 **(a)** (applied to $a_1 = a$ and $a_2 = 1$) would yield $a = 1$, which would contradict the fact that $a = 1$ does not hold. Thus, we do not have $a \equiv 1 \mod p$.

If we had $a \equiv p - 1 \mod p$, then Lemma 2.15.8 **(a)** (applied to $a_1 = a$ and $a_2 = p - 1$) would yield $a = p - 1$, which would contradict the fact that $a = p - 1$ does not hold. Thus, we do not have $a \equiv p - 1 \mod p$.

We have assumed that a is medium. In other words, $a = J(a)$. But (68) yields $aJ(a) \equiv 1 \mod p$. Thus, $a^2 = a \underbrace{a}_{=J(a)} = aJ(a) \equiv 1 \mod p$. Hence, Exercise 2.13.12 shows that $a \equiv 1 \operatorname{mod} p$ or $a \equiv -1 \operatorname{mod} p$. Hence, we must have $a \equiv -1 \mod p$ (since we do not have $a \equiv 1 \mod p$). Thus, $a \equiv -1 \equiv p - 1 \mod p$ (since $p - 1 \equiv -1 \mod p$). This contradicts the fact that we do not have $a \equiv p - 1 \mod p$.

This contradiction shows that our assumption was false. Hence, $a = 1$ or $a = p - 1$.

Now, forget that we fixed a. We thus have proven that every medium element a of A satisfies $a = 1$ or $a = p - 1$. In other words, every medium element of A is either 1 or $p - 1$. Since we know that 1 and $p - 1$ actually are medium elements of A, we thus conclude that the medium elements of A are precisely 1 and $p - 1$.]

So we have shown that the medium elements of A are precisely 1 and $p - 1$. Since these two elements are distinct (because $p - 1 \neq 1$), we thus obtain

$$\prod_{\substack{a \in A; \\ a \text{ is medium}}} a = 1 \cdot (p - 1) = p - 1 \equiv -1 \operatorname{mod} p. \tag{69}$$

It is easy to see that if a is a small element of A, then $J(a)$ is a large element of A [64]. Hence, the map

$$J^+ : \{\text{small elements of } A\} \to \{\text{large elements of } A\},$$
$$a \mapsto J(a)$$

is well-defined. Similarly, the map

$$J^- : \{\text{large elements of } A\} \to \{\text{small elements of } A\},$$
$$a \mapsto J(a)$$

is well-defined. These two maps J^+ and J^- are both restrictions of the map J, and thus are mutually inverse (since the map J is inverse to itself). Hence, the map J^+ is invertible, i.e., is a bijection. In other words, the map

$$\{\text{small elements of } A\} \to \{\text{large elements of } A\},$$
$$a \mapsto J(a)$$

is a bijection (since this map is just the map J^+). Thus, we can substitute $J(b)$ for a in the product $\prod_{\substack{a \in A; \\ a \text{ is large}}} a$. We thus obtain

$$\prod_{\substack{a \in A; \\ a \text{ is large}}} a = \prod_{\substack{b \in A; \\ b \text{ is small}}} J(b) = \prod_{\substack{a \in A; \\ a \text{ is small}}} J(a) \tag{70}$$

[64] *Proof.* Let a be a small element of A. Thus, $a < J(a)$. Note that $J(a) \in A$ (since J is a map from A to A). But $J \circ J = \operatorname{id}$, so that $(J \circ J)(a) = \operatorname{id} a = a < J(a)$. In view of $(J \circ J)(a) = J(J(a))$, this rewrites as $J(J(a)) < J(a)$. In other words, $J(a) > J(J(a))$. In other words, the element $J(a)$ of A is large (by the definition of "large"). Qed.

(here, we have renamed the index b as a in the product). Now, the definition of $(p-1)!$ yields

$$\begin{aligned}
(p-1)! &= 1 \cdot 2 \cdot \cdots \cdot (p-1) = \prod_{a \in A} a \\
&= \left(\prod_{\substack{a \in A; \\ a \text{ is small}}} a \right) \cdot \underbrace{\left(\prod_{\substack{a \in A; \\ a \text{ is medium}}} a \right)}_{\substack{\equiv -1 \bmod p \\ \text{(by (69))}}} \cdot \underbrace{\left(\prod_{\substack{a \in A; \\ a \text{ is large}}} a \right)}_{\substack{= \prod_{\substack{a \in A; \\ a \text{ is small}}} J(a) \\ \text{(by (70))}}} \\
&\qquad \left(\begin{array}{c} \text{since each } a \in A \text{ is either small or medium or large (but never} \\ \text{has more than one of these three attributes simultaneously)} \end{array} \right) \\
&\equiv \left(\prod_{\substack{a \in A; \\ a \text{ is small}}} a \right) \cdot (-1) \cdot \left(\prod_{\substack{a \in A; \\ a \text{ is small}}} J(a) \right) = - \underbrace{\left(\prod_{\substack{a \in A; \\ a \text{ is small}}} a \right) \cdot \left(\prod_{\substack{a \in A; \\ a \text{ is small}}} J(a) \right)}_{= \prod_{\substack{a \in A; \\ a \text{ is small}}} (aJ(a))} \\
&= - \prod_{\substack{a \in A; \\ a \text{ is small}}} (aJ(a)) \bmod p. \qquad (71)
\end{aligned}$$

But it is clear that $\prod_{\substack{a \in A; \\ a \text{ is small}}} \underbrace{(aJ(a))}_{\substack{\equiv 1 \bmod p \\ \text{(by (68))}}} \equiv 1 \bmod p$ [65]. Hence, (71) rewrites as

$$(p-1)! \equiv - \underbrace{\prod_{\substack{a \in A; \\ a \text{ is small}}} (aJ(a))}_{\equiv 1 \bmod p} \equiv -1 \bmod p. \qquad (72)$$

[65] *Proof.* Here is this argument in more detail:

Every $a \in \{\text{small elements of } A\}$ satisfies $aJ(a) \equiv 1 \bmod p$ (by (68)). Renaming the index a as s in this statement, we obtain the following: Every $s \in \{\text{small elements of } A\}$ satisfies $sJ(s) \equiv 1 \bmod p$. Hence, (9) (applied to $n = p$, $S = \{\text{small elements of } A\}$, $a_s = sJ(s)$ and $b_s = 1$) yields

$$\prod_{s \in \{\text{small elements of } A\}} (sJ(s)) \equiv \prod_{s \in \{\text{small elements of } A\}} 1 = 1 \bmod p.$$

In view of

$$\begin{aligned}
\prod_{s \in \{\text{small elements of } A\}} (sJ(s)) &= \prod_{a \in \{\text{small elements of } A\}} (aJ(a)) \qquad \left(\begin{array}{c} \text{here, we have renamed the} \\ \text{index } s \text{ as } a \text{ in the product} \end{array} \right) \\
&= \prod_{\substack{a \in A; \\ a \text{ is small}}} (aJ(a)),
\end{aligned}$$

this rewrites as $\prod_{\substack{a \in A; \\ a \text{ is small}}} (aJ(a)) \equiv 1 \bmod p$.

This proves Theorem 2.15.7. □

Later, in Section 3.5, we shall give a different version of this proof.
Theorem 2.15.7 has a converse:

Exercise 2.15.3. If an integer $p > 1$ satisfies $(p-1)! \equiv -1 \mod p$, then prove that p is a prime.

(This is actually easier to prove than Theorem 2.15.7 itself.)

Exercise 2.15.4. Let p be a prime. Prove that

$$(p-1)! \equiv p - 1 \mod 1 + 2 + \cdots + (p-1).$$

Exercise 2.15.5. Let p be an odd prime. Write p in the form $p = 2k+1$ for some $k \in \mathbb{N}$. Prove that $k!^2 \equiv -(-1)^k \mod p$.
[**Hint:** Each $j \in \mathbb{Z}$ satisfies $j(p-j) \equiv -j^2 \mod p$.]

2.16. The Chinese Remainder Theorem as a bijection

2.16.1. The bijection $K_{m,n}$

Here comes another of the many facts known as the "Chinese Remainder Theorem":

Theorem 2.16.1. Let m and n be two coprime positive integers. Then, the map

$$K_{m,n} : \{0, 1, \ldots, mn-1\} \to \{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, n-1\},$$
$$a \mapsto (a\%m, a\%n)$$

is well-defined and is a bijection.

Example 2.16.2. (a) Theorem 2.16.1 (applied to $m = 3$ and $n = 2$) says that the map

$$K_{3,2} : \{0, 1, 2, 3, 4, 5\} \to \{0, 1, 2\} \times \{0, 1\},$$
$$a \mapsto (a\%3, a\%2)$$

is a bijection. This map sends

$$\begin{array}{ccccccc} 0, & 1, & 2, & 3, & 4, & 5 & \text{to} \\ (0,0), & (1,1), & (2,0), & (0,1), & (1,0), & (2,1), & \end{array}$$

respectively (since $0\%3 = 0$ and $0\%2 = 0$ and $1\%3 = 1$ and $1\%2 = 1$ and $2\%3 = 2$ and $2\%2 = 0$ and so on). This list of values shows that this map is bijective (since it takes on every possible value in $\{0,1,2\} \times \{0,1\}$ exactly once). Theorem 2.16.1 says that this holds for arbitrary coprime m and n.

(b) Let us see how Theorem 2.16.1 fails when m and n are **not** coprime. For example, take $m = 6$ and $n = 4$. Then, the map

$$K_{6,4} : \{0,1,\ldots,23\} \to \{0,1,2,3,4,5\} \times \{0,1,2,3\},$$
$$a \mapsto (a\%6, a\%4)$$

is **not** a bijection. Indeed, it is neither injective (for example, it sends both 0 and 12 to the same pair $(0,0)$) nor surjective (for example, it never takes the value $(1,2)$).

Proof of Theorem 2.16.1. For every $a \in \{0,1,\ldots,mn-1\}$, we have $(a\%m, a\%n) \in \{0,1,\ldots,m-1\} \times \{0,1,\ldots,n-1\}$ [66]. Hence, the map $K_{m,n}$ is well-defined. It remains to prove that this map $K_{m,n}$ is a bijection. To that aim, we shall prove that $K_{m,n}$ is injective and surjective.

[*Proof that the map $K_{m,n}$ is injective:* Let $a,b \in \{0,1,\ldots,mn-1\}$ be such that $K_{m,n}(a) = K_{m,n}(b)$. We want to prove $a = b$.

The definition of $K_{m,n}$ yields $K_{m,n}(a) = (a\%m, a\%n)$ and $K_{m,n}(b) = (b\%m, b\%n)$. Hence, the equality $K_{m,n}(a) = K_{m,n}(b)$ (which is true by assumption) rewrites as $(a\%m, a\%n) = (b\%m, b\%n)$. In other words, $a\%m = b\%m$ and $a\%n = b\%n$.

Now, Exercise 2.6.1 (applied to $u = a$ and $v = b$) yields that $a \equiv b \mod n$ if and only if $a\%n = b\%n$. Hence, $a \equiv b \mod n$ (since $a\%n = b\%n$). In other words, $n \mid a - b$. The same argument (but applied to m instead of n) yields $m \mid a - b$.

Now, we have $m \perp n$ (since m and n are coprime) and $m \mid a - b$ and $n \mid a - b$. Hence, Theorem 2.10.7 (applied to m, n and $a - b$ instead of a, b and c) yields $mn \mid a - b$. In other words, $a \equiv b \mod mn$. Hence, Corollary 2.6.9 **(c)** (applied to mn, b and a instead of n, u and c) yields $a = b\%(mn)$ (since $a \in \{0,1,\ldots,mn-1\}$).

On the other hand, $b \equiv b \mod mn$. Hence, Corollary 2.6.9 **(c)** (applied to mn, b and b instead of n, u and c) yields $b = b\%(mn)$ (since $b \in \{0,1,\ldots,mn-1\}$). Comparing this with $a = b\%(mn)$, we obtain $a = b$.

Now, forget that we fixed a and b. We thus have shown that if $a,b \in \{0,1,\ldots,mn-1\}$ are such that $K_{m,n}(a) = K_{m,n}(b)$, then $a = b$. In other words, the map $K_{m,n}$ is injective.]

[*Proof that the map $K_{m,n}$ is surjective:* Fix $(a,b) \in \{0,1,\ldots,m-1\} \times \{0,1,\ldots,n-1\}$. We want to find a $c \in \{0,1,\ldots,mn-1\}$ such that $K_{m,n}(c) = (a,b)$.

We have $(a,b) \in \{0,1,\ldots,m-1\} \times \{0,1,\ldots,n-1\}$. In other words, $a \in \{0,1,\ldots,m-1\}$ and $b \in \{0,1,\ldots,n-1\}$. Theorem 2.12.1 **(a)** shows that there exists an integer

[66] *Proof.* Let $a \in \{0,1,\ldots,mn-1\}$. We must prove that $(a\%m, a\%n) \in \{0,1,\ldots,m-1\} \times \{0,1,\ldots,n-1\}$.

Corollary 2.6.9 **(a)** (applied to $u = a$) yields that $a\%n \in \{0,1,\ldots,n-1\}$ and $a\%n \equiv a \mod n$. Thus, $a\%n \in \{0,1,\ldots,n-1\}$. The same argument (applied to m instead of n) yields $a\%m \in \{0,1,\ldots,m-1\}$. Combining this with $a\%n \in \{0,1,\ldots,n-1\}$, we obtain $(a\%m, a\%n) \in \{0,1,\ldots,m-1\} \times \{0,1,\ldots,n-1\}$. Qed.

$x \in \mathbb{Z}$ such that

$$(x \equiv a \bmod m \text{ and } x \equiv b \bmod n).$$

Consider such an x. We have $x \equiv a \bmod m$, thus $a \equiv x \bmod m$. From $x \equiv b \bmod n$, we obtain $b \equiv x \bmod n$.

Let $y = x\% (mn)$. Then, Corollary 2.6.9 **(a)** (applied to mn and x instead of n and u) yields $x\% (mn) \in \{0, 1, \ldots, mn-1\}$ and $x\% (mn) \equiv x \bmod mn$. Hence, $x \equiv x\% (mn) = y \bmod mn$ (since $y = x\% (mn)$).

Since $m \mid mn$, we thus obtain $x \equiv y \bmod m$ (by Proposition 2.3.4 **(e)**, applied to mn, x, y and m instead of n, a, b and m). Thus, $a \equiv x \equiv y \bmod m$. Hence, Corollary 2.6.9 **(c)** (applied to m, y and a instead of n, u and c) yields $a = y\%m$ (since $a \in \{0, 1, \ldots, m-1\}$).

Also, from $x \equiv y \bmod mn$ and $n \mid mn$, we obtain $x \equiv y \bmod n$ (by Proposition 2.3.4 **(e)**, applied to mn, x, y and n instead of n, a, b and m). Thus, $b \equiv x \equiv y \bmod n$. Hence, Corollary 2.6.9 **(c)** (applied to y and b instead of u and c) yields $b = y\%n$ (since $b \in \{0, 1, \ldots, n-1\}$).

From $a = y\%m$ and $b = y\%n$, we obtain $(a, b) = (y\%m, y\%n)$.

We have $y = x\% (mn) \in \{0, 1, \ldots, mn-1\}$; thus, the definition of the map $K_{m,n}$ yields $K_{m,n}(y) = (y\%m, y\%n) = (a, b)$ (since $(a, b) = (y\%m, y\%n)$). Thus, there exists a $c \in \{0, 1, \ldots, mn-1\}$ such that $K_{m,n}(c) = (a, b)$ (namely, $c = y$).

Now, forget that we fixed (a, b). We thus have shown that for any $(a, b) \in \{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, n-1\}$, there exists a $c \in \{0, 1, \ldots, mn-1\}$ such that $K_{m,n}(c) = (a, b)$. In other words, the map $K_{m,n}$ is surjective.]

We have now proven that the map $K_{m,n}$ is both injective and surjective. Hence, this map $K_{m,n}$ is bijective, i.e., is a bijection. This proves Theorem 2.16.1.

[*Remark:* We could have saved ourselves some of the work done in this proof by invoking the Pigeonhole Principle. Indeed, our goal was to show that the map $K_{m,n}$ is bijective. By the Pigeonhole Principle for Injections (Theorem 2.15.5), it suffices to prove that it is injective, because $\{0, 1, \ldots, mn-1\}$ and $\{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, n-1\}$ are two finite sets of the same size. Alternatively, by the Pigeonhole Principle for Surjections (Theorem 2.15.6), it would instead suffice to prove that the map $K_{m,n}$ is surjective]. □

2.16.2. Coprime remainders

For the rest of this section, we shall use the following notation:

Definition 2.16.3. Let n be a positive integer. Then, let C_n be the subset $\{i \in \{0, 1, \ldots, n-1\} \mid i \perp n\}$ of $\{0, 1, \ldots, n-1\}$.

For instance,

$$C_4 = \{1, 3\}, \qquad C_5 = \{1, 2, 3, 4\}, \qquad C_6 = \{1, 5\} \qquad \text{and} \qquad C_1 = \{0\}.$$

Now, we claim the following:

Proposition 2.16.4. Let m and n be two coprime positive integers. Consider the map $K_{m,n}$ defined in Theorem 2.16.1. Then,

$$K_{m,n}\left(C_{mn}\right) = C_m \times C_n.$$

(Here, $K_{m,n}\left(C_{mn}\right)$ denotes the image of the subset C_{mn} of $\{0,1,\ldots,mn-1\}$ under the map $K_{m,n}$; that is, $K_{m,n}\left(C_{mn}\right) = \{K_{m,n}\left(x\right) \mid x \in C_{mn}\}$.)

Example 2.16.5. Theorem 2.16.1 (applied to $m = 3$ and $n = 5$) says that the map

$$\begin{aligned} K_{3,5} : \{0,1,\ldots,14\} &\to \{0,1,2\} \times \{0,1,2,3,4\}, \\ a &\mapsto (a\%3, a\%5) \end{aligned}$$

is a bijection. Proposition 2.16.4 (applied to $m = 3$ and $n = 5$) says that this map satisfies $K_{3,5}\left(C_{15}\right) = C_3 \times C_5$. In view of

$$\begin{aligned} C_{15} &= \{i \in \{0,1,\ldots,14\} \mid i \perp 15\} = \{1,2,4,7,8,11,13,14\}, \\ C_3 &= \{i \in \{0,1,2\} \mid i \perp 3\} = \{1,2\}, \qquad \text{and} \\ C_5 &= \{i \in \{0,1,2,3,4\} \mid i \perp 5\} = \{1,2,3,4\}, \end{aligned}$$

this rewrites as

$$K_{3,5}\left(\{1,2,4,7,8,11,13,14\}\right) = \{1,2\} \times \{1,2,3,4\}.$$

And indeed, this can easily be checked: The map $K_{3,5}$ sends

$$\begin{array}{ccccccccc} 1, & 2, & 4, & 7, & 8, & 11, & 13, & 14, & \text{to} \\ (1,1), & (2,2), & (1,4), & (1,2), & (2,3), & (2,1), & (1,3) & (2,4), & \end{array}$$

respectively, which entails

$$\begin{aligned} & K_{3,5}\left(\{1,2,4,7,8,11,13,14\}\right) \\ & = \{(1,1),(2,2),(1,4),(1,2),(2,3),(2,1),(1,3),(2,4)\} = \{1,2\} \times \{1,2,3,4\}. \end{aligned}$$

Proof of Proposition 2.16.4. Theorem 2.16.1 yields that the map $K_{m,n}$ is well-defined and is a bijection.

The definition of C_n yields

$$C_n = \{i \in \{0,1,\ldots,n-1\} \mid i \perp n\} \subseteq \{0,1,\ldots,n-1\}.$$

The definition of C_m yields

$$C_m = \{i \in \{0,1,\ldots,m-1\} \mid i \perp m\} \subseteq \{0,1,\ldots,m-1\}.$$

The definition of C_{mn} yields

$$C_{mn} = \{i \in \{0,1,\ldots,mn-1\} \mid i \perp mn\} \subseteq \{0,1,\ldots,mn-1\}.$$

Hence, $K_{m,n}(C_{mn})$ is well-defined. Also, from $C_m \subseteq \{0,1,\ldots,m-1\}$ and $C_n \subseteq \{0,1,\ldots,n-1\}$, we obtain

$$C_m \times C_n \subseteq \{0,1,\ldots,m-1\} \times \{0,1,\ldots,n-1\}.$$

Now, we claim that

$$K_{m,n}(C_{mn}) \subseteq C_m \times C_n. \tag{73}$$

[*Proof of (73):* Let $z \in K_{m,n}(C_{mn})$. Thus, $z = K_{m,n}(x)$ for some $x \in C_{mn}$. Consider this x.

We have $x \in C_{mn} = \{i \in \{0,1,\ldots,mn-1\} \mid i \perp mn\}$. In other words, x is an $i \in \{0,1,\ldots,mn-1\}$ satisfying $i \perp mn$. In other words, x is an element of $\{0,1,\ldots,mn-1\}$ and satisfies $x \perp mn$. In other words, $x \perp nm$ (since $mn = nm$).

We have $x \mid x$ and $m \mid mn$. Hence, Exercise 2.9.4 (applied to $a_1 = x$, $a_2 = m$, $b_1 = x$ and $b_2 = mn$) yields $\gcd(x,m) \mid \gcd(x,mn) = 1$ (since $x \perp mn$). Since $\gcd(x,m)$ is a nonnegative integer[67], this entails $\gcd(x,m) = 1$ (by Exercise 2.2.5, applied to $g = \gcd(x,m)$). In other words, $x \perp m$. But Corollary 2.6.9 **(a)** (applied to m and x instead of n and u) yields $x\%m \in \{0,1,\ldots,m-1\}$ and $x\%m \equiv x \mod m$. From $x\%m \equiv x \mod m$, we obtain $x \equiv x\%m \mod m$. Hence, Exercise 2.10.6 (applied to x, $x\%m$ and m instead of a, b and c) yields $x\%m \perp m$ (since $x \perp m$). Hence, $x\%m$ is an $i \in \{0,1,\ldots,m-1\}$ satisfying $i \perp m$ (since $x\%m \in \{0,1,\ldots,m-1\}$). In other words, $x\%m \in \{i \in \{0,1,\ldots,m-1\} \mid i \perp m\}$. In other words, $x\%m \in C_m$ (since $C_m = \{i \in \{0,1,\ldots,m-1\} \mid i \perp m\}$).

The same argument (with the roles of m and n swapped) yields $x\%n \in C_n$ (since $x \perp nm$). Now,

$$\begin{aligned} z = K_{m,n}(x) &= (x\%m, x\%n) && \text{(by the definition of } K_{m,n}) \\ &\in C_m \times C_n && \text{(since } x\%m \in C_m \text{ and } x\%n \in C_n). \end{aligned}$$

Now, forget that we fixed z. We thus have proven that $z \in C_m \times C_n$ for each $z \in K_{m,n}(C_{mn})$. In other words, $K_{m,n}(C_{mn}) \subseteq C_m \times C_n$. This proves (73).]

Next, we claim that

$$C_m \times C_n \subseteq K_{m,n}(C_{mn}). \tag{74}$$

[*Proof of (74):* Let $y \in C_m \times C_n$. We shall prove that $y \in K_{m,n}(C_{mn})$.

We have $y \in C_m \times C_n \subseteq \{0,1,\ldots,m-1\} \times \{0,1,\ldots,n-1\} = K_{m,n}(\{0,1,\ldots,mn-1\})$ (since the map $K_{m,n}$ is a bijection). In other words, there exists some $x \in \{0,1,\ldots,mn-1\}$ such that $y = K_{m,n}(x)$. Consider this x. The definition of $K_{m,n}$ yields $K_{m,n}(x) = (x\%m, x\%n)$. Hence,

$$(x\%m, x\%n) = K_{m,n}(x) = y \in C_m \times C_n.$$

In other words, $x\%m \in C_m$ and $x\%n \in C_n$.

We have $x\%m \in C_m = \{i \in \{0,1,\ldots,m-1\} \mid i \perp m\}$. In other words, $x\%m$ is an $i \in \{0,1,\ldots,m-1\}$ satisfying $i \perp m$. In other words, $x\%m$ is an element of $\{0,1,\ldots,m-1\}$ and satisfies $x\%m \perp m$.

[67] because any gcd is a nonnegative integer

But Corollary 2.6.9 **(a)** (applied to m and x instead of n and u) yields $x\%m \in \{0, 1, \ldots, m-1\}$ and $x\%m \equiv x \mod m$. Hence, Exercise 2.10.6 (applied to $x\%m$, x and m instead of a, b and c) yields $x \perp m$ (since $x\%m \perp m$). This yields $m \perp x$ (by Proposition 2.10.4). The same argument (applied to n instead of m) yields $n \perp x$ (since $x\%n \in C_n$). Hence, Theorem 2.10.9 (applied to m, n and x instead of a, b and c) yields $mn \perp x$. This yields $x \perp mn$ (by Proposition 2.10.4). Thus, x is an $i \in \{0, 1, \ldots, mn-1\}$ satisfying $i \perp mn$ (since $x \in \{0, 1, \ldots, mn-1\}$). In other words, $x \in \{i \in \{0, 1, \ldots, mn-1\} \mid i \perp mn\}$. In other words, $x \in C_{mn}$ (since $C_{mn} = \{i \in \{0, 1, \ldots, mn-1\} \mid i \perp mn\}$). Hence, $y = K_{m,n}\left(\underbrace{x}_{\in C_{mn}}\right) \in K_{m,n}(C_{mn})$.

Now, forget that we fixed y. We thus have shown that $y \in K_{m,n}(C_{mn})$ for each $y \in C_m \times C_n$. In other words, $C_m \times C_n \subseteq K_{m,n}(C_{mn})$. This proves (74).]

Combining (73) with (74), we obtain $K_{m,n}(C_{mn}) = C_m \times C_n$. This proves Proposition 2.16.4. □

2.16.3. Proving the formula for ϕ

We now can prove Theorem 2.14.4:

First proof of Theorem 2.14.4. The definition of C_n yields

$$C_n = \{i \in \{0, 1, \ldots, n-1\} \mid i \perp n\}. \tag{75}$$

Lemma 2.15.4 yields

$$\phi(n) = \left|\underbrace{\{i \in \{0, 1, \ldots, n-1\} \mid i \perp n\}}_{\substack{=C_n \\ \text{(by (75))}}}\right| = |C_n|.$$

The same argument (applied to mn instead of n) yields $\phi(mn) = |C_{mn}|$.

We have shown that $\phi(n) = |C_n|$, so that $|C_n| = \phi(n)$. The same argument (applied to m instead of n) yields $|C_m| = \phi(m)$.

It is well-known that any two finite sets A and B satisfy $|A \times B| = |A| \cdot |B|$ [68]. Applying this to $A = C_m$ and $B = C_n$, we obtain

$$|C_m \times C_n| = \underbrace{|C_m|}_{=\phi(m)} \cdot \underbrace{|C_n|}_{=\phi(n)} = \phi(m) \cdot \phi(n).$$

Note that C_{mn} is a subset of $\{0, 1, \ldots, mn-1\}$ (since the definition of C_{mn} yields $C_{mn} = \{i \in \{0, 1, \ldots, mn-1\} \mid i \perp mn\} \subseteq \{0, 1, \ldots, mn-1\}$).

[68] This is the so-called *product rule* in its simplest form (see, e.g., [Loehr11, 1.5] or [LeLeMe18, §15.2.1]).

Now, consider the map $K_{m,n}$ defined in Theorem 2.16.1. Then, Theorem 2.16.1 shows that this map $K_{m,n}$ is a bijection. Thus, in particular, $K_{m,n}$ is injective. Hence, $|K_{m,n}(S)| = |S|$ for each subset S of $\{0, 1, \ldots, mn-1\}$ [69]. Applying this to $S = C_{mn}$, we obtain $|K_{m,n}(C_{mn})| = |C_{mn}|$. Thus,

$$|C_{mn}| = \left| \underbrace{K_{m,n}(C_{mn})}_{\substack{=C_m \times C_n \\ \text{(by Proposition 2.16.4)}}} \right| = |C_m \times C_n| = \phi(m) \cdot \phi(n).$$

Hence, $\phi(mn) = |C_{mn}| = \phi(m) \cdot \phi(n)$. This proves Theorem 2.14.4. □

We now take aim at proving Theorem 2.14.5. First, let us extend Theorem 2.14.4 to products of k mutually coprime integers:

Exercise 2.16.1. Let $n_1, n_2, \ldots, n_k$ be mutually coprime positive integers. Prove that $\phi(n_1 n_2 \cdots n_k) = \phi(n_1) \cdot \phi(n_2) \cdot \cdots \cdot \phi(n_k)$.

Exercise 2.16.2. Let I be a finite set. For each $i \in I$, let n_i be a positive integer. Assume that

$$\text{every two distinct elements } i \text{ and } j \text{ of } I \text{ satisfy } n_i \perp n_j. \tag{76}$$

Prove that

$$\phi\left(\prod_{i \in I} n_i\right) = \prod_{i \in I} \phi(n_i).$$

We are finally ready to prove Theorem 2.14.5:

Proof of Theorem 2.14.5. The integer n is positive and thus nonzero. In other words, $n \neq 0$.

If p is a prime satisfying $p \nmid n$, then $v_p(n) = 0$ (by Corollary 2.13.26) and therefore

$$p^{v_p(n)} = p^0 = 1. \tag{77}$$

If p is a prime satisfying $p \mid n$, then $v_p(n)$ is a positive integer[70] and therefore satisfies

$$\phi\left(p^{v_p(n)}\right) = (p-1)\, p^{v_p(n)-1} \tag{78}$$

(by Exercise 2.14.1, applied to $k = v_p(n)$).

[69] This follows from the following general principle: If $f : X \to Y$ is an injective map between two finite sets X and Y, then $|f(S)| = |S|$ for each subset S of X.

[70] *Proof.* Let p be a prime satisfying $p \mid n$. If we had $v_p(n) = 0$, then we would have $p \nmid n$ (by Corollary 2.13.26), and this would contradict $p \mid n$. Hence, we cannot have $v_p(n) = 0$. Thus, $v_p(n) \neq 0$. But $v_p(n) \in \mathbb{N}$ (since n is nonzero). Thus, from $v_p(n) \neq 0$, we conclude that $v_p(n)$ is a positive integer. Qed.

Corollary 2.13.33 yields

$$n = \prod_{p \text{ prime}} p^{v_p(n)} = \left(\prod_{\substack{p \text{ prime;} \\ p \mid n}} p^{v_p(n)} \right) \cdot \left(\prod_{\substack{p \text{ prime;} \\ p \nmid n}} \underbrace{p^{v_p(n)}}_{\substack{=1 \\ (\text{by (77)})}} \right)$$

$$\left(\begin{array}{c} \text{since each prime } p \text{ satisfies either } p \mid n \text{ or } p \nmid n \\ \text{(but not both at the same time)} \end{array} \right)$$

$$= \left(\prod_{\substack{p \text{ prime;} \\ p \mid n}} p^{v_p(n)} \right) \cdot \underbrace{\left(\prod_{\substack{p \text{ prime;} \\ p \nmid n}} 1 \right)}_{=1} = \prod_{\substack{p \text{ prime;} \\ p \mid n}} p^{v_p(n)}. \tag{79}$$

Let P be the set of all primes p satisfying $p \mid n$. This set P is finite[71]. For each $i \in P$, the number $i^{v_i(n)}$ is a positive integer[72]. Moreover, every two distinct elements i and j of P satisfy $i^{v_i(n)} \perp j^{v_j(n)}$ [73]. Hence, Exercise 2.16.2 (applied to $I = P$ and $n_i = i^{v_i(n)}$) yields

$$\phi \left(\prod_{i \in P} i^{v_i(n)} \right) = \prod_{i \in P} \phi \left(i^{v_i(n)} \right).$$

Renaming the index i as p in both products, we can rewrite this equality as

$$\phi \left(\prod_{p \in P} p^{v_p(n)} \right) = \prod_{p \in P} \phi \left(p^{v_p(n)} \right). \tag{80}$$

But the product signs "$\prod_{p \in P}$" in this equality can be replaced by "$\prod_{\substack{p \text{ prime;} \\ p \mid n}}$" without changing their meaning (since P is the set of all primes p satisfying $p \mid n$). Hence,

[71] *Proof.* We shall show that $P \subseteq \{1, 2, \ldots, n\}$.

Indeed, let $p \in P$. Thus, p is a prime satisfying $p \mid n$ (by the definition of P). Hence, p is positive (since p is prime). Also, $n \neq 0$. Thus, from $p \mid n$, we obtain $|p| \leq |n|$ (by Proposition 2.2.3 **(b)**, applied to $a = p$ and $b = n$). In view of $|p| = p$ (since p is positive) and $|n| = n$ (since n is positive), this rewrites as $p \leq n$. Hence, $p \in \{1, 2, \ldots, n\}$ (since p is a positive integer).

Now, forget that we fixed p. We thus have shown that $p \in \{1, 2, \ldots, n\}$ for each $p \in P$. In other words, $P \subseteq \{1, 2, \ldots, n\}$. Hence, the set P is finite (since the set $\{1, 2, \ldots, n\}$ is finite).

[72] since $v_i(n) \in \mathbb{N}$ (since n is nonzero) and since i is a positive integer

[73] *Proof.* Let i and j be two distinct elements of P. All elements of P are primes (by the definition of P); thus, i and j are primes (since i and j are elements of P). Also, i and j are distinct. Hence, Exercise 2.13.1 (applied to $p = i$ and $q = j$) yields $i \perp j$. But $v_i(n) \in \mathbb{N}$ (since n is nonzero) and $v_j(n) \in \mathbb{N}$ (for the same reason). Hence, Exercise 2.10.4 (applied to i, j, $v_i(n)$ and $v_j(n)$ instead of a, b, n and m) yields $i^{v_i(n)} \perp j^{v_j(n)}$. Qed.

the equality (80) rewrites as

$$\phi\left(\prod_{\substack{p \text{ prime};\\ p\mid n}} p^{v_p(n)}\right) = \prod_{\substack{p \text{ prime};\\ p\mid n}} \phi\left(p^{v_p(n)}\right). \tag{81}$$

Now, applying the map ϕ to both sides of the equality (79), we find

$$\begin{aligned}
\phi(n) &= \phi\left(\prod_{\substack{p \text{ prime};\\ p\mid n}} p^{v_p(n)}\right) = \prod_{\substack{p \text{ prime};\\ p\mid n}} \underbrace{\phi\left(p^{v_p(n)}\right)}_{\substack{=(p-1)p^{v_p(n)-1}\\ \text{(by (78))}}} \qquad \text{(by (81))}\\
&= \prod_{\substack{p \text{ prime};\\ p\mid n}} \underbrace{\left((p-1)\,p^{v_p(n)-1}\right)}_{\substack{=pp^{v_p(n)-1}-p^{v_p(n)-1}\\ =p^{v_p(n)}-p^{v_p(n)-1}\\ =p^{v_p(n)}-p^{v_p(n)}/p\\ =p^{v_p(n)}\left(1-\dfrac{1}{p}\right)}} = \prod_{\substack{p \text{ prime};\\ p\mid n}} \left(p^{v_p(n)}\left(1-\frac{1}{p}\right)\right)\\
&= \underbrace{\left(\prod_{\substack{p \text{ prime};\\ p\mid n}} p^{v_p(n)}\right)}_{\substack{=n\\ \text{(by (79))}}} \cdot \prod_{\substack{p \text{ prime};\\ p\mid n}} \left(1-\frac{1}{p}\right) = n \cdot \prod_{\substack{p \text{ prime};\\ p\mid n}} \left(1-\frac{1}{p}\right).
\end{aligned}$$

This proves Theorem 2.14.5. □

Theorem 2.15.3 generalizes Theorem 2.15.1 **(a)**. Likewise, the following exercise generalizes Theorem 2.15.1 **(b)**:

Exercise 2.16.3. Let a be an integer, and let n be a positive integer. Prove that $a^n \equiv a^{n-\phi(n)} \bmod n$.

[**Hint:** Use Exercises 2.13.9 and 2.14.2 and Theorems 2.15.3 and 2.14.4.]

2.17. Binomial coefficients

2.17.1. Definitions and basics

Next, we shall introduce and briefly study binomial coefficients. While binomial coefficients belong more to (enumerative) combinatorics than to algebra, they are used significantly in algebra, so we have to derive some of their properties.

Here is the definition of binomial coefficients (at least the one I am going to follow in these notes):

Definition 2.17.1. Let $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$. Then, we define the *binomial coefficient* $\dbinom{n}{k}$ as follows:

(a) If $k \in \mathbb{N}$, then we set

$$\binom{n}{k} = \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)}{k!} = \frac{\prod\limits_{i=0}^{k-1}\left(n-i\right)}{k!}.$$

(b) If $k \notin \mathbb{N}$, then we set $\dbinom{n}{k} = 0$.

This definition is exactly the definition of $\dbinom{n}{k}$ that we used in homework set #0. It is also almost exactly the definition given in [GrKnPa94, (5.1)] (except that we are allowing k to be non-integer, while the authors of [GrKnPa94] do not). Definition 2.17.1 **(a)** is also identical with the definition of binomial coefficients in [Grinbe15]. Our choice to require $n \in \mathbb{Q}$ is more or less arbitrary – we could have as well made the same definition for $n \in \mathbb{R}$ or $n \in \mathbb{C}$ (but I am not aware of this generality being of much use).

Generally, when you read literature on binomial coefficients, be aware that some authors use somewhat different definitions of $\dbinom{n}{k}$. All known definitions give the same results when n and k are nonnegative integers, but in the other cases there may be discrepancies.

Here are some examples of binomial coefficients:

Example 2.17.2. (a) Definition 2.17.1 **(a)** yields $\dbinom{n}{2} = \dfrac{n\left(n-1\right)}{2!} = \dfrac{n\left(n-1\right)}{2}$ for all $n \in \mathbb{Q}$. Thus, for example,

$$\binom{5}{2} = \frac{5 \cdot 4}{2} = 10.$$

(b) Definition 2.17.1 **(a)** yields $\dbinom{n}{3} = \dfrac{n\left(n-1\right)\left(n-2\right)}{3!} = \dfrac{n\left(n-1\right)\left(n-2\right)}{6}$ for all $n \in \mathbb{Q}$. Thus, for example,

$$\begin{aligned}
\binom{5}{3} &= \frac{5 \cdot 4 \cdot 3}{6} = \frac{60}{6} = 10; \\
\binom{1}{3} &= \frac{1 \cdot 0 \cdot \left(-1\right)}{6} = \frac{0}{6} = 0; \\
\binom{-2}{3} &= \frac{\left(-2\right) \cdot \left(-3\right) \cdot \left(-4\right)}{6} = \frac{-24}{6} = -4; \\
\binom{1/2}{3} &= \frac{\left(1/2\right) \cdot \left(-1/2\right) \cdot \left(-3/2\right)}{6} = \frac{3/8}{6} = \frac{1}{16}.
\end{aligned}$$

(c) Definition 2.17.1 **(a)** yields $\dbinom{n}{1} = \dfrac{n}{1!} = \dfrac{n}{1} = n$ for all $n \in \mathbb{Q}$.

(d) Definition 2.17.1 **(b)** yields $\dbinom{4}{1/2} = 0$ (since $1/2 \notin \mathbb{N}$).

The binomial coefficients $\dbinom{n}{k}$ for $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$ are particularly important. They are usually tabulated in a triangle-shaped table known as *Pascal's triangle*, which starts as follows:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}.$$

In this table, the binomial coefficient $\dbinom{n}{k}$ appears as the k-th entry (from the left) of the n-th row (but we count the rows from 0; that is, the topmost row, consisting just of a single "1", is actually the 0-th row). We advise the reader to peruse the Wikipedia article for the history and the multiple illustrious properties of Pascal's triangle.

The expression $\dbinom{n}{k}$ is pronounced as "n choose k". The reason for the word "choose" will become clearer once we have seen Theorem 2.17.10 further below.

Some of these properties are so fundamental that we are going to list them right now:

Theorem 2.17.3. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$ be such that $n \geq k$. Then,

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Proof of Theorem 2.17.3. This was Exercise 3 **(a)** on homework set #0. □

Several authors use the formula $\dbinom{n}{k} = \dfrac{n!}{k!\,(n-k)!}$ as a definition of the binomial coefficients. However, this definition has the massive disadvantage of being less general than Definition 2.17.1 (since it only covers the case when $n, k \in \mathbb{N}$ and $n \geq k$). To us, this formula is not a definition, but a result that can be proven.

Theorem 2.17.4. Let $n \in \mathbb{N}$ and $k \in \mathbb{Q}$ be such that $k > n$. Then,

$$\binom{n}{k} = 0.$$

Proof of Theorem 2.17.4. This was Exercise 3 **(b)** on homework set #0. □

Theorem 2.17.5. Let $n \in \mathbb{Q}$. Then,

$$\binom{n}{0} = 1.$$

Proof of Theorem 2.17.5. Definition 2.17.1 **(a)** (applied to $k = 0$) yields

$$\binom{n}{0} = \frac{\prod\limits_{i=0}^{0-1} (n-i)}{0!} = \frac{1}{1}$$

(since $\prod\limits_{i=0}^{0-1} (n-i) = (\text{empty product}) = 1$ and $0! = 1$). Thus, $\binom{n}{0} = \frac{1}{1} = 1$. This proves Theorem 2.17.5. □

Theorem 2.17.6. Let $n \in \mathbb{N}$ and $k \in \mathbb{Q}$. Then,

$$\binom{n}{k} = \binom{n}{n-k}.$$

Theorem 2.17.6 is known as the *symmetry of binomial coefficients*. Note that it fails if $n \notin \mathbb{N}$; thus, be careful when applying it!

Proof of Theorem 2.17.6. This was Exercise 3 **(c)** on homework set #0. □

Theorem 2.17.7. Let $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$. Then,

$$\binom{-n}{k} = (-1)^k \binom{k+n-1}{k}.$$

Theorem 2.17.7 is one of the versions of the *upper negation formula*.

Proof of Theorem 2.17.7. This was Exercise 3 **(d)** on homework set #0. □

Theorem 2.17.8. Any $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$ satisfy

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Theorem 2.17.8 is known as the *recurrence of the binomial coefficients*, and is the reason why each entry of Pascal's triangle is the sum of the two entries above it[74].

Proof of Theorem 2.17.8. This was Exercise 3 **(e)** on homework set #0. □

Theorem 2.17.9. Any $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$ satisfy

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

Proof of Theorem 2.17.9. This was Exercise 3 **(f)** on homework set #0. □

2.17.2. Combinatorial interpretation

The next property of binomial coefficients is one of the major motivations for defining them:

Theorem 2.17.10. Let $n \in \mathbb{N}$ and $k \in \mathbb{Q}$. Let N be an n-element set. Then, $\binom{n}{k}$ is the number of k-element subsets of N.

We shall refer to Theorem 2.17.10 as the *Combinatorial interpretation of binomial coefficients*. Theorem 2.17.10 can be restated as "$\binom{n}{k}$ is the number of ways to choose k elements (with no repetitions and with no regard for the order) from a given n-element set (when $n \in \mathbb{N}$)". This is the reason why $\binom{n}{k}$ is called "n choose k". Note, however, that Theorem 2.17.10 does not directly help us compute $\binom{n}{k}$ when $n \notin \mathbb{N}$.

Proof of Theorem 2.17.10. What follows is an outline of the proof. For a detailed proof, see [Grinbe15, Exercise 3.4], where I thoroughly prove Theorem 2.17.10 in the case $k \in \mathbb{N}$. (The remaining case $k \notin \mathbb{N}$ is obvious, because in that case the theorem simply says $0 = 0$.)

We proceed by induction on n:

[74] Of course, this does not apply to the "1" at the apex of Pascal's triangle (unless we extend the triangle further to the top by a (-1)-st row).

Induction base: Let n, k and N be as in Theorem 2.17.10, and let us assume that $n = 0$. From $n = 0$, we obtain $\binom{n}{k} = \binom{0}{k} = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0 \end{cases}$ (this is easy to derive from Definition 2.17.1[75]). On the other hand, the set N is empty (since $|N| = n = 0$). Thus, its only subset is $\varnothing$, which is a 0-element subset. Hence, N has exactly one 0-element subset, and no subsets of any other size. Hence, the number of k-element subsets of N is $\begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0 \end{cases}$. Comparing this with $\binom{n}{k} = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0 \end{cases}$, we conclude that $\binom{n}{k}$ is the number of k-element subsets of N. Thus, we have proven Theorem 2.17.10 under the assumption that $n = 0$. This completes the induction base.

Induction step: Let m be a positive integer. Assume (as the induction hypothesis) that Theorem 2.17.10 holds for $n = m - 1$. We must now prove that Theorem 2.17.10 holds for $n = m$.

Let $k \in \mathbb{Q}$. Let N be an m-element set. Thus, $|N| = m > 0$. Hence, the set N is nonempty; in other words, there exists some $a \in N$. Pick such an a. (It does not matter which one we choose, but we need to leave it fixed from now on.) Clearly, $|N \setminus \{a\}| = m - 1$ (since $|N| = m$). In other words, $N \setminus \{a\}$ is an $(m-1)$-element set.

Now, the k-element subsets of N can be classified into two types:

- We say that a k-element subset is *type-1* if it doesn't contain a.
- We say that a k-element subset is *type-2* if it does contain a.

(We shall use the adjectives "type-1" and "type-2" for k-element subsets of N only. Thus, whenever we say "type-1 subset" in the following, we will always mean "type-1 k-element subset of N", and similarly for "type-2 subset".)

Clearly, any k-element subset of N is either type-1 or type-2 (but never both at the same time).

The type-1 subsets are precisely the k-element subsets of the $(m-1)$-element set $N \setminus \{a\}$. By our induction hypothesis, we know that Theorem 2.17.10 holds for

[75] To wit:

- If $k = 0$, then $\binom{0}{k} = \binom{0}{0} = 1$ (by Theorem 2.17.5).
- If $k > 0$, then Theorem 2.17.4 (applied to 0 instead of n) yields $\binom{0}{k} = 0$.
- If $k < 0$, then $k \notin \mathbb{N}$ and thus $\binom{0}{k} = 0$ (by Definition 2.17.1 **(b)**).

Thus, in all three cases ($k = 0$, $k > 0$ and $k < 0$), we conclude that $\binom{0}{k} = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0 \end{cases}$.

$n = m-1$. Hence, we can apply Theorem 2.17.10 to $m-1$ and $N \setminus \{a\}$ instead of n and N. We thus conclude that $\dbinom{m-1}{k}$ is the number of k-element subsets of $N \setminus \{a\}$. In other words, $\dbinom{m-1}{k}$ is the number of type-1 subsets (since the type-1 subsets are precisely the k-element subsets of $N \setminus \{a\}$). In other words,

$$\binom{m-1}{k} = (\text{the number of type-1 subsets}) . \qquad (82)$$

Now, let us count the type-2 subsets[76]. This is a bit harder, since they are not subsets of $N \setminus \{a\}$ anymore. However, they are in 1-to-1 correspondence (aka bijection) with some such subsets. Namely, there is a bijection

$$\begin{aligned} \{(k-1)\text{-element subsets of } N \setminus \{a\}\} &\to \{\text{type-2 subsets}\} , \\ S &\mapsto S \cup \{a\} . \end{aligned}$$

(The inverse of this bijection sends each type-2 subset T to $T \setminus \{a\}$. You can easily show that these two maps are actually well-defined and mutually inverse, so that they really are bijections.) This bijection shows that

$$|\{\text{type-2 subsets}\}| = |\{(k-1)\text{-element subsets of } N \setminus \{a\}\}| . \qquad (83)$$

But recall that Theorem 2.17.10 holds for $n = m-1$. Hence, we can apply Theorem 2.17.10 to $m-1$, $k-1$ and $N \setminus \{a\}$ instead of n, k and N. We thus conclude that $\dbinom{m-1}{k-1}$ is the number of $(k-1)$-element subsets of $N \setminus \{a\}$. In other words,

$$\binom{m-1}{k-1} = |\{(k-1)\text{-element subsets of } N \setminus \{a\}\}| .$$

Comparing this equality with (83), we obtain

$$\begin{aligned} \binom{m-1}{k-1} &= |\{\text{type-2 subsets}\}| \\ &= (\text{the number of type-2 subsets}) . \qquad (84) \end{aligned}$$

Now, recall that any k-element subset of N is either type-1 or type-2 (but never both at the same time). Hence, we can count all k-element subsets of N by first counting the type-1 subsets, then counting the type-2 subsets, and then adding

[76] Keep in mind that "type-2 subset" means "type-2 k-element subset of N".

these two results. We thus find[77]

$$\begin{aligned}
&(\text{the number of } k\text{-element subsets of } N) \\
&= \underbrace{(\text{the number of type-1 subsets})}_{\substack{=\binom{m-1}{k} \\ \text{(by (82))}}} + \underbrace{(\text{the number of type-2 subsets})}_{\substack{=\binom{m-1}{k-1} \\ \text{(by (84))}}} \\
&= \binom{m-1}{k} + \binom{m-1}{k-1} = \binom{m}{k}
\end{aligned}$$

(since Theorem 2.17.8 (applied to $n = m$) yields $\binom{m}{k} = \binom{m-1}{k} + \binom{m-1}{k-1}$). In other words, $\binom{m}{k}$ is the number of k-element subsets of N.

Now, forget that we fixed N and k. We thus have shown that if $k \in \mathbb{Q}$ and if N is an m-element set, then $\binom{m}{k}$ is the number of k-element subsets of N. In other words, Theorem 2.17.10 holds for $n = m$. This completes the induction step. Hence, Theorem 2.17.10 is proven. □

> **Corollary 2.17.11.** Let $n \in \mathbb{N}$ and $k \in \mathbb{Q}$. Then, $\binom{n}{k}$ is a nonnegative integer.

Proof of Corollary 2.17.11. Let $N = \{1, 2, \ldots, n\}$; thus, N is an n-element set. Hence, Theorem 2.17.10 shows that $\binom{n}{k}$ is the number of k-element subsets of N. But the latter number is clearly a nonnegative integer (since it counts something). Thus, $\binom{n}{k}$ is a nonnegative integer. This proves Corollary 2.17.11. □

> **Proposition 2.17.12.** Let $n \in \mathbb{Z}$ and $k \in \mathbb{Q}$. Then, $\binom{n}{k}$ is a integer.

Proof of Proposition 2.17.12. If $n \geq 0$, then this follows from Corollary 2.17.11 (because $n \geq 0$ implies $n \in \mathbb{N}$, and thus we can apply Corollary 2.17.11). Thus, for the rest of this proof, we WLOG assume that $n < 0$. Hence, $n \leq -1$ (since n is an integer), so that $n + 1 \leq 0$ and thus $-(n+1) \geq 0$. Therefore, $-(n+1) \in \mathbb{N}$ (since $-(n+1)$ is an integer).

If $k \notin \mathbb{N}$, then $\binom{n}{k}$ is a integer (since Definition 2.17.1 **(b)** yields $\binom{n}{k} = 0$ in this case). Thus, for the rest of this proof, we WLOG assume that $k \in \mathbb{N}$.

[77] The combinatorial principle we are using in the following computation is the so-called *sum rule* in its simplest form (see, e.g., [Loehr11, 1.1] or [LeLeMe18, §15.2.3]).

Thus, $k+(-n)-1=\underbrace{k}_{\in\mathbb{N}}+\underbrace{(-(n+1))}_{\in\mathbb{N}}\in\mathbb{N}$. Hence, Corollary 2.17.11 (applied to $k+(-n)-1$ instead of n) yields that $\dbinom{k+(-n)-1}{k}$ is a nonnegative integer. Thus, $\dbinom{k+(-n)-1}{k}\in\mathbb{Z}$.

Theorem 2.17.7 (applied to $-n$ instead of n) yields

$$\binom{-(-n)}{k}=\underbrace{(-1)^k}_{\in\mathbb{Z}}\underbrace{\binom{k+(-n)-1}{k}}_{\in\mathbb{Z}}\in\mathbb{Z}.$$

In other words, $\dbinom{n}{k}\in\mathbb{Z}$. In other words, $\dbinom{n}{k}$ is an integer. Thus, Proposition 2.17.12 is proven. □

Exercise 2.17.1. Let $k\in\mathbb{N}$. Prove that the product of any k consecutive integers is divisible by $k!$.

Exercise 2.17.2. In this exercise, we shall use the *Iverson bracket notation*: If $\mathcal{A}$ is any statement, then $[\mathcal{A}]$ stands for the integer $\begin{cases}1, & \text{if } \mathcal{A} \text{ is true;}\\ 0, & \text{if } \mathcal{A} \text{ is false}\end{cases}$ (which is also known as the *truth value* of $\mathcal{A}$). For instance, $[1+1=2]=1$ and $[1+1=1]=0$.

(a) Prove that $n//k=\sum\limits_{i=1}^{n}[k\mid i]$ for any $n\in\mathbb{N}$ and any positive integer k.

(b) Prove that $v_p(n)=\sum\limits_{i\geq1}\left[p^i\mid n\right]$ for any prime p and any nonzero integer n. Here, the sum $\sum\limits_{i\geq1}\left[p^i\mid n\right]$ is a sum over all positive integers; but it is well-defined, since it has only finitely many nonzero addends.

(c) Prove that $v_p(n!)=\sum\limits_{i\geq1}n//p^i$ for any prime p and any $n\in\mathbb{N}$. (Here, the expression "$\sum\limits_{i\geq1}n//p^i$" should be understood as $\sum\limits_{i\geq1}\left(n//p^i\right)$. Again, this sum $\sum\limits_{i\geq1}\left(n//p^i\right)$ is well-defined, since it has only finitely many nonzero addends.)

(d) Use part **(c)** to prove Corollary 2.17.11 again.

The claim of Exercise 2.17.2 **(c)** is usually rewritten in the form $v_p(n!)=\sum\limits_{i\geq1}\left\lfloor\dfrac{n}{p^i}\right\rfloor$ (which is equivalent, because of Proposition 2.8.3); in this form, it is known as Legendre's formula or as de Polignac's formula (see, e.g., [Grinbe16, Theorem 1.3.3]). It is often a helpful tool in proving divisibility properties of factorials and binomial coefficients. One application, for example, is to quickly compute how many zeroes the decimal expansion of $n!$ ends with. (Note that Exercise 2.17.2 **(b)** can be rewritten as $v_p(n)=\sum\limits_{\substack{i\geq1;\\ p^i\mid n}}1$; in this form it appears in [Grinbe16, Lemma 1.3.4].)

2.17.3. Binomial formula and Vandermonde convolution

One of the staples of enumerative combinatorics are identities that involve binomial coefficients. Hundreds of such identities have been found (see, e.g., Henry W. Gould's website for a list of some of them; see also [GrKnPa94, Chapter 5] and [Grinbe15, Chapter 3] for introductions). At this point, let us only show two of the most important ones (not counting the ones we have already shown above). Probably the most famous one is the *binomial formula*:

Theorem 2.17.13. Let x, y be any numbers (e.g., rational or real or complex numbers). Let $n \in \mathbb{N}$. Then,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Theorem 2.17.13 is known as the *binomial formula* or the *binomial theorem*. It generalizes the well-known and beloved identities

$$\begin{aligned}(x+y)^2 &= x^2 + 2xy + y^2;\\ (x+y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3;\\ (x+y)^4 &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4\end{aligned}$$

(as well as $(x+y)^1 = x^1 + y^1$ and $(x+y)^0 = 1$, of course).

Proof of Theorem 2.17.13 (sketched). This can be proven by a straightforward induction on n (using Theorem 2.17.8 in the induction step). See [Grinbe15, Exercise 3.6] for details of this proof. Alternatively, see [Galvin17, Identity 11.4] for combinatorial proofs (which rely on Theorem 2.17.10). □

The next identity we want to show is the *Vandermonde convolution identity*:

Theorem 2.17.14. Let $x, y \in \mathbb{Q}$ and $n \in \mathbb{N}$. Then,

$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}.$$

For example, for $n = 2$, Theorem 2.17.14 says that

$$\binom{x+y}{2} = \underbrace{\binom{x}{0}}_{=1} \binom{y}{2} + \underbrace{\binom{x}{1}}_{=x} \underbrace{\binom{y}{1}}_{=y} + \binom{x}{2} \underbrace{\binom{y}{0}}_{=1} = \binom{y}{2} + xy + \binom{x}{2}.$$

The proof of Theorem 2.17.14 that we are soon going to sketch is similar to the one given in [Grinbe15, §3.3.3] (but, unlike the latter proof, we will use polynomials in 1 variable only). It will not be a complete proof, since it will rely on some properties of polynomials, and not only have we not proven these properties – we have actually not rigorously defined polynomials yet! (We will do so later, in Chapter 7.) See [Grinbe15, §3.3.2] for another (more boring and tedious, but conceptually simpler) proof of Theorem 2.17.14.

Our proof of Theorem 2.17.14 proceeds via several intermediate steps. The first one is to prove Theorem 2.17.14 in the particular case when $x, y \in \mathbb{N}$:

Lemma 2.17.15. Let $a, b \in \mathbb{N}$ and $n \in \mathbb{N}$. Then,

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}.$$

(We have renamed the variables x and y from Theorem 2.17.14 as a and b here, since we will soon use the letter "x" for something completely different.)

Proof of Lemma 2.17.15 (sketched). Let

$$C = \{1, 2, \ldots, a\} \cup \{-1, -2, \ldots, -b\}.$$

Thus, C is an $(a+b)$-element set, containing only positive and negative integers. How many n-element subsets does C have?

- On the one hand: The set C is an $(a+b)$-element set. Hence, Theorem 2.17.10 (applied to $a+b$, n and C instead of n, k and N) shows that the number of n-element subsets of C is $\binom{a+b}{n}$.
- On the other hand: Let us classify the n-element subsets of C according to how many positive elements they have. We claim the following:

  Claim 1: For each $k \in \{0, 1, \ldots, n\}$, the number of n-element subsets of C having **exactly** k **positive elements** is $\binom{a}{k}\binom{b}{n-k}$.

  [*Proof of Claim 1:* Let $k \in \{0, 1, \ldots, n\}$. In order to choose an n-element subset of C having exactly k positive elements, we need to choose

  - its k positive elements from the set of all positive elements of C (that is, from the set $\{1, 2, \ldots, a\}$), and
  - its remaining $n-k$ (negative) elements from the set of all negative elements of C (that is, from the set $\{-1, -2, \ldots, -b\}$).

  In other words, we need to choose

  - a k-element subset of the set $\{1, 2, \ldots, a\}$, and
  - an $(n-k)$-element subset of the set $\{-1, -2, \ldots, -b\}$.

Theorem 2.17.10 (applied to a, k and $\{1, 2, \ldots, a\}$ instead of n, k and N) shows that the number of k-element subsets of the set $\{1, 2, \ldots, a\}$ is $\dbinom{a}{k}$ (since $\{1, 2, \ldots, a\}$ is an a-element set). Similarly, the number of $(n-k)$-element subsets of the set $\{-1, -2, \ldots, -b\}$ is $\dbinom{b}{n-k}$. Since we need to choose one of the former subsets and one of the latter subsets (and our choices are independent – i.e., any of the former subsets can be combined with any of the latter), we thus conclude that the total number of options we have is $\dbinom{a}{k}\dbinom{b}{n-k}$ [78]. In other words, the number of n-element subsets of C having **exactly** k **positive elements** is $\dbinom{a}{k}\dbinom{b}{n-k}$. This proves Claim 1.]

Now, the total number of n-element subsets of C is[79]

$$\begin{aligned}
&(\text{the number of } n\text{-element subsets of } C) \\
&= \sum_{k=0}^{n} \underbrace{(\text{the number of } n\text{-element subsets of } C \text{ having exactly } k \text{ positive elements})}_{\substack{=\binom{a}{k}\binom{b}{n-k} \\ \text{(by Claim 1)}}} \\
&\qquad \left(\begin{array}{c}\text{since the number of positive elements of an } n\text{-element} \\ \text{subset of } C \text{ must always be an integer between 0 and } n\end{array}\right) \\
&= \sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k}.
\end{aligned}$$

Now, we have computed the number of n-element subsets of C in two ways. The first way yielded the result $\dbinom{a+b}{n}$, while the second way yielded $\sum\limits_{k=0}^{n} \dbinom{a}{k}\dbinom{b}{n-k}$. But these two results clearly have to be equal. In other words, we have

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k}.$$

Thus, Lemma 2.17.15 holds.

(This was an example of a proof by *double counting*, also known as a *combinatorial proof*. See [LeLeMe18, §15.10] for some more examples of such proofs, and see most textbooks on combinatorics for more.) □

[78] The combinatorial principle we are using here is the so-called *product rule* (see, e.g., [Loehr11, 1.8] or [LeLeMe18, §15.2.1]).

[79] The combinatorial principle we are using in the following computation is the so-called *sum rule* (see, e.g., [Loehr11, 1.2] or [LeLeMe18, §15.2.3]).

This shows that Theorem 2.17.14 holds for all $x \in \mathbb{N}$ and $y \in \mathbb{N}$. In order to extend its reach to arbitrary rational a and b, we shall use the "polynomial identity trick". First, let us briefly explain what polynomials are, without giving a formal definition.

Informally, a *polynomial* (in 1 variable x, with rational coefficients) is an "expression" of the form $a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$, where $a_k, a_{k-1}, \ldots, a_0$ are (fixed) rational numbers and where x is a (so far meaningless) symbol (called *indeterminate* or *variable*). For example, $4x^3 + 2x^2 - \frac{1}{3}x + \frac{2}{7}$ is a polynomial, and so is $0x^3 + x^2 - 0x + \frac{1}{3}$. We can omit terms of the form "$0x^i$" when writing down a polynomial and treat the result as being the same polynomial; thus, $0x^3 + x^2 - 0x + \frac{1}{3}$ can also be written as $x^2 - 0x + \frac{1}{3}$ and as $x^2 + \frac{1}{3}$. Likewise, we can treat the "+" signs as signifying addition and behaving like it, so, e.g., commutativity holds: $2x^3 + 5x$ and $5x + 2x^3$ are the same polynomial (but $2x + 5x^3$ is different). We also pretend that distributivity holds, so "like terms" can be combined: e.g., we have $4x^3 + 9x^3 = (4+9)x^3 = 13x^3$ or $4x^3 - 12x^3 = (4-12)x^3 = -8x^3$. Thus, we can add two polynomials: for example,

$$\left(3x^2 - 1x + \frac{1}{2}\right) + (6x - 7) = 3x^2 + \underbrace{(-1+6)}_{=5} x + \underbrace{\left(\frac{1}{2} - 7\right)}_{=\frac{-13}{2}} = 3x^2 + 5x + \frac{-13}{2}.$$

By pretending that the x^i (with $i \in \mathbb{N}$) are actual powers of the symbol x, and that multiplication obeys the associativity law (so that $\left(\lambda x^i\right) x^j = \lambda \left(x^i x^j\right) = \lambda x^{i+j}$ for rational λ and $i, j \in \mathbb{N}$), we can multiply polynomials as well (first use distributivity to expand the product):

$$\begin{aligned}(3x-5)\left(x^2+3x+2\right) &= 3x\left(x^2+3x+2\right) - 5\left(x^2+3x+2\right) \\ &= \left(3x^3+9x^2+6x\right) - \left(5x^2+15x+10\right) \\ &= 3x^3+4x^2-9x-10.\end{aligned}$$

Most importantly, it is possible to *substitute* a number into a polynomial: If $u \in \mathbb{Q}$ and if $P = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ is a polynomial, then we define $P(u)$ (called the *evaluation* of P *at* u, or the *result of substituting* u *for* x *in* P) to be the number $a_k u^k + a_{k-1} u^{k-1} + \cdots + a_0$. More generally, if the polynomial P is given in any of its forms (e.g., as a product of other polynomials), then we can compute $P(u)$ by replacing each x appearing in this form by an u. For example, if $P = (2x+1)(3x+1) - (4x+1)(5x+1)$, then $P(u) = (2u+1)(3u+1) - (4u+1)(5u+1)$; thus, we do not need to expand P before substituting u into it.

Even more generally, u does not have to be a rational number in order to be substituted in a polynomial P – it can be (roughly speaking!) anything that can be taken to the i-th power for $i \in \mathbb{N}$ and that can be added and multiplied by a rational number. For example, u can be a real number or a square matrix or another polynomial. (We will later learn the precise meaning of "anything" here[80].)

We have been vague in our definition of polynomials, since making it rigorous would take us a fair way afield. But we **will** eventually (in Chapter 7) define polynomials rigorously and prove that all of the above claims (e.g., about associativity and distributivity) actually hold. For now, we need a basic property of polynomials:

Proposition 2.17.16. Let P and Q be two polynomials in 1 variable x with rational coefficients. Assume that infinitely many $u \in \mathbb{Q}$ satisfy $P(u) = Q(u)$. Then, $P = Q$ (as polynomials).

We will prove Proposition 2.17.16 later (in Section 7.7).[81]

Note that polynomials are not functions – despite the fact that we can substitute numbers into them and obtain other numbers. However, in many regards, they behave like functions. For what we are going to do in this section, the difference does not matter; we can treat polynomials as functions here.

With Lemma 2.17.15, we have proven Theorem 2.17.14 in the case when x and y belong to $\mathbb{N}$. Our goal, however, is to prove it for arbitrary $x, y \in \mathbb{Q}$. Let us first lift it to an intermediate level of generality – allowing x to be arbitrary, but still requiring $y \in \mathbb{N}$. Thus, we want to prove the following lemma:

Lemma 2.17.17. Let $a \in \mathbb{Q}$, $b \in \mathbb{N}$ and $n \in \mathbb{N}$. Then,

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}.$$

Proof of Lemma 2.17.17 (sketched). Let us define a polynomial P in 1 variable x with rational coefficients as follows:

$$P = \binom{x+b}{n}. \tag{85}$$

The "binomial coefficient" $\binom{x+b}{n}$ here is to be understood by extending Definition 2.17.1 **(a)** in the obvious fashion to the case when n is a polynomial (in our case, $x+b$) rather than a rational number. Thus,

$$\binom{x+b}{n} = \frac{(x+b)(x+b-1)(x+b-2)\cdots(x+b-n+1)}{n!}.$$

[80] Namely, "anything" will be concretized to mean "any element of a $\mathbb{Q}$-algebra". See Definition 7.6.1 for the details.

[81] Note that it is closely related to the Proposition 1.6.6 we used above.

Let us also define a polynomial Q in 1 variable x with rational coefficients as follows:

$$Q = \sum_{k=0}^{n} \binom{x}{k} \binom{b}{n-k}. \tag{86}$$

(Again, the "binomial coefficients" $\binom{x}{k}$ are defined via our extension of Definition 2.17.1 **(a)**, and can be explicitly written as $\binom{x}{k} = \dfrac{x(x-1)(x-2)\cdots(x-k+1)}{k!}$. Meanwhile, the $\binom{b}{n-k}$ are just constant integers.)

Now, for each $u \in \mathbb{N}$, we have

$$\begin{aligned} P(u) &= \binom{u+b}{n} \qquad \text{(by substituting } u \text{ for } x \text{ in the equality (85))} \\ &= \sum_{k=0}^{n} \binom{u}{k} \binom{b}{n-k} \end{aligned}$$

(by Lemma 2.17.15, applied to u instead of a) and

$$Q(u) = \sum_{k=0}^{n} \binom{u}{k} \binom{b}{n-k}$$

(by substituting u for x in the equality (86)). Comparing these two equalities, we obtain $P(u) = Q(u)$ for all $u \in \mathbb{N}$. Hence, infinitely many $u \in \mathbb{Q}$ satisfy $P(u) = Q(u)$ (since infinitely many $u \in \mathbb{Q}$ satisfy $u \in \mathbb{N}$). Thus, Proposition 2.17.16 yields $P = Q$. In view of (85) and (86), this rewrites as

$$\binom{x+b}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{b}{n-k}. \tag{87}$$

Now, substituting a for x in this equality of polynomials, we obtain $\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}$. This proves Lemma 2.17.17. □

Let us summarize the main idea of this proof: We replaced the rational number a by the indeterminate x, thus transforming the identity we were proving into an equality between two polynomials (namely, $P = Q$). But in order to prove an equality between polynomials, it suffices to prove that it holds at infinitely many numbers (by Proposition 2.17.16); thus, in particular, it suffices to check it at all nonnegative integers. But this is precisely what we did in Lemma 2.17.15 above. This kind of argument (with its use of Proposition 2.17.16) is known as the "polynomial identity trick".

Now, let us extend the reach of Lemma 2.17.17 further, allowing both a and b to be arbitrary (and thus obtaining the whole Theorem 2.17.14):

Lemma 2.17.18. Let $a, b \in \mathbb{Q}$ and $n \in \mathbb{N}$. Then,

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}.$$

Proof of Lemma 2.17.18 (sketched). Deriving Lemma 2.17.18 from Lemma 2.17.17 is very similar to deriving Lemma 2.17.17 from Lemma 2.17.15. The main difference is that we replace b (rather than a) by the indeterminate x now.

Here are the details: Let us define a polynomial P in 1 variable x with rational coefficients as follows:

$$P = \binom{a+x}{n}. \tag{88}$$

Let us also define a polynomial Q in 1 variable x with rational coefficients as follows:

$$Q = \sum_{k=0}^{n} \binom{a}{k} \binom{x}{n-k}. \tag{89}$$

Now, for each $u \in \mathbb{N}$, we have

$$\begin{aligned} P(u) &= \binom{a+u}{n} \qquad \text{(by substituting } u \text{ for } x \text{ in the equality (88))} \\ &= \sum_{k=0}^{n} \binom{a}{k} \binom{u}{n-k} \end{aligned}$$

(by Lemma 2.17.17, applied to u instead of b) and

$$Q(u) = \sum_{k=0}^{n} \binom{a}{k} \binom{u}{n-k}$$

(by substituting u for x in the equality (89)). Comparing these two equalities, we obtain $P(u) = Q(u)$ for all $u \in \mathbb{N}$. Hence, infinitely many $u \in \mathbb{Q}$ satisfy $P(u) = Q(u)$ (since infinitely many $u \in \mathbb{Q}$ satisfy $u \in \mathbb{N}$). Thus, Proposition 2.17.16 yields $P = Q$. In view of (88) and (89), this rewrites as

$$\binom{a+x}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{x}{n-k}.$$

Now, substituting b for x in this equality of polynomials, we obtain $\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}$. This proves Lemma 2.17.18. □

Proof of Theorem 2.17.14 (sketched). Theorem 2.17.14 is just Lemma 2.17.18, with a and b renamed as x and y. □

Exercise 2.17.3. Let $a, b \in \mathbb{N}$ and $m \in \mathbb{Q}$. Let A be an a-element set. Let B be a b-element subset of A. Prove that

$$(\text{the number of } m\text{-element subsets } S \text{ of } A \text{ satisfying } B \subseteq S) = \binom{a-b}{m-b}.$$

2.17.4. Some divisibilities and congruences

So far we have been proving identities between binomial coefficients. Let us now step to divisibilities and congruences.

Proposition 2.17.12 shows that binomial coefficients $\binom{n}{k}$ are integers whenever n is an integer. This allows us to study divisibilities and congruences between binomial coefficients (and you have seen a few of them on homework set #1). One of the most important such divisibilities is the following fact:

Theorem 2.17.19. Let p be a prime. Let $k \in \{1, 2, \ldots, p-1\}$. Then, $p \mid \binom{p}{k}$.

First proof of Theorem 2.17.19. Applying Theorem 2.17.9 to $n = p$, we obtain

$$k\binom{p}{k} = p\binom{p-1}{k-1}.$$

Thus, $p \mid k\binom{p}{k}$ (since $\binom{p-1}{k-1}$ is an integer[82]). But Proposition 2.13.4 (applied to $i = k$) yields that k is coprime to p. In other words, $k \perp p$, and thus $p \perp k$. Hence, Theorem 2.10.6 (applied to $a = p$, $b = k$ and $c = \binom{p}{k}$) yields $p \mid \binom{p}{k}$ (since $p \mid k\binom{p}{k}$). This proves Theorem 2.17.19. □

We shall see a second, combinatorial proof of Theorem 2.17.19 further below; it will rely on the concept of group actions.

Let us state two congruences for binomial coefficients, which we will show later using tools from abstract algebra:

Theorem 2.17.20 (Lucas's congruence)**.** Let p be a prime. Let $a, b \in \mathbb{Z}$. Let $c, d \in \{0, 1, \ldots, p-1\}$. Then,

$$\binom{pa+c}{pb+d} \equiv \binom{a}{b}\binom{c}{d} \bmod p.$$

[82] by an application of Proposition 2.17.12

Theorem 2.17.21 (Babbage's congruence)**.** Let p be a prime. Let $a, b \in \mathbb{Z}$. Then,

$$\binom{pa}{pb} \equiv \binom{a}{b} \operatorname{mod} p^2.$$

For the impatient: Elementary proofs of Theorem 2.17.20 and Theorem 2.17.21 can be found in [Grinbe17].

Remark 2.17.22. Lucas's congruence has the following consequence: Let p be a prime. Let $a, b \in \mathbb{N}$. Write a and b in base p as follows:

$$a = a_k p^k + a_{k-1} p^{k-1} + \cdots + a_0 p^0 \qquad \text{and}$$
$$b = b_k p^k + b_{k-1} p^{k-1} + \cdots + b_0 p^0$$

with $k \in \mathbb{N}$ and $a_k, a_{k-1}, \ldots, a_0, b_k, b_{k-1}, \ldots, b_0 \in \{0, 1, \ldots, p-1\}$. (Note that we allow "leading zeroes" – i.e., any of a_k and b_k can be 0.) Then,

$$\binom{a}{b} \equiv \binom{a_k}{b_k} \binom{a_{k-1}}{b_{k-1}} \cdots \binom{a_0}{b_0} \operatorname{mod} p.$$

(This can be easily proven by induction on k, using Theorem 2.17.20 in the induction step.) This allows for quick computation of remainders of $\binom{a}{b}$ modulo prime numbers, and also explains (when applied to $p = 2$) why we can obtain (an approximation of) Sierpinski's triangle from Pascal's triangle by coloring all even numbers white and all odd numbers black.

See [Mestro14] and [Granvi05] for overviews of more complicated divisibilities and congruences for binomial coefficients.

Exercise 2.17.4. Let p be a prime.

(a) Prove that $\binom{2p}{p} \equiv 2 \operatorname{mod} p$.

(b) Prove that $\binom{2p-1}{p} \equiv 1 \operatorname{mod} p$.

(c) Prove that $\binom{p-1+k}{k} \equiv 0 \operatorname{mod} p$ for each $k \in \{1, 2, \ldots, p-1\}$.

[**Hint:** This is very easy using Lucas's congruence, but you can also solve it without it.]

2.17.5. Integer-valued polynomials

Now that we have introduced polynomials (albeit informally and on somewhat shaky foundations) and binomial coefficients (albeit briefly), it would be a shame to leave unmentioned a subject that connects the two particularly closely: the *integer-valued polynomials*. We are going to state a few basic facts, but we will not prove them.

If $f = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ is a polynomial (in 1 variable x, with rational coefficients), then the rational numbers $a_k, a_{k-1}, \ldots, a_0$ are called the *coefficients* of f. The coefficients of a polynomial f are uniquely determined by f (except for the fact that we can always add terms of the form $0x^\ell$ and thus obtain extra coefficients that are equal to 0). (This fact is not obvious, given our "definition" of polynomials above[83]. We will later define polynomials more formally as sequences of coefficients; then this will become clear.)

If $f = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ is a polynomial (in 1 variable x, with rational coefficients) such that $a_k \neq 0$ (each polynomial that is not just 0 can be uniquely written in such a form), then the integer k is called the *degree* of f.

Definition 2.17.23. A polynomial P with rational coefficients is said to be *integer-valued* if $(P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z})$.

Of course, a polynomial with integer coefficients is always integer-valued. But there are other integer-valued polynomials, too:

Example 2.17.24. (a) The polynomial $\dbinom{x}{2} = \dfrac{x(x-1)}{2} = \dfrac{1}{2}x^2 - \dfrac{1}{2}x$ is integer-valued (since $\dbinom{n}{2} \in \mathbb{Z}$ for each $n \in \mathbb{Z}$), but its coefficients are $\dfrac{1}{2}, -\dfrac{1}{2}, 0$.

(b) More generally: If $k \in \mathbb{N}$ is arbitrary, then the polynomial $\dbinom{x}{k} = \dfrac{x(x-1)(x-2)\cdots(x-k+1)}{k!}$ is integer-valued (since $\dbinom{n}{k} \in \mathbb{Z}$ for each $n \in \mathbb{Z}$).

(c) If p is any prime, then the polynomial $\dfrac{x^p - x}{p}$ is integer-valued (since Theorem 2.15.1 **(b)** yields $a^p \equiv a \mod p$ for each $a \in \mathbb{Z}$, which means that $\dfrac{a^p - a}{p} \in \mathbb{Z}$ for each $a \in \mathbb{Z}$). Its coefficients are not integers.

This suggests the following question: How can we describe the integer-valued polynomials? The following result of Pólya [Polya19] gives an answer:

Theorem 2.17.25. Let $k \in \mathbb{N}$.

[83] For example, why cannot we start with (say) $6x^2 + 5x + 4$, then rewrite it as $(2x+1)(3x+1) + 3$, then do some other transformations (using commutativity, associativity and other laws), and finally end up with a polynomial that has different coefficients (say, $3x^2 + 9x + 4$) ? We cannot, but it is not easy to prove with what we have.

(a) Any polynomial P (in 1 variable x, with rational coefficients) of degree k can be uniquely written in the form

$$P(x) = a_k \binom{x}{k} + a_{k-1} \binom{x}{k-1} + \cdots + a_0 \binom{x}{0}$$

with **rational** $a_k, a_{k-1}, \ldots, a_0$.

(b) The polynomial P is integer-valued if and only if these $a_k, a_{k-1}, \ldots, a_0$ are integers.

For example, the integer-valued polynomial $\dfrac{x^3 - x}{3}$ can be written as

$$\frac{x^3 - x}{3} = a_3 \binom{x}{3} + a_2 \binom{x}{2} + a_1 \binom{x}{1} + a_0 \binom{x}{0}$$

for

$$a_3 = 2, \qquad a_2 = 2, \qquad a_1 = 0, \qquad a_0 = 0.$$

These a_3, a_2, a_1, a_0 are integers – exactly as Theorem 2.17.25 **(b)** says.

I sketched a proof of Theorem 2.17.25 **(b)** in a talk in 2013 (`https://www.cip.ifi.lmu.de/~grinberg/storrs2013.pdf`)[84]. See also [daSilv12] for a self-contained proof.

2.18. Counting divisors

2.18.1. The number of divisors of n

Now that we have seen some combinatorial reasoning (e.g., in the proof of Theorem 2.17.14), let us solve a rather natural counting problem: Let us count the divisors of a nonzero integer n.

Proposition 2.18.1. Let $n \in \mathbb{Z}$ be nonzero. Then:

(a) The product $\prod\limits_{p \text{ prime}} (v_p(n) + 1)$ is well-defined, since all but finitely many of its factors are 1.

(b) We have

$$(\text{the number of positive divisors of } n) = \prod_{p \text{ prime}} (v_p(n) + 1).$$

(c) We have

$$(\text{the number of divisors of } n) = 2 \prod_{p \text{ prime}} (v_p(n) + 1).$$

[84] In this talk, I refer to integer-valued polynomials as "integral-valued polynomials".

Example 2.18.2. If $n = 12$, then

$$(\text{the number of positive divisors of } n) = 6$$

(since the positive divisors of $n = 12$ are $1, 2, 3, 4, 6, 12$) and

$$\begin{aligned}\prod_{p \text{ prime}} (v_p(n) + 1) &= \left(\underbrace{v_2(n)}_{=2} + 1 \right) \left(\underbrace{v_3(n)}_{=1} + 1 \right) \prod_{\substack{p \text{ prime;} \\ p \notin \{2,3\}}} \left(\underbrace{v_p(n)}_{=0} + 1 \right) \\ &= (2+1)(1+1) \underbrace{\prod_{\substack{p \text{ prime;} \\ p \notin \{2,3\}}} 1}_{=1} = (2+1)(1+1) = 6.\end{aligned}$$

This confirms Proposition 2.18.1 **(b)** for $n = 12$. In order to confirm Proposition 2.18.1 **(c)** for $n = 12$ as well, we observe that $(\text{the number of divisors of } n) = 12$ (since the divisors of $n = 12$ are $-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12$).

The function

$$\begin{aligned}\{1, 2, 3, \ldots\} &\to \mathbb{N}, \\ n &\mapsto (\text{the number of positive divisors of } n)\end{aligned}$$

is known as the *divisor function* and is commonly denoted by τ. So Proposition 2.18.1 **(b)** gives a formula for $\tau(n)$. See [Grinbe16, Theorem 2.1.7 (proof sketched in §2.7)] for a different proof of this formula.

Our proof of Proposition 2.18.1 will rely on the following lemma, which classifies all divisors of a positive integer in terms of its prime factorization:

Lemma 2.18.3. Let $p_1, p_2, \ldots, p_u$ be finitely many distinct primes. For each $i \in \{1, 2, \ldots, u\}$, let a_i be a nonnegative integer. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}$.

Define a set T by

$$\begin{aligned}T &= \{0, 1, \ldots, a_1\} \times \{0, 1, \ldots, a_2\} \times \cdots \times \{0, 1, \ldots, a_u\} \\ &= \{(b_1, b_2, \ldots, b_u) \mid b_i \in \{0, 1, \ldots, a_i\} \text{ for each } i \in \{1, 2, \ldots, u\}\} \\ &= \{(b_1, b_2, \ldots, b_u) \in \mathbb{N}^u \mid b_i \leq a_i \text{ for each } i \in \{1, 2, \ldots, u\}\}.\end{aligned}$$

Then, the map

$$\begin{aligned}\Lambda : T &\to \{\text{positive divisors of } n\}, \\ (b_1, b_2, \ldots, b_u) &\mapsto p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u}\end{aligned}$$

is well-defined and bijective.

Example 2.18.4. For this example, let $u = 2$, $p_1 = 2$, $p_2 = 3$, $a_1 = 2$ and $a_2 = 1$. Define the integer n and the set T as in Lemma 2.18.3; then,

$$n = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u} = 2^2 \cdot 3^1 = 12$$

and

$$\begin{aligned} T &= \{0, 1, \ldots, a_1\} \times \{0, 1, \ldots, a_2\} \times \cdots \times \{0, 1, \ldots, a_u\} = \{0, 1, 2\} \times \{0, 1\} \\ &= \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1)\}. \end{aligned}$$

Now, Lemma 2.18.3 says that the map

$$\begin{aligned} \Lambda : T &\to \{\text{positive divisors of } n\}, \\ (b_1, b_2, \ldots, b_u) &\mapsto p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u} \end{aligned}$$

is well-defined and bijective. Here is a table of values of this map Λ:

$\mathbf{b}$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$
$\Lambda(\mathbf{b})$	1	3	2	6	4	12

.

Proof of Lemma 2.18.3. The numbers $p_1, p_2, \ldots, p_u$ are primes, and thus positive integers. Hence, the product $p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}$ is a positive integer as well (since $a_1, a_2, \ldots, a_u$ are nonnegative integers). In other words, n is a positive integer (since $n = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}$). Note that

$$n = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u} = \prod_{i=1}^{u} p_i^{a_i}.$$

Each $i \in \{1, 2, \ldots, u\}$ satisfies

$$v_{p_i}\left(\underbrace{n}_{=p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}}\right) = v_{p_i}\left(p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}\right) = a_i \qquad (90)$$

(by Exercise 2.13.7 **(a)**). Furthermore, if p is a prime satisfying $p \notin \{p_1, p_2, \ldots, p_u\}$, then

$$v_p\left(\underbrace{n}_{=p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}}\right) = v_p\left(p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}\right) = 0 \qquad (91)$$

(by Exercise 2.13.7 **(b)**).

For each $(b_1, b_2, \ldots, b_u) \in T$, we have

$$p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u} \in \{\text{positive divisors of } n\}. \qquad (92)$$

[*Proof of (92):* Let $(b_1, b_2, \ldots, b_u) \in T$. We must prove (92).

We have $(b_1, b_2, \ldots, b_u) \in T = \{0, 1, \ldots, a_1\} \times \{0, 1, \ldots, a_2\} \times \cdots \times \{0, 1, \ldots, a_u\}$. In other words, $b_i \in \{0, 1, \ldots, a_i\}$ for each $i \in \{1, 2, \ldots, u\}$. Hence, for each $i \in \{1, 2, \ldots, u\}$, we have

$$\begin{aligned} a_i - b_i &\in \{0, 1, \ldots, a_i\} \qquad (\text{since } b_i \in \{0, 1, \ldots, a_i\}) \\ &\subseteq \mathbb{N}, \end{aligned}$$

and thus $p_i^{a_i - b_i}$ is an integer. Hence, $\prod_{i=1}^{u} p_i^{a_i - b_i}$ is a product of integers, and thus is an integer as well. Likewise, $\prod_{i=1}^{u} p_i^{b_i}$ is an integer (since $b_i \in \{0, 1, \ldots, a_i\} \subseteq \mathbb{N}$ for each $i \in \{1, 2, \ldots, u\}$). Now,

$$n = \prod_{i=1}^{u} \underbrace{p_i^{a_i}}_{\substack{= p_i^{b_i + (a_i - b_i)} \\ = p_i^{b_i} p_i^{a_i - b_i}}} = \prod_{i=1}^{u} \left(p_i^{b_i} p_i^{a_i - b_i} \right) = \left(\prod_{i=1}^{u} p_i^{b_i} \right) \left(\prod_{i=1}^{u} p_i^{a_i - b_i} \right).$$

Thus, $\prod_{i=1}^{u} p_i^{b_i} \mid n$ (since $\prod_{i=1}^{u} p_i^{a_i - b_i}$ is an integer). In other words, $\prod_{i=1}^{u} p_i^{b_i}$ is a divisor of n. Hence, $\prod_{i=1}^{u} p_i^{b_i}$ is a positive divisor of n (since $\prod_{i=1}^{u} p_i^{b_i}$ is clearly positive). In other words, $\prod_{i=1}^{u} p_i^{b_i} \in \{\text{positive divisors of } n\}$. Hence, $p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u} = \prod_{i=1}^{u} p_i^{b_i} \in \{\text{positive divisors of } n\}$. This proves (92).]

The equality (92) shows that the map Λ in Lemma 2.18.3 is well-defined. It remains to prove that it is bijective.

We shall achieve this by constructing an inverse to Λ.

Indeed, for each $d \in \{\text{positive divisors of } n\}$, we have

$$\left(v_{p_1}(d), v_{p_2}(d), \ldots, v_{p_u}(d) \right) \in T. \tag{93}$$

[*Proof of (93):* Let $d \in \{\text{positive divisors of } n\}$. Thus, d is a positive divisor of n. In other words, d is a positive integer satisfying $d \mid n$.

Fix $i \in \{1, 2, \ldots, u\}$. We shall show that $v_{p_i}(d) \in \{0, 1, \ldots, a_i\}$.

The integer d is positive and thus nonzero. Hence, $v_{p_i}(d) \in \mathbb{N}$. But Proposition 2.13.35 (applied to d and n instead of n and m) shows that $d \mid n$ if and only if each prime p satisfies $v_p(d) \leq v_p(n)$. Thus, each prime p satisfies $v_p(d) \leq v_p(n)$ (since $d \mid n$). Applying this to $p = p_i$, we obtain $v_{p_i}(d) \leq v_{p_i}(n) = a_i$ (by (90)). Hence, $v_{p_i}(d) \in \{0, 1, \ldots, a_i\}$ (since $v_{p_i}(d) \in \mathbb{N}$).

Now, forget that we fixed i. We thus have shown that $v_{p_i}(d) \in \{0, 1, \ldots, a_i\}$ for each $i \in \{1, 2, \ldots, u\}$. In other words,

$$\left(v_{p_1}(d), v_{p_2}(d), \ldots, v_{p_u}(d) \right) \in \{0, 1, \ldots, a_1\} \times \{0, 1, \ldots, a_2\} \times \cdots \times \{0, 1, \ldots, a_u\}.$$

This rewrites as $\left(v_{p_1}(d), v_{p_2}(d), \ldots, v_{p_u}(d) \right) \in T$ (since $T = \{0, 1, \ldots, a_1\} \times \{0, 1, \ldots, a_2\} \times \cdots \times \{0, 1, \ldots, a_u\}$). Thus, (93) is proven.]

We now define a map

$$V : \{\text{positive divisors of } n\} \to T,$$
$$d \mapsto \left(v_{p_1}(d), v_{p_2}(d), \ldots, v_{p_u}(d)\right).$$

This map is well-defined, because of (93).

Now, we claim that $\Lambda \circ V = \operatorname{id}$.

[*Proof:* Let $d \in \{\text{positive divisors of } n\}$. We shall show that $(\Lambda \circ V)(d) = \operatorname{id}(d)$.

Indeed, d is a positive divisor of n (since $d \in \{\text{positive divisors of } n\}$). Hence, d is a positive integer and satisfies $d \mid n$. But Proposition 2.13.35 (applied to d and n instead of n and m) shows that $d \mid n$ if and only if each prime p satisfies $v_p(d) \leq v_p(n)$. Thus, each prime p satisfies $v_p(d) \leq v_p(n)$ (since $d \mid n$). Hence, if p is a prime satisfying $p \notin \{p_1, p_2, \ldots, p_u\}$, then we have

$$v_p(d) \leq v_p(n) = 0 \qquad \text{(by (91))}$$

and therefore

$$v_p(d) = 0 \qquad \left(\text{since } v_p(d) \in \mathbb{N} \cup \{\infty\} \text{ and } v_p(d) \leq 0\right)$$

and therefore

$$p^{v_p(d)} = p^0 = 1. \tag{94}$$

The elements $p_1, p_2, \ldots, p_u$ are distinct. Thus, the map $\{1, 2, \ldots, u\} \to \{p_1, p_2, \ldots, p_u\}$, $i \mapsto p_i$ is a bijection[85].

But d is a positive integer. Thus, Corollary 2.13.33 (applied to d instead of n) yields

$$d = \prod_{p \text{ prime}} p^{v_p(d)} = \left(\prod_{\substack{p \text{ prime};\\ p \in \{p_1, p_2, \ldots, p_u\}}} p^{v_p(d)}\right) \left(\prod_{\substack{p \text{ prime};\\ p \notin \{p_1, p_2, \ldots, p_u\}}} \underbrace{p^{v_p(d)}}_{\substack{=1\\ \text{(by (94))}}}\right)$$
$$\left(\begin{array}{c}\text{since each prime } p \text{ satisfies either } p \in \{p_1, p_2, \ldots, p_u\}\\ \text{or } p \notin \{p_1, p_2, \ldots, p_u\} \text{ (but not both simultaneously)}\end{array}\right)$$
$$= \left(\prod_{\substack{p \text{ prime};\\ p \in \{p_1, p_2, \ldots, p_u\}}} p^{v_p(d)}\right) \underbrace{\left(\prod_{\substack{p \text{ prime};\\ p \notin \{p_1, p_2, \ldots, p_u\}}} 1\right)}_{=1} = \underbrace{\prod_{\substack{p \text{ prime};\\ p \in \{p_1, p_2, \ldots, p_u\}}}}_{\substack{= \prod\limits_{p \in \{p_1, p_2, \ldots, p_u\}}\\ \text{(since each } p \in \{p_1, p_2, \ldots, p_u\}\\ \text{is a prime)}}} p^{v_p(d)}$$
$$= \prod_{p \in \{p_1, p_2, \ldots, p_u\}} p^{v_p(d)} = \prod_{i=1}^{u} p_i^{v_{p_i}(d)}$$
$$\left(\begin{array}{c}\text{here, we have substituted } p_i \text{ for } p \text{ in the product,}\\ \text{since the map } \{1, 2, \ldots, u\} \to \{p_1, p_2, \ldots, p_u\},\ i \mapsto p_i \text{ is a bijection}\end{array}\right).$$

[85] Indeed, this map is injective, since the elements $p_1, p_2, \ldots, p_u$ are distinct; and it is surjective, since its image is clearly $\{p_1, p_2, \ldots, p_u\}$.

Comparing this with

$$\begin{aligned}(\Lambda \circ V)(d) &= \Lambda\left(\underbrace{V(d)}_{\substack{=\left(v_{p_1}(d),v_{p_2}(d),\ldots,v_{p_u}(d)\right) \\ \text{(by the definition of } V\text{)}}}\right) = \Lambda\left(\left(v_{p_1}(d),v_{p_2}(d),\ldots,v_{p_u}(d)\right)\right) \\ &= p_1^{v_{p_1}(d)} p_2^{v_{p_2}(d)} \cdots p_u^{v_{p_u}(d)} = \prod_{i=1}^{u} p_i^{v_{p_i}(d)},\end{aligned}$$

we obtain $(\Lambda \circ V)(d) = d = \operatorname{id}(d)$.

Now, forget that we fixed d. We thus have shown that $(\Lambda \circ V)(d) = \operatorname{id}(d)$ for each $d \in \{\text{positive divisors of } n\}$. In other words, $\Lambda \circ V = \operatorname{id}$.]

Next, we claim that $V \circ \Lambda = \operatorname{id}$.

[*Proof:* Let $\mathbf{b} \in T$. We shall show that $(V \circ \Lambda)(\mathbf{b}) = \operatorname{id}(\mathbf{b})$.

Indeed, we have $\mathbf{b} \in T = \{0,1,\ldots,a_1\} \times \{0,1,\ldots,a_2\} \times \cdots \times \{0,1,\ldots,a_u\}$. Thus, $\mathbf{b}$ is a u-tuple of nonnegative integers. Hence, write $\mathbf{b}$ in the form $\mathbf{b} = (b_1,b_2,\ldots,b_u)$ for some u nonnegative integers $b_1,b_2,\ldots,b_u$. Then, the definition of Λ yields $\Lambda(\mathbf{b}) = p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u}$. Hence, for each $i \in \{1,2,\ldots,u\}$, we have

$$v_{p_i}\left(\underbrace{\Lambda(\mathbf{b})}_{=p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u}}\right) = v_{p_i}\left(p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u}\right) = b_i$$

(by Exercise 2.13.7 **(a)**, applied to b_i instead of a_i). In other words,

$$\left(v_{p_1}(\Lambda(\mathbf{b})), v_{p_2}(\Lambda(\mathbf{b})), \ldots, v_{p_u}(\Lambda(\mathbf{b}))\right) = (b_1,b_2,\ldots,b_u).$$

Now,

$$\begin{aligned}(V \circ \Lambda)(\mathbf{b}) &= V(\Lambda(\mathbf{b})) \\ &= \left(v_{p_1}(\Lambda(\mathbf{b})), v_{p_2}(\Lambda(\mathbf{b})), \ldots, v_{p_u}(\Lambda(\mathbf{b}))\right) \qquad \text{(by the definition of } V\text{)} \\ &= (b_1,b_2,\ldots,b_u) = \mathbf{b} = \operatorname{id}(\mathbf{b}).\end{aligned}$$

Now, forget that we fixed $\mathbf{b}$. We have thus proven that $(V \circ \Lambda)(\mathbf{b}) = \operatorname{id}(\mathbf{b})$ for each $\mathbf{b} \in T$. In other words, $V \circ \Lambda = \operatorname{id}$.]

We have now proven the equalities $\Lambda \circ V = \operatorname{id}$ and $V \circ \Lambda = \operatorname{id}$. These equalities show that the maps Λ and V are mutually inverse. Hence, the map Λ is invertible, i.e., bijective. This completes the proof of Lemma 2.18.3. □

Proof of Proposition 2.18.1. The integer $|n|$ is positive (since n is nonzero) and thus nonzero. We observe that

$$\{\text{positive divisors of } |n|\} = \{\text{positive divisors of } n\} \tag{95}$$

[86]. Hence,

$$\begin{aligned}&\left(\text{the number of positive divisors of } \left|n\right|\right)\\ &= \left(\text{the number of positive divisors of } n\right).\end{aligned} \tag{97}$$

The same argument (but with the word "positive" removed) yields

$$\left(\text{the number of divisors of } \left|n\right|\right) = \left(\text{the number of divisors of } n\right). \tag{98}$$

Finally, Exercise 2.13.5 yields that

$$v_p\left(\left|n\right|\right) = v_p\left(n\right) \qquad \text{for each prime } p. \tag{99}$$

The claim of Proposition 2.18.1 does not change if we replace n by $\left|n\right|$ (because of (97), (98) and (99)). Thus, we can WLOG assume that $n \geq 0$ (since otherwise, we can just replace n by $\left|n\right|$). Assume this. Combining $n \neq 0$ (since n is nonzero) with $n \geq 0$, we find $n > 0$. Hence, n is a positive integer.

(a) For every prime $p > \left|n\right|$, we have $v_p\left(n\right) = 0$ (by Lemma 2.13.32 **(a)**) and thus $\underbrace{v_p\left(n\right)}_{=0} + 1 = 1$. Thus, all but finitely many primes p satisfy $v_p\left(n\right) + 1 = 1$ (since all but finitely many primes p satisfy $p > \left|n\right|$). Therefore, all but finitely many factors of the product $\prod\limits_{p \text{ prime}} \left(v_p\left(n\right) + 1\right)$ are 1. In other words, the product $\prod\limits_{p \text{ prime}} \left(v_p\left(n\right) + 1\right)$ has only finitely many factors different from 1. Hence, this product is well-defined. This proves Proposition 2.18.1 **(a)**.

(b) For every prime $p > \left|n\right|$, we have $v_p\left(n\right) = 0$ (by Lemma 2.13.32 **(a)**). Thus, all but finitely many primes p satisfy $v_p\left(n\right) = 0$ (since all but finitely many primes

[86] *Proof of (95):* Let $d \in \left\{\text{positive divisors of } \left|n\right|\right\}$. Thus, d is a positive divisor of $\left|n\right|$. In other words, d is a positive integer and satisfies $d \mid \left|n\right|$. But $\left|n\right| \mid n$ (by Exercise 2.2.1 **(b)**, applied to $a = n$). Hence, Proposition 2.2.4 **(b)** (applied to $a = d$, $b = \left|n\right|$ and $c = n$) shows that $d \mid n$. Thus, d is a positive integer and satisfies $d \mid n$. In other words, d is a positive divisor of n. In other words, $d \in \left\{\text{positive divisors of } n\right\}$.

Now, forget that we fixed d. We thus have proven that $d \in \left\{\text{positive divisors of } n\right\}$ for each $d \in \left\{\text{positive divisors of } \left|n\right|\right\}$. In other words,

$$\left\{\text{positive divisors of } \left|n\right|\right\} \subseteq \left\{\text{positive divisors of } n\right\}. \tag{96}$$

Let $e \in \left\{\text{positive divisors of } n\right\}$. Thus, e is a positive divisor of n. In other words, e is a positive integer and satisfies $e \mid n$. But $n \mid \left|n\right|$ (by Exercise 2.2.1 **(a)**, applied to $a = n$). Hence, Proposition 2.2.4 **(b)** (applied to $a = e$, $b = n$ and $c = \left|n\right|$) shows that $e \mid \left|n\right|$. Thus, e is a positive integer and satisfies $e \mid \left|n\right|$. In other words, e is a positive divisor of $\left|n\right|$. In other words, $e \in \left\{\text{positive divisors of } \left|n\right|\right\}$.

Now, forget that we fixed e. We thus have proven that $e \in \left\{\text{positive divisors of } \left|n\right|\right\}$ for each $e \in \left\{\text{positive divisors of } n\right\}$. In other words,

$$\left\{\text{positive divisors of } n\right\} \subseteq \left\{\text{positive divisors of } \left|n\right|\right\}.$$

Combining this with (96), we obtain $\left\{\text{positive divisors of } \left|n\right|\right\} = \left\{\text{positive divisors of } n\right\}$. Thus, (95) is proven.

p satisfy $p > |n|$). In other words, the set of all primes p satisfying $v_p(n) \neq 0$ is finite. Let P be this set. Thus, P is finite.

Let $(p_1, p_2, \ldots, p_u)$ be a list of elements of P, with no repetitions.[87] Thus,

$$\{p_1, p_2, \ldots, p_u\} = P.$$

The elements $p_1, p_2, \ldots, p_u$ are distinct (since $(p_1, p_2, \ldots, p_u)$ is a list with no repetitions). Thus, the map $\{1, 2, \ldots, u\} \to \{p_1, p_2, \ldots, p_u\}$, $i \mapsto p_i$ is a bijection[88]. Moreover, the elements $p_1, p_2, \ldots, p_u$ belong to $\{p_1, p_2, \ldots, p_u\} = P$, and thus are primes (since P is a set of primes).

If p is a prime such that $p \notin \{p_1, p_2, \ldots, p_u\}$, then

$$v_p(n) = 0. \tag{100}$$

[*Proof of (100):* Recall that P is the set of all primes p satisfying $v_p(n) \neq 0$ (by the definition of P). Hence, every prime p satisfying $v_p(n) \neq 0$ must belong to P. Thus, if p is a prime that does not belong to P, then p cannot satisfy $v_p(n) \neq 0$. In other words, if p is a prime that does not belong to P, then p must satisfy $v_p(n) = 0$. In other words, if p is a prime such that $p \notin P$, then $v_p(n) = 0$. Since $\{p_1, p_2, \ldots, p_u\} = P$, this rewrites as follows: If p is a prime such that $p \notin \{p_1, p_2, \ldots, p_u\}$, then $v_p(n) = 0$. This proves (100).]

If p is a prime such that $p \notin \{p_1, p_2, \ldots, p_u\}$, then

$$\begin{aligned} p^{v_p(n)} &= p^0 \qquad \left(\text{since (100) yields } v_p(n) = 0\right) \\ &= 1 \end{aligned} \tag{101}$$

and

$$\underbrace{v_p(n)}_{\substack{=0 \\ (\text{by (100)})}} + 1 = 1. \tag{102}$$

For each $i \in \{1, 2, \ldots, u\}$, define a nonnegative integer a_i by

$$a_i = v_{p_i}(n). \tag{103}$$

This is well-defined, since p_i is a prime (because $p_1, p_2, \ldots, p_u$ are primes) and since n is nonzero.

Define a set T as in Lemma 2.18.3.

[87] Such a list exists, since P is finite.

[88] Indeed, this map is injective, since the elements $p_1, p_2, \ldots, p_u$ are distinct; and it is surjective, since its image is clearly $\{p_1, p_2, \ldots, p_u\}$.

Recall that n is a positive integer. Thus, Corollary 2.13.33 yields

$$\begin{aligned}
n &= \prod_{p \text{ prime}} p^{v_p(n)} = \left(\prod_{\substack{p \text{ prime;} \\ p \in \{p_1, p_2, \ldots, p_u\}}} p^{v_p(n)} \right) \left(\prod_{\substack{p \text{ prime;} \\ p \notin \{p_1, p_2, \ldots, p_u\}}} \underbrace{p^{v_p(n)}}_{\substack{=1 \\ \text{(by (101))}}} \right) \\
&\qquad \left(\begin{array}{c} \text{since each prime } p \text{ satisfies either } p \in \{p_1, p_2, \ldots, p_u\} \\ \text{or } p \notin \{p_1, p_2, \ldots, p_u\} \text{ (but not both simultaneously)} \end{array} \right) \\
&= \left(\prod_{\substack{p \text{ prime;} \\ p \in \{p_1, p_2, \ldots, p_u\}}} p^{v_p(n)} \right) \underbrace{\left(\prod_{\substack{p \text{ prime;} \\ p \notin \{p_1, p_2, \ldots, p_u\}}} 1 \right)}_{=1} = \underbrace{\prod_{\substack{p \text{ prime;} \\ p \in \{p_1, p_2, \ldots, p_u\}}}}_{\substack{= \prod_{p \in \{p_1, p_2, \ldots, p_u\}} \\ \text{(since each } p \in \{p_1, p_2, \ldots, p_u\} \\ \text{is a prime)}}} p^{v_p(n)} \\
&= \prod_{p \in \{p_1, p_2, \ldots, p_u\}} p^{v_p(n)} = \prod_{i=1}^{u} \underbrace{p_i^{v_{p_i}(n)}}_{\substack{= p_i^{a_i} \\ \text{(since (103)} \\ \text{yields } v_{p_i}(n) = a_i)}} \\
&\qquad \left(\begin{array}{c} \text{here, we have substituted } p_i \text{ for } p \text{ in the product,} \\ \text{since the map } \{1, 2, \ldots, u\} \to \{p_1, p_2, \ldots, p_u\},\ i \mapsto p_i \text{ is a bijection} \end{array} \right) \\
&= \prod_{i=1}^{u} p_i^{a_i} = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}.
\end{aligned}$$

Hence, Lemma 2.18.3 shows that the map

$$\Lambda : T \to \{\text{positive divisors of } n\},$$
$$(b_1, b_2, \ldots, b_u) \mapsto p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u}$$

is well-defined and bijective.

Thus, there is a bijective map from T to $\{\text{positive divisors of } n\}$ (namely, Λ). Hence,

$$\begin{aligned}
&|\{\text{positive divisors of } n\}| \\
&= |T| = |\{0, 1, \ldots, a_1\} \times \{0, 1, \ldots, a_2\} \times \cdots \times \{0, 1, \ldots, a_u\}| \\
&\qquad (\text{since } T = \{0, 1, \ldots, a_1\} \times \{0, 1, \ldots, a_2\} \times \cdots \times \{0, 1, \ldots, a_u\}) \\
&= |\{0, 1, \ldots, a_1\}| \cdot |\{0, 1, \ldots, a_2\}| \cdot \cdots \cdot |\{0, 1, \ldots, a_u\}| \\
&\qquad \left(\begin{array}{c} \text{since the product rule } |A_1 \times A_2 \times \cdots \times A_u| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_u| \\ \text{holds whenever } A_1, A_2, \ldots, A_u \text{ are any } u \text{ finite sets} \end{array} \right) \\
&= \prod_{i=1}^{u} \underbrace{|\{0, 1, \ldots, a_i\}|}_{= a_i + 1} = \prod_{i=1}^{u} (a_i + 1).
\end{aligned}$$

Comparing this with

$$\begin{aligned}
&\prod_{p \text{ prime}} \left(v_p\left(n\right)+1\right) \\
&= \left(\prod_{\substack{p \text{ prime;} \\ p \in \{p_1,p_2,\ldots,p_u\}}} \left(v_p\left(n\right)+1\right)\right) \left(\prod_{\substack{p \text{ prime;} \\ p \notin \{p_1,p_2,\ldots,p_u\}}} \underbrace{\left(v_p\left(n\right)+1\right)}_{\substack{=1 \\ \text{(by (102))}}}\right) \\
&\qquad \left(\begin{array}{c} \text{since each prime } p \text{ satisfies either } p \in \{p_1,p_2,\ldots,p_u\} \\ \text{or } p \notin \{p_1,p_2,\ldots,p_u\} \text{ (but not both simultaneously)} \end{array}\right) \\
&= \left(\prod_{\substack{p \text{ prime;} \\ p \in \{p_1,p_2,\ldots,p_u\}}} \left(v_p\left(n\right)+1\right)\right) \underbrace{\left(\prod_{\substack{p \text{ prime;} \\ p \notin \{p_1,p_2,\ldots,p_u\}}} 1\right)}_{=1} = \underbrace{\prod_{\substack{p \text{ prime;} \\ p \in \{p_1,p_2,\ldots,p_u\}}}}_{\substack{=\prod_{p \in \{p_1,p_2,\ldots,p_u\}} \\ \text{(since each } p \in \{p_1,p_2,\ldots,p_u\} \\ \text{is a prime)}}} \left(v_p\left(n\right)+1\right) \\
&= \prod_{p \in \{p_1,p_2,\ldots,p_u\}} \left(v_p\left(n\right)+1\right) = \prod_{i=1}^{u} \left(\underbrace{v_{p_i}\left(n\right)}_{\substack{=a_i \\ \text{(by (103))}}} +1\right) \\
&\qquad \left(\begin{array}{c} \text{here, we have substituted } p_i \text{ for } p \text{ in the product,} \\ \text{since the map } \{1,2,\ldots,u\} \to \{p_1,p_2,\ldots,p_u\},\ i \mapsto p_i \text{ is a bijection} \end{array}\right) \\
&= \prod_{i=1}^{u} \left(a_i+1\right),
\end{aligned}$$

we obtain

$$\left|\{\text{positive divisors of } n\}\right| = \prod_{p \text{ prime}} \left(v_p\left(n\right)+1\right).$$

Hence,

$$\begin{aligned}
(\text{the number of positive divisors of } n) &= \left|\{\text{positive divisors of } n\}\right| \\
&= \prod_{p \text{ prime}} \left(v_p\left(n\right)+1\right).
\end{aligned}$$

This proves Proposition 2.18.1 **(b)**.

(c) Every divisor of n is either positive or negative[89] (but clearly cannot be both

[89] *Proof.* Let d be a divisor of n. We must prove that d is either positive or negative.

We have $d \mid n$ (since d is a divisor of n). Thus, there is an integer e such that $n = de$. Consider this e. If we had $d = 0$, then we would have $n = \underbrace{d}_{=0} e = 0$, which would contradict the fact that n is nonzero. Hence, we cannot have $d = 0$. In other words, we have $d \neq 0$. Thus, d is a nonzero integer. Hence, d is either positive or negative. Qed.

at the same time). Hence,

$$\begin{aligned}&(\text{the number of divisors of } n)\\&=(\text{the number of positive divisors of } n)+(\text{the number of negative divisors of } n)\,.\end{aligned}$$

If d is a positive divisor of n, then $-d$ is a negative divisor of n [90]. Hence, we can define a map

$$A:\{\text{positive divisors of } n\}\to\{\text{negative divisors of } n\}\,,\qquad d\mapsto -d.$$

For similar reasons, we can define a map

$$B:\{\text{negative divisors of } n\}\to\{\text{positive divisors of } n\}\,,\qquad d\mapsto -d.$$

Consider these two maps A and B. Clearly, $A\circ B=\operatorname{id}$ (since each negative divisor d of n satisfies $(A\circ B)(d)=A\left(\underbrace{B(d)}_{=-d}\right)=A(-d)=-(-d)=d=\operatorname{id}(d)$) and $B\circ A=\operatorname{id}$ (similarly). Thus, these maps A and B are mutually inverse. Hence, the map A is invertible, i.e., a bijection.

Hence, there is a bijection between $\{\text{positive divisors of } n\}$ and $\{\text{negative divisors of } n\}$ (namely, A). Thus,

$$|\{\text{negative divisors of } n\}|=|\{\text{positive divisors of } n\}|\,,$$

so that

$$\begin{aligned}&(\text{the number of negative divisors of } n)\\&=|\{\text{negative divisors of } n\}|=|\{\text{positive divisors of } n\}|\\&=(\text{the number of positive divisors of } n)\,.\end{aligned}$$

Therefore,

$$\begin{aligned}&(\text{the number of divisors of } n)\\&=(\text{the number of positive divisors of } n)+\underbrace{(\text{the number of negative divisors of } n)}_{=(\text{the number of positive divisors of } n)}\\&=(\text{the number of positive divisors of } n)+(\text{the number of positive divisors of } n)\\&=2\cdot\underbrace{(\text{the number of positive divisors of } n)}_{\substack{=\prod\limits_{p\text{ prime}}(v_p(n)+1)\\(\text{by Proposition 2.18.1 }\textbf{(b)})}}=2\prod_{p\text{ prime}}(v_p(n)+1)\,.\end{aligned}$$

Hence, Proposition 2.18.1 **(c)** follows. □

[90] *Proof.* Let d be a positive divisor of n. We must prove that $-d$ is a negative divisor of n. Clearly, $-d$ is negative (since d is positive).

We have assumed that d is a positive divisor of n. In other words, d is a positive integer and satisfies $d\mid n$. But $d=(-d)(-1)$; thus, $-d\mid d$ (since -1 is an integer). Hence, $-d\mid d\mid n$. Hence, $-d$ is a divisor of n. Thus, $-d$ is a negative divisor of n (since $-d$ is negative). Qed.

> **Remark 2.18.5.** Proposition 2.18.1 can be used to re-prove Proposition 2.14.7. We leave the details of this argument to the reader.

2.18.2. The sum of the divisors of n

The method by which we proved Proposition 2.18.1 can be used (with a minor modification) to not just count the positive divisors of a positive integer n, but also (for example) to compute their sum or the sum of their squares. This relies on the following basic property of $\sum$ and $\prod$ signs:

> **Lemma 2.18.6.** Let $n \in \mathbb{N}$. For every $i \in \{1, 2, \ldots, n\}$, let Z_i be a finite set. For every $i \in \{1, 2, \ldots, n\}$ and every $k \in Z_i$, let $p_{i,k}$ be a number. Then,
>
> $$\prod_{i=1}^{n} \sum_{k \in Z_i} p_{i,k} = \sum_{(k_1,k_2,\ldots,k_n) \in Z_1 \times Z_2 \times \cdots \times Z_n} \prod_{i=1}^{n} p_{i,k_i}.$$
>
> (Note that if $n = 0$, then the Cartesian product $Z_1 \times Z_2 \times \cdots \times Z_n$ has no factors; it is what is called an *empty Cartesian product*. It is understood to be a 1-element set, and its single element is the 0-tuple $()$ (also known as the empty list).)

Lemma 2.18.6 is essentially a version of the distributivity law (or the FOIL method) for expanding a product of several sums, each of which has several factors. For example, if we take $n = 3$ and $Z_i = \{1, 2\}$ for each $i \in \{1, 2, 3\}$, then Lemma 2.18.6 says that

$$\begin{aligned} &(p_{1,1} + p_{1,2})(p_{2,1} + p_{2,2})(p_{3,1} + p_{3,2}) \\ &= p_{1,1}p_{2,1}p_{3,1} + p_{1,1}p_{2,1}p_{3,2} + p_{1,1}p_{2,2}p_{3,1} + p_{1,1}p_{2,2}p_{3,2} \\ &\qquad + p_{1,2}p_{2,1}p_{3,1} + p_{1,2}p_{2,1}p_{3,2} + p_{1,2}p_{2,2}p_{3,1} + p_{1,2}p_{2,2}p_{3,2} \end{aligned}$$

(which is precisely what you get if you expand the product $(p_{1,1} + p_{1,2})(p_{2,1} + p_{2,2})(p_{3,1} + p_{3,2})$ using the distributivity law). For another example, if we take $n = 2$ and $Z_i = \{1, 2, 3\}$ for each $i \in \{1, 2\}$, then Lemma 2.18.6 says that

$$\begin{aligned} (p_{1,1} + p_{1,2} + p_{1,3})(p_{2,1} + p_{2,2} + p_{2,3}) &= p_{1,1}p_{2,1} + p_{1,1}p_{2,2} + p_{1,1}p_{2,3} \\ &\quad + p_{1,2}p_{2,1} + p_{1,2}p_{2,2} + p_{1,2}p_{2,3} \\ &\quad + p_{1,3}p_{2,1} + p_{1,3}p_{2,2} + p_{1,3}p_{2,3} \end{aligned}$$

(which is, again, simply the result of expanding the left hand side). In the general case, the idea behind Lemma 2.18.6 is that if you expand the product[91]

$$\begin{aligned}
&\prod_{i=1}^{n} \sum_{k=1}^{m_i} p_{i,k} \\
&= \prod_{i=1}^{n} \left(p_{i,1} + p_{i,2} + \cdots + p_{i,m_i}\right) \\
&= \left(p_{1,1} + p_{1,2} + \cdots + p_{1,m_1}\right) \left(p_{2,1} + p_{2,2} + \cdots + p_{2,m_2}\right) \cdots \left(p_{n,1} + p_{n,2} + \cdots + p_{n,m_n}\right),
\end{aligned}$$

then you get a sum of $m_1 m_2 \cdots m_n$ terms, each of which has the form

$$p_{1,k_1} p_{2,k_2} \cdots p_{n,k_n} = \prod_{i=1}^{n} p_{i,k_i}$$

for some $(k_1, k_2, \ldots, k_n) \in \{1, 2, \ldots, m_1\} \times \{1, 2, \ldots, m_2\} \times \cdots \times \{1, 2, \ldots, m_n\}$. See [Grinbe15, proof of Lemma 7.160] for a rigorous proof of Lemma 2.18.6 (which uses induction and the distributivity law).

Now, we can state a formula for the sum of all positive divisors of a positive integer n, and more generally for the sum of the k-th powers of these positive divisors, where k is a fixed integer:

Exercise 2.18.1. Let n be a positive integer. Let $k \in \mathbb{Z}$. Prove that:

(a) The product $\prod_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(n) \cdot k}\right)$ is well-defined, since all but finitely many of its factors are 1.

(b) We have

$$\sum_{d \mid n} d^k = \prod_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(n) \cdot k}\right).$$

(Recall that the summation sign "$\sum_{d \mid n}$" means a sum over all **positive** divisors d of n.)

Example 2.18.7. If $n = 6$, then the positive divisors of n are $1, 2, 3, 6$. Thus, in this case, the claim of Exercise 2.18.1 **(b)** becomes

$$1^k + 2^k + 3^k + 6^k = \prod_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(6) \cdot k}\right).$$

[91] We are here assuming (for the sake of simplicity) that each set Z_i is $\{1, 2, \ldots, m_i\}$ for some $m_i \in \mathbb{N}$. This does not weaken the reach of Lemma 2.18.6, since each finite set Z_i can be relabelled as $\{1, 2, \ldots, m_i\}$ for $m_i = |Z_i|$.

This equality can easily be verified, since the right hand side is

$$\begin{aligned}
&\prod_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(6)\cdot k}\right) \\
&= \underbrace{\left(2^{0k} + 2^{1k} + \cdots + 2^{v_2(6)\cdot k}\right)}_{\substack{=2^{0k}+2^{1k} \\ (\text{since } v_2(6)=1)}} \cdot \underbrace{\left(3^{0k} + 3^{1k} + \cdots + 3^{v_3(6)\cdot k}\right)}_{\substack{=3^{0k}+3^{1k} \\ (\text{since } v_3(6)=1)}} \\
&\qquad \cdot \prod_{\substack{p \text{ prime;} \\ p\notin\{2,3\}}} \underbrace{\left(p^{0k} + p^{1k} + \cdots + p^{v_p(6)\cdot k}\right)}_{\substack{=p^{0k} \\ (\text{since } v_p(6)=0 \text{ (because } p\notin\{2,3\}))}} \\
&= \left(\underbrace{2^{0k}}_{=1} + \underbrace{2^{1k}}_{=2^k}\right) \cdot \left(\underbrace{3^{0k}}_{=1} + \underbrace{3^{1k}}_{=3^k}\right) \cdot \prod_{\substack{p \text{ prime;} \\ p\notin\{2,3\}}} \underbrace{p^{0k}}_{=1} \\
&= \left(1 + 2^k\right) \cdot \left(1 + 3^k\right) = \underbrace{1}_{=1^k} + 2^k + 3^k + \underbrace{2^k \cdot 3^k}_{=(2\cdot 3)^k = 6^k} = 1^k + 2^k + 3^k + 6^k.
\end{aligned}$$

Note that Proposition 2.18.1 **(b)** is the particular case of Exercise 2.18.1 **(b)** obtained when setting $k = 0$ (because each integer z satisfies $z^0 = 1$, and thus $\sum_{d \mid n} d^0$ is the number of positive divisors of n).

Exercise 2.18.2. Let n be a positive integer. Let

$$\begin{aligned}
z = &\left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4\right) \\
&\quad - \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4\right).
\end{aligned}$$

Prove the following:

(a) If there exists a prime p satisfying $p \equiv 3 \bmod 4$ and $v_p(n) \equiv 1 \bmod 2$, then $z = 0$.

(b) If there exists no prime p satisfying $p \equiv 3 \bmod 4$ and $v_p(n) \equiv 1 \bmod 2$, then

$$z = \prod_{\substack{p \text{ prime;} \\ p \equiv 1 \bmod 4}} \left(v_p(n) + 1\right).$$

[**Hint:** For every $u \in \mathbb{Z}$, set $L(u) = \begin{cases} 1, & \text{if } u\%4 = 1; \\ -1, & \text{if } u\%4 = 3; \\ 0, & \text{otherwise.} \end{cases}$ Prove that $L(uv) = L(u) \cdot L(v)$ for any integers u and v. Then, show that $z = \sum_{d \mid n} L(d)$. Exploit the similarity between the sum $\sum_{d \mid n} L(d)$ and the sum in Exercise 2.18.1 **(b)**.]

2.19. "Application": The Erdös–Ginzburg–Ziv theorem

In this section (which can be skipped at will), we shall apply some of what we learned above to prove a curious result found in 1961 by Erdős, Ginzburg and Ziv [ErGiZi61]:

Theorem 2.19.1. Let n be a positive integer. Let $a_1, a_2, \ldots, a_{2n-1}$ be any $2n-1$ integers (not necessarily distinct). Then, there exists an n-element subset S of $\{1, 2, \ldots, 2n-1\}$ such that $n \mid \sum\limits_{s \in S} a_s$.

In other words, this theorem says that if you are given $2n-1$ integers, then you can pick n of them (without picking the same one twice[92]) such that the sum of your pick is divisible by n.

Example 2.19.2. In the case when $n = 2$, Theorem 2.19.1 can be restated as follows: If a, b, c are three integers, then at least one of the sums $b + c$, $c + a$ and $a + b$ is even. This is easy to prove by contradiction: Assume the contrary; thus, all three sums $b + c$, $c + a$ and $a + b$ are odd. Hence, $(b + c) + (c + a) + (a + b)$ is a sum of three odd numbers, and thus itself must be odd (since odd + odd is even, and odd + even is odd). But this contradicts the fact that $(b + c) + (c + a) + (a + b) = 2(a + b + c)$ is even. Thus, we have proven Theorem 2.19.1 in the case when $n = 2$.

Many proofs of Theorem 2.19.1 are known (see [AloDub93] for an exposition), but none of them is overly easy. We shall present one of these proofs (the one in [AloDub93, §2.3]) that uses prime factorization, Fermat's little theorem and binomial coefficients.

First of all, we need a combinatorial lemma, which easily follows from Lemma 2.18.6:

Lemma 2.19.3. Let S be a finite set. For each $s \in S$, let a_s be an integer. Let $n \in \mathbb{N}$. Then,

$$\left(\sum_{s \in S} a_s \right)^n = \sum_{(k_1, k_2, \ldots, k_n) \in S^n} \prod_{i=1}^{n} a_{k_i}.$$

(Note that if $n = 0$, then the Cartesian power S^n has no factors; it consists of a single element, namely the empty 0-tuple $()$.)

Exercise 2.19.1. Prove Lemma 2.19.3.

We shall first prove Theorem 2.19.1 in the case when n is prime; i.e., we shall prove the following result:

[92] But if two of the $2n-1$ integers are equal, then you can have them both in your pick.

Lemma 2.19.4. Let p be a prime. Let $a_1, a_2, \ldots, a_{2p-1}$ be any $2p-1$ integers (not necessarily distinct). Then, there exists a p-element subset S of $\{1, 2, \ldots, 2p-1\}$ such that $p \mid \sum\limits_{s \in S} a_s$.

Proof of Lemma 2.19.4. Assume the contrary. Thus, there exists no p-element subset S of $\{1, 2, \ldots, 2p-1\}$ such that $p \mid \sum\limits_{s \in S} a_s$.

But $p > 1$ (since p is a prime) and thus $p - 1 > 0$, so that $p - 1 \in \mathbb{N}$. Also, $2p - 1 = p + \underbrace{(p-1)}_{>0} > p > 1$, so that $2p - 1 \in \mathbb{N}$.

Let A be the set $\{1, 2, \ldots, 2p-1\}$. This set A is a $(2p-1)$-element set (since $2p - 1 \in \mathbb{N}$). Hence, Theorem 2.17.10 (applied to $n = 2p-1$, $k = p$ and $N = A$) shows that $\dbinom{2p-1}{p}$ is the number of p-element subsets of A. In other words,

$$\dbinom{2p-1}{p} = (\text{the number of } p\text{-element subsets of } A). \qquad (104)$$

Recall that there exists no p-element subset S of $\{1, 2, \ldots, 2p-1\}$ such that $p \mid \sum\limits_{s \in S} a_s$. Since $A = \{1, 2, \ldots, 2p-1\}$, this rewrites as follows: There exists no p-element subset S of A such that $p \mid \sum\limits_{s \in S} a_s$. In other words, for each p-element subset S of A, we have $p \nmid \sum\limits_{s \in S} a_s$. Thus, for each p-element subset S of A, we have

$$\left(\sum_{s \in S} a_s\right)^{p-1} \equiv 1 \mod p$$

(by Theorem 2.15.1 **(a)**, applied to $a = \sum\limits_{s \in S} a_s$). Summing these congruences over all p-element subsets S of A, we obtain

$$\begin{aligned}
\sum_{\substack{S \subseteq A;\\ |S| = p}} \underbrace{\left(\sum_{s \in S} a_s\right)^{p-1}}_{\equiv 1 \mod p} &\equiv \sum_{\substack{S \subseteq A;\\ |S| = p}} 1 \\
&= (\text{the number of } p\text{-element subsets } S \text{ of } A) \cdot 1 \\
&= (\text{the number of } p\text{-element subsets } S \text{ of } A) \\
&= (\text{the number of } p\text{-element subsets of } A) \\
&= \dbinom{2p-1}{p} \qquad (\text{by } (104)) \\
&\equiv 1 \mod p \qquad (\text{by Exercise 2.17.4 } \textbf{(b)}). \qquad (105)
\end{aligned}$$

On the other hand, we are going to show that $\sum\limits_{\substack{S \subseteq A;\\ |S|=p}} \left(\sum\limits_{s\in S} a_s\right)^{p-1} \equiv 0 \mod p$. Comparing these two congruences, we will then obtain a contradiction.

Set $n = p-1$. Then, $n = p-1 > 0$.

Let S be any subset of A. Then, Lemma 2.19.3 yields

$$\left(\sum_{s\in S} a_s\right)^n = \sum_{(k_1,k_2,\ldots,k_n)\in S^n} \prod_{i=1}^n a_{k_i}. \tag{106}$$

But $S \subseteq A$. Hence, $S^n \subseteq A^n$. Thus, the n-tuples $(k_1, k_2, \ldots, k_n) \in S^n$ are precisely those n-tuples $(k_1, k_2, \ldots, k_n) \in A^n$ that happen to lie in S^n. Therefore, the summation sign "$\sum\limits_{(k_1,k_2,\ldots,k_n)\in S^n}$" can be replaced by "$\sum\limits_{\substack{(k_1,k_2,\ldots,k_n)\in A^n;\\ (k_1,k_2,\ldots,k_n)\in S^n}}$". Thus, we can rewrite the equality (106) as

$$\left(\sum_{s\in S} a_s\right)^n = \sum_{\substack{(k_1,k_2,\ldots,k_n)\in A^n;\\ (k_1,k_2,\ldots,k_n)\in S^n}} \prod_{i=1}^n a_{k_i}. \tag{107}$$

For any n-tuple $(k_1, k_2, \ldots, k_n) \in A^n$, we have the following chain of equivalences:

$$\begin{aligned} ((k_1, k_2, \ldots, k_n) \in S^n) &\iff (k_1, k_2, \ldots, k_n \text{ all belong to } S) \\ &\iff (\{k_1, k_2, \ldots, k_n\} \subseteq S). \end{aligned}$$

Hence, the summation sign "$\sum\limits_{\substack{(k_1,k_2,\ldots,k_n)\in A^n;\\ (k_1,k_2,\ldots,k_n)\in S^n}}$" can be replaced by "$\sum\limits_{\substack{(k_1,k_2,\ldots,k_n)\in A^n;\\ \{k_1,k_2,\ldots,k_n\}\subseteq S}}$". Thus, we can rewrite the equality (107) as

$$\left(\sum_{s\in S} a_s\right)^n = \sum_{\substack{(k_1,k_2,\ldots,k_n)\in A^n;\\ \{k_1,k_2,\ldots,k_n\}\subseteq S}} \prod_{i=1}^n a_{k_i}. \tag{108}$$

Now, forget that we fixed S. Thus, we have shown the equality (108) for every subset S of A. Now,

$$\begin{aligned}
&\sum_{\substack{S\subseteq A;\\ |S|=p}} \left(\sum_{s\in S} a_s\right)^{p-1} \\
&= \sum_{\substack{S\subseteq A;\\ |S|=p}} \underbrace{\left(\sum_{s\in S} a_s\right)^{n}}_{\substack{= \sum_{\substack{(k_1,k_2,\ldots,k_n)\in A^n;\\ \{k_1,k_2,\ldots,k_n\}\subseteq S}} \prod_{i=1}^{n} a_{k_i} \\ \text{(by (108))}}} \qquad\qquad (\text{since } p-1=n) \\
&= \underbrace{\sum_{\substack{S\subseteq A;\\ |S|=p}} \sum_{\substack{(k_1,k_2,\ldots,k_n)\in A^n;\\ \{k_1,k_2,\ldots,k_n\}\subseteq S}}}_{= \sum_{(k_1,k_2,\ldots,k_n)\in A^n} \sum_{\substack{S\subseteq A;\\ |S|=p;\\ \{k_1,k_2,\ldots,k_n\}\subseteq S}}} \underbrace{\prod_{i=1}^{n} a_{k_i}}_{=\left(\prod_{i=1}^{n} a_{k_i}\right)\cdot 1} \\
&= \sum_{(k_1,k_2,\ldots,k_n)\in A^n} \sum_{\substack{S\subseteq A;\\ |S|=p;\\ \{k_1,k_2,\ldots,k_n\}\subseteq S}} \left(\prod_{i=1}^{n} a_{k_i}\right)\cdot 1 \\
&= \sum_{(k_1,k_2,\ldots,k_n)\in A^n} \left(\prod_{i=1}^{n} a_{k_i}\right) \sum_{\substack{S\subseteq A;\\ |S|=p;\\ \{k_1,k_2,\ldots,k_n\}\subseteq S}} 1. \qquad (109)
\end{aligned}$$

Next, we shall analyze the inner sum on the right hand side of this equality.

Fix an n-tuple $(k_1,k_2,\ldots,k_n)\in A^n$. Let B be the subset $\{k_1,k_2,\ldots,k_n\}$ of A. Then, B consists of the n elements $k_1,k_2,\ldots,k_n$, which may and may not be distinct; but either way, this shows that B has at least one element (since $n>0$). In other words, $|B|\geq 1$. Also, $|B|\leq n$ (since B consists of the n elements $k_1,k_2,\ldots,k_n$). Combining $|B|\geq 1$ with $|B|\leq n$, we obtain $|B|\in\{1,2,\ldots,n\}=\{1,2,\ldots,p-1\}$ (since $n=p-1$). Therefore, $p-|B|\in\{1,2,\ldots,p-1\}$. Hence, Exercise 2.17.4 **(c)** (applied to $k=p-|B|$) yields

$$\binom{p-1+(p-|B|)}{p-|B|}\equiv 0 \bmod p. \qquad (110)$$

Moreover, B is clearly a $|B|$-element subset of A. Now,

$$\begin{aligned}
&\sum_{\substack{S\subseteq A;\\ |S|=p;\\ \{k_1,k_2,\ldots,k_n\}\subseteq S}} 1 \\
&= \sum_{\substack{S\subseteq A;\\ |S|=p;\\ B\subseteq S}} 1 \qquad \left(\text{since } \{k_1,k_2,\ldots,k_n\} = B \text{ (by the definition of } B\text{)}\right) \\
&= (\text{the number of } p\text{-element subsets } S \text{ of } A \text{ satisfying } B\subseteq S)\cdot 1 \\
&= (\text{the number of } p\text{-element subsets } S \text{ of } A \text{ satisfying } B\subseteq S) \\
&= \binom{(2p-1)-|B|}{p-|B|} \\
&\qquad (\text{by Exercise 2.17.3, applied to } a=2p-1,\ b=|B| \text{ and } m=p) \\
&= \binom{p-1+(p-|B|)}{p-|B|} \qquad \left(\text{since } (2p-1)-|B| = p-1+(p-|B|)\right) \\
&\equiv 0 \bmod p \qquad (\text{by (110)}) .
\end{aligned} \tag{111}$$

Now, forget that we fixed $(k_1,k_2,\ldots,k_n)$. We thus have proven (111) for each n-tuple $(k_1,k_2,\ldots,k_n)\in A^n$. Hence, (109) becomes

$$\begin{aligned}
\sum_{\substack{S\subseteq A;\\ |S|=p}} \left(\sum_{s\in S} a_s\right)^{p-1} &= \sum_{(k_1,k_2,\ldots,k_n)\in A^n} \left(\prod_{i=1}^n a_{k_i}\right) \underbrace{\sum_{\substack{S\subseteq A;\\ |S|=p;\\ \{k_1,k_2,\ldots,k_n\}\subseteq S}} 1}_{\substack{\equiv 0 \bmod p\\ \text{(by (111))}}} \\
&\equiv \sum_{(k_1,k_2,\ldots,k_n)\in A^n} \left(\prod_{i=1}^n a_{k_i}\right) 0 = 0 \bmod p.
\end{aligned}$$

Hence,

$$0 \equiv \sum_{\substack{S\subseteq A;\\ |S|=p}} \left(\sum_{s\in S} a_s\right)^{p-1} \equiv 1 \bmod p \qquad (\text{by (105)}) .$$

In other words, $p \mid 0-1$, so that $p \mid 0-1 = -1 \mid 1$. Hence, $p=1$ (by Exercise 2.2.5, applied to $g=p$). This contradicts $p>1$. This contradiction shows that our assumption was wrong. Hence, Lemma 2.19.4 is proven. □

Having established Lemma 2.19.4, we shall next extend it to a larger list of numbers:

Lemma 2.19.5. Let p be a prime. Let u be a positive integer. Let $a_1, a_2, \ldots, a_{up-1}$ be any $up-1$ integers (not necessarily distinct). Then, there exist $u-1$ disjoint p-element subsets $S_1, S_2, \ldots, S_{u-1}$ of $\{1, 2, \ldots, up-1\}$ such that

$$p \mid \sum_{s \in S_i} a_s \qquad \text{for all } i \in \{1, 2, \ldots, u-1\}.$$

Proof of Lemma 2.19.5 (sketched). We shall give the informal idea of the proof, and delegate the formalization to an exercise (Exercise 2.19.2 below).

Lemma 2.19.4 can be restated as follows:

> *Claim 1:* If you are given $2p-1$ integers, then you can pick p of them such that the sum of your pick is divisible by p.

Here and in the following, "picking" is always understood to mean choosing a subset – i.e., you cannot pick a number more than once. (But if two of the $2p-1$ integers are equal, then you can have them both in your pick.)

Now, imagine that our $up-1$ integers $a_1, a_2, \ldots, a_{up-1}$ are laid out on a desk, while $u-1$ empty bags are laid out on the floor. Lemma 2.19.5 claims that we can pack some of the integers from the desk into the bags in such a way that each bag is neatly filled. Here, we say that a bag is *neatly filled* if it is filled with exactly p integers and the sum of these p integers is divisible by p. (Note that if $u-1$ bags are neatly filled, then there are a total of $(u-1)p$ integers in these bags, while the remaining $up-1-(u-1)p = p-1$ integers remain on the desk.)

Let us consider the case $u = 5$. In this case, we have $5p-1$ integers on the desk and 4 bags that we want neatly filled. To fill the bags, we proceed as follows:

- We have $5p-1$ integers on the desk, thus at least $2p-1$ integers. Hence, Claim 1 tells us that we can pick p of them such that the sum of our pick is divisible by p. We do so, and move the p integers we have picked into the first bag.
- Now, we have $4p-1$ integers on the desk, thus at least $2p-1$ integers. Hence, Claim 1 tells us that we can pick p of them such that the sum of our pick is divisible by p. We do so, and move the p integers we have picked into the second bag.
- Now, we have $3p-1$ integers on the desk, thus at least $2p-1$ integers. Hence, Claim 1 tells us that we can pick p of them such that the sum of our pick is divisible by p. We do so, and move the p integers we have picked into the third bag.
- Now, we have $2p-1$ integers on the desk, thus at least $2p-1$ integers. Hence, Claim 1 tells us that we can pick p of them such that the sum of our pick is divisible by p. We do so, and move the p integers we have picked into the fourth bag.

Now, all four bags are neatly filled. This proves Lemma 2.19.5 in the case when $u = 5$. The general case proceeds in the same way (formally speaking, this is an induction over u). □

Exercise 2.19.2. Formalize the above proof of Lemma 2.19.5.

Now the hard part is done: It turns out that non-prime integers n in Theorem 2.19.1 can be dealt with by splitting out a prime factor p, and applying Lemma 2.19.5 to this p. Here is the argument in detail:

Proof of Theorem 2.19.1. We shall prove Theorem 2.19.1 by strong induction on n.

Induction step: Fix a positive integer m. Assume that Theorem 2.19.1 holds for all $n < m$. We must prove that Theorem 2.19.1 holds for $n = m$.

We have assumed that Theorem 2.19.1 holds for all $n < m$. In other words, the following claim holds:

> *Claim 1:* Let n be a positive integer such that $n < m$. Let $a_1, a_2, \ldots, a_{2n-1}$ be any $2n - 1$ integers. Then, there exists an n-element subset S of $\{1, 2, \ldots, 2n - 1\}$ such that $n \mid \sum\limits_{s \in S} a_s$.

We must prove that Theorem 2.19.1 holds for $n = m$. In other words, we must prove the following claim:

> *Claim 2:* Let $a_1, a_2, \ldots, a_{2m-1}$ be any $2m - 1$ integers. Then, there exists an m-element subset S of $\{1, 2, \ldots, 2m - 1\}$ such that $m \mid \sum\limits_{s \in S} a_s$.

[*Proof of Claim 2:* It is very easy to prove Claim 2 when $m = 1$ (just take $S = \{1\}$; then $m \mid \sum\limits_{s \in S} a_s$ will automatically hold because $m = 1$). Thus, for the rest of this proof, we WLOG assume that we don't have $m = 1$. Hence, $m > 1$ (since m is a positive integer).

Proposition 2.13.8 (applied to $n = m$) shows that there exists at least one prime p such that $p \mid m$. Consider this p. We are in one of the following two cases:

Case 1: We have $p = m$.

Case 2: We have $p \neq m$.

Let us first consider Case 1. In this case, we have $p = m$. Hence, the integer m is prime (since p is prime). Hence, Lemma 2.19.4 (applied to m instead of p) shows that there exists an m-element subset S of $\{1, 2, \ldots, 2m - 1\}$ such that $m \mid \sum\limits_{s \in S} a_s$. Hence, Claim 2 is proven in Case 1.

Let us now consider Case 2. In this case, we have $p \neq m$. But $p \mid m$; thus, there exists some integer c such that $m = pc$. Consider this c. We have $c > 0$ [93] and

[93] *Proof.* Assume the contrary. Thus, $c \leq 0$. We can multiply this inequality by p (since $p > 0$), and thus find $pc \leq p0 = 0$, so that $m = pc \leq 0$. This contradicts $m > 0$. This contradiction shows that our assumption was false. Qed.

$c < m$ [94]. From $c > 0$, we obtain $2c > 0$; thus, $2c$ is a positive integer.

From $m = pc$, we obtain $2m = 2pc = (2c)\,p$. Recall that we are given $2m - 1$ integers $a_1, a_2, \ldots, a_{2m-1}$. Since $2m = (2c)\,p$, this rewrites as follows: We are given $(2c)\,p - 1$ integers $a_1, a_2, \ldots, a_{(2c)p-1}$.

Hence, Lemma 2.19.5 (applied to $u = 2c$) shows that there exist $2c - 1$ disjoint p-element subsets $S_1, S_2, \ldots, S_{2c-1}$ of $\{1, 2, \ldots, (2c)\,p - 1\}$ such that

$$p \mid \sum_{s \in S_i} a_s \qquad \text{for all } i \in \{1, 2, \ldots, 2c - 1\}.$$

Consider these $2c - 1$ subsets $S_1, S_2, \ldots, S_{2c-1}$.

For each $i \in \{1, 2, \ldots, 2c - 1\}$, we have $p \mid \sum\limits_{s \in S_i} a_s$ and thus $\dfrac{\sum\limits_{s \in S_i} a_s}{p} \in \mathbb{Z}$. Thus, for each $i \in \{1, 2, \ldots, 2c - 1\}$, we can define an integer $b_i \in \mathbb{Z}$ by

$$b_i = \frac{\sum\limits_{s \in S_i} a_s}{p}. \qquad (112)$$

Consider these $2c - 1$ integers $b_1, b_2, \ldots, b_{2c-1}$. Recall that $c < m$. Hence, Claim 1 (applied to c and b_i instead of n and a_i) shows that there exists a c-element subset S of $\{1, 2, \ldots, 2c - 1\}$ such that $c \mid \sum\limits_{s \in S} b_s$. We can WLOG assume that this c-element subset is actually $\{1, 2, \ldots, c\}$ (because we can always achieve this by changing the order of the sets $S_1, S_2, \ldots, S_{2c-1}$). Assume this. Thus, $\{1, 2, \ldots, c\}$ is a c-element subset S of $\{1, 2, \ldots, 2c - 1\}$ such that $c \mid \sum\limits_{s \in S} b_s$. In other words, $\{1, 2, \ldots, c\}$ is a c-element subset of $\{1, 2, \ldots, 2c - 1\}$ and satisfies

$$c \mid \sum_{s \in \{1, 2, \ldots, c\}} b_s. \qquad (113)$$

From the divisibility (113), we conclude that there exists an integer d such that

$$\sum_{s \in \{1, 2, \ldots, c\}} b_s = cd. \qquad (114)$$

Consider this d.

The sets $S_1, S_2, \ldots, S_{2c-1}$ are subsets of $\{1, 2, \ldots, (2c)\,p - 1\}$. In other words, they are subsets of $\{1, 2, \ldots, 2m - 1\}$ (since $2m = (2c)\,p$).

The sets $S_1, S_2, \ldots, S_{2c-1}$ are disjoint. Hence, in particular, the sets $S_1, S_2, \ldots, S_c$ are disjoint. Thus, the size of their union is the sum of their sizes. In other words,

$$|S_1 \cup S_2 \cup \cdots \cup S_c| = |S_1| + |S_2| + \cdots + |S_c| = \sum_{i=1}^{c} \underbrace{|S_i|}_{\substack{=p \\ \text{(since } S_i \text{ is a} \\ p\text{-element set)}}} = \sum_{i=1}^{c} p = cp = pc = m.$$

[94] *Proof.* We have $p > 1$ (since p is prime). Multiplying this inequality by m, we obtain $pm > 1m$ (since $m > 0$). Thus, $pm > 1m = m = pc$. We can divide this inequality by p (since $p > 0$), and thus obtain $m > c$. Hence, $c < m$.

In other words, $S_1 \cup S_2 \cup \cdots \cup S_c$ is an m-element set. Of course, this set is a subset of $\{1, 2, \ldots, 2m-1\}$ (since $S_1, S_2, \ldots, S_c$ are subsets of $\{1, 2, \ldots, 2m-1\}$). Moreover, since the c sets $S_1, S_2, \ldots, S_c$ are disjoint, we see that each element of $S_1 \cup S_2 \cup \cdots \cup S_c$ belongs to exactly one of these c sets. Thus, we can split up the sum $\sum\limits_{s \in S_1 \cup S_2 \cup \cdots \cup S_c} a_s$ as follows:

$$\begin{aligned} \sum_{s \in S_1 \cup S_2 \cup \cdots \cup S_c} a_s &= \sum_{s \in S_1} a_s + \sum_{s \in S_2} a_s + \cdots + \sum_{s \in S_c} a_s = \sum_{i=1}^{c} \underbrace{\sum_{s \in S_i} a_s}_{\substack{=pb_i \\ \text{(by (112))}}} = \sum_{i=1}^{c} pb_i = \sum_{s=1}^{c} pb_s \\ &= \sum_{s \in \{1,2,\ldots,c\}} pb_s = p \underbrace{\sum_{s \in \{1,2,\ldots,c\}} b_s}_{\substack{=cd \\ \text{(by (114))}}} = \underbrace{pc}_{=m} d = md. \end{aligned}$$

Hence, $m \mid \sum\limits_{s \in S_1 \cup S_2 \cup \cdots \cup S_c} a_s$.

Thus, there exists an m-element subset S of $\{1, 2, \ldots, 2m-1\}$ such that $m \mid \sum\limits_{s \in S} a_s$ (namely, $S = S_1 \cup S_2 \cup \cdots \cup S_c$). Therefore, Claim 2 is proven in Case 2.

We have now proven Claim 2 in both Cases 1 and 2. Hence, Claim 2 always holds.]

So we have proven Claim 2. In other words, Theorem 2.19.1 holds for $n = m$. This completes the induction step, and with it the proof of Theorem 2.19.1. □

3. Equivalence relations and residue classes

3.1. Relations

Loosely speaking, a *relation* on a set S is a property that two elements a and b of S (or, more formally, a pair $(a, b) \in S \times S$ of two elements of S) can either have or not have. For example, equality (denoted $=$) is a relation, since two elements a and b of S are either equal (i.e., satisfy $a = b$) or not equal. Likewise, the divisibility relation (denoted $\mid$) is a relation on $\mathbb{Z}$, since two elements a and b of $\mathbb{Z}$ either satisfy $a \mid b$ or do not.

A formal definition of relations proceeds as follows:

Definition 3.1.1. Fix a set S. A *binary relation* on S is a subset of $S \times S$ (that is, a set of pairs of elements of S).

If R is a binary relation (on S), and if $a, b \in S$, then we write aRb for $(a, b) \in R$.

The word "*relation*" shall always mean "binary relation" unless we say otherwise.

So a relation on a set S is, formally speaking, a subset of $S \times S$ – but in practice, we think of it as a property that holds for some pairs $(a, b) \in S \times S$ (namely, for the ones that belong to this subset) and does not hold for some others (namely, for the ones that do not belong to this subset).[95] In order to define a relation R on a given set S, it suffices to tell which pairs $(a,b) \in S \times S$ satisfy aRb (because then, R will simply be the set of all these pairs (a,b)). Let us define several relations on the set $\mathbb{Z}$ by this strategy:

Example 3.1.2. Let $S = \mathbb{Z}$.

(a) The relation $=$ is a binary relation on S. As a subset of $S \times S$, this relation is

$$\begin{aligned} &\{(a,b) \in S \times S \mid a = b\} \\ &= \{(c,c) \mid c \in S\} = \{\ldots, (-1,-1), (0,0), (1,1), \ldots\}. \end{aligned}$$

(b) The relation $<$ is a binary relation on S. As a subset of $S \times S$, this relation is

$$\{(a,b) \in S \times S \mid a < b\}.$$

(c) The relation $\leq$ is a binary relation on S. As a subset of $S \times S$, this relation is

$$\{(a,b) \in S \times S \mid a \leq b\}.$$

(d) The relation $\neq$ is also a binary relation on S.

(e) Fix $n \in \mathbb{Z}$. Define a relation $\underset{n}{\equiv}$ on $S = \mathbb{Z}$ by

$$\left(a \underset{n}{\equiv} b\right) \iff (a \equiv b \operatorname{mod} n).$$

As a subset of $S \times S = \mathbb{Z} \times \mathbb{Z}$, this relation $\underset{n}{\equiv}$ is

$$\begin{aligned} &\{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \operatorname{mod} n\} \\ &= \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{there exists an integer } d \text{ such that } b = a + nd\} \\ &\qquad \text{(by Exercise 2.3.7)} \\ &= \{(a, a+nd) \mid a, d \in \mathbb{Z}\}. \end{aligned}$$

Note that the relation $\underset{0}{\equiv}$ is exactly the relation $=$ (by Example 2.3.2 **(c)**).

(f) Define a binary relation $\boxed{N}$ on S by

$$\left(a \boxed{N} b\right) \iff \text{(false)}$$

(that is, $a \boxed{N} b$ never holds, no matter what a and b are). As a subset of $S \times S$, this relation $\boxed{N}$ is just the empty subset of $S \times S$.

(g) On the other extreme: Define a binary relation $\boxed{A}$ on S by

$$\left(a \boxed{A} b\right) \iff \text{(true)}$$

[95] Here, the word "some" can mean "none" or "all" or anything inbetween.

(that is, $a \boxed{A} b$ holds for all a and b). As a subset of $S \times S$, this relation $\boxed{A}$ is the whole set $S \times S$. Note that the relation $\boxed{A}$ is exactly the relation $\underset{1}{\equiv}$ (by Example 2.3.2 **(d)**).

(h) The relation $\mid$ (divisibility) is also a relation on $S = \mathbb{Z}$.

(i) The relation $\perp$ (coprimality) is also a relation on $S = \mathbb{Z}$.

(j) We have defined several relations on the set $S = \mathbb{Z}$ now. The relations $=$, $\neq$, $\boxed{N}$ and $\boxed{A}$ (or, rather, relations analogous to them) can be defined on **any** set.

3.2. Equivalence relations

Relations occur frequently in mathematics, and there is a bunch of properties that a relation can have or not have. (See the Wikipedia article on binary relations for a long list of such properties.) We shall need only the following three:

Definition 3.2.1. Let R be a binary relation on a set S.

(a) We say that R is *reflexive* if every $a \in S$ satisfies aRa.

(b) We say that R is *symmetric* if every $a, b \in S$ satisfying aRb satisfy bRa.

(c) We say that R is *transitive* if every $a, b, c \in S$ satisfying aRb and bRc satisfy aRc.

(Here are mnemonics for the three words we just defined:

- "Reflexive" should make you think of R as a mirror through which a can see itself (that is, satisfy aRa).
- "Symmetric" means that the roles of a and b in aRb are interchangeable – a symmetry.
- "Transitive" means that you can "transit" an element b on your way from a to c (that is, if you treat aRb as the existence of a "path" from a to b, and bRc as the existence of a "path" from b to c, then you can combine a "path" from a to b with a "path" from b to c to get a "path" from a to c).)

Let us see some examples of these properties of relations[96]:

Example 3.2.2. Let S be the set $\mathbb{Z}$. Consider the relations on $\mathbb{Z}$ defined in Example 3.1.2.

(a) The relation $=$ is reflexive, symmetric and transitive.

(b) The relation $<$ is transitive, but neither reflexive nor symmetric.

(c) The relation $\leq$ is transitive and reflexive, but not symmetric.

(d) The relation $\neq$ is symmetric, but neither reflexive nor transitive.

(e) For each $n \in \mathbb{Z}$, the relation $\underset{n}{\equiv}$ is reflexive, symmetric and transitive.

[96] See further below for the proofs of the claims made in this example.

(f) The relation $\boxed{N}$ is symmetric and transitive, but not reflexive.
(g) The relation $\boxed{A}$ is reflexive, symmetric and transitive.
(h) The divisibility relation $\mid$ is reflexive and transitive, but not symmetric.
(i) The coprimality relation $\perp$ is symmetric, but neither reflexive nor transitive.

Proof of Example 3.2.2. **(a)** Indeed:

- The relation $=$ is reflexive, because every $a \in S$ satisfies $a = a$.
- The relation $=$ is symmetric, because every $a, b \in S$ satisfying $a = b$ satisfy $b = a$.
- The relation $=$ is transitive, because every $a, b, c \in S$ satisfying $a = b$ and $b = c$ satisfy $a = c$.

(b) Indeed:

- The relation $<$ is transitive (because every $a, b, c \in S$ satisfying $a < b$ and $b < c$ satisfy $a < c$).
- Not every $a \in S$ satisfies $a < a$ (in fact, no $a \in S$ satisfies $a < a$); thus, $<$ is not reflexive.
- Similarly, $<$ is not symmetric, since $a < b$ does not imply $b < a$ (quite the opposite).

(c) Indeed:

- The relation $\leq$ is transitive (because every $a, b, c \in S$ satisfying $a \leq b$ and $b \leq c$ satisfy $a \leq c$).
- The relation $\leq$ is reflexive (since every $a \in S$ satisfies $a \leq a$).
- The relation $\leq$ is not symmetric (since $a \leq b$ does not imply $b \leq a$; for example, $1 \leq 2$ holds but $2 \leq 1$ does not).

(d) Indeed:

- The relation $\neq$ is symmetric (because every $a, b \in S$ satisfying $a \neq b$ satisfy $b \neq a$).
- The relation $\neq$ is not reflexive (since we don't have $2 \neq 2$).
- The relation $\neq$ is not transitive (since $2 \neq 3$ and $3 \neq 2$ do not lead to $2 \neq 2$).

(e) Let $n \in \mathbb{Z}$.

- Proposition 2.3.4 **(b)** shows that every $a, b, c \in \mathbb{Z}$ satisfying $a \equiv b \mod n$ and $b \equiv c \mod n$ satisfy $a \equiv c \mod n$. In other words, every $a, b, c \in S$ satisfying $a \underset{n}{\equiv} b$ and $b \underset{n}{\equiv} c$ satisfy $a \underset{n}{\equiv} c$ (since the definition of $\underset{n}{\equiv}$ shows that the three statements
$$\left(a \underset{n}{\equiv} b\right), \qquad \left(b \underset{n}{\equiv} c\right), \qquad \left(a \underset{n}{\equiv} c\right)$$
are equivalent to
$$(a \equiv b \mod n), \qquad (b \equiv c \mod n), \qquad (a \equiv c \mod n),$$
respectively). But this means precisely that the relation $\underset{n}{\equiv}$ is transitive.

- Similarly, the relation $\underset{n}{\equiv}$ is reflexive (by Proposition 2.3.4 **(a)**).

- Similarly, the relation $\underset{n}{\equiv}$ is symmetric (by Proposition 2.3.4 **(c)**).

(f) This may appear strange, but is a completely straightforward consequence of the concept of "vacuous truth":

- Every $a, b \in S$ satisfying $a \boxed{N} b$ satisfy $b \boxed{N} a$ (because there are no such a, b to begin with – since $a \boxed{N} b$ never holds). Thus, $\boxed{N}$ is symmetric.

- Similarly, $\boxed{N}$ is transitive.

- But $\boxed{N}$ is not reflexive, since (for example) $1 \boxed{N} 1$ does not hold.

(g) All of this is trivial, because $a \boxed{A} b$ holds for all $a, b \in S$.

(h) The divisibility relation $\mid$ is reflexive (by Proposition 2.2.4 **(a)**) and transitive (by Proposition 2.2.4 **(b)**), but not symmetric (since $1 \mid 2$ does not lead to $2 \mid 1$).

(i) The coprimality relation is symmetric (by Proposition 2.10.4), but neither reflexive (since we don't have $2 \perp 2$) nor transitive (since $2 \perp 3$ and $3 \perp 2$ do not lead to $2 \perp 2$). □

Definition 3.2.3. An *equivalence relation* on a set S means a relation on S that is reflexive, symmetric and transitive.

Example 3.2.4. Let S be any set. The relation $=$ on the set S is an equivalence relation, because it is reflexive, symmetric and transitive.

Example 3.2.5. Let $n \in \mathbb{Z}$. The relation $\underset{n}{\equiv}$ on $\mathbb{Z}$ (defined in Example 3.1.2 **(e)**) is an equivalence relation, because (as we saw in Example 3.2.2 **(e)**) it is reflexive, symmetric and transitive.

Example 3.2.6. Here are some examples from elementary plane geometry: Congruence (e.g., of triangles) is an equivalence relation. Similarity is also an equivalence relation. The same holds for direct similarity (i.e., orientation-preserving similarity). The same holds for parallelism of lines.

Example 3.2.7. Let S and T be two sets, and let $f : S \to T$ be a map. Define a relation $\underset{f}{\equiv}$ on S by

$$\left(a \underset{f}{\equiv} b\right) \iff (f(a) = f(b)).$$

This relation $\underset{f}{\equiv}$ is an equivalence relation.

Proof of Example 3.2.7. Indeed:

- The relation $\underset{f}{\equiv}$ is reflexive, because every $a \in S$ satisfies $a \underset{f}{\equiv} a$ (since $f(a) = f(a)$).
- The relation $\underset{f}{\equiv}$ is symmetric, because every $a, b \in S$ satisfying $a \underset{f}{\equiv} b$ satisfy $b \underset{f}{\equiv} a$. (Indeed, $a \underset{f}{\equiv} b$ means $f(a) = f(b)$, which entails $f(b) = f(a)$, which in turn rewrites as $b \underset{f}{\equiv} a$.)
- The relation $\underset{f}{\equiv}$ is transitive, because every $a, b, c \in S$ satisfying $a \underset{f}{\equiv} b$ and $b \underset{f}{\equiv} c$ satisfy $a \underset{f}{\equiv} c$. (Indeed, the assumptions $a \underset{f}{\equiv} b$ and $b \underset{f}{\equiv} c$ rewrite as $f(a) = f(b)$ and $f(b) = f(c)$; therefore, $f(a) = f(b) = f(c)$, which rewrites as $a \underset{f}{\equiv} c$.)

Thus, $\underset{f}{\equiv}$ is an equivalence relation. □

We will soon learn that **every** equivalence relation on a set S is actually of the form $\underset{f}{\equiv}$ for some set T and some map $f : S \to T$. (Namely, this is proven in Exercise 3.3.3 below.)

Example 3.2.8. Let S be the set of all points on the landmass of the Earth, and let $\sim$ be the relation on S defined by

$$(a \sim b) \iff (\text{there is a land route from } a \text{ to } b).$$

This $\sim$ is an equivalence relation (with the caveat that S is not a mathematical object and thus not really well-defined).

Example 3.2.9. Let

$$S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) = \{(a_1, a_2) \mid a_1 \in \mathbb{Z} \text{ and } a_2 \in \mathbb{Z} \setminus \{0\}\}.$$

This is the set of all pairs whose first entry is an integer and whose second entry is a nonzero integer. We define a relation $\underset{*}{\sim}$ on S by

$$\Big((a_1, a_2) \underset{*}{\sim} (b_1, b_2)\Big) \iff (a_1 b_2 = a_2 b_1).$$

This relation $\underset{*}{\sim}$ is an equivalence relation.

Proof of Example 3.2.9. Indeed:

- The relation $\underset{*}{\sim}$ is reflexive.

  [*Proof:* Let $a \in S$. Thus, $a \in S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$; in other words, we can write a as $a = (a_1, a_2)$ for some $a_1 \in \mathbb{Z}$ and $a_2 \in \mathbb{Z} \setminus \{0\}$. Consider these a_1 and a_2.

  Clearly, $a_1 a_2 = a_2 a_1$. In other words, $(a_1, a_2) \underset{*}{\sim} (a_1, a_2)$ (because the definition of the relation $\underset{*}{\sim}$ yields that $(a_1, a_2) \underset{*}{\sim} (a_1, a_2)$ means $a_1 a_2 = a_2 a_1$). In other words, $a \underset{*}{\sim} a$ (since $a = (a_1, a_2)$).

  Now, forget that we fixed a. We thus have shown that every $a \in S$ satisfies $a \underset{*}{\sim} a$. In other words, the relation $\underset{*}{\sim}$ is reflexive.]

- The relation $\underset{*}{\sim}$ is symmetric.

  [*Proof:* Let $a, b \in S$ be such that $a \underset{*}{\sim} b$. We shall prove that $b \underset{*}{\sim} a$.

  We have $a \in S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$; in other words, we can write a as $a = (a_1, a_2)$ for some $a_1 \in \mathbb{Z}$ and $a_2 \in \mathbb{Z} \setminus \{0\}$. Similarly, we can write b as $b = (b_1, b_2)$ for some $b_1 \in \mathbb{Z}$ and $b_2 \in \mathbb{Z} \setminus \{0\}$. Consider these a_1, a_2, b_1 and b_2.

  We have assumed that $a \underset{*}{\sim} b$. In other words, $(a_1, a_2) \underset{*}{\sim} (b_1, b_2)$ (since $a = (a_1, a_2)$ and $b = (b_1, b_2)$). In other words, $a_1 b_2 = a_2 b_1$ (because this is what $(a_1, a_2) \underset{*}{\sim} (b_1, b_2)$ means, by the definition of the relation $\underset{*}{\sim}$). Thus, $b_2 a_1 = a_1 b_2 = a_2 b_1 = b_1 a_2$; in other words, $b_1 a_2 = b_2 a_1$. In other words, $(b_1, b_2) \underset{*}{\sim} (a_1, a_2)$ (by the definition of the relation $\underset{*}{\sim}$). In other words, $b \underset{*}{\sim} a$ (since $a = (a_1, a_2)$ and $b = (b_1, b_2)$).

  Now, forget that we fixed a and b. We thus have shown that every $a, b \in S$ satisfying $a \underset{*}{\sim} b$ satisfy $b \underset{*}{\sim} a$. In other words, the relation $\underset{*}{\sim}$ is symmetric.]

- The relation $\underset{*}{\sim}$ is transitive.

  [*Proof:* Let $a, b, c \in S$ be such that $a \underset{*}{\sim} b$ and $b \underset{*}{\sim} c$. We shall prove that $a \underset{*}{\sim} c$.

  We have $a \in S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$; in other words, we can write a as $a = (a_1, a_2)$ for some $a_1 \in \mathbb{Z}$ and $a_2 \in \mathbb{Z} \setminus \{0\}$. Similarly, we can write b as $b = (b_1, b_2)$ for some

$b_1 \in \mathbb{Z}$ and $b_2 \in \mathbb{Z} \setminus \{0\}$. Similarly, we can write c as $c = (c_1, c_2)$ for some $c_1 \in \mathbb{Z}$ and $c_2 \in \mathbb{Z} \setminus \{0\}$. Consider these a_1, a_2, b_1, b_2, c_1 and c_2. Note that $b_2 \in \mathbb{Z} \setminus \{0\}$, so that $b_2 \neq 0$.

We have assumed that $a \underset{*}{\sim} b$. In other words, $(a_1, a_2) \underset{*}{\sim} (b_1, b_2)$ (since $a = (a_1, a_2)$ and $b = (b_1, b_2)$). In other words, $a_1 b_2 = a_2 b_1$ (by the definition of the relation $\underset{*}{\sim}$). Similarly (by exploiting the assumption $b \underset{*}{\sim} c$ instead of $a \underset{*}{\sim} b$), we can obtain $b_1 c_2 = b_2 c_1$. Hence,

$$\underbrace{a_1 b_2}_{=a_2 b_1} c_2 = a_2 \underbrace{b_1 c_2}_{=b_2 c_1} = a_2 b_2 c_1.$$

We can cancel b_2 from this equality (since $b_2 \neq 0$), and thus obtain $a_1 c_2 = a_2 c_1$. In other words, $(a_1, a_2) \underset{*}{\sim} (c_1, c_2)$ (by the definition of the relation $\underset{*}{\sim}$). In other words, $a \underset{*}{\sim} c$ (since $a = (a_1, a_2)$ and $c = (c_1, c_2)$).

Now, forget that we fixed a, b, c. We thus have shown that every $a, b, c \in S$ satisfying $a \underset{*}{\sim} b$ and $b \underset{*}{\sim} c$ satisfy $a \underset{*}{\sim} c$. In other words, the relation $\underset{*}{\sim}$ is transitive.]

We have now proven that the relation $\underset{*}{\sim}$ is reflexive, symmetric and transitive. In other words, $\underset{*}{\sim}$ is an equivalence relation (by the definition of "equivalence relation"). This proves Example 3.2.9. □

The relation $\underset{*}{\sim}$ from Example 3.2.9 may appear familiar to you. In fact, its definition can be restated as follows:

$$\left((a_1, a_2) \underset{*}{\sim} (b_1, b_2) \right) \iff \left(\frac{a_1}{a_2} = \frac{b_1}{b_2} \right),$$

and this makes the claims of Example 3.2.9 a lot more obvious. However, this is (in a sense) circular reasoning: The statement "$\frac{a_1}{a_2} = \frac{b_1}{b_2}$" only makes sense if the rational numbers have been defined[97], but the definition of rational numbers (at least the usual definition, given in [Swanso18, §3.6] and in many other places) already relies on the claims of Example 3.2.9. (Namely, the rational numbers are defined as the equivalence classes of the relation $\underset{*}{\sim}$; this is explained in Example 3.3.6 below.) Thus, our above proof of Example 3.2.9 was not a waste of time, but rather an important prerequisite for the construction of rational numbers (one of the cornerstones of mathematics).

If you are familiar with basic linear algebra, you may notice that the relation $\underset{*}{\sim}$ from Example 3.2.9 can also be regarded as linear dependence. Namely, two pairs (a_1, a_2) and (b_1, b_2) in $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ satisfy $(a_1, a_2) \underset{*}{\sim} (b_1, b_2)$ if and only if the vectors (a_1, a_2) and (b_1, b_2) in $\mathbb{Q}^2$ are linearly dependent.[98]

[97] since $\frac{a_1}{a_2}$ and $\frac{b_1}{b_2}$ are (in general) not integers but rational numbers

[98] Note, however, that linear dependence is no longer an equivalence relation if we allow the vector $(0, 0)$ in our set S, because then, it is no longer transitive (for example, $(1, 1)$ and $(0, 0)$ are linearly dependent, and $(0, 0)$ and $(1, 2)$ are linearly dependent, but $(1, 1)$ and $(1, 2)$ are not).

One simple property of symmetric relations will come useful:

Proposition 3.2.10. Let $\sim$ be a symmetric relation on a set S. Let $a, b \in S$. Then, $a \sim b$ if and only if $b \sim a$.

Proof of Proposition 3.2.10. The relation $\sim$ is symmetric. Thus, if a and b satisfy $a \sim b$, then they also satisfy $b \sim a$ (by the definition of "symmetric"). In other words, we have the logical implication $(a \sim b) \Longrightarrow (b \sim a)$. But the same argument (with the roles of a and b interchanged) yields the implication $(b \sim a) \Longrightarrow (a \sim b)$. Combining these two implications, we obtain the equivalence $(a \sim b) \Longleftrightarrow (b \sim a)$. This proves Proposition 3.2.10. □

3.3. Equivalence classes

3.3.1. Definition of equivalence classes

We can now state one of the most important definitions in mathematics:

Definition 3.3.1. Let $\sim$ be an equivalence relation on a set S.

(a) For each $a \in S$, we define a subset $[a]_\sim$ of S by

$$[a]_\sim = \{b \in S \mid b \sim a\}. \tag{115}$$

This subset $[a]_\sim$ is called the *equivalence class* of a, or the *$\sim$-equivalence class* of a.

(b) The *equivalence classes* of $\sim$ are defined to be the sets $[a]_\sim$ for $a \in S$. They are also known as the *$\sim$-equivalence classes*.

Example 3.3.2. Consider the relation $\underset{3}{\equiv}$ on $\mathbb{Z}$ (defined in Example 3.1.2 **(e)**). We have

$$\begin{aligned}[5]_{\underset{3}{\equiv}} &= \left\{b \in \mathbb{Z} \mid b \underset{3}{\equiv} 5\right\} = \{b \in \mathbb{Z} \mid b \equiv 5 \bmod 3\} \\ &= \{\ldots, -4, -1, 2, 5, 8, 11, 14, \ldots\}\end{aligned}$$

and

$$\begin{aligned}[3]_{\underset{3}{\equiv}} &= \left\{b \in \mathbb{Z} \mid b \underset{3}{\equiv} 3\right\} = \{b \in \mathbb{Z} \mid b \equiv 3 \bmod 3\} \\ &= \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\}\end{aligned}$$

and

$$\begin{aligned}[2]_{\underset{3}{\equiv}} &= \left\{b \in \mathbb{Z} \mid b \underset{3}{\equiv} 2\right\} = \{b \in \mathbb{Z} \mid b \equiv 2 \bmod 3\} \\ &= \{\ldots, -4, -1, 2, 5, 8, 11, 14, \ldots\}.\end{aligned}$$

Note that $[5]_{\underset{3}{\equiv}} = [2]_{\underset{3}{\equiv}}$, as you can easily see.

3.3.2. Basic properties

Proposition 3.3.3. Let $\sim$ be an equivalence relation on a set S. Let $a \in S$. Then,

$$[a]_\sim = \{b \in S \mid a \sim b\}.$$

Proof of Proposition 3.3.3. The relation $\sim$ is symmetric (since it is an equivalence relation). Thus, for any $b \in S$, we have ($a \sim b$ if and only if $b \sim a$) (by Proposition 3.2.10). Hence, $\{b \in S \mid a \sim b\} = \{b \in S \mid b \sim a\}$. Comparing this with (115), we obtain $[a]_\sim = \{b \in S \mid a \sim b\}$. This proves Proposition 3.3.3. □

Proposition 3.3.3 shows that we can replace the condition "$b \sim a$" by "$a \sim b$" in Definition 3.3.1 **(a)** without changing the meaning of the definition. (Some authors, such as Swanson in [Swanso18, Definition 2.3.6], do exactly that.)

Proposition 3.3.4. Let $\sim$ be an equivalence relation on a set S. Let $a \in S$. Then, $a \in [a]_\sim$.

Proof of Proposition 3.3.4. The relation $\sim$ is reflexive (since it is an equivalence relation). Thus, $a \sim a$. In other words, a is a $b \in S$ satisfying $b \sim a$. In other words, $a \in \{b \in S \mid b \sim a\}$. But $[a]_\sim = \{b \in S \mid b \sim a\}$ (by the definition of $[a]_\sim$). Hence, $a \in \{b \in S \mid b \sim a\} = [a]_\sim$. This proves Proposition 3.3.4. □

Proposition 3.3.4 shows that all equivalence classes of an equivalence relation are nonempty sets (because each equivalence class $[a]_\sim$ contains at least the element a).

Theorem 3.3.5. Let $\sim$ be an equivalence relation on a set S. Let $x, y \in S$.

(a) If $x \sim y$, then $[x]_\sim = [y]_\sim$.

(b) If not $x \sim y$, then the sets $[x]_\sim$ and $[y]_\sim$ are disjoint.

(c) We have $x \sim y$ if and only if $x \in [y]_\sim$.

(d) We have $x \sim y$ if and only if $y \in [x]_\sim$.

(e) We have $x \sim y$ if and only if $[x]_\sim = [y]_\sim$.

Proof of Theorem 3.3.5. The relation $\sim$ is transitive (since it is an equivalence relation) and symmetric (for the same reason).

The definition of $[x]_\sim$ yields $[x]_\sim = \{b \in S \mid b \sim x\}$. Similarly, $[y]_\sim = \{b \in S \mid b \sim y\}$.

(a) Assume that $x \sim y$. Thus, $y \sim x$ (since the relation $\sim$ is symmetric).

Let $c \in [x]_\sim$. Thus, $c \in [x]_\sim = \{b \in S \mid b \sim x\}$. Thus, $c \sim x$. From $c \sim x$ and $x \sim y$, we obtain $c \sim y$ (since the relation $\sim$ is transitive). Hence, $c \in \{b \in S \mid b \sim y\}$. In other words, $c \in [y]_\sim$ (since $[y]_\sim = \{b \in S \mid b \sim y\}$).

Forget that we fixed c. We thus have proven that $c \in [y]_\sim$ for each $c \in [x]_\sim$. Thus, $[x]_\sim \subseteq [y]_\sim$. The same argument (with x and y switched) yields $[y]_\sim \subseteq [x]_\sim$ (since $y \sim x$). Combining $[x]_\sim \subseteq [y]_\sim$ with $[y]_\sim \subseteq [x]_\sim$, we obtain $[x]_\sim = [y]_\sim$. This proves Theorem 3.3.5 **(a)**.

(b) Assume that we don't have $x \sim y$. Let $c \in [x]_\sim \cap [y]_\sim$. We aim for a contradiction.

We have $c \in [x]_\sim \cap [y]_\sim \subseteq [x]_\sim = \{b \in S \mid b \sim x\}$, so that $c \sim x$. Likewise, $c \sim y$. From $c \sim x$, we obtain $x \sim c$ (since the relation $\sim$ is symmetric). Combining this with $c \sim y$, we obtain $x \sim y$ (since $\sim$ is transitive). This contradicts our assumption that we don't have $x \sim y$.

Now, forget that we fixed c. So we have found a contradiction for each $c \in [x]_\sim \cap [y]_\sim$. Thus, there is no such c. In other words, $[x]_\sim \cap [y]_\sim = \varnothing$. In other words, the sets $[x]_\sim$ and $[y]_\sim$ are disjoint. This proves Theorem 3.3.5 **(b)**.

(c) Recall that $[y]_\sim = \{b \in S \mid b \sim y\}$. Thus, we have $x \in [y]_\sim$ if and only if $x \sim y$. In other words, we have $x \sim y$ if and only if $x \in [y]_\sim$. This proves Theorem 3.3.5 **(c)**.

(d) Theorem 3.3.5 **(c)** (applied to y and x instead of x and y) shows that we have $y \sim x$ if and only if $y \in [x]_\sim$. In other words, we have the logical equivalence $(y \sim x) \iff (y \in [x]_\sim)$.

Proposition 3.2.10 (applied to $a = x$ and $b = y$) shows that we have $x \sim y$ if and only if $y \sim x$. Thus, we have the following chain of logical equivalences:

$$(x \sim y) \iff (y \sim x) \iff (y \in [x]_\sim) .$$

In other words, we have $x \sim y$ if and only if $y \in [x]_\sim$. This proves Theorem 3.3.5 **(d)**.

(e) $\Longrightarrow$: Assume that $x \sim y$. Then, Theorem 3.3.5 **(a)** yields $[x]_\sim = [y]_\sim$. Thus, the "$\Longrightarrow$" direction of Theorem 3.3.5 **(e)** is proven.

$\Longleftarrow$: Assume that $[x]_\sim = [y]_\sim$. Then, Proposition 3.3.4 (applied to $a = x$) yields $x \in [x]_\sim = [y]_\sim = \{b \in S \mid b \sim y\}$. In other words, $x \sim y$. This proves the "$\Longleftarrow$" direction of Theorem 3.3.5 **(e)**. □

Theorem 3.3.5 yields an important property of equivalence classes:

Exercise 3.3.1. Let $\sim$ be an equivalence relation on a set S. Prove that any two equivalence classes of $\sim$ are either identical or disjoint.

In the following, we will try to use Greek letters for equivalence classes and Roman letters for their representatives. (See the solution to Exercise 3.3.1 for an example.)

3.3.3. More examples

Example 3.3.6. Consider the relation $\underset{*}{\sim}$ on $S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ defined in Example 3.2.9. Its equivalence classes are the rational numbers. Indeed, the equivalence class $[(a_1, a_2)]_{\underset{*}{\sim}}$ of a pair $(a_1, a_2) \in S$ is commonly denoted by $\dfrac{a_1}{a_2}$ (or by a_1/a_2). This is how rational numbers are defined!

Equivalence classes appear in real life too, at least in the modern world. When you say that the sun rises approximately at 7 AM in February[99], what do "7 AM" and "February" mean? Clearly, "February" is not a specific month in history, since each year has its own February. Rather, it stands for an equivalence class of months, with respect to the relation of "being an integer number of years apart". Similarly, "7 AM" means an equivalence class of moments with respect to the relation of "being an integer number of days apart". Likewise, "the horse" in "the horse has a lifespan of 25 years" refers not to a specific horse, but to the whole species, which is an equivalence class of creatures with respect to a certain relation[100]. Finally, the equivalence classes of the relation $\sim$ in Example 3.2.8 are commonly referred to as "continents"[101] or "islands". Equivalence classes provide a way to refer to multiple objects (usually similar in some way) as if they were one.

3.3.4. The "is a permutation of" relation on tuples

Let us give a few more mathematical examples for equivalences and equivalence classes:

Definition 3.3.7. Let A be a set, and let $k \in \mathbb{N}$. As we know, A^k denotes the set of all k-tuples of elements of A.

The relation $\underset{\text{perm}}{\sim}$ on A^k is defined as follows:

$$\left(\mathbf{p} \underset{\text{perm}}{\sim} \mathbf{q}\right) \iff (\mathbf{p} \text{ is a permutation of } \mathbf{q}) .$$

(We are using Definition 2.13.16 here.) For example, $(3,8,8,2) \underset{\text{perm}}{\sim} (8,3,2,8)$.

Exercise 3.3.2. Prove that the relation $\underset{\text{perm}}{\sim}$ is an equivalence relation.

Definition 3.3.8. Let A be a set, and let $k \in \mathbb{N}$. The relation $\underset{\text{perm}}{\sim}$ on A^k is an equivalence relation (by Exercise 3.3.2). Its equivalence classes are called the *unordered k-tuples* of elements of A. For example, for $k = 2$ and $A = \mathbb{Z}$, the two 2-tuples $(6,8)$ and $(8,6)$ are permutations of each other, so $(6,8) \underset{\text{perm}}{\sim} (8,6)$ and thus $[(6,8)]_{\underset{\text{perm}}{\sim}} = [(8,6)]_{\underset{\text{perm}}{\sim}}$.

[99] in Minneapolis

[100] According to Darwin, the relation is "being able to procreate" – although this is not per se an equivalence relation, so some tweaks need to be made ("reflexive-and-transitive closure") to turn it into one.

[101] at least if one considers Eurasia to be a single continent

3.3.5. The "is a cyclic rotation of" relation on tuples

Another example of an equivalence relation is the following:

Definition 3.3.9. Again, let A be a set and $k \in \mathbb{N}$. If $\mathbf{a} = (a_1, a_2, \ldots, a_k) \in A^k$, then a *cyclic rotation* of $\mathbf{a}$ means a k-tuple of the form

$$(a_{i+1}, a_{i+2}, \ldots, a_k, a_1, a_2, \ldots, a_i) \in A^k$$

for some $i \in \{0, 1, \ldots, k\}$.

For example, the cyclic rotations of the 3-tuple $(1, 4, 5)$ are $(1, 4, 5)$, $(4, 5, 1)$ and $(5, 1, 4)$.

(Here is an equivalent description of cyclic rotations: Let C be the map $A^k \to A^k$ that sends each k-tuple $(a_1, a_2, \ldots, a_k)$ to $(a_2, a_3, \ldots, a_k, a_1)$. Then, it is easy to see that a cyclic rotation of $\mathbf{a}$ is the same as a k-tuple of the form $C^i(\mathbf{a})$ for some $i \in \{0, 1, \ldots, k\}$. But it is also easy to see that $C^k = \operatorname{id}$. Thus, the $C^i(\mathbf{a})$ for $i \in \{0, 1, \ldots, k\}$ are exactly the $C^i(\mathbf{a})$ for $i \in \mathbb{N}$.)

The relation $\underset{\text{cyc}}{\sim}$ on A^k is defined as follows:

$$\begin{aligned} \left(\mathbf{p} \underset{\text{cyc}}{\sim} \mathbf{q}\right) &\iff (\mathbf{p} \text{ is a cyclic rotation of } \mathbf{q}) \\ &\iff \left(\mathbf{p} = C^i(\mathbf{q}) \text{ for some } i \in \mathbb{N}\right). \end{aligned}$$

This relation $\underset{\text{cyc}}{\sim}$ is an equivalence relation. Its equivalence classes are called *necklaces* of length k over A.

We shall not prove the statements claimed in this definition, since they are particular cases of more general results that will be proven below (about groups acting on sets).

For example, the necklaces of length 3 over the set $A = \{1, 2\}$ are

$$\begin{aligned} [(1,1,1)]_{\underset{\text{cyc}}{\sim}} &= \{(1,1,1)\}, \\ [(1,1,2)]_{\underset{\text{cyc}}{\sim}} &= \{(1,1,2), (1,2,1), (2,1,1)\}, \\ [(1,2,2)]_{\underset{\text{cyc}}{\sim}} &= \{(1,2,2), (2,2,1), (2,1,2)\}, \\ [(2,2,2)]_{\underset{\text{cyc}}{\sim}} &= \{(2,2,2)\}. \end{aligned}$$

This may suggest that a necklace $[(a_1, a_2, \ldots, a_k)]_{\underset{\text{cyc}}{\sim}}$ is uniquely determined by how often each element appears in the tuple $(a_1, a_2, \ldots, a_k)$. But this is not true in general; for example, if $A = \{1,2,3\}$, then

$$[(1,2,3)]_{\underset{\text{cyc}}{\sim}} = \{(1,2,3), (2,3,1), (3,1,2)\} \qquad \text{and}$$
$$[(1,3,2)]_{\underset{\text{cyc}}{\sim}} = \{(1,3,2), (3,2,1), (2,1,3)\}$$

are two different necklaces of length 3 over the set $A = \{1,2,3\}$.

How many necklaces of length k over a q-element set A exist? It turns out that there is a nice formula for this, involving Euler's totient function ϕ:

Theorem 3.3.10. Let k be a positive integer. Let A be a q-element set (where $q \in \mathbb{N}$). Then, the number of necklaces of length k over the set A is

$$\frac{1}{k} \sum_{d \mid k} \phi(d) q^{k/d}.$$

Note that it is not (a priori) clear that $\frac{1}{k} \sum_{d \mid k} \phi(d) q^{k/d}$ is an integer! Actually, this holds even when q is a negative integer, even though there exist no q-element sets in that case. Thus, $\frac{1}{k} \sum_{d \mid k} \phi(d) x^{k/d}$ is another integer-valued polynomial for each positive integer k.

We will prove Theorem 3.3.10 using the concept of group actions further below.

3.3.6. Definition of the quotient set and the projection map

Definition 3.3.11. Let S be a set, and let $\sim$ be an equivalence relation on S.

(a) The set of equivalence classes of $\sim$ is denoted by $S/\sim$. It is called the *quotient* (or *quotient set*) of S by $\sim$.

(b) The map

$$S \to S/\sim,$$
$$s \mapsto [s]_{\sim}$$

(which sends each element $s \in S$ to its equivalence class) is called the *canonical projection (onto the quotient)*, and we will denote it by $\pi_{\sim}$.

(c) An element of an equivalence class of $\sim$ is also called a *representative* of this class.

Exercise 3.3.3. Let S be a set.

Recall that if T is a further set, and if $f : S \to T$ is a map, then an equivalence relation $\underset{f}{\equiv}$ is defined on the set S. (See Example 3.2.7 for its definition.)

Now, let $\sim$ be **any** equivalence relation on S. Prove that $\sim$ has the form $\underset{f}{\equiv}$ for a properly chosen set T and a properly chosen $f : S \to T$.

More precisely, prove that $\sim$ equals $\underset{f}{\equiv}$, where T is the quotient set $S/\sim$ and where $f : S \to T$ is the canonical projection $\pi_\sim : S \to S/\sim$.

[**Hint:** To prove that two relations R_1 and R_2 on S are equal, you need to check that every pair (a, b) of elements of S satisfies the equivalence $(aR_1b) \iff (aR_2b)$.]

3.4. $\mathbb{Z}/n$ ("integers modulo n")

We now come to one of the most important example of equivalence classes: the residue classes of integers modulo a given positive integer n.

Convention 3.4.1. For the whole Section 3.4, we fix an integer n.

3.4.1. Definition of $\mathbb{Z}/n$

Definition 3.4.2. **(a)** Define a relation $\underset{n}{\equiv}$ on the set $\mathbb{Z}$ by

$$\left(a \underset{n}{\equiv} b\right) \iff (a \equiv b \bmod n).$$

(This is precisely the relation $\underset{n}{\equiv}$ from Example 3.1.2 **(e)**.)

Recall that $\underset{n}{\equiv}$ is an equivalence relation (by Example 3.2.5).

(b) A *residue class modulo n* means an equivalence class of the relation $\underset{n}{\equiv}$.

For example,

$$\begin{aligned}
[0]_{\underset{5}{\equiv}} &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}, \\
[1]_{\underset{5}{\equiv}} &= \{\ldots, -14, -9, -4, 1, 6, 11, 16, 21, \ldots\}, \\
[2]_{\underset{5}{\equiv}} &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\}, \\
[3]_{\underset{5}{\equiv}} &= \{\ldots, -12, -7, -2, 3, 8, 13, 18, 23, \ldots\}, \\
[4]_{\underset{5}{\equiv}} &= \{\ldots, -11, -6, -1, 4, 9, 14, 19, 24, \ldots\}
\end{aligned}$$

are all the residue classes modulo 5. As you see, these classes are in 1-to-1 correspondence with the 5 possible remainders $0, 1, 2, 3, 4$ modulo 5. This generalizes (see Theorem 3.4.4 below). First, let us introduce a few notations:

Definition 3.4.3. **(a)** If i is an integer, then we denote the residue class $[i]_{\underset{n}{\equiv}}$ by $[i]_n$. (Some authors denote this residue class by $\overline{i}_n$ or $i \operatorname{mod} n$. Be careful with the notation $i \operatorname{mod} n$, since other authors use it for the integer $i \% n$ when n is positive.)

(b) The set $\mathbb{Z}/\underset{n}{\equiv}$ of all residue classes modulo n is called $\mathbb{Z}/n$. (Some authors call it $\mathbb{Z}/(n)$ or $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$. Be careful with the notation $\mathbb{Z}_n$, since it has a different meaning, too.)

3.4.2. What $\mathbb{Z}/n$ looks like

Let us now state and rigorously prove what we have just observed on the example of $n = 5$:

Theorem 3.4.4. Assume that the integer n is positive.

The set $\mathbb{Z}/n$ has exactly n elements, namely $[0]_n, [1]_n, \ldots, [n-1]_n$. (In particular, these elements $[0]_n, [1]_n, \ldots, [n-1]_n$ are distinct.)

Before we prove this, let us make a simple observation:

Proposition 3.4.5. **(a)** Each element of $\mathbb{Z}/n$ can be written in the form $[s]_n$ for some integer s.

(b) Let a and b be integers. Then, we have $[a]_n = [b]_n$ if and only if $a \equiv b \operatorname{mod} n$.

Proof of Proposition 3.4.5. **(a)** If $\sigma \in \mathbb{Z}/n$, then σ is a residue class modulo n (by the definition of $\mathbb{Z}/n$), and thus is an equivalence class of the relation $\underset{n}{\equiv}$ (by the definition of a residue class). Hence, this σ can be written in the form $[s]_{\underset{n}{\equiv}}$ for some integer s. In other words, this σ can be written in the form $[s]_n$ for some integer s (since we have defined $[s]_n$ to be a shorthand for $[s]_{\underset{n}{\equiv}}$). In other words, each element of $\mathbb{Z}/n$ can be written in the form $[s]_n$ for some integer s. This proves Proposition 3.4.5 **(a)**.

(b) Theorem 3.3.5 **(e)** (applied to $\mathbb{Z}$, $\underset{n}{\equiv}$, a and b instead of S, $\sim$, x and y) shows that we have $a \underset{n}{\equiv} b$ if and only if $[a]_{\underset{n}{\equiv}} = [b]_{\underset{n}{\equiv}}$. Thus, we have the logical equivalence

$$\left(a \underset{n}{\equiv} b\right) \iff \left([a]_{\underset{n}{\equiv}} = [b]_{\underset{n}{\equiv}}\right). \tag{116}$$

Definition 3.4.3 **(a)** shows that $[a]_n = [a]_{\underset{n}{\equiv}}$ and $[b]_n = [b]_{\underset{n}{\equiv}}$. Hence, we have the following chain of logical equivalences:

$$\begin{aligned}([a]_n = [b]_n) &\iff \left([a]_{\underset{n}{\equiv}} = [b]_{\underset{n}{\equiv}}\right) \iff \left(a \underset{n}{\equiv} b\right) \qquad \text{(by (116))} \\ &\iff (a \equiv b \operatorname{mod} n)\end{aligned}$$

(by the definition of the relation $\underset{n}{\equiv}$). In other words, we have $[a]_n = [b]_n$ if and only if $a \equiv b \bmod n$. This proves Proposition 3.4.5 **(b)**. □

Proof of Theorem 3.4.4. We have a map

$$\begin{aligned} \pi_{\underset{n}{\equiv}} : \mathbb{Z} &\to \mathbb{Z}/n, \\ s &\mapsto [s]_n . \end{aligned}$$

(This is simply the map $\pi_\sim$ defined in Definition 3.3.11 **(b)**, applied to the case when $S = \mathbb{Z}$ and when $\sim$ is the equivalence relation $\underset{n}{\equiv}$.)

We restrict this map $\underset{n}{\equiv}$ to the set $\{0, 1, \ldots, n-1\}$; we thus obtain a map

$$\begin{aligned} P : \{0, 1, \ldots, n-1\} &\to \mathbb{Z}/n, \\ s &\mapsto [s]_n . \end{aligned}$$

Our goal is to prove that this map P is bijective.

In general, there are two ways in which one usually proves that a map is bijective: One way is to prove that it is surjective and injective; the other way is by constructing an inverse to this map. Both ways can be used here; let us follow the second way, since it demonstrates an important point about equivalence classes.

So we want to construct an inverse to the map P. To do so, we try to define a map

$$\begin{aligned} R : \mathbb{Z}/n &\to \{0, 1, \ldots, n-1\}, \\ [s]_n &\mapsto s\%n \end{aligned}$$

(that is, a map $R : \mathbb{Z}/n \to \{0, 1, \ldots, n-1\}$ that sends each residue class $[s]_n$ to the remainder $s\%n$). Can we do this? Would this map R be actually well-defined?

First of all, our definition of R does indeed specify a value of $R(\sigma)$ for each $\sigma \in \mathbb{Z}/n$. This is because each element of $\mathbb{Z}/n$ can be written in the form $[s]_n$ for some integer s (because of Proposition 3.4.5 **(a)**), and therefore our definition tells us where this element should go under R.

Furthermore, if s is an integer, then $s\%n \in \{0, 1, \ldots, n-1\}$ (by Corollary 2.6.9 **(a)**, applied to $u = s$). Hence, our definition of R does not require the map R to take values lying outside of its target[102].

However, there is one more thing that could go wrong with our definition of R: One element σ of $\mathbb{Z}/n$ can be written as $[s]_n$ for several different integers s. For instance, $[2]_5 = [7]_5 = [12]_5 = [17]_5 = \cdots$. If the remainders $s\%n$ of these integers s were different, then the map R would have to send the class σ to several different

[102] This is one way in which maps can fail to be well-defined. For example, the map

$$\mathbb{N} \to \mathbb{N}, \qquad i \mapsto i - 1$$

is not well-defined for this reason (because $i - 1 \notin \mathbb{N}$ for $i = 0$).

numbers, and this is not something a map can do. To see an example where this does go wrong, let us try to define a map

$$\begin{aligned} R_{\text{wrong}} : \mathbb{Z}/n &\to \{0, 1, \ldots, n-1\}, \\ [s]_n &\mapsto s \% (n+1). \end{aligned}$$

So this definition of R_{wrong} is identical to our definition of R above, except that we are sending $[s]_n$ to $s \% (n+1)$ rather than to $s\%n$. However, R_{wrong} does not actually exist. In fact, if this ostensible map R_{wrong} would exist, then it would have to send $[0]_n$ to $0\% (n+1) = 0$ and send $[-n]_n$ to $(-n) \% (n+1) = 1$ [103]; however, $[0]_n$ and $[-n]_n$ are the same residue class (since $0 \equiv -n \mod n$), whereas 0 and 1 are not the same number, and thus this map R_{wrong} would send the same class to two different numbers. Thus, the map R_{wrong} does not exist.

We shall now check that our above definition of R does **not** suffer from this problem. In other words, we shall check that in the definition of

$$\begin{aligned} R : \mathbb{Z}/n &\to \{0, 1, \ldots, n-1\}, \\ [s]_n &\mapsto s\%n, \end{aligned}$$

any two possible integers s leading to the same class $[s]_n$ also lead to the same remainder $s\%n$. In other words, we shall prove the following claim:

> *Claim 1:* If s_1 and s_2 are two integers such that $[s_1]_n = [s_2]_n$, then $s_1\%n = s_2\%n$.

[*Proof of Claim 1:* Let s_1 and s_2 be two integers such that $[s_1]_n = [s_2]_n$.

Proposition 3.4.5 **(b)** (applied to s_1 and s_2 instead of a and b) shows that we have $[s_1]_n = [s_2]_n$ if and only if $s_1 \equiv s_2 \mod n$. Thus, we have $s_1 \equiv s_2 \mod n$ (since $[s_1]_n = [s_2]_n$). But Exercise 2.6.1 (applied to $u = s_1$ and $v = s_2$) shows that $s_1 \equiv s_2 \mod n$ if and only if $s_1\%n = s_2\%n$. Hence, we have $s_1\%n = s_2\%n$. This proves Claim 1.]

Claim 1 shows that if s is an integer, then $s\%n$ depends only on the **residue class** $[s]_n$, but not on the actual integer s. Thus, if we have a residue class $\sigma \in \mathbb{Z}/n$, then we can write σ in the form $\sigma = [s]_n$ for some integer s (since every residue class in $\mathbb{Z}/n$ can be written in this form), and then the integer $s\%n$ will depend only on the class σ and not on the specific choice of this integer s. Hence, the map R is well-defined.

Now we have two maps

$$\begin{aligned} P : \{0, 1, \ldots, n-1\} &\to \mathbb{Z}/n, \\ s &\mapsto [s]_n \end{aligned}$$

and

$$\begin{aligned} R : \mathbb{Z}/n &\to \{0, 1, \ldots, n-1\}, \\ [s]_n &\mapsto s\%n. \end{aligned}$$

We claim that they are mutually inverse. Indeed:

[103] The equality $(-n) \% (n+1) = 1$ follows from writing $-n$ in the form $-n = (-1) \cdot (n+1) + 1$.

- We have $P \circ R = \operatorname{id}$.

  [*Proof:* Let $\sigma \in \mathbb{Z}/n$. We shall prove that $(P \circ R)(\sigma) = \operatorname{id}(\sigma)$.

  Proposition 3.4.5 **(a)** says that each element of $\mathbb{Z}/n$ can be written in the form $[s]_n$ for some integer s. Hence, σ can be written in this form. In other words, $\sigma = [s]_n$ for some integer s. Consider this s. The definition of R yields $R([s]_n) = s\%n$. Corollary 2.6.9 **(a)** (applied to $u = s$) yields $s\%n \equiv s \mod n$. Now, from $\sigma = [s]_n$, we obtain

  $$\begin{aligned}(P \circ R)(\sigma) &= (P \circ R)([s]_n) = P\left(\underbrace{R([s]_n)}_{=s\%n}\right) = P(s\%n) \\ &= [s\%n]_n \qquad \text{(by the definition of } P\text{)} \\ &= [s]_n \qquad \text{(since } s\%n \equiv s \mod n\text{)} \\ &= \sigma = \operatorname{id}(\sigma).\end{aligned}$$

  Now, forget that we fixed σ. We thus have proven that $(P \circ R)(\sigma) = \operatorname{id}(\sigma)$ for each $\sigma \in \mathbb{Z}/n$. In other words, $P \circ R = \operatorname{id}$.]

- We have $R \circ P = \operatorname{id}$.

  [*Proof:* Let $s \in \{0, 1, \ldots, n-1\}$. Thus, Corollary 2.6.9 **(c)** (applied to $u = s$ and $c = s$) yields $s = s\%n$ (since $s \equiv s \mod n$). But the definition of P yields $P(s) = [s]_n$. Hence,

  $$\begin{aligned}(R \circ P)(s) &= R\left(\underbrace{P(s)}_{=[s]_n}\right) = R([s]_n) = s\%n \qquad \text{(by the definition of } R\text{)} \\ &= s = \operatorname{id}(s).\end{aligned}$$

  Now, forget that we fixed s. We thus have proven that $(R \circ P)(s) = \operatorname{id}(s)$ for each $s \in \{0, 1, \ldots, n-1\}$. In other words, $R \circ P = \operatorname{id}$.]

Combining $P \circ R = \operatorname{id}$ and $R \circ P = \operatorname{id}$, we conclude that the maps P and R are mutually inverse. Thus, the map P is invertible, i.e., bijective. Hence, P is surjective and injective. Since P is injective, we see that P must send the distinct elements $0, 1, \ldots, n-1$ of its domain to distinct elements. In other words, the n elements $P(0), P(1), \ldots, P(n-1)$ of $\mathbb{Z}/n$ must be distinct.

But recall that $P(s) = [s]_n$ for each $s \in \{0, 1, \ldots, n-1\}$ (by the definition of P). Thus, the n elements $P(0), P(1), \ldots, P(n-1)$ can be rewritten as $[0]_n, [1]_n, \ldots, [n-1]_n$. Hence, the n elements $[0]_n, [1]_n, \ldots, [n-1]_n$ are distinct (since the n elements $P(0), P(1), \ldots, P(n-1)$ are distinct).

Moreover, P is surjective. Thus,

$$\begin{aligned}\mathbb{Z}/n &= P\left(\{0,1,\ldots,n-1\}\right) \\ &= \{P(0), P(1), \ldots, P(n-1)\} \\ &= \{[0]_n, [1]_n, \ldots, [n-1]_n\}\end{aligned}$$

(since $P(s) = [s]_n$ for each $s \in \{0,1,\ldots,n-1\}$). In other words, the elements of $\mathbb{Z}/n$ are exactly the n elements $[0]_n, [1]_n, \ldots, [n-1]_n$. These n elements are distinct (as we have previously shown). Hence, the set $\mathbb{Z}/n$ has exactly n elements, namely $[0]_n, [1]_n, \ldots, [n-1]_n$. This proves Theorem 3.4.4. □

Let us summarize some of the facts we have shown in the above proof as a separate proposition:

Proposition 3.4.6. Let n be a positive integer.

(a) The two maps

$$\begin{aligned}P : \{0,1,\ldots,n-1\} &\to \mathbb{Z}/n, \\ s &\mapsto [s]_n\end{aligned}$$

and

$$\begin{aligned}R : \mathbb{Z}/n &\to \{0,1,\ldots,n-1\}, \\ [s]_n &\mapsto s\%n\end{aligned}$$

are well-defined and mutually inverse, and thus are bijections.

(b) Let $\alpha \in \mathbb{Z}/n$. Then, there exists a unique $a \in \{0,1,\ldots,n-1\}$ satisfying $\alpha = [a]_n$.

Proof of Proposition 3.4.6. **(a)** During the proof of Theorem 3.4.4 above, we have shown that the maps P and R are well-defined and mutually inverse. Hence, these maps P and R are invertible, i.e., are bijective. In other words, the maps P and R are bijections. Thus, Proposition 3.4.6 **(a)** is proven.

(b) Consider the maps P and R from Proposition 3.4.6 **(a)**. Then, Proposition 3.4.6 **(a)** shows that these two maps P and R are well-defined and mutually inverse, and thus are bijections.

We have $P \circ R = \operatorname{id}$ (since P and R are mutually inverse). Hence, $(P \circ R)(\alpha) = \operatorname{id}(\alpha) = \alpha$. Hence, $\alpha = (P \circ R)(\alpha) = P(R(\alpha)) = [R(\alpha)]_n$ (by the definition of P). Thus, there exists **at least one** $a \in \{0,1,\ldots,n-1\}$ satisfying $\alpha = [a]_n$ (namely, $a = R(\alpha)$). (Indeed, $R(\alpha) \in \{0,1,\ldots,n-1\}$ follows from the fact that R is a map from $\mathbb{Z}/n$ to $\{0,1,\ldots,n-1\}$.)

On the other hand, let $a \in \{0,1,\ldots,n-1\}$ be such that $\alpha = [a]_n$. We shall prove that $a = R(\alpha)$. Indeed, the definition of P yields $P(a) = [a]_n = \alpha$; hence, $a = P^{-1}(\alpha)$ (since the map P is invertible). But $P^{-1} = R$ (since P and R are mutually inverse). Thus, $a = \underbrace{P^{-1}}_{=R}(\alpha) = R(\alpha)$.

Now, forget that we fixed a. We thus have shown that every $a \in \{0, 1, \ldots, n-1\}$ satisfying $\alpha = [a]_n$ must satisfy $a = R(\alpha)$. In other words, every $a \in \{0, 1, \ldots, n-1\}$ satisfying $\alpha = [a]_n$ must be equal to $R(\alpha)$. Hence, there exists **at most one** such a.

Now, we conclude that there exists **a unique** $a \in \{0, 1, \ldots, n-1\}$ satisfying $\alpha = [a]_n$ (because we have shown that there exists **at least one** such a, and we have shown that there exists **at most one** such a). This proves Proposition 3.4.6 **(b)**. □

Proposition 3.4.6 **(b)** can be restated as follows: Each residue class $\alpha \in \mathbb{Z}/n$ has a unique representative in the set $\{0, 1, \ldots, n-1\}$.

3.4.3. Making choices that don't matter: The universal property of quotient sets

In the above proof of Theorem 3.4.4, we have witnessed an important issue in dealing with quotient sets: If you want to define a map f going **out** of a quotient set $S/\sim$ [104], then the easiest way to do so is often to specify $f([s]_\sim)$ for each $s \in S$; but in order to ensure that this definition is well-defined (i.e., that our map f actually exists), we need to verify that the value of $f([s]_\sim)$ we are specifying depends **only on the equivalence class** $[s]_\sim$ but not on the representative s. In other words, we need to verify that if s_1 and s_2 are two elements of S such that $[s_1]_\sim = [s_2]_\sim$, then our definition of f assigns the same value to $f([s_1]_\sim)$ as it does to $f([s_2]_\sim)$. This verification (which we did in our above proof by proving Claim 1) is often quite easy, but it is necessary.

Let us restate this strategy for defining maps out of a quotient set more rigorously:

> **Remark 3.4.7.** Let S and T be two sets, and let $\sim$ be an equivalence relation on S. Assume that we want to define a map
>
> $$f : S/\sim \rightarrow T, \qquad [s]_\sim \mapsto F(s),$$
>
> where $F(s)$ is some element of T for each $s \in S$. (That is, we want to define a map $f : S \rightarrow T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$.)
>
> In order to ensure that this f is well-defined, we need to verify that if s_1 and s_2 are two elements of S such that $[s_1]_\sim = [s_2]_\sim$, then $F(s_1) = F(s_2)$. If this verification has been done, the map f is well-defined.

Further examples of maps out of quotient sets defined in this way can be found in [ConradW][105].

[104] In our case, the quotient set was $\mathbb{Z}/\underset{n}{\equiv}$ (also known as $\mathbb{Z}/n$), and the map we wanted to define was R.

[105] When reading [ConradW, Example 1.1], keep in mind that rational numbers are defined as equivalence classes of elements of $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, as we have seen in Example 3.3.6. Thus, $\mathbb{Q}$ is actually a quotient set: namely, $\mathbb{Q} = S/\underset{*}{\sim}$ using the notations of Example 3.3.6.

Let us illustrate this method of defining maps on a few more examples:

Example 3.4.8. Let A be a set, and let $k \in \mathbb{N}$. Fix some $c \in A$. We can then define a map

$$\begin{aligned} \operatorname{mult}_c : A^k &\to \mathbb{N}, \\ (a_1, a_2, \ldots, a_k) &\mapsto (\text{the number of } i \in \{1, 2, \ldots, k\} \text{ such that } a_i = c). \end{aligned}$$

This map mult_c simply sends each k-tuple to the number of times that c appears in this k-tuple. For example, $\operatorname{mult}_5 (1, 5, 2, 4, 7, 5, 5, 6) = 3$, since 5 appears exactly 3 times in the 8-tuple $(1, 5, 2, 4, 7, 5, 5, 6)$ (assuming that $k = 8$ and $A = \mathbb{Z}$). It is clear that this map mult_c is well-defined. (The number $\operatorname{mult}_c \mathbf{a}$ for a k-tuple $\mathbf{a}$ is called the *multiplicity of c in* $\mathbf{a}$. Therefore the notation "mult_c".)

Now, it stands to reason that the same can be done with **unordered** k-tuples: After all, the number of times that c appears in a k-tuple should not depend on the order of the entries of the tuple. To formalize this, however, we need to deal with quotient sets. Indeed, recall that the "unordered k-tuples of elements of A" were defined (in Definition 3.3.8) as equivalence classes of the relation $\underset{\text{perm}}{\sim}$ on the set A^k. So $A^k / \underset{\text{perm}}{\sim}$ is the set of all unordered k-tuples of elements of A. The map that counts how often c appears in an unordered k-tuple should thus have the form

$$\begin{aligned} \operatorname{mult}'_c : A^k / \underset{\text{perm}}{\sim} &\to \mathbb{N}, \\ [(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}} &\mapsto (\text{the number of } i \in \{1, 2, \ldots, k\} \text{ such that } a_i = c). \end{aligned}$$

Or, to put it more compactly (making use of the map mult_c for **ordered** k-tuples defined above), it should have the form

$$\begin{aligned} \operatorname{mult}'_c : A^k / \underset{\text{perm}}{\sim} &\to \mathbb{N}, \\ [\mathbf{a}]_{\underset{\text{perm}}{\sim}} &\mapsto \operatorname{mult}_c \mathbf{a}. \end{aligned}$$

The question is: Why is this map mult'_c well-defined?

Remark 3.4.7 (applied to A^k, $\mathbb{N}$ and $\underset{\text{perm}}{\sim}$ instead of S, T and $\sim$) shows that in order to ensure that this map mult'_c is well-defined, we need to verify that if $\mathbf{a}_1$ and $\mathbf{a}_2$ are two elements of A^k (that is, two ordered k-tuples) such that $[\mathbf{a}_1]_{\underset{\text{perm}}{\sim}} = [\mathbf{a}_2]_{\underset{\text{perm}}{\sim}}$, then $\operatorname{mult}_c (\mathbf{a}_1) = \operatorname{mult}_c (\mathbf{a}_2)$. Let us do this: Let $\mathbf{a}_1$ and $\mathbf{a}_2$ be two elements of A^k (that is, two ordered k-tuples) such that $[\mathbf{a}_1]_{\underset{\text{perm}}{\sim}} = [\mathbf{a}_2]_{\underset{\text{perm}}{\sim}}$. Now, $[\mathbf{a}_1]_{\underset{\text{perm}}{\sim}} = [\mathbf{a}_2]_{\underset{\text{perm}}{\sim}}$ entails $\mathbf{a}_1 \underset{\text{perm}}{\sim} \mathbf{a}_2$ (indeed, Theorem 3.3.5 **(e)** shows that we have $\mathbf{a}_1 \underset{\text{perm}}{\sim} \mathbf{a}_2$ if and only if $[\mathbf{a}_1]_{\underset{\text{perm}}{\sim}} = [\mathbf{a}_2]_{\underset{\text{perm}}{\sim}}$). In other words, $\mathbf{a}_1$ is a permutation of $\mathbf{a}_2$ (by the definition of $\underset{\text{perm}}{\sim}$). In other words, the tuples $\mathbf{a}_1$ and $\mathbf{a}_2$ differ only in the order of their entries. Hence, Lemma 2.13.21 (applied to A, $\mathbf{a}_1$, $\mathbf{a}_2$ and c instead of P, $(a_1, a_2, \ldots, a_k)$, $(b_1, b_2, \ldots, b_\ell)$ and p) yields that

$$(\text{the number of times } c \text{ appears in } \mathbf{a}_1) = (\text{the number of times } c \text{ appears in } \mathbf{a}_2).$$

This rewrites as $\operatorname{mult}_c (\mathbf{a}_1) = \operatorname{mult}_c (\mathbf{a}_2)$ (since $(\text{the number of times } c \text{ appears in } \mathbf{a}_1) = \operatorname{mult}_c (\mathbf{a}_1)$ and $(\text{the number of times } c \text{ appears in } \mathbf{a}_2) = \operatorname{mult}_c (\mathbf{a}_2)$). This is what we needed to prove. Thus, we have shown that mult'_c is well-defined.

On the other hand, if we tried to define a map

$$\begin{aligned} \operatorname{first} : A^k / \underset{\text{perm}}{\sim} &\to \mathbb{N}, \\ [\mathbf{a}]_{\underset{\text{perm}}{\sim}} &\mapsto (\text{the first entry of } \mathbf{a}) \end{aligned}$$

(assuming that $k > 0$, so that an ordered k-tuple does indeed have a first entry), then we would run into troubles, because it is **not** true that if $\mathbf{a}_1$ and $\mathbf{a}_2$ are two elements of A^k such that $[\mathbf{a}_1]_{\underset{\text{perm}}{\sim}} = [\mathbf{a}_2]_{\underset{\text{perm}}{\sim}}$, then $(\text{the first entry of } \mathbf{a}_1) = (\text{the first entry of } \mathbf{a}_2)$. And this is no surprise: There is no such thing as "the first entry" of an unordered k-tuple. The first entry of a k-tuple is sensitive to reordering of its entries.

We can restate this method of defining maps as a rigorous theorem:

Theorem 3.4.9. Let S and T be two sets, and let $\sim$ be an equivalence relation on S. For each $s \in S$, let $F(s)$ be an element of T. (In other words, let F be a map from S to T.) Assume that the following assumption holds:

> *Assumption 1:* If s_1 and s_2 are two elements of S satisfying $s_1 \sim s_2$, then $F(s_1) = F(s_2)$.

Then, there exists a unique map $f : S/\sim \to T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$.

Theorem 3.4.9 says that (under the assumption that Assumption 1 holds) we can define a map

$$\begin{aligned} f : S/\sim &\to T, \\ [s]_\sim &\mapsto F(s). \end{aligned}$$

For example, the map R defined in our proof of Theorem 3.4.4 was defined in this way (with $\mathbb{Z}$, $\mathbb{Z}$, $\underset{n}{\equiv}$ and $s\%n$ playing the roles of S, T, $\sim$ and $F(s)$), and our proof of Claim 1 was essentially us verifying that Assumption 1 of Theorem 3.4.9 is satisfied.

For the sake of completeness, let us give a formal proof for Theorem 3.4.9 as well:

Proof of Theorem 3.4.9. We need to prove the following two statements:

> *Statement 1:* There exists **at least one** map $f : S/\sim \to T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$.
>
> *Statement 2:* There exists **at most one** map $f : S/\sim \to T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$.

[*Proof of Statement 1:* We define a map φ as follows:

Let $\sigma \in S/\sim$. Thus, σ is an equivalence class of $\sim$ (by the definition of $S/\sim$). In other words, $\sigma = [s]_\sim$ for some element $s \in S$. In other words, there exists some element $s \in S$

such that $\sigma = [s]_\sim$. If s_1 and s_2 are two such elements s, then $F(s_1) = F(s_2)$ [106]. Thus, the element $F(s) \in T$ obtained from such an element s does not depend on the choice of s (as long as σ is fixed). Hence, we can define $\varphi(\sigma)$ by setting

$$\varphi(\sigma) = F(s), \tag{117}$$

where s is any element of S satisfying $\sigma = [s]_\sim$.

Define $\varphi(\sigma)$ this way. Thus, we have defined an element $\varphi(\sigma)$ of T for each $\sigma \in S/\sim$. Hence, we have defined a map $\varphi : S/\sim \to T$. Moreover, this map has the property that every $s \in S$ satisfies $\varphi([s]_\sim) = F(s)$. (Indeed, this follows from (117) (applied to $\sigma = [s]_\sim$), since obviously $[s]_\sim = [s]_\sim$.)

Hence, there exists **at least one** map $f : S/\sim \to T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$ (namely, the map φ). This proves Statement 1.]

[*Proof of Statement 2:* Let f_1 and f_2 be two maps $f : S/\sim \to T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$. We shall show that $f_1 = f_2$.

We know that f_1 is a map $f : S/\sim \to T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$. In other words, f_1 is a map from $S/\sim$ to T and has the property that

$$\text{every } s \in S \text{ satisfies } f_1([s]_\sim) = F(s). \tag{118}$$

Likewise, f_2 is a map from $S/\sim$ to T and has the property that

$$\text{every } s \in S \text{ satisfies } f_2([s]_\sim) = F(s). \tag{119}$$

Now, let $\sigma \in S/\sim$ be arbitrary. Thus, σ is an equivalence class of $\sim$ (by the definition of $S/\sim$). In other words, $\sigma = [s]_\sim$ for some element $s \in S$. Consider this s. Then, from $\sigma = [s]_\sim$, we obtain $f_1(\sigma) = f_1([s]_\sim) = F(s)$ (by (118)). Similarly, $f_2(\sigma) = F(s)$. Comparing these two equalities, we find $f_1(\sigma) = f_2(\sigma)$.

Forget that we fixed σ. We thus have proven that $f_1(\sigma) = f_2(\sigma)$ for each $\sigma \in S/\sim$. In other words, $f_1 = f_2$.

Forget that we fixed f_1 and f_2. We thus have proven that if f_1 and f_2 are two maps $f : S/\sim \to T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$, then $f_1 = f_2$. In other words, there exists **at most one** such map f. This proves Statement 2.]

Now, we conclude that there exists a unique map $f : S/\sim \to T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$ (because Statement 1 shows that there exists **at least one** such map, while Statement 2 shows that there exists **at most one** such map). This proves Theorem 3.4.9. □

Theorem 3.4.9 is known as the *universal property of the quotient set*.

3.4.4. Projecting from $\mathbb{Z}/n$ to $\mathbb{Z}/d$

As another example of a map from a quotient set, let us define certain maps from $\mathbb{Z}/n$ to $\mathbb{Z}/d$ that exist whenever two integers n and d satisfy $d \mid n$:

[106] *Proof.* Let s_1 and s_2 be two such elements s. Then, $\sigma = [s_1]_\sim$ (since s_1 is an element $s \in S$ such that $\sigma = [s]_\sim$) and $\sigma = [s_2]_\sim$ (for similar reasons). Hence, $[s_1]_\sim = \sigma = [s_2]_\sim$. But Theorem 3.3.5 **(e)** (applied to $x = s_1$ and $y = s_2$) yields that we have $s_1 \sim s_2$ if and only if $[s_1]_\sim = [s_2]_\sim$. Hence, we have $s_1 \sim s_2$ (since $[s_1]_\sim = [s_2]_\sim$). Thus, Assumption 1 shows that $F(s_1) = F(s_2)$, qed.

Proposition 3.4.10. Let n be an integer. Let d be a divisor of n. Then, there is a map

$$\begin{aligned} \pi_{n,d} : \mathbb{Z}/n &\to \mathbb{Z}/d, \\ [s]_n &\mapsto [s]_d . \end{aligned}$$

Example 3.4.11. **(a)** For example, for $n = 6$ and $d = 2$, Proposition 3.4.10 says that there is a map

$$\begin{aligned} \pi_{6,2} : \mathbb{Z}/6 &\to \mathbb{Z}/2, \\ [s]_6 &\mapsto [s]_2 . \end{aligned}$$

This map sends the residue classes

$$\begin{aligned} & [0]_6 , [1]_6 , [2]_6 , [3]_6 , [4]_6 , [5]_6 \\ \text{to } & [0]_2 , [1]_2 , [2]_2 , [3]_2 , [4]_2 , [5]_2 , \text{ respectively.} \end{aligned}$$

In other words, it sends the residue classes

$$\begin{aligned} & [0]_6 , [1]_6 , [2]_6 , [3]_6 , [4]_6 , [5]_6 \\ \text{to } & [0]_2 , [1]_2 , [0]_2 , [1]_2 , [0]_2 , [1]_2 , \text{ respectively} \end{aligned}$$

(since $[2]_2 = [0]_2$ and $[3]_2 = [1]_2$ and $[4]_2 = [0]_2$ and $[5]_2 = [1]_2$). More generally, for arbitrary positive integers n and d satisfying $d \mid n$, the map $\pi_{n,d}$ sends the n residue classes $[0]_n , [1]_n , \ldots , [n-1]_n$ to

$$[0]_d , [1]_d , \ldots , [d-1]_d , [0]_d , [1]_d , \ldots , [d-1]_d , \ldots , [0]_d , [1]_d , \ldots , [d-1]_d$$

(that is, $[0]_d , [1]_d , \ldots , [d-1]_d$ in this order, repeated $\dfrac{n}{d}$ many times), respectively.

(b) For a non-example, set $n = 3$ and $d = 2$. Then, Proposition 3.4.10 does not apply, since 2 is not a divisor of 3. And for good reason: There is no map

$$\begin{aligned} \pi_{3,2} : \mathbb{Z}/3 &\to \mathbb{Z}/2, \\ [s]_3 &\mapsto [s]_2 . \end{aligned}$$

Indeed, this map would have to send $[0]_3$ and $[3]_3$ to $[0]_2$ and $[3]_2$, respectively; but this means sending two equal inputs to different outputs (since $[0]_3 = [3]_3$ but $[0]_2 \neq [3]_2$), which is impossible. More generally, if a positive integer d is **not** a divisor of a positive integer n, then there is no map

$$\begin{aligned} \pi_{n,d} : \mathbb{Z}/n &\to \mathbb{Z}/d, \\ [s]_n &\mapsto [s]_d . \end{aligned}$$

Proof of Proposition 3.4.10. We must prove that, for an integer $s \in \mathbb{Z}$, the class $[s]_d \in \mathbb{Z}/d$ depends only on the residue class $[s]_n$ but not on the integer s itself. In other words, we need to prove the following claim:

> *Claim 1:* If s_1 and s_2 are two integers such that $[s_1]_n = [s_2]_n$, then $[s_1]_d = [s_2]_d$.

[*Proof of Claim 1:* Let s_1 and s_2 be two integers such that $[s_1]_n = [s_2]_n$.

Proposition 3.4.5 **(b)** (applied to $a = s_1$ and $b = s_2$) shows that we have $[s_1]_n = [s_2]_n$ if and only if $s_1 \equiv s_2 \mod n$. Thus, we have $s_1 \equiv s_2 \mod n$ (since $[s_1]_n = [s_2]_n$). Hence, Proposition 2.3.4 **(e)** (applied to s_1, s_2 and d instead of a, b and m) yields $s_1 \equiv s_2 \mod d$ (since $d \mid n$).

But Proposition 3.4.5 **(b)** (applied to d, s_1 and s_2 instead of n, a and b) shows that we have $[s_1]_d = [s_2]_d$ if and only if $s_1 \equiv s_2 \mod d$. Thus, we have $[s_1]_d = [s_2]_d$ (since $s_1 \equiv s_2 \mod d$). This proves Claim 1.]

Having proven Claim 1, we can now conclude that the map

$$\pi_{n,d} : \mathbb{Z}/n \to \mathbb{Z}/d,$$
$$[s]_n \mapsto [s]_d$$

is well-defined. (This can be regarded as a consequence of applying Theorem 3.4.9 to $\mathbb{Z}$, $\mathbb{Z}/d$, $\underset{n}{\equiv}$ and $[s]_d$ instead of S, T, $\sim$ and $F(s)$. The Claim 1 that we proved above guarantees that Assumption 1 of Theorem 3.4.9 is satisfied.) Hence, Proposition 3.4.10 is proven. □

The next exercise is unrelated to $\mathbb{Z}/n$, but has been placed in this section because it relies on the same sort of "well-definedness" argument that we have seen in our proofs above:

Exercise 3.4.1. Fix a prime p. For each nonzero rational number r, define an integer $w_p(r)$ (called the *extended p-adic valuation* of r) as follows: We write r in the form $r = a/b$ for two nonzero integers a and b, and we set $w_p(r) = v_p(a) - v_p(b)$. (It also makes sense to set $w_p(0) = \infty$, but we shall not concern ourselves with this border case in this exercise.)

(a) Prove that this is well-defined – i.e., that $w_p(r)$ does not depend on the precise choice of a and b satisfying $r = a/b$.

(b) Prove that $w_p(n) = v_p(n)$ for each nonzero integer n.

(c) Prove that $w_p(ab) = w_p(a) + w_p(b)$ for any two nonzero rational numbers a and b.

(d) Prove that $w_p(a+b) \geq \min\{w_p(a), w_p(b)\}$ for any two nonzero rational numbers a and b if $a + b \neq 0$.

Exercise 3.4.2. Let r be a nonzero rational number. In Exercise 3.4.1, we have defined an integer $w_p(r)$ for each prime p. Prove the following:

(a) All but finitely many primes p satisfy $w_p(r) = 0$.

(b) We have $|r| = \prod\limits_{p \text{ prime}} p^{w_p(r)}$ (and in particular, the product $\prod\limits_{p \text{ prime}} p^{w_p(r)}$ is well-defined, i.e., has only finitely many factors different from 1).

(c) We have $r \in \mathbb{Z}$ if and only if each prime p satisfies $w_p(r) \geq 0$.

(d) We have the logical equivalence

$$\left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k r \in \mathbb{Z}\right)$$
$$\Longleftrightarrow \ \left(\text{every prime } p \text{ satisfying } w_p(r) < 0 \text{ satisfies } p \mid m\right).$$

Note that Exercise 3.4.2 **(b)** can be regarded as a canonical factorization for rational numbers. (Unlike the canonical factorization for integers, it allows negative exponents on the primes.)

3.4.5. Addition, subtraction and multiplication in $\mathbb{Z}/n$

Let us recall the concept of a binary operation (defined in Definition 1.6.1). We shall now define several such operations on the set $\mathbb{Z}/n$ [107]:

Definition 3.4.12. **(a)** We define a binary operation $+$ on $\mathbb{Z}/n$ (called *addition*) by setting

$$[a]_n + [b]_n = [a+b]_n \qquad \text{for any integers } a \text{ and } b.$$

(In other words, we define a binary operation $+$ on $\mathbb{Z}/n$ as follows: For any $\alpha, \beta \in \mathbb{Z}/n$, we let $\alpha + \beta = [a+b]_n$, where a and b are two integers satisfying $\alpha = [a]_n$ and $\beta = [b]_n$.)

(b) We define a binary operation $-$ on $\mathbb{Z}/n$ (called *subtraction*) by setting

$$[a]_n - [b]_n = [a-b]_n \qquad \text{for any integers } a \text{ and } b.$$

(c) We define a binary operation $\cdot$ on $\mathbb{Z}/n$ (called *multiplication*) by setting

$$[a]_n \cdot [b]_n = [a \cdot b]_n \qquad \text{for any integers } a \text{ and } b.$$

We also write $[a]_n [b]_n$ for $[a]_n \cdot [b]_n$.

Theorem 3.4.13. Everything defined in Definition 3.4.12 is well-defined.

Proof of Theorem 3.4.13. **(a)** Let us first prove that the binary operation $+$ in Definition 3.4.12 **(a)** is well-defined.

Indeed, here we are in the same situation in which we were when defining the map R in the proof of Theorem 3.4.4: We are trying to define a map (in the current case, the binary operation $+$, which should be a map from $(\mathbb{Z}/n) \times (\mathbb{Z}/n)$ to $\mathbb{Z}/n$) by specifying how it acts on inputs of the form $[a]_n$, but our definition refers to the

[107] We will check afterwards that these operations are indeed well-defined.

integer a. (Actually, it is a little bit more complicated: We have two inputs $[a]_n$ and $[b]_n$ and thus two integers a and b. But the problem we are facing is the same.) We want to prove that this map is well-defined. This requires checking that the output (that is, $[a+b]_n$) depends only on the two classes $[a]_n$ and $[b]_n$, but not on the integers a and b.

So we have to prove the following:

> *Claim 1:* Let a_1 and a_2 be two integers such that $[a_1]_n = [a_2]_n$. Let b_1 and b_2 be two integers such that $[b_1]_n = [b_2]_n$. Then,
> $$[a_1 + b_1]_n = [a_2 + b_2]_n .$$

[*Proof of Claim 1:* Proposition 3.4.5 **(b)** (applied to a_1 and a_2 instead of a and b) shows that we have $[a_1]_n = [a_2]_n$ if and only if $a_1 \equiv a_2 \mod n$. Thus, we have $a_1 \equiv a_2 \mod n$ (since $[a_1]_n = [a_2]_n$). Similarly, $b_1 \equiv b_2 \mod n$ (since $[b_1]_n = [b_2]_n$). Adding these two congruences together, we obtain $a_1 + b_1 \equiv a_2 + b_2 \mod n$.

But Proposition 3.4.5 **(b)** (applied to $a_1 + b_1$ and $a_2 + b_2$ instead of a and b) shows that we have $[a_1 + b_1]_n = [a_2 + b_2]_n$ if and only if $a_1 + b_1 \equiv a_2 + b_2 \mod n$. Thus, we have $[a_1 + b_1]_n = [a_2 + b_2]_n$ (since $a_1 + b_1 \equiv a_2 + b_2 \mod n$). This proves Claim 1.]

Claim 1 shows that in Definition 3.4.12 **(a)**, the residue class $[a+b]_n$ depends only on the two classes $[a]_n$ and $[b]_n$, but not on the integers a and b. Thus, the binary operation $+$ in Definition 3.4.12 **(a)** is indeed well-defined.

(b) The binary operation $-$ in Definition 3.4.12 **(b)** is well-defined. This can be proven in the same way as we just proved that the binary operation $+$ in Definition 3.4.12 **(a)** is well-defined; the only difference is that we now have to subtract the congruences $a_1 \equiv a_2 \mod n$ and $b_1 \equiv b_2 \mod n$ instead of adding them together.

(c) The binary operation $\cdot$ in Definition 3.4.12 **(c)** is well-defined. This can be proven in the same way as we just proved that the binary operation $+$ in Definition 3.4.12 **(a)** is well-defined; the only difference is that we now have to multiply the congruences $a_1 \equiv a_2 \mod n$ and $b_1 \equiv b_2 \mod n$ instead of adding them together.

Thus, we have proven that all three operations $+$, $-$ and $\cdot$ in Definition 3.4.12 are well-defined. This proves Theorem 3.4.13. □

Recall that $\mathbb{Z}/n$ is a finite set (of size n) whenever n is a positive integer. Hence, for each given positive integer n, we can tabulate all the values of the operations $+$, $-$ and $\cdot$; the resulting tables are called *addition tables*, *subtraction tables* and *multiplication tables* (like in high school, except that we are working with residue classes now).

Example 3.4.14. **(a)** If $n = 3$, then the addition, subtraction and multiplication tables for $\mathbb{Z}/n = \mathbb{Z}/3$ are

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

,

$-$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[2]_3$	$[1]_3$
$[1]_3$	$[1]_3$	$[0]_3$	$[2]_3$
$[2]_3$	$[2]_3$	$[1]_3$	$[0]_3$

,

$\cdot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

.

(Here, the entry in the row corresponding to α and the column corresponding to β is $\alpha + \beta$, $\alpha - \beta$ and $\alpha \cdot \beta$, respectively.)

(b) If $n = 2$, then the addition, subtraction and multiplication tables for $\mathbb{Z}/n = \mathbb{Z}/2$ are

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

,

$-$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

,

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

.

(In particular, the addition table is the same as the subtraction table, because any $\alpha, \beta \in \mathbb{Z}/2$ satisfy $\alpha + \beta = \alpha - \beta$. This follows from Exercise 2.3.1.)

Remark 3.4.15. We **cannot** define a division operation on $\mathbb{Z}/n$ by setting

$$[a]_n \,/\, [b]_n := [a/b]_n \qquad \text{for any integers } a \text{ and } b.$$

Indeed, leaving aside the issues that b could be 0 or a/b could be non-integer, this would still not be well-defined, because the class $[a/b]_n$ depends not just on $[a]_n$ and $[b]_n$ but also on the concrete choices of a and b. For example, for $n = 4$, this ostensible "division operation" would have to satisfy

$$\text{``}\,[6]_4 \,/\, [2]_4\,\text{''} = [6/2]_4 = [3]_4$$

and

$$\text{``}\,[2]_4 \,/\, [2]_4\,\text{''} = [2/2]_4 = [1]_4,$$

but this is impossible (since $[6]_4 = [2]_4$ but $[3]_4 \neq [1]_4$).

For similar reasons, we cannot define $\left([a]_n\right)^{[b]_n}$.

For the outputs of our binary operations $+$, $-$ and $\cdot$ on $\mathbb{Z}/n$, we shall use the same terminology as with integers:

Definition 3.4.16. **(a)** If α and β are two elements of $\mathbb{Z}/n$, then we shall refer to $\alpha + \beta$ as the *sum* of α and β.

(b) If α and β are two elements of $\mathbb{Z}/n$, then we shall refer to $\alpha - \beta$ as the *difference* of α and β.

(c) If α and β are two elements of $\mathbb{Z}/n$, then we shall refer to $\alpha \cdot \beta$ (also known as $\alpha\beta$) as the *product* of α and β.

(d) If α is an element of $\mathbb{Z}/n$, then the difference $[0]_n - \alpha$ shall be denoted by $-\alpha$.

Caution: While the remainder $i\%n$ and the residue class $[i]_n$ encode the same information about an integer i (for a fixed positive integer n), they are not the same thing! For example, any two integers u and v satisfy $[u]_n + [v]_n = [u + v]_n$ but don't always satisfy $u\%n + v\%n = (u+v)\%n$ [108]. Thus, it is important to distinguish between $i\%n$ and $[i]_n$.

Remark 3.4.17. We can view the residue classes modulo 24 (that is, the elements of $\mathbb{Z}/24$) as the hours of the day. For example, the time "2 AM" can be viewed as the residue class $[2]_{24}$, whereas the time "3 PM" can be viewed as the residue class $[15]_{24}$. From this point of view, addition of residue classes is a rather familiar operation: For example, the statement that "10 hours from 3 PM is 1 AM" is saying $[15]_{24} + [10]_{24} = [1]_{24}$.

3.4.6. Scaling by $r \in \mathbb{Z}$

Let us define another operation – not binary this time – on $\mathbb{Z}/n$:

Definition 3.4.18. Fix $r \in \mathbb{Z}$.

For any $\alpha \in \mathbb{Z}/n$, we define a residue class $r\alpha \in \mathbb{Z}/n$ by setting

$$\left(r\,[a]_n = [ra]_n \qquad \text{for any } a \in \mathbb{Z}\right).$$

(In other words, for any $\alpha \in \mathbb{Z}/n$, we let $r\alpha = [ra]_n$, where a is an integer satisfying $\alpha = [a]_n$.) This is well-defined, because of Proposition 3.4.19 **(a)** below.

We also write $r \cdot [a]_n$ for $r\,[a]_n$.

Proposition 3.4.19. Fix $r \in \mathbb{Z}$.

(a) For any $\alpha \in \mathbb{Z}/n$, the residue class $r\alpha \in \mathbb{Z}/n$ in Definition 3.4.18 is well-defined.

(b) For any $\alpha \in \mathbb{Z}/n$, we have $r\alpha = [r]_n \cdot \alpha$.

Proof of Proposition 3.4.19. **(a)** We are again in the same situation in which we were when defining the map R in the proof of Theorem 3.4.4: We are trying to define a map (in this case, the map

$$\begin{aligned} \mathbb{Z}/n &\to \mathbb{Z}/n, \\ \alpha &\mapsto r\alpha \end{aligned}$$

) by specifying how it acts on inputs of the form $[a]_n$, but our definition refers to the integer a. We want to prove that this map is well-defined. This requires checking that the output (that is, $[ra]_n$) depends only on the class $[a]_n$, but not on the integer a. So we have to prove the following:

[108] Here is a specific example:

$$\begin{aligned} [2]_5 + [3]_5 = [2+3]_5 = [5]_5 = [0]_5\,, \qquad &\text{but} \\ 2\%5 + 3\%5 = 2 + 3 = 5 \neq 0\%5; \end{aligned}$$

Exercise 2.6.3 **(a)** addresses how $u\%n + v\%n$ differs from $(u+v)\%n$.

> *Claim 1:* Let a_1 and a_2 be two integers such that $[a_1]_n = [a_2]_n$. Then, $[ra_1]_n = [ra_2]_n$.

[*Proof of Claim 1:* Proposition 3.4.5 **(b)** (applied to a_1 and a_2 instead of a and b) shows that we have $[a_1]_n = [a_2]_n$ if and only if $a_1 \equiv a_2 \mod n$. Thus, we have $a_1 \equiv a_2 \mod n$ (since $[a_1]_n = [a_2]_n$). On the other hand, we have the (obvious) congruence $r \equiv r \mod n$. Multiplying this congruence by the congruence $a_1 \equiv a_2 \mod n$, we obtain $ra_1 \equiv ra_2 \mod n$.

But Proposition 3.4.5 **(b)** (applied to ra_1 and ra_2 instead of a and b) shows that we have $[ra_1]_n = [ra_2]_n$ if and only if $ra_1 \equiv ra_2 \mod n$. Thus, we have $[ra_1]_n = [ra_2]_n$ (since $ra_1 \equiv ra_2 \mod n$). This proves Claim 1.]

Claim 1 shows that in Definition 3.4.18, the residue class $[ra]_n$ depends only on the class $[a]_n$, but not on the integer a. Thus, the residue class $r\alpha$ is indeed well-defined for each $\alpha \in \mathbb{Z}/n$. This proves Proposition 3.4.19 **(a)**.

(b) Let $\alpha \in \mathbb{Z}/n$. Proposition 3.4.5 **(a)** shows that each element of $\mathbb{Z}/n$ can be written in the form $[s]_n$ for some integer s. Thus, $\alpha \in \mathbb{Z}/n$ can be written in this form. In other words, $\alpha = [a]_n$ for some integer a. Consider this a. Comparing

$$r \underbrace{\alpha}_{=[a]_n} = r\,[a]_n = [ra]_n \qquad \text{(by Definition 3.4.18)}$$

with

$$\begin{aligned} [r]_n \cdot \underbrace{\alpha}_{=[a]_n} &= [r]_n \cdot [a]_n = [r \cdot a]_n \qquad \text{(by Definition 3.4.12 (c))} \\ &= [ra]_n , \end{aligned}$$

we obtain $r\alpha = [r]_n \cdot \alpha$. This proves Proposition 3.4.19 **(b)**. □

For a fixed $r \in \mathbb{Z}$, we shall refer to the map

$$\mathbb{Z}/n \to \mathbb{Z}/n,$$
$$\alpha \mapsto r\alpha$$

as *scaling by* r. This map is actually the same as multiplication by the residue class $[r]_n$ (by Proposition 3.4.19 **(b)**). So why did we define it "from scratch" rather than piggybacking on the already established definition of multiplication in $\mathbb{Z}/n$ (Definition 3.4.12 **(c)**)? The reason is that scaling operations appear much more frequently in algebra than multiplication operations. (For example, every vector space has a scaling operation, but usually there is no way of multiplying two vectors.) Thus, it is useful to have seen a scaling operation constructed independently.

3.4.7. k-th powers for $k \in \mathbb{N}$

Similarly to Definition 3.4.18, we can define what it means to take the k-th power of a residue class in $\mathbb{Z}/n$, when k is a nonnegative integer.

Definition 3.4.20. Fix $k \in \mathbb{N}$.

For any $\alpha \in \mathbb{Z}/n$, we define a residue class $\alpha^k \in \mathbb{Z}/n$ by setting

$$\left(\left([a]_n\right)^k = \left[a^k\right]_n \qquad \text{for any } a \in \mathbb{Z} \right).$$

(In other words, for any $\alpha \in \mathbb{Z}/n$, we let $\alpha^k = \left[a^k\right]_n$, where a is an integer satisfying $\alpha = [a]_n$.) This is well-defined, because of Proposition 3.4.21 below.

If $\alpha \in \mathbb{Z}/n$, then we shall refer to α^k as the *k-th power* of α.

Proposition 3.4.21. Fix $k \in \mathbb{N}$. For any $\alpha \in \mathbb{Z}/n$, the residue class $\alpha^k \in \mathbb{Z}/n$ in Definition 3.4.20 is well-defined.

Proof of Proposition 3.4.21. This proof is analogous to the above proof of Proposition 3.4.19 **(a)**; but instead of multiplying the two congruences $r \equiv r \bmod n$ and $a_1 \equiv a_2 \bmod n$, we now need to take the k-th power of the congruence $a_1 \equiv a_2 \bmod n$. (Exercise 2.3.4 allows us to do that.) □

3.4.8. Rules and properties for the operations

Convention 3.4.22. We shall follow the usual "PEMDAS" rules for the order of operations when interpreting expressions involving the operations defined in Definition 3.4.12, Definition 3.4.18 and Definition 3.4.20[109]. Thus, for example, the expression "$\alpha \cdot \beta + \gamma \cdot \delta$" means $(\alpha \cdot \beta) + (\gamma \cdot \delta)$ and not $\alpha \cdot (\beta + \gamma) \cdot \delta$. Likewise, the expression "$\alpha\beta^k + r\gamma$" (with $r \in \mathbb{Z}$) should be understood as "$\left(\alpha\left(\beta^k\right)\right) + (r\gamma)$" and not in any other way.

We shall now study some properties of the many "arithmetical" operations we have defined on $\mathbb{Z}/n$.

Theorem 3.4.23. The following rules for addition, subtraction, multiplication and scaling in $\mathbb{Z}/n$ hold:

(a) We have $\alpha + \beta = \beta + \alpha$ for any $\alpha, \beta \in \mathbb{Z}/n$.

(b) We have $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{Z}/n$.

(c) We have $\alpha + [0]_n = [0]_n + \alpha = \alpha$ for any $\alpha \in \mathbb{Z}/n$.

(d) We have $\alpha \cdot [1]_n = [1]_n \cdot \alpha = \alpha$ for any $\alpha \in \mathbb{Z}/n$.

(e) We have $\alpha \cdot \beta = \beta \cdot \alpha$ for any $\alpha, \beta \in \mathbb{Z}/n$.

(f) We have $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{Z}/n$.

(g) We have $\alpha \cdot (\beta + \gamma) = \alpha\beta + \alpha\gamma$ and $(\alpha + \beta) \cdot \gamma = \alpha\gamma + \beta\gamma$ for any $\alpha, \beta, \gamma \in \mathbb{Z}/n$.

(h) We have $\alpha \cdot [0]_n = [0]_n \cdot \alpha = [0]_n$ for any $\alpha \in \mathbb{Z}/n$.

(i) If $\alpha, \beta, \gamma \in \mathbb{Z}/n$, then we have the equivalence $(\alpha - \beta = \gamma) \iff (\alpha = \beta + \gamma)$.

(j) We have $r(\alpha + \beta) = r\alpha + r\beta$ for any $r \in \mathbb{Z}$ and $\alpha, \beta \in \mathbb{Z}/n$.

(k) We have $(r + s)\alpha = r\alpha + s\alpha$ for any $r, s \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}/n$.

(l) We have $r\left(s\alpha\right) = \left(rs\right)\alpha$ for any $r, s \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}/n$.

(m) We have $r\left(\alpha\beta\right) = \left(r\alpha\right)\beta = \alpha\left(r\beta\right)$ for any $r \in \mathbb{Z}$ and $\alpha, \beta \in \mathbb{Z}/n$.

(n) We have $-\left(r\alpha\right) = \left(-r\right)\alpha = r\left(-\alpha\right)$ for any $r \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}/n$.

(o) We have $1\alpha = \alpha$ for any $\alpha \in \mathbb{Z}/n$.

(p) We have $\left(-1\right)\alpha = -\alpha$ for any $\alpha \in \mathbb{Z}/n$.

(q) We have $-\left(\alpha + \beta\right) = \left(-\alpha\right) + \left(-\beta\right)$ for any $\alpha, \beta \in \mathbb{Z}/n$.

(r) We have $-\left[0\right]_n = \left[0\right]_n$.

(s) We have $-\left(-\alpha\right) = \alpha$ for any $\alpha \in \mathbb{Z}/n$.

(t) We have $-\left(\alpha\beta\right) = \left(-\alpha\right)\beta = \alpha\left(-\beta\right)$ for any $\alpha, \beta \in \mathbb{Z}/n$.

(u) We have $\alpha - \beta - \gamma = \alpha - \left(\beta + \gamma\right)$ for any $\alpha, \beta, \gamma \in \mathbb{Z}/n$. (Here and in the following, "$\alpha - \beta - \gamma$" should be read as "$\left(\alpha - \beta\right) - \gamma$".)

These properties should all look familiar, as they mirror the classical properties of the arithmetic operations on integers, rational numbers and real numbers (with the caveat that the residue classes $\left[0\right]_n$ and $\left[1\right]_n$ take on the roles of the numbers 0 and 1). For example, Theorem 3.4.23 **(g)** corresponds to the laws of distributivity for numbers. Parts **(a)**, **(b)**, **(c)**, **(i)**, **(j)**, **(k)**, **(l)** and **(o)** of Theorem 3.4.23 furthermore are reminiscent of the axioms for a vector space (with the caveat that scaling by r is only defined for integers r here, so $\mathbb{Z}/n$ is not precisely a vector space).

Proof of Theorem 3.4.23. Let us first prove Theorem 3.4.23 **(f)**:

(f) Let $\alpha, \beta, \gamma \in \mathbb{Z}/n$. Proposition 3.4.5 **(a)** shows that each element of $\mathbb{Z}/n$ can be written in the form $\left[s\right]_n$ for some integer s. Thus, in particular, the element α can be written in this form. In other words, there exists an integer a such that $\alpha = \left[a\right]_n$. Similarly, there exists an integer b such that $\beta = \left[b\right]_n$. Similarly, there exists an integer c such that $\gamma = \left[c\right]_n$. Consider these integers a, b, c.

Now,

$$\underbrace{\alpha}_{=\left[a\right]_n} \cdot \left(\underbrace{\beta}_{=\left[b\right]_n} \cdot \underbrace{\gamma}_{=\left[c\right]_n}\right) = \left[a\right]_n \cdot \underbrace{\left(\left[b\right]_n \cdot \left[c\right]_n\right)}_{\substack{=\left[b \cdot c\right]_n \\ \text{(by Definition 3.4.12 (c))}}} = \left[a\right]_n \cdot \left[b \cdot c\right]_n$$
$$= \left[a \cdot \left(b \cdot c\right)\right]_n \qquad (120)$$

(by Definition 3.4.12 **(c)**) and

$$\left(\underbrace{\alpha}_{=\left[a\right]_n} \cdot \underbrace{\beta}_{=\left[b\right]_n}\right) \cdot \underbrace{\gamma}_{=\left[c\right]_n} = \underbrace{\left(\left[a\right]_n \cdot \left[b\right]_n\right)}_{\substack{=\left[a \cdot b\right]_n \\ \text{(by Definition 3.4.12 (c))}}} \cdot \left[c\right]_n = \left[a \cdot b\right]_n \cdot \left[c\right]_n$$
$$= \left[\left(a \cdot b\right) \cdot c\right]_n \qquad (121)$$

(by Definition 3.4.12 **(c)**).

But it is well-known that multiplication of integers is associative. Thus, $a \cdot \left(b \cdot c\right) = \left(a \cdot b\right) \cdot c$. Hence, $\left[a \cdot \left(b \cdot c\right)\right]_n = \left[\left(a \cdot b\right) \cdot c\right]_n$. In other words, the right hand sides of the equalities (120) and (121) are equal. Hence, the left hand sides of these equalities must also be equal. In other words, $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$. This proves Theorem 3.4.23 **(f)**.

The idea of the above proof of Theorem 3.4.23 **(f)** was simple: We fixed a representative for each residue class involved (namely, we fixed representatives a, b, c for the residue classes α, β, γ), and rewrote each of the two sides of the alleged equality (which, in our case, was $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$) in terms of these representatives (obtaining $[a \cdot (b \cdot c)]_n$ for the left hand side, and $[(a \cdot b) \cdot c]_n$ for the right hand side). Thus, the equality that we had to prove followed from the analogous equality for integers (in our case, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$), which was well-known. In short, we have realized that the equality $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$ for $\alpha, \beta, \gamma \in \mathbb{Z}/n$ is "inherited from $\mathbb{Z}$" (in the sense that it follows straightforwardly from the corresponding property $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ of integers $a, b, c \in \mathbb{Z}$). This strategy proves all the other parts of Theorem 3.4.23 in the same way, except for part **(i)**.[110] Part **(i)** does not lend itself to such a proof, since it claims not an equality but rather an equivalence between two equalities. So let us prove part **(i)** separately:

(i) Let $\alpha, \beta, \gamma \in \mathbb{Z}/n$. Proposition 3.4.5 **(a)** shows that each element of $\mathbb{Z}/n$ can be written in the form $[s]_n$ for some integer s. Thus, in particular, the element α can be written in this form. In other words, there exists an integer a such that $\alpha = [a]_n$. Similarly, there exists an integer b such that $\beta = [b]_n$. Similarly, there exists an integer c such that $\gamma = [c]_n$. Consider these integers a, b, c.

We have $\underbrace{\alpha}_{=[a]_n} - \underbrace{\beta}_{=[b]_n} = [a]_n - [b]_n = [a-b]_n$ (by Definition 3.4.12 **(b)**) and $\underbrace{\beta}_{=[b]_n} + \underbrace{\gamma}_{=[c]_n} = [b]_n + [c]_n = [b+c]_n$ (by Definition 3.4.12 **(a)**). Now, we have the following chain of logical equivalences:

$$\begin{aligned}(\alpha - \beta = \gamma) &\iff ([a-b]_n = [c]_n) \qquad \text{(since } \alpha - \beta = [a-b]_n \text{ and } \gamma = [c]_n\text{)} \\ &\iff (a - b \equiv c \bmod n) \qquad (122)\end{aligned}$$

(since Proposition 3.4.5 **(b)** (applied to $a - b$ and c instead of a and b) shows that we have $[a-b]_n = [c]_n$ if and only if $a - b \equiv c \bmod n$). Also, we have the following chain of logical equivalences:

$$\begin{aligned}(\alpha = \beta + \gamma) &\iff ([a]_n = [b+c]_n) \qquad \text{(since } \alpha = [a]_n \text{ and } \beta + \gamma = [b+c]_n\text{)} \\ &\iff (a \equiv b + c \bmod n) \qquad (123)\end{aligned}$$

(since Proposition 3.4.5 **(b)** (applied to $b + c$ instead of b) shows that we have $[a]_n = [b+c]_n$ if and only if $a \equiv b + c \bmod n$). Finally, Exercise 2.3.8 shows that we have $a - b \equiv c \bmod n$ if and only if $a \equiv b + c \bmod n$; thus, we have the equivalence $(a - b \equiv c \bmod n) \iff (a \equiv b + c \bmod n)$.

[110] The reason why this works is that the operations $+, -, \cdot$ on $\mathbb{Z}/n$ as well as scaling by integers are defined by picking a representative of each residue class and doing the analogous operation **with the representatives** (and then taking the residue class again).

Now, we have the following chain of logical equivalences:

$$\begin{aligned}(\alpha - \beta = \gamma) &\iff (a - b \equiv c \operatorname{mod} n) \qquad (\text{by (122)}) \\ &\iff (a \equiv b + c \operatorname{mod} n) \iff (\alpha = \beta + \gamma) \qquad (\text{by (123)}) .\end{aligned}$$

This proves Theorem 3.4.23 **(i)**. □

Recall the concept of a finite sum of integers (i.e., a sum of the form $\sum_{i \in I} a_i$, where I is a finite set and a_i is an integer for each $i \in I$), and the analogous concept of a finite product of integers (i.e., a product of the form $\prod_{i \in I} a_i$). These concepts are defined recursively[111] and satisfy various rules[112]. See [Grinbe15, §1.4] for a comprehensive list of these rules and [Grinbe15, §2.14] for their proofs.

Definition 3.4.24. In the same vein, we define the concept of a finite sum of residue classes in $\mathbb{Z}/n$ (i.e., a sum of the form $\sum_{i \in I} \alpha_i$, where I is a finite set and $\alpha_i \in \mathbb{Z}/n$ for each $i \in I$), and the analogous concept of a finite product of residue classes in $\mathbb{Z}/n$ (i.e., a product of the form $\prod_{i \in I} \alpha_i$, where I is a finite set and $\alpha_i \in \mathbb{Z}/n$ for each $i \in I$).

More precisely, the concept of a finite sum $\sum_{i \in I} \alpha_i$ (with I being a finite set, and with $\alpha_i \in \mathbb{Z}/n$ for each $i \in I$) is defined recursively as follows:

- If the set I is empty (that is, $|I| = 0$), then $\sum_{i \in I} \alpha_i$ is defined to be $[0]_n \in \mathbb{Z}/n$ (and called an empty sum).
- Otherwise, we pick an arbitrary element $t \in I$, and set
$$\sum_{i \in I} \alpha_i = \alpha_t + \sum_{i \in I \setminus \{t\}} \alpha_i .$$
(The sum $\sum_{i \in I \setminus \{t\}} \alpha_i$ on the right hand side is a sum over a smaller set than I, whence we can assume it to already be defined in this recursive definition.)

This definition is well-defined (i.e., the choice of element t does not influence the final value of the sum), by Proposition 3.4.25 **(a)** below.

The concept of a finite product $\prod_{i \in I} \alpha_i$ is defined similarly, except that we use multiplication instead of addition (and we define the empty product to be $[1]_n$ instead of $[0]_n$).

[111] See [Grinbe15, §1.4.1 and §1.4.3] for their definitions, and [Grinbe15, §2.14] for a proof that these are well-defined.

[112] such as $\sum_{i \in I} (a_i + b_i) = \sum_{i \in I} a_i + \sum_{i \in I} b_i$ (where a_i and b_i are two integers for each $i \in I$) or $\sum_{i \in I} a_i = \sum_{i \in J} a_i + \sum_{i \in I \setminus J} a_i$ (where J is a subset of I)

We will use the usual shorthands for special kinds of finite sums and products. For example, if I is an interval $\{p, p+1, \ldots, q\}$ of integers (and if $\alpha_i \in \mathbb{Z}/n$ for each $i \in I$), then the sum $\sum\limits_{i\in I} \alpha_i$ will also be denoted by $\sum\limits_{i=p}^{q} \alpha_i$ or $\alpha_p + \alpha_{p+1} + \cdots + \alpha_q$. Likewise for products. Thus, for example, $\alpha_1 + \alpha_2 + \cdots + \alpha_k$ and $\alpha_1 \alpha_2 \cdots \alpha_k$ are well-defined whenever $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}/n$.

Proposition 3.4.25. **(a)** Definition 3.4.24 is well-defined.

(b) Finite sums ($\sum\limits_{i\in I} \alpha_i$) and finite products ($\prod\limits_{i\in I} \alpha_i$) of elements $\alpha_i \in \mathbb{Z}/n$ satisfy the same rules that finite sums and finite products of integers satisfy.

(c) If $a_1, a_2, \ldots, a_k$ are k integers, then

$$[a_1]_n + [a_2]_n + \cdots + [a_k]_n = [a_1 + a_2 + \cdots + a_k]_n \qquad \text{and}$$
$$[a_1]_n \cdot [a_2]_n \cdot \cdots \cdot [a_k]_n = [a_1 a_2 \cdots a_k]_n .$$

Proof of Proposition 3.4.25. **(a)** In [Grinbe15, Theorem 2.118 **(a)**], it is proven that finite sums of integers are well-defined. The same argument (but relying on Theorem 3.4.23 instead of the usual rules of commutativity, associativity etc. for integers) shows that finite sums of elements $\alpha_i \in \mathbb{Z}/n$ are well-defined. The analogous fact for products is proven in the same way, except that we need to replace $[0]_n$ by $[1]_n$ and properties of addition by corresponding properties of multiplication.

(b) The proofs of the properties of finite sums and finite products of elements of $\mathbb{Z}/n$ are identical to the analogous proofs for integers, but (again) rely on Theorem 3.4.23 instead of the usual rules of commutativity, associativity etc. for integers.

(c) This can be proven by a straightforward induction on k. □

Also, the standard rules for exponents apply to residue classes:

Theorem 3.4.26. **(a)** We have $\alpha^0 = [1]_n$ for any $\alpha \in \mathbb{Z}/n$.

(b) We have $\alpha^1 = \alpha$ for any $\alpha \in \mathbb{Z}/n$.

(c) We have $\alpha^k = \underbrace{\alpha\alpha\cdots\alpha}_{k \text{ times}}$ for any $\alpha \in \mathbb{Z}/n$ and $k \in \mathbb{N}$.

(d) We have $\alpha^{u+v} = \alpha^u \alpha^v$ for any $\alpha \in \mathbb{Z}/n$ and any $u, v \in \mathbb{N}$.

(e) We have $(\alpha\beta)^k = \alpha^k \beta^k$ for any $\alpha, \beta \in \mathbb{Z}/n$ and $k \in \mathbb{N}$.

(f) We have $(\alpha^u)^v = \alpha^{uv}$ for any $\alpha \in \mathbb{Z}/n$ and any $u, v \in \mathbb{N}$.

Proof of Theorem 3.4.26. Each part of Theorem 3.4.26 follows from the analogous property of integers, in the same way as we derived Theorem 3.4.23 **(f)** from the associativity of multiplication for integers. (Note that Proposition 3.4.25 **(c)** has to be used in proving Theorem 3.4.26 **(c)**.) □

Also, the binomial formula holds for residue classes:

Theorem 3.4.27. Let $\alpha, \beta \in \mathbb{Z}/n$ and $m \in \mathbb{N}$. Then,

$$(\alpha+\beta)^m = \sum_{k=0}^{m} \binom{m}{k} \alpha^k \beta^{m-k}.$$

Proof. This follows from Theorem 2.17.13, in the same way as we derived Theorem 3.4.23 **(f)** from the associativity of multiplication for integers. □

3.5. Modular inverses revisited

Convention 3.5.1. For the whole Section 3.5, we fix a positive integer n.

In this section, we will see how modular inverses become actual inverses when we consider residue classes instead of numbers.

Recall that if a is an integer, then an *inverse of a in $\mathbb{Z}$* means an integer $a' \in \mathbb{Z}$ satisfying $aa' = 1$. The only two integers that have an inverse in $\mathbb{Z}$ are 1 and -1. The integer 1 has only one inverse (namely, itself). The integer -1 has only one inverse (namely, itself). Thus, "inverse in $\mathbb{Z}$" is not a very interesting notion.

Let us now define an analogous notion for $\mathbb{Z}/n$:

Definition 3.5.2. Let $\alpha \in \mathbb{Z}/n$. An *inverse* of α means an $\alpha' \in \mathbb{Z}/n$ such that $\alpha \cdot \alpha' = [1]_n$.

For example, $[2]_5$ is an inverse of $[3]_5$ for $n = 5$, since $[3]_5 \cdot [2]_5 = [3 \cdot 2]_5 = [6]_5 = [1]_5$.

It turns out that inverses of residue classes $\alpha \in \mathbb{Z}/n$ exist much more frequently than inverses of integers in $\mathbb{Z}$:

Proposition 3.5.3. Let $a \in \mathbb{Z}$.

(a) If $[a]_n \in \mathbb{Z}/n$ has an inverse, then $a \perp n$.

(b) If $a \perp n$, then $[a]_n \in \mathbb{Z}/n$ has a unique inverse.

As we will see in the proof of this proposition, the inverse of a residue class $[a]_n$ is simply the residue class $[a']_n$ of a modular inverse a' of a modulo n; thus, the existence part of Proposition 3.5.3 **(b)** (i.e., the claim that $[a]_n$ has an inverse) is just Theorem 2.10.8 **(b)** in disguise. However, before we start proving Proposition 3.5.3, let us state the uniqueness part (i.e., the claim that the inverse of $[a]_n$ is unique) as a separate fact:

Proposition 3.5.4. Let $\alpha \in \mathbb{Z}/n$. Then, α has **at most one** inverse.

Proof of Proposition 3.5.4. Let β and γ be two inverses of α. We shall show that $\beta = \gamma$.

We have $\alpha \cdot \beta = [1]_n$ (since β is an inverse of α) and $\alpha \cdot \gamma = [1]_n$ (since γ is an inverse of α). Theorem 3.4.23 **(e)** (applied to γ and α instead of α and β) yields $\gamma \cdot \alpha = \alpha \cdot \gamma = [1]_n$.

Theorem 3.4.23 **(d)** (applied to γ instead of α) yields $\gamma \cdot [1]_n = [1]_n \cdot \gamma = \gamma$. Also, Theorem 3.4.23 **(d)** (applied to β instead of α) yields $\beta \cdot [1]_n = [1]_n \cdot \beta = \beta$.

Theorem 3.4.23 **(f)** (applied to γ, α and β instead of α, β and γ) shows that $\gamma \cdot (\alpha \cdot \beta) = (\gamma \cdot \alpha) \cdot \beta$. Now, comparing

$$\gamma \cdot \left(\underbrace{\alpha \cdot \beta}_{=[1]_n} \right) = \gamma \cdot [1]_n = \gamma$$

with

$$\gamma \cdot (\alpha \cdot \beta) = \left(\underbrace{\gamma \cdot \alpha}_{=[1]_n} \right) \cdot \beta = [1]_n \cdot \beta = \beta,$$

we obtain $\beta = \gamma$.

Now, forget that we fixed β and γ. We thus have proven that if β and γ are two inverses of α, then $\beta = \gamma$. In other words, any two inverses of α must be equal. In other words, α has at most one inverse. This proves Proposition 3.5.4. □

Note that in the above proof of Proposition 3.5.4, we have never had to pick a representative of the residue class α (nor of any other class). This is because this proof is actually an instance of a much more general argument. And indeed, you might recall that a very similar argument is used to prove the classical facts that

- a map has at most one inverse;
- a matrix has at most one inverse.

To be more precise, the proofs of these two facts differ slightly from our proof of Proposition 3.5.4, because the definitions of an inverse of a map and of an inverse of a matrix differ from Definition 3.5.2. Indeed, in Definition 3.5.2, we have only required the inverse α' of $\alpha \in \mathbb{Z}/n$ to satisfy the **single** equation $\alpha \cdot \alpha' = [1]_n$, whereas an inverse g of a map f is required to satisfy the **two** equations $f \circ g = \operatorname{id}$ and $g \circ f = \operatorname{id}$ (and likewise, an inverse B of a matrix A is required to satisfy the **two** equations $AB = I$ and $BA = I$ for the appropriate identity matrices I). But this difference is not substantial: The multiplication of residue classes in $\mathbb{Z}/n$ is commutative (by Theorem 3.4.23 **(e)**) (unlike the composition of maps or the multiplication of matrices); thus, the single equation $\alpha \cdot \alpha' = [1]_n$ automatically implies $\alpha' \cdot \alpha = [1]_n$. Hence, we could have as well required α' to satisfy both equations $\alpha \cdot \alpha' = [1]_n$ and $\alpha' \cdot \alpha = [1]_n$ in Definition 3.5.2, and nothing would change.

Let us now prove Proposition 3.5.3:

Proof of Proposition 3.5.3. **(a)** Assume that $[a]_n \in \mathbb{Z}/n$ has an inverse. Let β be this inverse. Write the residue class $\beta \in \mathbb{Z}/n$ in the form $[b]_n$ for some integer b. Now, β is an inverse of $[a]_n$. In other words, $[a]_n \cdot \beta = [1]_n$ (by the definition of "inverse"). But $[a]_n \cdot \underbrace{\beta}_{=[b]_n} = [a]_n \cdot [b]_n = [a \cdot b]_n$ (by the definition of multiplication on $\mathbb{Z}/n$). Comparing this with $[a]_n \cdot \beta = [1]_n$, we obtain $[a \cdot b]_n = [1]_n$. By Proposition 3.4.5 **(b)** (applied to $a \cdot b$ and 1 instead of a and b), this yields $a \cdot b \equiv 1 \mod n$. Hence, there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \mod n$ (namely, $a' = b$). Thus, Theorem 2.10.8 **(c)** yields $a \perp n$. This proves Proposition 3.5.3 **(a)**.

(b) Assume that $a \perp n$. Hence, Theorem 2.10.8 **(b)** yields that there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \mod n$. Consider this a'. From $aa' \equiv 1 \mod n$, we obtain $[aa']_n = [1]_n$ (by Proposition 3.4.5 **(b)**, applied to aa' and 1 instead of a and b). But the definition of multiplication on $\mathbb{Z}/n$ yields $[a]_n \cdot [a']_n = [a \cdot a']_n = [aa']_n = [1]_n$. In other words, $[a']_n$ is an inverse of $[a]_n$. Hence, $[a]_n$ has **at least** one inverse (namely, $[a']_n$).

But Proposition 3.5.4 (applied to $\alpha = [a]_n$) shows that $[a]_n$ has **at most** one inverse.

Thus, we conclude that $[a]_n$ has a unique inverse (since we already know that $[a]_n$ has **at least** one inverse and has **at most** one inverse). This proves Proposition 3.5.3. □

Corollary 3.5.5. Let U_n be the set of all residue classes $\alpha \in \mathbb{Z}/n$ that have an inverse. Then:

(a) For an integer a, we have the logical equivalence $([a]_n \in U_n) \iff (a \perp n)$.

(b) We have $|U_n| = \phi(n)$.

Proof of Corollary 3.5.5. **(a)** Let a be an integer. Proposition 3.5.3 **(a)** yields the logical implication

$$([a]_n \text{ has an inverse}) \implies (a \perp n). \tag{124}$$

But Proposition 3.5.3 **(b)** yields the logical implication

$$(a \perp n) \implies ([a]_n \text{ has a unique inverse}) \implies ([a]_n \text{ has an inverse}). \tag{125}$$

Combining the two implications (124) and (125), we obtain the equivalence

$$([a]_n \text{ has an inverse}) \iff (a \perp n). \tag{126}$$

But U_n was defined as the set of all residue classes $\alpha \in \mathbb{Z}/n$ that have an inverse. Hence, we have the following chain of equivalences:

$$([a]_n \in U_n) \iff ([a]_n \text{ has an inverse}) \iff (a \perp n)$$

(by (126)). This proves Corollary 3.5.5 **(a)**.

(b) Theorem 3.4.4 says that the set $\mathbb{Z}/n$ has exactly n elements, namely $[0]_n, [1]_n, \ldots, [n-1]_n$ (and in particular, these n elements are all distinct). Thus, the map

$$P : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n,$$
$$s \mapsto [s]_n$$

is bijective[113]. Consider this map P. For each integer a, we have the logical equivalence

$$\left(\underbrace{P\left(a\right)}_{\substack{=[a]_n \\ \text{(by the definition of } P\text{)}}} \in U_n \right) \iff \left([a]_n \in U_n \right) \iff \left(a \perp n \right) \qquad (127)$$

(by Corollary 3.5.5 **(a)**).

But the map P is bijective. Hence, we can substitute $P\left(a\right)$ for α when counting the number of $\alpha \in U_n$. We thus obtain

$$\begin{aligned} & \left(\text{the number of } \alpha \in U_n\right) \\ & = \left(\text{the number of } a \in \{0, 1, \ldots, n-1\} \text{ such that } P\left(a\right) \in U_n\right) \\ & = \left(\text{the number of } a \in \{0, 1, \ldots, n-1\} \text{ such that } a \perp n\right) \\ & \qquad \left(\begin{array}{c} \text{because for each } a \in \{0, 1, \ldots, n-1\}, \text{ we have the logical} \\ \text{equivalence } \left(P\left(a\right) \in U_n\right) \iff \left(a \perp n\right) \text{ (by (127))} \end{array}\right) \\ & = \left| \{a \in \{0, 1, \ldots, n-1\} \mid a \perp n\} \right| \\ & = \left| \{i \in \{0, 1, \ldots, n-1\} \mid i \perp n\} \right| \qquad \text{(here, we have renamed the index } a \text{ as } i\text{)} \\ & = \phi\left(n\right) \end{aligned}$$

(by Lemma 2.15.4). This proves Corollary 3.5.5 **(b)**. □

Definition 3.5.6. Let $\alpha \in \mathbb{Z}/n$ be a residue class that has an inverse. Then, Proposition 3.5.4 shows that α has **a unique** inverse. This inverse can thus be called "**the** *inverse*" of α; it will be denoted by α^{-1}.

For example, $\left([3]_5\right)^{-1} = [2]_5$ for $n = 5$, since $[2]_5$ is an inverse (and thus **the** inverse) of $[3]_5$.

Let us state a couple properties of inverses in $\mathbb{Z}/n$:

Exercise 3.5.1. **(a)** Let $\alpha \in \mathbb{Z}/n$ be a residue class that has an inverse. Prove that its inverse α^{-1} has an inverse as well, and this inverse is $\left(\alpha^{-1}\right)^{-1} = \alpha$.

(b) Let $\alpha, \beta \in \mathbb{Z}/n$ be two residue classes that have inverses. Prove that their product $\alpha\beta$ has an inverse as well, and this inverse is $\left(\alpha\beta\right)^{-1} = \alpha^{-1}\beta^{-1}$.

The concept of inverses in $\mathbb{Z}/n$ lets us prove Theorem 2.15.7 (Wilson's theorem) again – or, rather, restate our previous proof of Theorem 2.15.7 in more natural terms:

Second proof of Theorem 2.15.7 (sketched). Theorem 3.4.4 (applied to $n = p$) shows that the set $\mathbb{Z}/p$ has exactly p elements, namely $[0]_p, [1]_p, \ldots, [p-1]_p$. In particular, these elements $[0]_p, [1]_p, \ldots, [p-1]_p$ are distinct.

[113] We also have explicitly proven this fact during our proof of Theorem 3.4.4.

If $p = 2$, then the claim of Theorem 2.15.7 is easy to check (as we have done in our First proof above). Thus, we WLOG assume that $p \neq 2$ for the rest of this proof. Thus, $p - 1 \neq 1$; in other words, the numbers 1 and $p - 1$ are distinct. But p is a prime; thus, $p > 1$, so that the elements 1 and $p - 1$ belong to the set $\{0, 1, \ldots, p-1\}$. Thus, the two residue classes $[1]_p$ and $[p-1]_p$ are distinct[114].

Recall that

$$(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1).$$

Thus,

$$[(p-1)!]_p = [1 \cdot 2 \cdot \cdots \cdot (p-1)]_p = [1]_p \cdot [2]_p \cdot \cdots \cdot [p-1]_p$$

(by Proposition 3.4.25 **(c)**).

Let U_p be the set of all residue classes $\alpha \in \mathbb{Z}/p$ that have an inverse. Then, $[0]_p \notin U_p$ [115]. On the other hand, the $p - 1$ residue classes $[1]_p, [2]_p, \ldots, [p-1]_p$ all belong to U_p [116]. Combining these two sentences, we conclude that the $p - 1$ residue classes $[1]_p, [2]_p, \ldots, [p-1]_p$ are precisely the elements of U_p (since the set $\mathbb{Z}/p$ has exactly p elements, namely $[0]_p, [1]_p, \ldots, [p-1]_p$). Thus, these $p - 1$ residue classes have inverses (because belonging to U_p means having an inverse), and their inverses in turn have inverses (by Exercise 3.5.1 **(a)**) and thus belong to U_p (because belonging to U_p means having an inverse). Thus, the map

$$J : U_p \to U_p,$$
$$\alpha \mapsto \alpha^{-1}$$

(sending each of the $p - 1$ residue classes $[1]_p, [2]_p, \ldots, [p-1]_p$ to its inverse) is well-defined. Moreover, each $\alpha \in U_p$ satisfies $\left(\alpha^{-1}\right)^{-1} = \alpha$; in other words, each $\alpha \in U_p$ satisfies $J(J(\alpha)) = \alpha$. In other words, $J \circ J = \mathrm{id}$. Hence, the map J is inverse to itself. In particular, this shows that J is invertible, i.e., bijective.

(Note that this map J is similar to the map J constructed back in our first proof of Theorem 2.15.7 above, but unlike the latter, it acts on residue classes, not on actual numbers.)

[114] *Proof.* Recall that the elements $[0]_p, [1]_p, \ldots, [p-1]_p$ are distinct. In other words, if i and j are two distinct elements of $\{0, 1, \ldots, p-1\}$, then $[i]_p \neq [j]_p$. We can apply this to $i = 1$ and $j = p - 1$, since 1 and $p - 1$ are distinct. Thus, we obtain $[1]_p \neq [p-1]_p$. In other words, the two residue classes $[1]_p$ and $[p-1]_p$ are distinct.

[115] *Proof.* We have $p > 1$; thus, we don't have $|p| = 1$. But Exercise 2.10.1 **(b)** (applied to $a = p$) shows that we have $0 \perp p$ if and only if $|p| = 1$. Thus, we don't have $0 \perp p$ (since we don't have $|p| = 1$).

Corollary 3.5.5 **(a)** (applied to $n = p$ and $a = 0$) shows that we have the logical equivalence $\left([0]_p \in U_p\right) \iff (0 \perp p)$. Since we don't have $0 \perp p$, we thus conclude that we don't have $[0]_p \in U_p$. In other words, we have $[0]_p \notin U_p$.

[116] *Proof.* We must show that $[i]_p \in U_p$ for each $i \in \{1, 2, \ldots, p-1\}$.

So let $i \in \{1, 2, \ldots, p-1\}$. Then, Proposition 2.13.4 shows that i is coprime to p. In other words, $i \perp p$.

But Corollary 3.5.5 **(a)** (applied to $n = p$ and $a = i$) yields the equivalence $\left([i]_p \in U_p\right) \iff (i \perp p)$. Hence, we have $[i]_p \in U_p$ (since $i \perp p$). Qed.

Note that
$$[1]_p \cdot [2]_p \cdot \cdots \cdot [p-1]_p = \prod_{\alpha \in U_p} \alpha,$$
since the $p-1$ residue classes $[1]_p, [2]_p, \ldots, [p-1]_p$ are precisely the elements of U_p (and are distinct).

Now, we shall complete the proof using the same "pairing" that we used in our first proof of Theorem 2.15.7, except that we will now be pairing up residue classes rather than numbers. Namely, we will use the map J to establish a pairing between the factors of the product $[1]_p \cdot [2]_p \cdot \cdots \cdot [p-1]_p = \prod\limits_{\alpha \in U_p} \alpha$ (pairing up each factor α with the factor $J(\alpha) = \alpha^{-1}$), which will pair up almost all of them – more precisely, all of them except for the very first and very last factors (since these two factors would have to pair up with themselves)[117]. For example, if $p = 11$, then we have the following table of values of J:

α	$[1]_{11}$	$[2]_{11}$	$[3]_{11}$	$[4]_{11}$	$[5]_{11}$	$[6]_{11}$	$[7]_{11}$	$[8]_{11}$	$[9]_{11}$	$[10]_{11}$
$J(\alpha)$	$[1]_{11}$	$[6]_{11}$	$[4]_{11}$	$[3]_{11}$	$[9]_{11}$	$[2]_{11}$	$[8]_{11}$	$[7]_{11}$	$[5]_{11}$	$[10]_{11}$

(since, for example, $J([2]_{11}) = ([2]_{11})^{-1} = [6]_{11}$), and thus we pair up the factors of

[117] The reason **why** it is precisely these two factors that will not be paired up is the following:

Clearly, the factors $[a]_p$ that cannot be paired up are exactly the factors $[a]_p$ that satisfy $J\left([a]_p\right) = [a]_p$ – i.e., the ones that are their own inverses. So we must prove that a residue class $[a]_p$ with $a \in \{1, 2, \ldots, p-1\}$ is its own inverse if and only if a is either 1 or $p-1$. But this follows from the following chain of equivalences:

$$\begin{aligned}
&\left(\text{the residue class } [a]_p \text{ is its own inverse}\right) \\
\iff& \left([a]_p \cdot [a]_p = [1]_p\right) \iff \left(\left[a^2\right]_p = [1]_p\right) \qquad \left(\text{since } [a]_p \cdot [a]_p = [a \cdot a]_p = \left[a^2\right]_p\right) \\
\iff& \left(a^2 \equiv 1 \bmod p\right) \qquad (\text{by Proposition 3.4.5 } \textbf{(b)}) \\
\iff& (a \equiv 1 \bmod p \text{ or } a \equiv -1 \bmod p) \\
& \left(\begin{array}{c} \text{indeed, Exercise 2.13.12 yields the} \\ \text{implication } \left(a^2 \equiv 1 \bmod p\right) \implies (a \equiv 1 \bmod p \text{ or } a \equiv -1 \bmod p)\,; \\ \text{but the converse implication is easy to check} \end{array}\right) \\
\iff& \left([a]_p = [1]_p \text{ or } [a]_p = [-1]_p\right) \qquad (\text{by Proposition 3.4.5 } \textbf{(b)}) \\
\iff& \left([a]_p = [1]_p \text{ or } [a]_p = [p-1]_p\right) \qquad \left(\text{since } [-1]_p = [p-1]_p \text{ (because } -1 \equiv p-1 \bmod p)\right) \\
\iff& (a = 1 \text{ or } a = p-1)
\end{aligned}$$

(since the elements $[0]_p, [1]_p, \ldots, [p-1]_p$ are distinct).

the product $[1]_p \cdot [2]_p \cdot \cdots \cdot [p-1]_p$ as follows:

$$\begin{aligned} & [1]_p \cdot [2]_p \cdot \cdots \cdot [p-1]_p \\ & = [1]_{11} \cdot [2]_{11} \cdot [3]_{11} \cdot [4]_{11} \cdot [5]_{11} \cdot [6]_{11} \cdot [7]_{11} \cdot [8]_{11} \cdot [9]_{11} \cdot [10]_{11} \\ & = [1]_{11} \cdot ([2]_{11} \cdot [6]_{11}) \cdot ([3]_{11} \cdot [4]_{11}) \\ & \qquad \cdot ([5]_{11} \cdot [9]_{11}) \cdot ([7]_{11} \cdot [8]_{11}) \cdot [10]_{11} . \end{aligned} \tag{128}$$

By the definition of the map J, each pair has the form $(\alpha, J(\alpha)) = (\alpha, \alpha^{-1})$ for some $\alpha \in U_p$, and thus the product of any two different factors paired up with each other is $[1]_p$ (since $\alpha\alpha^{-1} = [1]_p$). For example, if $p = 11$, then we have

$$\begin{aligned} & [1]_p \cdot [2]_p \cdot \cdots \cdot [p-1]_p \\ & = [1]_{11} \cdot \underbrace{([2]_{11} \cdot [6]_{11})}_{=[1]_{11}} \cdot \underbrace{([3]_{11} \cdot [4]_{11})}_{=[1]_{11}} \cdot \underbrace{([5]_{11} \cdot [9]_{11})}_{=[1]_{11}} \cdot \underbrace{([7]_{11} \cdot [8]_{11})}_{=[1]_{11}} \cdot [10]_{11} \\ & = [1]_{11} \cdot [10]_{11} . \end{aligned}$$

Thus, any two different factors paired up with each other "neutralize" each other when being multiplied. Hence, the product of all the $p-1$ factors will reduce to the product of the two factors that have not been paired up, which will be $[1]_p \cdot [p-1]_p = [p-1]_p$. Since this product was $[(p-1)!]_p$, we thus obtain

$$[(p-1)!]_p = [p-1]_p . \tag{129}$$

In other words, $(p-1)! \equiv p-1 \equiv -1 \bmod p$. Hence, Theorem 2.15.7 is proven again.

Once again, if you like your proofs rigorous and formal, you may be wondering how this "pairing up" argument can be formalized. Here is one way to do so: We proceed similarly to how we formalized our first proof of Theorem 2.15.7 above, but with a minor complication. We want to call an element α of U_p

- *small* if $\alpha < J(\alpha)$;
- *medium* if $\alpha = J(\alpha)$;
- *large* if $\alpha > J(\alpha)$.

However, in order for this definition to make sense, we need to define two relations $<$ and $>$ on the set $\mathbb{Z}/p$; otherwise, it is not clear what "$\alpha < J(\alpha)$" and "$\alpha > J(\alpha)$" should mean. Fortunately, this is easy: For example, we can

- consider the bijection $R : \mathbb{Z}/p \to \{0, 1, \ldots, p-1\}$ defined in Proposition 3.4.6 **(a)** (applied to $n = p$);
- define the binary relation $<$ on the set $\mathbb{Z}/p$ by setting

$$(\alpha < \beta) \iff (R(\alpha) < R(\beta)) \qquad \text{for any } \alpha, \beta \in \mathbb{Z}/p;$$

- define the binary relation $>$ on the set $\mathbb{Z}/p$ by setting

$$(\alpha > \beta) \iff (R(\alpha) > R(\beta)) \qquad \text{for any } \alpha, \beta \in \mathbb{Z}/p.$$

The two relations we have just defined have the property that each $\alpha, \beta \in \mathbb{Z}/p$ satisfy either $\alpha < \beta$ or $\alpha = \beta$ or $\alpha > \beta$ but never two or more of these three statements simultaneously (indeed, this follows easily from the fact that R is a bijection). Thus, each element of U_p is either small or medium or large (and there is no overlap between these three classes of elements). Hence, the argument that we used to prove (72) in our first proof of Theorem 2.15.7[118] can be adapted in order to prove $[(p-1)!]_p = [-1]_p$, except that we have to use residue classes in U_p instead of elements of A. (We could have just as well used any other bijection from $\mathbb{Z}/p$ to $\{0, 1, \ldots, p-1\}$ instead of R here.) Of course, $[(p-1)!]_p = [-1]_p$ immediately yields $(p-1)! \equiv -1 \mod p$ (by an application of Proposition 3.4.5 **(b)**), and thus the proof of Theorem 2.15.7 is complete.

□

3.6. The Chinese Remainder Theorem as a bijection between residue classes

Definition 3.6.1. Let n be a positive integer. Let d be a positive divisor of n. Then, define the map

$$\pi_{n,d} : \mathbb{Z}/n \to \mathbb{Z}/d,$$
$$[s]_n \mapsto [s]_d .$$

(This is well-defined, according to Proposition 3.4.10.)

See Example 3.4.11 **(a)** for what this map looks like.

We can now state another version of the "Chinese Remainder Theorem", which claims the existence of a certain bijection. We have already seen such a version (Theorem 2.16.1), but that one claimed a bijection between two sets of **remainders**, whereas the following version claims a bijection between two sets of **residue classes**. Other than that, the two versions are rather similar.

Theorem 3.6.2. Let m and n be two coprime positive integers. Then, the map

$$S_{m,n} : \mathbb{Z}/(mn) \to (\mathbb{Z}/m) \times (\mathbb{Z}/n),$$
$$\alpha \mapsto (\pi_{mn,m}(\alpha), \pi_{mn,n}(\alpha))$$

is well-defined and is a bijection. It sends each $[s]_{mn}$ (with $s \in \mathbb{Z}$) to the pair $([s]_m, [s]_n)$.

[118] viz., by splitting up the product into a product over small elements, a product over medium elements, and a product over large elements

Example 3.6.3. **(a)** Theorem 3.6.2 (applied to $m = 3$ and $n = 2$) says that the map

$$\begin{aligned} S_{3,2} : \mathbb{Z}/6 &\to (\mathbb{Z}/3) \times (\mathbb{Z}/2), \\ \alpha &\mapsto (\pi_{6,3}(\alpha), \pi_{6,2}(\alpha)) \end{aligned}$$

is a bijection. This map sends

$$\begin{array}{cccccc} [0]_6, & [1]_6, & [2]_6, & [3]_6, & [4]_6, & [5]_6 \\ ([0]_3, [0]_2), & ([1]_3, [1]_2), & ([2]_3, [2]_2), & ([3]_3, [3]_2), & ([4]_3, [4]_2), & ([5]_3, [5]_2), \end{array} \quad \text{to}$$

respectively. In other words, it sends

$$\begin{array}{cccccc} [0]_6, & [1]_6, & [2]_6, & [3]_6, & [4]_6, & [5]_6 \\ ([0]_3, [0]_2), & ([1]_3, [1]_2), & ([2]_3, [0]_2), & ([0]_3, [1]_2), & ([1]_3, [0]_2), & ([2]_3, [1]_2), \end{array} \quad \text{to}$$

respectively (since $[2]_2 = [0]_2$ and $[3]_3 = [0]_3$ and $[3]_2 = [1]_2$ and so on). This list of values shows that this map is bijective (since it takes on every possible value in $(\mathbb{Z}/3) \times (\mathbb{Z}/2)$ exactly once). Theorem 3.6.2 says that this holds for arbitrary coprime m and n.

(b) Let us see how Theorem 3.6.2 fails when m and n are **not** coprime. For example, take $m = 6$ and $n = 4$. Then, the map

$$\begin{aligned} S_{6,4} : \mathbb{Z}/24 &\to (\mathbb{Z}/6) \times (\mathbb{Z}/4), \\ \alpha &\mapsto (\pi_{24,6}(\alpha), \pi_{24,4}(\alpha)) \end{aligned}$$

is **not** a bijection. Indeed, it is neither injective (for example, it sends both $[0]_{24}$ and $[12]_{24}$ to the same pair $([0]_6, [0]_4)$) nor surjective (for example, it never takes the value $([1]_6, [2]_4)$).

The following proof of Theorem 3.6.2 has the same structure as our proof of Theorem 2.16.1 above, but is shorter since residue classes are easier to deal with than remainders.

Proof of Theorem 3.6.2. The maps $\pi_{mn,m}$ and $\pi_{mn,n}$ are well-defined, since m and n are positive divisors of mn. Thus, the map

$$\begin{aligned} S_{m,n} : \mathbb{Z}/(mn) &\to (\mathbb{Z}/m) \times (\mathbb{Z}/n), \\ \alpha &\mapsto (\pi_{mn,m}(\alpha), \pi_{mn,n}(\alpha)) \end{aligned}$$

is well-defined. Consider this map $S_{m,n}$. Clearly, for each $s \in \mathbb{Z}$, we have

$$\begin{aligned} S_{m,n}\left([s]_{mn}\right) &= \left(\underbrace{\pi_{mn,m}\left([s]_{mn}\right)}_{\substack{=[s]_m \\ \text{(by the definition of } \pi_{mn,m}\text{)}}}, \underbrace{\pi_{mn,n}\left([s]_{mn}\right)}_{\substack{=[s]_n \\ \text{(by the definition of } \pi_{mn,n}\text{)}}} \right) \\ &\qquad \left(\text{by the definition of } S_{m,n}\right) \\ &= \left([s]_m, [s]_n\right). \end{aligned} \tag{130}$$

In other words, the map $S_{m,n}$ sends each $[s]_{mn}$ (with $s \in \mathbb{Z}$) to the pair $\left([s]_m, [s]_n\right)$.

It thus remains to prove that $S_{m,n}$ is a bijection. To that aim, we shall prove that $S_{m,n}$ is injective and surjective.

[*Proof that the map $S_{m,n}$ is injective:* Let $\alpha, \beta \in \mathbb{Z}/(mn)$ be such that $S_{m,n}(\alpha) = S_{m,n}(\beta)$. We want to prove $\alpha = \beta$.

Write the residue classes α and β in the forms $\alpha = [a]_{mn}$ and $\beta = [b]_{mn}$ for two integers a and b. (This is possible, because of Proposition 3.4.5 **(a)**.) From $\alpha = [a]_{mn}$, we obtain $S_{m,n}(\alpha) = S_{m,n}\left([a]_{mn}\right) = \left([a]_m, [a]_n\right)$ (by (130), applied to $s = a$). Similarly, $S_{m,n}(\beta) = \left([b]_m, [b]_n\right)$. Thus, the equality $S_{m,n}(\alpha) = S_{m,n}(\beta)$ (which we have assumed to hold) rewrites as $\left([a]_m, [a]_n\right) = \left([b]_m, [b]_n\right)$. In other words, $[a]_m = [b]_m$ and $[a]_n = [b]_n$.

Now, we have $[a]_m = [b]_m$; equivalently, $a \equiv b \mod m$ (by Proposition 3.4.5 **(b)**); in other words, $m \mid a - b$. Similarly, $n \mid a - b$.

Now, we have $m \perp n$ (since m and n are coprime) and $m \mid a - b$ and $n \mid a - b$. Hence, Theorem 2.10.7 (applied to m, n and $a - b$ instead of a, b and c) yields $mn \mid a - b$. In other words, $a \equiv b \mod mn$. In other words, $[a]_{mn} = [b]_{mn}$ (by Proposition 3.4.5 **(b)**). In other words, $\alpha = \beta$ (since $\alpha = [a]_{mn}$ and $\beta = [b]_{mn}$).

Now, forget that we fixed α and β. We thus have shown that if $\alpha, \beta \in \mathbb{Z}/(mn)$ are such that $S_{m,n}(\alpha) = S_{m,n}(\beta)$, then $\alpha = \beta$. In other words, the map $S_{m,n}$ is injective.]

[*Proof that the map $S_{m,n}$ is surjective:* Fix $(\alpha, \beta) \in (\mathbb{Z}/m) \times (\mathbb{Z}/n)$. We want to find a $\gamma \in \mathbb{Z}/(mn)$ such that $S_{m,n}(\gamma) = (\alpha, \beta)$.

We have $\alpha \in \mathbb{Z}/m$. Thus, we can write the residue class α as $\alpha = [a]_m$ for some integer a (because of Proposition 3.4.5 **(a)**). Similarly, we can write the residue class β as $\beta = [b]_n$ for some integer b. Consider these two integers a and b. Theorem 2.12.1 **(a)** shows that there exists an integer $x \in \mathbb{Z}$ such that

$$(x \equiv a \mod m \text{ and } x \equiv b \mod n).$$

Consider such an x. We have $[x]_m = [a]_m$ (since $x \equiv a \mod m$) and $[x]_n = [b]_n$ (since $x \equiv b \mod n$). Now, (130) (applied to $s = x$) yields

$$S_{m,n}\left([x]_{mn}\right) = \left(\underbrace{[x]_m}_{=[a]_m=\alpha}, \underbrace{[x]_n}_{=[b]_n=\beta} \right) = (\alpha, \beta).$$

Thus, there exists a $\gamma \in \mathbb{Z}/(mn)$ such that $S_{m,n}(\gamma) = (\alpha, \beta)$ (namely, $\gamma = [x]_{mn}$).

Now, forget that we fixed (α, β). We thus have shown that for any $(\alpha, \beta) \in (\mathbb{Z}/m) \times (\mathbb{Z}/n)$, there exists a $\gamma \in \mathbb{Z}/(mn)$ such that $S_{m,n}(\gamma) = (\alpha, \beta)$. In other words, the map $S_{m,n}$ is surjective.]

We have now proven that the map $S_{m,n}$ is both injective and surjective. Hence, this map $S_{m,n}$ is bijective, i.e., is a bijection. This completes the proof of Theorem 3.6.2.

[*Remark:* As in the proof of Theorem 2.16.1, we could have saved ourselves some of the work by invoking the Pigeonhole Principle. Indeed, our goal was to show that the map $S_{m,n}$ is bijective. By the Pigeonhole Principle, it suffices to prove that it is injective **or** that it is surjective, since $\mathbb{Z}/(mn)$ and $(\mathbb{Z}/m) \times (\mathbb{Z}/n)$ are finite sets of the same size. But such a proof would be harder to generalize to certain settings that we might later want to generalize Theorem 3.6.2 to.] □

We have already proven Theorem 2.14.4 using Theorem 2.16.1. Let us now reprove it using Theorem 3.6.2 instead (by a rather similar argument, but using residue classes instead of remainders):

Second proof of Theorem 2.14.4. For every positive integer g, we let U_g be the set of all residue classes $\alpha \in \mathbb{Z}/g$ that have an inverse. Then, U_n is exactly the set that was called U_n in Corollary 3.5.5. Hence, Corollary 3.5.5 **(b)** yields $\phi(n) = |U_n|$. Similarly, $\phi(m) = |U_m|$ and $\phi(mn) = |U_{mn}|$.

Theorem 3.6.2 says that the map

$$\begin{aligned} S_{m,n} : \mathbb{Z}/(mn) &\to (\mathbb{Z}/m) \times (\mathbb{Z}/n), \\ \alpha &\mapsto (\pi_{mn,m}(\alpha), \pi_{mn,n}(\alpha)) \end{aligned}$$

is well-defined and is a bijection. Consider this map $S_{m,n}$. This map $S_{m,n}$ is a bijection, i.e., is injective and surjective. Moreover, the definition of $S_{m,n}$ yields

$$S_{m,n}([1]_{mn}) = \left(\underbrace{\pi_{mn,m}([1]_{mn})}_{\substack{=[1]_m \\ \text{(by the definition of } \pi_{mn,m})}}, \underbrace{\pi_{mn,n}([1]_{mn})}_{\substack{=[1]_n \\ \text{(by the definition of } \pi_{mn,n})}} \right) = ([1]_m, [1]_n).$$

Let us first prove a trivial fact:

Claim 1: Let $\alpha, \beta \in \mathbb{Z}/(mn)$. Then, $\pi_{mn,m}(\alpha\beta) = \pi_{mn,m}(\alpha) \cdot \pi_{mn,m}(\beta)$.

[*Proof of Claim 1:* Write the residue classes α and β as $\alpha = [a]_{mn}$ and $\beta = [b]_{mn}$ for some integers a and b. (This can be done because of Proposition 3.4.5 **(a)**.) Now, $\underbrace{\alpha}_{=[a]_{mn}} \cdot \underbrace{\beta}_{=[b]_{mn}} = [a]_{mn} \cdot [b]_{mn} = [ab]_{mn}$ (by the definition of multiplication on

$\mathbb{Z}/(mn)$). Hence,

$$\pi_{mn,m}\left(\underbrace{\alpha\beta}_{=[ab]_{mn}}\right) = \pi_{mn,m}\left([ab]_{mn}\right) = [ab]_m \qquad \text{(by the definition of } \pi_{mn,m}\text{)}.$$

On the other hand, from $\alpha = [a]_{mn}$, we obtain $\pi_{mn,m}(\alpha) = \pi_{mn,m}([a]_{mn}) = [a]_m$ (by the definition of $\pi_{mn,m}$). Similarly, $\pi_{mn,m}(\beta) = [b]_m$. Hence,

$$\underbrace{\pi_{mn,m}(\alpha)}_{=[a]_m} \cdot \underbrace{\pi_{mn,m}(\beta)}_{=[b]_m} = [a]_m \cdot [b]_m = [ab]_m$$

(by the definition of multiplication on $\mathbb{Z}/m$). Comparing this with $\pi_{mn,m}(\alpha\beta) = [ab]_m$, we obtain $\pi_{mn,m}(\alpha) \cdot \pi_{mn,m}(\beta)$. This proves Claim 1.]

Also, from $U_m \subseteq \mathbb{Z}/m$ and $U_n \subseteq \mathbb{Z}/n$, we obtain $U_m \times U_n \subseteq (\mathbb{Z}/m) \times (\mathbb{Z}/n)$.

Now, we claim that

$$S_{m,n}(U_{mn}) \subseteq U_m \times U_n. \tag{131}$$

[*Proof of (131):* Let $\zeta \in S_{m,n}(U_{mn})$. Thus, $\zeta = S_{m,n}(\alpha)$ for some $\alpha \in U_{mn}$. Consider this α.

We have $\alpha \in U_{mn}$. In other words, α is a residue class in $\mathbb{Z}/(mn)$ that has an inverse (since U_{mn} was defined as the set of all residue classes in $\mathbb{Z}/(mn)$ that have an inverse). Thus, α is a residue class in $\mathbb{Z}/(mn)$ and has an inverse $\beta \in \mathbb{Z}/(mn)$. Consider this β. We know that β is an inverse of α; in other words, $\alpha\beta = [1]_{mn}$ (by the definition of "inverse").

Now, Claim 1 yields $\pi_{mn,m}(\alpha\beta) = \pi_{mn,m}(\alpha) \cdot \pi_{mn,m}(\beta)$, and thus

$$\pi_{mn,m}(\alpha) \cdot \pi_{mn,m}(\beta) = \pi_{mn,m}\left(\underbrace{\alpha\beta}_{=[1]_{mn}}\right) = \pi_{mn,m}([1]_{mn}) = [1]_m$$

(by the definition of $\pi_{mn,m}$). Thus, $\pi_{mn,m}(\beta)$ is an inverse of $\pi_{mn,m}(\alpha)$ in $\mathbb{Z}/m$ (by the definition of "inverse"). Hence, $\pi_{mn,m}(\alpha)$ is a residue class in $\mathbb{Z}/m$ that has an inverse (namely, $\pi_{mn,m}(\beta)$). In other words, $\pi_{mn,m}(\alpha) \in U_m$ (since U_m was defined as the set of all residue classes in $\mathbb{Z}/m$ that have an inverse). Similarly, $\pi_{mn,n}(\alpha) \in U_n$. Now,

$$\begin{aligned}\zeta = S_{m,n}(\alpha) &= \left(\underbrace{\pi_{mn,m}(\alpha)}_{\in U_m}, \underbrace{\pi_{mn,n}(\alpha)}_{\in U_n}\right) \qquad \text{(by the definition of } S_{m,n}\text{)}\\ &\in U_m \times U_n.\end{aligned}$$

Now, forget that we fixed ζ. We thus have proven that $\zeta \in U_m \times U_n$ for each $\zeta \in S_{m,n}(U_{mn})$. In other words, $S_{m,n}(U_{mn}) \subseteq U_m \times U_n$. This proves (131).]

Next, we claim that

$$U_m \times U_n \subseteq S_{m,n}(U_{mn}). \tag{132}$$

[*Proof of (132):* Let $\theta \in U_m \times U_n$. We shall prove that $\theta \in S_{m,n}(U_{mn})$.

We have $\theta \in U_m \times U_n \subseteq (\mathbb{Z}/m) \times (\mathbb{Z}/n) = S_{m,n}(\mathbb{Z}/(mn))$ (since the map $S_{m,n}$ is a bijection). In other words, there exists some $\alpha \in \mathbb{Z}/(mn)$ such that $\theta = S_{m,n}(\alpha)$. Consider this α. The definition of $S_{m,n}$ yields $S_{m,n}(\alpha) = (\pi_{mn,m}(\alpha), \pi_{mn,n}(\alpha))$. Hence,

$$(\pi_{mn,m}(\alpha), \pi_{mn,n}(\alpha)) = S_{m,n}(\alpha) = \theta \in U_m \times U_n.$$

In other words, $\pi_{mn,m}(\alpha) \in U_m$ and $\pi_{mn,n}(\alpha) \in U_n$.

We have $\pi_{mn,m}(\alpha) \in U_m$. In other words, $\pi_{mn,m}(\alpha)$ is a residue class in $\mathbb{Z}/m$ that has an inverse (since U_m was defined as the set of all residue classes in $\mathbb{Z}/m$ that have an inverse). In other words, $\pi_{mn,m}(\alpha)$ is a residue class in $\mathbb{Z}/m$ and has an inverse $\gamma \in \mathbb{Z}/m$. Likewise, $\pi_{mn,n}(\alpha)$ is a residue class in $\mathbb{Z}/n$ and has an inverse $\delta \in \mathbb{Z}/n$. Consider these γ and δ.

We have $(\gamma, \delta) \in (\mathbb{Z}/m) \times (\mathbb{Z}/n)$. Since the map $S_{m,n}$ is surjective, we can thus find a $\beta \in \mathbb{Z}/(mn)$ such that $S_{m,n}(\beta) = (\gamma, \delta)$. Consider this β. We have

$$(\gamma, \delta) = S_{m,n}(\beta) = (\pi_{mn,m}(\beta), \pi_{mn,n}(\beta)) \qquad \text{(by the definition of } S_{m,n}\text{)}.$$

In other words, $\gamma = \pi_{mn,m}(\beta)$ and $\delta = \pi_{mn,n}(\beta)$.

Now, we want to prove that β is an inverse of α (in $\mathbb{Z}/(mn)$).

Indeed,

$$\begin{aligned} \pi_{mn,m}(\alpha\beta) &= \pi_{mn,m}(\alpha) \cdot \underbrace{\pi_{mn,m}(\beta)}_{=\gamma} && \text{(by Claim 1)} \\ &= \pi_{mn,m}(\alpha) \cdot \gamma = [1]_m && \text{(since } \gamma \text{ is an inverse of } \pi_{mn,m}(\alpha)\text{)} \end{aligned}$$

and similarly $\pi_{mn,n}(\alpha\beta) = [1]_n$. Now, the definition of $S_{m,n}$ yields

$$S_{m,n}(\alpha\beta) = \left(\underbrace{\pi_{mn,m}(\alpha\beta)}_{=[1]_m}, \underbrace{\pi_{mn,n}(\alpha\beta)}_{=[1]_n} \right) = ([1]_m, [1]_n).$$

Comparing this with $S_{m,n}([1]_{mn}) = ([1]_m, [1]_n)$, we obtain $S_{m,n}(\alpha\beta) = S_{m,n}([1]_{mn})$. Since the map $S_{m,n}$ is injective, we thus conclude that $\alpha\beta = [1]_{mn}$. In other words, β is an inverse of α (by the definition of "inverse"). Hence, α is a residue class in $\mathbb{Z}/(mn)$ that has an inverse (namely, β). In other words, $\alpha \in U_{mn}$ (since U_{mn} was defined as the set of all residue classes in $\mathbb{Z}/(mn)$ that have an inverse). Now, $\theta = S_{m,n}\left(\underbrace{\alpha}_{\in U_{mn}} \right) \in S_{m,n}(U_{mn})$.

Now, forget that we fixed θ. We thus have shown that $\theta \in S_{m,n}(U_{mn})$ for each $\theta \in U_m \times U_n$. In other words, $U_m \times U_n \subseteq S_{m,n}(U_{mn})$. This proves (132).]

Combining (131) with (132), we obtain

$$S_{m,n}\left(U_{mn}\right) = U_m \times U_n. \tag{133}$$

It is well-known that any two finite sets A and B satisfy $|A \times B| = |A| \cdot |B|$ [119]. Applying this to $A = U_m$ and $B = U_n$, we obtain

$$|U_m \times U_n| = \underbrace{|U_m|}_{=\phi(m)} \cdot \underbrace{|U_n|}_{=\phi(n)} = \phi(m) \cdot \phi(n).$$

Note that U_{mn} is a subset of $\mathbb{Z}/(mn)$ (by its definition).

Recall that the map $S_{m,n}$ is injective. Hence, $|S_{m,n}(T)| = |T|$ for each subset T of $\mathbb{Z}/(mn)$ [120]. Applying this to $T = U_{mn}$, we obtain $|S_{m,n}(U_{mn})| = |U_{mn}|$. Thus,

$$|U_{mn}| = \left|\underbrace{S_{m,n}(U_{mn})}_{\substack{=U_m \times U_n \\ \text{(by (133))}}}\right| = |U_m \times U_n| = \phi(m) \cdot \phi(n).$$

Hence, $\phi(mn) = |U_{mn}| = \phi(m) \cdot \phi(n)$. So Theorem 2.14.4 is proven again. □

3.7. Substitutivity and chains of congruences revisited

Proposition 3.4.5 **(b)** can be stated as follows: Given an integer n, two integers a and b are congruent to each other modulo n if and only if their residue classes $[a]_n$ and $[b]_n$ are equal. This lets us see congruences modulo n in a new light (namely, as equalities). In particular, some previous results about congruences now become trivial. For example, we can obtain a very short proof of Proposition 2.4.5 using residue classes:

Proof of Proposition 2.4.5. We have the chain of congruences $a_1 \equiv a_2 \equiv \cdots \equiv a_k \mod n$. In other words,

$$a_i \equiv a_{i+1} \mod n \text{ holds for each } i \in \{1, 2, \ldots, k-1\}$$

(by Definition 2.4.4). Thus, for each $i \in \{1, 2, \ldots, k-1\}$, we have $a_i \equiv a_{i+1} \mod n$ and therefore $[a_i]_n = [a_{i+1}]_n$ (by Proposition 3.4.5 **(b)**, applied to $a = a_i$ and $b = a_{i+1}$). In other words, we have the chain of equalities $[a_1]_n = [a_2]_n = \cdots = [a_k]_n$. From this chain, we immediately obtain $[a_u]_n = [a_v]_n$ (by Proposition 2.4.3, applied to $[a_i]_n$ instead of a_i). Hence, Proposition 3.4.5 **(b)** (applied to $a = a_u$ and $b = a_v$) shows that $a_u \equiv a_v \mod n$. This proves Proposition 2.4.5. □

[119] This is the so-called *product rule* in its simplest form (see, e.g., [Loehr11, 1.5] or [LeLeMe18, §15.2.1]).

[120] This follows from the following general principle: If $f : X \to Y$ is an injective map between two finite sets X and Y, then $|f(T)| = |T|$ for each subset T of X.

We can also prove the Principle of substitutivity of congruences (which we informally stated in Section 2.5, and abbreviated as "PSC"):

Proof of the PSC (informal). We have $x \equiv x' \mod n$. Hence, Proposition 3.4.5 **(b)** (applied to $a = x$ and $b = x'$) yields $[x]_n = [x']_n$.

Now, let α be the expression A, except that each integer appearing in it has been replaced by its residue class modulo n. (For example, if A is the expression "$3 - 2 \cdot 7 + 6$", then α will be "$[3]_n - [2]_n \cdot [7]_n + [6]_n$".)

Likewise, let α' be the expression A', except that each integer appearing in it has been replaced by its residue class modulo n.

The expression A' differs from A only in that some appearance of x in it has been replaced by x'. Thus, the expression α' differs from α only in that some appearance of $[x]_n$ in it has been replaced by $[x']_n$. This replacement does not change the value of the expression, since $[x]_n = [x']_n$. Thus,

$$\left(\text{the value of } \alpha'\right) = \left(\text{the value of } \alpha\right).$$

We have defined α to be the expression A, except that each integer appearing in it has been replaced by its residue class modulo n. Thus, the value of α is the residue class of the value of A modulo n. (For example, if A is "$3 - 2 \cdot 7 + 6$", then α will be "$[3]_n - [2]_n \cdot [7]_n + [6]_n$", and thus

$$\begin{aligned}(\text{the value of } \alpha) &= [3]_n - \underbrace{[2]_n \cdot [7]_n}_{\substack{=[2\cdot 7]_n \\ \text{(by Definition 3.4.12 (c))}}} + [6]_n = \underbrace{[3]_n - [2\cdot 7]_n}_{\substack{=[3-2\cdot 7]_n \\ \text{(by Definition 3.4.12 (b))}}} + [6]_n \\ &= [3 - 2\cdot 7]_n + [6]_n = [3 - 2 \cdot 7 + 6]_n \qquad \text{(by Definition 3.4.12 (a))},\end{aligned}$$

which is precisely the residue class of the value of A modulo n.) In other words, we have

$$(\text{the value of } \alpha) = [\text{the value of } A]_n .$$

Similarly,

$$\left(\text{the value of } \alpha'\right) = \left[\text{the value of } A'\right]_n .$$

Hence,

$$\left[\text{the value of } A'\right]_n = \left(\text{the value of } \alpha'\right) = (\text{the value of } \alpha) = [\text{the value of } A]_n .$$

Hence, Proposition 3.4.5 **(b)** (applied to $a = (\text{the value of } A')$ and $b = (\text{the value of } A)$) yields $(\text{the value of } A') \equiv (\text{the value of } A) \mod n$. In other words, the value of the expression A' is congruent to the value of A modulo n. This proves the PSC. □

3.8. A couple of applications of elementary number theory

In the following short section, we shall see two practical applications of the above number-theoretical studies. The first is a method for encrypting information (the

RSA cryptosystem); the second is a trick by which computations with large integers can be split up into more manageable pieces (and distributed across several computers, or parallelized across several cores). We shall be brief, since applications are not a focus of these notes; for further details, see [GalQua17] and the MathOverflow answer `https://mathoverflow.net/a/10022/` . If you are interested in further applications, you may also want to consult the other answers to `https://mathoverflow.net/questions/10014` (for a list of uses of the Chinese Remainder Theorem – mostly, but not entirely, inside mathematics), as well as [UspHea39, Appendix to Chapter VII] (for applications of modular arithmetic to calendar computations), and the Wikipedia page on "Universal hashing" (for an application of residue classes modulo primes).

3.8.1. The RSA cryptosystem

Let us present the *RSA cryptosystem*. This is one of the first modern methods for encrypting data. (The name "RSA" stands for the initials of its three authors: Rivest, Shamir and Adleman.)

This cryptosystem addresses a fairly standard situation: Albert and Julia are communicating over a channel (e.g., the Internet), but the channel may have eavesdroppers. Julia wants to send a secret message to Albert over this channel – i.e., a message that eavesdroppers should not be able to understand[121]. But Albert and Julia have not exchanged any keys with each other in advance; they can start exchanging keys now, but the eavesdropper will know all the keys they are sending each other. How can Albert and Julia start secretly communicating without giving eavesdroppers all the information they want to give each other?

The RSA cryptosystem allows Albert and Julia to solve this problem as follows:

Setup:

- Julia tells Albert (openly, over the channel) that she wants to communicate and thus he should start creating keys for that purpose.

- Albert generates two distinct large and sufficiently random primes p and q. (This involves a lot of technicalities like actually finding large primes. See Keith Conrad's note *The Solovay-Strassen test* [Conrad*] for an algorithm for generating large primes[122], and [GalQua17] for a more comprehensive

[121] We assume that Julia is merely trying to keep the **content** of her message secret from the eavesdroppers; the eavesdroppers can still see **that she is sending something to Albert**. If Albert and Julia want to keep even this fact secret, they need a different branch of science – *steganography*, not cryptography. (For reasons that become obvious after a bit of thought, steganography is much less of an exact science than cryptography, and depends heavily on the real-life situation.)

[122] More precisely, the Solovay-Strassen test is an algorithm for checking (not with 100% surety, but with high probability, which suffices in practice) whether a given integer is prime. To make this into an algorithm for generating large primes, you can simply keep randomly picking large numbers until you hit one that is prime (which you can check using the Solovay–Strassen test).

treatment. A brief discussion is also found in Garrett's slides [Garret03]. As to what "large" means, we refer to the Wikipedia article on "key size".)

- Albert computes the positive integer $m = pq$. This number m (called the *modulus*) he makes public (i.e., sends to Julia over the channel). (Note that factoring a number into a product of primes is computationally a lot harder than multiplying a bunch of primes[123]. Thus, eavesdroppers will not (likely) be able to reconstruct the primes p and q from their (public) product m.)

- Albert computes the positive integer $\ell = (p-1)(q-1)$, but keeps this number private.

- Albert randomly picks an $e \in \{2, 3, \ldots, \ell - 1\}$ such that $e \perp \ell$. (Again, we omit the details of how to pick such an e randomly[124].) This number e will be called the *encryption key*, and Albert keeps it private.

- Albert computes a positive modular inverse d of e modulo ℓ (that is, a positive integer d such that $ed \equiv 1 \bmod \ell$). This number d exists by Theorem 2.10.8 **(b)**; it will be called the *decryption key*.

- Albert publishes the pair (e, m) as his *public key*.

- We assume that the message that Julia wants to send to Albert is an element of $\{0, 1, \ldots, m-1\}$. This assumption is perfectly reasonable, because this message originally exists in **some** digital form (e.g., as a bitstring), and it is easy to translate it from this form into an element of $\{0, 1, \ldots, m-1\}$ by some universally agreed rule (e.g., if a bitstring $(a_1, a_2, \ldots, a_k)$ is short enough, then the integer $a_1 2^{k-1} + a_2 2^{k-2} + \cdots + a_k 2^{k-k}$ will belong to $\{0, 1, \ldots, m-1\}$, and thus we can translate this bitstring into this latter integer; otherwise, we break it up into shorter chunks and send those as separate messages).

Encrypting a message:

If Julia wants to send a message $a \in \{0, 1, \ldots, m-1\}$ to Albert, then she does the following:

- She computes the residue class $\alpha := [a]_m \in \mathbb{Z}/m$.

This doesn't take **too** long, because the prime number theorem says that (very roughly speaking!) the probability for a k-digit number to be prime is $\approx 1/k$. (A precise statement of this result would require us to introduce notions that have nothing to do with algebra; it is commonly done in courses on *analytic number theory*. Needless to say, it is perfectly possible to profit from this result in practice without proving it.)

[123] See the Wikipedia page on "Integer factorization" for details on what this means. Note that this is not a proven theorem; any day, someone could come up with a quick algorithm for factoring integers into products of primes. You would hear about it in the news, though.

[124] The rough idea is "pick $e \in \{2, 3, \ldots, \ell - 1\}$ randomly; check (using the Euclidean algorithm) whether $e \perp \ell$; if not, then pick another e, and keep repeating this until you hit an e such that $e \perp \ell$". In theory, you could be unlucky and keep picking bad e's forever; but in reality, you will soon hit an e that satisfies $e \perp \ell$.

- She computes α^e in $\mathbb{Z}/m$. (This can be computed quickly using *binary exponentiation (also known as exponentiation by squaring)*: If $\beta \in \mathbb{Z}/m$, then all powers of β can be computed recursively via the formulas $\beta^{2k} = \left(\beta^k\right)^2$ and $\beta^{2k+1} = \left(\beta^k\right)^2 \beta$. Note that we are working with residue classes in $\mathbb{Z}/m$ here, not with integers, so that the powers β^k of β will not grow forever as k gets large; they stay in the finite set $\mathbb{Z}/m$.)

- She sends the residue class α^e (or, more precisely, its unique representative in the set $\{0, 1, \ldots, m-1\}$ [125]) to Albert.

Decrypting a message:

Albert receives the residue class $\beta = \alpha^e$ (or, more precisely, a representative thereof, which he can easily turn into the residue class), and recovers the original message a as follows:

- He sets $\gamma = \beta^d$. This γ is the same α that Julia computed, as we shall see below.

- He recovers the original message $a \in \{0, 1, \ldots, m-1\}$ as the unique representative of the residue class $\gamma = \alpha$ in $\{0, 1, \ldots, m-1\}$ (since Julia defined α as the residue class of a).

This way, Julia can send a message to Albert that no eavesdropper can read – unless said eavesdropper knows d, or possesses an algorithm hitherto unknown to the world, or has an incredibly fast computer, or Albert's randomly picked numbers were not random enough[126], or one of myriad other practical mistakes has been made. The proper implementation of the RSA cryptosystem, and the real-life

[125] This unique representative exists by Proposition 3.4.6 **(b)** (and can be computed by picking an arbitrary representative b first, and then taking its remainder $b\%m$).

[126] Computers cannot generate "truly" random numbers (whatever this would even mean!); thus, you have to get by with number generators which try their best at being unpredictable. Lots of creativity has gone into finding ways to come up with numbers that are "as random as possible". Software alone is, per se, deterministic and thus can at most come up with numbers that "look random" ("pseudorandom number generators"). Nondeterministic input must come from the outside world. This is why certain programs that generate keys ask you to move your mouse around the screen – they are, in fact, using your mouse movements as a source of randomness. Better randomness comes from hardware random number generators, such as Geiger counters or lava lamps.

What happens if your randomly picked prime numbers are not random enough? In the worst case, you never find two distinct primes to begin with. In a more realistic case, your distinct primes will all belong to a small and predictable set, and an eavesdropper can easily find them simply by checking all possibilities. In less obvious cases, different keys you generate for different purposes will occasionally have some primes in common, in which case an easy application of the Chinese Remainder Theorem will allow an eavesdropper to reconstruct them and decrypt your messages. See `https://factorable.net` for a study of RSA keys in the wild, which found a lot of common primes.

considerations needed to prevent "leakage" of sensitive data such as the decryption key d, are a subject in its own right, which we shall not discuss here.

Albert's method for recovering Julia's message relies on the following fact (which we shall prove a bit later):

> **Lemma 3.8.1.** Let p and q be two distinct primes. Let N be a positive integer such that $N \equiv 1 \operatorname{mod} (p-1)(q-1)$. Then:
> **(a)** Each $a \in \mathbb{Z}$ satisfies $a^N \equiv a \operatorname{mod} pq$.
> **(b)** Each $\alpha \in \mathbb{Z}/(pq)$ satisfies $\alpha^N = \alpha$.

Now, when Albert receives $\beta = \alpha^e$ from Julia, we have

$$\beta^d = (\alpha^e)^d = \alpha^{ed}.$$

But d was a modular inverse of e modulo ℓ; thus, $ed \equiv 1 \operatorname{mod} \ell$. Since $\ell = (p-1)(q-1)$, we thus have $ed \equiv 1 \operatorname{mod} (p-1)(q-1)$. Hence, Lemma 3.8.1 **(b)** (applied to $N = ed$) yields $\alpha^{ed} = \alpha$ (since $\alpha \in \mathbb{Z}/\underbrace{m}_{=pq} = \mathbb{Z}/(pq)$). Thus, $\beta^d = \alpha^{ed} = \alpha$. Thus, the residue class $\gamma = \beta^d$ that Albert computes is exactly Julia's α; hence, Albert correctly recovers the message.

Proof of Lemma 3.8.1 (sketched). **(a)** Let $a \in \mathbb{Z}$. We need to show that $a^N \equiv a \operatorname{mod} pq$. In other words, we need to show that $pq \mid a^N - a$. Since $p \perp q$, it suffices to prove that $p \mid a^N - a$ and $q \mid a^N - a$ (because then, Theorem 2.10.7 will yield $pq \mid a^N - a$).

Let us prove that $p \mid a^N - a$ first. Two cases are possible:

Case 1: We have $p \mid a$.

Case 2: We have $p \nmid a$.

Let us first consider Case 1. In this case, we have $p \mid a$. Thus, $a \equiv 0 \operatorname{mod} p$. Hence, $a^N \equiv 0^N = 0 \operatorname{mod} p$ (since N is positive). Thus, $\underbrace{a^N}_{\equiv 0 \operatorname{mod} p} - \underbrace{a}_{\equiv 0 \operatorname{mod} p} \equiv 0 - 0 = 0 \operatorname{mod} p$, so that $p \mid a^N - a$. Thus, we have proven $p \mid a^N - a$ in Case 1.

Now, let us consider Case 2. In this case, we have $p \nmid a$. But we have $p - 1 \mid (p-1)(q-1)$ and $N \equiv 1 \operatorname{mod} (p-1)(q-1)$; hence, Proposition 2.3.4 **(e)** (applied to $(p-1)(q-1)$, $p-1$, N and 1 instead of n, m, a and b) yields $N \equiv 1 \operatorname{mod} p - 1$. Hence, Exercise 2.15.2 (applied to $u = N$ and $v = 1$) yields $a^N \equiv a^1 = a \operatorname{mod} p$. In other words, $p \mid a^N - a$. Thus, we have proven $p \mid a^N - a$ in Case 2.

So we have proven $p \mid a^N - a$ in both Cases. Hence, $p \mid a^N - a$ always holds. Similarly, we can prove $q \mid a^N - a$. This completes our proof of Lemma 3.8.1 **(a)**.

(b) Let $\alpha \in \mathbb{Z}/(pq)$. Then, we can write α in the form $\alpha = [a]_{pq}$ for some $a \in \mathbb{Z}$ (by Proposition 3.4.5 **(a)**). Consider this a. From $\alpha = [a]_{pq}$, we obtain $\alpha^N = \left([a]_{pq}\right)^N = \left[a^N\right]_{pq} = [a]_{pq}$ (since Lemma 3.8.1 **(a)** yields $a^N \equiv a \operatorname{mod} pq$). Hence, $\alpha^N = [a]_{pq} = \alpha$. This proves Lemma 3.8.1 **(b)**. □

The RSA cryptosystem, as presented above, is more versatile than it may seem at first. Once Albert has generated his p, q, ℓ, m, d and e and sent (e,m) to Julia, Julia can send not just one but multiple messages to Albert using these keys. Albert can confidentially respond to these messages as well, by having Julia switch roles with him (i.e., Julia generates keys, Albert encrypts and Julia decrypts). Thus, a secure channel for communication can be established. Moreover, and less obviously, RSA can be used to digitally sign messages (i.e., convince the recipient that they really come from you – or at least from someone who possesses your private key); see, e.g., [Dummit16] or the Wikipedia.

3.8.2. Computing using the Chinese Remainder Theorem

Next, let us outline a simple yet unexpected application of the Chinese Remainder Theorem.

Assume that you have an expression a that is made of integers, addition, subtraction and multiplication. For example, say

$$a = 400 \cdot 405 \cdot 409 \cdot 413 - 401 \cdot 404 \cdot 408 \cdot 414. \tag{134}$$

Assume that computing a directly is too hard, because the intermediate results will be forbiddingly huge numbers, but you know (e.g., from some estimates) that the final result will be a fairly small number. Let's say (for simplicity) that you know that $0 \leq a < 500\,000$.

How can you use this information to compute a quickly?

One simple trick is to work with residue classes modulo 500 000 instead of working with integer. Thus, instead of computing the number a directly through the equality (134), we can instead compute its residue class

$$\begin{aligned}[a]_{500\,000} &= [400 \cdot 405 \cdot 409 \cdot 413 - 401 \cdot 404 \cdot 408 \cdot 414]_{500\,000} \\ &= [400]_{500\,000} \cdot [405]_{500\,000} \cdot [409]_{500\,000} \cdot [413]_{500\,000} \\ &\qquad - [401]_{500\,000} \cdot [404]_{500\,000} \cdot [408]_{500\,000} \cdot [414]_{500\,000}\end{aligned}$$

(which is an easier task, because we can always reduce our intermediate results using the fact that every integer a satisfies $[a]_{500\,000} = [a \,\%\, 500\,000]_{500\,000}$), and then recover a by observing that a must be the unique representative of its residue class $[a]_{500\,000}$ that belongs to $\{0, 1, \ldots, 499\,999\}$ (since $0 \leq a < 500\,000$). This is actually how integer arithmetic works in most low-level programming languages; for example, the most popular integer type of the C++ language is "`int`", which stands not for integers but rather for residue classes modulo 2^{64} (when working on a 64-bit system). (This is where integer overflow comes from.)

Computing $[a]_{500\,000}$ instead of computing a is already an improvement, but in practice, the "500 000" might actually be a significantly bigger number. Assume, for example, that instead of $0 \leq a < 500\,000$, you merely know that $0 \leq a < N$ for some fixed number N which is small enough that computing in $\mathbb{Z}/N$ is possible, but large enough that doing the **whole** computation of $[a]_N$ in $\mathbb{Z}/N$ is unviable. What can we do then?

One thing we can do is to compute the residue classes $[a]_n$ for several coprime "small" integers n. For example, we can compute $[a]_2$ (by performing the whole computation of a using residue classes modulo 2 instead of integers) and similarly $[a]_3$ and $[a]_5$ and $[a]_7$ etc.. (We are using prime numbers for n here, which has certain advantages, but is not strictly necessary; all we need is that the values of n we are using are coprime.[127])

The Chinese Remainder Theorem (in the form of Theorem 3.6.2) shows that if m and n are two coprime positive integers, then the map $S_{m,n}$ from Theorem 3.6.2 (sending each $[s]_{mn}$ to the pair $([s]_m, [s]_n)$) is a bijection. In our proof of Theorem 3.6.2 (when proving the surjectivity of $S_{m,n}$), we gave an explicit way of constructing preimages under this map $S_{m,n}$ (using Bezout's theorem, which has a fast algorithm underlying it – the Extended Euclidean algorithm). Thus, we have an explicit way of recovering the residue class $[s]_{mn}$ from the pair $([s]_m, [s]_n)$ whenever s is an (unknown) integer (and m and n are two coprime positive integers). We shall now refer to this way as the "patching procedure" (since it lets us "patch" two residue classes $[s]_m$ and $[s]_n$ together to a residue class $[s]_{mn}$).

Now, having computed a bunch of residue classes $[a]_2, [a]_3, [a]_5, [a]_7$ of our unknown integer a modulo coprime small integers, we can "patch" these classes together:

- From $[a]_2$ and $[a]_3$, we get $[a]_{2\cdot 3}$ by the "patching procedure".
- From $[a]_{2\cdot 3}$ and $[a]_5$, we get $[a]_{2\cdot 3\cdot 5}$ by the "patching procedure".
- From $[a]_{2\cdot 3\cdot 5}$ and $[a]_7$, we get $[a]_{2\cdot 3\cdot 5\cdot 7}$ by the "patching procedure".
- and so on.

We keep "patching" until the product $2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots$ becomes larger than our N (which will happen fairly soon, since this product grows super-exponentially with the number of "patching" steps). At that point, we have found the residue class $[a]_m$ of our unknown integer a modulo some integer $m > N$. Since $0 \leq a < N < m$, we can thus recover a itself (as the unique representative of the class $[a]_m$ that lies in the set $\{0, 1, \ldots, m-1\}$).

This technique is known as *Chinese Remaindering* (in its simplest form) and has been used a lot (for an example, see [Vogan07, pp. 1031–1033]). See [Knuth98, §4.3.2] for more details.

[127] Note that the computations of $[a]_n$ for different values of n are independent of each other, which comes handy if you have several processors.

3.9. Primitive roots: an introduction

3.9.1. Definition and examples

Let us finally discuss a kind of residue classes that come very useful when they exist: the *primitive roots* (modulo a positive integer n). We are not yet able to ascertain when they exist and when they don't (this will require some more abstract algebra); but we can already see some examples of them:

Convention 3.9.1. For the whole Subsection 3.9.1, we fix a positive integer n.

Definition 3.9.2. Let $\alpha \in \mathbb{Z}/n$ be a residue class.

(a) We say that α is *invertible* if α has an inverse.

(b) A *power of* α means a residue class of the form α^m for some $m \in \mathbb{N}$.

(c) Assume that α is invertible. Then, α is said to be a *primitive root modulo n* if every invertible residue class $\beta \in \mathbb{Z}/n$ is a power of α.

Example 3.9.3. Let $n = 9$. The invertible residue classes in $\mathbb{Z}/9$ are $[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9$.

Clearly, the residue class $[1]_9$ is not a primitive root modulo 9, since all its powers equal $[1]_9$.

The powers of $[2]_9$ are

$$\begin{aligned}
([2]_9)^0 &= [1]_9, \\
([2]_9)^1 &= [2]_9, \\
([2]_9)^2 &= [4]_9, \\
([2]_9)^3 &= [8]_9, \\
([2]_9)^4 &= [7]_9, \\
([2]_9)^5 &= [5]_9, \\
&\ldots.
\end{aligned}$$

[128] Thus, they cover all the six invertible residue classes $[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9$. Hence, $[2]_9$ is a primitive root modulo 9.

It is easy to see that $[5]_9$ also is a primitive root modulo 9, and these two primitive roots are the only ones.

Note that Corollary 3.5.5 **(b)** shows that there are exactly $\phi(n)$ invertible residue classes in $\mathbb{Z}/n$. It is easy to see that any power of an invertible residue class is again invertible.

Euler's theorem (Theorem 2.15.3) yields that if $\alpha \in \mathbb{Z}/n$ is an invertible residue class, then $\alpha^{\phi(n)} = [1]_n$ (because Corollary 3.5.5 **(a)** shows that α can be written in the form $\alpha = [a]_n$ for some integer a satisfying $a \perp n$). Thus, it is easy to see that an invertible residue class $\alpha \in \mathbb{Z}/n$ has at most $\phi(n)$ distinct powers. When an invertible residue class $\alpha \in \mathbb{Z}/n$ has **exactly** $\phi(n)$ distinct powers, it is a primitive root (since there are exactly $\phi(n)$ invertible residue classes in $\mathbb{Z}/n$).

Example 3.9.4. Let $n = 8$. The invertible residue classes in $\mathbb{Z}/8$ are $[1]_8, [3]_8, [5]_8, [7]_8$.

Again, $[1]_8$ is certainly not a primitive root.

The powers of $[3]_8$ are

$$\begin{aligned} ([3]_8)^0 &= [1]_8, \\ ([3]_8)^1 &= [3]_8, \\ ([3]_8)^2 &= [9]_8 = [1]_8, \\ &\ldots \end{aligned}$$

(so the even powers are $[1]_8$ and the odd powers are $[3]_8$). So $[3]_8$ is not a primitive root.

The same behavior prevents $[5]_8$ and $[7]_8$ from being primitive roots.

Thus, we see that there are no primitive roots modulo 8.

[128] Here is a fast way to compute these powers:

$$\begin{aligned} ([2]_9)^0 &= [1]_9, \\ ([2]_9)^1 &= [2]_9, \\ ([2]_9)^2 &= \Big[\underbrace{2^2}_{=4}\Big]_9 = [4]_9, \\ ([2]_9)^3 &= \Big[\underbrace{2^3}_{=8}\Big]_9 = [8]_9, \\ ([2]_9)^4 &= \Big[\underbrace{2^4}_{=16}\Big]_9 = [16]_9 = [7]_9 \qquad (\text{since } 16 \equiv 7 \bmod 9), \\ ([2]_9)^5 &= [2]_9 \cdot \underbrace{([2]_9)^4}_{=[7]_9} = [2]_9 \cdot [7]_9 = \Big[\underbrace{2 \cdot 7}_{=14}\Big]_9 = [14]_9 = [5]_9 \qquad (\text{since } 14 \equiv 5 \bmod 9), \\ &\ldots. \end{aligned}$$

Examples 3.9.4 and 3.9.3 suggest the following questions: For what n does a primitive root modulo n exist, and when it does, how many of them are there? The following theorem – a result proven in 1801 by Gauss – answers both of these questions:

Theorem 3.9.5. **(a)** A primitive root modulo n exists if and only if n is

- either 1,
- or a prime p,
- or a power p^k of an odd prime[129] p (with k being a positive integer),
- or 4,
- or $2p^k$ for an odd prime p (with k being a positive integer).

(b) If a primitive root modulo n exists, then there are precisely $\phi\left(\phi\left(n\right)\right)$ many of them.

This theorem would be fairly difficult to prove at this point, but will be doable with some abstract algebra (at least in the case $n = p$). See [GalQua17, Chapter 4] for a proof.

4. Complex numbers and Gaussian integers

4.1. Complex numbers

4.1.1. An informal introduction

We now leave (at least for the time being) the study of integers and proceed to consider a much larger "number system": the *complex numbers*.

Before we define these numbers rigorously, let me sketch the idea behind their construction. Please suspend your disbelief about the not-quite-kosher reasoning that will follow; we will return to rigorous mathematics in Definition 4.1.1 below.

We know that the number -1 (like any other negative number) has no square root in $\mathbb{R}$ (because the square of any real number is ≥ 0). But let us audaciously pretend that it does have a square root somewhere else. In other words, let us pretend that there exists a mythical "number" i such that $i^2 = -1$. Of course, such a "number" i will not be a real number, but let us assume (without real justification, for now) that it behaves like a usual number would (to some extent). In particular, let us assume that it can be added, subtracted and multiplied like the numbers that we know and love.

So we have extended the set $\mathbb{R}$ of real numbers by a new number i. Now, by applying addition, subtraction and multiplication to this new number (and our

[129] Recall: Odd primes are the same as primes $\neq 2$.

old numbers), we get a bunch of further new numbers – namely, all numbers of the form $a_0 + a_1 i + a_2 i^2 + \cdots + a_k i^k$, where $k \in \mathbb{N}$ and where $a_0, a_1, \ldots, a_k$ are real numbers. (These can be described as the polynomials in i with real coefficients.) However, some of these numbers will be equal; in fact, any number of this form can be reduced to a number of the form $a + bi$ (with $a, b \in \mathbb{R}$), because[130]

$$i^2 = -1, \qquad i^3 = i \underbrace{i^2}_{=-1} = -i, \qquad i^4 = i \underbrace{i^3}_{=-i} = - \underbrace{i^2}_{=-1} = -(-1) = 1,$$
$$i^5 = i \underbrace{i^4}_{=1} = i, \qquad \text{etc..}$$

For example, the number $3 + 5i + 9i^2 + 7i^3$ equals $3 + 5i + 9(-1) + 7(-i) = (3-9) + (5-7)i = -6 - 2i$.

So all our new numbers have the form $a + bi$ for two reals a and b. We call them "complex numbers". (As we have said, we will give a rigorous definition later.) Since we are assuming that the standard rules of arithmetic still hold for our new numbers, we can easily find formulas for computing the sum, the difference, the product and the quotient of two complex numbers written in the form $a + bi$: Namely, for any two complex numbers $a + bi$ and $c + di$ (with $a, b, c, d \in \mathbb{R}$), we have

$$(a+bi) + (c+di) = (a+c) + (b+d)i; \qquad (135)$$
$$(a+bi) - (c+di) = (a-c) + (b-d)i; \qquad (136)$$
$$(a+bi)(c+di) = ac + adi + bci + bd \underbrace{i^2}_{=-1} = ac + adi + bci - bd$$
$$= (ac - bd) + (ad + bc)i; \qquad (137)$$
$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac - adi + bci + bdi^2}{cc - cdi + dci - ddi^2} = \frac{ac - adi + bci + bd(-1)}{cc - cdi + dci - dd(-1)}$$
$$= \frac{(ac+bd) + (bc-ad)i}{c^2 + d^2} \qquad (\text{if } c, d \text{ are not both } 0). \qquad (138)$$

(Note that the latter formula is an analogue of the standard procedure for rationalizing denominators that involve square roots:

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{\left(a + b\sqrt{2}\right)\left(c - d\sqrt{2}\right)}{\left(c + d\sqrt{2}\right)\left(c - d\sqrt{2}\right)} = \frac{(ac - 2bd) + (bc - ad)\sqrt{2}}{c^2 - 2d^2},$$

except that the square root that we are trying to exorcise from the denominator is not $\sqrt{2}$ but $\sqrt{-1} = i$ now.)

However, not all features of real numbers carry over to complex numbers: Inequalities do not make sense for complex numbers. Indeed, if they would make sense, then we would get a contradiction as follows:

[130] Of course, we are assuming that the standard rules – such as associativity of multiplication – apply to our "new" numbers.

- If $i \geq 0$, then $i^2 \geq 0$, contradicting $i^2 = -1 < 0$.
- If $i < 0$, then $i^2 = (-i)^2 > 0$ (since $i < 0$ yields $-i > 0$), contradicting $i^2 = -1 < 0$.

Here, we have assumed two things about our relations: First, we have assumed that i is either ≥ 0 or < 0; and second, we have assumed that the square of a nonnegative complex number is nonnegative. Sure, we could avoid the contradiction by forfeiting one of these assumptions; but then, the $\geq$ and $<$ relations would not be worth their names any more.

So we appear to be able to extend the four operations $+, -, \cdot, /$ to our weird new numbers, but not the relations $<, \leq, >, \geq$ (at least not in any meaningful way). But how can we be sure that the four operations $+, -, \cdot, /$ don't already lead to some contradictions?

To answer this question, let us forget our daring postulation of the existence of i, and instead give a formal definition of complex numbers:

4.1.2. Rigorous definition of the complex numbers

Definition 4.1.1. (a) A *complex number* is defined as a pair (a, b) of two real numbers.

(b) We let $\mathbb{C}$ be the set of all complex numbers.

(c) For each real number r, we denote the complex number $(r, 0)$ by $r_{\mathbb{C}}$.

(d) We let i be the complex number $(0, 1)$. When the notation "i" is ambiguous, I will be calling it "$i_{\mathbb{C}}$" instead. (Some authors call it j or ι or $\sqrt{-1}$.)

(e) We define three binary operations $+$, $-$ and $\cdot$ on $\mathbb{C}$ by setting

$$\begin{aligned}(a,b)+(c,d)&=(a+c,b+d),\\(a,b)-(c,d)&=(a-c,b-d),\qquad\text{and}\\(a,b)\cdot(c,d)&=(ac-bd,ad+bc)\end{aligned}$$

for all $(a, b) \in \mathbb{C}$ and $(c, d) \in \mathbb{C}$.

(f) If α and β are two complex numbers, then we write $\alpha\beta$ for $\alpha \cdot \beta$.

(g) If α is a complex number, then the complex number $0_{\mathbb{C}} - \alpha$ shall be denoted by $-\alpha$.

For example, the definition of the operation $\cdot$ on $\mathbb{C}$ yields

$$\underbrace{i}_{=(0,1)}\underbrace{i}_{=(0,1)} = (0,1)\,(0,1) = \left(\underbrace{0\cdot 0 - 1\cdot 1}_{=-1}, \underbrace{0\cdot 1 + 1\cdot 0}_{=0}\right) = (-1,0) = (-1)_{\mathbb{C}}.$$

We will later[131] equate the complex number $(-1)_{\mathbb{C}}$ with the real number -1; thus, this equation will simplify to $ii = -1$. So i "behaves like a square root of -1". But

[131] in Convention 4.1.7

we also have $(-i)(-i) = (-1)_{\mathbb{C}}$, so $-i$ fits the same bill. Thus, we didn't have to postulate the existence of a mythical number i satisfying $i^2 = 1$; we simply found such a number in the set $\mathbb{C}$.

The definitions of the operations $+$, $-$ and $\cdot$ in Definition 4.1.1 are not chosen by accident. We shall later identify each complex number (a, b) with $a + bi$; then, these definitions will become exactly the equalities (135), (136) and (137) that we derived unrigorously.

We are leaving division of complex numbers undefined so far, because we will later get it more or less for free.

We shall follow the usual "PEMDAS" rules for the order of operations when interpreting expressions involving the operations $+$, $-$ and $\cdot$ on $\mathbb{C}$. Thus, for example, the expression "$\alpha + \beta \cdot \gamma$" shall mean $\alpha + (\beta \cdot \gamma)$ and not $(\alpha + \beta) \cdot \gamma$.

4.1.3. Rules for $+$, $-$ and $\cdot$

So we have defined complex numbers as pairs of real numbers, and we have defined three operations on them which we called $+$, $-$ and $\cdot$. But do these operations really deserve these names? Do they still behave as nicely as the corresponding operations on real numbers? Do they, in particular, satisfy the standard rules of arithmetic such as commutativity, associativity and distributivity? The next theorem shows that they indeed do:

Theorem 4.1.2. The following rules for addition, subtraction and multiplication in $\mathbb{C}$ hold:

(a) We have $\alpha + \beta = \beta + \alpha$ for any $\alpha, \beta \in \mathbb{C}$.

(b) We have $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{C}$.

(c) We have $\alpha + 0_{\mathbb{C}} = 0_{\mathbb{C}} + \alpha = \alpha$ for any $\alpha \in \mathbb{C}$.

(d) We have $\alpha \cdot 1_{\mathbb{C}} = 1_{\mathbb{C}} \cdot \alpha = \alpha$ for any $\alpha \in \mathbb{C}$.

(e) We have $\alpha \cdot \beta = \beta \cdot \alpha$ for any $\alpha, \beta \in \mathbb{C}$.

(f) We have $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{C}$.

(g) We have $\alpha \cdot (\beta + \gamma) = \alpha\beta + \alpha\gamma$ and $(\alpha + \beta) \cdot \gamma = \alpha\gamma + \beta\gamma$ for any $\alpha, \beta, \gamma \in \mathbb{C}$.

(h) We have $\alpha \cdot 0_{\mathbb{C}} = 0_{\mathbb{C}} \cdot \alpha = 0_{\mathbb{C}}$ for any $\alpha \in \mathbb{C}$.

(i) If $\alpha, \beta, \gamma \in \mathbb{C}$, then we have the equivalence $(\alpha - \beta = \gamma) \Longleftrightarrow (\alpha = \beta + \gamma)$.

(j) We have $-(\alpha + \beta) = (-\alpha) + (-\beta)$ for any $\alpha, \beta \in \mathbb{C}$.

(k) We have $-0_{\mathbb{C}} = 0_{\mathbb{C}}$.

(l) We have $-(-\alpha) = \alpha$ for any $\alpha \in \mathbb{C}$.

(m) We have $-(\alpha\beta) = (-\alpha)\beta = \alpha(-\beta)$ for any $\alpha, \beta \in \mathbb{C}$.

(n) We have $\alpha - \beta - \gamma = \alpha - (\beta + \gamma)$ for any $\alpha, \beta, \gamma \in \mathbb{C}$. (Here and in the following, "$\alpha - \beta - \gamma$" should be read as "$(\alpha - \beta) - \gamma$".)

Proof of Theorem 4.1.2. All parts of this theorem are straightforward. I will only prove the two parts **(f)** and **(i)**.

(f) Let $\alpha, \beta, \gamma \in \mathbb{C}$. Thus, α is a complex number; in other words, α is a pair of two real numbers (by the definition of complex numbers). Hence, we can write α in the form $\alpha = (a, a')$ for two real numbers a, a'. Similarly, we can write β and γ in the forms $\beta = (b, b')$ and $\gamma = (c, c')$ for four real numbers b, b', c, c'. Consider these six real numbers a, a', b, b', c, c'. Now, from the equalities $\alpha = (a, a')$, $\beta = (b, b')$ and $\gamma = (c, c')$, we obtain

$$\begin{aligned}
\alpha \cdot (\beta \cdot \gamma) &= (a, a') \cdot \underbrace{\left((b, b') \cdot (c, c')\right)}_{\substack{=(bc-b'c', bc'+b'c) \\ \text{(by the definition of} \\ \text{the operation } \cdot \text{ on } \mathbb{C})}} \\
&= (a, a') \cdot \left(bc - b'c', bc' + b'c\right) \\
&= \left(\underbrace{a\left(bc - b'c'\right) - a'\left(bc' + b'c\right)}_{=abc-ab'c'-a'bc'-a'b'c}, \underbrace{a\left(bc' + b'c\right) + a'\left(bc - b'c'\right)}_{=abc'+ab'c+a'bc-a'b'c'} \right) \\
&\qquad \text{(by the definition of the operation } \cdot \text{ on } \mathbb{C}) \\
&= \left(abc - ab'c' - a'bc' - a'b'c, abc' + ab'c + a'bc - a'b'c'\right)
\end{aligned}$$

and

$$\begin{aligned}
(\alpha \cdot \beta) \cdot \gamma &= \underbrace{\left((a, a') \cdot (b, b')\right)}_{\substack{=(ab-a'b', ab'+a'b) \\ \text{(by the definition of} \\ \text{the operation } \cdot \text{ on } \mathbb{C})}} \cdot (c, c') \\
&= \left(ab - a'b', ab' + a'b\right) \cdot (c, c') \\
&= \left(\underbrace{\left(ab - a'b'\right)c - \left(ab' + a'b\right)c'}_{=abc-ab'c'-a'bc'-a'b'c}, \underbrace{\left(ab - a'b'\right)c' + \left(ab' + a'b\right)c}_{=abc'+ab'c+a'bc-a'b'c'} \right) \\
&\qquad \text{(by the definition of the operation } \cdot \text{ on } \mathbb{C}) \\
&= \left(abc - ab'c' - a'bc' - a'b'c, abc' + ab'c + a'bc - a'b'c'\right).
\end{aligned}$$

Comparing these two equalities, we see that $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$. So Theorem 4.1.2 **(f)** is proven.

(i) Let $\alpha, \beta, \gamma \in \mathbb{C}$. Thus, α is a complex number; in other words, α is a pair of two real numbers (by the definition of complex numbers). Hence, we can write α in the form $\alpha = (a, a')$ for two real numbers a, a'. Similarly, we can write β and γ in the forms $\beta = (b, b')$ and $\gamma = (c, c')$ for four real numbers b, b', c, c'. Consider these six real numbers a, a', b, b', c, c'. Now, we have the following chain of logical equivalences:

$$\left(\underbrace{\alpha}_{=(a,a')} - \underbrace{\beta}_{=(b,b')} = \underbrace{\gamma}_{=(c,c')}\right)$$
$$\Longleftrightarrow \left(\underbrace{(a,a') - (b,b')}_{\substack{=(a-b,a'-b') \\ \text{(by the definition of the} \\ \text{operation } - \text{ on } \mathbb{C})}} = (c,c')\right)$$
$$\Longleftrightarrow \left((a-b,a'-b') = (c,c')\right) \Longleftrightarrow \left(\underbrace{a-b=c}_{\Longleftrightarrow (a=b+c)} \text{ and } \underbrace{a'-b'=c'}_{\Longleftrightarrow (a'=b'+c')}\right)$$
$$\Longleftrightarrow \left(a=b+c \text{ and } a'=b'+c'\right) \Longleftrightarrow \left((a,a') = (b+c,b'+c')\right)$$
$$\Longleftrightarrow \left(\underbrace{(a,a')}_{=\alpha} = \underbrace{(b,b')}_{=\beta} + \underbrace{(c,c')}_{=\gamma}\right) \qquad \left(\begin{array}{c}\text{since } (b+c,b'+c') = (b,b') + (c,c') \\ \text{(by the definition of the} \\ \text{operation } + \text{ on } \mathbb{C})\end{array}\right)$$
$$\Longleftrightarrow (\alpha = \beta + \gamma).$$

This proves Theorem 4.1.2 **(i)**.

All the other parts of Theorem 4.1.2 can be proven by direct computations, just as we proved Theorem 4.1.2 **(f)**. □

4.1.4. Finite sums and finite products

Recall the concept of a finite sum of real numbers (i.e., a sum of the form $\sum\limits_{i \in I} a_i$, where I is a finite set and a_i is a real number for each $i \in I$), and the analogous concept of a finite product of real numbers (i.e., a product of the form $\prod\limits_{i \in I} a_i$).

Definition 4.1.3. In the same vein, we define the concept of a finite sum of complex numbers (i.e., a sum of the form $\sum\limits_{i \in I} \alpha_i$, where I is a finite set and $\alpha_i \in \mathbb{C}$ for each $i \in I$), and the analogous concept of a finite product of complex numbers (i.e., a product of the form $\prod\limits_{i \in I} \alpha_i$, where I is a finite set and $\alpha_i \in \mathbb{C}$ for each $i \in I$).

These concepts are well-defined, by Proposition 4.1.4 **(a)** below.

We will use the usual shorthands for special kinds of finite sums and products. For example, if I is an interval $\{p, p+1, \ldots, q\}$ of integers (and if $\alpha_i \in \mathbb{C}$ for each $i \in I$), then the sum $\sum\limits_{i \in I} \alpha_i$ will also be denoted by $\sum\limits_{i=p}^{q} \alpha_i$ or $\alpha_p + \alpha_{p+1} + \cdots + \alpha_q$.

Likewise for products. Thus, for example, $\alpha_1 + \alpha_2 + \cdots + \alpha_k$ and $\alpha_1 \alpha_2 \cdots \alpha_k$ are well-defined whenever $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{C}$.

Proposition 4.1.4. **(a)** Definition 4.1.3 is well-defined.

(b) Finite sums ($\sum\limits_{i \in I} \alpha_i$) and finite products ($\prod\limits_{i \in I} \alpha_i$) of complex numbers $\alpha_i \in \mathbb{C}$ satisfy the same rules that finite sums and finite products of real numbers satisfy.

Proof of Proposition 4.1.4. **(a)** In [Grinbe15, Theorem 2.118 **(a)**], it is proven that finite sums of real numbers are well-defined. The same argument (but relying on Theorem 4.1.2 instead of the usual rules of commutativity, associativity etc. for real numbers) shows that finite sums of complex numbers $\alpha_i \in \mathbb{C}$ are well-defined. The analogous fact for products is proven in the same way, except that we need to replace 0 by 1 and properties of addition by corresponding properties of multiplication.

(b) The proofs of the properties of finite sums and finite products of elements of $\mathbb{C}$ are identical to the analogous proofs for real numbers, but (again) rely on Theorem 4.1.2 instead of the usual rules of commutativity, associativity etc. for real numbers. □

4.1.5. Embedding $\mathbb{R}$ into $\mathbb{C}$

Theorem 4.1.5. For any real numbers a and b, we have

$$(a+b)_{\mathbb{C}} = a_{\mathbb{C}} + b_{\mathbb{C}} \qquad \text{and} \tag{139}$$

$$(a-b)_{\mathbb{C}} = a_{\mathbb{C}} - b_{\mathbb{C}} \qquad \text{and} \tag{140}$$

$$(ab)_{\mathbb{C}} = a_{\mathbb{C}} b_{\mathbb{C}}. \tag{141}$$

Proof of Theorem 4.1.5. Let a and b be two real numbers. Then, the definitions of $a_{\mathbb{C}}$, $b_{\mathbb{C}}$ and $(ab)_{\mathbb{C}}$ yield $a_{\mathbb{C}} = (a,0)$ and $b_{\mathbb{C}} = (b,0)$ and $(ab)_{\mathbb{C}} = (ab,0)$. Now, (141) follows from

$$\begin{aligned} \underbrace{a_{\mathbb{C}}}_{=(a,0)} \underbrace{b_{\mathbb{C}}}_{=(b,0)} &= (a,0)\,(b,0) = (a,0)\cdot(b,0) = \left(\underbrace{ab - 0\cdot 0}_{=ab}, \underbrace{a\cdot 0 + 0\cdot b}_{=0} \right) \\ &\qquad \left(\text{by the definition of the operation } \cdot \text{ on } \mathbb{C}\right) \\ &= (ab,0) = (ab)_{\mathbb{C}}. \end{aligned}$$

Similar straightforward computations prove the equalities (139) and (140). Thus, Theorem 4.1.5 is proven. □

Remark 4.1.6. If $a_1, a_2, \ldots, a_k$ are k reals, then

$$(a_1)_{\mathbb{C}} + (a_2)_{\mathbb{C}} + \cdots + (a_k)_{\mathbb{C}} = (a_1 + a_2 + \cdots + a_k)_{\mathbb{C}} \qquad \text{and}$$
$$(a_1)_{\mathbb{C}} \cdot (a_2)_{\mathbb{C}} \cdot \cdots \cdot (a_k)_{\mathbb{C}} = (a_1 a_2 \cdots a_k)_{\mathbb{C}}.$$

Proof of Remark 4.1.6. This can be proven by a straightforward induction on k. □

Convention 4.1.7. From now on, for each real number r, we shall identify the real number r with the complex number $r_{\mathbb{C}} = (r, 0)$.

Identifying different things is always risky in mathematics; for example, we have seen above why it would be a bad idea to identify residue classes $[a]_n$ of integers modulo a positive integer n with the corresponding remainders $a\%n$ (even though there is a 1-to-1 correspondence between the former and the latter). Nevertheless, the identification made in Convention 4.1.7 is harmless, due to Theorem 4.1.5[132] and because the map

$$\mathbb{R} \to \mathbb{C}, \qquad r \mapsto r_{\mathbb{C}}$$

is injective (so we are not identifying two different real numbers with one and the same complex numbers).

So we have identified each real number with a complex number. Thus, the complex numbers can be seen as an extension of the real numbers: $\mathbb{R} \subseteq \mathbb{C}$. (Of course, this is not **literally** true, since formally speaking $r_{\mathbb{C}}$ is a pair while r is a single real number. Nevertheless, we will work as if this was true, and hope that the reader can insert "$_{\mathbb{C}}$" subscripts wherever necessary in order to make our computations literally true.)

When we defined complex numbers as pairs of real numbers in Definition 4.1.1, we were intending that the pair (a, b) would correspond to the complex number $a + bi$ in our previous informal construction of the complex numbers. Convention 4.1.7 makes this actually hold:

Proposition 4.1.8. For any $(a, b) \in \mathbb{C}$, we have $(a, b) = a + bi$.

Proof. Let $(a, b) \in \mathbb{C}$. Thus, a and b are real numbers. By Convention 4.1.7, we identify these real numbers a and b with the complex numbers $a_{\mathbb{C}} = (a, 0)$ and

[132] Why does Theorem 4.1.5 matter here? Well, let us assume for a moment that Theorem 4.1.5 was false; specifically, let us assume that there are two real numbers a and b such that $(ab)_{\mathbb{C}} \neq a_{\mathbb{C}} b_{\mathbb{C}}$. Consider these a and b. Now, Convention 4.1.7 lets us identify the real numbers a, b and ab with the complex numbers $a_{\mathbb{C}}$, $b_{\mathbb{C}}$ and $(ab)_{\mathbb{C}}$. Thus, $ab = (ab)_{\mathbb{C}} \neq \underbrace{a_{\mathbb{C}}}_{=a} \underbrace{b_{\mathbb{C}}}_{=b} = ab$, which is nonsense.

To make sure that Convention 4.1.7 cannot spawn such absurdities, we had to prove Theorem 4.1.5.

$b_{\mathbb{C}} = (b,0)$, respectively. Thus, $a = a_{\mathbb{C}} = (a,0)$ and $b = b_{\mathbb{C}} = (b,0)$. Hence,

$$\begin{aligned}
\underbrace{a}_{=(a,0)} + \underbrace{b}_{=(b,0)} \underbrace{i}_{=(0,1)} &= (a,0) + \underbrace{(b,0)\,(0,1)}_{\substack{=(b\cdot 0-0\cdot 1,b\cdot 1+0\cdot 0) \\ \text{(by the definition of} \\ \text{the operation } \cdot \text{ on } \mathbb{C})}} = (a,0) + \left(\underbrace{b\cdot 0 - 0\cdot 1}_{=0}, \underbrace{b\cdot 1 + 0\cdot 0}_{=b}\right) \\
&= (a,0) + (0,b) = \left(\underbrace{a+0}_{=a}, \underbrace{0+b}_{=b}\right) \\
&\qquad \text{(by the definition of the operation } + \text{ on } \mathbb{C}) \\
&= (a,b).
\end{aligned}$$

This proves Proposition 4.1.8. □

The next proposition shows that if we multiply a complex number (b,c) with a **real** number a (of course, understanding this real number a as the complex number $a_{\mathbb{C}} = (a,0)$), then the result will simply be (ab,ac) (that is, multiplying a complex number by a merely multiplies both of its entries by a):

Proposition 4.1.9. For any $a \in \mathbb{R}$ and $(b,c) \in \mathbb{C}$, we have $a\,(b,c) = (ab,ac)$. (Here, of course, "$a\,(b,c)$" means the product $a_{\mathbb{C}}\,(b,c)$.)

Proof. This is straightforward: Let $a \in \mathbb{R}$ and $(b,c) \in \mathbb{C}$. By Convention 4.1.7, we identify the real number a with the complex number $a_{\mathbb{C}} = (a,0)$. Hence, $a = a_{\mathbb{C}} = (a,0)$. Now,

$$\begin{aligned}
\underbrace{a}_{=(a,0)} (b,c) &= (a,0)\cdot(b,c) = \left(\underbrace{ab - 0c}_{=ab}, \underbrace{ac + 0b}_{=ac}\right) \\
&\qquad \text{(by the definition of the operation } \cdot \text{ on } \mathbb{C}) \\
&= (ab,ac).
\end{aligned}$$

This proves Proposition 4.1.9. □

4.1.6. Inverses and division of complex numbers

Definition 4.1.10. A complex number α is said to be *nonzero* if and only if it is distinct from the complex number $0_{\mathbb{C}} = (0,0)$.

In other words, a complex number α is nonzero if and only if it is distinct from 0 (since we are identifying the real number 0 with $0_{\mathbb{C}}$). Equivalently, a complex number $\alpha = (a,b)$ is nonzero if and only if $(a,b) \neq (0,0)$ as pairs (i.e., if and only if at least one of the real numbers a and b are nonzero).

We have so far been adding, subtracting and multiplying complex numbers, but never dividing them (except briefly, before we formally defined them). We could define division in the same way as we defined addition, subtraction and multiplication – namely, by an explicit formula for $\dfrac{(a,b)}{(c,d)}$ whenever (c,d) is nonzero[133]. However, it is more instructive to proceed differently, and construct the division from the multiplication that was already defined. After all, if our division is to deserve its name, it should undo multiplication; and this determines it uniquely. We will not define division right away; instead, we start out by defining an *inverse* of a complex number:

Definition 4.1.11. Let α be a complex number. An *inverse* of α means a complex number β such that $\alpha\beta = 1$. (Recall that $1 = 1_{\mathbb{C}}$ by Convention 4.1.7.)

The complex number 0 has no inverse (because $0\beta = 0 \neq 1$, no matter what β is). But it turns out that all the other complex numbers have one:

Theorem 4.1.12. Let α be a nonzero complex number. Then, α has a unique inverse.

Proof of Theorem 4.1.12. We shall separately prove the existence and the uniqueness of an inverse of α.

Proof of the existence of the inverse: Write the complex number α as $\alpha = (c,d)$ for two real numbers c and d. Then, $(c,d) = \alpha \neq 0$ (since α is nonzero). Thus, $(c,d) \neq 0 = (0,0)$. In other words, at least one of the two real numbers c and d is nonzero. Hence, at least one of the two real numbers c^2 and d^2 is positive[134]. The other among these two numbers must, of course, be nonnegative[135]. Hence, $c^2 + d^2$ is the sum of a positive real number with a nonnegative real number. Therefore, $c^2 + d^2$ itself is positive. Thus, $c^2 + d^2$ is a nonzero real number; hence, we can divide by $c^2 + d^2$. In particular, we can define a complex number β by

$$\beta = \left(\frac{c}{c^2+d^2}, \frac{-d}{c^2+d^2} \right).$$

Consider this β. Multiplying the equalities $\alpha = (c,d)$ and $\beta = \left(\dfrac{c}{c^2+d^2}, \dfrac{-d}{c^2+d^2} \right)$,

[133] This formula would be

$$\frac{(a,b)}{(c,d)} = \left(\frac{ac+bd}{c^2+d^2}, \frac{bc-ad}{c^2+d^2} \right).$$

[134] since the square of a nonzero real number is always positive

[135] since the square of a real number is always nonnegative

we find

$$\begin{aligned}\alpha\beta &= (c,d)\left(\frac{c}{c^2+d^2}, \frac{-d}{c^2+d^2}\right) \\ &= \left(\underbrace{c\cdot\frac{c}{c^2+d^2} - d\cdot\frac{-d}{c^2+d^2}}_{=1}, \underbrace{c\cdot\frac{-d}{c^2+d^2} + d\cdot\frac{c}{c^2+d^2}}_{=0}\right) \\ &\qquad (\text{by the definition of the operation } \cdot \text{ on } \mathbb{C}) \\ &= (1,0) = 1_{\mathbb{C}}.\end{aligned}$$

Thus, β is an inverse of α (by the definition of an inverse of α). Hence, α has **at least one** inverse (namely, β).

Proof of the uniqueness of the inverse: We must prove that α has at most one inverse. This is exactly the statement of Proposition 3.5.4, except that our α is an element of $\mathbb{C}$ rather than of $\mathbb{Z}/n$. But the same argument that we used to prove Proposition 3.5.4 can be applied to $\alpha \in \mathbb{C}$ instead of $\alpha \in \mathbb{Z}/n$ [136]. Hence, we obtain that α has **at most one** inverse.

We have now shown that α has at least one inverse, and we have shown that α has at most one inverse. Combining these two results, we conclude that α has a unique inverse. This proves Theorem 4.1.12. □

Definition 4.1.13. Let α be a nonzero complex number. Theorem 4.1.12 shows that α has a unique inverse. This inverse is called α^{-1}, and will be referred to as *the inverse* of α.

Definition 4.1.14. (a) Let α and β be two complex numbers such that $\beta \neq 0$. Then, the quotient $\frac{\alpha}{\beta}$ is defined to be the complex number $\alpha \cdot \beta^{-1}$. It is sometimes also denoted by α/β.

(b) The operation that transforms a pair (α, β) of two complex numbers (with β nonzero) into α/β is called *division*.

It is easy to see that division undoes multiplication:

Proposition 4.1.15. Let α, β, γ be three complex numbers with $\beta \neq 0$. Then, we have the equivalence

$$\left(\gamma = \frac{\alpha}{\beta}\right) \iff (\alpha = \beta\gamma).$$

Proof of Proposition 4.1.15. We have $\beta \neq 0$. Thus, β has a well-defined inverse β^{-1}. The definition of this inverse yields $\beta\beta^{-1} = 1$; now, Theorem 4.1.2 **(e)** yields $\beta^{-1}\beta =$

[136] Of course, we need to make some obvious modifications, such as replacing every appearance of "$[1]_n$" by "1", and replacing every reference to Theorem 3.4.23 with a reference to Theorem 4.1.2.

$\beta\beta^{-1} = 1$. Also, Theorem 4.1.2 **(e)** yields $\gamma\beta = \beta\gamma$ and $\beta^{-1}\alpha = \alpha\beta^{-1}$. The definition of $\frac{\alpha}{\beta}$ yields $\frac{\alpha}{\beta} = \alpha \cdot \beta^{-1} = \alpha\beta^{-1}$.

We have to prove the equivalence $\left(\gamma = \frac{\alpha}{\beta}\right) \iff (\alpha = \beta\gamma)$. Let us prove the "$\Longrightarrow$" and "$\Longleftarrow$" directions of this equivalence separately:

$\Longrightarrow$: Assume that $\gamma = \frac{\alpha}{\beta}$. We shall show that $\alpha = \beta\gamma$.

We have $\gamma = \frac{\alpha}{\beta} = \alpha\beta^{-1}$. Multiplying both sides of this equality with β, we obtain

$$\gamma\beta = \alpha \underbrace{\beta^{-1}\beta}_{=1} = \alpha \cdot 1 = \alpha.$$

Hence, $\alpha = \gamma\beta = \beta\gamma$. This proves the "$\Longrightarrow$" direction of the equivalence $\left(\gamma = \frac{\alpha}{\beta}\right) \iff (\alpha = \beta\gamma)$.

$\Longleftarrow$: Assume that $\alpha = \beta\gamma$. We shall show that $\gamma = \frac{\alpha}{\beta}$.

We have $\beta^{-1} \underbrace{\alpha}_{=\beta\gamma} = \underbrace{\beta^{-1}\beta}_{=1} \gamma = 1\gamma = \gamma 1 = \gamma$, so that $\gamma = \beta^{-1}\alpha = \alpha\beta^{-1} = \frac{\alpha}{\beta}$. This proves the "$\Longleftarrow$" direction of the equivalence $\left(\gamma = \frac{\alpha}{\beta}\right) \iff (\alpha = \beta\gamma)$.

Thus, the equivalence $\left(\gamma = \frac{\alpha}{\beta}\right) \iff (\alpha = \beta\gamma)$ holds (since we have proven both of its directions). That is, we have proven Proposition 4.1.15. □

Inverses also have the following properties:

Proposition 4.1.16. **(a)** Let $\alpha \in \mathbb{C}$ be a complex number that has an inverse (i.e., is nonzero). Then, its inverse α^{-1} has an inverse as well, and this inverse is $\left(\alpha^{-1}\right)^{-1} = \alpha$.

(b) Let $\alpha, \beta \in \mathbb{C}$ be two complex numbers that have inverses (i.e., are nonzero). Then, their product $\alpha\beta$ has an inverse as well, and this inverse is $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$.

Proof of Proposition 4.1.16. This proof is completely analogous to the solution to Exercise 3.5.1. (Just replace $\mathbb{Z}/n$ by $\mathbb{C}$.) □

Corollary 4.1.17. Let $\alpha, \beta \in \mathbb{C}$ be two nonzero complex numbers. Then, the complex number $\alpha\beta$ is nonzero as well.

Proof of Corollary 4.1.17 (sketched). The complex numbers α and β are nonzero, and thus have inverses (by Theorem 4.1.12). Hence, Proposition 4.1.16 **(b)** shows that their product $\alpha\beta$ has an inverse as well. Thus, $\alpha\beta \neq 0$ (since 0 has no inverse). This proves Corollary 4.1.17. □

4.1.7. Powers of complex numbers

Let us now define powers of complex numbers, where the exponent is a nonnegative integer.

Definition 4.1.18. Let $\alpha \in \mathbb{C}$ and $n \in \mathbb{N}$. We define a complex number α^n (called the *n-th power of* α) by setting $\alpha^n = \underbrace{\alpha\alpha\cdots\alpha}_{n \text{ times}}$.

Definition 4.1.18 yields

$$i^2 = ii = (-1)_{\mathbb{C}} = -1.$$

Moreover, Definition 4.1.18 yields

$$\alpha^0 = \underbrace{\alpha\alpha\cdots\alpha}_{0 \text{ times}} = (\text{empty product}) = 1 \qquad \text{and}$$
$$\alpha^1 = \underbrace{\alpha\alpha\cdots\alpha}_{1 \text{ times}} = \alpha$$

for each $\alpha \in \mathbb{C}$.

For another example, Definition 4.1.18 yields

$$(1+i)^2 = (1+i)(1+i) = 1+i+i+\underbrace{ii}_{=-1} = 1+i+i+(-1) = i+i = 2i$$

and

$$(1+i)^4 = \underbrace{(1+i)(1+i)}_{=2i}\underbrace{(1+i)(1+i)}_{=2i} = 2i\cdot 2i = 4\underbrace{ii}_{=-1} = 4(-1) = -4.$$

We shall use the PEMDAS convention for the order of operations when powers are involved. For example, the expression "$\alpha\beta^k + \gamma$" means $\left(\alpha\left(\beta^k\right)\right) + \gamma$ rather than (say) $(\alpha\beta)^k + \gamma$.

Recall that any nonzero complex number α has an inverse α^{-1} (by Definition 4.1.13). This allows us to extend our definition of α^n to **negative** n as well:

Definition 4.1.19. Let $\alpha \in \mathbb{C}$ be nonzero. For any negative $n \in \mathbb{Z}$, we define a complex number α^n (called the *n-th power of* α) by $\alpha^n = \left(\alpha^{-1}\right)^{-n}$. (This is well-defined, since $\left(\alpha^{-1}\right)^{-n}$ is already defined by Definition 4.1.18 (because n is negative and thus $-n \in \mathbb{N}$).)

The attentive reader will have noticed that Definition 4.1.19 redefines α^{-1} when α is nonzero (indeed, -1 is a negative integer, and thus can be substituted for n in Definition 4.1.19). Fortunately, this new definition of α^{-1} does not clash with the original definition (Definition 4.1.13), because if we set $n = -1$ in Definition 4.1.19, then we get $\alpha^{-1} = \left(\alpha^{-1}\right)^1 = \alpha^{-1}$ (where the "α^{-1}" on the left hand side is the new meaning defined in Definition 4.1.19, whereas the "α^{-1}" on the right hand side is the old meaning defined in Definition 4.1.13).

If $\alpha = 0$ and if $n \in \mathbb{Z}$ is negative, then we leave α^n undefined.

Powers of complex numbers satisfy the usual rules for exponents:

Proposition 4.1.20. **(a)** We have $\alpha^{n+1} = \alpha\alpha^n$ for all $\alpha \in \mathbb{C}$ and $n \in \mathbb{N}$.

(b) We have $\alpha^{n+m} = \alpha^n\alpha^m$ for all $\alpha \in \mathbb{C}$ and $n, m \in \mathbb{N}$.

(c) We have $(\alpha\beta)^n = \alpha^n\beta^n$ for all $\alpha, \beta \in \mathbb{C}$ and $n \in \mathbb{N}$.

(d) We have $(\alpha^n)^m = \alpha^{nm}$ for all $\alpha \in \mathbb{C}$ and $n, m \in \mathbb{N}$.

(e) We have $1^n = 1$ for all $n \in \mathbb{N}$.

(f) We have $\alpha^{n+1} = \alpha\alpha^n$ for all nonzero $\alpha \in \mathbb{C}$ and all $n \in \mathbb{Z}$.

(g) We have $\alpha^{-n} = \left(\alpha^{-1}\right)^n$ for all nonzero $\alpha \in \mathbb{C}$ and all $n \in \mathbb{Z}$.

(h) We have $\alpha^{n+m} = \alpha^n\alpha^m$ for all nonzero $\alpha \in \mathbb{C}$ and all $n, m \in \mathbb{Z}$.

(i) We have $(\alpha\beta)^n = \alpha^n\beta^n$ for all nonzero $\alpha, \beta \in \mathbb{C}$ and all $n \in \mathbb{Z}$.

(j) We have $1^n = 1$ for all $n \in \mathbb{Z}$.

(k) We have $(\alpha^n)^{-1} = \alpha^{-n}$ for all nonzero $\alpha \in \mathbb{C}$ and all $n \in \mathbb{Z}$. (In particular, α^n is nonzero, so that $(\alpha^n)^{-1}$ is well-defined.)

(l) We have $(\alpha^n)^m = \alpha^{nm}$ for all nonzero $\alpha \in \mathbb{C}$ and all $n, m \in \mathbb{Z}$. (In particular, α^n is nonzero, so that $(\alpha^n)^m$ is well-defined for all $m \in \mathbb{Z}$.)

(m) Complex numbers satisfy the binomial formula: That is, if $\alpha, \beta \in \mathbb{C}$, then

$$(\alpha + \beta)^n = \sum_{k=0}^{n} \binom{n}{k} \alpha^k \beta^{n-k} \qquad \text{for } n \in \mathbb{N}.$$

Proposition 4.1.20 can be proven in the same way as the corresponding claims are proven for real (or rational) numbers:

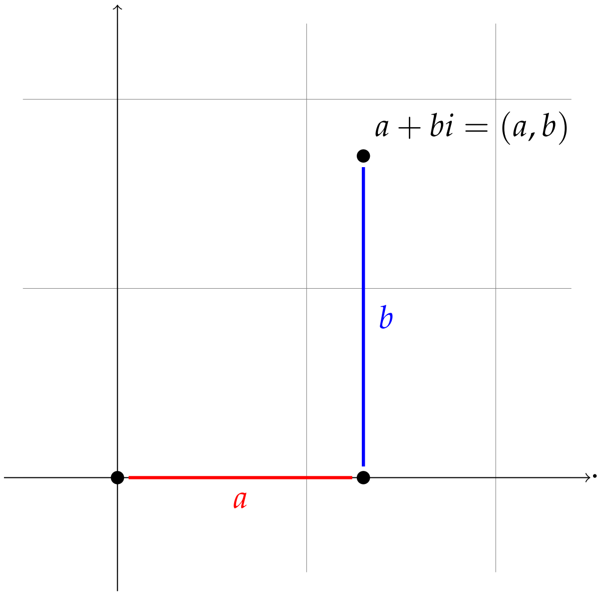
Exercise 4.1.1. Prove Proposition 4.1.20.

It may be tempting to try to extend Definition 4.1.19 further by defining fractional powers (such as $\alpha^{1/2}$). There is a way to do so, but such a definition would be of questionable use and somewhat fragile (in the sense that it would fail to satisfy the rules of exponents). For example, if you wanted to define $(-1)^{1/2}$, then the only reasonable choices would be i and $-i$ (since these are the only two complex numbers whose squares are -1); but with either option, the equality $(\alpha\beta)^{1/2} = \alpha^{1/2}\beta^{1/2}$ would fail if we took $\alpha = -1$ and $\beta = -1$. Thus, we prefer to leave powers of the form α^n for $n \notin \mathbb{Z}$ undefined.

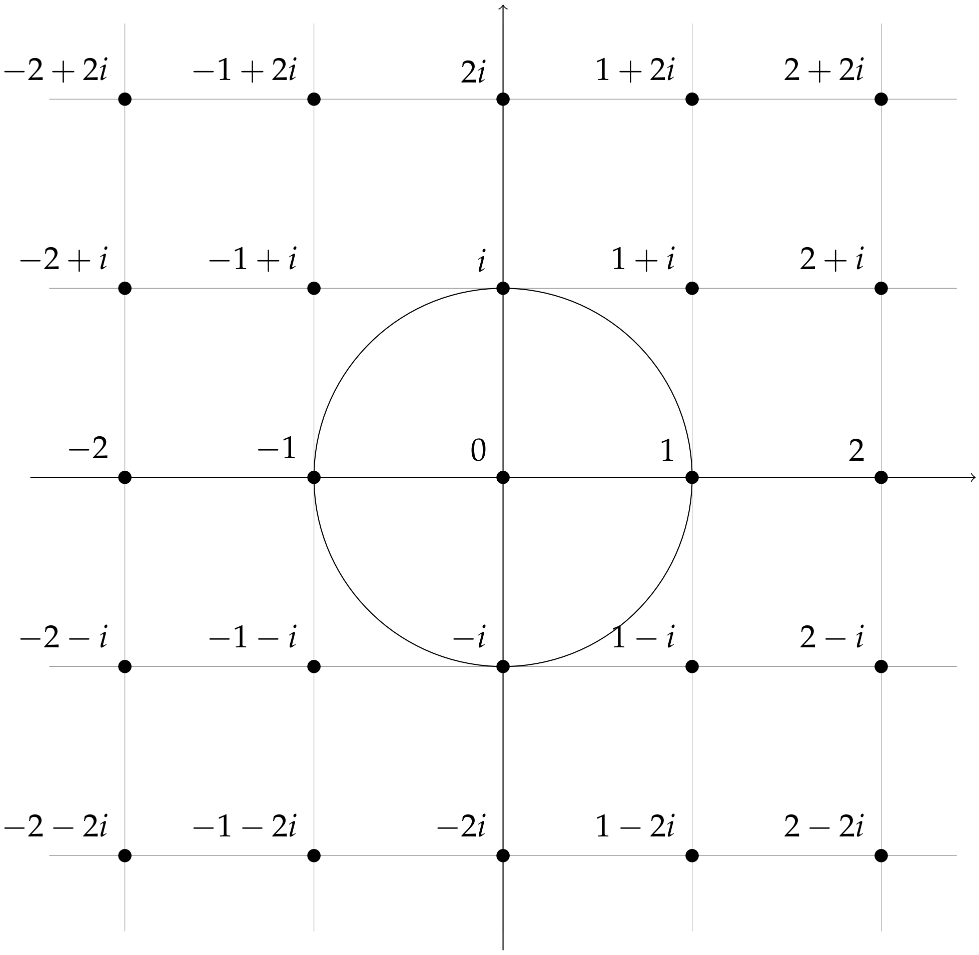
4.1.8. The Argand diagram

Let us next make a small detour to demonstrate a geometric representation of the complex numbers which, while not strictly necessary for what we intend to do with them, is conducive both to understanding them and to applying them.

Recall that a complex number was defined as a pair of real numbers. On the other hand, a point in the Cartesian plane is also defined as a pair of real numbers (its x-coordinate and its y-coordinate). Thus, it is natural to identify each complex number $(a, b) = a + bi$ with the point $(a, b) \in \mathbb{R}^2$ on the Cartesian plane (i.e., the point with x-coordinate a and y-coordinate b). This identification equates each complex number with a unique point in the Cartesian plane, and vice versa:



The picture below shows some of the points (specifically, all the 25 points $(a, b) \in \{-2, -1, 0, 1, 2\}^2$ whose both coordinates are integers between -2 and 2) labeled with the corresponding complex numbers:



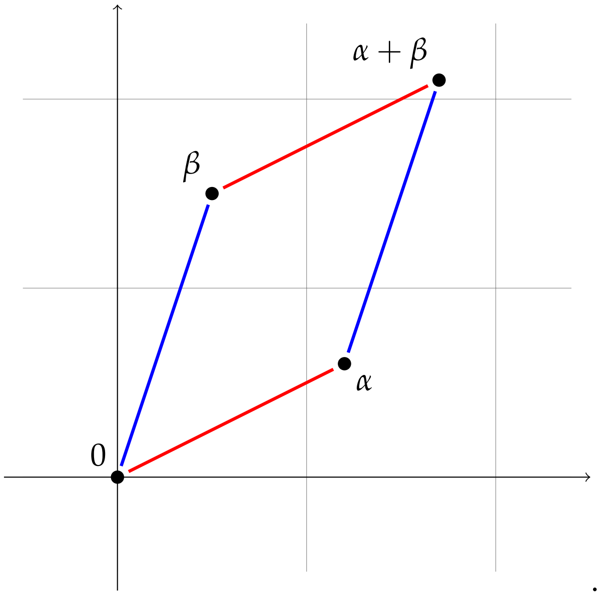
(142)

(as well as the unit circle, which passes through the four points labeled $1, i, -1, -i$; we will encounter these four points rather often in the following).

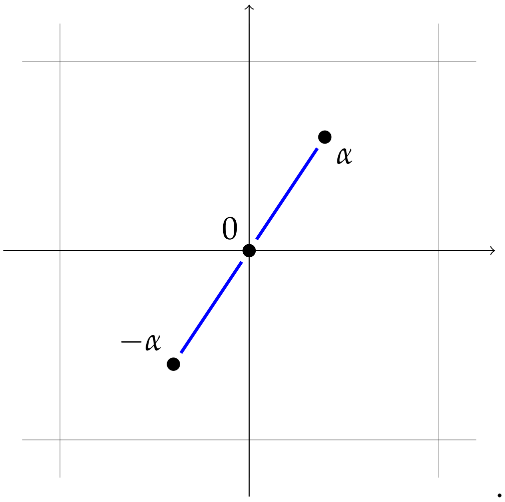
This identification of complex numbers with points is called the *Argand diagram* or the *complex plane* (although the latter word has yet another, different meaning). The complex number 0 corresponds to the origin $(0,0)$ of the plane.

In Definition 4.1.1 **(e)**, we have introduced three operations on complex numbers; what do they mean geometrically for the corresponding points? The two operations $+$ and $-$ are easiest to understand: They are exactly the usual operations of addition and subtraction for vectors. Thus, if α and β are two complex numbers, then the points labeled by the four complex numbers 0, α, $\alpha+\beta$ and β

form a parallelogram:



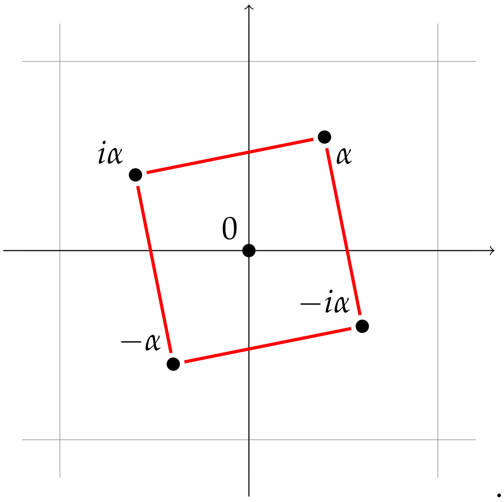
Likewise, the points labeled by the four complex numbers 0, α, β and $\beta - \alpha$ form a parallelogram. These parallelograms can be degenerate; in particular, the point $-\alpha$ is the reflection of the point α through the origin:[137]



Multiplication is less evident. The easiest case is multiplying by i: If α is a complex number, then the point $i\alpha$ is obtained from the point α by a 90° rotation (counterclockwise) around the origin. Thus, the four points α, $i\alpha$, $-\alpha$ and $-i\alpha$ are

[137] We no longer say "the point labeled by α", but simply equate α with that point now.

the vertices of a square centered at the origin:



.

More generally, if β is a complex number, then multiplication by β (that is, the map $\mathbb{C} \to \mathbb{C}$, $\alpha \mapsto \alpha\beta$) is a similitude transformation (so it preserves angles and ratios of lengths); more precisely it is a rotation around the origin composed with a homothety from the origin. Combined with the fact that it sends 1 to β, this uniquely determines it.

This is just the beginning of a rather helpful dictionary between elementary plane geometry and the algebra of complex numbers. See [AndAnd14] for many applications of this point of view, particularly to proving results in plane geometry.

4.1.9. Norms and conjugates

Let us now define some further features of complex numbers.

Definition 4.1.21. Let $\alpha = (a, b)$ be a complex number.

The *norm* of α is defined to be the real number $a^2 + b^2 \in \mathbb{R}$. This norm is called $\operatorname{N}(\alpha)$.

Proposition 4.1.22. Let α be a complex number.

(a) We have $\operatorname{N}(\alpha) \geq 0$.

(b) We have $\operatorname{N}(\alpha) = 0$ if and only if $\alpha = 0$.

(c) If $\alpha \neq 0$, then $\operatorname{N}(\alpha) > 0$.

Proof of Proposition 4.1.22. Write the complex number α in the form $\alpha = (a, b)$ for two real numbers a and b. Then, $\operatorname{N}(\alpha) = a^2 + b^2$ (by the definition of the norm). But a^2 and b^2 are squares of real numbers and thus ≥ 0 (since a square of a real number is always ≥ 0). Hence, $\operatorname{N}(\alpha) = \underbrace{a^2}_{\geq 0} + \underbrace{b^2}_{\geq 0} \geq 0$. This proves Proposition 4.1.22 **(a)**.

(b) We know that a^2 and b^2 are ≥ 0. In other words, a^2 and b^2 are two nonnegative reals. But the sum of two nonnegative reals is 0 if and only if both of these reals are 0. Applying this to the two nonnegative reals a^2 and b^2, we conclude that $a^2 + b^2 = 0$ if and only if both a^2 and b^2 are 0. In other words, we have the logical equivalence $\left(a^2 + b^2 = 0\right) \iff \left(\text{both } a^2 \text{ and } b^2 \text{ are } 0\right)$.

Now, we have the following chain of equivalences:

$$\begin{aligned} (\operatorname{N}(\alpha) = 0) &\iff \left(a^2 + b^2 = 0\right) \qquad \left(\text{since } \operatorname{N}(\alpha) = a^2 + b^2\right) \\ &\iff \left(\text{both } a^2 \text{ and } b^2 \text{ are } 0\right) \\ &\iff \left(a^2 = 0 \text{ and } b^2 = 0\right) \iff (a = 0 \text{ and } b = 0) \\ &\iff \left(\underbrace{(a,b)}_{=\alpha} = \underbrace{(0,0)}_{=0_{\mathbb{C}}}\right) \iff \left(\alpha = 0_{\mathbb{C}}\right) \iff (\alpha = 0). \end{aligned}$$

This proves Proposition 4.1.22 **(b)**.

(c) Assume that $\alpha \neq 0$. But Proposition 4.1.22 **(b)** shows that we have $\operatorname{N}(\alpha) = 0$ if and only if $\alpha = 0$. Hence, we have $\operatorname{N}(\alpha) \neq 0$ (since $\alpha \neq 0$). Combining this with $\operatorname{N}(\alpha) \geq 0$, we obtain $\operatorname{N}(\alpha) > 0$. This proves Proposition 4.1.22 **(c)**. □

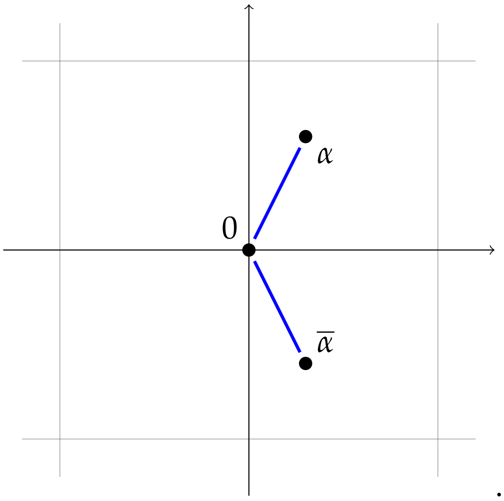
Proposition 4.1.23. Let $a \in \mathbb{R}$. Then, $\operatorname{N}(a_{\mathbb{C}}) = a^2$.

Proof of Proposition 4.1.23. We have $a_{\mathbb{C}} = (a, 0)$ (by the definition of $a_{\mathbb{C}}$). Hence, the definition of the norm yields $\operatorname{N}(a_{\mathbb{C}}) = a^2 + 0^2 = a^2$. This proves Proposition 4.1.23. □

Definition 4.1.24. Let $\alpha = (a, b) \in \mathbb{C}$.

The *conjugate* $\overline{\alpha}$ of α is defined to be the complex number $(a, -b) \in \mathbb{C}$.

From the viewpoint of the Argand diagram, the conjugate $\overline{\alpha}$ of a complex number α is simply the result of reflecting α (or, to be pedantic, the point labeled by α) across the x-axis:



.

Thus, the following is completely self-evident:

Proposition 4.1.25. Let $\alpha \in \mathbb{C}$.

(a) We have $\alpha = \overline{\alpha}$ if and only if $\alpha \in \mathbb{R}$. (Keep in mind that we are following Convention 4.1.7, so that the statement "$\alpha \in \mathbb{R}$" (for a complex number α) actually means "$\alpha = r_{\mathbb{C}}$ for some $r \in \mathbb{R}$".)

(b) We always have $\overline{\overline{\alpha}} = \alpha$.

Since we don't want to depend on geometric reasoning, let us nevertheless prove this fact algebraically:

Proof of Proposition 4.1.25. Write the complex number α in the form $\alpha = (a, b)$ for two real numbers a and b. Then, $\overline{\alpha} = (a, -b)$ (by the definition of $\overline{\alpha}$). Hence, the definition of $\overline{\overline{\alpha}}$ yields $\overline{\overline{\alpha}} = \left(a, \underbrace{-(-b)}_{=b}\right) = (a, b) = \alpha$. This proves Proposition 4.1.25 **(b)**.

(a) $\Longleftarrow$: Assume that $\alpha \in \mathbb{R}$. We must prove that $\alpha = \overline{\alpha}$.

We have $\alpha \in \mathbb{R}$. In other words, there exists an $r \in \mathbb{R}$ such that $\alpha = r_{\mathbb{C}}$. Consider this r. We have $\alpha = r_{\mathbb{C}} = (r, 0)$ (by the definition of $r_{\mathbb{C}}$). Hence, the definition of $\overline{\alpha}$ yields $\overline{\alpha} = \left(r, \underbrace{-0}_{=0}\right) = (r, 0) = \alpha$. Thus, $\alpha = \overline{\alpha}$. This proves the "$\Longleftarrow$" direction of Proposition 4.1.25 **(a)**.

$\Longrightarrow$: Assume that $\alpha = \overline{\alpha}$. We must prove that $\alpha \in \mathbb{R}$.

We have $\alpha = \overline{\alpha}$. Thus, $(a, b) = \alpha = \overline{\alpha} = (a, -b)$. In other words, $a = a$ and $b = -b$. From $b = -b$, we obtain $2b = 0$, thus $b = 0$. Hence, $\alpha = \left(a, \underbrace{b}_{=0}\right) = (a, 0) = a_{\mathbb{C}}$ (since $a_{\mathbb{C}}$ is defined to be $(a, 0)$). Thus, there exists an $r \in \mathbb{R}$ such that $\alpha = r_{\mathbb{C}}$ (namely, $r = a$). In other words, $\alpha \in \mathbb{R}$. This proves the "$\Longrightarrow$" direction of Proposition 4.1.25 **(a)**. □

Proposition 4.1.26. Let $\alpha \in \mathbb{C}$.

(a) We have $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$ (or, more formally: $(\mathrm{N}(\alpha))_{\mathbb{C}} = \alpha\overline{\alpha}$).

(b) We have $\mathrm{N}(\overline{\alpha}) = \mathrm{N}(\alpha)$.

Proof of Proposition 4.1.26. Write the complex number α in the form $\alpha = (a, b)$ for two real numbers a and b. Then, $\overline{\alpha} = (a, -b)$ (by the definition of $\overline{\alpha}$) and $\mathrm{N}(\alpha) = a^2 + b^2$ (by the definition of $\mathrm{N}(\alpha)$).

(a) Multiplying the equalities $\alpha = (a,b)$ and $\overline{\alpha} = (a,-b)$, we obtain

$$\alpha\overline{\alpha} = (a,b)\,(a,-b) = \left(\underbrace{aa - b\,(-b)}_{=a^2+b^2}, \underbrace{a\,(-b) + ba}_{=0}\right)$$

(by the definition of the operation $\cdot$ on $\mathbb{C}$)

$$= \left(\underbrace{a^2+b^2}_{=\operatorname{N}(\alpha)}, 0\right) = (\operatorname{N}(\alpha), 0) = (\operatorname{N}(\alpha))_{\mathbb{C}}$$

(since $\operatorname{N}(\alpha)_{\mathbb{C}}$ is defined to be $(\operatorname{N}(\alpha), 0)$). In other words, $(\operatorname{N}(\alpha))_{\mathbb{C}} = \alpha\overline{\alpha}$. According to Convention 4.1.7, we are equating the real number $\operatorname{N}(\alpha)$ with the complex number $(\operatorname{N}(\alpha))_{\mathbb{C}}$; hence, this equality rewrites as $\operatorname{N}(\alpha) = \alpha\overline{\alpha}$. This proves Proposition 4.1.26 **(a)**.

(b) Recall that $\overline{\alpha} = (a,-b)$. Thus, the definition of $\operatorname{N}(\overline{\alpha})$ yields $\operatorname{N}(\overline{\alpha}) = a^2 + \underbrace{(-b)^2}_{=b^2} = a^2 + b^2 = \operatorname{N}(\alpha)$. This proves Proposition 4.1.26 **(b)**. □

Proposition 4.1.27. Let α and β be two complex numbers. Then:

(a) We have $\overline{\alpha+\beta} = \overline{\alpha} + \overline{\beta}$.

(b) We have $\overline{\alpha-\beta} = \overline{\alpha} - \overline{\beta}$.

(c) We have $\overline{\alpha\cdot\beta} = \overline{\alpha}\cdot\overline{\beta}$.

(d) We have $\operatorname{N}(\alpha\beta) = \operatorname{N}(\alpha)\cdot\operatorname{N}(\beta)$.

(e) If $\beta \neq 0$, then $\operatorname{N}\left(\dfrac{\alpha}{\beta}\right) = \dfrac{\operatorname{N}(\alpha)}{\operatorname{N}(\beta)}$.

Proof of Proposition 4.1.27. Write the complex number α in the form $\alpha = (a,b)$ for two real numbers a and b. Then, $\overline{\alpha} = (a,-b)$ (by the definition of $\overline{\alpha}$) and $\operatorname{N}(\alpha) = a^2 + b^2$ (by the definition of $\operatorname{N}(\alpha)$).

Write the complex number β in the form $\beta = (c,d)$ for two real numbers c and d. Then, $\overline{\beta} = (c,-d)$ (by the definition of $\overline{\beta}$) and $\operatorname{N}(\beta) = c^2 + d^2$ (by the definition of $\operatorname{N}(\beta)$).

(c) Multiplying the equalities $\alpha = (a,b)$ and $\beta = (c,d)$, we obtain $\alpha\cdot\beta = (a,b)\,(c,d) = (ac-bd, ad+bc)$ (by the definition of the operation $\cdot$ on $\mathbb{C}$). Hence, Definition 4.1.24 yields $\overline{\alpha\cdot\beta} = (ac-bd, -(ad+bc))$.

On the other hand, multiplying the equalities $\overline{\alpha} = (a,-b)$ and $\overline{\beta} = (c,-d)$ yields

$$\overline{\alpha}\cdot\overline{\beta} = \left(\underbrace{ac - (-b)\,(-d)}_{=ac-bd}, \underbrace{a\,(-d) + b\,(-c)}_{=-(ad+bc)}\right) = (ac-bd, -(ad+bc))$$

(by the definition of the operation $\cdot$ on $\mathbb{C}$). Comparing this with $\overline{\alpha\cdot\beta} = (ac-bd, -(ad+bc))$, we obtain $\overline{\alpha\cdot\beta} = \overline{\alpha}\cdot\overline{\beta}$. This proves Proposition 4.1.27 **(c)**.

Parts **(a)** and **(b)** of Proposition 4.1.27 follow by similar (but easier) computations.

(d) Proposition 4.1.26 **(a)** yields $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$. Similarly, $\mathrm{N}(\beta) = \beta\overline{\beta}$ and $\mathrm{N}(\alpha\beta) = \alpha\beta\overline{\alpha\beta}$. Hence,

$$\mathrm{N}(\alpha\beta) = \alpha\beta \underbrace{\overline{\alpha\beta}}_{\substack{=\overline{\alpha\cdot\beta}=\overline{\alpha}\cdot\overline{\beta} \\ \text{(by Proposition 4.1.27 (c))}}} = \alpha\beta\overline{\alpha}\cdot\overline{\beta} = \underbrace{(\alpha\overline{\alpha})}_{=\mathrm{N}(\alpha)} \cdot \underbrace{(\beta\overline{\beta})}_{=\mathrm{N}(\beta)} = \mathrm{N}(\alpha)\cdot\mathrm{N}(\beta).$$

This proves Proposition 4.1.27 **(d)**.

(e) Assume that $\beta \neq 0$. Thus, the quotient $\dfrac{\alpha}{\beta} \in \mathbb{C}$ is defined (by Definition 4.1.14 **(a)**). Proposition 4.1.27 **(d)** (applied to $\dfrac{\alpha}{\beta}$ instead of α) yields $\mathrm{N}\left(\dfrac{\alpha}{\beta}\cdot\beta\right) = \mathrm{N}\left(\dfrac{\alpha}{\beta}\right)\cdot\mathrm{N}(\beta)$. In view of $\dfrac{\alpha}{\beta}\cdot\beta = \alpha$, this rewrites as

$$\mathrm{N}(\alpha) = \mathrm{N}\left(\frac{\alpha}{\beta}\right)\cdot\mathrm{N}(\beta). \tag{143}$$

Also, Proposition 4.1.22 **(c)** (applied to β instead of α) yields that we have $\mathrm{N}(\beta) > 0$ (since $\beta \neq 0$); thus, $\mathrm{N}(\beta) \neq 0$. Thus, we can divide both sides of the equality (143) by $\mathrm{N}(\beta)$. We thus obtain $\dfrac{\mathrm{N}(\alpha)}{\mathrm{N}(\beta)} = \mathrm{N}\left(\dfrac{\alpha}{\beta}\right)$. Proposition 4.1.27 **(e)** follows. □

The properties of the norm of a complex numbers let us see an old fact in new light: Remember the Brahmagupta–Fibonacci identity (1), which said that

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = (ad+bc)^2 + (ac-bd)^2$$

for $a, b, c, d \in \mathbb{R}$. This identity is equivalent to the identity

$$\mathrm{N}(\alpha)\cdot\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta)$$

for the complex numbers $\alpha = (a,b) = a+bi$ and $\beta = (c,d) = c+di$. Thus, the identity (1) is just Proposition 4.1.27 **(d)**, restated without the use of complex numbers. This answers the question of how you could have come up with this identity – at least if you know complex numbers. (Brahmagupta must have found it in a different way, since complex numbers were not known to him.)

Corollary 4.1.28. Let $\alpha \in \mathbb{C}$ and $k \in \mathbb{N}$. Then:

(a) We have $\overline{\alpha^k} = \overline{\alpha}^k$.

(b) We have $\mathrm{N}\left(\alpha^k\right) = (\mathrm{N}(\alpha))^k$.

Proof of Corollary 4.1.28. **(a)** This follows by induction on k, using Proposition 4.1.27 **(c)** and the fact that $\overline{1} = 1$.

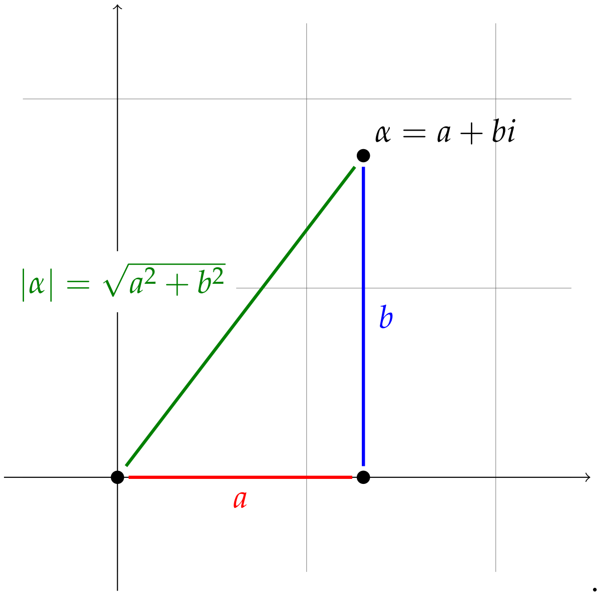
(b) This follows by induction on k, using Proposition 4.1.27 **(d)** and the fact that $\mathrm{N}(1) = 1$. □

Using the norm of a complex number, we can define a notion of absolute value of a complex number:

Definition 4.1.29. Let $\alpha = (a, b)$ be a complex number. The *absolute value* (or *modulus* or *length*) of α is defined to be $\sqrt{\mathrm{N}(\alpha)} = \sqrt{a^2 + b^2} \in \mathbb{R}$. (This is well-defined, because Proposition 4.1.22 **(a)** shows that $\mathrm{N}(\alpha) \geq 0$.)

The absolute value of α is denoted by $|\alpha|$. (This notation does not conflict with the classical notation $|a|$ for the absolute value of a real number a, because if a is a real number, then Proposition 4.1.23 yields $\mathrm{N}(a_{\mathbb{C}}) = a^2$ and therefore $\sqrt{\mathrm{N}(a_{\mathbb{C}})} = \sqrt{a^2} = |a|$, where "$|a|$" means the classical concept of absolute value of a.)

In the Argand diagram, the absolute value $|\alpha|$ of a complex number α is simply the distance of α from the origin. The reason for this is the Pythagorean theorem:



Good references for the basic properties of complex numbers are [LaNaSc16] and [Swanso18, §3.9–§3.12]. The book [AndAnd14] is a treasure trove of applications and exercises.

4.1.10. Re, Im and the 2 × 2-matrix representation

We define some more attributes of a complex number.

Definition 4.1.30. Let $\alpha = (a, b)$ be a complex number (so that a and b are real numbers and $\alpha = a + bi$).

Then, a is called the *real part* of α and denoted $\operatorname{Re} \alpha$ (or $\Re \alpha$).

Also, b is called the *imaginary part* of α and denoted $\operatorname{Im} \alpha$ (or $\Im \alpha$).

The following proposition assigns a real 2×2-matrix to each complex number:

Proposition 4.1.31. Let $\mathbb{R}^{2\times 2}$ be the set of all 2×2-matrices with real entries. Define a map $\mu : \mathbb{C} \to \mathbb{R}^{2\times 2}$ by setting

$$\mu(a,b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \text{for each } (a,b) \in \mathbb{C}.$$

(a) We have $\mu(\alpha+\beta) = \mu(\alpha) + \mu(\beta)$ for all $\alpha, \beta \in \mathbb{C}$.
(b) We have $\mu(\alpha-\beta) = \mu(\alpha) - \mu(\beta)$ for all $\alpha, \beta \in \mathbb{C}$.
(c) We have $\mu(\alpha\cdot\beta) = \mu(\alpha) \cdot \mu(\beta)$ for all $\alpha, \beta \in \mathbb{C}$.
(d) The map μ is injective.

Proof of Proposition 4.1.31. **(c)** This is a straightforward computation: Let $\alpha, \beta \in \mathbb{C}$. Write the complex number α in the form $\alpha = (a,b)$ for two real numbers a and b. Write the complex number β in the form $\beta = (c,d)$ for two real numbers c and d. Multiplying the equalities $\alpha = (a,b)$ and $\beta = (c,d)$, we obtain

$$\alpha \cdot \beta = (a,b) \cdot (c,d) = (ac - bd, ad + bc)$$

(by the definition of $\cdot$). Hence,

$$\mu(\alpha\cdot\beta) = \mu(ac-bd, ad+bc) = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \tag{144}$$

(by the definition of μ). On the other hand, from $\alpha = (a,b)$, we obtain

$$\mu(\alpha) = \mu(a,b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \text{(by the definition of } \mu\text{)},$$

and similarly we can find

$$\mu(\beta) = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}.$$

Multiplying these two equalities together, we find

$$\begin{aligned}\mu(\alpha)\cdot\mu(\beta) &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac + b(-d) & ad+bc \\ (-b)c + a(-d) & (-b)d + ac \end{pmatrix} \\ &= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}.\end{aligned}$$

Comparing this with (144), we find $\mu(\alpha\cdot\beta) = \mu(\alpha)\cdot\mu(\beta)$. This proves Proposition 4.1.31 **(c)**.

Similar (but much simpler) computations prove parts **(a)** and **(b)** of Proposition 4.1.31.

(d) We need to show that a complex number α can always be recovered from its image $\mu(\alpha)$.

But this is easy: If $\alpha = (a, b)$ is a complex number, then $\mu(\alpha) = \mu(a, b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ (by the definition of μ), and therefore we can recover a and b from $\mu(\alpha)$ (namely, a and b are the two entries of the first row of the matrix $\mu(\alpha)$). Hence, we can recover α from $\mu(\alpha)$. This shows that the map μ is injective; this proves Proposition 4.1.31 **(d)**. □

Proposition 4.1.31 really says that (instead of regarding complex numbers as pairs of real numbers) we can regard complex numbers as a specific kind of 2×2-matrices with real entries (by identifying each complex number α with the matrix $\mu(\alpha)$). This viewpoint has the advantage that multiplication of complex numbers becomes a particular case of matrix multiplication. (We could have saved ourselves the trouble of proving the associativity of multiplication for complex numbers if we had taken this viewpoint.)

4.1.11. The fundamental theorem of algebra

Finally, let me mention without proof the so-called *Fundamental Theorem of Algebra*:

Theorem 4.1.32. Let $p(x)$ be a polynomial of degree n with complex coefficients. Then, there exist complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ and β such that

$$p(x) = \beta(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

In other words, any polynomial with complex coefficients can be factored into linear factors. This is in contrast to real numbers, where polynomials can at best be factored into linear and quadratic factors. (For example, the polynomial $x^2 + 1$ cannot be factored further over the real numbers, but factors as $(x + i)(x - i)$ over the complex numbers.)

The Fundamental Theorem of Algebra is not actually a theorem of algebra. It relies heavily on the concepts of real and complex numbers. So it is actually a theorem of analysis. For a proof, see [LaNaSc16, Theorem 3.2.2].

4.2. Gaussian integers

Inside the set $\mathbb{C}$ of all complex numbers (an uncountable set) lies a much smaller (countable) set of numbers, which are much closer to integers than to real numbers. We shall study them partly for their own sake, partly as an instructive example of what we will later call a commutative ring, and partly in order to answer the questions from Section 1.4 (although complex numbers were never mentioned in that section).

We shall follow Keith Conrad's notes [ConradG] for most of this section (but at the end we will go a bit further in order to answer Question 1.4.2 **(b)**).

4.2.1. Definitions and basics

We shall now define the *Gaussian integers*: a middle ground between integers and complex numbers.

Definition 4.2.1. A *Gaussian integer* is a complex number (a, b) with $a, b \in \mathbb{Z}$.

For example, $3 + 5i = (3, 5)$ and $3 - 7i = (3, -7)$ are Gaussian integers. So are $0 = (0, 0)$, $1 = (1, 0)$ and $i = (0, 1)$. Every integer is a Gaussian integer[138]. But $\dfrac{1}{2} + 3i = \left(\dfrac{1}{2}, 3\right)$ and $\sqrt{2} + 4i = \left(\sqrt{2}, 4\right)$ are not Gaussian integers.

Recall that in the Argand diagram, complex numbers correspond to points in the Cartesian plane. The Gaussian integers thus correspond to a special type of points – the ones whose both coordinates are integers. These points are called *lattice points*, as they form the nodes of a square lattice covering the plane. In the picture (142), the 25 marked points are precisely the lattice points (i.e., the Gaussian integers) that happen to fall inside the region drawn.

Remark 4.2.2. In Definition 4.2.1, we have defined Gaussian integers using complex numbers. This can be viewed as somewhat of an overkill, as the notion of complex numbers depends on the notion of real numbers, which are mostly useless for Gaussian integers. Thus, one might ask for a different definition of Gaussian integers – one which relies only on integers and not on real numbers.

Such a definition is easy to make: Just replace every appearance of real numbers in Definition 4.1.1 by integers! Thus, define the Gaussian integers as pairs of two integers; let $\mathbb{C}_{\mathbb{Z}}$ be the set of these pairs; denote the Gaussian integer $(r, 0)$ by $r_{\mathbb{C}}$ whenever r is an integer; define the operations $+$, $-$ and $\cdot$ on the set $\mathbb{C}_{\mathbb{Z}}$ by the same formulas as in Definition 4.1.1 **(e)**; likewise, adapt the rest of Definition 4.1.1 to integers. Most of what we have done in Section 4.1 can be straightforwardly adapted to this notion of Gaussian integers (by making the obvious changes – i.e., mostly, replacing real numbers by integers); the main exceptions are the following:

- Not every nonzero Gaussian integer has an inverse (in the set of Gaussian integers). (In fact, as we will soon see, the only Gaussian integers that have inverses are $1, i, -1, -i$.) Thus, division and negative powers of Gaussian integers are usually not defined (without leaving the set of Gaussian integers).

- The absolute value $|\alpha|$ of a Gaussian integer α will usually not be an integer (since it is defined as a square root).

This alternative definition of Gaussian integers is equivalent to Definition 4.2.1; we are using the latter mainly because it is shorter.

[138] This relies on Convention 4.1.7, of course. If we avoid this convention, then we should instead say that for every integer r, the complex number $r_{\mathbb{C}} = (r, 0)$ is a Gaussian integer.

Likewise, we could have defined "Gaussian rationals" by adapting Definition 4.1.1 to rational (instead of real) numbers. Unlike the Gaussian integers, these "Gaussian rationals" do have inverses (when they are nonzero), and thus division and negative powers are well-defined for them.

Definition 4.2.3. We let $\mathbb{Z}[i]$ be the set of all Gaussian integers.

Elementary number theory concerns itself with integers (mostly). Our goal in this section is to replicate as much as we can of this theory in the setting of Gaussian integers, and then see how it can be applied back to answer some questions about the usual integers.

We will try to use Greek letters for Gaussian integers and Roman letters for integers.

Proposition 4.2.4. **(a)** If α and β are two Gaussian integers, then $\alpha+\beta$, $\alpha-\beta$ and $\alpha\cdot\beta$ are Gaussian integers.

(b) If α is a Gaussian integer, then $-\alpha$ is a Gaussian integer.

(c) Sums and products of finitely many Gaussian integers are Gaussian integers.

Proposition 4.2.4. **(a)** Let α and β be two Gaussian integers. Write the complex numbers α and β as $\alpha=(a,b)$ and $\beta=(c,d)$, respectively (with $a,b,c,d\in\mathbb{R}$). The definition of a Gaussian integer shows that $a,b\in\mathbb{Z}$ (since $(a,b)=\alpha$ is a Gaussian integer) and that $c,d\in\mathbb{Z}$ (since $(c,d)=\beta$ is a Gaussian integer). Now,

$$\underbrace{\alpha}_{=(a,b)}\cdot\underbrace{\beta}_{=(c,d)}=(a,b)\cdot(c,d)=(ac-bd,ad+bc)$$

(by the definition of the operation $\cdot$ on $\mathbb{C}$). Since $ac-bd,ad+bc\in\mathbb{Z}$ (because $a,b,c,d\in\mathbb{Z}$), this entails that $\alpha\cdot\beta$ is a Gaussian integer (by the definition of a Gaussian integer). Similarly (using the definitions of the operations $+$ and $-$ on $\mathbb{C}$), we can see that $\alpha+\beta$ and $\alpha-\beta$ are Gaussian integers. This proves Proposition 4.2.4 **(a)**.

(b) Let α be a Gaussian integer. Recall that 0 is a Gaussian integer. Thus, Proposition 4.2.4 **(a)** (applied to 0 and α instead of α and β) yields that $0+\alpha$, $0-\alpha$ and $0\cdot\alpha$ are Gaussian integers. Thus, in particular, $0-\alpha$ is a Gaussian integer. In other words, $-\alpha$ is a Gaussian integer (since $0-\alpha=-\alpha$). This proves Proposition 4.2.4 **(b)**.

(c) This follows by induction. (The induction base relies on the fact that 0 and 1 are Gaussian integers; the induction step uses Proposition 4.2.4 **(a)**.) □

Proposition 4.2.5. Let α be a Gaussian integer. Then, $\overline{\alpha}$ is a Gaussian integer.

Proof of Proposition 4.2.5. Write the complex number α as $\alpha=(a,b)$ with $a,b\in\mathbb{R}$. Then, $a,b\in\mathbb{Z}$ (since α is a Gaussian integer). Hence, $a,-b\in\mathbb{Z}$. Now, the definition of $\overline{\alpha}$ yields $\overline{\alpha}=(a,-b)$. Hence, $\overline{\alpha}$ is a Gaussian integer (since $a,-b\in\mathbb{Z}$). This proves Proposition 4.2.5. □

Proposition 4.2.6. Let $\alpha \in \mathbb{Z}[i]$. Then, $\operatorname{N}(\alpha) \in \mathbb{N}$.

Proof of Proposition 4.2.6. Write the complex number α as $\alpha = (a, b)$ with $a, b \in \mathbb{R}$. Then, $a, b \in \mathbb{Z}$ (since α is a Gaussian integer). In other words, a and b are integers. Hence, a^2 and b^2 are nonnegative integers (since the square of an integer is always a nonnegative integer). In other words, $a^2, b^2 \in \mathbb{N}$. Hence, $a^2 + b^2 \in \mathbb{N}$. But the definition of $\operatorname{N}(\alpha)$ yields $\operatorname{N}(\alpha) = a^2 + b^2 \in \mathbb{N}$. This proves Proposition 4.2.6. □

4.2.2. Units and unit-equivalence

Any nonzero Gaussian integer α has an inverse (by Theorem 4.1.12). But usually, this inverse is not a Gaussian integer, i.e., does not lie in $\mathbb{Z}[i]$. For example, $2^{-1} \notin \mathbb{Z}[i]$ and $(1+i)^{-1} = \dfrac{1-i}{2} \notin \mathbb{Z}[i]$. The Gaussian integers whose inverses do lie in $\mathbb{Z}[i]$ have a special name:

Definition 4.2.7. (a) A Gaussian integer $\alpha \in \mathbb{Z}[i]$ is said to be *invertible in* $\mathbb{Z}[i]$ if it has an inverse in $\mathbb{Z}[i]$.

A *unit* will mean a Gaussian integer that is invertible in $\mathbb{Z}[i]$.

(b) We define a relation $\sim$ on $\mathbb{Z}[i]$ by

$$(\alpha \sim \beta) \iff (\alpha = \gamma\beta \text{ for some unit } \gamma \in \mathbb{Z}[i]).$$

This relation will be called *unit-equivalence* (or *equality up to unit*). We say that two Gaussian integers α and β are *unit-equivalent* if $\alpha \sim \beta$.

For comparison, let us consider analogous concepts for integers instead of Gaussian integers. The units of $\mathbb{Z}$ (that is, the integers that are invertible in $\mathbb{Z}$) are 1 and -1. So if we defined a relation $\underset{\mathbb{Z}}{\sim}$ on $\mathbb{Z}$ in the same way as we defined the relation $\sim$ on $\mathbb{Z}[i]$ (but requiring $\gamma \in \mathbb{Z}$ instead of $\gamma \in \mathbb{Z}[i]$), then this relation would just be given by

$$\begin{aligned}\left(a \underset{\mathbb{Z}}{\sim} b\right) &\iff (a = cb \text{ for some } c \in \{1, -1\}) \\ &\iff (a = b \text{ or } a = -b) \iff (|a| = |b|). \qquad (145)\end{aligned}$$

So the relation $\underset{\mathbb{Z}}{\sim}$ is not very exciting: it is simply "equality up to sign".[139] But the relation $\sim$ on $\mathbb{Z}[i]$ cannot be described as simply as this: It is easy to find two Gaussian integers α and β such that $|\alpha| = |\beta|$ holds but $\alpha \sim \beta$ does not (for example, the Gaussian integers $\alpha = 16 + 63i$ and $\beta = 33 + 56i$ both have absolute value 65 but are not unit-equivalent).

[139] In other words, it is precisely the relation $\underset{\text{abs}}{\equiv}$, where $\text{abs} : \mathbb{Z} \to \mathbb{N}$ is the map sending each integer n to its absolute value $|n|$. (See Example 3.2.7 for how this relation $\underset{\text{abs}}{\equiv}$ is defined.)

Proposition 4.2.8. The relation $\sim$ on $\mathbb{Z}[i]$ is an equivalence relation.

Proof of Proposition 4.2.8. Observe the following:

- The relation $\sim$ is reflexive.

  [*Proof:* Let $\alpha \in \mathbb{Z}[i]$. Then, $\alpha = 1\alpha$. But 1 is invertible in $\mathbb{Z}[i]$ (since $1^{-1} = 1 \in \mathbb{Z}[i]$). In other words, 1 is a unit. Hence, $\alpha = \gamma\alpha$ for some unit $\gamma \in \mathbb{Z}[i]$ (namely, $\gamma = 1$). In other words, $\alpha \sim \alpha$ (by the definition of the relation $\sim$).

  Now, forget that we fixed α. We thus have shown that every $\alpha \in \mathbb{Z}[i]$ satisfies $\alpha \sim \alpha$. In other words, the relation $\sim$ is reflexive.]

- The relation $\sim$ is symmetric.

  [*Proof:* Let $\alpha, \beta \in \mathbb{Z}[i]$ be such that $\alpha \sim \beta$. We shall prove that $\beta \sim \alpha$.

  We have $\alpha \sim \beta$. In other words, $\alpha = \delta\beta$ for some unit $\delta \in \mathbb{Z}[i]$ (by the definition of the relation $\sim$). Consider this δ. Note that δ is a unit; in other words, δ is a Gaussian integer that has an inverse in $\mathbb{Z}[i]$. Thus, δ^{-1} is well-defined (since δ has an inverse), and $\delta^{-1} \in \mathbb{Z}[i]$ (since δ has an inverse in $\mathbb{Z}[i]$). Now, δ^{-1} is a Gaussian integer (since $\delta^{-1} \in \mathbb{Z}[i]$) and itself has an inverse in $\mathbb{Z}[i]$ (since its inverse is $\left(\delta^{-1}\right)^{-1} = \delta \in \mathbb{Z}[i]$). In other words, δ^{-1} is a unit. Furthermore, dividing both sides of the equality $\alpha = \delta\beta$ by δ, we find $\delta^{-1}\alpha = \beta$, so that $\beta = \delta^{-1}\alpha$. Thus, $\beta = \gamma\alpha$ for some unit $\gamma \in \mathbb{Z}[i]$ (namely, for $\gamma = \delta^{-1}$). In other words, $\beta \sim \alpha$ (by the definition of the relation $\sim$).

  Now, forget that we fixed α and β. We thus have shown that every $\alpha, \beta \in \mathbb{Z}[i]$ satisfying $\alpha \sim \beta$ satisfy $\beta \sim \alpha$. In other words, the relation $\sim$ is symmetric.]

- The relation $\sim$ is transitive.

  [*Proof:* Let $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ be such that $\alpha \sim \beta$ and $\beta \sim \gamma$. We shall prove that $\alpha \sim \gamma$.

  From $\alpha \sim \beta$, we conclude that $\alpha = \delta\beta$ for some unit $\delta \in \mathbb{Z}[i]$ (by the definition of the relation $\sim$). From $\beta \sim \gamma$, we conclude that $\beta = \varepsilon\gamma$ for some unit $\varepsilon \in \mathbb{Z}[i]$ (by the definition of the relation $\sim$). Consider these two units δ and ε. Both δ and ε are units, and thus have inverses in $\mathbb{Z}[i]$ (by the definition of "unit"). In other words, they have inverses, and these inverses δ^{-1} and ε^{-1} belong to $\mathbb{Z}[i]$. Now, Proposition 4.1.16 **(b)** (applied to δ and ε instead of α and β) yields that the product $\delta\varepsilon$ has an inverse as well, and this inverse is $(\delta\varepsilon)^{-1} = \delta^{-1}\varepsilon^{-1}$. Hence, $(\delta\varepsilon)^{-1} = \delta^{-1}\varepsilon^{-1} \in \mathbb{Z}[i]$ (since both δ^{-1} and ε^{-1} belong to $\mathbb{Z}[i]$). Thus, $\delta\varepsilon$ is a Gaussian integer (since δ and ε are Gaussian integers) that has an inverse in $\mathbb{Z}[i]$ (since $(\delta\varepsilon)^{-1} \in \mathbb{Z}[i]$). In other words, $\delta\varepsilon$ is a unit (by the definition of a "unit"). This unit $\delta\varepsilon$ satisfies $\alpha = (\delta\varepsilon)\gamma$ (since $\alpha = \delta \underbrace{\beta}_{=\varepsilon\gamma} = \delta\varepsilon\gamma = (\delta\varepsilon)\gamma$). Hence, $\alpha = \rho\gamma$ for some unit $\rho \in \mathbb{Z}[i]$ (namely, for $\rho = \delta\varepsilon$). In other words, $\alpha \sim \gamma$ (by the definition of the relation $\sim$).

  Now, forget that we fixed α, β, γ. We thus have shown that every $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ satisfying $\alpha \sim \beta$ and $\beta \sim \gamma$ satisfy $\alpha \sim \gamma$. In other words, the relation $\sim$ is transitive.]

We have now proven that the relation $\sim$ is reflexive, symmetric and transitive. In other words, $\sim$ is an equivalence relation (by the definition of "equivalence relation"). This proves Proposition 4.2.8. □

Proposition 4.2.9. Let α be a Gaussian integer.

(a) We have $\operatorname{N}(\alpha) = 0$ if and only if $\alpha = 0$.

(b) We have $\operatorname{N}(\alpha) = 1$ if and only if α is a unit.

(c) If α is nonzero and not a unit, then $\operatorname{N}(\alpha) > 1$.

Proof of Proposition 4.2.9. **(a)** This is a particular case of Proposition 4.1.22 **(b)**.

(b) $\Longrightarrow$: Assume that $\operatorname{N}(\alpha) = 1$. We must prove that α is a unit.

Proposition 4.1.26 **(a)** yields $\operatorname{N}(\alpha) = \alpha\overline{\alpha}$. Hence, $\alpha\overline{\alpha} = \operatorname{N}(\alpha) = 1$.

But Proposition 4.2.5 shows that $\overline{\alpha}$ is a Gaussian integer. In other words, $\overline{\alpha} \in \mathbb{Z}[i]$. This Gaussian integer $\overline{\alpha} \in \mathbb{Z}[i]$ is an inverse of α (since $\alpha\overline{\alpha} = 1$). Thus, α has an inverse in $\mathbb{Z}[i]$ (namely, $\overline{\alpha}$). In other words, α is a unit (by the definition of "unit"). This proves the "$\Longrightarrow$" direction of Proposition 4.2.9 **(b)**.

$\Longleftarrow$: Assume that α is a unit. We must prove that $\operatorname{N}(\alpha) = 1$.

We know that α is a unit. In other words, α is invertible in $\mathbb{Z}[i]$. In other words, α has an inverse $\alpha^{-1} \in \mathbb{Z}[i]$.

This inverse α^{-1} satisfies $\alpha\alpha^{-1} = 1 = 1_{\mathbb{C}} = (1,0)$, so that

$$\begin{aligned} \operatorname{N}\left(\alpha\alpha^{-1}\right) &= \operatorname{N}((1,0)) = 1^2 + 0^2 \qquad \text{(by the definition of } \operatorname{N}((1,0))\text{)} \\ &= 1. \end{aligned}$$

But Proposition 4.1.27 **(d)** (applied to $\beta = \alpha^{-1}$) yields $\operatorname{N}\left(\alpha\alpha^{-1}\right) = \operatorname{N}(\alpha) \cdot \operatorname{N}\left(\alpha^{-1}\right)$. Hence, $\operatorname{N}(\alpha) \cdot \operatorname{N}\left(\alpha^{-1}\right) = \operatorname{N}\left(\alpha\alpha^{-1}\right) = 1$. But Proposition 4.2.6 yields $\operatorname{N}(\alpha) \in \mathbb{N}$. The same argument (applied to α^{-1} instead of α) yields $\operatorname{N}\left(\alpha^{-1}\right) \in \mathbb{N}$ (since $\alpha^{-1} \in \mathbb{Z}[i]$). Hence, the equality $\operatorname{N}(\alpha) \cdot \operatorname{N}\left(\alpha^{-1}\right) = 1$ entails that $\operatorname{N}(\alpha) \mid 1$. Consequently, $\operatorname{N}(\alpha) = 1$ (since $\operatorname{N}(\alpha) \in \mathbb{N}$). This proves the "$\Longleftarrow$" direction of Proposition 4.2.9 **(b)**.

(c) Assume that α is nonzero and not a unit. Then, $\alpha \neq 0$ (since α is nonzero). Hence, Proposition 4.1.22 **(c)** yields $\operatorname{N}(\alpha) > 0$. But Proposition 4.2.6 yields $\operatorname{N}(\alpha) \in \mathbb{N}$. Combining this with $\operatorname{N}(\alpha) > 0$, we obtain $\operatorname{N}(\alpha) \geq 1$. But Proposition 4.2.9 **(b)** shows that we have $\operatorname{N}(\alpha) = 1$ if and only if α is a unit. Hence, we don't have $\operatorname{N}(\alpha) = 1$ (since α is not a unit). In other words, we have $\operatorname{N}(\alpha) \neq 1$. Combining this with $\operatorname{N}(\alpha) \geq 1$, we find $\operatorname{N}(\alpha) > 1$. This proves Proposition 4.2.9 **(c)**. □

Proposition 4.2.10. The units (in $\mathbb{Z}[i]$) are $1, -1, i, -i$.

Proof of Proposition 4.2.10. Each of the four Gaussian integers $1, -1, i, -i$ is a unit[140]. It remains to prove that there are no other units.

[140] *Proof.* We have $i(-i) = 1$. Hence, the Gaussian integer i has an inverse, namely $i^{-1} = -i$. Similarly, the Gaussian integer $-i$ has an inverse, namely $(-i)^{-1} = i$.

The Gaussian integer 1 is invertible in $\mathbb{Z}[i]$ (since its inverse is $1^{-1} = 1 \in \mathbb{Z}[i]$), and thus is a unit.

The Gaussian integer -1 is invertible in $\mathbb{Z}[i]$ (since its inverse is $(-1)^{-1} = -1 \in \mathbb{Z}[i]$), and thus is a unit.

The Gaussian integer i is invertible in $\mathbb{Z}[i]$ (since its inverse is $i^{-1} = -i \in \mathbb{Z}[i]$), and thus is a unit.

So let $\alpha \in \mathbb{Z}[i]$ be a unit. We shall prove that α is either 1 or -1 or i or $-i$.

Proposition 4.2.9 **(b)** shows that we have $\operatorname{N}(\alpha) = 1$ if and only if α is a unit. Hence, we have $\operatorname{N}(\alpha) = 1$ (since α is a unit).

Our goal is to prove that α is either 1 or -1 or i or $-i$. If you don't insist on full rigor, then you can easily read this off from the Argand diagram: We have $|\alpha| = \sqrt{\operatorname{N}(\alpha)} = 1$ (since $\operatorname{N}(\alpha) = 1$). Now, the point α is a Gaussian integer, i.e., a lattice point, and lies on the unit circle (since its distance to the origin is $|\alpha| = 1$). But a look at the picture (142) reveals that the only lattice points lying on the unit circle are $1, -1, i, -i$. Hence, if you believe this kind of reasoning, you have shown that α is either 1 or -1 or i or $-i$.

Here is a rigorous argument for this:

Let us write the complex number α as $\alpha = (a, b)$. Then, $a, b \in \mathbb{Z}$ (since $\alpha \in \mathbb{Z}[i]$). Furthermore, the definition of $\operatorname{N}(\alpha)$ yields $\operatorname{N}(\alpha) = a^2 + b^2$, so that $a^2 + b^2 = \operatorname{N}(\alpha) = 1$. If both integers a and b were nonzero, then both their squares a^2 and b^2 would be ≥ 1 (because the square of any nonzero integer is ≥ 1), and thus the sum of these squares would be $\underbrace{a^2}_{\geq 1} + \underbrace{b^2}_{\geq 1} \geq 1 + 1 > 1$; but this would contradict $a^2 + b^2 = 1$. Hence, the two integers a and b cannot both be nonzero. In other words, at least one of them is 0. In other words, we have $a = 0$ or $b = 0$. Thus, we are in one of the following two cases:

Case 1: We have $a = 0$.

Case 2: We have $b = 0$.

(These two cases could theoretically overlap, though it is easy to see that they don't.)

Let us first consider Case 1. In this case, we have $a = 0$. Hence, $a^2 + b^2 = 0^2 + b^2 = b^2$, so that $b^2 = a^2 + b^2 = 1$. Hence, b is either 1 or -1. Thus, the complex number $(0, b)$ is either $(0, 1)$ or $(0, -1)$. In other words, the complex number α is either i or $-i$ (since $\alpha = \left(\underbrace{a}_{=0}, b\right) = (0, b)$ and $i = (0, 1)$ and $-\underbrace{i}_{=(0,1)} = -(0, 1) = (0, -1)$). Thus, α is either 1 or -1 or i or $-i$. So we have shown in Case 1 that α is either 1 or -1 or i or $-i$.

Let us next consider Case 2. In this case, we have $b = 0$. Hence, $a^2 + b^2 = a^2 + 0^2 = a^2$, so that $a^2 = a^2 + b^2 = 1$. Hence, a is either 1 or -1. Thus, the complex number $(a, 0)$ is either $(1, 0)$ or $(-1, 0)$. In other words, the complex number α is either 1 or -1 (since $\alpha = \left(a, \underbrace{b}_{=0}\right) = (a, 0)$ and $1 = (1, 0)$ and $-1 = (-1, 0)$). Thus, α is either 1 or -1 or i or $-i$. So we have shown in Case 2 that α is either 1 or -1 or i or $-i$.

The Gaussian integer $-i$ is invertible in $\mathbb{Z}[i]$ (since its inverse is $(-i)^{-1} = i \in \mathbb{Z}[i]$), and thus is a unit.

Thus, each of the four Gaussian integers $1, -1, i, -i$ is a unit.

We have now proven in both Cases 1 and 2 that α is either 1 or -1 or i or $-i$. Hence, this always holds.

Now, forget that we fixed α. We thus have shown that if $\alpha \in \mathbb{Z}[i]$ is a unit, then α is either 1 or -1 or i or $-i$. Thus, $1, -1, i, -i$ are the only possible units. Since we already know that $1, -1, i, -i$ are units, we thus conclude that the units are $1, -1, i, -i$. This proves Proposition 4.2.10. □

As a consequence of Proposition 4.2.10, if we are given two Gaussian integers α and β, we can easily check whether $\alpha \sim \beta$ holds:

Proposition 4.2.11. Let α and β be two Gaussian integers. Then, we have $\alpha \sim \beta$ if and only if

$$(\alpha = \beta \text{ or } \alpha = -\beta \text{ or } \alpha = i\beta \text{ or } \alpha = -i\beta).$$

Proof of Proposition 4.2.11. Proposition 4.2.10 shows that the units are $1, -1, i, -i$. In other words,

$$\{\text{the units}\} = \{1, -1, i, -i\}.$$

Now, we have the following chain of logical equivalences:

$$\begin{aligned}
(\alpha \sim \beta) &\iff (\alpha = \gamma\beta \text{ for some unit } \gamma \in \mathbb{Z}[i]) \\
&\qquad \text{(by the definition of the relation } \sim\text{)} \\
&\iff \left(\alpha = \gamma\beta \text{ for some } \gamma \in \underbrace{\{\text{the units}\}}_{=\{1,-1,i,-i\}}\right) \\
&\iff (\alpha = \gamma\beta \text{ for some } \gamma \in \{1, -1, i, -i\}) \\
&\iff \left(\alpha = \underbrace{1\beta}_{=\beta} \text{ or } \alpha = \underbrace{-1\beta}_{=-\beta} \text{ or } \alpha = i\beta \text{ or } \alpha = -i\beta\right) \\
&\iff (\alpha = \beta \text{ or } \alpha = -\beta \text{ or } \alpha = i\beta \text{ or } \alpha = -i\beta).
\end{aligned}$$

This proves Proposition 4.2.11. □

Definition 4.2.12. We know from Proposition 4.2.8 that the relation $\sim$ on $\mathbb{Z}[i]$ is an equivalence relation.

The equivalence classes of this relation $\sim$ shall be called the *unit-equivalence classes*. More specifically, for each $\alpha \in \mathbb{Z}[i]$, we shall denote the $\sim$-equivalence class of α as the *unit-equivalence class of α*.

Proposition 4.2.13. **(a)** For each $\alpha \in \mathbb{Z}[i]$, we have

$$(\text{the unit-equivalence class of } \alpha) = \{\alpha, i\alpha, -\alpha, -i\alpha\}.$$

(b) The unit-equivalence classes are the sets of the form $\{\alpha, i\alpha, -\alpha, -i\alpha\}$ for some $\alpha \in \mathbb{Z}[i]$.

Proof of Proposition 4.2.13. **(a)** Let $\alpha \in \mathbb{Z}[i]$. Thus, both i and α belong to $\mathbb{Z}[i]$. Hence, all four of the complex numbers $\alpha, -\alpha, i\alpha, -i\alpha$ belong to $\mathbb{Z}[i]$ (by Proposition 4.2.4 **(a)** and Proposition 4.2.4 **(b)**).

If $b \in \mathbb{Z}[i]$ is any Gaussian integer, then we have $b \sim \alpha$ if and only if $(b = \alpha \text{ or } b = -\alpha \text{ or } b = i\alpha \text{ or } b = -i\alpha)$ (by Proposition 4.2.11, applied to b and α instead of α and β). In other words, the logical equivalence

$$(b \sim \alpha) \iff (b = \alpha \text{ or } b = -\alpha \text{ or } b = i\alpha \text{ or } b = -i\alpha) \tag{146}$$

holds for each $b \in \mathbb{Z}[i]$.

Then,

$$\begin{aligned}
&(\text{the unit-equivalence class of } \alpha) \\
&= (\text{the } \sim\text{-equivalence class of } \alpha) \qquad (\text{by Definition 4.2.12}) \\
&= [\alpha]_{\sim} = \{b \in \mathbb{Z}[i] \mid b \sim \alpha\} \qquad (\text{by Definition 3.3.1 } \textbf{(a)}) \\
&= \{b \in \mathbb{Z}[i] \mid b = \alpha \text{ or } b = -\alpha \text{ or } b = i\alpha \text{ or } b = -i\alpha\} \\
&\qquad (\text{since the equivalence (146) holds for each } b \in \mathbb{Z}[i]) \\
&= \{\alpha, -\alpha, i\alpha, -i\alpha\} \qquad (\text{since } \alpha, -\alpha, i\alpha, -i\alpha \text{ belong to } \mathbb{Z}[i]) \\
&= \{\alpha, i\alpha, -\alpha, -i\alpha\}.
\end{aligned} \tag{147}$$

This proves Proposition 4.2.13 **(a)**.

(b) The unit-equivalence classes are the sets of the form

$$(\text{the unit-equivalence class of } \alpha) \qquad \text{for some } \alpha \in \mathbb{Z}[i].$$

Since each $\alpha \in \mathbb{Z}[i]$ satisfies (147), this rewrites as follows: The unit-equivalence classes are the sets of the form

$$\{\alpha, i\alpha, -\alpha, -i\alpha\} \qquad \text{for some } \alpha \in \mathbb{Z}[i].$$

This proves Proposition 4.2.13 **(b)**. □

Recall that (as we have seen in Subsection 4.1.8) if α is a complex number, then the four complex numbers α, $i\alpha$, $-\alpha$ and $-i\alpha$ (represented as points in the Argand diagram) are the vertices of a square centered at the origin. But when α is a Gaussian integer, these four complex numbers constitute the unit-equivalence class of α (by Proposition 4.2.13 **(a)**). Thus, geometrically speaking, the unit-equivalence class of a Gaussian integer α consists of the four vertices of a square centered at the origin. (When $\alpha = 0$, these four vertices coincide.)

Proposition 4.2.14. Let α be a Gaussian integer. Then, $\alpha \sim 1$ if and only if α is a unit.

Proof of Proposition 4.2.14. We have the following chain of logical equivalences:

$$\begin{aligned}(\alpha \sim 1) &\iff \left(\alpha = \underbrace{\gamma \cdot 1}_{=\gamma} \text{ for some unit } \gamma \in \mathbb{Z}[i]\right) \\ &\qquad \text{(by the definition of the relation } \sim) \\ &\iff (\alpha = \gamma \text{ for some unit } \gamma \in \mathbb{Z}[i]) \\ &\iff (\alpha \text{ is a unit}).\end{aligned}$$

This proves Proposition 4.2.14. □

Proposition 4.2.15. Let α and β be two unit-equivalent Gaussian integers. Then, $\mathrm{N}(\alpha) = \mathrm{N}(\beta)$.

Proof of Proposition 4.2.15. We have $\alpha \sim \beta$ (since α and β are unit-equivalent). In other words, we have $\alpha = \gamma\beta$ for some unit $\gamma \in \mathbb{Z}[i]$ (by the definition of the relation $\sim$). Consider this γ. Since γ is a unit, we have $\mathrm{N}(\gamma) = 1$ (by Proposition 4.2.9 **(b)**, applied to γ instead of α). Now,

$$\begin{aligned}\mathrm{N}\left(\underbrace{\alpha}_{=\gamma\beta}\right) &= \mathrm{N}(\gamma\beta) = \underbrace{\mathrm{N}(\gamma)}_{=1}\mathrm{N}(\beta) \qquad \left(\begin{array}{c}\text{by Proposition 4.1.27 } \textbf{(d)}, \\ \text{applied to } \gamma \text{ instead of } \alpha\end{array}\right) \\ &= \mathrm{N}(\beta).\end{aligned}$$

This proves Proposition 4.2.15. □

The converse of Proposition 4.2.15 does not hold: There exist Gaussian integers α and β satisfying $\mathrm{N}(\alpha) = \mathrm{N}(\beta)$ that are not unit-equivalent.

At this point, let us briefly take a look at a seemingly random question: Which Gaussian integers α are unit-equivalent to their own conjugates (i.e., satisfy $\alpha \sim \overline{\alpha}$) ? Besides being an instructive exercise, answering this question will surprisingly aid us answer Question 1.4.2 later on!

Here are some examples:

- Every integer g satisfies $g \sim \overline{g}$, since an integer g always satisfies $\overline{g} = g$.
- Every integer g satisfies $gi \sim \overline{gi}$. Indeed, if g is an integer, then Proposition 4.1.27 **(c)** (applied to $\alpha = g$ and $\beta = i$) yields

$$\overline{gi} = \underbrace{\overline{g}}_{\substack{=g \\ (\text{since } g \in \mathbb{Z} \subseteq \mathbb{R})}} \cdot \underbrace{\overline{i}}_{=-i} = g(-i) = -gi = (-1)\cdot(gi),$$

  and this leads to $\overline{gi} \sim gi$ (since -1 is a unit); but this, in turn, yields $gi \sim \overline{gi}$ (since Proposition 4.2.8 shows that $\sim$ is an equivalence relation).

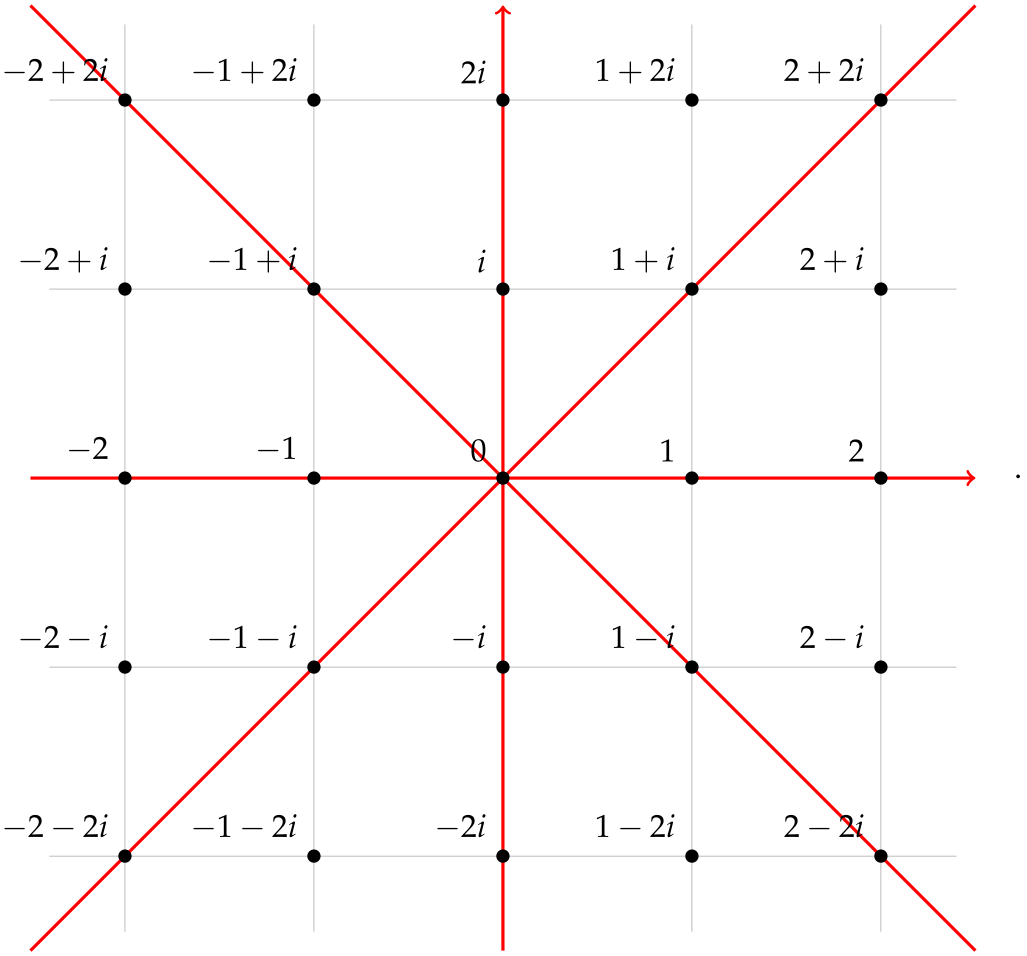
- Every integer g satisfies $g(1+i) \sim \overline{g(1+i)}$. Indeed, if g is an integer, then Proposition 4.1.27 **(c)** (applied to $\alpha = g$ and $\beta = 1+i$) yields

$$\overline{g(1+i)} = \underbrace{\overline{g}}_{\substack{=g \\ (\text{since } g\in\mathbb{Z}\subseteq\mathbb{R})}} \cdot \underbrace{\overline{(1+i)}}_{\substack{=1-i \\ =(-i)(1+i) \\ (\text{check this!})}} = g(-i)(1+i) = (-i)\cdot(g(1+i)),$$

  and this leads to $\overline{g(1+i)} \sim g(1+i)$ (since $-i$ is a unit); but this, in turn, yields $g(1+i) \sim \overline{g(1+i)}$ (since Proposition 4.2.8 shows that $\sim$ is an equivalence relation).

- Every integer g satisfies $g(1-i) \sim \overline{g(1-i)}$. This can be checked similarly to how we just checked $g(1+i) \sim \overline{g(1+i)}$.

Thus, in total, we have found four families of Gaussian integers α satisfying $\alpha \sim \overline{\alpha}$: namely, those of the form $g \in \mathbb{Z}$; those of the form gi with $g \in \mathbb{Z}$; those of the form $g(1+i)$ with $g \in \mathbb{Z}$; and those of the form $g(1-i)$ with $g \in \mathbb{Z}$. On the Argand diagram, these are precisely the lattice points on the four bold red lines on the following picture:



Are there any other Gaussian integers α satisfying $\alpha \sim \overline{\alpha}$? As the following exercise (or, rather, its part **(a)**) shows, the answer is "no"; we have found all such α.

Exercise 4.2.1. Let α be a Gaussian integer satisfying $\alpha \sim \overline{\alpha}$. Prove the following:
(a) There exist some $g \in \mathbb{Z}$ and $\tau \in \{1, i, 1+i, 1-i\}$ such that $\alpha = g\tau$.
(b) These g and τ satisfy $\operatorname{N}(\alpha) \in \{g^2, 2g^2\}$.
(c) The norm $\operatorname{N}(\alpha)$ cannot be an odd prime.

(Part **(c)** of this exercise, strange as it sounds, is the one we will end up using later.)

For the sake of the next subsection, let us state a simple property of integers:

Lemma 4.2.16. Let a and b be two integers. Then, we have the logical equivalence

$$(a \mid b) \iff (\text{there exists a Gaussian integer } \gamma \text{ such that } b = a\gamma).$$

Proof of Lemma 4.2.16. $\Longrightarrow$: Assume that $a \mid b$. We must prove that there exists a Gaussian integer γ such that $b = a\gamma$.

We have $a \mid b$. Thus, there exists an integer c such that $b = ac$ (by Definition 2.2.1). Consider this c. Then, c is an integer, and thus is a Gaussian integer. Hence, there there exists a Gaussian integer γ such that $b = a\gamma$ (namely, $\gamma = c$). Thus, the "$\Longrightarrow$" direction of Lemma 4.2.16 is proven.

$\Longleftarrow$: Assume that there exists a Gaussian integer γ such that $b = a\gamma$. We must prove that $a \mid b$.

We have assumed that there exists a Gaussian integer γ such that $b = a\gamma$. Consider this γ. Write the complex number γ as $\gamma = (c, d)$ with $c, d \in \mathbb{R}$. Then, $c, d \in \mathbb{Z}$ (since γ is a Gaussian integer). In other words, c and d are integers. Furthermore, $b = a \underbrace{\gamma}_{=(c,d)} = a(c,d) = (ac, ad)$ (by Proposition 4.1.9, applied to (c,d) instead of (b,c)). This is an equality between a real number (namely, b) and a complex number (namely, (ac, ad)); thus, it means $b_{\mathbb{C}} = (ac, ad)$ (according to Convention 4.1.7). But $b_{\mathbb{C}} = (b, 0)$ (by the definition of $b_{\mathbb{C}}$). Hence, $(b, 0) = b_{\mathbb{C}} = (ac, ad)$. In other words, $b = ac$ and $0 = ad$. Now, from $b = ac$, we obtain $a \mid b$ (since c is an integer). This proves the "$\Longleftarrow$" direction of Lemma 4.2.16. □

4.2.3. Divisibility and congruence

Now, let us begin to do proper number theory with Gaussian integers. The next definition is the straightforward analogue of Definition 2.2.1.

Definition 4.2.17. Let α and β be two Gaussian integers. We say that $\alpha \mid \beta$ (or "α *divides* β" or "β is *divisible by* α" or "β is a *multiple* of α") if there exists a Gaussian integer γ such that $\beta = \alpha\gamma$.

We furthermore say that $\alpha \nmid \beta$ if α does not divide β.

When making such a definition, we need to be careful: Potentially, it might create a clash of notations. In fact, if a and b are integers, then the statement "$a \mid b$" already has a meaning (explained in Definition 2.2.1). Definition 4.2.17 gives this statement a new meaning, because we can consider our integers a and b as Gaussian integers (since every integer is a Gaussian integer). If these two meanings are not equivalent, then the statement "$a \mid b$" becomes ambiguous (as it now has two different meanings) – so we have laid ourselves a landmine!

Fortunately, these two meanings **are** equivalent. That is: If a and b are two integers, then the statement "$a \mid b$" interpreted according to Definition 2.2.1 is equivalent to the statement "$a \mid b$" interpreted according to Definition 4.2.17. Indeed, if a and b are two integers, then we have the following chain of equivalences:

$$\begin{aligned} & (a \mid b \text{ in the sense of Definition 2.2.1}) \\ \iff & (\text{there exists a Gaussian integer } \gamma \text{ such that } b = a\gamma) \qquad (\text{by Lemma 4.2.16}) \\ \iff & (a \mid b \text{ in the sense of Definition 4.2.17}) . \end{aligned}$$

Thus, the two possible meanings of "$a \mid b$" are equivalent, and so we are spared of any ambiguity.

More generally, the following proposition holds:

Proposition 4.2.18. Let $a \in \mathbb{Z}$ and $\beta = (b, c) \in \mathbb{Z}[i]$. Then, $a \mid \beta$ if and only if a divides both b and c.

Proof of Proposition 4.2.18. $\Longrightarrow$: Assume that $a \mid \beta$. We must prove that a divides both b and c.

The statement $a \mid \beta$ means that there exists a Gaussian integer γ such that $\beta = a\gamma$ (according to Definition 4.2.17). Thus, there exists a Gaussian integer γ such that $\beta = a\gamma$ (since $a \mid \beta$). Consider this γ. Write the complex number γ in the form $\gamma = (u, v)$ for some $u, v \in \mathbb{R}$. Then, $u, v \in \mathbb{Z}$ (since γ is a Gaussian integer). In other words, u and v are integers.

Recall that $\beta = (b, c)$. Hence, $(b, c) = \beta = a \underbrace{\gamma}_{=(u,v)} = a(u, v) = (au, av)$ (by Proposition 4.1.9, applied to (u, v) instead of (b, c)). In other words, $b = au$ and $c = av$. From $b = au$, we obtain $a \mid b$ (since u is an integer). From $c = av$, we obtain $a \mid c$ (since v is an integer). Thus, we have $a \mid b$ and $a \mid c$. In other words, a divides both b and c. This proves the "$\Longrightarrow$" direction of Proposition 4.2.18.

$\Longleftarrow$: Assume that a divides both b and c. We must prove that $a \mid \beta$.

We have assumed that a divides both b and c. In other words, $a \mid b$ and $a \mid c$. From $a \mid b$, we conclude that there exists an integer u such that $b = au$ (by the definition of divisibility). Consider this u. From $a \mid c$, we conclude that there exists an integer v such that $c = av$ (by the definition of divisibility). Consider this v. Note that u and v are integers; in other words, $u, v \in \mathbb{Z}$.

The complex number (u, v) is a Gaussian integer (since $u, v \in \mathbb{Z}$). Moreover, Proposition 4.1.9 (applied to (u, v) instead of (b, c)) yields $a(u, v) = (au, av)$. Comparing this with $\beta = \left(\underbrace{b}_{=au}, \underbrace{c}_{=av} \right) = (au, av)$, we obtain $\beta = a(u,v)$. Hence, there exists a Gaussian integer γ such that $\beta = a\gamma$ (namely, $\gamma = (u,v)$).

The statement $a \mid \beta$ means that there exists a Gaussian integer γ such that $\beta = a\gamma$ (according to Definition 4.2.17). Thus, $a \mid \beta$ (since there exists a Gaussian integer γ such that $\beta = a\gamma$). This proves the "$\Longleftarrow$" direction of Proposition 4.2.18. □

The next proposition is a (partial) analogue of Proposition 2.2.3:

Proposition 4.2.19. Let α and β be two Gaussian integers.

(a) If $\alpha \mid \beta$, then $\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$.

(b) If $\alpha \mid \beta$ and $\beta \neq 0$, then $\mathrm{N}(\alpha) \leq \mathrm{N}(\beta)$.

(c) Assume that $\alpha \neq 0$. Then, $\alpha \mid \beta$ if and only if $\dfrac{\beta}{\alpha} \in \mathbb{Z}[i]$.

Note that we are using the norms $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ as analogues of $|a|$ and $|b|$ here, since the absolute values $|\alpha|$ and $|\beta|$ of Gaussian integers are often irrational and thus it makes no sense to talk of their divisibility. (At least, this prevents us from using the absolute values of α and β in Proposition 4.2.19 **(a)**. We could use them in Proposition 4.2.19 **(b)**.)

Note that the converse of Proposition 4.2.19 **(a)** does not hold. (That is, $\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$ does not yield $\alpha \mid \beta$.)

Proof of Proposition 4.2.19. Proposition 4.2.6 yields $\mathrm{N}(\alpha) \in \mathbb{N}$; thus, $\mathrm{N}(\alpha)$ is an integer. Similarly, $\mathrm{N}(\beta)$ is an integer. Hence, the statement "$\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$" makes sense.

(a) Assume that $\alpha \mid \beta$. Thus, there exists a Gaussian integer γ such that $\beta = \alpha\gamma$ (by Definition 4.2.17). Consider this γ. We have $\mathrm{N}(\gamma) \in \mathbb{N}$ (by Proposition 4.2.6, applied to γ instead of α). Now, from $\beta = \alpha\gamma$, we obtain $\mathrm{N}(\beta) = \mathrm{N}(\alpha\gamma) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\gamma)$ (by Proposition 4.1.27 **(d)**, applied to γ instead of β). Thus, $\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$ (since $\mathrm{N}(\gamma) \in \mathbb{N} \subseteq \mathbb{Z}$). This proves Proposition 4.2.19 **(a)**.

(b) Assume that $\alpha \mid \beta$ and $\beta \neq 0$. Proposition 4.1.22 **(c)** (applied to β instead of α) shows that $\mathrm{N}(\beta) > 0$ (since $\beta \neq 0$). Hence, $\mathrm{N}(\beta) \neq 0$. Furthermore, Proposition 4.2.19 **(a)** yields $\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$. Thus, Proposition 2.2.3 **(b)** (applied to $a = \mathrm{N}(\alpha)$ and $b = \mathrm{N}(\beta)$) yields $|\mathrm{N}(\alpha)| \leq |\mathrm{N}(\beta)|$.

But recall that $\mathrm{N}(\alpha) \in \mathbb{N}$, so that $\mathrm{N}(\alpha) \geq 0$ and therefore $|\mathrm{N}(\alpha)| = \mathrm{N}(\alpha)$. Similarly, $|\mathrm{N}(\beta)| = \mathrm{N}(\beta)$. Hence, $\mathrm{N}(\alpha) = |\mathrm{N}(\alpha)| \leq |\mathrm{N}(\beta)| = \mathrm{N}(\beta)$. This proves Proposition 4.2.19 **(b)**.

(c) The proof of Proposition 4.2.19 **(c)** is analogous to the proof of Proposition 2.2.3 **(c)**. (Of course, we need to replace a and b by α and β, and replace integers by Gaussian integers throughout the argument.) □

The next proposition is a straightforward analogue of Proposition 2.2.4:

Proposition 4.2.20. **(a)** We have $\alpha \mid \alpha$ for every $\alpha \in \mathbb{Z}[i]$. (This is called the *reflexivity of divisibility* for Gaussian integers.)

(b) If $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ satisfy $\alpha \mid \beta$ and $\beta \mid \gamma$, then $\alpha \mid \gamma$. (This is called the *transitivity of divisibility* for Gaussian integers.)

(c) If $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}[i]$ satisfy $\alpha_1 \mid \beta_1$ and $\alpha_2 \mid \beta_2$, then $\alpha_1\alpha_2 \mid \beta_1\beta_2$.

Proof of Proposition 4.2.20. This proof is completely analogous to the proof of Proposition 2.2.4. (The only changes you need to make are replacing the Roman letters $a, b, c, a_1, a_2, b_1, b_2$ by the corresponding Greek letters $\alpha, \beta, \gamma, \alpha_1, \alpha_2, \beta_1, \beta_2$, and replacing integers by Gaussian integers. Of course, the resulting argument will use Proposition 4.2.4 **(a)**, specifically the fact that the product of two Gaussian integers is a Gaussian integer.) □

The next exercise is a Gaussian-integer analogue of Exercise 2.2.2:

Exercise 4.2.2. Let α and β be two Gaussian integers such that $\alpha \mid \beta$ and $\beta \mid \alpha$. Prove that $\alpha \sim \beta$.

Note that the conclusion "$\alpha \sim \beta$" in Exercise 4.2.2 is the proper Gaussian-integer analogue of the conclusion "$|a| = |b|$" in Exercise 2.2.2 (since (145) shows that unit-equivalence on $\mathbb{Z}[i]$ is an analogue of the "have the same absolute value" relation on $\mathbb{Z}$). (We could have stated the weaker conclusion $|\alpha| = |\beta|$ as well, but it would not be half as useful.)

A converse of Exercise 4.2.2 holds as well, so we have the following equivalent description of unit-equivalence:

Exercise 4.2.3. Let α and β be two Gaussian integers. Prove that we have the logical equivalence

$$(\alpha \sim \beta) \iff (\alpha \mid \beta \text{ and } \beta \mid \alpha).$$

The next exercise is an analogue of Exercise 2.2.3:

Exercise 4.2.4. Let α, β, γ be three Gaussian integers such that $\gamma \neq 0$. Prove that $\alpha \mid \beta$ holds if and only if $\alpha\gamma \mid \beta\gamma$.

The next exercise is an analogue of Exercise 2.2.4:

Exercise 4.2.5. Let $\nu \in \mathbb{Z}[i]$. Let $a, b \in \mathbb{N}$ be such that $a \leq b$. Prove that $\nu^a \mid \nu^b$.

Needless to say, the a and b in this exercise still have to be nonnegative integers, since Gaussian integers make no sense as exponents.

The next exercise is an analogue of Exercise 2.2.5:

Exercise 4.2.6. Let γ be a Gaussian integer such that $\gamma \mid 1$. Prove that $\gamma \sim 1$ (that is, γ is a unit, i.e., either 1 or -1 or i or $-i$).

Next come two more trivial facts:

Exercise 4.2.7. Let α and β be Gaussian integers such that $\alpha \mid \beta$. Prove that $\overline{\alpha} \mid \overline{\beta}$.

Exercise 4.2.8. Let α, β and γ be three Gaussian integers. Prove the following:
(a) If $\beta \sim \gamma$, then we have the logical equivalence $(\alpha \mid \beta) \iff (\alpha \mid \gamma)$.
(b) If $\alpha \sim \beta$, then we have the logical equivalence $(\alpha \mid \gamma) \iff (\beta \mid \gamma)$.
(c) Let δ be a further Gaussian integer. Assume that $\alpha \sim \beta$ and $\gamma \sim \delta$. Then, we have the logical equivalence $(\alpha \mid \gamma) \iff (\beta \mid \delta)$.

Another useful and easily proven fact is the following:

Exercise 4.2.9. Let α and β be Gaussian integers such that $\alpha \mid \beta$ and $\mathrm{N}(\alpha) = \mathrm{N}(\beta)$. Prove that $\alpha \sim \beta$.

We have defined congruence for integers in Definition 2.3.1. We can repeat the same definition for Gaussian integers:

Definition 4.2.21. Let $\nu, \alpha, \beta \in \mathbb{Z}[i]$. We say that α *is congruent to* β *modulo* ν if and only if $\nu \mid \alpha - \beta$. We shall use the notation "$\alpha \equiv \beta \mod \nu$" for "$\alpha$ is congruent to β modulo ν".

We furthermore shall use the notation "$\alpha \not\equiv \beta \mod \nu$" for "$\alpha$ is not congruent to β modulo ν".

Once again, such a definition risks sneaking in ambiguity, but fortunately this one does not: If $n, a, b \in \mathbb{Z}$, then the statement "$a \equiv b \mod n$" interpreted according to Definition 2.3.1 is equivalent to the statement "$a \equiv b \mod n$" interpreted according to Definition 4.2.21 (by treating n, a, b as Gaussian integers). To see why, recall that both statements are defined to mean "$n \mid a - b$", and the meaning of the latter statement does not depend on whether we interpret n, a, b as integers or as Gaussian integers[141].

The next proposition is a straightforward analogue of Proposition 2.3.3:

Proposition 4.2.22. Let $\nu \in \mathbb{Z}[i]$ and $\alpha \in \mathbb{Z}[i]$. Then, $\alpha \equiv 0 \mod \nu$ if and only if $\nu \mid \alpha$.

Proof of Proposition 4.2.22. This proof is analogous to the proof of Proposition 2.3.3. □

The next proposition is a straightforward analogue of Proposition 2.3.4:

[141] We have proven this latter fact shortly after Definition 4.2.17.

Proposition 4.2.23. Let $\nu \in \mathbb{Z}[i]$.

(a) We have $\alpha \equiv \alpha \bmod \nu$ for every $\alpha \in \mathbb{Z}[i]$.

(b) If $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ satisfy $\alpha \equiv \beta \bmod \nu$ and $\beta \equiv \gamma \bmod \nu$, then $\alpha \equiv \gamma \bmod \nu$.

(c) If $\alpha, \beta \in \mathbb{Z}[i]$ satisfy $\alpha \equiv \beta \bmod \nu$, then $\beta \equiv \alpha \bmod \nu$.

(d) If $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}[i]$ satisfy $\alpha_1 \equiv \beta_1 \bmod \nu$ and $\alpha_2 \equiv \beta_2 \bmod \nu$, then

$$\alpha_1 + \alpha_2 \equiv \beta_1 + \beta_2 \bmod \nu; \tag{148}$$

$$\alpha_1 - \alpha_2 \equiv \beta_1 - \beta_2 \bmod \nu; \tag{149}$$

$$\alpha_1 \alpha_2 \equiv \beta_1 \beta_2 \bmod \nu. \tag{150}$$

(e) Let $\mu \in \mathbb{Z}[i]$ be such that $\mu \mid \nu$. If $\alpha, \beta \in \mathbb{Z}[i]$ satisfy $\alpha \equiv \beta \bmod \nu$, then $\alpha \equiv \beta \bmod \mu$.

Proof of Proposition 4.2.23. This proof is analogous to the proof of Proposition 2.3.4. (Of course, it relies on parts **(a)** and **(b)** of Proposition 4.2.4, and it uses Proposition 4.2.20 instead of Proposition 2.2.4.) □

Exercise 4.2.10. Let n be an integer. Let (a, b) and (c, d) be two Gaussian integers. Prove that we have the following logical equivalence:

$$((a, b) \equiv (c, d) \bmod n) \iff (a \equiv c \bmod n \text{ and } b \equiv d \bmod n).$$

(Of course, the statement "$(a, b) \equiv (c, d) \bmod n$" is to be understood by treating the integer n as a Gaussian integer.)

Exercise 4.2.11. For any Gaussian integer τ, we let $\underset{\tau}{\equiv}$ be the binary relation on $\mathbb{Z}[i]$ defined by

$$\left(\alpha \underset{\tau}{\equiv} \beta\right) \iff (\alpha \equiv \beta \bmod \tau).$$

(a) Prove that the relation $\underset{\tau}{\equiv}$ is an equivalence relation whenever $\tau \in \mathbb{Z}[i]$.

We shall refer to the equivalence classes of this relation $\underset{\tau}{\equiv}$ as the *Gaussian residue classes modulo* τ; let $\mathbb{Z}[i]/\tau$ be the set of all these classes.

(b) Let n be a positive integer. Thus, a relation $\underset{n}{\equiv}$ on $\mathbb{Z}[i]$ is defined (by treating the integer n as a Gaussian integer). Exercise 4.2.11 **(a)** (applied to $\tau = n$) shows that this relation $\underset{n}{\equiv}$ is an equivalence relation.

Prove that the equivalence classes of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) are the n^2 classes $[a + bi]_{\underset{n}{\equiv}}$ for $(a, b) \in \{0, 1, \ldots, n-1\}^2$, and that these n^2 classes are all distinct.

Example 4.2.24. For $n = 3$, Exercise 4.2.11 **(b)** is saying that the equivalence classes of the relation $\underset{3}{\equiv}$ (on $\mathbb{Z}[i]$) are the 3^2 classes

$$\begin{array}{ccc} [0+0i]_{\underset{3}{\equiv}}, & [0+1i]_{\underset{3}{\equiv}}, & [0+2i]_{\underset{3}{\equiv}}, \\ [1+0i]_{\underset{3}{\equiv}}, & [1+1i]_{\underset{3}{\equiv}}, & [1+2i]_{\underset{3}{\equiv}}, \\ [2+0i]_{\underset{3}{\equiv}}, & [2+1i]_{\underset{3}{\equiv}}, & [2+2i]_{\underset{3}{\equiv}}, \end{array}$$

and that these 3^2 classes are distinct. In contrast, the equivalence classes of the analogous relation $\underset{3}{\equiv}$ on $\mathbb{Z}$ are merely the 3 classes $[0]_{\underset{3}{\equiv}}, [1]_{\underset{3}{\equiv}}, [2]_{\underset{3}{\equiv}}$ (by Theorem 3.4.4).

Remark 4.2.25. Exercise 4.2.11 **(b)** yields $|\mathbb{Z}[i]/n| = n^2 = \mathrm{N}(n)$ for any positive integer n. This is essentially [ConradG, Lemma 7.15]. (Conrad proves this "by example"; you can follow the argument but you should write it up in full generality.)

More generally, $|\mathbb{Z}[i]/\tau| = \mathrm{N}(\tau)$ for any nonzero Gaussian integer τ. This is proven in [ConradG, Theorem 7.14] (using Exercise 4.2.11 as a stepping stone).

4.2.4. Division with remainder

Now, let us try to make division with remainder work for Gaussian integers. This turns out to be tricky: There is no straightforward analogue of Theorem 2.6.1 for Gaussian integers. (In fact, it is not clear what $\{0, 1, \ldots, b-1\}$ would mean if we let b be a Gaussian integer.) The best thing we can get for Gaussian integers is an analogue of Exercise 2.6.2 **(a)**:

Theorem 4.2.26. Let α and $\beta \neq 0$ be Gaussian integers. There exist Gaussian integers γ and ρ such that $\alpha = \gamma\beta + \rho$ and $\mathrm{N}(\rho) \leq \mathrm{N}(\beta)/2$.

Note that the pair (γ, ρ) in this theorem is not unique. As we have said, Theorem 4.2.26 is an analogue of Exercise 2.6.2 **(a)** (with α, β, γ and ρ taking the roles of u, n, q and r), not an analogue of Theorem 2.6.1; nevertheless, it is the closest we can get to Theorem 2.6.1 in $\mathbb{Z}[i]$, and can often be substituted in places where one would usually want to apply Theorem 2.6.1 (as long as one does not try to use uniqueness of quotient and remainder).

Theorem 4.2.26 can be visualized geometrically (similarly to the visualizations shown in Remark 2.6.8 and Remark 2.6.10, but using the Argand diagram). See [ConradG, §7] for the details.

The following proof of Theorem 4.2.26 follows [ConradG, proof of Theorem 3.1].

Proof of Theorem 4.2.26. Let $n = \mathrm{N}(\beta)$. Then, $n = \mathrm{N}(\beta) > 0$ (by Proposition 4.1.22 **(c)**, applied to β instead of α), since $\beta \neq 0$. Also, Proposition 4.2.6 (applied to β

instead of α) yields $\operatorname{N}(\beta) \in \mathbb{N}$. Thus, $n = \operatorname{N}(\beta) \in \mathbb{N}$. Hence, n is a positive integer (since $n > 0$).

Proposition 4.1.26 **(a)** (applied to β instead of α) yields $\operatorname{N}(\beta) = \beta\overline{\beta}$. Thus, $\beta\overline{\beta} = \operatorname{N}(\beta) = n$.

Furthermore, Proposition 4.1.26 **(b)** (applied to β instead of α) yields $\operatorname{N}\left(\overline{\beta}\right) = \operatorname{N}(\beta) = n$.

Note that $\overline{\beta}$ is a Gaussian integer[142]. Furthermore, $\beta\overline{\beta} = n \neq 0$, so that $\beta \neq 0$ and $\overline{\beta} \neq 0$. Hence, we can divide complex numbers by β and by $\overline{\beta}$. Thus,

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{n} \qquad \left(\text{since } \beta\overline{\beta} = n\right).$$

Note that $\alpha\overline{\beta}$ is a Gaussian integer (since α and $\overline{\beta}$ are Gaussian integers); thus, we can write it in the form

$$\alpha\overline{\beta} = (u_1, u_2) \qquad \text{for some } u_1, u_2 \in \mathbb{Z}.$$

Consider these u_1, u_2.

Exercise 2.6.2 **(a)** (applied to $u = u_1$) shows that there exists a pair $(q_1, r_1) \in \mathbb{Z} \times \mathbb{Z}$ such that

$$u_1 = q_1 n + r_1 \qquad \text{and} \qquad |r_1| \leq n/2.$$

Consider this pair.

Exercise 2.6.2 **(a)** (applied to $u = u_2$) shows that there exists a pair $(q_2, r_2) \in \mathbb{Z} \times \mathbb{Z}$ such that

$$u_2 = q_2 n + r_2 \qquad \text{and} \qquad |r_2| \leq n/2.$$

Consider this pair.

Squaring the inequality $|r_1| \leq n/2$, we obtain $|r_1|^2 \leq (n/2)^2$ (since $|r_1|$ and $n/2$ are nonnegative (because $n > 0$)). But $|r_1|^2 = r_1^2$ (since $|r|^2 = r^2$ for every real r). Hence, $r_1^2 = |r_1|^2 \leq (n/2)^2 = n^2/4$. Similarly, $r_2^2 \leq n^2/4$. Now, the complex number $r_1 + r_2 i = (r_1, r_2)$ satisfies

$$\begin{aligned} \operatorname{N}(r_1 + r_2 i) &= \underbrace{r_1^2}_{\leq n^2/4} + \underbrace{r_2^2}_{\leq n^2/4} \qquad (\text{by the definition of } \operatorname{N}(r_1 + r_2 i)) \\ &\leq n^2/4 + n^2/4 = n^2/2. \end{aligned}$$

We can divide this inequality by n (since $n > 0$); thus, we find

$$\frac{\operatorname{N}(r_1 + r_2 i)}{n} \leq \frac{n^2/2}{n} = n/2 = \operatorname{N}(\beta)/2 \tag{151}$$

(since $n = \operatorname{N}(\beta)$).

[142] by Proposition 4.2.5, applied to β instead of α

But

$$\begin{aligned}
\frac{\alpha}{\beta} &= \frac{\alpha\overline{\beta}}{n} = \frac{(q_1 n + r_1) + (q_2 n + r_2)\, i}{n} \\
&\qquad \left(\text{since } \alpha\overline{\beta} = (u_1, u_2) = \underbrace{u_1}_{=q_1 n + r_1} + \underbrace{u_2}_{=q_2 n + r_2} i = (q_1 n + r_1) + (q_2 n + r_2)\, i\right) \\
&= (q_1 + q_2 i) + \frac{r_1 + r_2 i}{n}. \qquad (152)
\end{aligned}$$

Set $\gamma = q_1 + q_2 i$ and $\rho = \alpha - \gamma\beta$. Note that γ is a Gaussian integer (since $\gamma = q_1 + q_2 i = (q_1, q_2)$ with $q_1, q_2 \in \mathbb{Z}$). Hence, all of α, γ, β are Gaussian integers; thus, $\rho = \alpha - \gamma\beta$ is a Gaussian integer (by multiple applications of Proposition 4.2.4).

From $\rho = \alpha - \gamma\beta$, we obtain $\alpha = \gamma\beta + \rho$. Thus, it remains to prove $\mathrm{N}(\rho) \leq \mathrm{N}(\beta)/2$.

The equation (152) rewrites as $\dfrac{\alpha}{\beta} = \gamma + \dfrac{r_1 + r_2 i}{n}$ (since $q_1 + q_2 i = \gamma$). Hence,

$$\frac{r_1 + r_2 i}{n} = \frac{\alpha}{\beta} - \gamma = \frac{\alpha - \gamma\beta}{\beta} = \frac{\rho}{\beta}$$

(since $\alpha - \gamma\beta = \rho$). Therefore,

$$\begin{aligned}
\rho &= \beta \cdot \frac{r_1 + r_2 i}{n} = \beta \cdot \frac{r_1 + r_2 i}{\beta\overline{\beta}} \qquad \left(\text{since } n = \beta\overline{\beta}\right) \\
&= \frac{r_1 + r_2 i}{\overline{\beta}}
\end{aligned}$$

and thus

$$\begin{aligned}
\mathrm{N}(\rho) &= \mathrm{N}\left(\frac{r_1 + r_2 i}{\overline{\beta}}\right) = \frac{\mathrm{N}(r_1 + r_2 i)}{\mathrm{N}(\overline{\beta})} \\
&\qquad \left(\begin{array}{c}\text{by Proposition 4.1.27 } \textbf{(e)}\text{, applied to } r_1 + r_2 i \\ \text{and } \overline{\beta} \text{ instead of } \alpha \text{ and } \beta\end{array}\right) \\
&= \frac{\mathrm{N}(r_1 + r_2 i)}{n} \qquad \left(\text{since } \mathrm{N}(\overline{\beta}) = n\right) \\
&\leq \mathrm{N}(\beta)/2 \qquad (\text{by (151)}).
\end{aligned}$$

Thus, we have found two Gaussian integers γ and ρ such that $\alpha = \gamma\beta + \rho$ and $\mathrm{N}(\rho) \leq \mathrm{N}(\beta)/2$. This proves Theorem 4.2.26. □

Note that we cannot define $\alpha // \beta$ or $\alpha \% \beta$ for Gaussian integers α and β, since there is no uniqueness statement in Theorem 4.2.26.

4.2.5. Common divisors

Next, we define the Gaussian divisors of a Gaussian integer (in analogy to Definition 2.9.1):

Definition 4.2.27. Let $\beta \in \mathbb{Z}[i]$. The *Gaussian divisors* of β are defined as the Gaussian integers that divide β.

Note that we are calling them "Gaussian divisors" and not "divisors", because when β is an actual integer, there are (usually) Gaussian divisors of β that are not divisors of β (in the sense of Definition 2.9.1). For example, $1+i$ is a Gaussian divisor of 2 (since $2 = (1+i)(1-i)$), but the only divisors of 2 (in the sense of Definition 2.9.1) are $-2, -1, 1, 2$. This is one of those situations where using the same name for a concept and its Gaussian-integer analogue would lead to ambiguities.

The following is an analogue of Proposition 2.9.2:

Proposition 4.2.28. **(a)** If $\beta \in \mathbb{Z}[i]$, then 1 and β are Gaussian divisors of β.

(b) The Gaussian divisors of 0 are all the Gaussian integers.

(c) Let $\beta \in \mathbb{Z}[i]$ be nonzero. Then, all Gaussian divisors of β belong to the set

$$\left\{x + yi \mid x, y \in \mathbb{Z} \text{ satisfying } x^2 \leq \mathrm{N}(\beta) \text{ and } y^2 \leq \mathrm{N}(\beta)\right\}.$$

Proof of Proposition 4.2.28. **(a)** Let $\beta \in \mathbb{Z}[i]$. Then, $\beta = 1\beta$. Hence, $1 \mid \beta$ (since β is a Gaussian integer). In other words, 1 is a Gaussian divisor of β.

Also, $\beta = \beta \cdot 1$. Hence, $\beta \mid \beta$ (since 1 is a Gaussian integer). In other words, β is a Gaussian divisor of β.

So we have shown that 1 and β are Gaussian divisors of β. This proves Proposition 4.2.28 **(a)**.

(b) If β is a Gaussian integer, then $0 = \beta \cdot 0$, and thus β is a Gaussian divisor of 0 (since 0 is a Gaussian integer). In other words, each Gaussian integer is a Gaussian divisor of 0. Conversely, each Gaussian divisor of 0 is a Gaussian integer (by definition). Combining these two statements, we conclude that the Gaussian divisors of 0 are all the Gaussian integers. This proves Proposition 4.2.28 **(b)**.

(c) Let α be a Gaussian divisor of β. Write the complex number α in the form $\alpha = (a, b)$ with $a, b \in \mathbb{C}$. Then, $a, b \in \mathbb{Z}$ (since α is a Gaussian integer) and $\mathrm{N}(\alpha) = a^2 + b^2$ (by the definition of $\mathrm{N}(\alpha)$). But $\alpha \mid \beta$ (since α is a Gaussian divisor of β) and $\beta \neq 0$ (since β is nonzero). Hence, Proposition 4.2.19 **(b)** yields $\mathrm{N}(\alpha) \leq \mathrm{N}(\beta)$. But a, b are reals, and thus a^2, b^2 are nonnegative reals (since the square of a real is always a nonnegative real). In other words, $a^2 \geq 0$ and $b^2 \geq 0$.

Now, $\mathrm{N}(\alpha) = a^2 + \underbrace{b^2}_{\geq 0} \geq a^2$, so that $a^2 \leq \mathrm{N}(\alpha) \leq \mathrm{N}(\beta)$. Also, $\mathrm{N}(\alpha) = \underbrace{a^2}_{\geq 0} + b^2 \geq b^2$, so that $b^2 \leq \mathrm{N}(\alpha) \leq \mathrm{N}(\beta)$. Also, $\alpha = (a, b) = a + bi$. Hence, we have $\alpha = x + yi$ for some $x, y \in \mathbb{Z}$ satisfying $x^2 \leq \operatorname{N}(\beta)$ and $y^2 \leq \operatorname{N}(\beta)$ (namely, for $x = a$ and $y = b$). In other words,

$$\alpha \in \left\{ x + yi \mid x, y \in \mathbb{Z} \text{ satisfying } x^2 \leq \operatorname{N}(\beta) \text{ and } y^2 \leq \operatorname{N}(\beta) \right\}.$$

Now, forget that we fixed α. We thus have shown that if α is a Gaussian divisor of β, then

$$\alpha \in \left\{ x + yi \mid x, y \in \mathbb{Z} \text{ satisfying } x^2 \leq \operatorname{N}(\beta) \text{ and } y^2 \leq \operatorname{N}(\beta) \right\}.$$

In other words, all Gaussian divisors of β belong to the set

$$\left\{ x + yi \mid x, y \in \mathbb{Z} \text{ satisfying } x^2 \leq \operatorname{N}(\beta) \text{ and } y^2 \leq \operatorname{N}(\beta) \right\}.$$

This proves Proposition 4.2.28 **(c)**. □

Thus, again, finding all Gaussian divisors of a Gaussian integer β is a problem solvable in finite time. (Indeed, if $\beta = 0$, then Proposition 4.2.28 **(b)** answers this question; but otherwise, the set in Proposition 4.2.28 **(c)** is clearly finite.)

The following is a straightforward analogue of Definition 2.9.3:

Definition 4.2.29. Let $\beta_1, \beta_2, \ldots, \beta_k$ be Gaussian integers. Then, the *common Gaussian divisors* of $\beta_1, \beta_2, \ldots, \beta_k$ are defined to be the Gaussian integers α that satisfy

$$(\alpha \mid \beta_i \text{ for all } i \in \{1, 2, \ldots, k\}) \tag{153}$$

(in other words, that divide all of the Gaussian integers $\beta_1, \beta_2, \ldots, \beta_k$). We let $\operatorname{Div}_{\mathbb{Z}[i]}(\beta_1, \beta_2, \ldots, \beta_k)$ denote the set of these common Gaussian divisors.

The reason why I chose the notation $\operatorname{Div}_{\mathbb{Z}[i]}(\beta_1, \beta_2, \ldots, \beta_k)$ rather than the simpler notation $\operatorname{Div}(\beta_1, \beta_2, \ldots, \beta_k)$ is that the latter would be ambiguous. In fact, when $\beta_1, \beta_2, \ldots, \beta_k$ are integers, the set $\operatorname{Div}(\beta_1, \beta_2, \ldots, \beta_k)$ of common divisors of $\beta_1, \beta_2, \ldots, \beta_k$ is **not** the set $\operatorname{Div}_{\mathbb{Z}[i]}(\beta_1, \beta_2, \ldots, \beta_k)$ of common Gaussian divisors of $\beta_1, \beta_2, \ldots, \beta_k$. (For example, the former set does not contain i, while the latter does.)

We cannot directly define a "greatest common Gaussian divisor of $\beta_1, \beta_2, \ldots, \beta_k$" to be the greatest element of $\operatorname{Div}_{\mathbb{Z}[i]}(\beta_1, \beta_2, \ldots, \beta_k)$, since "greatest" does not make sense for complex numbers. (Even if we wanted "greatest in norm", it would not a-priori be obvious that there are no ties, i.e., that such a greatest common Gaussian divisor is unique.)

However, it turns out that a "greatest common Gaussian divisor" $\gcd_{\mathbb{Z}[i]}(\beta_1, \beta_2, \ldots, \beta_k)$ actually can be defined reasonably (although only up to multiplication by units). Before we can do so, let us state some basic properties of common Gaussian divisors:[143]

[143] Proposition 4.2.30 is an analogue of part of Lemma 2.9.10. Thus, we have chosen to label its claims in a way that matches the corresponding claims in Lemma 2.9.10. This forced us to skip claim **(e)**, since there is no analogue of Lemma 2.9.10 **(e)** for Gaussian integers (because $\beta \% \alpha$ is not defined when β and α are Gaussian integers).

Proposition 4.2.30. **(a)** We have $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, 0) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha)$ for all $\alpha \in \mathbb{Z}[i]$.

(b) We have $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\beta, \alpha)$ for all $\alpha, \beta \in \mathbb{Z}[i]$.

(c) We have $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \eta\alpha + \beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ for all $\alpha, \beta, \eta \in \mathbb{Z}[i]$.

(d) If $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ satisfy $\beta \equiv \gamma \mod \alpha$, then $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \gamma)$.

(f) We have $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) \subseteq \operatorname{Div}_{\mathbb{Z}[i]}(\alpha)$ and $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) \subseteq \operatorname{Div}_{\mathbb{Z}[i]}(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$.

(g) We have $\operatorname{Div}_{\mathbb{Z}[i]}(\eta\alpha, \beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$ and every unit $\eta \in \mathbb{Z}[i]$.

(h) We have $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \eta\beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$ and every unit $\eta \in \mathbb{Z}[i]$.

(i) If $\alpha, \beta \in \mathbb{Z}[i]$ satisfy $\alpha \mid \beta$, then $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha)$.

(j) The common Gaussian divisors of the empty list of Gaussian integers are $\operatorname{Div}_{\mathbb{Z}[i]}() = \mathbb{Z}[i]$.

Proof of Proposition 4.2.30. Parts **(a)**, **(b)**, **(c)**, **(d)**, **(f)**, **(i)** and **(j)** of Proposition 4.2.30 are analogues of the corresponding parts of Lemma 2.9.10. Their proofs also are straightforward adaptations of the proofs of the latter parts; we trust the reader to perform the necessary replacements. Thus, it remains to prove parts **(g)** and **(h)** of Proposition 4.2.30 (which are similar to parts **(g)** and **(h)** of Lemma 2.9.10, but perhaps not in a completely evident way). Let us do this now.

(g) Let $\alpha, \beta \in \mathbb{Z}[i]$. Let $\eta \in \mathbb{Z}[i]$ be a unit.

Let ξ be a Gaussian integer. We have $\eta\alpha = \gamma\alpha$ for some unit $\gamma \in \mathbb{Z}[i]$ (namely, for $\gamma = \eta$). In other words, $\eta\alpha \sim \alpha$ (by the definition of the relation $\sim$ on $\mathbb{Z}[i]$). Hence, Exercise 4.2.8 **(a)** (applied to ξ, $\eta\alpha$ and α instead of α, β and γ) shows that we have the logical equivalence $(\xi \mid \alpha) \iff (\xi \mid \eta\alpha)$.

But we have the following chain of equivalences:

$$\begin{aligned}
&\left(\xi \in \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)\right) \\
\iff &\ (\xi \text{ is a common Gaussian divisor of } \alpha \text{ and } \beta) \\
&\ \left(\text{by the definition of } \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)\right) \\
\iff &\ \left(\underbrace{\xi \mid \alpha}_{\iff (\xi \mid \eta\alpha)} \text{ and } \xi \mid \beta\right) \\
&\ (\text{by the definition of a ``common Gaussian divisor''}) \\
\iff &\ (\xi \mid \eta\alpha \text{ and } \xi \mid \beta) \\
\iff &\ (\xi \text{ is a common Gaussian divisor of } \eta\alpha \text{ and } \beta) \\
&\ (\text{by the definition of a ``common Gaussian divisor''}) \\
\iff &\ \left(\xi \in \operatorname{Div}_{\mathbb{Z}[i]}(\eta\alpha, \beta)\right) \qquad \left(\text{by the definition of } \operatorname{Div}_{\mathbb{Z}[i]}(\eta\alpha, \beta)\right).
\end{aligned}$$

Now, forget that we fixed ξ. We thus have proved the logical equivalence

$\left(\xi \in \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)\right) \iff \left(\xi \in \operatorname{Div}_{\mathbb{Z}[i]}(\eta\alpha, \beta)\right)$ for each Gaussian integer ξ. In other words, a Gaussian integer belongs to $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ if and only if it belongs to $\operatorname{Div}_{\mathbb{Z}[i]}(\eta\alpha, \beta)$. Thus, $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\eta\alpha, \beta)$ (since both $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ and $\operatorname{Div}_{\mathbb{Z}[i]}(\eta\alpha, \beta)$ are sets of Gaussian integers). This proves Proposition 4.2.30 **(g)**.

(h) We can prove Proposition 4.2.30 **(h)** in a similar way to Proposition 4.2.30 **(g)**. Alternatively, we can derive it from the already proven parts of Proposition 4.2.30 as follows:

Let $\alpha, \beta \in \mathbb{Z}[i]$. Let $\eta \in \mathbb{Z}[i]$ be a unit. Then, Proposition 4.2.30 **(b)** (applied to $\eta\beta$ instead of β) yields

$$\begin{aligned}\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \eta\beta) &= \operatorname{Div}_{\mathbb{Z}[i]}(\eta\beta, \alpha) = \operatorname{Div}_{\mathbb{Z}[i]}(\beta, \alpha) \\ &\qquad \left(\begin{array}{c}\text{by Proposition 4.2.30 } \textbf{(g)}\text{, applied to } \beta \text{ and } \alpha \\ \text{instead of } \alpha \text{ and } \beta\end{array}\right) \\ &= \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) \qquad (\text{by Proposition 4.2.30 } \textbf{(b)}).\end{aligned}$$

Thus, Proposition 4.2.30 **(h)** is proven. □

You have reached the end of the finished part.
TODO: Write on from here.

Recall that Proposition 2.9.7 gave us a quick way to compute $\gcd(a, b)$ for two nonnegative integers a and b; this is called the Euclidean algorithm. Likewise, we can use Proposition 4.2.30 to compute $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ for two Gaussian integers α and β (or, more precisely, to rewrite $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ in the form $\operatorname{Div}_{\mathbb{Z}[i]}(\gamma)$ for a single Gaussian integer γ). For example, we can compute $\operatorname{Div}_{\mathbb{Z}[i]}(32 + 9i, 4 + 11i)$

as follows:[144]

$$\begin{aligned}
&\operatorname{Div}_{\mathbb{Z}[i]}(32+9i, 4+11i)\\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(4+11i, \underbrace{32+9i}_{=(2-2i)(4+11i)+(2-5i)}\right) \qquad \text{(by Proposition 4.2.30 \textbf{(b)})}\\
&= \operatorname{Div}_{\mathbb{Z}[i]}(4+11i, (2-2i)(4+11i)+(2-5i))\\
&= \operatorname{Div}_{\mathbb{Z}[i]}(4+11i, 2-5i) \qquad \text{(by Proposition 4.2.30 \textbf{(c)})}\\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(2-5i, \underbrace{4+11i}_{=(-2+i)(2-5i)+(3-i)}\right) \qquad \text{(by Proposition 4.2.30 \textbf{(b)})}\\
&= \operatorname{Div}_{\mathbb{Z}[i]}(2-5i, (-2+i)(2-5i)+(3-i))\\
&= \operatorname{Div}_{\mathbb{Z}[i]}(2-5i, 3-i) \qquad \text{(by Proposition 4.2.30 \textbf{(c)})}\\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(3-i, \underbrace{2-5i}_{=(1-i)(3-i)-i}\right) \qquad \text{(by Proposition 4.2.30 \textbf{(b)})}
\end{aligned}$$

$$\begin{aligned}
&= \operatorname{Div}_{\mathbb{Z}[i]}(3-i, (1-i)(3-i)-i)\\
&= \operatorname{Div}_{\mathbb{Z}[i]}(3-i, -i) \qquad \text{(by Proposition 4.2.30 \textbf{(c)})}\\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(-i, \underbrace{3-i}_{=(1+3i)(-i)+0}\right) \qquad \text{(by Proposition 4.2.30 \textbf{(b)})}\\
&= \operatorname{Div}_{\mathbb{Z}[i]}(-i, (1+3i)(-i)+0)\\
&= \operatorname{Div}_{\mathbb{Z}[i]}(-i, 0) \qquad \text{(by Proposition 4.2.30 \textbf{(c)})}\\
&= \operatorname{Div}_{\mathbb{Z}[i]}(-i) \qquad \text{(by Proposition 4.2.30 \textbf{(a)})}\\
&= \{1, i, -1, -i\}.
\end{aligned}$$

In the same way, for **any** two Gaussian integers α and β we can find a Gaussian integer γ such that $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\gamma)$. This resulting γ will actually be unique up to multiplication by units (i.e., its unit-equivalence class will be unique). Better yet, we have the following analogue of Bezout's theorem for Gaussian integers:

Theorem 4.2.31. Let $\alpha, \beta \in \mathbb{Z}[i]$. Then:

(a) There exists a $\mathbb{Z}[i]$-linear combination γ of α and β that is a common Gaussian divisor of α and β. (Note: A $\mathbb{Z}[i]$*-linear combination of α and β* means a Gaussian integer of the form $\lambda\alpha + \mu\beta$ with $\lambda, \mu \in \mathbb{Z}[i]$.)

(b) Any such γ satisfies $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\gamma)$.

(c) The unit-equivalence class of this γ is uniquely determined.

[144] This is [ConradG, Example 4.4].

This theorem is, in a sense, a generalization of Theorem 2.9.12, even though (unlike the latter theorem) it does not rely on an already existing concept of "greatest common divisor" but rather builds the foundation for such a concept. With Theorem 4.2.31 in hand, it makes sense to call γ the "greatest common Gaussian divisor" of α and β, but rigorously speaking this name should be reserved for the unit-equivalence class of γ since γ itself is not unique.

Proof of Theorem 4.2.31 (sketched). **(a)** This is somewhat similar to the proof of Lemma 2.9.13:

For any $\alpha, \beta \in \mathbb{Z}[i]$, we let $\operatorname{Lin}_{\mathbb{Z}[i]}(\alpha, \beta)$ be the set of all $\mathbb{Z}[i]$-linear combinations of α and β. (This will be called the *$\mathbb{Z}[i]$-linear span of α and β* later on, in analogy to spans in classical linear algebra.) Now, the claim of Theorem 4.2.31 **(a)** can be restated as follows:

$$\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) \cap \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha, \beta) \neq \varnothing \qquad (154)$$

for any $\alpha, \beta \in \mathbb{Z}[i]$.

We shall prove (154) by strong induction on $\mathrm{N}(\alpha) + \mathrm{N}(\beta)$.

So we fix $n \in \mathbb{N}$, and assume as the induction hypothesis that (154) holds for all $\alpha, \beta \in \mathbb{Z}[i]$ satisfying $\mathrm{N}(\alpha) + \mathrm{N}(\beta) < n$. We must now prove (154) for all $\alpha, \beta \in \mathbb{Z}[i]$ satisfying $\mathrm{N}(\alpha) + \mathrm{N}(\beta) = n$.

So let $\alpha, \beta \in \mathbb{Z}[i]$ be such that $\mathrm{N}(\alpha) + \mathrm{N}(\beta) = n$. We must prove $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) \cap \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha, \beta) \neq \varnothing$. We can WLOG assume $\mathrm{N}(\beta) \geq \mathrm{N}(\alpha)$, since otherwise we can swap α with β without changing any of the sets $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ and $\operatorname{Lin}_{\mathbb{Z}[i]}(\alpha, \beta)$. Assume this. Furthermore, we WLOG assume that $\alpha \neq 0$ (since otherwise, the set $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) \cap \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha, \beta) = \operatorname{Div}_{\mathbb{Z}[i]}(0, \beta) \cap \operatorname{Lin}_{\mathbb{Z}[i]}(0, \beta)$ clearly contains β and thus is $\neq \varnothing$). Hence, $\mathrm{N}(\alpha) > 0$. Now, Theorem 4.2.26 (applied to β and α instead of α and β) yields that there exist Gaussian integers γ and ρ such that $\beta = \gamma\alpha + \rho$ and $\mathrm{N}(\rho) \leq \mathrm{N}(\alpha)/2$. Consider these γ and ρ. From $\beta = \gamma\alpha + \rho$, we obtain $\rho = \beta - \gamma\alpha$ and $\beta - \rho = \gamma\alpha$. From $\mathrm{N}(\rho) \leq \mathrm{N}(\alpha)/2$, we obtain

$$\mathrm{N}(\rho) \leq \mathrm{N}(\alpha)/2 < \mathrm{N}(\alpha).$$

(This is the only inequality that we will need concerning $\mathrm{N}(\rho)$. So, in a sense, the inequality $\mathrm{N}(\rho) \leq \mathrm{N}(\alpha)/2$ in Theorem 4.2.26 is better than we need it to be.)

The Gaussian integers β and ρ satisfy $\beta \equiv \rho \mod \alpha$ (since $\alpha \mid \gamma\alpha = \beta - \rho$). Hence, Proposition 4.2.30 **(d)** yields

$$\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \rho). \qquad (155)$$

Also, it is easy to see that $\operatorname{Lin}_{\mathbb{Z}[i]}(\alpha, \beta) \subseteq \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha, \rho)$ (since every $\lambda, \mu \in \mathbb{Z}[i]$ satisfy

$$\lambda\alpha + \mu \underbrace{\beta}_{=\gamma\alpha+\rho} = \lambda\alpha + \mu(\gamma\alpha + \rho) = (\lambda + \mu\gamma)\alpha + \mu\rho \in \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha, \rho)$$

) and $\operatorname{Lin}_{\mathbb{Z}[i]}(\alpha,\rho) \subseteq \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha,\beta)$ (since every $\lambda,\mu \in \mathbb{Z}[i]$ satisfy

$$\lambda\alpha + \mu \underbrace{\rho}_{=\beta-\gamma\alpha} = \lambda\alpha + \mu(\beta-\gamma\alpha) = (\lambda-\mu\gamma)\alpha + \mu\beta \in \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha,\beta)$$

). Combining these two relations, we obtain

$$\operatorname{Lin}_{\mathbb{Z}[i]}(\alpha,\beta) = \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha,\rho). \tag{156}$$

Thus,

$$\underbrace{\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta)}_{=\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\rho)} \cap \underbrace{\operatorname{Lin}_{\mathbb{Z}[i]}(\alpha,\beta)}_{=\operatorname{Lin}_{\mathbb{Z}[i]}(\alpha,\rho)} = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\rho) \cap \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha,\rho).$$

Hence, proving $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) \cap \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha,\beta) \neq \varnothing$ boils down to proving $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\rho) \cap \operatorname{Lin}_{\mathbb{Z}[i]}(\alpha,\rho) \neq \varnothing$. But this follows from the induction hypothesis (applied to ρ instead of β), since

$$\operatorname{N}(\alpha) + \underbrace{\operatorname{N}(\rho)}_{<\operatorname{N}(\alpha)\leq\operatorname{N}(\beta)} < \operatorname{N}(\alpha) + \operatorname{N}(\beta) = n.$$

This completes the induction step. Hence, (154) (and thus Theorem 4.2.31 **(a)**) follows by strong induction.

(b) We shall prove $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) \subseteq \operatorname{Div}_{\mathbb{Z}[i]}(\gamma)$ and $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) \supseteq \operatorname{Div}_{\mathbb{Z}[i]}(\gamma)$ separately:

$\subseteq$: Since γ is a $\mathbb{Z}[i]$-linear combination of α and β, every common Gaussian divisor of α and β must also divide γ. Thus, $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) \subseteq \operatorname{Div}_{\mathbb{Z}[i]}(\gamma)$.

$\supseteq$: Since γ is a common Gaussian divisor of α and β, every Gaussian divisor of γ must be a common Gaussian divisor of α and β. Thus, $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) \supseteq \operatorname{Div}_{\mathbb{Z}[i]}(\gamma)$.

(c) Let γ_1 and γ_2 be two such γ's. We must prove that $\gamma_1 \sim \gamma_2$.

We have $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\gamma_1)$ and $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\gamma_2)$. Comparing these two equalities, we obtain $\operatorname{Div}_{\mathbb{Z}[i]}(\gamma_1) = \operatorname{Div}_{\mathbb{Z}[i]}(\gamma_2)$. Now, $\gamma_1 \in \operatorname{Div}_{\mathbb{Z}[i]}(\gamma_1) = \operatorname{Div}_{\mathbb{Z}[i]}(\gamma_2)$, thus $\gamma_1 \mid \gamma_2$. Similarly, $\gamma_2 \mid \gamma_1$. Combining these, we obtain $\gamma_1 \sim \gamma_2$ (by Exercise 4.2.2). This proves Theorem 4.2.31 **(c)**. □

Definition 4.2.32. The *greatest common Gaussian divisor* (or, short, *gcd*) of two Gaussian integers α and β is defined to be the γ from Theorem 4.2.31 **(a)**. It is called $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$.

So it is a common Gaussian divisor of α and β and also a $\mathbb{Z}[i]$-linear combination of α and β and satisfies

$$\operatorname{Div}_{\mathbb{Z}[i]}\left(\gcd_{\mathbb{Z}[i]}(\alpha,\beta)\right) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta). \tag{157}$$

However, it is only well-defined up to unit-equivalence. Thus, if you have $\gamma_1 = \gcd_{\mathbb{Z}[i]}(\alpha,\beta)$ and $\gamma_2 = \gcd_{\mathbb{Z}[i]}(\alpha,\beta)$, then you cannot conclude that $\gamma_1 = \gamma_2$

(you can only conclude $\gamma_1 \sim \gamma_2$). So, strictly speaking, we should have defined $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$ as a unit-equivalence class, not as a concrete Gaussian integer. But we will allow ourselves this abuse of notation. We shall not write equality signs like the one in "$\gamma_1 = \gcd_{\mathbb{Z}[i]}(\alpha,\beta)$", however; we instead prefer to write "$\gamma_1 \sim \gcd_{\mathbb{Z}[i]}(\alpha,\beta)$". Generally, whenever you see $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$ in a statement, you should be understanding the statement to hold for **every** possible choice of $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$.

Proposition 4.2.33. Let a and b be two integers. Then,

$$\gcd(a,b) \sim \gcd_{\mathbb{Z}[i]}(a,b).$$

(Of course, the gcd on the left hand side is the gcd of the two integers a and b as defined in Definition 2.9.6, whereas the $\gcd_{\mathbb{Z}[i]}$ on the right hand side is the greatest common Gaussian divisor of the Gaussian integers a and b.)

Proof of Proposition 4.2.33. The integer $\gcd(a,b)$ is a common divisor of a and b and also is a $\mathbb{Z}$-linear combination of a and b (by Bezout's theorem). Therefore, it is also a common Gaussian divisor of the Gaussian integers a and b and also is a $\mathbb{Z}[i]$-linear combination of a and b. But this yields that it is $\gcd_{\mathbb{Z}[i]}(a,b)$ (due to the definition of $\gcd_{\mathbb{Z}[i]}(a,b)$). □

This proposition allows us to write "gcd" for both concepts of gcd without having to disambiguate the meaning. (We shall not do so, however.)

Proposition 4.2.34. Let α and β be two Gaussian integers, not both equal to 0. Then, the possible values of $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$ (that is, strictly speaking, all four elements of the unit-equivalence class $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$) are exactly the elements of $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta)$ having the largest norm.

Proof. First of all, $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$ is a common Gaussian divisor of α and β, and thus is $\neq 0$ (since α and β are not both equal to 0). Thus, there are exactly four Gaussian integers unit-equivalent to $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$. In other words, there are exactly four possible values of $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$. We must show that these values are exactly the elements of $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta)$ having the largest norm.

In other words, we must show the following two claims:

Claim 1: We have $\operatorname{N}\left(\gcd_{\mathbb{Z}[i]}(\alpha,\beta)\right) > \operatorname{N}(\gamma)$ for each $\gamma \in \operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta)$ that does not satisfy $\gamma \sim \gcd_{\mathbb{Z}[i]}(\alpha,\beta)$.

Claim 2: We have $\operatorname{N}\left(\gcd_{\mathbb{Z}[i]}(\alpha,\beta)\right) = \operatorname{N}(\gamma)$ for each $\gamma \in \operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta)$ that does satisfy $\gamma \sim \gcd_{\mathbb{Z}[i]}(\alpha,\beta)$.

Claim 2 is obvious, since any two unit-equivalent Gaussian integers have the same norm (by Proposition 4.2.15).

[*Proof of Claim 1:* Let $\gamma \in \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ do not satisfy $\gamma \sim \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$. Now, $\gamma \in \operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta) = \operatorname{Div}_{\mathbb{Z}[i]}\left(\gcd_{\mathbb{Z}[i]}(\alpha, \beta)\right)$ (by (157)). Hence, $\gamma \mid \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$.

Let us set $\delta = \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$. So $\gamma \mid \delta$. We have $\delta \neq 0$ (because α and β are not both zero) and thus $\gamma \neq 0$ (since $\gamma \mid \delta$). Thus, $\gamma \mid \delta$ yields that $\frac{\delta}{\gamma}$ is a Gaussian integer, which is furthermore nonzero (since $\delta \neq 0$). If this Gaussian integer $\frac{\delta}{\gamma}$ was a unit, then we would have $\gamma \sim \delta = \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$, which would contradict the assumption that γ does not satisfy $\gamma \sim \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$. So $\frac{\delta}{\gamma}$ is a nonzero Gaussian integer that is not a unit. Hence, $\operatorname{N}\left(\frac{\delta}{\gamma}\right) > 1$ (because Proposition 4.2.9 yields that every nonzero Gaussian integer that is not a unit must have norm > 1). Now,

$$\operatorname{N}(\delta) = \underbrace{\operatorname{N}\left(\frac{\delta}{\gamma}\right)}_{>1} \cdot \operatorname{N}(\gamma) > \operatorname{N}(\gamma).$$

In other words, $\operatorname{N}\left(\gcd_{\mathbb{Z}[i]}(\alpha, \beta)\right) > \operatorname{N}(\gamma)$. This proves Claim 1.] □

Proposition 4.2.34 shows that $\gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ is uniquely determined by the set $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$. (Yes, you have to consider the case $\alpha = \beta = 0$ separately in proving this.) Hence, Proposition 4.2.30 yields:

Proposition 4.2.35. **(a)** We have $\gcd_{\mathbb{Z}[i]}(\alpha, 0) \sim \gcd_{\mathbb{Z}[i]}(\alpha)$ for all $\alpha \in \mathbb{Z}[i]$.

(b) We have $\gcd_{\mathbb{Z}[i]}(\alpha, \beta) \sim \gcd_{\mathbb{Z}[i]}(\beta, \alpha)$ for all $\alpha, \beta \in \mathbb{Z}[i]$.

(c) We have $\gcd_{\mathbb{Z}[i]}(\alpha, \eta\alpha + \beta) \sim \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ for all $\alpha, \beta, \eta \in \mathbb{Z}[i]$.

(d) If $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ satisfy $\beta \equiv \gamma \bmod \alpha$, then $\gcd_{\mathbb{Z}[i]}(\alpha, \beta) \sim \gcd_{\mathbb{Z}[i]}(\alpha, \gamma)$.

(g) We have $\gcd_{\mathbb{Z}[i]}(\eta\alpha, \beta) \sim \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$ and every unit $\eta \in \mathbb{Z}[i]$.

(h) We have $\gcd_{\mathbb{Z}[i]}(\alpha, \eta\beta) \sim \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$ and every unit $\eta \in \mathbb{Z}[i]$.

(i) If $\alpha, \beta \in \mathbb{Z}[i]$ satisfy $\alpha \mid \beta$, then $\gcd_{\mathbb{Z}[i]}(\alpha, \beta) \sim \gcd_{\mathbb{Z}[i]}(\alpha)$.

(j) The greatest common Gaussian divisor of the empty list of Gaussian integers is $\gcd_{\mathbb{Z}[i]}() = 0$.

Theorem 2.9.15 still holds for Gaussian integers.
Theorem 2.9.17 still holds for Gaussian integers.
Theorem 2.9.19 still holds for Gaussian integers.
Theorem 2.9.20 has to be modified as follows:

Corollary 4.2.36. Let $\sigma, \alpha, \beta \in \mathbb{Z}[i]$. Then,

$$\gcd_{\mathbb{Z}[i]}(\sigma\alpha, \sigma\beta) \sim \sigma \gcd_{\mathbb{Z}[i]}(\alpha, \beta).$$

Exercise 2.9.4 still holds for Gaussian integers.

Exercise 2.9.5 becomes the claim that if $\alpha_1 \sim \alpha_2$ and $\beta_1 \sim \beta_2$, then $\gcd_{\mathbb{Z}[i]}(\alpha_1, \beta_1) \sim \gcd_{\mathbb{Z}[i]}(\alpha_2, \beta_2)$. The solution does not carry over, but you can easily prove this new claim by hand.

Greatest common Gaussian divisors of k Gaussian integers can also be defined.

The next definition is an analogue of Definition 2.10.1:

Definition 4.2.37. Let α and β be two Gaussian integers. We say that α is *coprime* to β if and only if $\gcd_{\mathbb{Z}[i]}(\alpha, \beta) \sim 1$ (that is, $\gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ is a unit).

Thus, any two coprime integers are also two coprime Gaussian integers (because of Proposition 4.2.33), and vice versa (for the same reason). This is why we can afford speaking of "coprime Gaussian integers" and not just "Gaussian-coprime Gaussian integers".

Everything we said about coprimality of integers still holds for Gaussian integers. In particular, Proposition 2.10.4, Theorem 2.10.6, Theorem 2.10.7, Theorem 2.10.8 and Theorem 2.10.9 still hold if all integers are replaced by Gaussian integers (with the caveat that the gcd is no longer unique, so for example "$ab \equiv \gcd(a, n) \bmod n$" must be interpreted as "ab is congruent to **some** of the possible values of $\gcd_{\mathbb{Z}[i]}(a, n)$ modulo n").

We could define *Gaussian rationals* (their set is called $\mathbb{Q}[i]$) as complex numbers $a + bi$ with $a, b \in \mathbb{Q}$. These are exactly the quotients of Gaussian integers.

Lowest common multiples of Gaussian integers still exist, but their definition has to be modified. For example, we can define $\operatorname{lcm}_{\mathbb{Z}[i]}(\alpha, \beta)$ as the (unique up to unit-equivalence) Gaussian integer γ such that the Gaussian common multiples of α and β are the Gaussian multiples of γ. (We would have to prove that it actually is unique and exists.) Theorem 2.11.6 still holds, in the sense that $\gcd_{\mathbb{Z}[i]}(\alpha, \beta) \cdot \operatorname{lcm}_{\mathbb{Z}[i]}(\alpha, \beta) \sim \alpha\beta$. Many other properties of lowest common multiples extend to Gaussian integers.

The Chinese remainder theorem (Theorem 2.12.1) still holds for coprime Gaussian integers μ and ν. A similar fact holds for k mutually coprime Gaussian integers.

4.2.6. Gaussian primes

The next definition is an analogue of Definition 2.13.1:

Definition 4.2.38. Let π be a nonzero Gaussian integer that is not a unit. We say that π is a *Gaussian prime* if each Gaussian divisor of π is either a unit or unit-equivalent to π.

The letter "π" in this definition is unrelated to the irrational number $\pi = 3.14159\ldots$. It just happens to be the Greek letter corresponding to the Roman "p".

The Gaussian primes are **not** a superset of the primes. For example:

Example 4.2.39. The Gaussian integer 2 is not a Gaussian prime.

Proof. We have $2 = (1+i)(1-i)$. The factors $1+i$ and $1-i$ have norms 2, which means that they are neither units themselves (since units would have norm 1) nor unit-equivalent to 2 (since 2 has norm 4, but unit-equivalent Gaussian integers have equal norms). Thus, $1+i$ is a Gaussian divisor of 2 that is neither a unit nor is unit-equivalent to 2. Hence, 2 is not a Gaussian prime (by the definition of "Gaussian prime"). □

So don't forget the word "Gaussian" when you mean it!

Let us search for Gaussian primes. So we know that 2 is not a Gaussian prime. What about 3?

Example 4.2.40. The Gaussian integer 3 is a Gaussian prime.

Proof of Example 4.2.40. Assume the contrary. Thus, there exists a Gaussian divisor α of 3 that is neither a unit nor unit-equivalent to 3 (since 3 is a nonzero Gaussian integer that is not a unit). Consider this α. Then, α is a Gaussian integer and satisfies $\alpha \mid 3$ (since α is a Gaussian divisor of 3). Hence, Proposition 4.2.19 **(a)** (applied to $\beta = 3$) yields $\operatorname{N}(\alpha) \mid \operatorname{N}(3) = 3^2 + 0^2 = 9$. Also, $\operatorname{N}(\alpha) \in \mathbb{N}$ (by Proposition 4.2.6). Hence, $\operatorname{N}(\alpha)$ is a nonnegative integer. Thus, $\operatorname{N}(\alpha)$ is a nonnegative divisor of 9 (because $\operatorname{N}(\alpha) \mid 9$).

If we had $\operatorname{N}(\alpha) = \operatorname{N}(3)$, then we would have $\alpha \sim 3$ (by Exercise 4.2.9, applied to $\beta = 3$); but this would contradict the fact that α is not unit-equivalent to 3. Hence, we cannot have $\operatorname{N}(\alpha) = \operatorname{N}(3)$. Thus, we have $\operatorname{N}(\alpha) \neq \operatorname{N}(3) = 9$.

If we had $\operatorname{N}(\alpha) = 1$, then α would be a unit (by Proposition 4.2.9 **(b)**); but this would contradict the fact that α is not a unit. Hence, we cannot have $\operatorname{N}(\alpha) = 1$. Thus, we have $\operatorname{N}(\alpha) \neq 1$.

But the only nonnegative divisors of 9 are $1, 3, 9$. Hence, $\operatorname{N}(\alpha)$ must be either 1 or 3 or 9 (since $\operatorname{N}(\alpha)$ is a nonnegative divisor of 9). Since we have shown that $\operatorname{N}(\alpha) \neq 1$ and $\operatorname{N}(\alpha) \neq 9$, we thus conclude that $\operatorname{N}(\alpha) = 3$.

But let us write the Gaussian integer α as (a, b) for some $a, b \in \mathbb{Z}$. Thus, $\operatorname{N}(\alpha) = a^2 + b^2$, so that $a^2 + b^2 = \operatorname{N}(\alpha) = 3 \equiv 3 \bmod 4$. This contradicts Exercise 2.7.2 **(c)**. This contradiction shows that our assumption was false. So 3 is a Gaussian prime. □

So we know that 3 is a Gaussian prime, but 2 is not. Is there a way to tell which integers are Gaussian primes, without checking all Gaussian divisors?

Let us first state a positive criterion, which generalizes Example 4.2.40:

Lemma 4.2.41. Let p be a prime such that $p \equiv 3 \bmod 4$. Then, p is a Gaussian prime.

Proof of Lemma 4.2.41. Assume the contrary. Thus, there exists a Gaussian divisor α of p that is neither a unit nor unit-equivalent to p (since p is a nonzero Gaussian integer that is not a unit[145]). Consider this α. Then, α is a Gaussian integer and satisfies $\alpha \mid p$ (since α is a Gaussian divisor of p). Hence, Proposition 4.2.19 **(a)** (applied to $\beta = p$) yields $\mathrm{N}(\alpha) \mid \mathrm{N}(p) = p^2 + 0^2 = p^2$. Also, $\mathrm{N}(\alpha) \in \mathbb{N}$ (by Proposition 4.2.6). Hence, $\mathrm{N}(\alpha)$ is a nonnegative integer. Thus, $\mathrm{N}(\alpha)$ is a nonnegative divisor of p^2 (because $\mathrm{N}(\alpha) \mid p^2$).

If we had $\mathrm{N}(\alpha) = \mathrm{N}(p)$, then we would have $\alpha \sim p$ (by Exercise 4.2.9, applied to $\beta = p$); but this would contradict the fact that α is not unit-equivalent to p. Hence, we cannot have $\mathrm{N}(\alpha) = \mathrm{N}(p)$. Thus, we have $\mathrm{N}(\alpha) \neq \mathrm{N}(p) = p^2$.

If we had $\mathrm{N}(\alpha) = 1$, then α would be a unit (by Proposition 4.2.9 **(b)**); but this would contradict the fact that α is not a unit. Hence, we cannot have $\mathrm{N}(\alpha) = 1$. Thus, we have $\mathrm{N}(\alpha) \neq 1$.

But the only nonnegative divisors of p^2 are $1, p, p^2$ (indeed, this follows by applying Exercise 2.13.13 to $k = 2$). Hence, $\mathrm{N}(\alpha)$ must be either 1 or p or p^2 (since $\mathrm{N}(\alpha)$ is a nonnegative divisor of p^2). Since we have shown that $\mathrm{N}(\alpha) \neq 1$ and $\mathrm{N}(\alpha) \neq p^2$, we thus conclude that $\mathrm{N}(\alpha) = p$.

But let us write the Gaussian integer α as (a, b) for some $a, b \in \mathbb{Z}$. Thus, $\mathrm{N}(\alpha) = a^2 + b^2$, so that $a^2 + b^2 = \mathrm{N}(\alpha) = p \equiv 3 \bmod 4$. This contradicts Exercise 2.7.2 **(c)**. This contradiction shows that our assumption was false. Thus, Lemma 4.2.41 is proven. □

It is clear that no prime is divisible by 4. Thus, there are three types of primes:

- *Type 1:* Primes that are $\equiv 1 \bmod 4$: these are $5, 13, 17, 29, \ldots$.
- *Type 2:* Primes that are even: there is only one of these, namely 2.
- *Type 3:* Primes that are $\equiv 3 \bmod 4$: these are $3, 7, 11, 19, 23, \ldots$.

(One can show that there are infinitely many primes of Type 1 and infinitely many primes of Type 3. It can also be shown that there are "roughly the same amount" of Type-1 primes and of Type-3 primes "in theory", but "in practice" the Type-3 primes are more frequent. For the concrete meaning of this weird paradoxical claim, google for "Chebyshev's bias".)

Lemma 4.2.41 says that all Type-3 primes are Gaussian primes. What about the other primes – are they Gaussian primes? We already know that 2 is not, since $2 = (1+i)(1-i)$. Likewise, 5 is not, since $5 = (1+2i)(1-2i)$. Likewise, 13 is not, since $13 = (2+3i)(2-3i)$.

[145] Why is p not a unit? Because the units are $1, -1, i, -i$, and none of these numbers is p.

This may suggest that primes p satisfying $p = 2$ or $p \equiv 1 \bmod 4$ (that is, primes of Type 1 or Type 2) not only factor nontrivially, but actually factor as

$$p = (x + yi)(x - yi) \qquad \text{for some integers } x \text{ and } y.$$

Of course, this equation rewrites as $p = x^2 + y^2$. Thus, we are back to asking Question 1.4.1, at least for primes.

We shall now answer this question, and actually prove a bit more:

Theorem 4.2.42. Let p be a prime such that either $p = 2$ or $p \equiv 1 \bmod 4$.

(a) There exist integers x and y such that $p = x^2 + y^2$.

(b) If $p \equiv 1 \bmod 4$, then there exist exactly 8 pairs (x, y) of integers such that $p = x^2 + y^2$. (For example, if $p = 5$, then these 8 pairs are $(1, 2)$, $(2, 1)$, $(1, -2)$, $(-2, 1)$, $(-1, 2)$, $(2, -1)$, $(-1, -2)$ and $(-2, -1)$.)

(c) There exists a Gaussian prime π such that $p = \pi\overline{\pi}$.

(d) The Gaussian integer p itself is not a Gaussian prime.

(e) Assume that $p \equiv 1 \bmod 4$. Consider the Gaussian prime π from Theorem 4.2.42 **(c)**. Then, $\overline{\pi}$ is also a Gaussian prime, and we do not have $\pi \sim \overline{\pi}$.

For example, the Type-1 prime 17 satisfies

$$\begin{aligned} 17 &= 1^2 + 4^2 = (1 + 4i)(1 - 4i) = (1 + 4i)\left(\overline{1 + 4i}\right) \\ &= (1 - 4i)\left(\overline{1 - 4i}\right) = (4 + i)\left(\overline{4 + i}\right). \end{aligned}$$

Note that the claim of Theorem 4.2.42 **(a)** (at least for $p \neq 2$) also appears in [AigZie18, Proposition in Chapter 4], with a very different proof.

Before we can prove Theorem 4.2.42, we will have to build up the theory of Gaussian primes a bit more. We first state the Gaussian-integer analogue of Proposition 2.13.5:

Proposition 4.2.43. Let π be a Gaussian prime. Let $\alpha \in \mathbb{Z}[i]$. Then, either $\pi \mid \alpha$ or $\pi \perp \alpha$.

Proof of Proposition 4.2.43. Analogous to our proof of Proposition 2.13.5 above. □

Next, we state the analogue to Theorem 2.13.6:

Theorem 4.2.44. Let π be a Gaussian prime. Let $\alpha, \beta \in \mathbb{Z}[i]$ such that $\pi \mid \alpha\beta$. Then, $\pi \mid \alpha$ or $\pi \mid \beta$.

Proof of Theorem 4.2.44. Analogous to our proof of Theorem 2.13.6 above. □

We also need the following simple fact:

Lemma 4.2.45. Let α be a Gaussian integer. If $\operatorname{N}(\alpha)$ is prime, then α is a Gaussian prime.

This shows, for example, that $1+i$ and $1+2i$ are Gaussian primes. The converse of Lemma 4.2.45 does not hold (e.g., since 3 is a Gaussian prime, but $\operatorname{N}(3) = 9$ is not prime).

Proof of Lemma 4.2.45. Assume that $\operatorname{N}(\alpha)$ is prime. We must prove that α is a Gaussian prime.

Assume the contrary. Thus, α is not a Gaussian prime, but α is neither zero nor a unit (since $\operatorname{N}(\alpha)$ is prime and therefore > 1). Hence, α has a Gaussian divisor δ that is neither a unit nor unit-equivalent to α. Consider this δ.

Now, δ is a Gaussian divisor of α; in other words, δ is a Gaussian integer and satisfies $\delta \mid \alpha$. Hence, Proposition 4.2.19 **(a)** (applied to δ and α instead of α and β) yields $\operatorname{N}(\delta) \mid \operatorname{N}(\alpha)$. Also, $\operatorname{N}(\delta) \in \mathbb{N}$ (by Proposition 4.2.6, applied to δ instead of α). Hence, $\operatorname{N}(\delta)$ is a nonnegative integer. Thus, $\operatorname{N}(\delta)$ is a nonnegative divisor of $\operatorname{N}(\alpha)$ (because $\operatorname{N}(\delta) \mid \operatorname{N}(\alpha)$). But the only nonnegative divisors of $\operatorname{N}(\alpha)$ are 1 and $\operatorname{N}(\alpha)$ [146]. Thus, $\operatorname{N}(\delta)$ equals either 1 or $\operatorname{N}(\alpha)$ (since $\operatorname{N}(\delta)$ is a nonnegative divisor of $\operatorname{N}(\alpha)$). But if we had $\operatorname{N}(\delta) = 1$, then δ would be a unit, which is impossible (by the definition of δ). Thus, we cannot have $\operatorname{N}(\delta) = 1$. Hence, we must have $\operatorname{N}(\delta) = \operatorname{N}(\alpha)$ (since $\operatorname{N}(\delta)$ equals either 1 or $\operatorname{N}(\alpha)$). Hence, Exercise 4.2.9 (applied to δ and α instead of α and β) shows that $\delta \sim \alpha$. This contradicts the assumption that δ is not unit-equivalent to α. This contradiction proves that our assumption was wrong. Lemma 4.2.45 is proven. □

Next, let us show that conjugation does not change Gaussian primeness:

Lemma 4.2.46. Let π be a Gaussian prime. Then, $\overline{\pi}$ is a Gaussian prime, too.

Proof of Lemma 4.2.46. Conjugation (of complex numbers) sends Gaussian integers to Gaussian integers (by Proposition 4.2.5), products to products (by Proposition 4.1.27 **(c)**) and inverses to inverses (i.e., we have $\overline{\alpha^{-1}} = \overline{\alpha}^{-1}$ whenever $\alpha \in \mathbb{C}$ is nonzero). Furthermore, it is an involution (since $\overline{\overline{\alpha}} = \alpha$ for each $\alpha \in \mathbb{C}$). Thus, conjugation preserves all "intrinsic" properties of Gaussian integers; for example:

- If π is nonzero, then $\overline{\pi}$ is nonzero, and vice versa.
- If π is not a unit, then $\overline{\pi}$ is not a unit, and vice versa.
- If δ is a Gaussian divisor of π, then $\overline{\delta}$ is a Gaussian divisor of $\overline{\pi}$, and vice versa.

[146] *Proof.* The only positive divisors of $\operatorname{N}(\alpha)$ are 1 and $\operatorname{N}(\alpha)$ (since $\operatorname{N}(\alpha)$ is prime). Hence, the only nonnegative divisors of $\operatorname{N}(\alpha)$ are 1 and $\operatorname{N}(\alpha)$ and possibly 0. But since 0 is not a nonnegative divisor of $\operatorname{N}(\alpha)$ (indeed, if it was, then $\operatorname{N}(\alpha)$ would be a multiple of 0 and therefore equal to 0, which would contradict the fact that $\operatorname{N}(\alpha)$ is prime), this yields that the only nonnegative divisors of $\operatorname{N}(\alpha)$ are 1 and $\operatorname{N}(\alpha)$.

- If δ is not a unit, then $\overline{\delta}$ is not a unit, and vice versa.
- If δ is not unit-equivalent to π, then $\overline{\delta}$ is not unit-equivalent to $\overline{\pi}$, and vice versa.

(These facts are straightforward to prove; see, for example, Exercise 4.2.7 for a proof of the third one.)

Hence, if you compare what it means for π to be a Gaussian prime with what it means for $\overline{\pi}$ to be a Gaussian prime, then you will see that it means the same thing. This proves Lemma 4.2.46. □

Now, we can prove Theorem 4.2.42:

Proof of Theorem 4.2.42. **(d)** Assume the contrary. Thus, p is a Gaussian prime. But 2 is not a Gaussian prime (by Example 4.2.39). Hence, $p \neq 2$. Thus, $p \equiv 1 \operatorname{mod} 4$ (since we assumed that either $p = 2$ or $p \equiv 1 \operatorname{mod} 4$). Therefore, $p = 2k+1$ for some **even** $k \in \mathbb{N}$. Consider this k.

Exercise 2.15.5 yields $k!^2 \equiv - \underbrace{(-1)^k}_{\substack{=1 \\ \text{(since } k \text{ is even)}}} = -1 \operatorname{mod} p$. Set $u = k!$; thus, this becomes $u^2 \equiv -1 \operatorname{mod} p$. In other words,

$$p \mid u^2 - (-1) = u^2 - i^2 = (u+i)(u-i).$$

This is a divisibility in $\mathbb{Z}$, thus also a divisibility in $\mathbb{Z}[i]$.

Hence, Theorem 4.2.44 (applied to $\pi = p$, $\alpha = u+i$ and $\beta = u-i$) yields that $p \mid u+i$ or $p \mid u-i$ (since p is a Gaussian prime). But if $p \mid u-i$, then $p \mid u+i$ holds as well (since Exercise 4.2.7 shows that $p \mid u-i$ implies $\overline{p} \mid \overline{u-i} = u+i$, which means $p = \overline{p} \mid u+i$). Hence, we have $p \mid u+i$ in both cases.

This means that there exists a Gaussian integer γ such that $u+i = p\gamma$. Consider this γ. Write γ as $\gamma = (a,b)$ with $a,b \in \mathbb{Z}$. Then, $(u,1) = u+i = p \underbrace{\gamma}_{=(a,b)} = p(a,b) = (pa,pb)$. Thus, $u = pa$ and $1 = pb$. But $1 = pb$ leads to $p \mid 1$ in $\mathbb{Z}$ (since $b \in \mathbb{Z}$), which is absurd (since p is prime). This contradiction shows that our assumption was wrong. Thus, Theorem 4.2.42 **(d)** is proven.

(a) We have $\operatorname{N}(p) = p^2 + 0^2 = p^2 > 1$ (since $p > 1$). Thus, p is nonzero and not a unit. But Theorem 4.2.42 **(d)** shows that p is not a Gaussian prime. Since p is nonzero and not a unit, this shows that p has a Gaussian divisor δ that is neither a unit nor unit-equivalent to p. Consider this δ. Then, δ is a Gaussian integer and satisfies $\delta \mid p$ (since δ is a Gaussian divisor of p). Hence, Proposition 4.2.19 **(a)** (applied to $\alpha = \delta$ and $\beta = p$) yields $\operatorname{N}(\delta) \mid \operatorname{N}(p) = p^2 + 0^2 = p^2$. Also, $\operatorname{N}(\delta) \in \mathbb{N}$ (by Proposition 4.2.6, applied to $\alpha = \delta$). Hence, $\operatorname{N}(\delta)$ is a nonnegative integer. Thus, $\operatorname{N}(\delta)$ is a nonnegative divisor of p^2 (because $\operatorname{N}(\delta) \mid p^2$).

If we had $\operatorname{N}(\delta) = \operatorname{N}(p)$, then we would have $\delta \sim p$ (by Exercise 4.2.9, applied to $\alpha = \delta$ and $\beta = p$); but this would contradict the fact that δ is not unit-equivalent to p. Hence, we cannot have $\operatorname{N}(\delta) = \operatorname{N}(p)$. Thus, we have $\operatorname{N}(\delta) \neq \operatorname{N}(p) = p^2$.

If we had $\operatorname{N}(\delta) = 1$, then δ would be a unit (by Proposition 4.2.9 **(b)**, applied to $\alpha = \delta$); but this would contradict the fact that δ is not a unit. Hence, we cannot have $\operatorname{N}(\delta) = 1$. Thus, we have $\operatorname{N}(\delta) \neq 1$.

But the only nonnegative divisors of p^2 are $1, p, p^2$ (indeed, this follows by applying Exercise 2.13.13 to $k = 2$). Hence, $\operatorname{N}(\delta)$ must be either 1 or p or p^2 (since $\operatorname{N}(\delta)$ is a nonnegative divisor of p^2). Since we have shown that $\operatorname{N}(\delta) \neq 1$ and $\operatorname{N}(\delta) \neq p^2$, we thus conclude that $\operatorname{N}(\delta) = p$.

But let us write the Gaussian integer δ as (a, b) for some $a, b \in \mathbb{Z}$. Thus, $\operatorname{N}(\delta) = a^2 + b^2$, so that $a^2 + b^2 = \operatorname{N}(\delta) = p$. Hence, there exist integers x and y such that $p = x^2 + y^2$ (namely, $x = a$ and $y = b$). This proves Theorem 4.2.42 **(a)**.

(c) Theorem 4.2.42 **(a)** shows that there exist integers x and y such that $p = x^2 + y^2$. Consider these x and y. Let π be the Gaussian integer $x + iy$. Then, $\pi\overline{\pi} = (x + iy)\left(\overline{x + iy}\right) = x^2 + y^2 = p$. Thus, $p = \pi\overline{\pi}$. It remains to prove that π is a Gaussian prime.

The norm of π is $\operatorname{N}(\pi) = x^2 + y^2 = p$, which is prime. Hence, Lemma 4.2.45 (applied to $\alpha = \pi$) shows that π is a Gaussian prime. This completes the proof of Theorem 4.2.42 **(c)**.

(b) Assume that $p \equiv 1 \bmod 4$. We must prove that there exist exactly 8 pairs (x, y) of integers such that $p = x^2 + y^2$.

One such pair is provided by Theorem 4.2.42 **(a)**. Let us call it (a, b). To get the other 7, we notice that it must satisfy $a \neq 0$ (since p is not a perfect square) and $b \neq 0$ (for the same reason) and $a \neq b$ (since p is not $2n^2$ for any $n \in \mathbb{Z}$). Thus, the 8 pairs

$$\begin{array}{cccc} (a,b), & (b,a), & (a,-b), & (-b,a), \\ (-a,b), & (b,-a), & (-a,-b), & (-b,-a) \end{array}$$

are all distinct. Each of these 8 distinct pairs is a pair (x, y) of integers such that $p = x^2 + y^2$ (because $p = a^2 + b^2 = b^2 + a^2 = a^2 + (-b)^2$ etc.).

It thus remains to prove that these 8 pairs are the **only** pairs (x, y) of integers such that $p = x^2 + y^2$.

In other words, we need to prove that if (x, y) is a pair of integers such that $p = x^2 + y^2$, then (x, y) is one of the above 8 pairs. So let us fix a pair (x, y) of integers such that $p = x^2 + y^2$. We must prove that (x, y) is one of the above 8 pairs. In other words, we must prove that (x, y) equals (a, b) up to order and signs. This is equivalent to proving that $x + yi \sim a + bi$ or $x - yi \sim a + bi$.

Set $\pi = x + yi$ and $\alpha = a + bi$. Then, π and α are Gaussian integers having norms $\operatorname{N}(\pi) = x^2 + y^2 = p$ and $\operatorname{N}(\alpha) = a^2 + b^2 = p$ (by the definition of (a, b)). Thus, $\operatorname{N}(\alpha) = p$ is prime. Hence, Lemma 4.2.45 shows that α is a Gaussian prime. Similarly, π is a Gaussian prime.

We must prove that $x + yi \sim a + bi$ or $x - yi \sim a + bi$. In other words, we must prove that $\pi \sim \alpha$ or $\overline{\pi} \sim \alpha$ (since $x + yi = \pi$ and $x - yi = \overline{\pi}$ and $a + bi = \alpha$).

Now,

$$\alpha = a + bi \mid (a + bi)(a - bi) = a^2 + b^2 = p = \operatorname{N}(\pi) = \pi\overline{\pi}.$$

Since α is a Gaussian prime, this yields that $\alpha \mid \pi$ or $\alpha \mid \overline{\pi}$ (by Theorem 4.2.44). Thus, we are in one of the following two Cases:

Case 1: We have $\alpha \mid \pi$.

Case 2: We have $\alpha \mid \overline{\pi}$.

In Case 1, we have $\alpha \mid \pi$. In other words, there exists a Gaussian integer ξ such that $\pi = \alpha\xi$. Consider this ξ. We have $\pi = \alpha\xi$, thus $\operatorname{N}(\pi) = \operatorname{N}(\alpha\xi) = \operatorname{N}(\alpha)\operatorname{N}(\xi)$. Since both $\operatorname{N}(\pi)$ and $\operatorname{N}(\alpha)$ are p (because $\operatorname{N}(\pi) = x^2 + y^2 = p$ and $\operatorname{N}(\alpha) = a^2 + b^2 = p$), this rewrites as $p = p\operatorname{N}(\xi)$. We can cancel p from this equality, and obtain $\operatorname{N}(\xi) = 1$. Hence, ξ is a unit. Therefore, $\pi = \alpha\xi$ yields $\pi \sim \alpha$. In other words, $x + yi \sim a + bi$ (since $\pi = x + yi$ and $\alpha = a + bi$).

In Case 2, we similarly obtain $x - yi \sim a + bi$ (since $\operatorname{N}(\overline{\pi}) = \operatorname{N}(\pi) = x^2 + y^2 = p$ and $\overline{\pi} = x - yi$).

Hence, in both Cases, we have proven that $x + yi \sim a + bi$ or $x - yi \sim a + bi$. This completes our proof of Theorem 4.2.42 **(b)**.

(e) Lemma 4.2.46 yields that $\overline{\pi}$ is a Gaussian prime. It remains to prove that we do not have $\pi \sim \overline{\pi}$.

Assume the contrary. Thus, $\pi \sim \overline{\pi}$. Hence, Exercise 4.2.1 **(c)** (applied to π instead of α) yields that the norm $\operatorname{N}(\pi)$ cannot be an odd prime. In view of $\operatorname{N}(\pi) = \pi\overline{\pi} = p$, this rewrites as follows: p cannot be an odd prime.

But p is odd (since $p \equiv 1 \bmod 4$) and prime. In other words, p is an odd prime. This contradicts the fact that p cannot be an odd prime. This contradiction shows that our assumption was false. Thus, the proof of Theorem 4.2.42 **(e)** is complete. □

We have thus answered Question 1.4.2 **(b)** in the case when n is a prime: We have shown that a prime p is a sum of two perfect squares if and only if either $p = 2$ or $p \equiv 1 \bmod 4$; and we have shown that the number of pairs $(x, y) \in \mathbb{Z}^2$ satisfying $p = x^2 + y^2$ is 8 when $p \equiv 1 \bmod 4$ and is 4 when $p = 2$ (the latter claim is easy to check).

What about the case of arbitrary n?

For $n = 21$, we have $n \equiv 1 \bmod 4$, but n is not a sum of two perfect squares. So the answer we gave for the case of prime n does not generalize to arbitrary n.

It turns out that the right answer for arbitrary n will come from the analogue of prime factorization in $\mathbb{Z}[i]$.

Proposition 4.2.47. Let ν be a nonzero Gaussian integer that is not a unit. Then, there exists at least one Gaussian prime π such that $\pi \mid \nu$.

Proof of Proposition 4.2.47. This is an analogue of Proposition 2.13.8, and can be proven in the same way. Just replace d (the smallest positive divisor of n) by δ (a Gaussian divisor of ν that is not a unit and has the smallest norm among all such divisors). □

Proposition 4.2.48. Let ν be a nonzero Gaussian integer. Then, ν is unit-equivalent to a certain product of finitely many Gaussian primes.

Proof of Proposition 4.2.48. This is an analogue of Proposition 2.13.10, and can be proven in the same way: Strong induction on $\mathrm{N}(\nu)$. The main difference is that the case of $\mathrm{N}(\nu) = 1$ leads to ν being a unit (hence unit-equivalent to an empty product of Gaussian primes) rather than ν being 1. □

Definition 4.2.49. Let ν be a nonzero Gaussian integer. A *Gaussian prime factorization* of ν means a tuple $(\pi_1, \pi_2, \ldots, \pi_k)$ of Gaussian primes such that $\nu \sim \pi_1 \pi_2 \cdots \pi_k$.

Why did we require only $\nu \sim \pi_1 \pi_2 \cdots \pi_k$ and not $\nu = \pi_1 \pi_2 \cdots \pi_k$? Because we want -1 to have a Gaussian prime factorization, but there is no way to literally write -1 as a product of Gaussian primes.

Exercise 4.2.12. Let π and κ be two Gaussian primes that do not satisfy $\pi \sim \kappa$. Prove that $\pi \perp \kappa$.

Solution sketch. This is an analogue of Exercise 2.13.1, and its solution goes accordingly. □

Lemma 4.2.50. Let π be a Gaussian prime. Let α be a nonzero Gaussian integer. Then, there exists a largest $m \in \mathbb{N}$ such that $\pi^m \mid \alpha$.

Proof of Lemma 4.2.50. This is an analogue of Lemma 2.13.22 for Gaussian integers (with π and α playing the roles of p and n), and the proof also proceeds similarly. Here are the main differences: Instead of $p > 1$, we now have $\mathrm{N}(\pi) > 1$ (which is because π is nonzero and not a unit). Again, let W be the set of all $m \in \mathbb{N}$ satisfying $\pi^m \mid \alpha$. Then, W is a nonempty set of integers (this is proven as in the proof of Lemma 2.13.22). Let $u = \mathrm{N}(\alpha)$. Thus, $u \in \mathbb{N}$. It is easy to see that $\mathrm{N}\left(\pi^k\right) > k$ for each $k \in \mathbb{N}$ (indeed, Corollary 4.1.28 **(b)** yields $\mathrm{N}\left(\pi^k\right) = \left(\mathrm{N}(\pi)\right)^k > k$ by Exercise 2.13.4 (applied to $p = \mathrm{N}(\pi)$)). From this point, we proceed similarly as in the proof of Lemma 2.13.22. □

Similarly to Definition 2.13.23, we can define π-adic valuations:

Definition 4.2.51. Let π be a Gaussian prime.

(a) Let α be a nonzero Gaussian integer. Then, $v_\pi(\alpha)$ shall denote the largest $m \in \mathbb{N}$ such that $\pi^m \mid \alpha$. This is well-defined (by Lemma 4.2.50). This nonnegative integer $v_\pi(\alpha)$ will be called the *π-valuation* (or the *π-adic valuation*) of α.

(b) We extend this definition of $v_\pi(\alpha)$ to the case of $\alpha = 0$ as follows: Set $v_\pi(0) = \infty$.

Definition 4.2.51 does not conflict with Definition 2.13.23. Indeed, if a prime p happens to also be a Gaussian prime, and if n is an integer, then both definitions yield the same value of $v_p(n)$ (since $p^m \mid a$ means the same thing whether we treat p and a as integers or as Gaussian integers).

Theorem 4.2.52. Let π be a Gaussian prime.

(a) We have $v_\pi(\alpha\beta) = v_\pi(\alpha) + v_\pi(\beta)$ for any two Gaussian integers α and β.

(b) We have $v_\pi(\alpha+\beta) \geq \min\{v_\pi(\alpha), v_\pi(\beta)\}$ for any two Gaussian integers α and β.

(c) We have $v_\pi(1) = 0$. More generally, $v_\pi(\alpha) = 0$ for any unit $\alpha \in \mathbb{Z}[i]$.

(d) We have $v_\pi(\kappa) = \begin{cases} 1, & \text{if } \kappa \sim \pi; \\ 0, & \text{otherwise} \end{cases}$ for any Gaussian prime κ.

Proof. This is an analogue of Theorem 2.13.28, and is proven similarly. □

Proposition 4.2.53. Let ν be a nonzero Gaussian integer. Let $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ be a Gaussian prime factorization of ν. Let π be a Gaussian prime. Then,

$$\begin{aligned}
&(\text{the number of times a Gaussian integer unit-equivalent to } \pi \\
&\qquad \text{appears in the tuple } (\alpha_1, \alpha_2, \ldots, \alpha_k)) \\
&= (\text{the number of times } [\pi]_\sim \text{ appears in the tuple } ([\alpha_1]_\sim, [\alpha_2]_\sim, \ldots, [\alpha_k]_\sim)) \\
&= (\text{the number of } i \in \{1,2,\ldots,k\} \text{ such that } \alpha_i \sim \pi) \\
&= (\text{the number of } i \in \{1,2,\ldots,k\} \text{ such that } [\alpha_i]_\sim = [\pi]_\sim) \\
&= v_\pi(\nu).
\end{aligned}$$

Proof. This is an analogue of Proposition 2.13.30, and is proven similarly. □

Theorem 4.2.54. Let ν be a nonzero Gaussian integer.

(a) There exists a Gaussian prime factorization of ν.

(b) Any two such factorizations differ only by reordering their entries and multiplying them by units. More precisely: If $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $(\beta_1, \beta_2, \ldots, \beta_\ell)$ are two Gaussian prime factorizations of ν, then $([\alpha_1]_\sim, [\alpha_2]_\sim, \ldots, [\alpha_k]_\sim)$ is a permutation of $([\beta_1]_\sim, [\beta_2]_\sim, \ldots, [\beta_\ell]_\sim)$.

Proof. This is an analogue of Theorem 2.13.31, and is proven similarly. □

Example 4.2.55. We have

$$5 = (1+2i)(1-2i) = (2+i)(2-i).$$

Thus, both $(1+2i, 1-2i)$ and $(2+i, 2-i)$ are Gaussian prime factorizations of 5. They may look different, but actually you get the second one from the first by swapping the two entries and multiplying the first entry by the unit i and multiplying the second entry by the unit $-i$. This perfectly agrees with Theorem 4.2.54.

In analogy to Exercise 2.13.5 (and with the same proof), we have:

Exercise 4.2.13. Let π be a Gaussian prime. Let $\alpha, \beta \in \mathbb{Z}[i]$ be such that $\alpha \sim \beta$. Prove that $v_\pi(\alpha) = v_\pi(\beta)$.

We also have the following:

Exercise 4.2.14. Let π be a Gaussian prime. Let $\alpha \in \mathbb{Z}[i]$. Then, $\overline{\pi}$ is a Gaussian prime as well, and satisfies

$$v_{\overline{\pi}}(\overline{\alpha}) = v_\pi(\alpha).$$

Solution sketch. Conjugation is a symmetry, taking Gaussian integers to Gaussian integers and preserving divisibility. Thus, any $i \in \mathbb{N}$ satisfying $\pi^i \mid \alpha$ must also satisfy $\overline{\pi}^i \mid \overline{\alpha}$, and vice versa. Hence, $v_{\overline{\pi}}(\overline{\alpha}) = v_\pi(\alpha)$ easily follows. □

Definition 4.2.56. For the rest of this section, let GP be the set of all Gaussian primes of the form $x + yi$ with $x \in \{1, 2, 3, \ldots\}$ and $y \in \{0, 1, 2, \ldots\}$.

The following is easy to see:

Lemma 4.2.57. Let π be a Gaussian prime. Then, there exists **exactly one** $\sigma \in \mathrm{GP}$ such that $\pi \sim \sigma$.

In other words, each Gaussian prime is unit-equivalent to exactly one $\sigma \in \mathrm{GP}$. Thus, the set GP contains exactly one element of each unit-equivalence class of Gaussian primes. (Thus, GP is what is called a "system of distinct representatives" for the unit-equivalence classes of all Gaussian primes.)

In analogy to Corollary 2.13.34, we have:

Corollary 4.2.58. Let α be a nonzero Gaussian integer. Then,

$$\alpha \sim \prod_{\pi \in \mathrm{GP}} \pi^{v_\pi(\alpha)}.$$

Here, the infinite product $\prod_{\pi \in \mathrm{GP}} \pi^{v_\pi(\alpha)}$ is well-defined (according to the Gaussian-integer analogue of Lemma 2.13.32 **(b)**).

In analogy to Proposition 2.13.35, we have the following:

Proposition 4.2.59. Let α and β be Gaussian integers. Then, $\alpha \mid \beta$ if and only if each Gaussian prime π satisfies $v_\pi(\alpha) \leq v_\pi(\beta)$.

If α is a Gaussian integer, and c is a unit-equivalence class of Gaussian integers, then either all elements of c divide α or none of them does.[147] Thus, we can talk of

[147] This is easy to check. Indeed, it boils down to the fact that any two elements of c divide each other (because they are unit-equivalent).

unit-equivalence classes of Gaussian divisors of α (by which we mean unit-equivalence classes of Gaussian integers whose elements all divide α).

Here is an analogue of Proposition 2.18.1 for Gaussian integers:

Proposition 4.2.60. Let $\alpha \in \mathbb{Z}[i]$ be a nonzero Gaussian integer. Then:

(a) The product $\prod_{\pi \in \mathrm{GP}} (v_\pi(\alpha) + 1)$ is well-defined, since all but finitely many of its factors are 1.

(b) We have

$$\begin{aligned} &(\text{the number of unit-equivalence classes of Gaussian divisors of } \alpha) \\ &= \prod_{\pi \in \mathrm{GP}} (v_\pi(\alpha) + 1). \end{aligned}$$

(c) We have

$$(\text{the number of Gaussian divisors of } \alpha) = 4 \cdot \prod_{\pi \in \mathrm{GP}} (v_\pi(\alpha) + 1).$$

Proof. Same proof as for Proposition 2.18.1, but you have to be more careful with unit-equivalence (since in part **(b)**, you are counting unit-equivalence classes rather than positive divisors). The analogue of Lemma 2.18.3 we need to use for this proof is the following lemma: □

Lemma 4.2.61. Let $\pi_1, \pi_2, \ldots, \pi_u$ be finitely many Gaussian primes, no two of which are unit-equivalent. For each $i \in \{1, 2, \ldots, u\}$, let a_i be a nonnegative integer. Let $\alpha = \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_u^{a_u}$.

Define a set T by

$$\begin{aligned} T &= \{0, 1, \ldots, a_1\} \times \{0, 1, \ldots, a_2\} \times \cdots \times \{0, 1, \ldots, a_u\} \\ &= \{(b_1, b_2, \ldots, b_u) \mid b_i \in \{0, 1, \ldots, a_i\} \text{ for each } i \in \{1, 2, \ldots, u\}\} \\ &= \{(b_1, b_2, \ldots, b_u) \in \mathbb{N}^u \mid b_i \leq a_i \text{ for each } i \in \{1, 2, \ldots, u\}\}. \end{aligned}$$

Then, the map

$$\begin{aligned} \Lambda : T &\to \{\text{unit-equivalence classes of Gaussian divisors of } \alpha\}, \\ (b_1, b_2, \ldots, b_u) &\mapsto \left[\pi_1^{b_1} \pi_2^{b_2} \cdots \pi_u^{b_u}\right]_\sim \end{aligned}$$

is well-defined and bijective.

Now, we can finally answer Question 1.4.2 **(b)** (following [DumFoo04, §8.3, Corollary 19]):

Theorem 4.2.62. Let n be a positive integer.

(a) If there is at least one prime $p \equiv 3 \bmod 4$ such that $v_p(n)$ is odd, then there is **no** pair $(x, y) \in \mathbb{Z}^2$ such that $n = x^2 + y^2$.

(b) Assume that for each prime $p \equiv 3 \bmod 4$, the number $v_p(n)$ is even. Then,

$$\begin{aligned}&\left(\text{the number of pairs } (x,y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2\right)\\&= 4 \cdot \prod_{\substack{p \text{ prime;}\\ p \equiv 1 \bmod 4}} \left(v_p(n) + 1\right).\end{aligned}$$

Example 4.2.63. **(a)** Let $n = 35$. Then, Theorem 4.2.62 **(a)** yields that there are **no** integers x and y such that $n = x^2 + y^2$. In fact, the prime $7 \equiv 3 \bmod 4$ satisfies $v_7(n) = 1$.

(b) Let $n = 45$. Then, for each prime $p \equiv 3 \bmod 4$, the number $v_p(n)$ is even. Indeed, $n = 45 = 3^2 \cdot 5$, so $v_3(n) = 2$ is even and $v_p(n) = 0$ for all other primes p of Type 3. Hence, Theorem 4.2.62 **(b)** yields

$$\begin{aligned}&\left(\text{the number of pairs } (x,y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2\right)\\&= 4 \cdot \underbrace{\prod_{\substack{p \text{ prime;}\\ p \equiv 1 \bmod 4}} \left(v_p(n) + 1\right)}_{\substack{= v_5(n) + 1\\ = 1 + 1 = 2}} = 4 \cdot 2 = 8.\end{aligned}$$

Proof of Theorem 4.2.62 (sketched). **(a)** Assume that there is at least one prime $p \equiv 3 \bmod 4$ such that $v_p(n)$ is odd. We must prove that there is **no** pair $(x, y) \in \mathbb{Z}^2$ such that $n = x^2 + y^2$.

Indeed, let $(x, y) \in \mathbb{Z}^2$ be a pair such that $n = x^2 + y^2$. We must derive a contradiction.

Let α be the Gaussian integer $x + yi$. Thus, $\alpha\overline{\alpha} = x^2 + y^2 = n$.

We have assumed that there is at least one prime $p \equiv 3 \bmod 4$ such that $v_p(n)$ is odd. Consider this p. Note that p is a Gaussian prime (by Lemma 4.2.41).

Thus, Exercise 4.2.14 (applied to $\pi = p$) yields $v_{\overline{p}}(\overline{\alpha}) = v_p(\alpha)$. In view of $\overline{p} = p$, this rewrites as $v_p(\overline{\alpha}) = v_p(\alpha)$. But

$$v_p\left(\underbrace{n}_{=\alpha\overline{\alpha}}\right) = v_p(\alpha\overline{\alpha}) = v_p(\alpha) + \underbrace{v_p(\overline{\alpha})}_{=v_p(\alpha)} = v_p(\alpha) + v_p(\alpha) = 2v_p(\alpha).$$

Thus, $v_p(n)$ is even. This contradicts the fact that $v_p(n)$ is odd. Thus, we have found a contradiction for each pair $(x, y) \in \mathbb{Z}^2$ such that $n = x^2 + y^2$. Hence, there exists no such pair. This proves Theorem 4.2.62 **(a)**.

(b) We have

$$\begin{aligned}&\left(\text{the number of } \alpha \in \mathbb{Z}\left[i\right] \text{ such that } n = \alpha\overline{\alpha}\right)\\&= \left(\text{the number of pairs } \left(x,y\right) \in \mathbb{Z}^2 \text{ such that } n = x^2+y^2\right),\end{aligned}$$

since the map

$$\begin{aligned}\left\{\left(x,y\right) \in \mathbb{Z}^2 \ \mid\ n = x^2+y^2\right\} &\to \left\{\alpha \in \mathbb{Z}\left[i\right] \ \mid\ n = \alpha\overline{\alpha}\right\},\\ \left(x,y\right) &\mapsto x+yi\end{aligned}$$

is a bijection.

Write the canonical factorization of n as

$$n = 2^c \cdot p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \cdot q_1^{b_1} q_2^{b_2} \cdots q_\ell^{b_\ell}, \tag{158}$$

where all the exponents c, a_h, b_j are $\in \mathbb{N}$, and where $p_1, p_2, \ldots, p_k$ are distinct primes of Type 1, and where $q_1, q_2, \ldots, q_\ell$ are distinct primes of Type 3. Note that $c = 0$ if n is odd.

We have assumed that for each prime $p \equiv 3 \bmod 4$, the number $v_p\left(n\right)$ is even. In other words, for each prime p of Type 3, the number $v_p\left(n\right)$ is even. In other words, $b_1, b_2, \ldots, b_\ell$ are even (since $q_1, q_2, \ldots, q_\ell$ are primes of Type 3, and thus the corresponding exponents $b_j = v_{q_j}\left(n\right)$ must be even). Hence, $b_j/2 \in \mathbb{N}$ for each j.

Each q_j is a prime of Type 3, and thus is a Gaussian prime (by Lemma 4.2.41). Meanwhile, each p_h is a prime of Type 1, and thus can be written in the form $p_h = \pi_h\overline{\pi_h}$ for some Gaussian prime π_h (by Theorem 4.2.42 **(c)**). Consider these π_h. For every h, Theorem 4.2.42 **(e)** shows that the conjugate $\overline{\pi_h}$ is also a Gaussian prime, and that we do not have $\pi_h \sim \overline{\pi_h}$.

Finally, let ρ be the Gaussian prime $1+i$; thus $2 = \rho\overline{\rho}$. But note that $\rho \sim \overline{\rho}$ (indeed, $\overline{\rho} = 1-i = \left(-i\right)\underbrace{\left(1+i\right)}_{=\rho} = \left(-i\right)\rho$). Now, (158) becomes

$$\begin{aligned}n &= \underbrace{2^c}_{\substack{=\rho^c\overline{\rho}^c\\ \text{(since } 2=\rho\overline{\rho})}} \cdot \left(\prod_{h=1}^{k} \underbrace{p_h^{a_h}}_{\substack{=\pi_h^{a_h}\overline{\pi_h}^{a_h}\\ \text{(since } p_h=\pi_h\overline{\pi_h})}}\right) \cdot q_1^{b_1} q_2^{b_2} \cdots q_\ell^{b_\ell}\\ &= \rho^c\overline{\rho}^c \cdot \left(\prod_{h=1}^{k}\left(\pi_h^{a_h}\overline{\pi_h}^{a_h}\right)\right) \cdot q_1^{b_1} q_2^{b_2} \cdots q_\ell^{b_\ell},\end{aligned} \tag{159}$$

and this is a decomposition of n as a product of powers of Gaussian primes (albeit ρ and $\overline{\rho}$ are unit-equivalent).

No two of the Gaussian primes $\rho, \pi_h, \overline{\pi_h}, q_j$ are unit-equivalent. (*Proof:* Compare their norms (since unit-equivalent Gaussian integers have equal norms). The only of these Gaussian primes that have equal norms are π_h and $\overline{\pi_h}$. So we merely need to rule out $\pi_h \sim \overline{\pi_h}$. But this is clear, since we already showed that we do not have $\pi_h \sim \overline{\pi_h}$.)

Now, define a map

$$F : \{1, i, -1, -i\} \times \prod_{h=1}^{k} \{0, 1, \ldots, a_h\} \to \{\alpha \in \mathbb{Z}[i] \mid n = \alpha\overline{\alpha}\},$$
$$(\gamma, (d_1, d_2, \ldots, d_k)) \mapsto \gamma \cdot \rho^c \cdot \left(\prod_{h=1}^{k} \left(\pi_h^{d_h} \overline{\pi_h}^{a_h - d_h} \right) \right) \cdot q_1^{b_1/2} q_2^{b_2/2} \cdots q_\ell^{b_\ell/2}.$$

It is easy to check that this map F is well-defined[148]. We claim that this map F is a bijection.

[*Proof:* To see that F is injective, we must find a way to reconstruct $(\gamma, (d_1, d_2, \ldots, d_k)) \in \{1, i, -1, -i\} \times \prod_{h=1}^{k} \{0, 1, \ldots, a_h\}$ from

$$\begin{aligned} \alpha :&= F((\gamma, (d_1, d_2, \ldots, d_k))) \\ &= \gamma \cdot \rho^c \cdot \left(\prod_{h=1}^{k} \left(\pi_h^{d_h} \overline{\pi_h}^{a_h - d_h} \right) \right) \cdot q_1^{b_1/2} q_2^{b_2/2} \cdots q_\ell^{b_\ell/2}. \end{aligned}$$

But this is easy: You first reconstruct the k-tuple $(d_1, d_2, \ldots, d_k)$ by observing that $d_h = v_{\pi_h}(\alpha)$ for each h. Once you have that, you can reconstruct γ by

$$\gamma = \frac{\alpha}{\rho^c \cdot \left(\prod_{h=1}^{k} \left(\pi_h^{d_h} \overline{\pi_h}^{a_h - d_h} \right) \right) \cdot q_1^{b_1/2} q_2^{b_2/2} \cdots q_\ell^{b_\ell/2}}.$$

So F is injective.

To see that F is surjective, we must prove that each $\alpha \in \mathbb{Z}[i]$ satisfying $n = \alpha\overline{\alpha}$ has the form

$$\alpha = \gamma \cdot \rho^c \cdot \left(\prod_{h=1}^{k} \left(\pi_h^{d_h} \overline{\pi_h}^{a_h - d_h} \right) \right) \cdot q_1^{b_1/2} q_2^{b_2/2} \cdots q_\ell^{b_\ell/2}$$

for some $(\gamma, (d_1, d_2, \ldots, d_k))$. To prove this, use canonical factorization of α inside $\mathbb{Z}[i]$ to see that

$$\alpha = \gamma \cdot \rho^{c'} \cdot \left(\prod_{h=1}^{k} \left(\pi_h^{d'_h} \overline{\pi_h}^{e'_h} \right) \right) \cdot q_1^{b'_1} q_2^{b'_2} \cdots q_\ell^{b'_\ell} \qquad (160)$$

[148] Just multiply out $\alpha\overline{\alpha}$ for $\alpha = \gamma \cdot \rho^c \cdot \left(\prod_{h=1}^{k} \left(\pi_h^{d_h} \overline{\pi_h}^{a_h - d_h} \right) \right) \cdot q_1^{b_1/2} q_2^{b_2/2} \cdots q_\ell^{b_\ell/2}$ and check that you obtain n. Corollary 4.1.28 **(a)** needs to be used.

for some $c', d'_h, e'_h, b'_j \in \mathbb{N}$. Consider these $c', d'_h, e'_h, b'_j \in \mathbb{N}$. From (160), we obtain

$$\begin{aligned}
\alpha\overline{\alpha} &= \gamma \cdot \rho^{c'} \cdot \left(\prod_{h=1}^{k} \left(\pi_h^{d'_h} \overline{\pi_h}^{e'_h} \right) \right) \cdot q_1^{b'_1} q_2^{b'_2} \cdots q_\ell^{b'_\ell} \cdot \overline{\gamma \cdot \rho^{c'} \cdot \left(\prod_{h=1}^{k} \left(\pi_h^{d'_h} \overline{\pi_h}^{e'_h} \right) \right) \cdot q_1^{b'_1} q_2^{b'_2} \cdots q_\ell^{b'_\ell}} \\
&= \underbrace{\gamma\overline{\gamma}}_{\substack{=\mathrm{N}(\gamma)=1 \\ \text{(since } \gamma \text{ is a unit)}}} \cdot \underbrace{\rho^{c'}\overline{\rho}^{c'}}_{\substack{=(\rho\overline{\rho})^{c'}=2^{c'} \\ \text{(since } \rho\overline{\rho}=2\text{)}}} \cdot \left(\prod_{h=1}^{k} \left(\pi_h^{d'_h} \overline{\pi_h}^{e'_h} \overline{\pi_h^{d'_h} \overline{\pi_h}^{e'_h}} \right) \right) \cdot q_1^{b'_1} q_2^{b'_2} \cdots q_\ell^{b'_\ell} \cdot \underbrace{\overline{q_1^{b'_1} q_2^{b'_2} \cdots q_\ell^{b'_\ell}}}_{\substack{=q_1^{b'_1} q_2^{b'_2} \cdots q_\ell^{b'_\ell} \\ \text{(since } q_1, q_2, \ldots, q_\ell \\ \text{are reals)}}} \\
&= 2^{c'} \cdot \left(\prod_{h=1}^{k} \underbrace{\left(\pi_h^{d'_h} \overline{\pi_h}^{e'_h} \overline{\pi_h^{d'_h} \overline{\pi_h}^{e'_h}} \right)}_{=(\pi_h\overline{\pi_h})^{d'_h+e'_h}} \right) \cdot \underbrace{q_1^{b'_1} q_2^{b'_2} \cdots q_\ell^{b'_\ell} \cdot q_1^{b'_1} q_2^{b'_2} \cdots q_\ell^{b'_\ell}}_{=q_1^{2b'_1} q_2^{2b'_2} \cdots q_\ell^{2b'_\ell}} \\
&= 2^{c'} \cdot \left(\prod_{h=1}^{k} \left(\underbrace{\pi_h\overline{\pi_h}}_{=p_h} \right)^{d'_h+e'_h} \right) \cdot q_1^{2b'_1} q_2^{2b'_2} \cdots q_\ell^{2b'_\ell} = 2^{c'} \cdot \left(\prod_{h=1}^{k} p_h^{d'_h+e'_h} \right) \cdot q_1^{2b'_1} q_2^{2b'_2} \cdots q_\ell^{2b'_\ell}.
\end{aligned}$$

Thus,

$$n = \alpha\overline{\alpha} = 2^{c'} \cdot \left(\prod_{h=1}^{k} p_h^{d'_h+e'_h} \right) \cdot q_1^{2b'_1} q_2^{2b'_2} \cdots q_\ell^{2b'_\ell}. \qquad (161)$$

This is a prime factorization of n as an integer. But so is (158). Since the prime factorization of an integer is unique (or by comparing p-valuations of the right hand sides on (161) and (158)), we thus conclude

$$\begin{aligned}
&c' = c; \qquad && d'_h + e'_h = a_h \qquad && \text{for all } h; \\
&2b'_j = b_j \qquad && \text{for all } j.
\end{aligned}$$

In other words,

$$\begin{aligned}
&c' = c; \qquad && e'_h = a_h - d'_h \qquad && \text{for all } h; \\
&b'_j = b_j/2 \qquad && \text{for all } j.
\end{aligned}$$

Hence, (160) rewrites as

$$\begin{aligned}
\alpha &= \gamma \cdot \rho^{c} \cdot \left(\prod_{h=1}^{k} \left(\pi_h^{d'_h} \overline{\pi_h}^{a_h-d'_h} \right) \right) \cdot q_1^{b_1/2} q_2^{b_2/2} \cdots q_\ell^{b_\ell/2} \\
&= F\left(\left(\gamma, \left(d'_1, d'_2, \ldots, d'_k \right) \right) \right) \qquad \text{(by the definition of } F\text{)}.
\end{aligned}$$

Thus, we have shown that α is a value of F. This proves that F is surjective.

Now, F is injective and surjective, hence bijective.]

So F is a bijection. Thus,

$$\begin{aligned}
&\left|\{1,i,-1,-i\} \times \prod_{h=1}^{k} \{0,1,\ldots,a_h\}\right| \\
&= \left|\{\alpha \in \mathbb{Z}[i] \mid n = \alpha\overline{\alpha}\}\right| \\
&= (\text{the number of } \alpha \in \mathbb{Z}[i] \text{ such that } n = \alpha\overline{\alpha}) \\
&= \left(\text{the number of pairs } (x,y) \in \mathbb{Z}^2 \text{ such that } n = x^2+y^2\right),
\end{aligned}$$

so that

$$\begin{aligned}
&\left(\text{the number of pairs } (x,y) \in \mathbb{Z}^2 \text{ such that } n = x^2+y^2\right) \\
&= \left|\{1,i,-1,-i\} \times \prod_{h=1}^{k} \{0,1,\ldots,a_h\}\right| = \underbrace{\left|\{1,i,-1,-i\}\right|}_{=4} \cdot \prod_{h=1}^{k} \underbrace{\left|\{0,1,\ldots,a_h\}\right|}_{=a_h+1} \\
&= 4 \cdot \prod_{h=1}^{k} \left(\underbrace{a_h}_{=v_{p_h}(n)} + 1\right) = 4 \cdot \prod_{h=1}^{k} \left(v_{p_h}(n)+1\right) = 4 \cdot \prod_{\substack{p \text{ prime;} \\ p \equiv 1 \bmod 4}} \left(v_p(n)+1\right).
\end{aligned}$$

(The last equality sign is a consequence of the fact that $p_1, p_2, \ldots, p_h$ are distinct primes of Type 1, and that all other primes $p \notin \{p_1, p_2, \ldots, p_h\}$ of Type 1 satisfy $v_p(n) = 0$.) This proves Theorem 4.2.62 **(b)**. □

One consequence of Theorem 4.2.62 is that a positive integer n can be written in the form x^2+y^2 with $x, y \in \mathbb{Z}$ if and only if it has the property that for each prime $p \equiv 3 \bmod 4$, the number $v_p(n)$ is even. A different proof of this fact appears in [AigZie18, Theorem in Chapter 4].

4.2.7. What are the Gaussian primes?

We have so far seen the following Gaussian primes:

- Each prime of Type 3 is a Gaussian prime.
- $1+i$ is a Gaussian prime.
- For each prime p of Type 1, we have a Gaussian prime π such that $p = \pi\overline{\pi}$, and then $\overline{\pi}$ is also a Gaussian prime.

Theorem 4.2.64. Each Gaussian prime is unit-equivalent to one of the Gaussian primes in this list.

Proof. See homework set #5 exercise 3. □

4.3. Brief survey of similar number systems

- Let us now see when a prime p can be written as $x^2 + 2y^2$ with $x, y \in \mathbb{Z}$.

  The set
  $$\mathbb{Z}\left[\sqrt{-2}\right] = \mathbb{Z}\left[\sqrt{2}i\right]$$
  is defined as the set of all complex numbers of the form $a + b\sqrt{2}i$ with $a, b \in \mathbb{Z}$. It is perhaps easier to regard it as its own variant of Gaussian integers, which I will call the "2-Gaussian integers". These "2-Gaussian integers" can be defined as pairs $(a, b) \in \mathbb{Z}^2$ with addition and subtraction defined entrywise and multiplication defined by
  $$(a,b)(c,d) = (ac - 2bd, ad + bc).$$
  [149] You can then write such pairs (a, b) as $a + b\sqrt{2}i$, where $\sqrt{2}i$ is simply a symbol for the 2-Gaussian integer $(0, 1)$. Each 2-Gaussian integer (a, b) has a norm, defined by $\operatorname{N}((a,b)) = a^2 + 2b^2$.

  Much of the theory of Gaussian integers still applies verbatim to 2-Gaussian integers. In particular, division with remainder still works for 2-Gaussian integers (like it does for Gaussian integers, i.e., non-uniquely), and the proof uses the same argument, but this time we have $\operatorname{N}(\rho) \leq 3\operatorname{N}(\beta)/4$ instead of $\operatorname{N}(\rho) \leq \operatorname{N}(\beta)/2$. Hence, 2-Gaussian integers have unique factorizations into "2-Gaussian primes".

  This can be used to show that a prime p can be written as $x^2 + 2y^2$ if and only if there is an integer u satisfying $u^2 \equiv -2 \mod p$. It can furthermore be shown that such an integer u exists if and only if $p = 2$ or $p \equiv 1, 3 \mod 8$ (where "$p \equiv 1, 3 \mod 8$" is shorthand for "$p \equiv 1 \mod 8$ or $p \equiv 3 \mod 8$"). The proof uses a fact called *quadratic reciprocity*, which we **may** see later in this course.

- When can a prime p be written as $x^2 + 3y^2$ with $x, y \in \mathbb{Z}$?

  The logical continuation of the above pattern would be "when $p = 3$ or $p \equiv 1 \mod 3$", since these are the cases when there is an integer u satisfying $u^2 \equiv -3 \mod p$. And that is indeed true, but the proof is more complicated. Indeed, the "3-Gaussian integers" no longer have division with remainder, as $\operatorname{N}(\rho) \leq \operatorname{N}(\beta)/2$ turns into $\operatorname{N}(\rho) \leq \operatorname{N}(\beta)$ which is not a strict inequality. Nevertheless we can prove our guess with more complicated reasoning: We need to use not $\mathbb{Z}\left[\sqrt{-3}\right]$ but rather the *Eisenstein integers* $a + b\omega$ with $a, b \in \mathbb{Z}$ and $\omega = \dfrac{-1 + i\sqrt{3}}{2}$. These are best understood as pairs $(a, b) \in \mathbb{Z}^2$

[149] Be careful, however: This definition of 2-Gaussian integers as pairs of integers conflicts with the definition of complex numbers as pairs of reals; the 2-Gaussian integer (a, b) and the complex number (a, b) are two different numbers (unless $b = 0$).

with addition and subtraction defined entrywise and multiplication defined by

$$(a,b)(c,d) = (ac - bd, ad + bc - bd).$$

Their norm is $\mathrm{N}((a,b)) = a^2 - ab + b^2$. They form a triangular lattice, not a rectangular one, and they do have division with remainder. Note that $\mathrm{N}(a + b\omega) = a^2 - ab + b^2$, so some more work is needed to turn them into $x^2 + 3y^2$ solutions, but it's doable.

- When can a prime p be written as $x^2 + 4y^2$ with $x, y \in \mathbb{Z}$?

  This is easy: $4y^2 = (2y)^2$, so we are looking for a way of writing p as $x^2 + y^2$ with y even.

  I claim that the answer is "when $p \equiv 1 \bmod 4$". Do you see why?

- When can a prime p be written as $x^2 + 5y^2$ with $x, y \in \mathbb{Z}$?

  Our guess, by following the above pattern, would be "when $p = 2$ or $p = 5$ or $p \equiv 1, 3, 7, 9 \bmod 20$", since these are the cases when there is an integer u satisfying $u^2 \equiv -5 \bmod p$. But this is not true anymore. The right answer is "when $p = 2$ or $p = 5$ or $p \equiv 1, 9 \bmod 20$". And unsurprisingly, $\mathbb{Z}\left[\sqrt{-5}\right]$ does not have division with remainder.

- More generally, you can fix $n \in \mathbb{N}$ and ask when a prime can be written in the form $x^2 + ny^2$. There is a whole book [Cox13] devoted to this question! The answer becomes more complicated with n getting large, and touches on a surprising number of different fields of mathematics (geometry, complex analysis, elliptic functions and elliptic curves).

- We can also ask when a prime p can be written as $x^2 - ny^2$. The appropriate analogue of $\mathbb{Z}[i]$ tailored to this question is $\mathbb{Z}\left[\sqrt{n}\right]$, which however behaves much differently, since $\sqrt{n}$ is real. For example, as you saw on homework set #4 (in the Remark after Exercise 4), there are infinitely many units in $\mathbb{Z}\left[\sqrt{2}\right]$; the same is true for each $\mathbb{Z}\left[\sqrt{n}\right]$ with $n > 1$ and n not being a perfect square (but this is much harder to prove).

- When can an $n \in \mathbb{N}$ be written as a sum of three squares? Legendre's three-squares theorem says that the answer is "if and only if n is not of the form $n = 4^a(8b + 7)$ for $a, b \in \mathbb{N}$". This is very hard to prove ([UspHea39, Chapter XIII] might have the only elementary proof).

- When can an $n \in \mathbb{N}$ be written as a sum of four squares? Lagrange's four-squares theorem reveals that the answer to this question is "always"![150] This

[150] An application (fortunately, no longer relevant):

"`Warning: Due to a known bug, the default Linux document viewer evince prints N*N copies of a PDF file when N copies requested. As a workaround, use Adobe Reader acroread for printing multiple copies of PDF documents, or use the fact that every natural number is a sum of at most four squares.`"

is easier to show, and there is even a formula for the number of representations: it is $8 \sum\limits_{\substack{d \mid n; \\ 4 \nmid d}} d$. The existence part can be proven using "Hurwitz integers", which are certain quaternions.

5. Rings and fields

5.1. Definition of a ring

We have seen several "number systems" in the above chapters:

- $\mathbb{N}$ (the nonnegative integers);
- $\mathbb{Z}$ (the integers);
- $\mathbb{R}$ (the real numbers);
- $\mathbb{Z}/n$ (the residue classes modulo n) for an integer n;
- $\mathbb{C}$ (the complex numbers);
- $\mathbb{Z}[i]$ (the Gaussian integers);
- $\mathbb{D}$ (the dual numbers – see homework set #4 exercise 3);
- $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$ (see homework set #4 exercise 4);
- $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ (the Eisenstein integers);
- $\mathbb{Z}\left[\sqrt{-3}\right]$ (see homework set #5 exercise 6).

It may be a stretch to refer to the elements of some of these systems as "numbers", but it is not taboo (the word "number" has no precise meaning in mathematics), and these sets have a lot in common: We can add, subtract and multiply their elements (except for $\mathbb{N}$, which does not allow subtraction); these operations satisfy the usual rules (e.g., associativity of multiplication, distributivity, etc.); these sets contain some element "behaving like 0" (that is, an element $\mathbf{0}$ such that $a + \mathbf{0} = \mathbf{0} + a = a$ and $a \cdot \mathbf{0} = \mathbf{0} \cdot a = \mathbf{0}$ for all a) and some element "behaving like 1" (that is, an element $\mathbf{1}$ such that $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ for all a). It turns out that just a few of these rules are sufficient to make "all the other rules" (in a certain appropriate sense) follow from them. Thus, it is reasonable to crystallize these few rules into a common, general notion (of which the above examples – excluding $\mathbb{N}$ – will be particular cases); this notion will be called a "**ring**". Hence, we shall define a **ring** to be (roughly speaking) a set with operations $+$ and $\cdot$ and elements 0 and 1 that satisfy these few rules. Let us be specific about what these rules are:[151]

[151] Recall the definition of a "binary operation" (Definition 1.6.1). In particular, a binary operation on a set S must have all its values in S.

Definition 5.1.1. **(a)** A *ring* means a set $\mathbb{K}$ endowed with

- two binary operations called *"addition"* and *"multiplication"*, and denoted by $+_{\mathbb{K}}$ and $\cdot_{\mathbb{K}}$, respectively, and
- two elements called *"zero"* (or *"origin"*) and *"unity"* (or *"one"*), and denoted by $0_{\mathbb{K}}$ and $1_{\mathbb{K}}$, respectively

such that the following axioms are satisfied:

- **Commutativity of addition:** We have $a +_{\mathbb{K}} b = b +_{\mathbb{K}} a$ for all $a, b \in \mathbb{K}$.
- **Associativity of addition:** We have $a +_{\mathbb{K}} (b +_{\mathbb{K}} c) = (a +_{\mathbb{K}} b) +_{\mathbb{K}} c$ for all $a, b, c \in \mathbb{K}$.
- **Neutrality of zero:** We have $a +_{\mathbb{K}} 0_{\mathbb{K}} = 0_{\mathbb{K}} +_{\mathbb{K}} a = a$ for all $a \in \mathbb{K}$.
- **Existence of additive inverses:** For any $a \in \mathbb{K}$, there exists an element $a' \in \mathbb{K}$ such that $a +_{\mathbb{K}} a' = a' +_{\mathbb{K}} a = 0_{\mathbb{K}}$. (It is not **immediately** obvious, but will be shown later, that such an a' is unique. Thus, a' is called the *additive inverse* of a, and is denoted by $-a$.)
- **Associativity of multiplication:** We have $a (bc) = (ab) c$ for all $a, b, c \in \mathbb{K}$. Here and in the following, we use "xy" as an abbreviation for "$x \cdot_{\mathbb{K}} y$".
- **Neutrality of one:** We have $a 1_{\mathbb{K}} = 1_{\mathbb{K}} a = a$ for all $a \in \mathbb{K}$.
- **Annihilation:** We have $a 0_{\mathbb{K}} = 0_{\mathbb{K}} a = 0_{\mathbb{K}}$ for all $a \in \mathbb{K}$.
- **Distributivity:** We have
$$a (b +_{\mathbb{K}} c) = ab +_{\mathbb{K}} ac \qquad \text{and} \qquad (a +_{\mathbb{K}} b) c = ac +_{\mathbb{K}} bc$$
for all $a, b, c \in \mathbb{K}$. Here and in the following, we are using the PEMDAS convention for order of operations; thus, for example, "$ab +_{\mathbb{K}} ac$" must be understood as "$(ab) +_{\mathbb{K}} (ac)$".

These eight axioms will be called the *ring axioms*.

(Note that we do not require the existence of a "subtraction" operation $-_{\mathbb{K}}$. But we will later construct such an operation out of the existing operations and axioms; it is thus unnecessary to require it. We also do not require the existence of multiplicative inverses; nor do we require commutativity of multiplication yet.)

(b) A ring $\mathbb{K}$ (with operations $+_{\mathbb{K}}$ and $\cdot_{\mathbb{K}}$) is called *commutative* if it satisfies the following extra axiom:

- **Commutativity of multiplication:** We have $ab = ba$ for all $a, b \in \mathbb{K}$.

Note a few things:

- We shall abbreviate $+_{\mathbb{K}}$, $\cdot_{\mathbb{K}}$, $0_{\mathbb{K}}$ and $1_{\mathbb{K}}$ as $+$, $\cdot$, 0 and 1 unless there is a chance of confusion with the "usual" notions of addition, multiplication, zero and one. (The example of the ring $\mathbb{Z}'$ shown below is a case where such confusion is possible; but most of the time, it is not.)

- We have not required our rings to be endowed with a "subtraction" operation. Nevertheless, each ring $\mathbb{K}$ automatically has a subtraction operation: Namely, for any $a, b \in \mathbb{K}$, we can define $a - b$ to be $a + b'$, where b' is the additive inverse of b. (We will later see that this operation is well-defined (Definition 5.4.4) and satisfies the rules you would expect (Definition 5.4.5).)

- Some of the ring axioms we required in Definition 5.1.1 are redundant, i.e., they follow from other ring axioms. (For example, Annihilation follows from the other axioms.) We don't mind this, as long as these axioms are natural and easy to check in real examples.

- We have required commutativity of addition to hold for all rings, but commutativity of multiplication only to hold for commutative rings. You may wonder what happens if we also omit the commutativity of addition. The answer is "nothing new": Commutativity of addition follows from the other axioms! (Proving this is a fun, although inconsequential, puzzle.)

- By our definition, a ring consists of a set $\mathbb{K}$, two operations $+$ and $\cdot$ and two elements 0 and 1. Thus, strictly speaking, a ring is a 5-tuple $(\mathbb{K}, +, \cdot, 0, 1)$. In reality, we will often just speak of the "ring $\mathbb{K}$" (so we will mention only the set and not the other four pieces of data) and assume that the reader can figure out the rest of the 5-tuple. This is okay as long as the rest of the 5-tuple can be inferred from the context. For example, when we say "the ring $\mathbb{Z}$", it is clear that we mean the ring $(\mathbb{Z}, +, \cdot, 0, 1)$ with the usual addition and multiplication operations and the usual numbers 0 and 1. The same applies when we speak of "the ring $\mathbb{R}$" or "the ring $\mathbb{C}$" or "the ring $\mathbb{Z}[i]$". In general, whenever a set S is equipped with two operations that are called $+$ and $\cdot$ and two elements that are called 0 and 1 (even if these elements are not literally the numbers 0 and 1), we automatically understand "the ring S" to be the ring $(S, +, \cdot, 0, 1)$ that is defined using these operations and elements. If we want to make a different ring out of the set S, then we have to say this explicitly.

- Some authors do not require the element 1 as part of what it means to be a ring. But we do. Be careful when reading the literature, as the truth or falsehood of many results depends on whether the 1 is included in the definition of a ring or not. (When authors do not require the element 1 in the definition of a ring, they reserve the notion of a "unital ring" for a ring that does come equipped with a 1 that satisfies the "Neutrality of one" axiom; i.e., they call "unital ring" what we call "ring".)

The variant of the notion of rings in which the element 1 is not required is most commonly called a *nonunital ring*; it appears in Exercises 1 and 2 of midterm #3.

5.2. Examples of rings

Many of the "number systems" seen above, and several others, are examples of rings:

- The sets $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ (each endowed with the usual addition, multiplication, 0 and 1) are commutative rings. In each case, the additive inverse of an element a is what we know as $-a$ from high school. (Rigorous proofs of the ring axioms, as well as rigorous definitions of $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, can be found in textbooks and lecture notes on the construction of the number system – such as [Swanso18, Chapter 3].)

- The set $\mathbb{N}$ (again endowed with the usual addition, multiplication, 0 and 1) is not a ring. Indeed, the "existence of additive inverses" axiom fails for $a = 1$, because the element 1 has no additive inverse in $\mathbb{N}$ (that is, there is no $1' \in \mathbb{N}$ such that $1 + 1' = 1' + 1 = 0$).

- The sets $\mathbb{C}$, $\mathbb{Z}[i]$, $\mathbb{D}$, $\mathbb{Z}\left[\sqrt{2}\right]$, $\mathbb{Z}[\omega]$ and $\mathbb{Z}\left[\sqrt{-3}\right]$ (from Chapter 4 and from the homework sets) are commutative rings. All of the axioms are easy to check, and some of them we have checked. (For example, the ring axioms for $\mathbb{C}$ follow easily from Theorem 4.1.2.) In each case, the element a' in the "existence of additive inverses" axiom is $-a$.

- If you have seen polynomials: The set $\mathbb{Z}[x]$ of all polynomials in a single variable x with integer coefficients is a commutative ring. Similarly for other kinds of coefficients, and several variables. We will come back to this once we have rigorously defined polynomials in Chapter 7.

- We can define a commutative ring $\mathbb{Z}'$ as follows:

  We define a binary operation $\widetilde{\times}$ on $\mathbb{Z}$ by

  $$\left(a \widetilde{\times} b = -ab \qquad \text{for all } a, b \in \mathbb{Z}\right).$$

  Now, let $\mathbb{Z}'$ be the **set** $\mathbb{Z}$, endowed with the usual addition $+$ and the unusual multiplication $\widetilde{\times}$ and the elements $0_{\mathbb{Z}'} = 0$ and $1_{\mathbb{Z}'} = -1$.

  Is this $\mathbb{Z}'$ a commutative ring? Let us check the axioms:

  - The first four axioms involve only addition and 0 (but not multiplication and 1), and therefore still hold for $\mathbb{Z}'$ (because $\mathbb{Z}'$ has the same addition and 0 as $\mathbb{Z}$).

- Associativity of multiplication in $\mathbb{Z}'$: We must check that

  $$a \widetilde{\times} \left(b \widetilde{\times} c\right) = \left(a \widetilde{\times} b\right) \widetilde{\times} c \qquad \text{for all } a, b, c \in \mathbb{Z}'.$$

  (Note that we cannot omit the "multiplication sign" $\widetilde{\times}$ here and simply write "bc" for "$b \widetilde{\times} c$", because "bc" already means something different. Note also that "$a, b, c \in \mathbb{Z}'$" means the same as "$a, b, c \in \mathbb{Z}$", because $\mathbb{Z}' = \mathbb{Z}$ as sets.)

  Checking this is straightforward: Let $a, b, c \in \mathbb{Z}'$. Then, comparing

  $$a \widetilde{\times} \underbrace{\left(b \widetilde{\times} c\right)}_{=-bc} = a \widetilde{\times} (-bc) = -a(-bc) = abc \qquad \text{with}$$
  $$\underbrace{\left(a \widetilde{\times} b\right)}_{=-ab} \widetilde{\times} c = (-ab) \widetilde{\times} c = -(-ab) c = abc,$$

  we obtain $a \widetilde{\times} \left(b \widetilde{\times} c\right) = \left(a \widetilde{\times} b\right) \widetilde{\times} c$. Thus, associativity of multiplication holds for $\mathbb{Z}'$.

- Neutrality of one in $\mathbb{Z}'$: We must check that

  $$a \widetilde{\times} 1_{\mathbb{Z}'} = 1_{\mathbb{Z}'} \widetilde{\times} a = a \qquad \text{for all } a \in \mathbb{Z}'.$$

  This, too, is straightforward: If $a \in \mathbb{Z}'$, then $a \widetilde{\times} \underbrace{1_{\mathbb{Z}'}}_{=-1} = a \widetilde{\times} (-1) = -a(-1) = a$ and similarly $1_{\mathbb{Z}'} \widetilde{\times} a = a$.

- Annihilation and commutativity of multiplication are just as easy to check.

- Distributivity for $\mathbb{Z}'$: We must check that

  $$a \widetilde{\times} (b + c) = a \widetilde{\times} b + a \widetilde{\times} c \qquad \text{and} \qquad (a + b) \widetilde{\times} c = a \widetilde{\times} c + b \widetilde{\times} c$$

  for all $a, b, c \in \mathbb{Z}'$.

  So let $a, b, c \in \mathbb{Z}'$. In order to verify $a \widetilde{\times} (b + c) = a \widetilde{\times} b + a \widetilde{\times} c$, we compare

  $$a \widetilde{\times} (b + c) = -a(b + c) = -ab - ac$$

  with

  $$a \widetilde{\times} b + a \widetilde{\times} c = (-ab) + (-ac) = -ab - ac.$$

  Similarly we can check $(a + b) \widetilde{\times} c = a \widetilde{\times} c + b \widetilde{\times} c$.

So $\mathbb{Z}'$ is a ring.

(Note that $\left(\mathbb{Z}, +, \widetilde{\times}, 0, 1\right)$ is not a ring.)

However, $\mathbb{Z}'$ is not a **new** ring. It is just $\mathbb{Z}$ with its elements renamed. Namely, if we rename each integer a as $-a$, then the operations of $+$ and $\cdot$ and the elements 0 and 1 of $\mathbb{Z}$ turn into the operations $+$ and $\widetilde{\times}$ and the elements 0 and $1_{\mathbb{Z}'}$ of $\mathbb{Z}'$. This is a confusing thing to say (please don't actually rename numbers as other numbers!); the rigorous (and hopefully not confusing) way to say this is as follows: The bijection

$$\varphi : \mathbb{Z} \to \mathbb{Z}', \qquad a \mapsto -a$$

satisfies

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b) && \text{for all } a, b \in \mathbb{Z}; && (162) \\ \varphi(ab) &= \varphi(a) \widetilde{\times} \varphi(b) && \text{for all } a, b \in \mathbb{Z}; && (163) \\ \varphi(0) &= 0 = 0_{\mathbb{Z}'}; &&&& (164) \\ \varphi(1) &= -1 = 1_{\mathbb{Z}'}. &&&& (165) \end{aligned}$$

Thus, we can view φ as a way of relabelling the integers so that the data $+, \cdot, 0, 1$ of the ring $\mathbb{Z}$ become the data $+, \widetilde{\times}, 0_{\mathbb{Z}'}, 1_{\mathbb{Z}'}$ of the ring $\mathbb{Z}'$. We will later call bijections like φ "ring isomorphisms". (See Definition 5.10.1 for the definition of a ring homomorphism.)

- Recall: If A and B are two sets, then

$$B^A := \{\text{maps } A \to B\}.$$

(This notation is not wantonly chosen to annoy you with its seeming backwardness; instead, it harkens back to the fact that $\left|B^A\right| = |B|^{|A|}$.)

The set $\mathbb{Q}^{\mathbb{Q}}$ of all the maps from $\mathbb{Q}$ to $\mathbb{Q}$ is a commutative ring, where

- addition and multiplication are defined pointwise: i.e., if $f, g \in \mathbb{Q}^{\mathbb{Q}}$ are two maps, then the maps $f + g$ and $f \cdot g$ are defined by

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) && \text{and} \\ (f \cdot g)(x) &= f(x) \cdot g(x) && \text{for all } x \in \mathbb{Q}; \end{aligned}$$

- 0 means the "constant 0" function (i.e., the map $\mathbb{Q} \to \mathbb{Q},\ x \mapsto 0$);
- 1 means the "constant 1" function (i.e., the map $\mathbb{Q} \to \mathbb{Q},\ x \mapsto 1$).

All the ring axioms are easy to check. For example, each $f \in \mathbb{Q}^{\mathbb{Q}}$ has an additive inverse (namely, the map $-f \in \mathbb{Q}^{\mathbb{Q}}$ that sends each $x \in \mathbb{Q}$ to $-f(x)$).

Similarly, the sets $\mathbb{Q}^{\mathbb{C}}$ or $\mathbb{Q}^{\mathbb{N}}$ or $\mathbb{R}^{\mathbb{R}}$ (the set of "functions" you know from calculus) or $\mathbb{C}^{\mathbb{C}}$ (or, more generally, for $\mathbb{K}^S$, where $\mathbb{K}$ is any commutative ring and S is any set) can be made into commutative rings; but the set $\mathbb{N}^{\mathbb{Q}}$ cannot. The problem with $\mathbb{N}^{\mathbb{Q}}$ is that "existence of additive inverses" is not satisfied, since $-a \notin \mathbb{N}$ for positive $a \in \mathbb{N}$.

- Recall that
$$\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\} \text{ is a ring.}$$
But the set $\left\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\right\}$ (with the usual addition and multiplication) is **not** a ring. The reason is that multiplication is not a binary operation on this set, since it is possible that two numbers α and β lie in this set but their product $\alpha\beta$ does not. For example, $1 + \sqrt[3]{2}$ lies in this set, but
$$\left(1 + \sqrt[3]{2}\right)\left(1 + \sqrt[3]{2}\right) = 1 + 2\sqrt[3]{2} + \sqrt[3]{4}$$
does not. (That said, this set does satisfy all the eight ring axioms.)

- The set of 2 × 2-matrices with rational entries (endowed with matrix addition as $+$, matrix multiplication as $\cdot$, the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ as 0, and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ as 1) is a ring, but **not** a commutative ring. Indeed, the ring axioms are true (this is known from linear algebra), but commutativity of multiplication is not (the product AB of two 2×2-matrices A and B is not always equal to BA). The same applies to $n \times n$-matrices for arbitrary $n \in \mathbb{N}$. (We will see this in Corollary 5.8.11 below, in greater generality.)

- If you like the empty set, you will enjoy the *zero ring*. This is the one-element set $\{0\}$, endowed with the only possible addition (given by $0 + 0 = 0$), the only possible multiplication (given by $0 \cdot 0 = 0$), the only possible zero (namely, 0) and the only possible unity (also 0). This is a commutative ring, and is known as the *zero ring*. Resist the temptation of denoting its unity by 1, as this will quickly lead to painful confusion.

  (Some authors choose to forbid this ring, usually for no good reasons.)

- If n is an integer, then $\mathbb{Z}/n$ is a ring (with the operations $+$ and $\cdot$ that we defined, with the zero $[0]_n$ and the unity $[1]_n$). When the integer n is positive, this ring $\mathbb{Z}/n$ has n elements. (When n is prime, it can be shown that $\mathbb{Z}/n$ is the only ring with exactly n elements, up to relabeling its elements. In general, however, there can be several rings with n elements.)

- In set theory, the *symmetric difference* $A \triangle B$ of two sets A and B is defined to be the set
$$\begin{aligned}(A \cup B) \setminus (A \cap B) &= (A \setminus B) \cup (B \setminus A) \\ &= \{x \mid x \text{ belongs to } \textbf{exactly one} \text{ of } A \text{ and } B\}.\end{aligned}$$
Now, let S be any set. Let $\mathcal{P}(S)$ denote the power set of S (that is, the set of

all subsets of S). Then, it is easy to check that the following properties hold:

$$\begin{gathered}
A \triangle B = B \triangle A \qquad \text{for any sets } A \text{ and } B; \\
A \cap B = B \cap A \qquad \text{for any sets } A \text{ and } B; \\
(A \triangle B) \triangle C = A \triangle (B \triangle C) \qquad \text{for any sets } A, B, C; \\
(A \cap B) \cap C = A \cap (B \cap C) \qquad \text{for any sets } A, B, C; \\
A \triangle \varnothing = \varnothing \triangle A = A \qquad \text{for any set } A; \\
A \cap S = S \cap A = A \qquad \text{for any subset } A \text{ of } S; \\
A \triangle A = \varnothing \qquad \text{for any set } A; \\
\varnothing \cap A = A \cap \varnothing = \varnothing \qquad \text{for any set } A; \\
A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C) \qquad \text{for any sets } A, B, C; \\
(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C) \qquad \text{for any sets } A, B, C.
\end{gathered}$$

Therefore, the set $\mathcal{P}(S)$, endowed with the addition $\triangle$, the multiplication $\cap$, the zero $\varnothing$ and the unity S is a commutative ring. Furthermore, the additive inverse of any $A \in \mathcal{P}(S)$ is A itself (since $A \triangle A = \varnothing$). Moreover, each $A \in \mathcal{P}(S)$ satisfies $A \cap A = A$, which means (in the language of ring operations) that its square is itself. Thus, $\mathcal{P}(S)$ is what is called a *Boolean ring*. (See Exercise 2 on midterm #2 for the precise definition and a few properties of Boolean rings.)

Let us now see some non-examples – i.e., examples of things that are not rings:

- You probably remember the *cross product* from analytic geometry. In a nutshell: The set $\mathbb{R}^3$ of vectors in 3-dimensional space has a binary operation $\times$ defined on it, which is given by

  $$(a_1, a_2, a_3) \times (b_1, b_2, b_3) = (a_2b_3 - a_3b_2, a_3b_1 - a_1b_3, a_1b_2 - a_2b_1).$$

  Is the set $\mathbb{R}^3$, equipped with the addition $+$ and the multiplication $\times$ (and some elements playing the roles of zero and unity) a ring?

  The answer is "no", no matter which elements you want to play the roles of zero and unity. Indeed, the "Associativity of multiplication" axiom does not hold, because three vectors $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{R}^3$ usually do **not** satisfy $\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = (\mathbf{a} \times \mathbf{b}) \times \mathbf{c}$.

  Nevertheless, not all is lost; for example, the "Distributivity" axiom holds. The structure formed by the set $\mathbb{R}^3$, its addition $+$ and its cross product $\times$ is an instance of a different concept – namely, of a Lie algebra.

- So the cross product does not work; what about the dot product? The dot product of two vectors (a_1, a_2, a_3) and (b_1, b_2, b_3) in $\mathbb{R}^3$ is a real number given by

  $$(a_1, a_2, a_3) \cdot (b_1, b_2, b_3) = a_1b_1 + a_2b_2 + a_3b_3.$$

Can this be used to make $\mathbb{R}^3$ into a ring?

No, because the dot product is not even a binary operation on $\mathbb{R}^3$. Indeed, our definition of a binary operation requires that its output belongs to the same domain as its two inputs; this is clearly not true of the dot product (since its output is a real number, while its two inputs are vectors).

- The set $\left\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\right\}$ is not a ring (despite the superficial similarity to $\left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$, which is a ring), at least not if we try to use the usual multiplication of real numbers as its multiplication. In fact, this multiplication is not a binary operation on this set, because the product of $\sqrt[3]{2}$ and $\sqrt[3]{2}$ is not an element of this set.

  However, the larger set $\left\{a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 \mid a, b \in \mathbb{Z}\right\}$ is a ring (endowed with the usual addition, the usual multiplication, the usual 0 and the usual 1). (Check this!)

- For each $a, b \in \mathbb{R}$, we let $A_{a,b}$ be the function

$$\mathbb{R} \to \mathbb{R}, \qquad x \mapsto ax + b.$$

  This sort of function is called "linear function" in high school; research mathematicians prefer to call it "affine-linear function" instead (while reserving the word "linear" for a more restrictive class of functions). Let ALF be the set of these affine-linear functions $A_{a,b}$ for all $a, b \in \mathbb{R}$.

  We can define a pointwise addition $+$ on ALF; that is, for any $f, g \in A_{a,b}$, we define a function $f + g \in A_{a,b}$ by

$$(f + g)(x) = f(x) + g(x) \qquad \text{for all } x \in \mathbb{R}.$$

  We can also try to define a multiplication $\cdot$ on ALF. One obvious choice would be to define multiplication to be composition (that is, $f \cdot g = f \circ g$); another would be pointwise multiplication (that is, $(f \cdot g)(x) = f(x) \cdot g(x)$ for all $x \in \mathbb{R}$). Does any of these lead to a ring?

  No. If we define multiplication to be composition, then the "Distributivity" axiom is violated, since affine-linear functions f, g, h do not always satisfy $f \circ (g + h) = f \circ g + f \circ h$. If we define multiplication to be pointwise multiplication, then it is not a binary operation on ALF, since the pointwise product of two affine-linear functions is not an affine-linear function in general.

- You know from high school that you cannot divide by 0. Why not?

  Let us make the question precise. Of course, we cannot find an integer a that satisfies $0 \cdot a = 1$, or a real, or a complex number, etc. But could we perhaps find such a number a in some larger "number system"?

The answer, of course, depends on what "number system" means for you. If it means a ring, then we cannot find such an a in any ring.

Indeed, assume that we can. In other words, assume that there is a ring $\mathbb{K}$ that contains the usual set $\mathbb{Z}$ of integers as well as a new element ∞ such that $0 \cdot \infty = 1$. And assume (this is a very reasonable assumption) that the numbers 0 and 1 are indeed the zero and the unity of this ring. Then, the Annihilation axiom yields $0 \cdot \infty = 0$, so that $0 = 0 \cdot \infty = 1$, which is absurd. So such a ring $\mathbb{K}$ cannot exist. Thus, we cannot divide by 0, even if we extend our "number system".

- Here is an "almost-ring" beloved to combinatorialists: the *max-plus semiring* $\mathbb{T}$ (also known as the *tropical semiring*[152]).

  We introduce a new symbol $-\infty$, and we set $\mathbb{T} = \mathbb{Z} \cup \{-\infty\}$ as sets. But we do **not** "inherit" the addition and multiplication from $\mathbb{Z}$. Instead, let us define two new "addition" and "multiplication" operations $+_{\mathbb{T}}$ and $\cdot_{\mathbb{T}}$ (not to be mistaken for the original addition $+$ and multiplication $\cdot$ of integers) as follows:

$$a +_{\mathbb{T}} b = \max\{a, b\};$$
$$a \cdot_{\mathbb{T}} b = a + b \qquad \text{(usual addition of integers)},$$

  where we set

$$\max\{-\infty, n\} = \max\{n, -\infty\} = n \qquad \text{and}$$
$$(-\infty) + n = n + (-\infty) = -\infty \qquad \text{for any } n \in \mathbb{Z} \cup \{-\infty\}.$$

  This set $\mathbb{T}$ endowed with the "addition" $+_{\mathbb{T}}$, "multiplication" $\cdot_{\mathbb{T}}$, "zero" $-\infty$ and "unity" 0 satisfies all but one of the ring axioms.[153] The only one that it does not satisfy is the existence of additive inverses. Such a structure is called a *semiring*.

- Consider the set

$$2\mathbb{Z} := \{2a \mid a \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = \{\text{all even integers}\}.$$

  Endowing this set with the usual addition and multiplication (and 0), we obtain a structure that is like a ring but has no unity. This is called a *nonunital ring*. There is no way to find a unity for it, because (for example) 2 is not a product of any two elements of $2\mathbb{Z}$.

[152] To be pedantic: The name "tropical semiring" refers to several different objects, of which $\mathbb{T}$ is but one.

[153] For example, the distributivity axiom for $\mathbb{T}$ boils down to the two identities

$$a + \max\{b, c\} = \max\{a + b, a + c\} \qquad \text{and}$$
$$\max\{a, b\} + c = \max\{a + c, b + c\}.$$

5.3. Subrings

Looking back at the examples of rings listed above, you might notice that a lot of them are "nested" inside one another: For example, the rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ form a chain $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ in which each ring not only is a subset of the subsequent one[154], but also has "the same" addition, multiplication, zero and unity as the subsequent one. Of course, when we are saying "the same" here, we do not literally mean "the same binary operation"[155]; we mean that, e.g., if we add two integers in $\mathbb{Z}$, we get the same result as if we add the same two integers as elements of $\mathbb{Q}$, or as elements of $\mathbb{R}$, or as elements of $\mathbb{C}$. In other words, the addition operation of the ring $\mathbb{Z}$ is a **restriction** of the addition operation of the ring $\mathbb{Q}$, which in turn is a restriction of the addition operation of the ring $\mathbb{R}$, etc.. The same holds for multiplication. The zeroes of the rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are literally identical, as are the unities of these rings.

It is worth introducing a name for this situation:

> **Definition 5.3.1.** Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. We say that $\mathbb{K}$ is a *subring* of $\mathbb{L}$ if and only if it satisfies the following five requirements:
>
> - the set $\mathbb{K}$ is a subset of $\mathbb{L}$;
> - the addition of $\mathbb{K}$ is a restriction of the addition of $\mathbb{L}$ (that is, we have $a_1 +_{\mathbb{K}} a_2 = a_1 +_{\mathbb{L}} a_2$ for all $a_1, a_2 \in \mathbb{K}$);
> - the multiplication of $\mathbb{K}$ is a restriction of the multiplication of $\mathbb{L}$ (that is, we have $a_1 \cdot_{\mathbb{K}} a_2 = a_1 \cdot_{\mathbb{L}} a_2$ for all $a_1, a_2 \in \mathbb{K}$);
> - the zero of $\mathbb{K}$ is the zero of $\mathbb{L}$ (that is, we have $0_{\mathbb{K}} = 0_{\mathbb{L}}$);
> - the unity of $\mathbb{K}$ is the unity of $\mathbb{L}$ (that is, we have $1_{\mathbb{K}} = 1_{\mathbb{L}}$).

Thus, according to this definition:

- the ring $\mathbb{Z}$ is a subring of $\mathbb{Q}$;
- the ring $\mathbb{Q}$ is a subring of $\mathbb{R}$;
- the ring $\mathbb{R}$ is a subring of $\mathbb{C}$;

[154] To be fully honest, we are relying on Convention 4.1.7 in order to make $\mathbb{R}$ a subset of $\mathbb{C}$. And if you look closely at the definitions of $\mathbb{Q}$ and $\mathbb{R}$, the relations $\mathbb{Z} \subseteq \mathbb{Q}$ and $\mathbb{Q} \subseteq \mathbb{R}$ are also not immediately satisfied but rather rely on similar conventions. For example, rational numbers are defined as equivalence classes of pairs of integers; an integer is not an equivalence class of such pairs. Thus, we need a convention which identifies each integer z with an appropriate rational number in order to turn $\mathbb{Z}$ into a subset of $\mathbb{Q}$. Similarly for turning $\mathbb{Q}$ into a subset of $\mathbb{R}$. But let us not worry about this issue for now.

[155] The addition of $\mathbb{R}$ is a map from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, while the addition of $\mathbb{C}$ is a map from $\mathbb{C} \times \mathbb{C}$ to $\mathbb{C}$. Thus, of course, these two additions are not literally the same binary operation.

- the ring $\mathbb{Z}[i]$ (of Gaussian integers) is a subring of $\mathbb{C}$;
- every ring $\mathbb{K}$ is a subring of itself.

What is an example of two rings $\mathbb{K}$ and $\mathbb{L}$ for which the set $\mathbb{K}$ is a **subset** of $\mathbb{L}$ yet the ring $\mathbb{K}$ is **not a subring** of $\mathbb{L}$? Here is one example of an "almost-subring":

Example 5.3.2. One of our above examples of rings (in Section 5.2) is the power set of any set S. Namely, if S is any set, then we have observed that its power set $\mathcal{P}(S)$, endowed with the addition $\triangle$, the multiplication $\cap$, the zero $\varnothing$ and the unity S is a commutative ring. We shall refer to this ring by $\mathcal{P}(S)$ (omitting mention of its addition, multiplication, zero and unity).

Now, let T be a subset of a set S. Is $\mathcal{P}(T)$ a subring of the ring $\mathcal{P}(S)$? The first four requirements of Definition 5.3.1 are satisfied: The set $\mathcal{P}(T)$ is a subset of $\mathcal{P}(S)$; its addition is a restriction of the addition of $\mathcal{P}(S)$ (indeed, both of these additions turn two sets A and B into $A \triangle B$); its multiplication is a restriction of the multiplication of $\mathcal{P}(S)$; its zero is the zero of $\mathcal{P}(S)$. But its unity is not the unity of $\mathcal{P}(S)$ (unless $T = S$); indeed, the former unity is T, while the latter unity is S. Thus, $\mathcal{P}(T)$ is not a subring of $\mathcal{P}(S)$ (unless $T = S$). It fails the fifth requirement of Definition 5.3.1.

(As we have remarked, some authors do not require rings to have a unity. Correspondingly, these authors do not pose the fifth requirement in Definition 5.3.1. Thus, for these authors, $\mathcal{P}(T)$ is a subring of $\mathcal{P}(S)$.)

For a less subtle example, recall the ring $\mathbb{Z}'$ constructed in Section 5.2. The sets $\mathbb{Z}'$ and $\mathbb{Z}$ are identical, but the rings $\mathbb{Z}'$ and $\mathbb{Z}$ are not, so the ring $\mathbb{Z}'$ is not a subring of $\mathbb{Z}$ despite being a subset of $\mathbb{Z}$.

When we have two rings $\mathbb{K}$ and $\mathbb{L}$ such that $\mathbb{K} \subseteq \mathbb{L}$ as sets (or, more generally, such that $\mathbb{K}$ and $\mathbb{L}$ have elements in common), we generally need to be careful using the symbol "$+$": This symbol may mean both the addition of $\mathbb{K}$ and the addition of $\mathbb{L}$, and these additions might not be the same. Thus it is prudent to disambiguate its meaning by attaching a subscript "$_{\mathbb{K}}$" or "$_{\mathbb{L}}$" to it. The same applies to the symbols "$\cdot$", "0" and "1" and expressions like "ab" (which have an implicit multiplication sign). However, when $\mathbb{K}$ is a subring of $\mathbb{L}$, we do not need to take this precaution; in this case, the meaning of expressions like "$a + b$" does not depend on whether you read "$+$" as the addition of $\mathbb{K}$ or as the addition of $\mathbb{L}$.

The following facts are essentially obvious:

Proposition 5.3.3. A subring of a commutative ring is always commutative.

Proof of Proposition 5.3.3. Let $\mathbb{K}$ be a subring of a commutative ring $\mathbb{L}$. We must prove that $\mathbb{K}$ is commutative.

We have $ab = ba$ for all $a, b \in \mathbb{L}$ (since $\mathbb{L}$ is commutative). Thus, $ab = ba$ for all $a, b \in \mathbb{K}$ (since $\mathbb{K}$ is a subring of $\mathbb{L}$). In other words, $\mathbb{K}$ is commutative. This completes our proof.

Note how we were able to write expressions like "ab" and "ba" without specifying whether we were using the multiplication of $\mathbb{K}$ or the multiplication of $\mathbb{L}$. This was legitimate because $\mathbb{K}$ is a subring (not just a subset) of $\mathbb{L}$. □

Proposition 5.3.4. Let $\mathbb{L}$ be a ring. Let S be a subset of $\mathbb{L}$ that satisfies the following four conditions:[156]

- We have $0 \in S$ and $1 \in S$.
- The subset S is *closed under addition*. (This means that all $a, b \in S$ satisfy $a + b \in S$.)
- The subset S is *closed under additive inverses*. (This means that all $a \in S$ satisfy $-a \in S$.)
- The subset S is *closed under multiplication*. (This means that all $a, b \in S$ satisfy $ab \in S$.)

Then, the set S itself becomes a ring if we endow it with the following two operations:

- an addition operation $+$ which is defined as the restriction of the addition operation of the ring $\mathbb{L}$;
- a multiplication operation $\cdot$ which is defined as the restriction of the multiplication operation of the ring $\mathbb{L}$,

and the zero 0 and the unity 1. Furthermore, this ring S is a subring of $\mathbb{L}$.

Proof of Proposition 5.3.4. The addition operation $+$ that we are trying to define on S is indeed a well-defined binary operation on S, because S is closed under addition. Ditto for the multiplication operation $\cdot$. Also, 0 and 1 are elements of S (by the first of our four conditions). Thus, in order to prove that the subset S becomes a ring (when endowed with these two operations and two elements), we just need to check that it satisfies the ring axioms. This is easy: The "Existence of additive inverses" axiom follows from the fact that S is closed under additive inverses; all the remaining axioms follow from the fact that $\mathbb{L}$ is a ring. Finally, this ring S is a subring of $\mathbb{L}$, because of how we defined it. Thus, Proposition 5.3.4 is proven. □

Definition 5.3.5. Let $\mathbb{L}$ be a ring. Let S be a subset of $\mathbb{L}$ that satisfies the four conditions of Proposition 5.3.4. Then, we shall say that "S is a subring of $\mathbb{L}$". Technically speaking, this is premature, since S is so far just a subset of $\mathbb{L}$ without the structure of a ring; however, Proposition 5.3.4 shows that there is an obvious

[156] In this proposition, the symbols "$+$", "$\cdot$", "0" and "1" mean the addition, the multiplication, the zero and the unity of $\mathbb{L}$.

way of turning S into a ring (viz.: define two operations $+$ and $\cdot$ by restricting the corresponding operations of $\mathbb{L}$, and steal the zero and the unity from $\mathbb{L}$), and we shall automatically regard S as becoming a ring in this way (unless we say otherwise). We say that the operations $+$ and $\cdot$ on S (obtained by restricting the corresponding operations on $\mathbb{L}$) and the zero and the unity of S (which are exactly those of $\mathbb{L}$) are *inherited from* $\mathbb{L}$.

Thus, finding subrings of a ring $\mathbb{L}$ boils down to finding subsets that contain its 0 and 1 and are closed under addition, under additive inverses and under multiplication; the ring axioms don't need to be re-checked. This offers an easy way to discover subrings:

Example 5.3.6. Let us define a few subsets of the ring $\mathbb{Z}[i]$ and see whether they are subrings.

(a) Let

$$S_1 = \{a + bi \mid a, b \in \mathbb{Z}, \text{ and } b \text{ is even}\} = \{a + 2ci \mid a, c \in \mathbb{Z}\}.$$

Is S_1 a subring of $\mathbb{Z}[i]$?

It is easy to check that $0 \in S_1$ and $1 \in S_1$. Let us now check that S_1 is closed under multiplication: Let $\alpha, \beta \in S_1$; we need to show that $\alpha\beta \in S_1$. We have $\alpha \in S_1 = \{a + 2ci \mid a, c \in \mathbb{Z}\}$; in other words, we can write α in the form $\alpha = x + 2yi$ for some $x, y \in \mathbb{Z}$. Similarly, we can write β in the form $\beta = z + 2wi$ for some $z, w \in \mathbb{Z}$. Now, multiplying the two equalities $\alpha = x + 2yi$ and $\beta = z + 2wi$, we obtain

$$\begin{aligned}\alpha\beta &= (x + 2yi)(z + 2wi) = xz + 2xwi + 2yzi + 4yw\underbrace{i^2}_{=-1} \\ &= (xz - 4yw) + 2(xw + yz)i.\end{aligned}$$

Thus, $\alpha\beta$ can be written in the form $a + 2ci$ for some $a, c \in \mathbb{Z}$ (namely, for $a = xz - 4yw$ and $c = xw + yz$). Thus, $\alpha\beta \in S_1$. Now, forget that we fixed α, β. We thus have shown that all $\alpha, \beta \in S_1$ satisfy $\alpha\beta \in S_1$. In other words, S_1 is closed under multiplication. Similar arguments show that S_1 is closed under addition and under additive inverses. Thus, S_1 is a subring of $\mathbb{Z}[i]$.

This subring S_1 is only "half as large" as $\mathbb{Z}[i]$ (in a vague sense that can be made precise), but it has rather different properties. For example, $\mathbb{Z}[i]$ has greatest common divisors and unique factorization into primes; the subring S_1 does not.

There is nothing special about the number 2; we could have just as easily shown that $\{a + kci \mid a, c \in \mathbb{Z}\}$ is a subring of $\mathbb{Z}[i]$ for each $k \in \mathbb{Z}$.

(b) Let

$$S_2 = \{a + bi \mid a, b \in \mathbb{Z}, \text{ and } a \text{ is even}\} = \{2c + bi \mid c, b \in \mathbb{Z}\}.$$

Is S_2 a subring of $\mathbb{Z}[i]$? No, since $1 \notin S_2$.

(c) Let

$$S_3 = \{a+bi \mid a,b \in \mathbb{Z}, \text{ and } b \text{ is a multiple of } a\} = \{a+aci \mid a,c \in \mathbb{Z}\}.$$

Is S_3 a subring of $\mathbb{Z}[i]$? The subset S_3 does contain both 0 and 1 and is closed under additive inverses; but S_3 is not closed under addition (nor under multiplication). Thus, S_3 is not a subring of $\mathbb{Z}[i]$. (For a concrete example: The numbers $1+2i$ and $1+3i$ both belong to S_3, but their sum $2+5i$ does not.)

(d) Let

$$S_4 = \{a+bi \mid a,b \in \mathbb{N}\}.$$

Is S_4 a subring of $\mathbb{Z}[i]$? No, because S_4 is not closed under additive inverses (although S_4 satisfies two of the other conditions of Proposition 5.3.4).

(e) A pattern emerges: It appears that the only subrings of $\mathbb{Z}[i]$ are the ones of the form $\{a+kci \mid a,c \in \mathbb{Z}\}$ for $k \in \mathbb{Z}$. This is indeed true. (It is not hard to prove, if you are so inclined! **Hint:** Let S be any subring of $\mathbb{Z}[i]$. Clearly, S contains 1 and therefore all the integer multiples of 1; in other words, $\mathbb{Z} \subseteq S$. Hence, if $S \subseteq \mathbb{Z}$, then clearly $S = \mathbb{Z}$, which means that $S = \{a+kci \mid a,c \in \mathbb{Z}\}$ for $k=0$. Thus, we can WLOG assume that $S \not\subseteq \mathbb{Z}$. Hence, there exists at least one $a+bi \in S$ with $b \neq 0$. Thus, there exists at least one $a+bi \in S$ with $b > 0$ (indeed, if $b < 0$, then we replace this element by its additive inverse). Pick the one with the **smallest** b. Then, from $a+bi \in S$ and $a \in \mathbb{Z} \subseteq S$, we obtain $(a+bi) - a \in S$ (since S is a ring), which means that $bi \in S$. Next, argue that $S = \{a+kci \mid a,c \in \mathbb{Z}\}$ for $k=b$.)

5.4. Additive inverses, sums, powers and their properties

What can you do when you have a ring?

Convention 5.4.1. For the rest of this section, we fix a ring $\mathbb{K}$, and we denote its addition, multiplication, zero and unity by $+$, $\cdot$, 0 and 1.

One thing you can do is subtraction. This relies on the following fact:

Theorem 5.4.2. Let $a \in \mathbb{K}$. Then, a has exactly one additive inverse.

Before we prove this, let us recall how additive inverses are defined:

Definition 5.4.3. Let $a \in \mathbb{K}$. An *additive inverse* of a means an element a' of $\mathbb{K}$ such that $a + a' = a' + a = 0$.

Proof of Theorem 5.4.2. By the ring axioms, a has **at least one** additive inverse. We must thus only show that a has **at most one** additive inverse.

This can be done by the same argument that we used previously to prove that a residue class in $\mathbb{Z}/n$ has at most one inverse (in the proof of Proposition 3.5.4), but now we need to replace $\mathbb{Z}/n$, multiplication and $[1]_n$ by $\mathbb{K}$, addition and 0, respectively.

In detail: Let b and c be two additive inverses of a. We must prove that $b = c$. We have $a + b = 0$ (since b is an additive inverse of a) and $c + a = 0$ (since c is an additive inverse of a). Hence, the associativity of addition yields

$$(c + a) + b = c + \underbrace{(a + b)}_{=0} = c + 0 = c$$

(by the neutrality of zero). Comparing this with

$$\underbrace{(c + a)}_{=0} + b = 0 + b = b \qquad \text{(by the neutrality of zero)},$$

we obtain $b = c$, so our two additive inverses are equal. This shows that the additive inverse is unique. Thus, Theorem 5.4.2 is proven. □

Definition 5.4.4. **(a)** If $a \in \mathbb{K}$, then the additive inverse of a will be called $-a$. (This is well-defined, since Theorem 5.4.2 shows that this additive inverse is unique.)

(b) If $a \in \mathbb{K}$ and $b \in \mathbb{K}$, then we define the *difference* $a - b$ to be the element $a + (-b)$ of $\mathbb{K}$. This new binary operation $-$ on $\mathbb{K}$ is called "*subtraction*".

Additive inverses and subtraction satisfy certain rules that should not surprise you:

Proposition 5.4.5. Let $a, b, c \in \mathbb{K}$.

(a) We have $a - b = c$ if and only if $a = b + c$. (Roughly speaking, this means that subtraction undoes addition.)

(b) We have $-(a + b) = (-a) + (-b)$.

(c) We have $-0 = 0$.

(d) We have $0 - a = -a$.

(e) We have $-(-a) = a$.

(f) We have $-(ab) = (-a)b = a(-b)$.

(g) We have $a - b - c = a - (b + c)$. (Here and in the following, "$a - b - c$" should be read as "$(a - b) - c$".)

(h) We have $a(b - c) = ab - ac$ and $(a - b)c = ac - bc$.

(i) We have $-(a - b) = b - a$.

(j) We have $a - (-b) = a + b$.

(k) We have $(-1)a = -a$. (Here, the "1" on the left hand side means the unity of $\mathbb{K}$.)

(l) If $-a = -b$, then $a = b$.

Proof of Proposition 5.4.5. All of this is fairly straightforward to prove:

(a) $\Longrightarrow$: Assume $a - b = c$. Thus, $c = a - b = a + (-b)$ (by the definition of $a - b$). Adding b on both sides of this equation, we get

$$c + b = (a + (-b)) + b = a + \underbrace{((-b) + b)}_{\substack{=0 \\ \text{(since } -b \text{ is the} \\ \text{additive inverse of } b)}} \qquad \text{(by associativity of addition)}$$

$$= a + 0 = a$$

(by the neutrality of zero), so that $a = c + b = b + c$. This proves the "$\Longrightarrow$" direction of Proposition 5.4.5 **(a)**.

$\Longleftarrow$: Assume $a = b + c$. Adding $-b$ to both sides of this equation, we get

$$a + (-b) = \underbrace{(b + c)}_{\substack{=c+b \\ \text{(by commutativity} \\ \text{of addition)}}} + (-b) = (c + b) + (-b) = c + \underbrace{(b + (-b))}_{\substack{=0 \\ \text{(since } -b \text{ is the} \\ \text{additive inverse of } b)}}$$

$$\text{(by associativity of addition)}$$

$$= c + 0 = c$$

(by the neutrality of zero), so that $c = a + (-b) = a - b$. In other words, $a - b = c$. This proves the "$\Longleftarrow$" direction of Proposition 5.4.5 **(a)**. Thus, Proposition 5.4.5 **(a)** is proven.

(b) We need to prove that $(-a) + (-b) = -(a + b)$. In other words, we need to prove that $(-a) + (-b)$ is the additive inverse of $a + b$ (because that's what $-(a + b)$ is). In other words, we need to prove that

$$(a + b) + ((-a) + (-b)) = ((-a) + (-b)) + (a + b) = 0.$$

Associativity of addition yields

$$(a + b) + ((-a) + (-b)) = a + \left(b + \underbrace{((-a) + (-b))}_{=(-b)+(-a)} \right) = a + \underbrace{(b + ((-b) + (-a)))}_{\substack{=(b+(-b))+(-a) \\ \text{(by associativity} \\ \text{of addition)}}}$$

$$= a + \left(\underbrace{(b + (-b))}_{\substack{=0 \\ \text{(since } -b \text{ is the} \\ \text{additive inverse of } b)}} + (-a) \right) = a + \underbrace{(0 + (-a))}_{=-a}$$

$$= a + (-a) = 0$$

(since $-a$ is the additive inverse of a). Also, $(a + b) + ((-a) + (-b)) = ((-a) + (-b)) + (a + b)$ (by commutativity of addition). Combining these two equalities, we obtain

$$(a + b) + ((-a) + (-b)) = ((-a) + (-b)) + (a + b) = 0.$$

This completes the proof of Proposition 5.4.5 **(b)**.

(c) We have $0+0=0$ (by the neutrality of 0). But this shows precisely that 0 is an additive inverse of 0. In other words, $0=-0$. This proves Proposition 5.4.5 **(c)**.

(d) The definition of subtraction yields $0-a=0+(-a)=-a$ (by the neutrality of 0). This proves Proposition 5.4.5 **(d)**.

(e) Since $-a$ is an additive inverse of a, we have $(-a)+a=0$ and $a+(-a)=0$. But the same two equations say that a is an additive inverse of $-a$. In other words, $a=-(-a)$. This proves Proposition 5.4.5 **(e)**.

(f) We have $(-a)+a=0$ (since $-a$ is an additive inverse of a). But distributivity yields $(-a)\,b+ab=\underbrace{((-a)+a)}_{=0}b=0b=0$ (by annihilation). Likewise, $ab+(-a)\,b=0$. Hence, $(-a)\,b$ is an additive inverse of ab. In other words, $(-a)\,b=-(ab)$.

We have $b+(-b)=0$ (since $-b$ is an additive inverse of b). But distributivity yields $ab+a\,(-b)=a\underbrace{(b+(-b))}_{=0}=a0=0$ (by annihilation). Likewise, $a\,(-b)+ab=0$. Hence, $a\,(-b)$ is an additive inverse of ab. In other words, $a\,(-b)=-(ab)$. Combining this with $(-a)\,b=-(ab)$, we obtain $-(ab)=(-a)\,b=a\,(-b)$. This proves Proposition 5.4.5 **(f)**.

(g) The definition of subtraction yields

$$a-b-c=\underbrace{(a-b)}_{\substack{=a+(-b)\\ \text{(by the definition of}\\ \text{subtraction)}}}+(-c)=(a+(-b))+(-c)=a+((-b)+(-c))$$

(by associativity of addition). But Proposition 5.4.5 **(b)** (applied to b and c instead of a and b) yields $-(b+c)=(-b)+(-c)$. The definition of subtraction yields

$$a-(b+c)=a+\underbrace{(-(b+c))}_{=(-b)+(-c)}=a+((-b)+(-c)).$$

Comparing this with $a-b-c=a+((-b)+(-c))$, we obtain $a-b-c=a-(b+c)$. This proves Proposition 5.4.5 **(g)**.

(h) Proposition 5.4.5 **(f)** (applied to c instead of b) yields $-(ac)=(-a)\,c=a\,(-c)$.

The definition of subtraction yields $b-c=b+(-c)$ and

$$\begin{aligned}ab-ac=ab+\underbrace{(-(ac))}_{=a(-c)}=ab+a\,(-c)&=a\underbrace{(b+(-c))}_{=b-c} \qquad \text{(by distributivity)}\\ &=a\,(b-c).\end{aligned}$$

Thus, $a\,(b-c)=ab-ac$. A similar argument show that $(a-b)\,c=ac-bc$. This proves Proposition 5.4.5 **(h)**.

(i) Proposition 5.4.5 **(e)** (applied to b instead of a) yields $-(-b) = b$. But the definition of subtraction yields $a - b = a + (-b)$. Hence,

$$\begin{aligned} -(a-b) &= -(a+(-b)) = (-a) + \underbrace{(-(-b))}_{=b} \\ &\qquad \text{(by Proposition 5.4.5 **(b)**, applied to } -b \text{ instead of } b\text{)} \\ &= (-a) + b = b + (-a) \qquad \text{(by commutativity of addition)} \\ &= b - a \end{aligned}$$

(since $b - a$ is defined to be $b + (-a)$). This proves Proposition 5.4.5 **(i)**.

(j) Proposition 5.4.5 **(e)** (applied to b instead of a) yields $-(-b) = b$. The definition of subtraction yields

$$a - (-b) = a + \underbrace{(-(-b))}_{=b} = a + b.$$

This proves Proposition 5.4.5 **(j)**.

(k) Proposition 5.4.5 **(f)** (applied to 1 and a instead of a and b) yields $-(1a) = (-1)a = 1(-a)$. Hence, $(-1)a = -\underbrace{(1a)}_{=a} = -a$. This proves Proposition 5.4.5 **(k)**.

(l) Assume that $-a = -b$. Proposition 5.4.5 **(e)** (applied to b instead of a) yields $-(-b) = b$. Proposition 5.4.5 **(e)** yields $-(-a) = a$. Thus, $a = -\underbrace{(-a)}_{=-b} = -(-b) = b$. This proves Proposition 5.4.5 **(l)**. □

If $a, b \in \mathbb{K}$, then the expression "$-ab$" can be considered ambiguous, since it can be read either as "$(-a)b$" or as "$-(ab)$". But Proposition 5.4.5 **(f)** shows that these two readings yield the same result; therefore, you need not fear this ambiguity.

Furthermore, we don't need to parenthesize expressions like $a + b + c$ or abc. Indeed:

Theorem 5.4.6. Finite sums of elements of $\mathbb{K}$ can be defined in the same way as finite sums of usual (i.e., real or rational) numbers (with the empty sum defined to be 0). That is, if S is a finite set, and if $a_s \in \mathbb{K}$ for each $s \in S$, then $\sum\limits_{s\in S} a_s$ is well-defined and satisfies the usual rules, such as

$$\sum_{s\in S} (a_s + b_s) = \sum_{s\in S} a_s + \sum_{s\in S} b_s.$$

Thus, in particular, sums like $\sum\limits_{i=p}^{q} a_i$ or $a_1 + a_2 + \cdots + a_k$ are well-defined. We don't need to put parentheses or specify the order of summation in order to make them non-ambiguous.

Proof of Theorem 5.4.6. This is proven just as for numbers. (See [Grinbe15, §2.14 and §1.4] for how it is proven for numbers.) □

What about finite products? Is $\prod\limits_{s\in S} a_s$ well-defined? Not always, but only for commutative rings. Indeed, a product like $\prod\limits_{s\in S} a_s$ has no pre-defined order of multiplication (in general), so for it to be well-defined, it would have to be independent of the order; but this would require the commutativity of multiplication.

Theorem 5.4.7. **(a)** Finite products of elements of $\mathbb{K}$ can be defined in the same way as finite products of usual (i.e., real or rational) numbers (with the empty product defined to be 1) **as long as the ring $\mathbb{K}$ is commutative**.

(b) For general (not necessarily commutative) rings $\mathbb{K}$, we can still define products with a pre-determined order, such as $a_1a_2\cdots a_k$ (where $a_1, a_2, \ldots, a_k \in \mathbb{K}$). These products can be defined recursively as follows:

$$a_1a_2\cdots a_k = 1 \qquad \text{if } k = 0;$$

otherwise,

$$a_1a_2\cdots a_k = (a_1a_2\cdots a_{k-1})\, a_k.$$

These products still satisfy the rule

$$a_1a_2\cdots a_k = (a_1a_2\cdots a_i)\,(a_{i+1}a_{i+2}\cdots a_k) \qquad \text{for all } i \in \{0,1,\ldots,k\}.$$

Proof of Theorem 5.4.7. **(a)** This is proven just as for numbers. (See [Grinbe15, §2.14 and §1.4] for how it is proven for numbers, and replace every appearance of $\mathbb{A}$ in that proof by $\mathbb{K}$.)

(b) This follows from Exercise 4 **(b)** on homework set #0 (applied to the set $S = \mathbb{K}$, the binary operation $\cdot = *$, and the neutral element $e = 1$). [157]

[157] To be fully honest, we are skipping over a little subtlety here. Exercise 4 **(b)** on homework set #0 (applied to $S = \mathbb{K}$, $\cdot = *$ and $e = 1$) does indeed show that

$$a_1a_2\cdots a_k = (a_1a_2\cdots a_i)\,(a_{i+1}a_{i+2}\cdots a_k) \qquad \text{for all } i \in \{0,1,\ldots,k\}.$$

However, this exercise assumes a slightly different definition of the "k-tuple product" $a_1a_2\cdots a_k$ (which is denoted by $P(a_1,a_2,\ldots,a_k)$ in this exercise); namely, it assumes the following recursive definition:

- For $k = 0$, we set $a_1a_2\cdots a_k = 1$. (This is written as "$P() = e$" in the exercise.)
- For $k = 1$, we set $a_1a_2\cdots a_k = a_1$. (This is written as "$P(a_1) = a_1$" in the exercise.)
- For $k > 1$, we set $a_1a_2\cdots a_k = (a_1a_2\cdots a_{k-1})\, a_k$. (This is written as "$P(a_1,a_2,\ldots,a_k) = (P(a_1,a_2,\ldots,a_{k-1})) * a_k$" in the exercise.)

Comparing this definition to the one we gave in Theorem 5.4.7 **(b)**, we realize that it is slightly different; to wit, it treats the cases $k = 1$ and $k > 1$ separately, while the definition in Theorem 5.4.7 **(b)** uses the same recursive formula for all $k > 0$.

Fortunately, these two definitions are nevertheless equivalent, i.e., they yield the same value for $a_1a_2\cdots a_k$ whenever $k \in \mathbb{N}$ and $a_1, a_2, \ldots, a_k \in \mathbb{K}$. To see this, you can argue by induction on k as follows:

(Alternatively, you can find proofs in various texts on algebra, such as [Artin10, Proposition 2.1.4] or [Warner71, Appendix A], or at `https://groupprops.subwiki.org/wiki/Associative_implies_generalized_associative` .) □

Theorem 5.4.7 **(b)** is called the *general associativity theorem for rings*. Note that Theorem 5.4.7 **(b)** entails that if we have k elements $a_1, a_2, \ldots, a_k$ of a ring $\mathbb{K}$, then any two ways of parenthesizing the product $a_1 a_2 \cdots a_k$ yield the same result. For example, for $k = 4$, we have

$$\left(\left(a_1 a_2\right) a_3\right) a_4 = \left(a_1 \left(a_2 a_3\right)\right) a_4 = \left(a_1 a_2\right) \left(a_3 a_4\right) = a_1 \left(\left(a_2 a_3\right) a_4\right) = a_1 \left(a_2 \left(a_3 a_4\right)\right).$$

(It is not hard to prove this particular chain of identities by applying the associativity of multiplication in the appropriate places; but for higher values of k, such a manual approach becomes more and more cumbersome.)

What else can we do with our ring $\mathbb{K}$?

By definition, we know how to multiply two elements of $\mathbb{K}$. But there is also a natural way to multiply an element of $\mathbb{K}$ with an integer. This is defined as follows:

Definition 5.4.8. Let $a \in \mathbb{K}$ and $n \in \mathbb{Z}$. Then, we define an element na of $\mathbb{K}$ by

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{a + a + \cdots + a}_{-n \text{ times}}\right), & \text{if } n < 0 \end{cases}.$$

The "na" that we have just defined has nothing to do with the multiplication $\cdot$ of $\mathbb{K}$, since n is not (generally) an element of $\mathbb{K}$. However, when $\mathbb{K}$ is one of the usual

- When $k = 0$, the two definitions clearly yield the same value for $a_1 a_2 \cdots a_k$ (namely, the value 1).
- When $k = 1$, the two definitions also yield the same value for $a_1 a_2 \cdots a_k$ (indeed, the definition from Exercise 4 **(b)** on homework set #0 defines $a_1 a_2 \cdots a_k$ to be a_1 in this case, whereas the definition we gave in Theorem 5.4.7 **(b)** defines it to be

  $$\begin{aligned} \left(a_1 a_2 \cdots a_{k-1}\right) a_k &= \underbrace{\left(a_1 a_2 \cdots a_0\right)}_{=1} a_1 \qquad (\text{since } k = 1) \\ &= 1 a_1 = a_1 \qquad (\text{by the "Neutrality of one" axiom}), \end{aligned}$$

  and obviously these two values are the same).
- When $k > 1$, the two definitions yield the same value for $a_1 a_2 \cdots a_k$, because they define $a_1 a_2 \cdots a_k$ by the same recursive formula (viz., $a_1 a_2 \cdots a_k = \left(a_1 a_2 \cdots a_{k-1}\right) a_k$) in this case. (Here, we need the inductive hypothesis to tell us that the two definitions yield the same value for $a_1 a_2 \cdots a_{k-1}$.)

Thus, Exercise 4 **(b)** on homework set #0 can indeed be applied to our definition of $a_1 a_2 \cdots a_k$, and as a result, Theorem 5.4.7 **(b)** follows.

rings of numbers (like $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), then this kind of multiplication is a restriction of the multiplication $\cdot$ of $\mathbb{K}$ (that is, na means the same thing). Indeed, Definition 5.4.8 clearly generalizes the definition of na for rational numbers a. Furthermore, when $\mathbb{K} = \mathbb{Z}/n$ for some integer n, Definition 5.4.8 agrees with Definition 3.4.18 (in the sense that both definitions yield the same result for $r\alpha$ when $r \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}/n$). (This is easy to prove by induction.)

The "na" multiplication introduced in Definition 5.4.8 has several properties that you would expect such an operation to have:

Proposition 5.4.9. We have

$$(n+m)\,a = na + ma \qquad \text{for all } a \in \mathbb{K} \text{ and } n, m \in \mathbb{Z}; \tag{166}$$

$$n\,(a+b) = na + nb \qquad \text{for all } a, b \in \mathbb{K} \text{ and } n \in \mathbb{Z}; \tag{167}$$

$$-\,(na) = (-n)\,a = n\,(-a) \qquad \text{for all } a \in \mathbb{K} \text{ and } n \in \mathbb{Z}; \tag{168}$$

$$(nm)\,a = n\,(ma) \qquad \text{for all } a \in \mathbb{K} \text{ and } n, m \in \mathbb{Z}; \tag{169}$$

$$n\,(ab) = (na)\,b = a\,(nb) \qquad \text{for all } a, b \in \mathbb{K} \text{ and } n \in \mathbb{Z}; \tag{170}$$

$$n0_{\mathbb{K}} = 0_{\mathbb{K}} \qquad \text{for all } n \in \mathbb{Z}; \tag{171}$$

$$1a = a \qquad \text{for all } a \in \mathbb{K} \tag{172}$$
$$\text{(here, the "1" means the integer 1)};$$

$$0a = 0_{\mathbb{K}} \qquad \text{for all } a \in \mathbb{K} \tag{173}$$
$$\text{(here, the "0" on the left hand side means the integer 0)};$$

$$(-1)\,a = -a \qquad \text{for all } a \in \mathbb{K}; \tag{174}$$
$$\text{(here, the "} -1\text{" means the integer } -1).$$

In particular:

- The equality (168) shows that the expression "$-na$" (with $a \in \mathbb{K}$ and $n \in \mathbb{Z}$) is unambiguous (since its two possible interpretations, namely $-\,(na)$ and $(-n)\,a$, yield equal results).
- The equality (169) shows that the expression "nma" (with $a \in \mathbb{K}$ and $n, m \in \mathbb{Z}$) is unambiguous.
- The equality (170) shows that the expression "nab" (with $a, b \in \mathbb{K}$ and $n \in \mathbb{Z}$) is unambiguous.

Exercise 5.4.1. Prove Proposition 5.4.9.

[**Hint:** The proofs of the rules in Proposition 5.4.9 are analogous to the proofs of the corresponding rules for rationals – at least if you know the right proofs of the latter. One way is to start by proving the equalities (173), (172) and (174), which follow almost immediately from Definition 5.4.8; then, prove (166) for $n, m \in \mathbb{N}$; then, prove (171) and (167) for $n \in \mathbb{N}$; then, prove (169) for $n, m \in \mathbb{N}$;

then, prove (170) for $n \in \mathbb{N}$; then, show that $(-n)\,a = -(na)$ for all $a \in \mathbb{K}$ and $n \in \mathbb{Z}$ (by distinguishing between the cases $n > 0$, $n = 0$ and $n < 0$); and then extend the identities that have already been shown for elements of $\mathbb{N}$ to elements of $\mathbb{Z}$ (using Proposition 5.4.5). Note that this is rather similar to the process by which we proved Proposition 4.1.20 in the solution to Exercise 4.1.1, with the main difference being that we now are studying multiples instead of powers (and addition instead of multiplication). Our solution to Exercise 4.1.1 cannot be copied literally, however, because the way we defined na for negative n in Definition 5.4.8 is somewhat different from the way we defined α^n for negative n in Definition 4.1.19.]

We can also define powers of elements of a ring:

Definition 5.4.10. Let $a \in \mathbb{K}$ and $n \in \mathbb{N}$. Then, we define an element a^n of $\mathbb{K}$ by

$$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ times}}.$$

This definition clearly generalizes the definition of a^n for rational numbers a. Furthermore, when $\mathbb{K} = \mathbb{Z}/n$ for some integer n, Definition 5.4.10 agrees with Definition 3.4.20 (in the sense that both definitions yield the same result for α^k when $\alpha \in \mathbb{Z}/n$ and $k \in \mathbb{N}$). (This follows from Theorem 3.4.26 **(c)**.) Furthermore, when $\mathbb{K} = \mathbb{C}$, Definition 5.4.10 agrees with Definition 4.1.18.

Powers of elements of a ring satisfy some properties you would expect but fail to satisfy some others:

Proposition 5.4.11. (a) We have

$$a^0 = 1 \qquad \text{for all } a \in \mathbb{K}; \tag{175}$$

$$1^n = 1 \qquad \text{for all } n \in \mathbb{N} \tag{176}$$

$$\text{(here, the "1" means the unity of } \mathbb{K}\text{)};$$

$$0^n = \begin{cases} 0, & \text{if } n > 0 \\ 1, & \text{if } n = 0 \end{cases} \qquad \text{for all } n \in \mathbb{N} \tag{177}$$

$$\text{(here, the "0" in "}0^n\text{" means the zero of } \mathbb{K}\text{)};$$

$$a^{n+m} = a^n a^m \qquad \text{for all } a \in \mathbb{K} \text{ and } n, m \in \mathbb{N}; \tag{178}$$

$$(a^n)^m = a^{nm} \qquad \text{for all } a \in \mathbb{K} \text{ and } n, m \in \mathbb{N}. \tag{179}$$

(b) For any $a, b \in \mathbb{K}$, we have

$$\begin{aligned}(a+b)^2 &= (a+b)\,(a+b) = a\,(a+b) + b\,(a+b) \\ &= aa + ab + ba + bb = a^2 + ab + ba + b^2.\end{aligned}$$

This further equals $a^2 + 2ab + b^2$ if $\mathbb{K}$ is commutative.

(c) Let $a, b \in \mathbb{K}$ satisfy $ab = ba$. (This holds automatically when $\mathbb{K}$ is commutative.) Then:

$$ab^n = b^n a \qquad \text{for all } n \in \mathbb{N}; \tag{180}$$

$$a^i b^j = b^j a^i \qquad \text{for all } i, j \in \mathbb{N}; \tag{181}$$

$$(ab)^n = a^n b^n \qquad \text{for all } n \in \mathbb{N}; \tag{182}$$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad \text{for all } n \in \mathbb{N}. \tag{183}$$

(d) Let $a, b \in \mathbb{K}$ satisfy $ab = ba$. Then,

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right) \qquad \text{for all } n \in \mathbb{N}.$$

Proof of Proposition 5.4.11 (sketched). **(a)** The equality (175) follows from the definition of products (specifically, the part when empty products were defined to be 1). The proof of (176) is analogous to the proof of Proposition 4.1.20 **(e)**. The proof of (177) is almost obvious (just observe that $0^n = 0 \cdot 0^{n-1} = 0$ whenever $n > 0$). The proof of (178) is analogous to the proof of Proposition 4.1.20 **(b)**. The proof of (179) is analogous to the proof of Proposition 4.1.20 **(d)**.

(b) Expand using distributivity.

(c) First prove (180) by induction on n [158]. Then, prove (181) by induction on j (using (180) in the induction step)[159]. Then, prove (182) by induction on n

[158] Here are the details:

Proof of (180): We shall prove (180) by induction on n:

Induction base: Applying (175) to b instead of a, we conclude that $b^0 = 1$. Thus, $a \underbrace{b^0}_{=1} = a$ and $\underbrace{b^0}_{=1} a = a$. Comparing these two equalities, we find $ab^0 = b^0 a$. In other words, (180) holds for $n = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume that (180) holds for $n = m$. We must prove that (180) holds for $n = m + 1$.

We have assumed that (180) holds for $n = m$. In other words, we have $ab^m = b^m a$. But the definition of b^1 yields $b^1 = \underbrace{b \cdot b \cdot \cdots \cdot b}_{1 \text{ times}} = b$. Now, (178) (applied to b, m and 1 instead of a, n and m) yields $b^{m+1} = b^m \underbrace{b^1}_{=b} = b^m b$. Hence,

$$a \underbrace{b^{m+1}}_{=b^m b} = \underbrace{ab^m}_{=b^m a} b = b^m \underbrace{ab}_{=ba} = \underbrace{b^m b}_{=b^{m+1}} a = b^{m+1} a.$$

In other words, (180) holds for $n = m + 1$. This completes the induction step. Hence, the induction proof of (180) is complete.

[159] Alternatively, you can prove (181) as follows:

Let $i, j \in \mathbb{N}$. We must prove that $a^i b^j = b^j a^i$.

We have $ab = ba$, thus $ba = ab$. Hence, (180) (applied to b, a and i instead of a, b and n) yields (using (180) in the induction step)[160]. Finally, prove (183) by induction on n, just as Theorem 2.17.13 is proven (but using (181) in the induction step in order to move powers of a past powers of b).

(d) For $\mathbb{K} = \mathbb{Q}$, this was proven in Exercise 1 on homework set #0. The proof in the case of general rings $\mathbb{K}$ is analogous[161]. □

5.5. Multiplicative inverses and fields

Convention 5.5.1. For the rest of this section, we fix a ring $\mathbb{K}$, and we denote its addition, multiplication, zero and unity by $+$, $\cdot$, 0 and 1.

Each element a of the ring $\mathbb{K}$ has an additive inverse $-a$, which satisfies $(-a) + a = a + (-a) = 0$. What about a "multiplicative inverse"?

$ba^i = a^i b$. In other words, $a^i b = ba^i$. Thus, (180) (applied to a^i and j instead of a and n) yields $a^i b^j = b^j a^i$. Thus, (181) is proven.

[160] Here is the argument in detail:

Proof of (182): We shall prove (182) by induction on n:

Induction base: From (175), we obtain $a^0 = 1$. Similarly, $b^0 = 1$ and $(ab)^0 = 1$. Hence, $(ab)^0 = 1 = \underbrace{1}_{=a^0} \cdot \underbrace{1}_{=b^0} = a^0 b^0$. In other words, (182) holds for $n = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume that (182) holds for $n = m$. We must prove that (182) holds for $n = m + 1$.

We have assumed that (182) holds for $n = m$. In other words, we have $(ab)^m = a^m b^m$. But the definition of b^1 yields $b^1 = \underbrace{b \cdot b \cdot \cdots \cdot b}_{1 \text{ times}} = b$. Now, (178) (applied to b, m and 1 instead of a, n and m) yields $b^{m+1} = b^m \underbrace{b^1}_{=b} = b^m b$. Similarly, $a^{m+1} = a^m a$.

But (180) (applied to $n = m$) yields $ab^m = b^m a$. Now,

$$\underbrace{a^{m+1}}_{=a^m a} \underbrace{b^{m+1}}_{=b^m b} = a^m \underbrace{ab^m}_{=b^m a} b = a^m b^m ab. \tag{184}$$

But the same argument that we used to show that $b^{m+1} = b^m b$ can be applied to ab instead of b. We thus obtain

$$(ab)^{m+1} = \underbrace{(ab)^m}_{=a^m b^m} (ab) = a^m b^m (ab) = a^m b^m ab.$$

Comparing this with (184), we obtain $(ab)^{m+1} = a^{m+1} b^{m+1}$. In other words, (182) holds for $n = m + 1$. This completes the induction step. Hence, the induction proof of (182) is complete.

[161] There is only one minor complication: We need to justify that $(a - b) a = a (a - b)$ (since this was used in the proof). Luckily, this is very easy: Just note that

$$(a - b) a = aa - \underbrace{ba}_{=ab} = aa - ab = a (a - b).$$

Definition 5.5.2. Let $a \in \mathbb{K}$. A *multiplicative inverse* of a means an element a' of $\mathbb{K}$ such that $aa' = a'a = 1$.

Multiplicative inverses don't always exist. In the ring $\mathbb{Q}$, the number 0 has none. In the ring $\mathbb{Z}$, the number 2 has none (since $\frac{1}{2} \notin \mathbb{Z}$). But when they do exist, they are unique:

Theorem 5.5.3. Let $a \in \mathbb{K}$. Then, a has **at most one** multiplicative inverse.

Proof of Theorem 5.5.3. This is analogous to Theorem 5.4.2, but we have to replace $+$ and 0 by $\cdot$ and 1. □

Warning: In Definition 5.4.3, we could have replaced "$a + a' = a' + a = 0$" by "$a + a' = 0$", since $a + a' = a' + a$ already follows from commutativity of addition. But in Definition 5.5.2, we cannot replace "$aa' = a'a = 1$" by "$aa' = 1$", since $\mathbb{K}$ need not be commutative. If we require $aa' = 1$ only, then a' is just a *right inverse* of a; such a right inverse is not necessarily unique.

The following definition generalizes Definition 3.5.6, Definition 4.1.13 and Definition 4.1.14:

Definition 5.5.4. (a) An element $a \in \mathbb{K}$ is said to be *invertible* if it has a multiplicative inverse. An invertible element is also called a *unit*.

(b) If $a \in \mathbb{K}$ is invertible, then the multiplicative inverse of a will be called a^{-1}. (This is well-defined, since Theorem 5.5.3 shows that this multiplicative inverse is unique.)

(c) Assume that $\mathbb{K}$ is commutative. If $a \in \mathbb{K}$ and $b \in \mathbb{K}$ are such that b is invertible, then we define the *quotient* a/b (also called $\frac{a}{b}$) to be the element ab^{-1} of $\mathbb{K}$. This new binary partial operation $/$ on $\mathbb{K}$ is called "*division*".

The word "partial" in "partial operation" means that it is not always defined. We already have seen this for rational numbers: We cannot divide by 0.

Again, we follow PEMDAS rules as far as division is concerned. Do not use the ambiguous expression "a/bc"; it can mean either $a/(bc)$ or $(a/b)\,c$, depending on whom you ask, and thus should always be parenthesized.

The notion of "unit" we have just defined generalizes the units of $\mathbb{Z}[i]$. Don't confuse "unit" (= invertible element) with "unity" (= $1_{\mathbb{K}}$). The unity is always a unit (by Exercise 5.5.1 **(a)** further below), but often not the only unit.

Definition 5.5.4 **(c)** generalizes the usual meaning of a/b in $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

Please do not use Definition 5.5.4 **(c)** when $\mathbb{K}$ is not commutative; that would cause confusion, since ab^{-1} and $b^{-1}a$ would have equal rights to the name "$\frac{a}{b}$".

If $\mathbb{K} = \mathbb{Z}/n$ for a positive integer n, and if $\alpha \in \mathbb{K}$, then the multiplicative inverse of α is the same as an inverse of α (as defined in Definition 3.5.2). Thus, multiplicative inverses in arbitrary rings generalize the concept of inverses in $\mathbb{Z}/n$. Likewise, they generalize inverses in $\mathbb{C}$; that is, an inverse of a complex number $\alpha \in \mathbb{C}$ (as defined in Definition 4.1.11) is the same as a multiplicative inverse of α.

Again, it is not hard to check that multiplicative inverses and division have the properties you would hope them to have:

Exercise 5.5.1. Prove the following:

(a) The element $1_{\mathbb{K}}$ of $\mathbb{K}$ is always invertible.

(b) The element $-1_{\mathbb{K}}$ of $\mathbb{K}$ is always invertible. (Note that $-1_{\mathbb{K}}$ is not always distinct from $1_{\mathbb{K}}$.)

(c) Let $a \in \mathbb{K}$ be invertible. Then, its inverse a^{-1} is invertible as well, and its inverse is $\left(a^{-1}\right)^{-1} = a$.

(d) Let $a, b \in \mathbb{K}$ be invertible. Then, their product ab is invertible as well, and its inverse is $(ab)^{-1} = b^{-1}a^{-1}$. (Mind the order of multiplication: it is $b^{-1}a^{-1}$, not $a^{-1}b^{-1}$.)

(e) Assume that $\mathbb{K}$ is commutative. Let $a, b, c, d \in \mathbb{K}$ be such that b and d are invertible. Then,

$$a/b + c/d = (ad + bc) / (bd) \qquad \text{and} \qquad (a/b)(c/d) = (ac) / (bd).$$

Some rings have many invertible elements (such as $\mathbb{Q}$, where each nonzero element is invertible), while others have few (such as $\mathbb{Z}$, whose only invertible elements are 1 and -1). The extreme case on the former end is called a *skew field* or a *field*, depending on its commutativity:

Definition 5.5.5. (a) An element $a \in \mathbb{K}$ is said to be *nonzero* if $a \neq 0$. (Here, of course, 0 means the zero of $\mathbb{K}$.)

(b) We say that $\mathbb{K}$ is a *skew field* if $0 \neq 1$ in $\mathbb{K}$ and if every nonzero $a \in \mathbb{K}$ is invertible. (Here, "$0 \neq 1$ in $\mathbb{K}$" means "$0_{\mathbb{K}} \neq 1_{\mathbb{K}}$"; we are clearly not requiring the **integers** 0 and 1 to be distinct.)

(c) We say that $\mathbb{K}$ is a *field* if $\mathbb{K}$ is a commutative skew field.

The condition "$0 \neq 1$ in $\mathbb{K}$" has been made to rule out an annoying exception. It is easy to see that if a ring $\mathbb{K}$ satisfies $0 = 1$ in $\mathbb{K}$, then it has only one element (to wit: any $a \in \mathbb{K}$ must satisfy $a = \underbrace{1}_{=0} \cdot a = 0 \cdot a = 0$), which entails that $\mathbb{K}$ is the zero ring (up to relabeling of its element 0). We do not want the zero ring to count as a skew field[162]; thus we require $0 \neq 1$ in $\mathbb{K}$ in Definition 5.5.5.

Some authors call skew fields *division rings*.

Remark 5.5.6. If you work in constructive logic, you will want to replace the condition

$$\text{"every nonzero } a \in \mathbb{K} \text{ is invertible"} \tag{185}$$

[162] just as we don't want the number 1 to count as a prime

in Definition 5.5.5 **(b)** by the stronger condition

$$\text{“every } a \in \mathbb{K} \text{ equals } 0_{\mathbb{K}} \text{ or is invertible”.} \qquad (186)$$

While the condition (186) is clearly equivalent to (185) in classical logic, it is stronger in constructive logic, because it can be applied to any $a \in \mathbb{K}$ that is not a-priori known to be either zero or nonzero (whereas (185) requires a to be known to be nonzero, which is too burdensome a requirement to make it useful in constructive logic).

Example 5.5.7. **(a)** The rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

If you work in constructive logic, then you cannot prove that $\mathbb{R}$ and $\mathbb{C}$ are fields, because constructively there is no way to tell whether a real number is 0 or not. This is not a big issue for us, since we never truly use $\mathbb{R}$ and $\mathbb{C}$ in these notes (and when we do, we can replace them by smaller subrings of $\mathbb{C}$ that can be shown to be fields constructively – such as the Gaussian rationals).

(b) The rings $\mathbb{Z}$, $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\sqrt{2}\right]$ are not fields (since, for example, 2 is not invertible in any of these rings). However, $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\sqrt{2}\right]$ would become fields if we had used $\mathbb{Q}$ instead of $\mathbb{Z}$ in their definitions.

(c) The polynomial ring $\mathbb{Z}[x]$ (which we will formally define in Chapter 7) is not a field (since, for example, x is not invertible in it). There is a way to get a field out of it, similarly to how $\mathbb{Q}$ is obtained from $\mathbb{Z}$. (This leads to the so-called *rational functions*.)

(d) Recall the commutative ring $\mathbb{Q}^{\mathbb{Q}}$; the elements of this ring are functions from $\mathbb{Q}$ to $\mathbb{Q}$, and the operations $+$ and $\cdot$ are defined pointwise. Is this ring a field?

Let us see what the multiplicative inverse of a function $f \in \mathbb{Q}^{\mathbb{Q}}$ is. If $f, g \in \mathbb{Q}^{\mathbb{Q}}$ are two functions, then we have the following chain of equivalences:

$$\begin{aligned}
& (g \text{ is the multiplicative inverse of } f) \\
\Longleftrightarrow\ & \left(fg = gf = 1_{\mathbb{Q}^{\mathbb{Q}}}\right) \\
\Longleftrightarrow\ & \left((fg)(x) = (gf)(x) = 1_{\mathbb{Q}^{\mathbb{Q}}}(x) \text{ for all } x \in \mathbb{Q}\right) \\
\Longleftrightarrow\ & (f(x) \cdot g(x) = g(x) \cdot f(x) = 1 \text{ for all } x \in \mathbb{Q}) \\
& \left(\begin{array}{c} \text{since each } x \in \mathbb{Q} \text{ satisfies } (fg)(x) = f(x) \cdot g(x) \\ \text{and } (gf)(x) = g(x) \cdot f(x) \text{ and } 1_{\mathbb{Q}^{\mathbb{Q}}}(x) = 1 \end{array}\right) \\
\Longleftrightarrow\ & \left(g(x) = \frac{1}{f(x)} \text{ for all } x \in \mathbb{Q}\right).
\end{aligned}$$

(Note that this is **not** the same as saying that f and g are inverse maps! The multiplication of $\mathbb{Q}^{\mathbb{Q}}$ is not given by composition of maps.)

This shows that a function $f \in \mathbb{Q}^{\mathbb{Q}}$ is invertible in $\mathbb{Q}^{\mathbb{Q}}$ if and only if it never takes the value 0 (because its multiplicative inverse g would have to satisfy

$g(x) = \dfrac{1}{f(x)}$ for all $x \in \mathbb{Q}$). But a function $f \in \mathbb{Q}^{\mathbb{Q}}$ can be 0 at some point and $\neq 0$ at another. Then, it is not invertible (since it is 0 at some point) yet nonzero (since it is $\neq 0$ at another). For example, the function $\operatorname{id} \in \mathbb{Q}^{\mathbb{Q}}$ is not invertible yet nonzero. Thus, $\mathbb{Q}^{\mathbb{Q}}$ is not a field.

(e) The ring $\mathbb{Q}^{2\times 2}$ of 2×2-matrices with rational entries is not a skew field. Indeed, the 2×2-matrix $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ is nonzero but not invertible. (More generally: For each $n \in \mathbb{N}$, the $n \times n$-matrices over $\mathbb{Q}$ form a ring, which we will study later. Our notion of "invertible" for elements of this ring coincides with the usual notion of "invertible" for $n \times n$-matrices in linear algebra.)

What about $\mathbb{Z}/n$?

Theorem 5.5.8. Let n be a positive integer. The ring $\mathbb{Z}/n$ is a field if and only if n is prime.

Proof of Theorem 5.5.8. $\Longleftarrow$: Assume that n is prime. We must prove that $\mathbb{Z}/n$ is a field.

First of all, $n > 1$ (since n is prime). Thus, $n \nmid 1$, so that $1 \not\equiv 0 \bmod n$, so that $0 \not\equiv 1 \bmod n$. In other words, $[0]_n \neq [1]_n$. In other words, $0 \neq 1$ in $\mathbb{Z}/n$ (since $0_{\mathbb{Z}/n} = [0]_n$ and $1_{\mathbb{Z}/n} = [1]_n$).

Also, the ring $\mathbb{Z}/n$ is commutative.

So it remains to prove that every nonzero $\alpha \in \mathbb{Z}/n$ is invertible (because then, we will immediately conclude that $\mathbb{Z}/n$ is a skew field and therefore a field).

Indeed, let $\alpha \in \mathbb{Z}/n$ be nonzero. We must prove that α is invertible.

Proposition 3.4.6 **(b)** shows that there exists a unique $a \in \{0, 1, \ldots, n-1\}$ satisfying $\alpha = [a]_n$. Consider this a. If we had $a = 0$, then $\alpha = [a]_n$ would become $\alpha = [0]_n = 0_{\mathbb{Z}/n}$, which would contradict the assumption that α is nonzero. So $a \neq 0$. Thus, $a \in \{1, 2, \ldots, n-1\}$ (since $a \in \{0, 1, \ldots, n-1\}$). Hence, Proposition 2.13.4 (applied to $i = a$ and $p = n$) shows that a is coprime to n. In other words, $a \perp n$.

Now, define a set U_n as in Corollary 3.5.5. Then, Corollary 3.5.5 **(a)** yields $[a]_n \in U_n$ (since $a \perp n$). In other words, $[a]_n$ has an inverse (by the definition of U_n). In other words, α has an inverse (since $\alpha = [a]_n$). In other words, α has a multiplicative inverse (because inverses in $\mathbb{Z}/n$ are precisely what we now call multiplicative inverses). In other words, α is invertible. So we have proven the "$\Longleftarrow$" direction of Theorem 5.5.8.

$\Longrightarrow$: Rough idea: Assume that $\mathbb{Z}/n$ is a field. We must prove that n is a prime. Assume the contrary.

We have $0 \neq 1$ in $\mathbb{Z}/n$ (since $\mathbb{Z}/n$ is a field); in other words, $0 \not\equiv 1 \bmod n$. Hence, $n \neq 1$, so that $n > 1$ (since n is a positive integer). Hence, there must exist two elements $d, e \in \{1, 2, \ldots, n-1\}$ such that $n = de$ (since n is not a prime). Consider these d and e. Theorem 3.4.4 shows that the n residue classes $[0]_n, [1]_n, \ldots, [n-1]_n$

are distinct. Hence, the residue classes $[d]_n$ and $[e]_n$ are nonzero (since $d, e \in \{1, 2, \ldots, n-1\}$ are distinct from 0). Thus, these two residue classes are invertible (since $\mathbb{Z}/n$ is a field). Thus, by Exercise 5.5.1 **(d)**, their product $[d]_n [e]_n$ is invertible as well. But this product is $[d]_n [e]_n = [de]_n = [n]_n = [0]_n = 0_{\mathbb{Z}/n}$, which is not invertible. Contradiction. Thus, the "$\Longrightarrow$" direction of Theorem 5.5.8 is proven. □

It is tricky to find a skew field that is not a field. Here is the simplest example of such a skew field:

Example 5.5.9. Informally, we have obtained $\mathbb{C}$ from $\mathbb{R}$ by throwing in a new number i that satisfies $i^2 = -1$. In order for i not to feel alone, let us introduce yet another new "number" j such that $j^2 = -1$ and $ji = -ij$. Now we try to calculate with these i and j. Of course, i and j cannot belong to a commutative ring together, but let us assume that they (and the further numbers we obtain from them) at least satisfy the ring axioms.

We have

$$i \cdot ij = \underbrace{ii}_{=i^2=-1} j = (-1) j = -j \qquad \text{and}$$
$$j \cdot ij = \underbrace{ji}_{=-ij} j = -i \underbrace{jj}_{=j^2=-1} = -i(-1) = i \qquad \text{and}$$
$$ij \cdot ij = i \underbrace{ji}_{=-ij} j = - \underbrace{ii}_{=i^2=-1} \underbrace{jj}_{=j^2=-1} = -(-1)(-1) = -1$$

and (using the distributivity laws)

$$\begin{aligned}(1 + 2i + 3ij)(2 - 3j) &= 2 + 4i + 6ij - 3j - 6ij - 9i \underbrace{j^2}_{=-1} \\ &= 2 + 4i - 3j + 9i = 2 + 13i - 3j.\end{aligned}$$

Similarly, any of these new "numbers" can be written in the form $a + bi + cj + dij$ for reals a, b, c, d.

Blithely introducing new "numbers" like this can be risky. It could happen that (just as with defining ∞ to be $\frac{1}{0}$) our new numbers would lead to contradictions. For example, what if we have some expression that involves i and j and that can be simplified to 0 in one way and simplified to 1 in another; would that mean that $0 = 1$? No; it would simply mean that the new "numbers" we have introduced do not actually exist. (Or, speaking more abstractly: that the new numbers are just the zero ring in a complicated disguise.)

So it makes sense to look for a rigorous definition of our new numbers. There is a direct (though rather painful) way of doing this: We can rigorously define our new numbers as 4-tuples (a,b,c,d) of real numbers, with addition and subtraction defined entrywise, and with multiplication given by

$$\begin{aligned}&(x_1,x_2,x_3,x_4)\cdot(y_1,y_2,y_3,y_4)\\ &=(x_1y_1-x_2y_2-x_3y_3-x_4y_4,x_1y_2+x_2y_1+x_3y_4-x_4y_3,\\ &\qquad x_1y_3-x_2y_4+x_3y_1+x_4y_2,x_1y_4+x_2y_3-x_3y_2+x_4y_1).\end{aligned}$$

(The 4-tuple (a,b,c,d) is a rigorous model for the "number" $a+bi+cj+dij$.)

These new numbers are known as the *quaternions*. It turns out that they form a skew field, albeit not a field (since commutativity is lacking). They have several properties that make them useful in physics and space geometry. For one, they encode both the dot product and the cross product of two vectors in $\mathbb{R}^3$: Namely, if $\mathbf{a}=\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}\in\mathbb{R}^3$ and $\mathbf{b}=\begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix}\in\mathbb{R}^3$ are two vectors, then the quaternion

$$\begin{aligned}&(0,a_1,a_2,a_3)\cdot(0,b_1,b_2,b_3)\\ &=\left(\underbrace{-a_1b_1-a_2b_2-a_3b_3}_{\substack{=-\mathbf{a}\cdot\mathbf{b}\\ \text{(where }\cdot\text{ stands for}\\ \text{the dot product)}}},\underbrace{a_2b_3-a_3b_2,a_3b_1-a_1b_3,a_1b_2-a_2b_1}_{\substack{\text{the three coordinates}\\ \text{of the cross product }\mathbf{a}\times\mathbf{b}}}\right).\end{aligned}$$

Also, the quaternions can be used to encode rotations in 3-dimensional space (see, e.g., [Jia13]).

Exercise 5.5.2. Let $\mathbb{K}$ be a skew field. Let $x,y\in\mathbb{K}$ satisfy $xy=0$. (Here, of course, "0" means the zero of $\mathbb{K}$.) Prove that $x=0$ or $y=0$.

Solution to Exercise 5.5.2. Assume the contrary. Thus, neither $x=0$ nor $y=0$. In other words, we have $x\neq 0$ and $y\neq 0$.

We know that $\mathbb{K}$ is a skew field. Thus, every nonzero $a\in\mathbb{K}$ is invertible (by the definition of a skew field).

The element x of $\mathbb{K}$ is nonzero (since $x\neq 0$) and thus invertible (since every nonzero $a\in\mathbb{K}$ is invertible). Hence, its inverse x^{-1} exists. Comparing $x^{-1}\underbrace{xy}_{=0}=x^{-1}0=0$ with $\underbrace{x^{-1}x}_{=1}y=1y=y$, we obtain $y=0$; this contradicts $y\neq 0$. This contradiction shows that our assumption was false. Hence, Exercise 5.5.2 is solved. □

Exercise 5.5.3. Let $\mathbb{K}$ be a ring. Let $a,b,c\in\mathbb{K}$ be such that $ab=1$ and $bc=1$. Prove that the element b is invertible and its multiplicative inverse satisfies $b^{-1}=a=c$.

Solution to Exercise 5.5.3. Comparing $abc = \underbrace{(ab)}_{=1} c = c$ with $abc = a \underbrace{(bc)}_{=1} = a$, we obtain $a = c$. Furthermore, a is a multiplicative inverse of b (since $ab = 1$ and $b \underbrace{a}_{=c} = bc = 1$). Thus, the element b has a multiplicative inverse, i.e., is invertible. Furthermore, we have $b^{-1} = a$ (since a is a multiplicative inverse of b), thus $b^{-1} = a = c$. This solves Exercise 5.5.3. □

5.6. Hunting for finite fields I

Definition 5.6.1. **(a)** The *ground set* of a ring $(\mathbb{K}, +, \cdot, 0, 1)$ is defined to be the set $\mathbb{K}$.

(b) The *elements* of a ring are defined to be the elements of its ground set.

(c) The *size* (or *cardinality*) of a ring is defined to be the size of its ground set.

(d) A ring is said to be *finite* if its size is finite (i.e., if it has only finitely many elements).

(e) A ring is said to be *trivial* if its size is 1.

We have seen a bunch of finite rings. For example, if S is a finite set, then the commutative ring $(\mathcal{P}(S), \triangle, \cap, \varnothing, S)$ (which was constructed in one of the examples in Section 5.2) has size $|\mathcal{P}(S)| = 2^{|S|}$, and thus is finite.

We also have seen infinitely many finite fields:

$$\mathbb{Z}/2, \qquad \mathbb{Z}/3, \qquad \mathbb{Z}/5, \qquad \mathbb{Z}/7, \qquad \mathbb{Z}/11, \qquad \ldots$$

Indeed, Theorem 5.5.8 yields that $\mathbb{Z}/p$ is a finite field whenever p is a prime.

Question 5.6.2. Are there any further finite fields?

Remark 5.6.3. Why do we care?

Recall Shamir's Secret Sharing Scheme, which we introduced in Subsection 1.6.7. The way we defined the Scheme, it had a problem: It relied on a spurious notion of a "uniformly random rational number", which does not exist in nature. Now we can fix this problem: Replace rational numbers by elements of a finite field. More precisely, let N again be the length of the bitstring that we want to encrypt. Pick a prime p that satisfies both $p \geq 2^N$ and $p > n$; this exists due to Theorem 2.13.43. Now, use elements of the finite field $\mathbb{Z}/p$ instead of integers. (Thus, a bitstring $a_{N-1}a_{N-2}\cdots a_0$ will be encoded as the residue class $\left[a_{N-1} \cdot 2^{N-1} + a_{N-2} \cdot 2^{N-2} + \cdots + a_0 \cdot 2^0\right]_p \in \mathbb{Z}/p$ rather than as the number $a_{N-1} \cdot 2^{N-1} + a_{N-2} \cdot 2^{N-2} + \cdots + a_0 \cdot 2^0 \in \mathbb{Z}$. This encoding can be uniquely decoded, because $p \geq 2^N$.) Instead of picking two uniformly random bitstrings **c** and **b** and transforming them into numbers c and b, just pick two uniformly random residue classes $c, b \in \mathbb{Z}/p$. (This is possible, since $\mathbb{Z}/p$ is a finite set.)

This relies on having a well-behaved notion of polynomials over $\mathbb{Z}/p$, which should satisfy the obvious analogue of Proposition 1.6.6 (with "numbers" replaced by "elements of $\mathbb{Z}/p$"). We will give a rigorous definition of this notion in Chapter 7.

Finite fields have many uses – not just in making Shamir's Secret Sharing Scheme work. One great source of applications is *coding theory*, which we will briefly encounter in Subsection 7.7.5.

Let us take some first steps towards addressing Question 5.6.2. We have found a field of size p for each prime p. Are there fields of other finite sizes? Let us first focus on the probably simplest case beyond $\mathbb{Z}/p$: Given a prime p, can we construct a field of size p^2 ?

First idea: Let us try to get such a field by "duplicating" the known field $\mathbb{Z}/p$. Thus, we fix a prime p, and consider the Cartesian product $(\mathbb{Z}/p) \times (\mathbb{Z}/p)$. Define addition, subtraction and multiplication on this Cartesian product entrywise[163]. This will yield a commutative ring with zero $\left([0]_p, [0]_p\right)$ and unity $\left([1]_p, [1]_p\right)$.

However, the element $\left([0]_p, [1]_p\right)$ of this ring is nonzero (because it is not $\left([0]_p, [0]_p\right)$) but has no inverse (since multiplying it by anything will never make its first entry anything other than $[0]_p$). So this ring is not a field.

(This is not a useless construction – we will see it in greater generality in Section 5.7 below. But it does not help us find new fields.)

Second idea: We obtained $\mathbb{C}$ from $\mathbb{R}$ by "adjoining" a square root of -1. (In abstract algebra, the verb "adjoin" means "insert" or "add" – not in the sense of the addition operation $+$, but in the sense of throwing in something new into an existing collection.)

Let us try to do this with $\mathbb{Z}/p$ instead of $\mathbb{R}$.

More generally, let us start with an arbitrary commutative ring $\mathbb{K}$, and try to "adjoin" a square root of -1 to it. We are bold and don't care whether there might already be such a square root in $\mathbb{K}$; if there is, then we will get a second one!

Let 0 and 1 stand for the zero and the unity of $\mathbb{K}$. If $\mathbb{K} = \mathbb{Z}/n$ for some integer n, then these are the residue classes $[0]_n$ and $[1]_n$.

Now, we want to define a new commutative ring $\mathbb{K}'$ by "adjoining" a square root of -1 to $\mathbb{K}$. A way to make this rigorous is as follows (just as we defined $\mathbb{C}$ rigorously in Definition 4.1.1):

[163] That is,

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d); \\ (a,b) - (c,d) &= (a-c, b-d); \\ (a,b)(c,d) &= (ac, bd) \end{aligned}$$

for all $(a,b), (c,d) \in (\mathbb{Z}/p) \times (\mathbb{Z}/p)$.

Definition 5.6.4. Let $\mathbb{K}$ be a commutative ring.

(a) Let $\mathbb{K}'$ be the set of all pairs $(a,b) \in \mathbb{K} \times \mathbb{K}$.

(b) For each $r \in \mathbb{K}$, we denote the pair $(r,0) \in \mathbb{K}'$ by $r_{\mathbb{K}'}$. We identify $r \in \mathbb{K}$ with $r_{\mathbb{K}'} = (r,0) \in \mathbb{K}'$, so that $\mathbb{K}$ becomes a subset of $\mathbb{K}'$.

(c) We let i be the pair $(0,1) \in \mathbb{K}'$.

(d) We define three binary operations $+$, $-$ and $\cdot$ on $\mathbb{K}'$ by setting

$$(a,b) + (c,d) = (a+c, b+d),$$
$$(a,b) - (c,d) = (a-c, b-d), \qquad \text{and}$$
$$(a,b) \cdot (c,d) = (ac - bd, ad + bc)$$

for all $(a,b) \in \mathbb{K}'$ and $(c,d) \in \mathbb{K}'$.

(e) If $\alpha, \beta \in \mathbb{K}'$, then we write $\alpha\beta$ for $\alpha \cdot \beta$.

You will, of course, recognize this definition to be a calque of Definition 4.1.1 with $\mathbb{R}$ and $\mathbb{C}$ replaced by $\mathbb{K}$ and $\mathbb{K}'$. The elements of $\mathbb{K}'$ are like complex numbers, but built upon $\mathbb{K}$ instead of $\mathbb{R}$.

Proposition 5.6.5. **(a)** The set $\mathbb{K}'$ defined in Definition 5.6.4 (equipped with the operations $+$ and $\cdot$ and the elements $0_{\mathbb{K}'}$ and $1_{\mathbb{K}'}$) is a commutative ring. Its subtraction is the binary operation $-$ defined in Definition 5.6.4 **(d)**.

(b) Furthermore, the ring $\mathbb{K}$ is a subring of $\mathbb{K}'$ (where we regard $\mathbb{K}$ as a subset of $\mathbb{K}'$ as explained in Definition 5.6.4 **(b)**).

Proof of Proposition 5.6.5. **(a)** Same argument as we did for $\mathbb{C}$ in the proof of Theorem 4.1.2.

(b) This is straightforward to check. □

Convention 5.6.6. For the rest of this section, we let $\mathbb{K}'$ be the commutative ring constructed in Proposition 5.6.5 (i.e., the set $\mathbb{K}'$ equipped with the operations $+$ and $\cdot$ and the elements $0_{\mathbb{K}'}$ and $1_{\mathbb{K}'}$).

Thus, if $\mathbb{K} = \mathbb{Z}/p$, then $\mathbb{K}'$ is a commutative ring with p^2 elements.

Question 5.6.7. When is $\mathbb{K}'$ is a field?

Assume that $0 \neq 1$ in $\mathbb{K}$; thus, $0 \neq 1$ in $\mathbb{K}'$ as well (since $0_{\mathbb{K}'} = (0,0) \neq (1,0) = 1_{\mathbb{K}'}$). Hence, in order for $\mathbb{K}'$ to be a field, every nonzero $\xi \in \mathbb{K}'$ needs to have a multiplicative inverse. Thus, in particular, every nonzero element of $\mathbb{K}$ must have a multiplicative inverse in $\mathbb{K}'$. It is easy to see that such an inverse, if it exists, must belong to $\mathbb{K}$ as well (i.e., it must have the form $r_{\mathbb{K}'}$ for some $r \in \mathbb{K}$); thus, this means that every nonzero element of $\mathbb{K}$ must have a multiplicative inverse in $\mathbb{K}$. In other words, $\mathbb{K}$ itself must be a field.

Thus, we assume from now on that $\mathbb{K}$ is a field. But we are not done yet. It is definitely not always true that $\mathbb{K}'$ is a field. For example, if $\mathbb{K} = \mathbb{Z}/2$, then the element $(1,1)$ of $\mathbb{K}'$ has no inverse (check this!), and so $\mathbb{K}'$ is not a field in this case. What must $\mathbb{K}$ satisfy in order for $\mathbb{K}'$ to be a field?

We know what it must satisfy: The condition is that every nonzero $\xi \in \mathbb{K}'$ has a multiplicative inverse. We just need to see when this condition holds.

So let $\xi = (x,y) \in \mathbb{K}'$ (with $x,y \in \mathbb{K}$) be nonzero. Thus, $(x,y) \neq (0,0)$.

How to find ξ^{-1} ? Notice that $\xi = (x,y) = x + yi$ (this is proven just as for complex numbers). Thus, you can try to compute ξ^{-1} by rationalizing the denominator (just as we learned to divide complex numbers):

$$\frac{1}{\xi} = \frac{1}{x+yi} = \frac{x-yi}{(x+yi)(x-yi)} = \frac{x-yi}{x^2+y^2}$$

(since $(x+yi)(x-yi) = (x,y)(x,-y) = \left(x^2+y^2,0\right)$, as you can easily see using the definition of $\cdot$ on $\mathbb{K}'$).

We need $x^2+y^2 \neq 0$ in $\mathbb{K}$ for this to work. In other words, we need the following condition to hold:

> *Condition 1:* For every pair $(x,y) \in \mathbb{K} \times \mathbb{K}$ satisfying $(x,y) \neq (0,0)$, we have $x^2+y^2 \neq 0$ in $\mathbb{K}$.

Thus, $\mathbb{K}'$ is a field if Condition 1 holds. Conversely, if $\mathbb{K}'$ is a field, then Condition 1 holds (because if $(x,y) \in \mathbb{K} \times \mathbb{K}$ satisfies $(x,y) \neq (0,0)$, then $(x,y)(x,-y) = \left(x^2+y^2,0\right)$ would have to be $\neq (0,0)$ in order for $\mathbb{K}'$ to be a field[164]). So $\mathbb{K}'$ is a field if and only if Condition 1 holds.

If $\mathbb{K} = \mathbb{Z}/p$ for some prime p, then Condition 1 can be restated as follows:

> *Condition 1':* For every pair $(x,y) \in (\mathbb{Z}/p) \times (\mathbb{Z}/p)$ satisfying $(x,y) \neq (0,0)$, we have $x^2+y^2 \neq 0$ in $\mathbb{Z}/p$.

We can further restate Condition $1'$ in terms of integers by replacing the residue classes x and y with their representatives a and b:

> *Condition 2:* For every pair $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ such that **not both** a and b are divisible by p, the sum a^2+b^2 is not divisible by p.

So the ring $\mathbb{K}'$ constructed from $\mathbb{K} = \mathbb{Z}/p$ is a field if and only if Condition 2 holds. When does Condition 2 hold?

Example 5.6.8. Let $\mathbb{K} = \mathbb{Z}/p$.

(a) If $p = 2$, then Condition 2 fails for $(a,b) = (1,1)$. So $\mathbb{K}'$ is not a field for $p = 2$.

(b) If $p = 3$, then Condition 2 holds. So $\mathbb{K}'$ is a field for $p = 3$. Thus we have found a field with $3^2 = 9$ elements.

(c) If $p = 5$, then Condition 2 fails for $(a,b) = (1,2)$. So $\mathbb{K}'$ is not a field for $p = 5$.

[164] by Exercise 5.5.2

This suggests that the following:

Proposition 5.6.9. A prime p satisfies Condition 2 if and only if $p \equiv 3 \mod 4$.

Proof of Proposition 5.6.9 (sketched). $\Longrightarrow$: Assume that a prime p satisfies Condition 2. Assume (for contradiction) that $p \not\equiv 3 \mod 4$. So p is a prime of Type 1 or 2. Thus, $p = x^2 + y^2$ for two integers x, y (by Theorem 4.2.42 **(a)**). Now, (x, y) is a pair in $\mathbb{Z} \times \mathbb{Z}$ such that **not both** x and y are divisible by p (why not?), but the sum $x^2 + y^2 = p$ is divisible by p. So Condition 2 fails for $(a, b) = (x, y)$. This proves the "$\Longrightarrow$" direction of Proposition 5.6.9.

$\Longleftarrow$: Assume that a prime p satisfies $p \equiv 3 \mod 4$. Thus, $(p-1)/2$ is an odd nonnegative integer.

We must prove that Condition 2 holds. In other words, we must prove that for every pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ such that **not both** a and b are divisible by p, the sum $a^2 + b^2$ is not divisible by p.

Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ be a pair such that **not both** a and b are divisible by p. We must prove that the sum $a^2 + b^2$ is not divisible by p.

Assume the contrary. Thus, $a^2 + b^2 \equiv 0 \mod p$.

If we had $p \mid a$, then we would have $a \equiv 0 \mod p$ and thus $a^2 + b^2 \equiv 0^2 + b^2 = b^2 \mod p$, so that $b^2 \equiv a^2 + b^2 \equiv 0 \mod p$ and thus $p \mid b^2$ and therefore $p \mid b$; but this would contradict our assumption that **not both** a and b are divisible by p. Hence, we cannot have $p \mid a$. Thus, we have $p \nmid a$. Hence, Fermat's Little Theorem (Theorem 2.15.1 **(a)**) yields $a^{p-1} \equiv 1 \mod p$. Similarly, $b^{p-1} \equiv 1 \mod p$.

From $a^2 + b^2 \equiv 0 \mod p$, we get $a^2 \equiv -b^2 \mod p$. Taking this congruence to the $(p-1)/2$-th power[165], we find

$$\left(a^2\right)^{(p-1)/2} \equiv \left(-b^2\right)^{(p-1)/2} = \underbrace{(-1)^{(p-1)/2}}_{\substack{=-1 \\ \text{(since } (p-1)/2 \text{ is odd)}}} \underbrace{\left(b^2\right)^{(p-1)/2}}_{\substack{=b^{p-1} \\ \equiv 1 \mod p}} \equiv -1 \mod p.$$

Hence,

$$-1 \equiv \left(a^2\right)^{(p-1)/2} = a^{p-1} \equiv 1 \mod p.$$

Hence, $p \mid (-1) - 1 = -2 \mid 2$, so $p = 2$ (since p is prime). This contradicts $p \equiv 3 \mod 4$. This contradiction shows that our assumption was false; thus, Condition 2 holds. This proves the "$\Longleftarrow$" direction of Proposition 5.6.9. □

Thus, if we set $\mathbb{K} = \mathbb{Z}/p$ where p is a prime of Type 3, then $\mathbb{K}'$ will be a field. So we have found a field $\mathbb{K}'$ with p^2 elements for any prime p of Type 3. What about the other primes?

We can try to vary the construction above: Instead of adjoining a square root of -1, we adjoin a square root of some other element $\eta \in \mathbb{Z}/p$.

[165] We can do this, since $(p-1)/2$ is a nonnegative integer.

Definition 5.6.10. Let $\mathbb{K}$ be a ring. A *square* (in $\mathbb{K}$) means an element of the form a^2 for some $a \in \mathbb{K}$.

Now, we generalize Definition 5.6.4 as follows:

Definition 5.6.11. Let $\mathbb{K}$ be a commutative ring. Let $\eta \in \mathbb{K}$.

(a) Let $\mathbb{K}'_\eta$ be the set of all pairs $(a, b) \in \mathbb{K} \times \mathbb{K}$.

(b) For each $r \in \mathbb{K}$, we denote the pair $(r, 0) \in \mathbb{K}'_\eta$ by $r_{\mathbb{K}'_\eta}$. We identify $r \in \mathbb{K}$ with $r_{\mathbb{K}'_\eta} = (r, 0) \in \mathbb{K}'_\eta$, so that $\mathbb{K}$ becomes a subset of $\mathbb{K}'_\eta$.

(c) We let i_η be the pair $(0, 1) \in \mathbb{K}'_\eta$.

(d) We define three binary operations $+$, $-$ and $\cdot$ on $\mathbb{K}'_\eta$ by setting

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d), \\ (a,b) - (c,d) &= (a-c, b-d), \qquad \text{and} \\ (a,b) \cdot (c,d) &= (ac + \eta bd, ad + bc) \end{aligned}$$

for all $(a, b) \in \mathbb{K}'_\eta$ and $(c, d) \in \mathbb{K}'_\eta$.

(e) If $\alpha, \beta \in \mathbb{K}'_\eta$, then we write $\alpha\beta$ for $\alpha \cdot \beta$.

Note that $\mathbb{K}'_\eta$ differs from $\mathbb{K}'$ only in how the multiplication is defined. Note also that $\mathbb{K}'_{-1} = \mathbb{K}'$.

Theorem 5.6.12. **(a)** The set $\mathbb{K}'_\eta$ defined in Definition 5.6.11 (equipped with the operations $+$ and $\cdot$ and the elements $0_{\mathbb{K}'_\eta}$ and $1_{\mathbb{K}'_\eta}$) is a commutative ring. Its subtraction is the operation $-$ defined in Definition 5.6.11 **(d)**.

(b) If $\mathbb{K}$ is a field and η is not a square in $\mathbb{K}$, then $\mathbb{K}'_\eta$ is a field.

(c) Let p be a prime. There always exists an element $\eta \in \mathbb{Z}/p$ that is not a square, **unless** $p = 2$.

Proof of Theorem 5.6.12. **(a)** This is similar to our above proof that $\mathbb{C}$ is a commutative ring.

(b) Assume that $\mathbb{K}$ is a field and that η is not a square in $\mathbb{K}$. We need to prove that $\mathbb{K}'_\eta$ is a field. In other words, we need to prove that each nonzero $\zeta \in \mathbb{K}'_\eta$ is invertible.

So let $\zeta \in \mathbb{K}'_\eta$ be nonzero, and write ζ as $\zeta = (x, y)$ with $x, y \in \mathbb{K}$. We must show that ζ is invertible.

We have $(x, y)(x, -y) = (x^2 - \eta y^2, 0)$ (by the definition of the operation $\cdot$ on $\mathbb{K}'_\eta$). If $x^2 - \eta y^2$ is nonzero, then this shows quickly that $\left(\frac{x}{x^2 - \eta y^2}, \frac{-y}{x^2 - \eta y^2} \right)$ is an inverse of $(x, y) = \zeta$, and thus ζ is invertible. So we need to prove that $x^2 - \eta y^2$ is nonzero.

Assume the contrary. Thus, $x^2 - \eta y^2 = 0$, so that $x^2 = \eta y^2$. If y is nonzero, then this can be rewritten as $\frac{x^2}{y^2} = \eta$, whence $\eta = \frac{x^2}{y^2} = \left(\frac{x}{y} \right)^2$, which contradicts the fact that η is not a square. So y cannot be nonzero. Thus, $y = 0$. Hence, $x^2 = \eta \underbrace{y^2}_{=0^2} = 0$. Since $\xi = \left(x, \underbrace{y}_{=0} \right) = (x, 0)$, we know that x is nonzero (since ξ is nonzero). Hence, x has a multiplicative inverse (since $\mathbb{K}$ is a field). Hence, multiplying $x^2 = 0$ by x^{-1}, we obtain $x = 0$, which contradicts x being nonzero. So our assumption was wrong. Theorem 5.6.12 **(b)** is proven.

(c) Assume that $p \neq 2$. Thus, $p > 2$. Hence, the two residue classes $[1]_p$ and $[p-1]_p$ in $\mathbb{Z}/p$ are distinct.

Consider the map

$$\mathbb{Z}/p \to \mathbb{Z}/p, \qquad \alpha \mapsto \alpha^2.$$

This map is **not** injective (since it sends the two distinct residue classes $[1]_p$ and $[p-1]_p$ both to $[1]_p$). Hence, it cannot be surjective either (since otherwise, the Pigeonhole Principle for Surjections would entail that it is bijective, hence injective). In other words, there exists some $\eta \in \mathbb{Z}/p$ that is not in its image. In other words, there exists an element $\eta \in \mathbb{Z}/p$ that is not a square. This proves Theorem 5.6.12 **(c)**. □

Now, if p is a prime with $p > 2$, then Theorem 5.6.12 **(c)** yields that there exists an element $\eta \in \mathbb{Z}/p$ that is not a square; therefore, Theorem 5.6.12 **(b)** shows that $\mathbb{K}'_\eta$ is a field where $\mathbb{K} = \mathbb{Z}/p$. This is a field with p^2 elements.

Is there a field of size 4, too?

We cannot get such a field by adjoining a square root to $\mathbb{Z}/2$. So let us instead try to adjoin an element j such that $j^2 = j + 1$. Formally, we can do this as follows: We define $\mathbb{K}''$ as the set of all pairs $(a, b) \in (\mathbb{Z}/2) \times (\mathbb{Z}/2)$, and we define three operations $+$, $-$ and $\cdot$ on $\mathbb{K}''$ by

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d), \\ (a,b) - (c,d) &= (a-c, b-d), \qquad \text{and} \\ (a,b) \cdot (c,d) &= (ac+bd, ad+bc+bd). \end{aligned}$$

You can check that this is a field with 4 elements.

Thus, for each prime p, we have found a field with p^2 elements.

For the sake of completeness, let me mention a **third idea** for constructing fields of size p^2: Recall that our field $\mathbb{Z}/p$ of size p consisted of residue classes of integers modulo p. What happens if we take the residue classes of Gaussian integers modulo a Gaussian prime π ?

I will not go into details, but here is a summary:

- The result is always a field of size $\mathrm{N}(\pi)$.
- If π is not unit-equivalent to an integer, then this is a field that we already know (namely, $\mathbb{Z}/p$ for $p = \mathrm{N}(\pi)$) with its elements relabelled.

- If π is unit-equivalent to an integer, then π is unit-equivalent to a prime p of Type 3, and the field of residue classes modulo π will be a field with p^2 elements. Namely, it will be the field $\mathbb{K}'$ we constructed above (for $\mathbb{K} = \mathbb{Z}/p$), with its elements relabelled.

So this approach only gets us fields of size p^2 when p is a prime of Type 3; it is thus inferior to the second idea above. Nevertheless, it illustrates a general idea: that residue classes make sense not only for integers.

Warning: When p is a prime, the ring $\mathbb{Z}/p^2$ is **not** a field; thus, the field with p^2 elements that we constructed is not $\mathbb{Z}/p^2$.

Now, what about finite fields of size $p^3, p^4, \ldots$? What about finite fields of size 6 ?

Spoiler: It turns out that the former exist, while the latter do not. We will hopefully prove this later. More generally, for an integer $n > 1$, there exists a field of size n if and only if n is a prime power (= a positive power of a prime). Even better, if n is a prime power, then a field of size n is unique up to relabeling. We hope to see a proof of this (at least of the existence part) further on in this class.

5.7. Cartesian products

Next comes a basic and unimaginative way of constructing new rings from old:

Definition 5.7.1. Let $\mathbb{K}_1, \mathbb{K}_2, \ldots, \mathbb{K}_n$ be n rings. Consider the set $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$, whose elements are n-tuples $(k_1, k_2, \ldots, k_n)$ with $k_i \in \mathbb{K}_i$.

We define operations $+$ and $\cdot$ on $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$ by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \qquad \text{and}$$
$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n).$$

Proposition 5.7.2. Let $\mathbb{K}_1, \mathbb{K}_2, \ldots, \mathbb{K}_n$ be n rings.

(a) The set $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$, endowed with the operations $+$ and $\cdot$ we just defined and with the zero $(0, 0, \ldots, 0)$ and the unity $(1, 1, \ldots, 1)$, is a ring.

(b) If the rings $\mathbb{K}_1, \mathbb{K}_2, \ldots, \mathbb{K}_n$ are commutative, then so is the ring $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$.

Proof of Proposition 5.7.2. All axioms are checked entrywise: For example, associativity of multiplication follows from comparing

$$\begin{aligned}
&\underbrace{((a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n))}_{=(a_1 b_1, a_2 b_2, \ldots, a_n b_n)} \cdot (c_1, c_2, \ldots, c_n) \\
&= (a_1 b_1, a_2 b_2, \ldots, a_n b_n) \cdot (c_1, c_2, \ldots, c_n) \\
&= ((a_1 b_1) c_1, (a_2 b_2) c_2, \ldots, (a_n b_n) c_n) \\
&= (a_1 (b_1 c_1), a_2 (b_2 c_2), \ldots, a_n (b_n c_n))
\end{aligned}$$

with

$$\begin{aligned}
&(a_1, a_2, \ldots, a_n) \cdot \underbrace{(b_1, b_2, \ldots, b_n) \cdot (c_1, c_2, \ldots, c_n)}_{=(b_1c_1, b_2c_2, \ldots, b_nc_n)} \\
&= (a_1, a_2, \ldots, a_n) \cdot (b_1c_1, b_2c_2, \ldots, b_nc_n) \\
&= (a_1 (b_1c_1), a_2 (b_2c_2), \ldots, a_n (b_nc_n)) .
\end{aligned}$$

The additive inverse of $(a_1, a_2, \ldots, a_n)$ is $(-a_1, -a_2, \ldots, -a_n)$. □

Definition 5.7.3. The ring $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$ constructed in Proposition 5.7.2 is called the *Cartesian product* (or *direct product*) of the rings $\mathbb{K}_1, \mathbb{K}_2, \ldots, \mathbb{K}_n$.

Example 5.7.4. We have already seen a Cartesian product. Indeed, recall the binary operations XOR defined back in Subsection 1.6.4.

(a) We first defined an operation XOR on bits (Definition 1.6.3), and then defined an operation XOR on bitstrings (Definition 1.6.4). It is easy to see that

$$(\{0, 1\}, \mathrm{XOR}, \cdot, 0, 1)$$

is a commutative ring. Let me call this ring $\mathbb{X}$ for now. Note that this ring $\mathbb{X}$ can be seen as $\mathbb{Z}/2$ with its elements relabeled (more precisely, the elements $[0]_2$ and $[1]_2$ of $\mathbb{Z}/2$ need to be relabelled as 0 and 1 in order to get $\mathbb{X}$); for example, the correspondence between the XOR operation on $\mathbb{X}$ and the addition on $\mathbb{Z}/2$ can be seen by comparing their results face to face:

$$\begin{array}{lcl}
0 \,\mathrm{XOR}\, 0 = 0 & \text{and} & [0]_2 + [0]_2 = [0]_2 , \\
0 \,\mathrm{XOR}\, 1 = 1 & \text{and} & [0]_2 + [1]_2 = [1]_2 , \\
1 \,\mathrm{XOR}\, 0 = 1 & \text{and} & [1]_2 + [0]_2 = [1]_2 , \\
1 \,\mathrm{XOR}\, 1 = 0 & \text{and} & [1]_2 + [1]_2 = [0]_2 .
\end{array}$$

(b) Let $m \in \mathbb{N}$. In Definition 1.6.4, we defined a binary operation XOR on $\{0, 1\}^m$, i.e., on length-m bitstrings. This gives a ring

$$\left(\{0, 1\}^m, \mathrm{XOR}, \text{entrywise multiplication}, 00 \cdots 0, 11 \cdots 1\right)$$

of bitstrings. This ring is precisely the Cartesian product

$$\underbrace{\mathbb{X} \times \mathbb{X} \times \cdots \times \mathbb{X}}_{m \text{ times}} .$$

5.8. Matrices and matrix rings

Convention 5.8.1. In this section, we fix a ring $\mathbb{K}$.

We take the familiar concept of matrices, and generalize it in a straightforward way, allowing matrices with entries in $\mathbb{K}$:

Definition 5.8.2. Given $n, m \in \mathbb{N}$, we define an *$n \times m$-matrix over* $\mathbb{K}$ to be a rectangular table with n rows and m columns whose entries are elements of $\mathbb{K}$. When $\mathbb{K}$ is clear from the context (or irrelevant), we just say "$n \times m$-matrix" instead of "$n \times m$-matrix over $\mathbb{K}$".

For example, if $\mathbb{K} = \mathbb{Q}$, then

$$\begin{pmatrix} 0 & 1/3 & -6 \\ -1 & -2/5 & 1 \end{pmatrix}$$

is a 2×3-matrix over $\mathbb{K}$.

(Formally, an $n \times m$-matrix is defined as a map from $\{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$ to $\mathbb{K}$. Its entry in row i and column j is then defined to be the image of the pair (i, j) under this map.)

Note that the "$\times$" symbol in the notion of an "$n \times m$-matrix" is just a symbol, not an invitation to actually multiply the numbers n and m together! For example, $2 \cdot 3 = 3 \cdot 2$, yet a 2×3-matrix is not the same as a 3×2-matrix.

Let us define two pieces of notation:

Definition 5.8.3. Let A be an $n \times m$-matrix over $\mathbb{K}$. Let $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, m\}$. The *$(i, j)$-th entry of A* is defined to be the entry of A in row i and column j.

Definition 5.8.4. Let $n, m \in \mathbb{N}$. Assume that we are given some element $a_{i,j} \in \mathbb{K}$ for every $(i, j) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$. Then, we shall use the notation

$$\left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m} \tag{187}$$

for the $n \times m$-matrix

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{pmatrix}$$

(this is the $n \times m$-matrix whose (i, j)-th entry is $a_{i,j}$ for all i and j).

For example,

$$(i+j)_{1\leq i\leq 3,\ 1\leq j\leq 4} = \begin{pmatrix} 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 7 \end{pmatrix} \qquad \text{and}$$

$$(i-j)_{1\leq i\leq 3,\ 1\leq j\leq 4} = \begin{pmatrix} 0 & -1 & -2 & -3 \\ 1 & 0 & -1 & -2 \\ 2 & 1 & 0 & -1 \end{pmatrix}.$$

The letters i and j in the notation (187) are not set in stone; we can use any other letters instead. For example,

$$(i-j)_{1\leq i\leq 3,\ 1\leq j\leq 4} = (x-y)_{1\leq x\leq 3,\ 1\leq y\leq 4} = (j-i)_{1\leq j\leq 3,\ 1\leq i\leq 4}.$$

Definition 5.8.5. Let $n, m \in \mathbb{N}$. Then, $\mathbb{K}^{n\times m}$ will denote the set of all $n \times m$-matrices. (Some call it $\operatorname{M}_{n,m}(\mathbb{K})$ instead.)

Again, the "×" symbol in this notation is just a symbol; it does not stand for a product of numbers.

Definition 5.8.6. **(a)** A *matrix* means an $n \times m$-matrix for some $n, m \in \mathbb{N}$.

(b) A *square matrix* means an $n \times n$-matrix for some $n \in \mathbb{N}$.

For example, $\begin{pmatrix} 1 & 2 & 6 \\ 3 & 4 & 5 \end{pmatrix}$ is a matrix, and $\begin{pmatrix} 2 & 6 \\ 4 & 5 \end{pmatrix}$ is a square matrix.

We now define various operations with matrices:

Definition 5.8.7. Fix $n, m \in \mathbb{N}$.

(a) The *sum* $A + B$ of two $n \times m$-matrices A and B is defined entrywise: i.e., if $A = (a_{i,j})_{1\leq i\leq n,\ 1\leq j\leq m}$ and $B = (b_{i,j})_{1\leq i\leq n,\ 1\leq j\leq m}$, then

$$A + B = (a_{i,j} + b_{i,j})_{1\leq i\leq n,\ 1\leq j\leq m}.$$

(b) The *difference* $A - B$ of two $n \times m$-matrices A and B is defined entrywise: i.e., if $A = (a_{i,j})_{1\leq i\leq n,\ 1\leq j\leq m}$ and $B = (b_{i,j})_{1\leq i\leq n,\ 1\leq j\leq m}$, then

$$A - B = (a_{i,j} - b_{i,j})_{1\leq i\leq n,\ 1\leq j\leq m}.$$

(c) We define *scaling* of $n \times m$-matrices as follows: If $\lambda \in \mathbb{K}$ and $A \in \mathbb{K}^{n\times m}$, then the matrix $\lambda A \in \mathbb{K}^{n\times m}$ is defined by multiplying each entry of A by λ. Formally speaking: if $A = (a_{i,j})_{1\leq i\leq n,\ 1\leq j\leq m}$, then

$$\lambda A = (\lambda a_{i,j})_{1\leq i\leq n,\ 1\leq j\leq m}.$$

To be more honest, the operation we defined in Definition 5.8.7 **(c)** should have been called "left scaling" rather than "scaling". And we should have defined an analogous operation called "right scaling", which takes an element $\lambda \in \mathbb{K}$ and a matrix $A = \left(a_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq m} \in \mathbb{K}^{n\times m}$, and returns a new matrix

$$A\lambda = \left(a_{i,j}\lambda\right)_{1\leq i\leq n,\ 1\leq j\leq m}.$$

But we will mostly be dealing with the case when the ring $\mathbb{K}$ is commutative; and in this case, we always have $A\lambda = \lambda A$ (meaning that "right scaling" and "left scaling" are the same operation). Thus, we take the liberty to neglect the "right scaling" operation. (Its properties are analogous to the corresponding properties of "left scaling" anyway.)

Let us now define an operation on matrices that is **not** computed entrywise: their product.

Definition 5.8.8. Let $n, m, p \in \mathbb{N}$. Let $A = \left(a_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq m}$ be an $n \times m$-matrix. Let $B = \left(b_{i,j}\right)_{1\leq i\leq m,\ 1\leq j\leq p}$ be an $m \times p$-matrix. Then, we define the *product AB* of the two matrices A and B by

$$AB = \left(\sum_{k=1}^{m} a_{i,k}b_{k,j}\right)_{1\leq i\leq n,\ 1\leq j\leq p}.$$

This is an $n \times p$-matrix.

So you can add together two $n \times m$-matrices, but only multiply an $n \times m$-matrix with an $m \times p$-matrix. (You cannot multiply two $n \times m$-matrices, unless $n = m$.)

Next, we define two special families of matrices:

Definition 5.8.9. **(a)** If $n, m \in \mathbb{N}$, then the *$n \times m$ zero matrix* is defined to be the $n \times m$-matrix

$$(0)_{1\leq i\leq n,\ 1\leq j\leq m} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

It is called $0_{n\times m}$.

(b) If $n \in \mathbb{N}$, then the *$n \times n$ identity matrix* is defined to be the $n \times n$-matrix

$$\left(\delta_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

where

$$\delta_{i,j} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j \end{cases}.$$

(Note that using the Iverson bracket notation we introduced in Exercise 2.17.2, we have $\delta_{i,j} = [i = j] \cdot 1_{\mathbb{K}}$.)

The $n \times n$ identity matrix is called I_n.

Note that the 0 and the 1 here are the zero and the unity of $\mathbb{K}$.

Thus, a zero matrix can be of any size, but an identity matrix has to be a square matrix.

If $n, m \in \mathbb{N}$ and $A \in \mathbb{K}^{n \times m}$, then $-A$ shall denote the matrix $0_{n\times m} - A \in \mathbb{K}^{n \times m}$.

The following rules hold for addition, subtraction, multiplication and scaling of matrices:

Theorem 5.8.10. Let $n, m, p, q \in \mathbb{N}$.

(a) We have $A + B = B + A$ for any $A, B \in \mathbb{K}^{n \times m}$.

(b) We have $A + (B + C) = (A + B) + C$ for any $A, B, C \in \mathbb{K}^{n \times m}$.

(c) We have $A + 0_{n\times m} = 0_{n\times m} + A = A$ for any $A \in \mathbb{K}^{n \times m}$.

(d) We have $A \cdot I_m = I_n \cdot A = A$ for any $A \in \mathbb{K}^{n \times m}$.

(e) In general, we **do not** have $AB = BA$. In fact, it can happen that one of AB and BA is defined and the other is not; but even if both are defined, they can be distinct (even if $\mathbb{K}$ is commutative).

(f) We have $A(BC) = (AB)C$ for any $A \in \mathbb{K}^{n \times m}$, $B \in \mathbb{K}^{m \times p}$ and $C \in \mathbb{K}^{p \times q}$.

(g) We have $A(B + C) = AB + AC$ for any $A \in \mathbb{K}^{n \times m}$ and $B, C \in \mathbb{K}^{m \times p}$.

We have $(A + B)C = AC + BC$ for any $A, B \in \mathbb{K}^{n \times m}$ and $C \in \mathbb{K}^{m \times p}$.

(h) We have $A \cdot 0_{m\times p} = 0_{n\times p}$ and $0_{p\times n} \cdot A = 0_{p\times m}$ for any $A \in \mathbb{K}^{n \times m}$.

(i) If $A, B, C \in \mathbb{K}^{n \times m}$, then we have the equivalence $(A - B = C) \iff (A = B + C)$.

(j) We have $r(A + B) = rA + rB$ for any $r \in \mathbb{K}$ and $A, B \in \mathbb{K}^{n \times m}$.

(k) We have $(r + s)A = rA + sA$ for any $r, s \in \mathbb{K}$ and $A \in \mathbb{K}^{n \times m}$.

(l) We have $r(sA) = (rs)A$ for any $r, s \in \mathbb{K}$ and $A \in \mathbb{K}^{n \times m}$.

(m) We have $r(AB) = (rA)B = A(rB)$ for any $r \in \mathbb{K}$ and $A \in \mathbb{K}^{n \times m}$ and $B \in \mathbb{K}^{m \times p}$ if $\mathbb{K}$ is commutative. The first equality also holds in general.

(n) We have $-(rA) = (-r)A = r(-A)$ for any $r \in \mathbb{K}$ and $A \in \mathbb{K}^{n \times m}$.

(o) We have $1A = A$ for any $A \in \mathbb{K}^{n \times m}$.

(p) We have $(-1)A = -A$ for any $A \in \mathbb{K}^{n \times m}$.

(q) We have $-(A + B) = (-A) + (-B)$ for any $A, B \in \mathbb{K}^{n \times m}$.

(r) We have $-0_{n\times m} = 0_{n\times m}$.

(s) We have $-(-A) = A$ for any $A \in \mathbb{K}^{n \times m}$.

(t) We have $-(AB) = (-A)B = A(-B)$ for any $A \in \mathbb{K}^{n \times m}$ and $B \in \mathbb{K}^{m \times p}$.

(u) We have $A - B - C = A - (B + C)$ for any $A, B, C \in \mathbb{K}^{n \times m}$. (Here and in the following, "$A - B - C$" should be read as "$(A - B) - C$".)

Proof of Theorem 5.8.10. Most of these are trivial. The hardest one is part **(f)**. See [Grinbe18, §2.9] for its proof[166]. □

[166] To be precise, the proof in [Grinbe18, §2.9] only handles the case when $\mathbb{K} = \mathbb{R}$. But the same argument works whenever $\mathbb{K}$ is a commutative ring. With a little modification, it works whenever $\mathbb{K}$ is any ring.

Corollary 5.8.11. Let $n \in \mathbb{N}$. The set $\mathbb{K}^{n \times n}$ of all $n \times n$-matrices (endowed with addition $+$, multiplication $\cdot$, zero $0_{n \times n}$ and unity I_n) is a ring.

Proof of Corollary 5.8.11. This follows from Theorem 5.8.10. (For example, the "Distributivity" axiom follows from Theorem 5.8.10 **(g)**, whereas the "Existence of additive inverses" follows from the fact that any $A \in \mathbb{K}^{n \times n}$ has additive inverse $-A$ [167].) □

Definition 5.8.12. Let $n \in \mathbb{N}$. The ring $\mathbb{K}^{n \times n}$ defined in Corollary 5.8.11 is called the *n-th matrix ring* over $\mathbb{K}$.

So we know that $\mathbb{K}^{n \times n}$ is a ring whenever $n \in \mathbb{N}$. Hence, Proposition 5.4.6 shows that we can define finite sums and finite products in $\mathbb{K}^{n \times n}$ (but finite products need to have the order of their factors specified: i.e., we can make sense of "$A_1 A_2 \cdots A_k$" but not of "$\prod\limits_{s \in S} A_s$"). These also make sense for non-square matrices whenever "their sizes match": e.g., you can define a sum of finitely many $n \times m$-matrices, and a product $A_1 A_2 \cdots A_k$ where each A_i is an $n_i \times n_{i+1}$-matrix (for any $n_1, n_2, \ldots, n_{k+1} \in \mathbb{N}$). Standard rules for sums and products hold, at least to the extent they don't rely on commutativity of multiplication.

But $\mathbb{K}^{n \times n}$ is not the only ring we can make out of matrices. In fact, $\mathbb{K}^{n \times n}$ is full of interesting subrings, which are obtained by restricting ourselves to special kinds of matrices. Here are some of these:

Definition 5.8.13. Let $n \in \mathbb{N}$. Let $A = \left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}$ be an $n \times n$-matrix.

(a) We say that A is *lower-triangular* if and only if

$$a_{i,j} = 0 \qquad \text{whenever } i < j.$$

(b) We say that A is *upper-triangular* if and only if

$$a_{i,j} = 0 \qquad \text{whenever } i > j.$$

(c) We say that A is *diagonal* if and only if

$$a_{i,j} = 0 \qquad \text{whenever } i \neq j.$$

For example, the 2×2-matrix $\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ is upper-triangular (but not lower-triangular), while the 2×2-matrix $\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}$ is lower-triangular (but not upper-triangular).

[167] This fact can be easily derived from Theorem 5.8.10 **(p)** and Theorem 5.8.10 **(k)**, for example (or just checked by hand).

Proposition 5.8.14. Let $n \in \mathbb{N}$.

(a) The set of all lower-triangular $n \times n$-matrices is a subring of $\mathbb{K}^{n \times n}$.

(b) The set of all upper-triangular $n \times n$-matrices is a subring of $\mathbb{K}^{n \times n}$.

(c) The set of all diagonal $n \times n$-matrices is a subring of $\mathbb{K}^{n \times n}$.

Example 5.8.15. For $n = 2$, the multiplication of lower-triangular $n \times n$-matrices looks as follows:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix},$$

and the multiplication of diagonal $n \times n$-matrices looks as follows:

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & 0 \\ 0 & cz \end{pmatrix}.$$

Proof of Proposition 5.8.14. The main "difficulty" is showing that the product of two upper-triangular matrices is upper-triangular (and similarly for lower-triangular matrices). This is [Grinbe18, Theorem 3.23 **(a)**]. □

Note that diagonal $n \times n$-matrices are "essentially" the same as n-tuples of elements of $\mathbb{K}$; the ring they form is $\underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ times}}$ in disguise. We will make this precise in Example 5.10.3 (using the notion of a ring isomorphism).

One of the most important operations on matrices is taking the transpose:

Definition 5.8.16. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $A = \left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$ be an $n \times m$-matrix. Then, we define an $m \times n$-matrix A^T by

$$A^T = \left(a_{j,i}\right)_{1 \leq i \leq m,\ 1 \leq j \leq n}.$$

Thus, for each $i \in \{1, 2, \ldots, m\}$ and $j \in \{1, 2, \ldots, n\}$, the (i, j)-th entry of A^T is the (j, i)-th entry of A. This matrix A^T is called the *transpose* of A.

For example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}^T = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}.$$

Let us use this occasion to define column vectors and row vectors:

Definition 5.8.17. Let $n \in \mathbb{N}$.

(a) A *column vector of size n* will mean an $n \times 1$-matrix.

(b) A *row vector of size n* will mean a $1 \times n$-matrix.

For example, $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ is a column vector of size 2, while $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ is a row vector of size 3. We will often identify a row vector $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \in \mathbb{K}^{1\times n}$ with the corresponding n-tuple $(a_1, a_2, \ldots, a_n)$.

If v is a column vector of size n, then v^T is a row vector of size n.

5.9. Ring homomorphisms

Definition 5.9.1. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. A *ring homomorphism* from $\mathbb{K}$ to $\mathbb{L}$ means a map $f : \mathbb{K} \to \mathbb{L}$ that satisfies the following four axioms:

- **(a)** We have $f(a+b) = f(a) + f(b)$ for all $a, b \in \mathbb{K}$. (This is called "f respects addition" or "f preserves addition".)
- **(b)** We have $f(0) = 0$. (This, of course, means $f(0_{\mathbb{K}}) = 0_{\mathbb{L}}$.)
- **(c)** We have $f(ab) = f(a) f(b)$ for all $a, b \in \mathbb{K}$. (This is called "f respects multiplication" or "f preserves multiplication".)
- **(d)** We have $f(1) = 1$. (This, of course, means $f(1_{\mathbb{K}}) = 1_{\mathbb{L}}$.)

Remark 5.9.2. The statement "$f(a+b) = f(a) + f(b)$" in Definition 5.9.1 should, of course, be understood as "$f(a +_{\mathbb{K}} b) = f(a) +_{\mathbb{L}} f(b)$". Likewise, the statement "$f(ab) = f(a) f(b)$" should be understood as "$f(a \cdot_{\mathbb{K}} b) = f(a) \cdot_{\mathbb{L}} f(b)$". In Definition 5.9.1, we could afford omitting the "$_{\mathbb{K}}$" and "$_{\mathbb{L}}$" subscripts under the "$+$" and "$\cdot$" signs because it is always clear whether the things being added (or multiplied) are in $\mathbb{K}$ or in $\mathbb{L}$; but in many practical situations we do not have such luxury (for example, because $\mathbb{K}$ and $\mathbb{L}$ have elements in common) and thus need to include these subscripts. (See Example 5.10.6 for an example of such a situation.)

Remark 5.9.3. The axiom **(b)** in Definition 5.9.1 is redundant – it follows from axiom **(a)**.

Proof of Remark 5.9.3. Assume that axiom **(a)** holds. Apply axiom **(a)** to $a = 0$ and $b = 0$. Thus, you get

$$f(0+0) = f(0) + f(0).$$

Since $0 + 0 = 0$, this rewrites as

$$f(0) = f(0) + f(0).$$

Subtracting $f(0)$ on both sides (we can do this, since $\mathbb{L}$ is a ring), we obtain $0 = f(0)$, thus $f(0) = 0$. Thus, axiom **(b)** holds. □

If the axiom **(b)** in Definition 5.9.1 is redundant, then why did we require it? One reason to do so is purely aesthetic: It ensures that each of the two "multiplicative" axioms (viz., axioms **(c)** and **(d)**) is matched by a corresponding "additive" axiom (viz., axioms **(a)** and **(b)**). We cannot omit axiom **(d)**[168]; thus, to avoid breaking the symmetry, I prefer not to omit axiom **(b)** either. But there is also another reason to keep axiom **(b)**. Indeed, if we want to define *semiring homomorphisms* (i.e., the analogue of ring homomorphisms in which rings are replaced by semirings), then axiom **(b)** is no longer redundant (since we cannot subtract elements in a semiring); thus, if we omitted axiom **(b)**, our definition of ring homomorphisms would become less robust with respect to replacing "ring" by "semiring".

Example 5.9.4. Let $\mathbb{K}$ be any ring. The map $\operatorname{id} : \mathbb{K} \to \mathbb{K}$ is a ring homomorphism.

Proof of Example 5.9.4. Let us check that id satisfies the axiom **(c)** in Definition 5.9.1: Indeed, this simply means checking that $\operatorname{id}(ab) = \operatorname{id}(a)\operatorname{id}(b)$ for all $a, b \in \mathbb{K}$. But this rewrites as $ab = ab$, which is obvious. Similarly, the other three axioms hold. □

We can slightly generalize Example 5.9.4 as follows:

Example 5.9.5. Let $\mathbb{K}$ be a subring of a ring $\mathbb{L}$. Let $\iota : \mathbb{K} \to \mathbb{L}$ be the map that sends each $a \in \mathbb{K}$ to a itself. (This map is called the *inclusion map* from $\mathbb{K}$ to $\mathbb{L}$.) Then, ι is a ring homomorphism.

Proof of Example 5.9.5. The four axioms in Definition 5.9.1 follow straight from the five requirements in Definition 5.3.1. □

Example 5.9.6. Let $\mathbb{K}$ be any ring, and let $\mathbb{M}$ be the zero ring $\{0\}$. Then, the map

$$\mathbb{K} \to \mathbb{M}, \qquad a \mapsto 0$$

is a ring homomorphism.

Proof of Example 5.9.6. Each of the four axioms in Definition 5.9.1 holds trivially for this map (since $\mathbb{M}$ has only one element, and thus any two elements of $\mathbb{M}$ are equal). □

Example 5.9.7. Let n be an integer. Consider the projection

$$\pi_{\underset{n}{\equiv}} : \mathbb{Z} \to \mathbb{Z}/n, \\ s \mapsto [s]_n .$$

This is a ring homomorphism.

[168] More precisely: if we did, then we would obtain a weaker, less useful notion of ring homomorphism.

Proof of Example 5.9.7. Again, let us check axiom **(c)** only. So let $a, b \in \mathbb{Z}$. We must prove that $\pi_{\underset{n}{\equiv}}(ab) = \pi_{\underset{n}{\equiv}}(a) \cdot \pi_{\underset{n}{\equiv}}(b)$.

The left hand side is $[ab]_n$, while the right hand side is $[a]_n \cdot [b]_n$. So they are equal, because this is how $[a]_n \cdot [b]_n$ was defined. Thus, axiom **(c)** holds. □

Example 5.9.8. Let n be a positive integer. Consider the map

$$R_n : \mathbb{Z}/n \to \mathbb{Z},$$
$$[s]_n \mapsto s\%n.$$

(This is the map sending $[0]_n, [1]_n, \ldots, [n-1]_n$ to the numbers $0, 1, \ldots, n-1$.) This map R_n is **not** a ring homomorphism.

Proof of Example 5.9.8. Assume the contrary. Thus, R_n is a ring homomorphism. We want a contradiction.

We are in one of the following two cases:

Case 1: We have $n > 1$.

Case 2: We have $n = 1$.

Let us first consider Case 1. In this case, we have $n > 1$.

We have assumed that R_n is a ring homomorphism. Thus, axiom **(a)** can be applied to $a = [1]_n$ and $b = [n-1]_n$, and thus we get $R_n([1]_n + [n-1]_n) = R_n([1]_n) + R_n([n-1]_n)$. But comparing

$$R_n([1]_n + [n-1]_n) = R_n([n]_n) = R_n([0]_n) = 0$$

with

$$\underbrace{R_n([1]_n)}_{=1} + \underbrace{R_n([n-1]_n)}_{=n-1} = 1 + (n-1) = n,$$

we see that this is not true. So we have found a contradiction in Case 1.

Let us now consider Case 2. In this case, we have $n = 1$. Thus, $[1]_1 = [0]_1$. But the map R_n maps $[0]_1$ to 0 (by its definition). However, axiom **(d)** forces $R_n([1]_1) = 1$, which contradicts $R_n([1]_1) = R_n([0]_1) = 0$. So we have found a contradiction in Case 2.

Thus, we always get a contradiction. □

Warning: The same people who don't require rings to have a unity, of course, do not require ring homomorphisms to satisfy axiom **(d)**. So for them, R_n would be a ring homomorphism for $n = 1$.

Example 5.9.9. Let n and d be integers such that $d \mid n$. Then, the map

$$\pi_{n,d} : \mathbb{Z}/n \to \mathbb{Z}/d,$$
$$[s]_n \mapsto [s]_d$$

is a ring homomorphism.

Proof of Example 5.9.9. Let us check axiom **(c)**. So we must prove that $\pi_{n,d}(\alpha\beta) = \pi_{n,d}(\alpha) \cdot \pi_{n,d}(\beta)$ for all $\alpha, \beta \in \mathbb{Z}/n$.

Fix $\alpha, \beta \in \mathbb{Z}/n$. Write α as $\alpha = [a]_n$ with $a \in \mathbb{Z}$. Write β as $\beta = [b]_n$ with $b \in \mathbb{Z}$.

Thus, $\pi_{n,d}(\alpha) = \pi_{n,d}([a]_n) = [a]_d$ and $\pi_{n,d}(\beta) = \pi_{n,d}([b]_n) = [b]_d$. Multiplying these two equalities, we obtain

$$\underbrace{\pi_{n,d}(\alpha)}_{=[a]_d} \cdot \underbrace{\pi_{n,d}(\beta)}_{=[b]_d} = [a]_d \cdot [b]_d = [ab]_d . \tag{188}$$

But $\underbrace{\alpha}_{=[a]_n} \underbrace{\beta}_{=[b]_n} = [a]_n \cdot [b]_n = [ab]_n$ and thus $\pi_{n,d}(\alpha\beta) = \pi_{n,d}([ab]_n) = [ab]_d$. Comparing this equality to (188), we conclude $\pi_{n,d}(\alpha\beta) = \pi_{n,d}(\alpha) \cdot \pi_{n,d}(\beta)$. Thus, axiom **(c)** is proven. The other three axioms are proven similarly (we leave the details to the reader). □

Remark 5.9.10. Let n and d be integers. Then:

(a) If $d \mid n$, then the only ring homomorphism from $\mathbb{Z}/n$ to $\mathbb{Z}/d$ is $\pi_{n,d}$.

(b) If $d \nmid n$, then there is no ring homomorphism from $\mathbb{Z}/n$ to $\mathbb{Z}/d$.

Remark 5.9.10 is not hard to prove, but we won't do this here.

Example 5.9.11. Consider the map $\mu : \mathbb{C} \to \mathbb{R}^{2\times 2}$ defined in Proposition 4.1.31. This map μ is a ring homomorphism.

Proof. Proposition 4.1.31 yields that the map μ satisfies axioms **(a)** and **(c)**. It is easy to see that it satisfies the other two. □

Example 5.9.12. Let $\iota_{\mathbb{C}}$ be the map

$$\mathbb{R} \to \mathbb{C},$$
$$r \mapsto r_{\mathbb{C}} = (r, 0) .$$

This is a ring homomorphism.

Proof. Theorem 4.1.5 shows that $\iota_{\mathbb{C}}$ satisfies axioms **(a)** and **(c)**. As for **(b)** and **(d)**, these follow from the fact that the zero of $\mathbb{C}$ is $0_{\mathbb{C}} = (0, 0)$ and the unity of $\mathbb{C}$ is $1_{\mathbb{C}} = (1, 0)$. □

Example 5.9.13. Let $\mathbb{K}$ be a commutative ring.

Let $\mathbb{K}^{2\leq 2}$ be the ring of upper-triangular 2×2-matrices. (This is a ring, by Proposition 5.8.14.)

Let $\mathbb{K}^{2\geq 2}$ be the ring of lower-triangular 2×2-matrices. (This is a ring, by Proposition 5.8.14.)

(a) Consider the map

$$\begin{aligned} \mathbb{K}^{2\leq 2} &\to \mathbb{K}^{2\geq 2}, \\ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} &\mapsto \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}. \end{aligned}$$

In other words, this is the map sending each A to A^T (the transpose of A). Is this a ring homomorphism? No, because $(AB)^T$ is $B^T A^T$, not $A^T B^T$ (in general). This is called a *ring antihomomorphism*. Note that if $\mathbb{K}$ was an arbitrary (not commutative) ring, then $(AB)^T$ would (in general!) equal neither $B^T A^T$ nor $A^T B^T$.

(b) Consider the map

$$\begin{aligned} \mathbb{K}^{2\leq 2} &\to \mathbb{K}^{2\geq 2}, \\ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} &\mapsto \begin{pmatrix} c & 0 \\ b & a \end{pmatrix}. \end{aligned}$$

In other words, this is the map that reverses the order of the rows and reverses the order of the columns. You can check that this is a ring homomorphism. This holds even if $\mathbb{K}$ is an arbitrary (not commutative) ring.

Proposition 5.9.14. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism.

(a) We have $f(-a) = -f(a)$ for all $a \in \mathbb{K}$. (In other words, f "preserves additive inverses".)

(b) If $a \in \mathbb{K}$ is invertible, then $f(a) \in \mathbb{L}$ is also invertible, and we have $f\left(a^{-1}\right) = (f(a))^{-1}$. (In other words, f "preserves multiplicative inverses".)

(c) We have $f(a-b) = f(a) - f(b)$ for all $a, b \in \mathbb{K}$.

(d) If the rings $\mathbb{K}$ and $\mathbb{L}$ are commutative, then we have $f\left(\dfrac{a}{b}\right) = \dfrac{f(a)}{f(b)}$ for all $a, b \in \mathbb{K}$ for which b is invertible.

(e) We have $f\left(\sum\limits_{s\in S} a_s\right) = \sum\limits_{s\in S} f(a_s)$ whenever S is a finite set and $a_s \in \mathbb{K}$ for all $s \in S$.

(f) We have $f(a_1 a_2 \cdots a_k) = f(a_1) f(a_2) \cdots f(a_k)$ whenever $a_1, a_2, \ldots, a_k \in \mathbb{K}$.

(g) If the rings $\mathbb{K}$ and $\mathbb{L}$ are commutative, then $f\left(\prod\limits_{s\in S} a_s\right) = \prod\limits_{s\in S} f(a_s)$ whenever S is a finite set and $a_s \in \mathbb{K}$ for all $s \in S$.

(h) We have $f(a^n) = (f(a))^n$ for each $a \in \mathbb{K}$ and each $n \in \mathbb{N}$.

(i) We have $f(na) = nf(a)$ for each $a \in \mathbb{K}$ and each $n \in \mathbb{Z}$.

Proof of Proposition 5.9.14. The map f is a ring homomorphism, and thus satisfies the four axioms **(a)**, **(b)**, **(c)** and **(d)** of Definition 5.9.1.

(b) Let $a \in \mathbb{K}$ be invertible. We have

$$f\left(a^{-1}a\right) = f\left(a^{-1}\right) f\left(a\right) \qquad \text{(by axiom (c))}.$$

Thus,

$$f\left(a^{-1}\right) f\left(a\right) = f\left(\underbrace{a^{-1}a}_{=1}\right) = f\left(1\right) = 1 \qquad \text{(by axiom (d))}.$$

Similarly, $f\left(a\right) f\left(a^{-1}\right) = 1$. These two equations are saying that $f\left(a^{-1}\right)$ is a multiplicative inverse of $f\left(a\right)$. Thus, $f\left(a\right)$ is invertible, and $f\left(a^{-1}\right) = \left(f\left(a\right)\right)^{-1}$. This proves Proposition 5.9.14 **(b)**.

(a) Repeat the proof we just gave for Proposition 5.9.14 **(b)**, but replace multiplication and 1 by addition and 0 (and forget about invertibility, because every element of $\mathbb{K}$ or $\mathbb{L}$ has an additive inverse).

(c) Let $a, b \in \mathbb{K}$. Then, $a - b = a + (-b)$ (by the definition of subtraction). Thus,

$$\begin{aligned} f\left(a-b\right) &= f\left(a+(-b)\right) = f\left(a\right) + \underbrace{f\left(-b\right)}_{\substack{=-f(b) \\ \text{(by Proposition 5.9.14 (a))}}} \qquad \text{(by axiom (a))} \\ &= f\left(a\right) + \left(-f\left(b\right)\right) = f\left(a\right) - f\left(b\right) \end{aligned}$$

(since the definition of subtraction yields $f\left(a\right) - f\left(b\right) = f\left(a\right) + \left(-f\left(b\right)\right)$). This proves Proposition 5.9.14 **(c)**.

(d) Similar to part **(c)**, but addition is replaced by multiplication.

(e) Induction on $|S|$. The induction base uses axiom **(b)**; the induction step uses axiom **(a)**.

(f) Induction on k. The induction base uses axiom **(d)**; the induction step uses axiom **(c)**.

(g) Induction on $|S|$. The induction base uses axiom **(d)**; the induction step uses axiom **(c)**.

(h) Follows from Proposition 5.9.14 **(f)**, applied to $k = n$ and $a_i = a$.

(i) If $n \geq 0$, then Definition 5.4.8 yields $na = \underbrace{a + a + \cdots + a}_{n \text{ times}}$ and $nf\left(a\right) = \underbrace{f\left(a\right) + f\left(a\right) + \cdots + f\left(a\right)}_{n \text{ times}}$. Thus, if $n \geq 0$, then Proposition 5.9.14 **(i)** boils down to

$$f\left(\underbrace{a + a + \cdots + a}_{n \text{ times}}\right) = \underbrace{f\left(a\right) + f\left(a\right) + \cdots + f\left(a\right)}_{n \text{ times}},$$

which follows from Proposition 5.9.14 **(e)** (applied to $S = \{1, 2, \ldots, n\}$ and $a_s = a$). The case when $n < 0$ can be reduced to the case when $n \geq 0$ by using Proposition 5.9.14 **(a)**. □

The composition of two ring homomorphisms is again a ring homomorphism, as the following proposition shows:

Proposition 5.9.15. Let $\mathbb{K}$, $\mathbb{L}$ and $\mathbb{M}$ be three rings. Let $f : \mathbb{K} \to \mathbb{L}$ and $g : \mathbb{L} \to \mathbb{M}$ be two ring homomorphisms. Then, the composition $g \circ f : \mathbb{K} \to \mathbb{M}$ is also a ring homomorphism.

Proof of Proposition 5.9.15. This is exercise 4 **(a)** on homework set #6. □

5.10. Ring isomorphisms

Definition 5.10.1. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a map. Then, f is called a *ring isomorphism* if and only if f is invertible (i.e., bijective) and both f and f^{-1} are ring homomorphisms.

Example 5.10.2. Let $\mathbb{K}$ be a ring. The identity map id : $\mathbb{K} \to \mathbb{K}$ is a ring isomorphism.

Example 5.10.3. Let $\mathbb{K}$ be a ring. Let $n \in \mathbb{N}$. Consider the map

$$\begin{aligned} \mathbf{d}_n : \underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ times}} &\to \{\text{diagonal } n \times n\text{-matrices over } \mathbb{K}\}, \\ (d_1, d_2, \ldots, d_n) &\mapsto \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_n \end{pmatrix}. \end{aligned}$$

Note that both $\underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ times}}$ and $\{\text{diagonal } n \times n\text{-matrices over } \mathbb{K}\}$ are rings (the former by Definition 5.7.3; the latter by Proposition 5.8.14 **(c)**).

The map $\mathbf{d}_n$ is invertible. I claim that furthermore, $\mathbf{d}_n$ is a ring isomorphism. This is easiest to check using Proposition 5.10.5 further below. Note that this claim is a rigorous version of our earlier informal statement that the ring formed by the diagonal $n \times n$-matrices is just $\underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ times}}$ in disguise. The isomorphism $\mathbf{d}_n$ is responsible for the disguise!

Example 5.10.4. The map from $\mathbb{K}^{2\leq 2}$ to $\mathbb{K}^{2\geq 2}$ introduced in Example 5.9.13 **(b)** is a ring isomorphism. Its inverse is the map

$$\begin{aligned} \mathbb{K}^{2\geq 2} &\to \mathbb{K}^{2\leq 2}, \\ \begin{pmatrix} c & 0 \\ b & a \end{pmatrix} &\mapsto \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}. \end{aligned}$$

Proposition 5.10.5. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be an invertible ring homomorphism. Then, f is a ring isomorphism.

Proof of Proposition 5.10.5. We just need to show that f^{-1} is a ring homomorphism.

Let us verify axiom **(c)** for f^{-1}. This means that we must prove that

$$f^{-1}(ab) = f^{-1}(a) f^{-1}(b) \qquad \text{for all } a, b \in \mathbb{L}.$$

So let $a, b \in \mathbb{L}$. We know that f is a ring homomorphism; thus it satisfies axiom **(c)**. Applying this axiom to $f^{-1}(a)$ and $f^{-1}(b)$ instead of a and b, we find

$$f\left(f^{-1}(a) f^{-1}(b)\right) = \underbrace{f\left(f^{-1}(a)\right)}_{=a} \cdot \underbrace{f\left(f^{-1}(b)\right)}_{=b} = ab = f\left(f^{-1}(ab)\right).$$

Since f is injective (because f is invertible), we thus conclude

$$f^{-1}(a) f^{-1}(b) = f^{-1}(ab),$$

which is precisely what we wanted to prove.

So axiom **(c)** for f^{-1} is verified. Axiom **(a)** follows by the same argument with $+$ instead of $\cdot$.

Since f satisfies axiom **(d)** (being a ring homomorphism), we have $f(1) = 1$. But this yields $f^{-1}(1) = 1$; thus, f^{-1} satisfies axiom **(d)**. Similarly, f^{-1} satisfies axiom **(b)**.

Thus, the map $f^{-1} : \mathbb{L} \to \mathbb{K}$ satisfies all four axioms for a ring homomorphism. Hence, f^{-1} is a ring homomorphism. Thus, f is a ring isomorphism (by the definition of a ring isomorphism). This proves Proposition 5.10.5. □

Example 5.10.6. Recall the ring $\mathbb{Z}'$ introduced in Section 5.2. It is the **set** $\mathbb{Z}$, endowed with the usual addition $+$ and the unusual multiplication $\widetilde{\times}$ and the elements $0_{\mathbb{Z}'} = 0$ and $1_{\mathbb{Z}'} = -1$.

As we have suggested back in that section, this ring $\mathbb{Z}'$ is simply a relabelled version of $\mathbb{Z}$. We now have the proper language for this: The map

$$\varphi : \mathbb{Z} \to \mathbb{Z}', \qquad a \mapsto -a$$

is a ring isomorphism. This can easily be checked using Proposition 5.10.5, since this map φ is invertible (actually, $\varphi \circ \varphi = \mathrm{id}$), and since φ is a ring homomorphism (because of (162), (163), (164) and (165)).

Example 5.10.7. Let m and n be two coprime positive integers. Then, $(\mathbb{Z}/m) \times (\mathbb{Z}/n)$ is a ring (according to Definition 5.7.3). Theorem 3.6.2 says that the map

$$S_{m,n} : \mathbb{Z}/(mn) \to (\mathbb{Z}/m) \times (\mathbb{Z}/n),$$
$$\alpha \mapsto (\pi_{mn,m}(\alpha), \pi_{mn,n}(\alpha))$$

is well-defined and is a bijection. This map $S_{m,n}$ is furthermore a ring isomorphism.

Proof of Example 5.10.7. The map $S_{m,n}$ is a bijection, thus invertible.

Let us next prove that the map $S_{m,n}$ is a ring homomorphism.

For each $s \in \mathbb{Z}$, we have

$$S_{m,n}\left([s]_{mn}\right) = \left(\underbrace{\pi_{mn,m}\left([s]_{mn}\right)}_{=[s]_m}, \underbrace{\pi_{mn,n}\left([s]_{mn}\right)}_{=[s]_n}\right) = \left([s]_m, [s]_n\right). \tag{189}$$

Let us check axiom **(c)** from Definition 5.9.1 for $f = S_{m,n}$. Let $\alpha, \beta \in \mathbb{Z}/(mn)$. We must prove that $S_{m,n}(\alpha\beta) = S_{m,n}(\alpha) \cdot S_{m,n}(\beta)$.

Write α and β in the form $\alpha = [a]_{mn}$ and $\beta = [b]_{mn}$ for some $a, b \in \mathbb{Z}$. Then, $\alpha\beta = [a]_{mn}[b]_{mn} = [ab]_{mn}$, so

$$S_{m,n}(\alpha\beta) = S_{m,n}\left([ab]_{mn}\right) = \left([ab]_m, [ab]_n\right) \qquad \text{(by (189))}.$$

Comparing this with

$$\begin{aligned}
& S_{m,n}\left(\underbrace{\alpha}_{=[a]_{mn}}\right) \cdot S_{m,n}\left(\underbrace{\beta}_{=[b]_{mn}}\right) \\
&= \underbrace{S_{m,n}\left([a]_{mn}\right)}_{\substack{=([a]_m,[a]_n) \\ \text{(by (189))}}} \cdot \underbrace{S_{m,n}\left([b]_{mn}\right)}_{\substack{=([b]_m,[b]_n) \\ \text{(by (189))}}} \\
&= \left([a]_m, [a]_n\right) \cdot \left([b]_m, [b]_n\right) = \left(\underbrace{[a]_m [b]_m}_{=[ab]_m}, \underbrace{[a]_n [b]_n}_{=[ab]_n}\right) \\
&\qquad \left(\begin{array}{c}\text{since the multiplication } \cdot \text{ on the Cartesian product } (\mathbb{Z}/m) \times (\mathbb{Z}/n) \\ \text{is defined entrywise}\end{array}\right) \\
&= \left([ab]_m, [ab]_n\right),
\end{aligned}$$

we obtain $S_{m,n}(\alpha\beta) = S_{m,n}(\alpha) \cdot S_{m,n}(\beta)$. This proves axiom **(c)** for our map $S_{m,n}$. Similarly, the other axioms can be shown. Thus, $S_{m,n}$ is a ring homomorphism. Therefore, Proposition 5.10.5 shows that $S_{m,n}$ is a ring isomorphism (since $S_{m,n}$ is invertible). □

Note one more simple general fact:

Proposition 5.10.8. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring isomorphism. Then, $f^{-1} : \mathbb{L} \to \mathbb{K}$ is also a ring isomorphism.

Proof of Proposition 5.10.8. Clearly, f^{-1} is a ring homomorphism (since f is a ring isomorphism). Furthermore, f^{-1} is invertible (with inverse $\left(f^{-1}\right)^{-1} = f$) and its inverse $\left(f^{-1}\right)^{-1} = f$ is a ring homomorphism as well. Thus, f^{-1} is a ring isomorphism. This proves Proposition 5.10.8. □

Let me attempt to discuss the use of ring isomorphisms; unfortunately, I will have to be vague at this point. Ring homomorphisms allow us to transfer some things from one ring into another. For example, if $f : \mathbb{K} \to \mathbb{L}$ is a ring homomorphism from a ring $\mathbb{K}$ to a ring $\mathbb{L}$, then f sends any invertible element of $\mathbb{K}$ to an invertible element of $\mathbb{L}$ (by Proposition 5.9.14 **(b)**). However, they are generally only "one-way roads". For instance, if $f : \mathbb{K} \to \mathbb{L}$ is a ring homomorphism from a ring $\mathbb{K}$ to a ring $\mathbb{L}$, and if $a \in \mathbb{K}$ is such that $f(a) \in \mathbb{L}$ is invertible, then a may and may not be invertible. A ring homomorphism from a ring $\mathbb{K}$ to a ring $\mathbb{L}$ does not determine either ring in terms of the other. You can have homomorphisms between completely different rings, such as from $\mathbb{Z}$ to the zero ring, or from $\mathbb{Z}$ to $\mathbb{C}$.

On the other hand, ring isomorphisms let us go "back and forth" between the rings they connect; if we have a ring isomorphism $f : \mathbb{K} \to \mathbb{L}$, we can regard $\mathbb{L}$ as being "the same ring as $\mathbb{K}$, with its elements renamed". (The isomorphism f does the renaming: you should think of each $a \in \mathbb{K}$ being renamed as $f(a)$.)

Thus, when you have a ring isomorphism $f : \mathbb{K} \to \mathbb{L}$, you can take any "intrinsic" property[169] of $\mathbb{K}$ and obtain the corresponding property of $\mathbb{L}$, and vice versa. Here is an example:

Proposition 5.10.9. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring isomorphism.

(a) If $\mathbb{K}$ is commutative, then $\mathbb{L}$ is commutative.

(b) If $0 \neq 1$ in $\mathbb{K}$, then $0 \neq 1$ in $\mathbb{L}$.

(c) If $\mathbb{K}$ is a skew field, then $\mathbb{L}$ is a skew field.

(d) If $\mathbb{K}$ is a field, then $\mathbb{L}$ is a field.

Proof of Proposition 5.10.9. The proofs given below are exemplary; you should be able to similarly transfer any other property of $\mathbb{K}$ to $\mathbb{L}$ and vice versa.

Recall that f is a ring isomorphism. Thus, the map f is invertible, and both f and f^{-1} are ring homomorphisms (by the definition of a ring isomorphism).

(a) Assume that $\mathbb{K}$ is commutative. We must prove that $\mathbb{L}$ is commutative. In other words, we must prove that $ab = ba$ for any $a, b \in \mathbb{L}$.

Fix $a, b \in \mathbb{L}$. We know that f is invertible. Hence, $f^{-1}(a), f^{-1}(b) \in \mathbb{K}$ are well-defined. Since $\mathbb{K}$ is commutative, these satisfy

$$f^{-1}(a) f^{-1}(b) = f^{-1}(b) f^{-1}(a).$$

Applying f to this equality, we get

$$f\left(f^{-1}(a) f^{-1}(b)\right) = f\left(f^{-1}(b) f^{-1}(a)\right). \tag{190}$$

[169] What do we mean by "intrinsic"? Roughly speaking, an *intrinsic* property of a ring is a property that can be stated entirely in terms of its structure (i.e., its ground set and its operations $+$ and $\cdot$ and its elements 0 and 1), without referring to outside objects. For instance, "every element a of the ring satisfies $a^3 = a^2$" is an intrinsic property (since $a^3 = aaa$ and $a^2 = aa$ are defined purely in terms of the operation $\cdot$), and "the ring has two nonzero elements a and b such that $ab = 0$" is an intrinsic property as well (provided that "nonzero" and "0" refer to the zero of the ring, rather than the number 0), but "the ring contains the number $\sqrt[3]{2}$" is not an intrinsic property (since it refers to an outside object – namely, the number $\sqrt[3]{2}$).

But since f is a ring homomorphism, we can apply axiom **(c)** of Definition 5.9.1 to $f^{-1}(a)$ and $f^{-1}(b)$ instead of a and b. We thus obtain

$$f\left(f^{-1}(a)\,f^{-1}(b)\right) = \underbrace{f\left(f^{-1}(a)\right)}_{=a}\underbrace{f\left(f^{-1}(b)\right)}_{=b} = ab$$

and similarly $f\left(f^{-1}(b)\,f^{-1}(a)\right) = ba$; thus, the equality (190) becomes $ab = ba$. This shows that $\mathbb{L}$ is commutative. This proves Proposition 5.10.9 **(a)**.

Before I move on to the next part of Proposition 5.10.9, let me explain how the above proof could be found straightforwardly, without any creative input. The point of this is to show how to prove not just Proposition 5.10.9 **(a)**, but any similar claim as well.

The (only) idea involved in the above proof was the following: The two mutually inverse bijections $f : \mathbb{K} \to \mathbb{L}$ and $f^{-1} : \mathbb{L} \to \mathbb{K}$ provide a "railway system" that can be used to transport anything (elements, equalities, subsets, etc.) between $\mathbb{K}$ and $\mathbb{L}$. Since these bijections are ring homomorphisms, the structure of the objects that we are transporting does not get "damaged in transit": Products remain products (i.e., if we have three elements a, b and c of $\mathbb{K}$ satisfying $ab = c$, and if we transport these three elements to $\mathbb{L}$ via f, then the resulting three elements of $\mathbb{L}$ will still satisfy $f(a)\,f(b) = f(c)$), sums remain sums, etc.. Thus, we can move back and forth between $\mathbb{K}$ and $\mathbb{L}$ without keeping track of where precisely we take our sums and products.

With this in mind, our above proof of Proposition 5.10.9 **(a)** can be discovered as follows:

Assume that $\mathbb{K}$ is commutative. We must prove that $\mathbb{L}$ is commutative. In other words, we must prove that $ab = ba$ for any $a, b \in \mathbb{L}$. So let us fix $a, b \in \mathbb{L}$. We want to prove $ab = ba$, but all we have is an analogous identity for elements of $\mathbb{K}$ (since we know that $\mathbb{K}$ is commutative). In other words, we have

$$a'b' = b'a' \qquad \text{for all } a', b' \in \mathbb{K}. \tag{191}$$

So we transport our two elements a, b of $\mathbb{L}$ to $\mathbb{K}$ (by our "railway system" – specifically, using the map f^{-1}), in order to be able to apply (191) to them. The result are the two elements $f^{-1}(a), f^{-1}(b)$ of $\mathbb{K}$. Applying the identity (191) to $a' = f^{-1}(a)$ and $b' = f^{-1}(b)$, we obtain $f^{-1}(a)\,f^{-1}(b) = f^{-1}(b)\,f^{-1}(a)$. This is an equality inside $\mathbb{K}$, whereas our goal is to prove an equality inside $\mathbb{L}$ (namely, the equality $ab = ba$). So we transport this equality back into $\mathbb{L}$ by applying f to its two sides. We thus obtain

$$f\left(f^{-1}(a)\,f^{-1}(b)\right) = f\left(f^{-1}(b)\,f^{-1}(a)\right). \tag{192}$$

But recalling that f is a ring homomorphism and thus no structure gets "damaged in transit", we see that

$$f\left(f^{-1}(a)\,f^{-1}(b)\right) = \underbrace{f\left(f^{-1}(a)\right)}_{=a}\underbrace{f\left(f^{-1}(b)\right)}_{=b} = ab$$

and similarly $f\left(f^{-1}(b)\,f^{-1}(a)\right) = ba$. Hence, the equality (192) that we have just proven rewrites as $ab = ba$, which is precisely what we wanted to prove. Thus, we have proven Proposition 5.10.9 **(a)** by merely going back and forth between $\mathbb{K}$ and $\mathbb{L}$.

Let us now prove the rest of Proposition 5.10.9:

(b) Assume $0 \neq 1$ in $\mathbb{K}$. We must prove $0 \neq 1$ in $\mathbb{L}$.

The map f is an isomorphism, thus invertible, thus bijective, thus injective. Hence, from $0 \neq 1$ in $\mathbb{K}$, we conclude $f(0) \neq f(1)$ in $\mathbb{L}$. But since f is a ring homomorphism, we have $f(0) = 0$ and $f(1) = 1$; so this rewrites as $0 \neq 1$ in $\mathbb{L}$. This proves Proposition 5.10.9 **(b)**.

(c) Assume that $\mathbb{K}$ is a skew field. We must prove that $\mathbb{L}$ is a skew field.

Since $\mathbb{K}$ is a skew field, we have $0 \neq 1$ in $\mathbb{K}$, thus $0 \neq 1$ in $\mathbb{L}$ (by Proposition 5.10.9 **(b)**). Hence, it remains to prove that every nonzero element $a \in \mathbb{L}$ has a multiplicative inverse.

Let $a \in \mathbb{L}$ be nonzero. Then, $f^{-1}(a) \in \mathbb{K}$ is nonzero (because if it was zero, then we would have $f^{-1}(a) = 0$ and thus $f\left(f^{-1}(a)\right) = f(0) = 0$ (since f is a ring homomorphism); but this would contradict the fact that $f\left(f^{-1}(a)\right) = a$ is nonzero). Hence, $f^{-1}(a) \in \mathbb{K}$ has a multiplicative inverse b (since $\mathbb{K}$ is a skew field). Consider this b. Thus, $f^{-1}(a)\,b = bf^{-1}(a) = 1$ (since b is a multiplicative inverse of $f^{-1}(a)$). Applying f to this chain of equalities, we obtain

$$f\left(f^{-1}(a)\,b\right) = f\left(bf^{-1}(a)\right) = f(1).$$

This quickly rewrites as

$$af(b) = f(b)\,a = 1$$

(since f is a ring homomorphism). Thus, $f(b)$ is a multiplicative inverse of a. Hence, a has a multiplicative inverse. Thus, we have shown that every nonzero element $a \in \mathbb{L}$ has a multiplicative inverse. Since $0 \neq 1$ in $\mathbb{L}$, this shows that $\mathbb{L}$ is a skew field. This proves Proposition 5.10.9 **(c)**.

(d) Assume that $\mathbb{K}$ is a field. We must prove that $\mathbb{L}$ is a field.

Since $\mathbb{K}$ is a field, $\mathbb{K}$ is commutative, and thus $\mathbb{L}$ is commutative (by Proposition 5.10.9 **(a)**).

But $\mathbb{K}$ is a field, and thus a skew field. Hence, Proposition 5.10.9 **(c)** shows that $\mathbb{L}$ is a skew field. Since $\mathbb{L}$ is commutative, this yields that $\mathbb{L}$ is a field. This proves Proposition 5.10.9 **(d)**. □

The idea of the above proof (and of many similar proofs, which we will omit) is that if you have a ring isomorphism $f : \mathbb{K} \to \mathbb{L}$, you can transport any equality or element from $\mathbb{K}$ to $\mathbb{L}$ (via f) or vice versa (via f^{-1}); and each time, the ring operations ($+$, $-$, $\cdot$, $\sum$, 0, 1) do not get damaged on the way (since f and f^{-1} are ring homomorphisms).

Here is another example of this sort of reasoning:

Proposition 5.10.10. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring isomorphism. Then:

(a) We have

$$\left|\left\{\text{invertible elements of } \mathbb{K}\right\}\right| = \left|\left\{\text{invertible elements of } \mathbb{L}\right\}\right|.$$

(b) We have

$$\left|\left\{\text{idempotent elements of } \mathbb{K}\right\}\right| = \left|\left\{\text{idempotent elements of } \mathbb{L}\right\}\right|.$$

Here, an element a of a ring $\mathbb{K}$ is said to be *idempotent* if $a^2 = a$.

Proof of Proposition 5.10.10. Proposition 5.10.10 is another instance of the "anything can be transported along a ring isomorphism" principle (which we have used in Proposition 5.10.9). Here is a proof in more detail:

(a) If a is an invertible element of $\mathbb{K}$, then $f(a)$ is an invertible element of $\mathbb{L}$ (since we can pick a multiplicative inverse b of a in $\mathbb{K}$, and then $f(b)$ will be a multiplicative inverse of $f(a)$ in $\mathbb{L}$). Hence, the map

$$\left\{\text{invertible elements of } \mathbb{K}\right\} \to \left\{\text{invertible elements of } \mathbb{L}\right\},$$
$$a \mapsto f(a)$$

is well-defined. Similarly, the map

$$\left\{\text{invertible elements of } \mathbb{L}\right\} \to \left\{\text{invertible elements of } \mathbb{K}\right\},$$
$$a \mapsto f^{-1}(a)$$

is also well-defined (since Proposition 5.10.8 shows that the map $f^{-1} : \mathbb{L} \to \mathbb{K}$ is also a ring isomorphism). These two maps are clearly mutually inverse, and therefore are bijections. Hence, we have found a bijection from $\{\text{invertible elements of } \mathbb{K}\}$ to $\{\text{invertible elements of } \mathbb{L}\}$. Thus,

$$\left|\left\{\text{invertible elements of } \mathbb{K}\right\}\right| = \left|\left\{\text{invertible elements of } \mathbb{L}\right\}\right|.$$

This proves Proposition 5.10.10 **(a)**.

(b) If a is an idempotent element of $\mathbb{K}$, then $f(a)$ is an idempotent element of $\mathbb{L}$ (since f is a ring homomorphism and thus $(f(a))^2 = f\left(\underbrace{a^2}_{=a}\right) = f(a)$). Hence, the map

$$\left\{\text{idempotent elements of } \mathbb{K}\right\} \to \left\{\text{idempotent elements of } \mathbb{L}\right\},$$
$$a \mapsto f(a)$$

is well-defined. Similarly, the map

$$\left\{\text{idempotent elements of } \mathbb{L}\right\} \to \left\{\text{idempotent elements of } \mathbb{K}\right\},$$
$$a \mapsto f^{-1}(a)$$

is also well-defined (since Proposition 5.10.8 shows that the map $f^{-1} : \mathbb{L} \to \mathbb{K}$ is also a ring isomorphism). These two maps are clearly mutually inverse, and therefore are bijections. Hence, we have found a bijection from $\{\text{idempotent elements of } \mathbb{K}\}$ to $\{\text{idempotent elements of } \mathbb{L}\}$. Thus,

$$\left|\{\text{idempotent elements of } \mathbb{K}\}\right| = \left|\{\text{idempotent elements of } \mathbb{L}\}\right|.$$

This proves Proposition 5.10.10 **(b)**. □

Now let us see some applications of ring isomorphisms.

Recall that we proved Theorem 2.14.4 using the Chinese Remainder Theorem in Section 3.6. Let us redo this proof in a shorter way:

New version of our Second proof of Theorem 2.14.4. Example 5.10.7 says that the map

$$\begin{aligned} S_{m,n} : \mathbb{Z}/\left(mn\right) &\to \left(\mathbb{Z}/m\right) \times \left(\mathbb{Z}/n\right), \\ \alpha &\mapsto \left(\pi_{mn,m}\left(\alpha\right), \pi_{mn,n}\left(\alpha\right)\right) \end{aligned}$$

is a ring isomorphism. Thus,

$$\begin{aligned} &\left|\{\text{invertible elements of } \mathbb{Z}/\left(mn\right)\}\right| \\ &= \left|\{\text{invertible elements of } \left(\mathbb{Z}/m\right) \times \left(\mathbb{Z}/n\right)\}\right| \end{aligned} \tag{193}$$

(by Proposition 5.10.10 **(a)**).

But if $\mathbb{K}$ and $\mathbb{L}$ are any two rings, then

$$\begin{aligned} &\{\text{invertible elements of } \mathbb{K} \times \mathbb{L}\} \\ &= \{\text{invertible elements of } \mathbb{K}\} \times \{\text{invertible elements of } \mathbb{L}\} \end{aligned}$$

(since multiplication on $\mathbb{K} \times \mathbb{L}$ is defined entrywise, so an element $(a, b) \in \mathbb{K} \times \mathbb{L}$ is invertible if and only if both $a \in \mathbb{K}$ and $b \in \mathbb{L}$ are invertible). Hence,

$$\begin{aligned} &\{\text{invertible elements of } \left(\mathbb{Z}/m\right) \times \left(\mathbb{Z}/n\right)\} \\ &= \{\text{invertible elements of } \mathbb{Z}/m\} \times \{\text{invertible elements of } \mathbb{Z}/n\}, \end{aligned}$$

so that

$$\begin{aligned} &\left|\{\text{invertible elements of } \left(\mathbb{Z}/m\right) \times \left(\mathbb{Z}/n\right)\}\right| \\ &= \left|\{\text{invertible elements of } \mathbb{Z}/m\} \times \{\text{invertible elements of } \mathbb{Z}/n\}\right| \\ &= \left|\{\text{invertible elements of } \mathbb{Z}/m\}\right| \cdot \left|\{\text{invertible elements of } \mathbb{Z}/n\}\right|. \end{aligned}$$

Hence, (193) becomes

$$\begin{aligned} &\left|\{\text{invertible elements of } \mathbb{Z}/\left(mn\right)\}\right| \\ &= \left|\{\text{invertible elements of } \left(\mathbb{Z}/m\right) \times \left(\mathbb{Z}/n\right)\}\right| \\ &= \left|\{\text{invertible elements of } \mathbb{Z}/m\}\right| \cdot \left|\{\text{invertible elements of } \mathbb{Z}/n\}\right|. \end{aligned} \tag{194}$$

On the other hand, we know that

$$\phi(n) = |\{\text{invertible elements of } \mathbb{Z}/n\}|$$

(in fact, this is Corollary 3.5.5 **(b)**, since what we called U_n in this corollary is exactly $\{\text{invertible elements of } \mathbb{Z}/n\}$). Similarly,

$$\phi(m) = |\{\text{invertible elements of } \mathbb{Z}/m\}| \qquad \text{and}$$
$$\phi(mn) = |\{\text{invertible elements of } \mathbb{Z}/(mn)\}|.$$

So the equality (194) rewrites as $\phi(mn) = \phi(m) \cdot \phi(n)$. So Theorem 2.14.4 is proven again. □

The next exercise offers another example of the same strategy:

Exercise 5.10.1. Let p and q be two distinct primes. How many idempotent elements does the ring $\mathbb{Z}/(pq)$ have?

Solution to Exercise 5.10.1 (sketched). The primes p and q are distinct, so they are coprime. Hence, Example 5.10.7 (applied to $m = p$ and $n = q$) says that the map

$$S_{p,q} : \mathbb{Z}/(pq) \to (\mathbb{Z}/p) \times (\mathbb{Z}/q),$$
$$\alpha \mapsto (\pi_{pq,p}(\alpha), \pi_{pq,q}(\alpha))$$

is a ring isomorphism. Hence, Proposition 5.10.10 **(b)** yields

$$\begin{aligned} &|\{\text{idempotent elements of } \mathbb{Z}/(pq)\}| \\ &= |\{\text{idempotent elements of } (\mathbb{Z}/p) \times (\mathbb{Z}/q)\}| \\ &= |\{\text{idempotent elements of } \mathbb{Z}/p\} \times \{\text{idempotent elements of } \mathbb{Z}/q\}| \end{aligned}$$

(since for any two rings $\mathbb{K}$ and $\mathbb{L}$, we have

$$\begin{aligned} &\{\text{idempotent elements of } \mathbb{K} \times \mathbb{L}\} \\ &= \{\text{idempotent elements of } \mathbb{K}\} \times \{\text{idempotent elements of } \mathbb{L}\}, \end{aligned}$$

because of the entrywise multiplication on $\mathbb{K} \times \mathbb{L}$). Thus, it remains to find the number of idempotent elements of $\mathbb{Z}/p$ and the number of idempotent elements of $\mathbb{Z}/q$.

How many idempotent elements does $\mathbb{Z}/p$ have? For any $a \in \mathbb{Z}$, we have the following chain of equivalences:

$$\begin{aligned}
&\left([a]_p \text{ is idempotent}\right) \\
\Longleftrightarrow\ &\left(\left([a]_p\right)^2 = [a]_p\right) \qquad \text{(by the definition of "idempotent")} \\
\Longleftrightarrow\ &\left(\left[a^2\right]_p = [a]_p\right) \qquad \left(\text{since } \left([a]_p\right)^2 = \left[a^2\right]_p\right) \\
\Longleftrightarrow\ &\left(a^2 \equiv a \bmod p\right) \\
\Longleftrightarrow\ &\left(p \mid \underbrace{a^2 - a}_{=a(a-1)}\right) \Longleftrightarrow (p \mid a(a-1)) \\
\Longleftrightarrow\ &(p \mid a \text{ or } p \mid a-1) \qquad \text{(since } p \text{ is prime)} \\
\Longleftrightarrow\ &(a \equiv 0 \bmod p \text{ or } a \equiv 1 \bmod p) \\
\Longleftrightarrow\ &\left([a]_p = [0]_p \text{ or } [a]_p = [1]_p\right).
\end{aligned}$$

In other words, for a given $a \in \mathbb{Z}$, the residue class $[a]_p$ is idempotent if and only if $[a]_p$ equals $[0]_p$ or $[1]_p$. Since every residue class $\alpha \in \mathbb{Z}/p$ has the form $[a]_p$ for some $a \in \mathbb{Z}$, we can restate this as follows: A residue class $\alpha \in \mathbb{Z}/p$ is idempotent if and only if it equals $[0]_p$ or $[1]_p$. Thus, the ring $\mathbb{Z}/p$ has exactly two idempotent elements (namely, $[0]_p$ and $[1]_p$). In other words,

$$|\{\text{idempotent elements of } \mathbb{Z}/p\}| = 2.$$

Similarly,

$$|\{\text{idempotent elements of } \mathbb{Z}/q\}| = 2.$$

Now, the above computation becomes

$$\begin{aligned}
&|\{\text{idempotent elements of } \mathbb{Z}/(pq)\}| \\
&= |\{\text{idempotent elements of } \mathbb{Z}/p\} \times \{\text{idempotent elements of } \mathbb{Z}/q\}| \\
&= \underbrace{|\{\text{idempotent elements of } \mathbb{Z}/p\}|}_{=2} \cdot \underbrace{|\{\text{idempotent elements of } \mathbb{Z}/q\}|}_{=2} \\
&= 2 \cdot 2 = 4.
\end{aligned}$$

In other words, the ring $\mathbb{Z}/(pq)$ has 4 idempotent elements.

Side-note: What are these 4 idempotent elements?

Two of them are easy to find: $[0]_{pq}$ and $[1]_{pq}$ (in fact, 0 and 1 are idempotent elements in any ring). But how to get the other two?

Here is a systematic approach: Recall that $S_{p,q} : \mathbb{Z}/(pq) \to (\mathbb{Z}/p) \times (\mathbb{Z}/q)$ is a ring isomorphism. Thus, looking back at the proof of Proposition 5.10.10 **(b)**, we see that the idempotent elements of $\mathbb{Z}/(pq)$ are the preimages of the idempotent elements of $(\mathbb{Z}/p) \times (\mathbb{Z}/q)$ under this isomorphism $S_{p,q}$.

The 4 idempotent elements of $(\mathbb{Z}/p) \times (\mathbb{Z}/q)$ are

$$\left([0]_p, [0]_q\right), \qquad \left([1]_p, [1]_q\right), \qquad \left([0]_p, [1]_q\right), \qquad \left([1]_p, [0]_q\right).$$

To find the 4 idempotent elements in $\mathbb{Z}/(pq)$, we thus have to apply the inverse $(S_{p,q})^{-1}$ of the isomorphism $S_{p,q}$ to them.

- The first gets sent to $[0]_{pq}$.
- The second gets sent to $[1]_{pq}$.
- The last two get sent to $[xp]_{pq}$ and $[yq]_{pq}$, where x is a modular inverse of p modulo q, and where y is a modular inverse of q modulo p. (It does not matter which inverses we choose; we get the same elements.)

  Here is a slightly different way to get the last two idempotent elements: Bezout's theorem yields that there exist integers x and y such that $xp + yq = 1$. Then, $[xp]_{pq}$ and $[yq]_{pq}$ are the two missing idempotents. (In truth, this is not different from the previous answer; in fact, if x and y are integers such that $xp + yq = 1$, then x is a modular inverse of p modulo q, and y is a modular inverse of q modulo p.)

□

Example 5.10.11. Let A be the 2×2-matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{Z}^{2\times 2}$.

On midterm #2 exercise 5, you have encountered the ring

$$\mathcal{F} = \{aA + bI_2 \mid a, b \in \mathbb{Z}\} = \left\{ \begin{pmatrix} b & a \\ a & a+b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}.$$

This is a subring of the matrix ring $\mathbb{Z}^{2\times 2}$.

On homework set #5 exercise 5, you have encountered the ring

$$\mathbb{Z}[\phi] = \{a + b\phi \mid a, b \in \mathbb{Z}\},$$

where $\phi = \dfrac{1+\sqrt{5}}{2} = 1.618\ldots$ is the golden ratio. This is a subring of $\mathbb{R}$.

I claim that there is an isomorphism from $\mathbb{Z}[\phi]$ to $\mathcal{F}$. Namely, the map

$$f : \mathbb{Z}[\phi] \to \mathcal{F},$$
$$a + b\phi \mapsto bA + aI_2 = \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}$$

is a ring isomorphism (but not the only one!).

(Check this by hand.)

Definition 5.10.12. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. We say that the rings $\mathbb{K}$ and $\mathbb{L}$ are *isomorphic* if there exists a ring isomorphism $f : \mathbb{K} \to \mathbb{L}$.

We write "$\mathbb{K} \cong \mathbb{L}$ (as rings)" to say that the rings $\mathbb{K}$ and $\mathbb{L}$ are isomorphic.

Example 5.10.13. Let $\mathbb{K}$ be any ring, and let $\mathbb{M}$ be the zero ring $\{0\}$. In Example 5.9.6, we saw that the map

$$\mathbb{K} \to \mathbb{M}, \qquad a \mapsto 0$$

is a ring homomorphism. This homomorphism is a ring isomorphism if and only if the ring $\mathbb{K}$ is trivial (i.e., has only one element). Thus, each trivial ring is isomorphic to the zero ring.

5.11. Freshman's Dream

Let us now prove a property of p-th powers in rings. At this point, this property appears to be a mere curiosity, but it will come useful later (in proving Theorem 2.17.20).

Theorem 5.11.1. Let p be a prime. Let $\mathbb{K}$ be a ring such that $p \cdot 1_{\mathbb{K}} = 0$. Let $a, b \in \mathbb{K}$ be such that $ab = ba$. Then,

$$(a+b)^p = a^p + b^p.$$

Theorem 5.11.1 is often called "Freshman's Dream" (in writing) or "Idiot's Binomial Formula" (colloquially).

Example 5.11.2. Let p be a prime.

(a) The simplest example of a ring $\mathbb{K}$ in which $p \cdot 1_{\mathbb{K}} = 0$ (apart from the zero ring) is the ring $\mathbb{Z}/p$. Unfortunately, this is too simple to make a good example for Theorem 5.11.1. Indeed, if $\mathbb{K} = \mathbb{Z}/p$, then any $\alpha \in \mathbb{K}$ satisfies $\alpha^p = \alpha$ (because we can write α as $[a]_p$ for some $a \in \mathbb{Z}$, and then apply Theorem 2.15.1 **(b)** to this a). Thus, as long as we are staying in $\mathbb{K} = \mathbb{Z}/p$, the equality $(a+b)^p = a^p + b^p$ claimed by Theorem 5.11.1 boils down to $a + b = a + b$ (since $(a+b)^p = a + b$ and $a^p = a$ and $b^p = b$).

(b) In Section 5.6, we have taken a prime $p > 2$, and constructed a finite field $\mathbb{K}'_\eta$ of size p^2 (by picking a non-square $\eta \in \mathbb{Z}/p$ and performing the construction in Definition 5.6.11). This field satisfies $p \cdot 1_{\mathbb{K}'_\eta} = 0$, so we can apply Theorem 5.11.1 to it as well. This time, $\alpha^p = \alpha$ will no longer hold for all α in the field, so the result we get will not be obvious.

(c) Here is another example. Let $n \in \mathbb{N}$, and let $\mathbb{K}$ be the matrix ring $(\mathbb{Z}/p)^{n \times n}$. This matrix ring $\mathbb{K}$ satisfies $p \cdot 1_{\mathbb{K}} = 0$ (since scaling is defined entrywise on matrices). Thus, Theorem 5.11.1 yields that any $a, b \in \mathbb{K}$ satisfying $ab = ba$ must satisfy $(a+b)^p = a^p + b^p$. Of course, not every two matrices $a, b \in \mathbb{K}$ satisfy $ab = ba$, but there are many matrices that do.

A particularly striking situation is the following: Assume that $n \leq p$, and let $N \in \mathbb{K}$ be a strictly lower-triangular $n \times n$-matrix. For example, if $n = 3$, then N has the form $\begin{pmatrix} 0 & 0 & 0 \\ u & 0 & 0 \\ v & w & 0 \end{pmatrix}$. Then, I claim that

$$(I_n + N)^p = I_n. \tag{195}$$

To prove this, we observe that $I_n \cdot N = N = N \cdot I_n$. Hence, Theorem 5.11.1 can be applied to $a = I_n$ and $b = N$. As a result, we obtain $(I_n + N)^p = I_n^p + N^p$. But N is a strictly lower-triangular $n \times n$-matrix, and therefore satisfies $N^n = 0_{n \times n}$ (by [Grinbe18, Corollary 3.78]), and therefore

$$\begin{aligned} N^p &= \underbrace{N^n}_{=0_{n\times n}} N^{p-n} \qquad \text{(since } n \leq p\text{)} \\ &= 0_{n\times n} N^{p-n} = 0_{n\times n}. \end{aligned}$$

Furthermore, $I_n^p = I_n$ (since I_n is the unity of the ring $\mathbb{K}$). Hence, $(I_n + N)^p = \underbrace{I_n^p}_{=I_n} + \underbrace{N^p}_{=0_{n\times n}} = I_n + 0_{n\times n} = I_n$. This proves (195).

Proof of Theorem 5.11.1. For each $k \in \{1, 2, \ldots, p-1\}$, we have $p \mid \binom{p}{k}$ (by Theorem 2.17.19) and thus

$$\binom{p}{k} 1_{\mathbb{K}} = 0 \tag{196}$$

(since $p \cdot 1_{\mathbb{K}} = 0$) [170].

But $ab = ba$. Hence, the binomial formula (more precisely, the identity (183),

[170] Here is this argument in more detail:

Let $k \in \{1, 2, \ldots, p-1\}$. Then, $p \mid \binom{p}{k}$ (by Theorem 2.17.19). Hence, there exists an integer c such that $\binom{p}{k} = pc$. Consider this c. Then,

$$\underbrace{\binom{p}{k}}_{=pc=cp} 1_{\mathbb{K}} = c \underbrace{p \cdot 1_{\mathbb{K}}}_{=0} = c \cdot 0 = 0,$$

qed.

applied to $n = p$) yields

$$\begin{aligned}
(a+b)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \\
&= \underbrace{\binom{p}{0}}_{=1} \underbrace{a^0}_{=1} \underbrace{b^{p-0}}_{=b^p} + \sum_{k=1}^{p-1} \binom{p}{k} \underbrace{a^k}_{=1_{\mathbb{K}} \cdot a^k} b^{p-k} + \underbrace{\binom{p}{p}}_{=1} a^p \underbrace{b^{p-p}}_{=b^0=1} \\
&\qquad \left(\begin{array}{c} \text{here, we have split off the addends for } k=0 \text{ and for } k=p \\ \text{from the sum} \end{array} \right) \\
&= b^p + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k} 1_{\mathbb{K}}}_{\substack{=0 \\ \text{(by (196))}}} a^k b^{p-k} + a^p = b^p + \underbrace{\sum_{k=1}^{p-1} 0 a^k b^{p-k}}_{=0} + a^p \\
&= b^p + a^p = a^p + b^p .
\end{aligned}$$

This proves Theorem 5.11.1. □

We note that Theorem 5.11.1 would be false if p wasn't assumed to be prime. For example, it would be false for $p = 4$ (a simple counterexample being $\mathbb{K} = \mathbb{Z}/4$, $a = 1$ and $b = 1$).

As a consequence of Theorem 5.11.1, we obtain some unexpected ring homomorphisms:

> **Corollary 5.11.3.** Let p be a prime. Let $\mathbb{K}$ be a commutative ring such that $p \cdot 1_{\mathbb{K}} = 0$. Let F be the map
>
> $$\mathbb{K} \to \mathbb{K}, \qquad a \mapsto a^p.$$
>
> Then, F is a ring homomorphism.

Proof of Corollary 5.11.3. According to Definition 5.9.1, we must prove that it satisfies the following four axioms:

(a) We have $F(a+b) = F(a) + F(b)$ for all $a, b \in \mathbb{K}$.

(b) We have $F(0) = 0$.

(c) We have $F(ab) = F(a) F(b)$ for all $a, b \in \mathbb{K}$.

(d) We have $F(1) = 1$.

The axiom **(a)** boils down to $(a+b)^p = a^p + b^p$, which follows from Theorem 5.11.1 (since the commutativity of $\mathbb{K}$ entails $ab = ba$).

The axiom **(c)** boils down to $(ab)^p = a^p b^p$, which follows from (182) (again because $ab = ba$).

The axioms **(b)** and **(d)** are obviously satisfied (since $0^p = 0$ and $1^p = 1$). Thus, Corollary 5.11.3 is proven. □

The ring homomorphism F in Corollary 5.11.3 is called the *Frobenius endomorphism*[171] of $\mathbb{K}$.

6. Linear algebra over commutative rings

We shall now continue studying rings, but slowly shift our focus: So far, we have been studying rings themselves, but now we are going to move towards structures "over" rings, such as matrices and $\mathbb{K}$-modules (a generalization of vector spaces). The rings will no longer be the place where everything happens, but rather they will "act" on our structures in the way scalars act on vectors in linear algebra.

6.1. An overview of matrix algebra over fields

Next I shall give a quick review of matrix algebra adapted to the situation in which the entries of the vectors belong to an arbitrary field. This review will be quick and terse, but can be skipped, since the rest of this course will not depend on it. It does, however, provide context and examples for several constructions we will do further on.

I assume you have seen some basic matrix algebra: Gaussian elimination, ranks of matrices, inverses of matrices, determinants, etc. (If not, see [Heffer17].)

Usually, these things are done for matrices over $\mathbb{R}$ or $\mathbb{C}$. But we can try doing the same with matrices over an arbitrary commutative ring $\mathbb{K}$.

6.1.1. Matrices over fields

Let us first study the situation when $\mathbb{K}$ is a field.

Example: Let $\mathbb{K} = \mathbb{Z}/3$, and let $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in \mathbb{K}^{3\times 3}$. (Here, of course, "0" and "1" mean $[0]_3$ and $[1]_3$.) Let $b = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in \mathbb{K}^{3\times 1}$. We want to find a column vector $x \in \mathbb{K}^{3\times 1}$ such that $Ax = b$. This means, explicitly, to find $x_1, x_2, x_3 \in \mathbb{K}$ such that

$$\begin{cases} 0x_1 + 1x_2 + 1x_3 = 1; \\ 1x_1 + 0x_2 + 1x_3 = 1; \\ 1x_1 + 1x_2 + 0x_3 = 1. \end{cases}$$

Can we do this? Well, we can try: Augment the matrix A with the column b,

[171] The word "endomorphism" means "homomorphism of some object (here, a ring) to itself", i.e., "homomorphism whose domain and codomain are the same".

obtaining the augmented matrix

$$(A \mid b) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Now, we shall transform this matrix into reduced row echelon form (see [Strick13, §5] or [Heffer17, Chapter One, §III][172]) by a series of row operations (this is called *Gauss–Jordan reduction* in [Heffer17, Chapter One, §III], and also appears as Method 6.3 in [Strick13]):

$$\begin{aligned}
(A \mid b) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} &\overset{\text{swap row 2 with row 1}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \\
&\overset{\text{subtract row 1 from row 3}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 \end{pmatrix} \qquad (\text{since } -1 = 2 \text{ in } \mathbb{Z}/3) \\
&\overset{\text{subtract row 2 from row 3}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} \\
&(\text{this is a row echelon form, but not a reduced one}) \\
&\overset{\text{subtract row 3 from row 1}}{\mapsto} \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} \\
&\overset{\text{subtract row 3 from row 2}}{\mapsto} \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{pmatrix}.
\end{aligned}$$

[172] The reduced row echelon form is called "reduced echelon form" in [Heffer17].

So for any vector $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{K}^{3\times 1}$, we have the following chain of equivalences:

$$\begin{aligned}
&(Ax = b) \\
\iff\ & (Ax - b = 0_{3\times 1}) \\
\iff\ & \left((A \mid b) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ -1 \end{pmatrix} = 0_{3\times 1} \right) \qquad \left(\text{since } Ax - b = (A \mid b) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ -1 \end{pmatrix} \right) \\
\iff\ & \left(\begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ -1 \end{pmatrix} = 0_{3\times 1} \right) \\
& \qquad \left(\text{since } (A \mid b) \mapsto \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{pmatrix} \text{ by a sequence of row operations} \right) \\
\iff\ & \left(\begin{pmatrix} x_1 - 2 \\ x_2 - 2 \\ x_3 - 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right) \iff \left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix} \right).
\end{aligned}$$

So our linear system has the unique solution

$$x = \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix}.$$

Next, let us try doing the same for $\mathbb{K} = \mathbb{Z}/2$, with the "same" matrix. (It will not be literally the same matrix, of course, since 0 and 1 will now mean $[0]_2$ and $[1]_2$.)

Thus, let $\mathbb{K} = \mathbb{Z}/2$, and let $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in \mathbb{K}^{3\times 3}$. (Here, of course, "0" and "1" mean $[0]_2$ and $[1]_2$.) Let $b = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in \mathbb{K}^{3\times 1}$. We want to find a column vector $x \in \mathbb{K}^{3\times 1}$ such that $Ax = b$. This means, explicitly, to find $x_1, x_2, x_3 \in \mathbb{K}$ such that

$$\begin{cases} 0x_1 + 1x_2 + 1x_3 = 1; \\ 1x_1 + 0x_2 + 1x_3 = 1; \\ 1x_1 + 1x_2 + 0x_3 = 1. \end{cases}$$

Can we do this? We can try as before: Augment the matrix A with the column

b, obtaining

$$(A \mid b) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Now, we shall transform this matrix into reduced row echelon form by a series of row operations:

$$\begin{aligned}
(A \mid b) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} &\overset{\text{swap row 2 with row 1}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \\
&\overset{\text{subtract row 1 from row 3}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad (\text{since } -1 = 1 \text{ in } \mathbb{Z}/2) \\
&\overset{\text{subtract row 2 from row 3}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&\overset{\text{subtract row 3 from row 1}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&\overset{\text{subtract row 3 from row 2}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.
\end{aligned}$$

So for any vector $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{K}^{3\times 1}$, we have the following chain of equivalences:

$$\begin{aligned}
& (Ax = b) \\
\Longleftrightarrow\ & (Ax - b = 0_{3\times 1}) \\
\Longleftrightarrow\ & \left((A \mid b) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ -1 \end{pmatrix} = 0_{3\times 1} \right) \\
\Longleftrightarrow\ & \left(\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ -1 \end{pmatrix} = 0_{3\times 1} \right) \\
\Longleftrightarrow\ & \left(\begin{pmatrix} x_1 + x_3 \\ x_2 + x_3 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right) \Longleftrightarrow (\text{false})
\end{aligned}$$

(since $-1 \neq 0$ in $\mathbb{K}$). So our linear system has no solution.

By the way, you could have easily seen this from the system itself:

$$\begin{cases} 0x_1 + 1x_2 + 1x_3 = 1; \\ 1x_1 + 0x_2 + 1x_3 = 1; \\ 1x_1 + 1x_2 + 0x_3 = 1. \end{cases}$$

Adding together the three equations, we get $0 = 1$ (since $1 + 1 = 0$ and $1 + 1 + 1 = 1$ in $\mathbb{Z}/2$), which is absurd. So the system has no solution.

Upshot: We can do linear algebra over any field more or less in the same as we did over real/complex numbers. But the result may depend on the field.

Let me recall a couple theorems from linear algebra that hold (with the same proofs) over any field:

Theorem 6.1.1. Let $\mathbb{K}$ be a field.

(a) Any matrix over $\mathbb{K}$ has a unique reduced row echelon form (abbreviated RREF).

(b) If $A \in \mathbb{K}^{n\times m}$ is any matrix and R is its RREF, then the row space, kernel (= nullspace) and rank of A are equal to those of R. (Here, the *row space*, *kernel* and *rank* of a matrix are defined in the same way as for real/complex matrices.)

(c) If $A \in \mathbb{K}^{n\times m}$ is any matrix, and if $b \in \mathbb{K}^{n\times 1}$ is any column vector, then the equation $Ax = b$ (for an unknown column vector $x \in \mathbb{K}^{m\times 1}$) can be solved using the Gaussian elimination algorithm (e.g., by forming the augmented matrix $(A \mid b)$, then transforming it into RREF, and reading off the solutions from this RREF by the same method as you learned in Linear Algebra).

(d) If $A \in \mathbb{K}^{n\times m}$ is a matrix with $n < m$, then there exists a nonzero $x \in \mathbb{K}^{m\times 1}$ such that $Ax = 0_{n\times 1}$. ("Nonzero" means "distinct from $0_{m\times 1}$"; a nonzero vector can have some zero entries.)

(e) Let $A \in \mathbb{K}^{n\times n}$. Then, the following are equivalent:

- The matrix A is invertible.
- The matrix A is row-equivalent to I_n. (Two matrices are said to be *row-equivalent* if one can be transformed into the other via row operations: swapping rows, scaling rows and adding a multiple of one row to another.)
- The matrix A is column-equivalent to I_n. (The definition of "*column-equivalent*" is the same as of "row-equivalent", but with columns being used instead of rows.)
- The RREF of A is I_n.
- The RREF of A has n pivots.
- The rank of A is n.
- The equation $Ax = 0_{n\times 1}$ (for an unknown $x \in \mathbb{K}^{n\times 1}$) has only the trivial solution (that is, $x = 0_{n\times 1}$).

- For each vector $b \in \mathbb{K}^{n\times 1}$, the equation $Ax = b$ has a solution.
- For each vector $b \in \mathbb{K}^{n\times 1}$, the equation $Ax = b$ has a unique solution.
- The columns of A are linearly independent.
- The rows of A are linearly independent.
- There is a matrix $B \in \mathbb{K}^{n\times n}$ such that $AB = I_n$.
- There is a matrix $B \in \mathbb{K}^{n\times n}$ such that $BA = I_n$.
- We have $\det A \neq 0$. (We will later define determinants.)

(Matrices satisfying these equivalent conditions are called *nonsingular*.)

Proof of Theorem 6.1.1 (sketched). I shall give references to places where these facts are proven. Most of these places only consider matrices with real or complex entries, but the proofs still work for an arbitrary field $\mathbb{K}$.

(a) See [Strick13, §6, proof of Theorem 6.2 (a)] or [Carrel17, Proposition 3.7] or [GalQua18, Proposition 8.14] for the proof that any matrix has a RREF; see [Heffer17, Section One.III, Theorem 2.6] or [Carrel05, Proposition 3.18] or [Carrel17, Proposition 3.12] or [GalQua18, Proposition 8.19] for a proof that this RREF is unique.

(b) The RREF R of A is obtained from A by a sequence of row operations. Thus, it suffices to show that the row space, the kernel and the rank of a matrix are preserved under row operations. This is well-known and simple. (See, e.g., [Strick13, Lemma 9.15] or [GalQua18, Proposition 8.13] for a proof that the row space is preserved under row operations. The fact that the kernel and the rank are preserved under row operations is showed in [GalQua18, proof of Proposition 8.13] as well.)

(c) See [Strick13, Method 6.9] or [Knapp16a, Example before Proposition 1.26] or [GalQua18, §8.11].

(d) This is [Knapp16a, Proposition 1.26 **(d)**], and also appears in [Strick13, Remark 8.9] (because a relation $\lambda_1 v_1 + \cdots + \lambda_m v_m = 0$ between the columns $v_1, v_2, \ldots, v_m$ of A means precisely that the vector $x = (v_1, v_2, \ldots, v_m)^T \in \mathbb{K}^{m\times 1}$ satisfies $Ax = 0_{n\times 1}$) and in [GalQua18, Proposition 8.17].

(e) The Wikipedia calls Theorem 6.1.1 **(e)** (or similar results which have some more or fewer equivalent conditions) the "invertible matrix theorem". Most of it is proven in [Strick13, Theorem 11.5] (for $\mathbb{K} = \mathbb{R}$ only, but the general case works in the same way). Some parts are also proven in [Knapp16a, Theorem 1.30 and Corollary 1.32] and in [GalQua18, Proposition 8.18]. □

6.1.2. What if $\mathbb{K}$ is not a field?

Things get weird when $\mathbb{K}$ is not a field. For an example, set $\mathbb{K} = \mathbb{Z}/26$. This is not a field, since 26 is not prime (after all, $26 = 2 \cdot 13$). The ring $\mathbb{Z}/26$ has been used in classical cryptography, since its elements are in bijection with the letters of the (modern) Roman alphabet:

$$0 \mapsto A, \qquad 1 \mapsto B, \qquad 2 \mapsto C, \qquad \ldots .$$

For example, the *Hill cipher* lets you encrypt a word using a 3×3-matrix over $\mathbb{Z}/26$ as a key. The idea is simple: You split the word into 3-letter chunks; you turn each chunk into a column vector in $(\mathbb{Z}/26)^{3\times 1}$; and you multiply each of these columns vectors by your key matrix. To decrypt, you would have to invert the key matrix.

So we want to know how to invert a matrix over $\mathbb{Z}/26$.

If $\mathbb{Z}/26$ was a field, you would know how to do this via Gaussian elimination.

Most of Theorem 6.1.1 collapses when $\mathbb{K}$ is not a field. For example, let $\mathbb{K} = \mathbb{Z}/26$ and

$$A = \begin{pmatrix} 2 & 13 \\ 13 & 20 \end{pmatrix} \in \mathbb{K}^{2\times 2}.$$

(We are abusing notation here: In truth, the entries of A are not the integers $2, 13, 13, 20$ but rather their residue classes $[2]_{26}, [13]_{26}, [13]_{26}, [20]_{26}$. But we shall simply write the integers instead and hope that the reader knows what we mean.)

Is this matrix A invertible?

Let us first try to find the RREF of A. If we would blindly follow the Gaussian elimination algorithm, we would fail very quickly: None of the 4 entries of A has a multiplicative inverse; thus we could not transform any entry of A into 1 by scaling a row of A. But we can try to loosen Gaussian elimination by allowing more strategic row operations: Instead of trying to get a 1 in a pivot position immediately by scaling a row, we can attempt to obtain a 1 by row addition operations. For example, we can transform our matrix A above as follows:

$$\begin{aligned}
&\begin{pmatrix} 2 & 13 \\ 13 & 20 \end{pmatrix} \\
&\overset{\text{subtract 6 times row 1 from row 2}}{\mapsto} \begin{pmatrix} 2 & 13 \\ 1 & 20 \end{pmatrix} \\
&\overset{\text{swap row 1 with row 2}}{\mapsto} \begin{pmatrix} 1 & 20 \\ 2 & 13 \end{pmatrix} \\
&\overset{\text{subtract 2 times row 1 from row 2}}{\mapsto} \begin{pmatrix} 1 & 20 \\ 0 & 25 \end{pmatrix} \\
&\overset{\text{scale row 2 by } -1}{\mapsto} \begin{pmatrix} 1 & 20 \\ 0 & 1 \end{pmatrix} \\
&\overset{\text{subtract 20 times row 2 from row 1}}{\mapsto} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.
\end{aligned}$$

So our matrix A does have a RREF (namely, I_2), and even is invertible! (We can find an inverse of A by computing an RREF of the block matrix $(A \mid I_2)$; see, e.g., [Strick13, Method 11.11] for this procedure.)

What exactly was the method behind our above row-reduction procedure? Let us see how the first column has been transformed:

$$\begin{pmatrix} 2 \\ 13 \end{pmatrix} \overset{\text{subtract 6 times row 1 from row 2}}{\mapsto} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \overset{\text{swap row 1 with row 2}}{\mapsto} \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$
$$\overset{\text{subtract 2 times row 1 from row 2}}{\mapsto} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

So what we did was progressively making the entries of the first column smaller by subtracting a multiple of the first entry from the second entry (and swapping the two entries, in order to move the smaller entry into the first position). This is exactly the Euclidean algorithm! (Or, rather, it would be the Euclidean algorithm if we had used honest integers instead of residue classes in $\mathbb{Z}/26$.)

What happens in general? In general, when $\mathbb{K} = \mathbb{Z}/n$, the Gaussian elimination algorithm as defined in linear algebra does not always work. Nevertheless, a variant of it works, in which you do not directly scale rows to turn entries into 1, but instead "minimize" the whole column using the Euclidean algorithm as we did with our matrix A above. You will not always be able to get 1's in pivot positions, because the gcd (which the Euclidean algorithm computes) may not be 1; thus, the result will not always be an RREF in the classical sense, but rather something loosely resembling it.

For details, look up the *Smith normal form* (e.g., in [Elman18, §113]). Note that for $n = 0$, we have $\mathbb{Z}/n \cong \mathbb{Z}$ (as rings), so this applies to matrices with integer entries.

6.1.3. Review of basic notions from linear algebra

Convention 6.1.2. For the rest of this section, we fix a field $\mathbb{K}$. The elements of $\mathbb{K}$ will be referred to as *scalars*.

In the linear algebra you have seen before, the scalars are usually real numbers (i.e., we have $\mathbb{K} = \mathbb{R}$), but much of the theory works in the same way for every field.

Definition 6.1.3. Let $n \in \mathbb{N}$. Recall that $\mathbb{K}^{1\times n}$ is the set of all row vectors of size n.

A *subspace* of $\mathbb{K}^{1\times n}$ means a subset $S \subseteq \mathbb{K}^{1\times n}$ satisfying the following axioms:

- **(a)** We have $0_{1\times n} \in S$.
- **(b)** If $a, b \in S$, then $a + b \in S$.
- **(c)** If $a \in S$ and $\lambda \in \mathbb{K}$, then $\lambda a \in S$.

In other words, a subspace of $\mathbb{K}^{1\times n}$ is a subset of $\mathbb{K}^{1\times n}$ that contains the zero vector and is closed under addition and scaling.

Subspaces are often called *vector subspaces*.

A similar definition defines subspaces of $\mathbb{K}^{n\times 1}$ (column vectors).

There is a more general version of this definition, which extends it to subspaces of arbitrary vector spaces (see Definition 6.7.3).

Definition 6.1.4. Let $n \in \mathbb{N}$. Let $v_1, v_2, \ldots, v_k$ be some row vectors in $\mathbb{K}^{1\times n}$.

(a) A *linear combination* of $v_1, v_2, \ldots, v_k$ means a row vector of the form

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k, \qquad \text{with } \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}.$$

(b) The *span* of $v_1, v_2, \ldots, v_k$ is defined to be the subset

$$\begin{aligned} &\{\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k \mid \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}\} \\ &= \{\text{linear combinations of } v_1, v_2, \ldots, v_k\} \end{aligned}$$

of $\mathbb{K}^{1\times n}$. This span is a subspace of $\mathbb{K}^{1\times n}$. (This is easy to check.)

(c) The vectors $v_1, v_2, \ldots, v_k$ are said to be *linearly independent* if the only k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k = 0_{1\times n}$ is $\left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$.

(d) Let U be a subspace of $\mathbb{K}^{1\times n}$. We say that $v_1, v_2, \ldots, v_k$ form a *basis* of U (or, more formally, $(v_1, v_2, \ldots, v_k)$ is a basis of U) if and only if the vectors $v_1, v_2, \ldots, v_k$ are linearly independent and their span is U.

(e) Let U be a subspace of $\mathbb{K}^{1\times n}$. We say that the list $(v_1, v_2, \ldots, v_k)$ *spans* U if and only if the span of $v_1, v_2, \ldots, v_k$ is U. (More informally, instead of saying "the list $(v_1, v_2, \ldots, v_k)$ *spans* U", we can say "the vectors $v_1, v_2, \ldots, v_k$ *span* U"; of course, this is not the same as saying that each of these k vectors on its own spans U.)

All the terminology we have just introduced depends on $\mathbb{K}$. Whenever the field $\mathbb{K}$ is not clear from the context, you can insert it into this terminology to make it unambiguous: e.g., say "$\mathbb{K}$-linear combination" instead of "linear combination", and "$\mathbb{K}$-span" instead of "span".

Theorem 6.1.5. Let $n \in \mathbb{N}$. Let U be a subspace of $\mathbb{K}^{1\times n}$.

(a) There exists at least one basis of U.

(b) Any two bases of U have the same size (= number of vectors).

(c) Given k linearly independent vectors in U, and given ℓ vectors that span U, we always have $k \leq \ell$.

(d) Any list of k linearly independent vectors in U can be extended to a basis of U.

(e) Any list of ℓ vectors that span U can be shrunk to a basis of U (i.e., we can remove some vectors from this list to get a basis of U).

Proof of Theorem 6.1.5 (sketched). This all is proven just as in standard linear algebra. Here are some specific references:

Theorem 6.1.5 **(a)** appears in [Strick13, Proposition 20.3, last sentence][173], and also is a particular case of [ConradD, Theorem 4][174] (applied to $V = \mathbb{K}^{1\times n}$ and $W = U$). It also follows from [Payne09, Theorem 3.2.3 and Lemma 3.2.4][175].

Theorem 6.1.5 **(b)** is proven in [Heffer17, Chapter Two, Theorem III.2.5], in [ConradD, Corollary 1], in [GalQua18, Theorem 3.11, last sentence] and in [Payne09, Lemma 3.2.5]. It also follows from [Strick13, Corollary 20.5 (c)].

Theorem 6.1.5 **(d)** is proven in [Heffer17, Chapter Two, Corollary III.2.13], in [ConradD, Theorem 3] (since Theorem 6.1.5 **(a)** shows that U has a basis) and [Payne09, Lemma 3.2.8] (since Theorem 6.1.5 **(a)** shows that U has a basis).

Theorem 6.1.5 **(e)** is proven in [Heffer17, Chapter Two, Corollary III.2.14], in [ConradD, Theorem 3], in [Walker87, Theorem 3.3.3], in [GalQua18, Theorem 3.11, second sentence] and in [Payne09, Theorem 3.2.7].

Theorem 6.1.5 **(c)** follows from parts **(b)**, **(d)** and **(e)** once you extend your list of k linearly independent vectors in U to a basis of U and shrink your list of ℓ vectors spanning U to a basis of U. Alternatively, Theorem 6.1.5 **(c)** follows from [GalQua18, Proposition 3.10, last sentence] or from [Payne09, Theorem 3.2.2]. □

Again, the same holds for column vectors.

Definition 6.1.6. Let $n \in \mathbb{N}$. Let U be a subspace of $\mathbb{K}^{1\times n}$.

The *dimension* of U is defined to be the size of a basis of U. (Parts **(a)** and **(b)** of Theorem 6.1.5 show that this is indeed well-defined.) The dimension of U is denoted by $\dim U$.

Proposition 6.1.7. Let $n \in \mathbb{N}$. Let U and V be two subspaces of $\mathbb{K}^{1\times n}$ such that $U \subseteq V$.

(a) We have $\dim U \leq \dim V$.

(b) If $\dim U = \dim V$, then $U = V$.

Proof sketch. Pick a basis of U. This basis is a list of $\dim U$ many linearly independent vectors in V (since $U \subseteq V$). Thus, Theorem 6.1.5 **(d)** (applied to $\dim U$ and V instead of k and U) shows that this list can be extended to a basis of V. The latter basis, of course, has size $\dim V$. Thus, $\dim U \leq \dim V$ (since we have extended a list of size $\dim U$ and obtained a list of size $\dim V$). This proves Proposition 6.1.7 **(a)**.

(b) Assume that $\dim U = \dim V$. We have just found a basis of V by extending a basis of U. In light of $\dim U = \dim V$, this extension must have been trivial – i.e.,

[173] Note that Strickland works with column vectors in [Strick13, Proposition 20.3, last sentence], while our U consists of row vectors. But the arguments are the same.

[174] Note that in the (otherwise excellent) note [ConradD], Conrad follows the inane convention that an empty list () cannot be a basis. This forces him to make the unnatural requirement "$V \neq \{0\}$" in [ConradD, Theorem 1] and in various other places throughout his note. You should ignore this special treatment (or, rather, non-treatment) of empty lists when you read the note.

[175] Note that [Payne09] (just as various other texts) defines a basis as a set rather than a list of vectors. This is somewhat awkward, but it is not hard to translate between the two concepts of "basis".

we must have extended our basis of U by no further vectors. This means that our basis of U was already a basis of V to begin with. From this, it is easy to see that $U = V$ (because the span of a basis of U is always U, whereas the span of a basis of V is always V). This proves Proposition 6.1.7 **(b)**. □

Now, let us connect this with matrices:

Definition 6.1.8. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be a matrix.

(a) The *row space* of A is defined to be the span of the rows of A. This is a subspace of $\mathbb{K}^{1 \times m}$, and is called $\operatorname{Row} A$.

(b) The *column space* of A is defined to be the span of the columns of A. This is a subspace of $\mathbb{K}^{n \times 1}$, and is called $\operatorname{Col} A$.

Theorem 6.1.9. Let $A \in \mathbb{K}^{n \times m}$ be a matrix. Then, $\dim \operatorname{Row} A = \dim \operatorname{Col} A$.

Proof of Theorem 6.1.9 (sketched). One way to prove this is to transform A into RREF, and argue that both $\dim \operatorname{Row} A$ and $\dim \operatorname{Col} A$ equal the number of pivots in the RREF. There are other, more abstract ways. See linear algebra textbooks for this proof: for example, [Heffer17, Chapter Two, Theorem III.3.11] (where $\dim \operatorname{Row} A$ is called the "row rank" of A, and $\dim \operatorname{Col} A$ is called the "column rank" of A). □

Definition 6.1.10. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be a matrix. Theorem 6.1.9 shows that $\dim \operatorname{Row} A = \dim \operatorname{Col} A$. This number $\dim \operatorname{Row} A = \dim \operatorname{Col} A$ is called the *rank* of A and is denoted by $\operatorname{rank} A$.

The following is easy to see:

Proposition 6.1.11. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be a matrix. Then, $\operatorname{rank} A$ is an integer between 0 and $\min \{n, m\}$.

So we have seen that a matrix gives rise to two subspaces: its row space and its column space. But there is more:

Definition 6.1.12. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be a matrix.

(a) The *kernel* (or *nullspace*) of A is defined to be the set of all column vectors $v \in \mathbb{K}^{m \times 1}$ such that $Av = 0_{n \times 1}$. This is a subspace of $\mathbb{K}^{m \times 1}$, and is called $\operatorname{Ker} A$.

(b) The *left kernel* (or *left nullspace*) of A is defined to be the set of all row vectors $w \in \mathbb{K}^{1 \times n}$ such that $wA = 0_{1 \times m}$. This is a subspace of $\mathbb{K}^{1 \times n}$.

Altogether, we have thus found four subspaces coming out of a matrix A. These are the famous "four fundamental subspaces" (in Gilbert Strang's terminology). One result that connects two of them is the following fact, known as the *rank-nullity theorem*:

Theorem 6.1.13. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be a matrix. Then,

$$\operatorname{rank} A + \dim \operatorname{Ker} A = m.$$

Proof of Theorem 6.1.13 (sketched). Most textbooks state Theorem 6.1.13 not in terms of matrices, but rather in the (equivalent) language of linear maps. For example, this is how it is stated in [Heffer17, Chapter Three, Theorem II.2.14] or [Carrel05, Theorem 7.17] or [Knapp16a, Corollary 2.15] or [Payne09, Theorem 4.2.2]. □

Note that the number $\dim \operatorname{Ker} A$ is known as the *nullity* of a matrix A.

6.1.4. Linear algebra over $\mathbb{Z}/2$: "button madness" / "lights out"

We now discuss an old puzzle, which is known as "button madness" or "lights out" (more precisely, these are two slightly different variants of the same puzzle). You can try it out on

`https://bz.var.ru/comp/web/js/floor.html`

(see also `https://www.win.tue.nl/~aeb/ca/madness/madrect.html` for a list of mathematical sources on this puzzle).

One version of this puzzle gives you 16 lamps arranged into a 4 × 4-grid. Each lamp comes with a lightswitch; but flipping this lightswitch toggles not just this lamp, but also its four adjacent lamps (or three or two adjacent lamps, if the switch you have flipped is at the border of the grid). For example, if your grid looks like this:

1	0	0	1
0	1	1	0
0	0	1	0
1	1	0	1

(where an entry 1 means a lamp turned on, and an entry 0 means a lamp turned off), and you flip the lightswitch in cell $(2, 3)$ (that is, the third cell from the left in the second row from the top), then you obtain the grid

1	0	1	1
0	0	0	1
0	0	0	0
1	1	0	1

.

(A total of 5 lamps have changed their state: three have been turned off, and two have been turned on.) If you then flip the lightswitch in cell $(1, 3)$ of this new grid, then you obtain the grid

1	1	0	0
0	0	1	1
0	0	0	0
1	1	0	1

.

At the beginning, all lamps are turned off. Your goal is to achieve the opposite state (i.e., all lamps being on at the same time) by flipping a sequence of lightswitches. Is this possible, and how? (In some versions of this puzzle – such as the "lights out" version – it's exactly the other way round: The lights are all on initially, and you must turn them all off. Of course, this makes no difference to the solution.)

In some versions of this puzzle, the grid is "toroidal", in the sense that it is understood to wrap around – for example, the cells $(1,4)$ and $(1,1)$ are considered to be adjacent, and so are the cells $(4,1)$ and $(1,1)$. We shall not consider this case here, but it can be solved by the same method.

Of course, you can play the same game on larger grids, triangular grids, etc.. But in order to get a grip on how to solve such a puzzle, we shall first analyze a much simpler version: the "1-dimensional version" of the puzzle.

Here is this "1-dimensional version": We have 4 lamps in a row (numbered $1,2,3,4$), each equipped with a lightswitch. The lightswitch at lamp i toggles lamp i, lamp $i-1$ (if it exists) and lamp $i+1$ (if it exists). Initially, all 4 lamps are off. Can we turn them all on by flipping a sequence of lightswitches?

Yes, of course: we just have to flip the lightswitches at lamps 1 and 4. But let us pretend that we aren't that smart, and instead try to solve the puzzle systematically.

We model the states of our lamps by a row vector in $(\mathbb{Z}/2)^{1\times 4}$. We write a row vector $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$ as $(a_1, a_2, \ldots, a_n)$.

More precisely, we model each state by the row vector $(a_1, a_2, a_3, a_4) \in (\mathbb{Z}/2)^{1\times 4}$, where

$$a_i = \begin{cases} [0]_2, & \text{if lamp } i \text{ is off;} \\ [1]_2, & \text{if lamp } i \text{ is on} \end{cases} = \underbrace{\left[\underbrace{[\text{lamp } i \text{ is on}]}_{\text{Iverson bracket}} \right]_2}_{\text{residue class}} .$$

We shall write 0 and 1 for $[0]_2$ and $[1]_2$ throughout this subsection (except in Proposition 6.1.14), so we can rewrite this as

$$a_i = \begin{cases} 0, & \text{if lamp } i \text{ is off;} \\ 1, & \text{if lamp } i \text{ is on} \end{cases} = \underbrace{[\text{lamp } i \text{ is on}]}_{\text{Iverson bracket}},$$

but keep in mind that these values are understood to be in $\mathbb{Z}/2$.

The initial state is $(0,0,0,0)$. The final state that we want to achieve is $(1,1,1,1)$. Flipping a lightswitch corresponds to adding a certain row vector to our state. Namely:

- Flipping lightswitch 1 means adding $(1,1,0,0)$.
- Flipping lightswitch 2 means adding $(1,1,1,0)$.
- Flipping lightswitch 3 means adding $(0,1,1,1)$.
- Flipping lightswitch 4 means adding $(0,0,1,1)$.

Thus, flipping a lightswitch means adding the corresponding row of the matrix

$$A := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \in (\mathbb{Z}/2)^{4\times 4}$$

to our state. The reachable states are thus exactly the elements of $\operatorname{Row} A$, the row space of A.

Hence, our goal is to show that $(1,1,1,1) \in \operatorname{Row} A$.

This is quite easy for the concrete matrix A above (just notice that $(1,1,1,1)$ is the sum of the 1-st and 4-th rows of A); but let us try a theoretical argument. It will rely on the following general fact:

Proposition 6.1.14. Let $n, m \in \mathbb{N}$. Let $\mathbb{K}$ be any field. Let $A \in \mathbb{K}^{n\times m}$ and $b \in \mathbb{K}^{1\times m}$. Assume the following:

> *Assumption 1:* If $c \in \mathbb{K}^{m\times 1}$ satisfies $Ac = 0$, then $bc = 0$. (Here, of course, the "0" in "$Ac = 0$" means $0_{n\times 1}$.)

Then, $b \in \operatorname{Row} A$.

Proof of Proposition 6.1.14. Let $\begin{pmatrix} A \\ b \end{pmatrix}$ denote the $(n+1)\times m$-matrix formed from the $n \times m$-matrix A by attaching the row vector b to its bottom. For example, if $A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$ and $b = \begin{pmatrix} b_1 & b_2 \end{pmatrix}$, then $\begin{pmatrix} A \\ b \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \\ b_1 & b_2 \end{pmatrix}$.

Theorem 6.1.13 yields $\operatorname{rank} A + \dim \operatorname{Ker} A = m$. Thus,

$$\operatorname{rank} A = m - \dim \operatorname{Ker} A. \tag{197}$$

The same argument can be applied to the matrix $\begin{pmatrix} A \\ b \end{pmatrix}$ instead of A. We thus obtain

$$\operatorname{rank} \begin{pmatrix} A \\ b \end{pmatrix} = m - \dim \operatorname{Ker} \begin{pmatrix} A \\ b \end{pmatrix}. \tag{198}$$

But each $c \in \operatorname{Ker} A$ satisfies $Ac = 0$ and thus $bc = 0$ (by Assumption 1), and therefore $c \in \operatorname{Ker} \begin{pmatrix} A \\ b \end{pmatrix}$ (because the "row-by-column" nature of matrix multiplication shows that $\begin{pmatrix} A \\ b \end{pmatrix} c = \begin{pmatrix} Ac \\ bc \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0$). So we have $\operatorname{Ker} A \subseteq \operatorname{Ker} \begin{pmatrix} A \\ b \end{pmatrix}$. Also, clearly, $\operatorname{Ker} \begin{pmatrix} A \\ b \end{pmatrix} \subseteq \operatorname{Ker} A$ (because if $c \in \operatorname{Ker} \begin{pmatrix} A \\ b \end{pmatrix}$, then $\begin{pmatrix} A \\ b \end{pmatrix} c = 0$, so that $0 = \begin{pmatrix} A \\ b \end{pmatrix} c = \begin{pmatrix} Ac \\ bc \end{pmatrix}$ and thus $Ac = 0$, so that $c \in \operatorname{Ker} A$). Combining these two relations, we obtain $\operatorname{Ker} A = \operatorname{Ker} \begin{pmatrix} A \\ b \end{pmatrix}$. Hence, the right hand sides of (197) and (198) are equal. Thus, the left hand sides are equal as well. In other words, $\operatorname{rank} A = \operatorname{rank} \begin{pmatrix} A \\ b \end{pmatrix}$. In other words,

$$\dim \operatorname{Row} A = \dim \operatorname{Row} \begin{pmatrix} A \\ b \end{pmatrix}$$

(since $\operatorname{rank} B = \dim \operatorname{Row} B$ for any matrix B). But $\operatorname{Row} A \subseteq \operatorname{Row} \begin{pmatrix} A \\ b \end{pmatrix}$ (by the definition of a row space). Combining these facts, we obtain

$$\operatorname{Row} A = \operatorname{Row} \begin{pmatrix} A \\ b \end{pmatrix}$$

(by Proposition 6.1.7 **(b)**, applied to $U = \operatorname{Row} A$ and $V = \operatorname{Row} \begin{pmatrix} A \\ b \end{pmatrix}$). But the definition of a row space yields $b \in \operatorname{Row} \begin{pmatrix} A \\ b \end{pmatrix} = \operatorname{Row} A$. This proves Proposition 6.1.14. □

Over the field $\mathbb{Z}/2$, this fact has the following consequence:

Corollary 6.1.15. Let $n \in \mathbb{N}$. Let $A \in (\mathbb{Z}/2)^{n \times n}$ be a symmetric matrix. ("*Symmetric*" means that the (i,j)-th entry of A equals the (j,i)-th entry of A for all i and j. In other words, it means that $A^T = A$.)

Let d be the diagonal of A, written as a row vector. (In other words, let $d = (a_{1,1}, a_{2,2}, \ldots, a_{n,n})$, where $a_{i,j}$ is the (i,j)-th entry of A.)

Then, $d \in \operatorname{Row} A$.

Note that Corollary 6.1.15 brutally fails over fields different from $\mathbb{Z}/2$. For example, if we allow A to be a matrix in $\mathbb{Z}^{n \times n}$ instead, then $A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ is symmetric but its diagonal $d = (1,1)$ does not belong to $\operatorname{Row} A$.

Proof of Corollary 6.1.15. Set $\mathbb{K} = \mathbb{Z}/2$. By Proposition 6.1.14 (applied to $m = n$ and $b = d$), it suffices to show the following:

Assumption 1: If $c \in \mathbb{K}^{n \times 1}$ satisfies $Ac = 0$, then $dc = 0$.

[*Proof of Assumption 1:* Let $c \in \mathbb{K}^{n \times 1}$ satisfy $Ac = 0$. We must prove that $dc = 0$.

I claim that $dc = c^T Ac$.

To see this, write c as $c = (c_1, c_2, \ldots, c_n)^T$ and A as $A = (a_{i,j})_{1 \leq i \leq n,\ 1 \leq j \leq n}$. Then, expanding $c^T Ac$ yields

$$\begin{aligned}
c^T Ac &= \sum_{i,j} c_i a_{i,j} c_j = \sum_{i,j} a_{i,j} c_i c_j \\
&= \underbrace{\sum_{i<j} a_{i,j} c_i c_j}_{\substack{= \sum\limits_{j<i} a_{j,i} c_j c_i \\ \text{(here, we have renamed} \\ \text{the indices } i \text{ and } j \text{ as } j \text{ and } i)}} + \underbrace{\sum_{i=j} a_{i,j} c_i c_j}_{= \sum\limits_{i} a_{i,i} c_i c_i} + \underbrace{\sum_{i>j}}_{= \sum\limits_{j<i}} \underbrace{a_{i,j}}_{\substack{= a_{j,i} \\ \text{(since } A \\ \text{is symmetric)}}} \underbrace{c_i c_j}_{= c_j c_i} \\
&= \sum_{j<i} a_{j,i} c_j c_i + \sum_{i} a_{i,i} c_i c_i + \sum_{j<i} a_{j,i} c_j c_i = \underbrace{2}_{\substack{=0 \\ \text{(since we are} \\ \text{in } \mathbb{Z}/2)}} \sum_{j<i} a_{j,i} c_j c_i + \sum_{i} a_{i,i} c_i c_i \\
&= \sum_{i} a_{i,i} \underbrace{c_i c_i}_{\substack{= c_i^2 = c_i \\ \text{(since } x^2 = x \\ \text{for all } x \in \mathbb{Z}/2)}} = \sum_{i} a_{i,i} c_i = dc
\end{aligned}$$

(since $c = (c_1, c_2, \ldots, c_n)^T$ and $d = (a_{1,1}, a_{2,2}, \ldots, a_{n,n})$). So $dc = c^T \underbrace{Ac}_{=0} = c^T 0 = 0$.

Thus, Assumption 1 is proven.]

Corollary 6.1.15 now follows. □

Now, why can the "lights out" puzzle be solved?

We want to prove that $(1, 1, 1, 1) \in \operatorname{Row} A$ for our matrix $A \in (\mathbb{Z}/2)^{4 \times 4}$.

This follows from Corollary 6.1.15, since the matrix A is symmetric, and since its diagonal is $(1, 1, 1, 1)$.

The same argument works for the "proper" (2-dimensional) "lights out" puzzle; we just have to use row vectors of size 16 (not 4) and 16×16-matrices (not 4×4-matrices). More generally, the same argument works for any such puzzle on any "grid" as long as:

- each lamp i has a lightswitch which toggles at least lamp i;
- if the lightswitch at lamp i toggles lamp j, then the lightswitch at lamp j toggles lamp i.

These conditions guarantee that the corresponding matrix A will be symmetric and its diagonal will be $(1, 1, \ldots, 1)$ (and thus we can apply Corollary 6.1.15).

How to find the exact sequence of flips that results in all lights being on? This is tantamount to finding the coefficients of a linear combination of the rows of A that equals $(1, 1, \ldots, 1)$. This boils down to solving a system of linear equations over $\mathbb{Z}/2$, which can be achieved using Gaussian elimination.

What other states can be achieved by flipping lightswitches? Again, for each specific grid and each specific state, this can be solved by Gaussian elimination; but characterizing the reachable states more explicitly is a hard problem with no unified answer. (See the link above.)

6.1.5. A warning about orthogonality and positivity

I have said above that "more or less" all linear algebra over $\mathbb{R}$ works identically over any field $\mathbb{K}$. There is an exception: Anything that uses positivity will break down over some fields $\mathbb{K}$. Let me briefly telegraph what can go wrong. (Don't worry if the things I am mentioning are not familiar to you.)

One thing that uses positivity is QR-decomposition. And indeed, not every matrix over an arbitrary field has a QR-decomposition.

You can still define dot products and orthogonal complements of subspaces. But it is no longer true that $\mathbb{K}^{n\times 1} = U \oplus U^{\perp}$ for any subspace U of $\mathbb{K}^{n\times 1}$. It can happen that $U \cap U^{\perp} \neq \{0\}$. For example, there are column vectors $v \neq 0_{n\times 1}$ that are orthogonal to themselves with respect to the dot product (that is, $v^T v = 0$).

Example: In $\mathbb{Z}/3$, we have

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}^T \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = (1,1,1) \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = 1\cdot 1 + 1\cdot 1 + 1\cdot 1 = 3 = 0.$$

So the vector $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in (\mathbb{Z}/3)^{3\times 1}$ is orthogonal to itself.

6.2. Matrix algebra vs. coordinate-free linear algebra

There are two common approaches to linear algebra: The first is the study of matrices and column vectors (or row vectors); this is down-to-earth but often clumsy and unenlightening. The second is the study of vector spaces and linear transformations; this is more abstract but more general and often better for conceptual understanding. The first approach is known as *matrix algebra*; the second is called *coordinate-free linear algebra*.

These two approaches are closely connected: The first can be viewed as a particular case of the second (as the column vectors of a given size n form a vector space, and any matrix defines a linear map between two such vector spaces); the second appears more general but in reality can often be reduced to the first (viz., theorems about vector spaces can often be proven by "picking bases" and representing linear maps by matrices with respect to these bases). Thus, a sufficiently deep course on linear algebra will necessarily survey both of these approaches, and practitioners of the subject will often apply whichever approach fits a problem better.

In the previous section, we have seen how the first approach can be generalized from real or complex matrices to matrices over any field (and, as far as the basics are concerned, over any commutative ring). We shall now try this with the second approach. Over a field, the second approach turns out to work out in pretty much the same way as over the real or complex numbers; however, over a commutative ring, things become a lot more interesting.

6.3. $\mathbb{K}$-modules: the definition

Let us begin by defining the analogue of a vector space: a *module*. Roughly speaking, a module is the same as a vector space, except that it is over a commutative ring instead of a field:

Definition 6.3.1. Let $\mathbb{K}$ be a commutative ring.

A $\mathbb{K}$-*module* means a set M equipped with

- a binary operation $+$ on M (called "*addition*", and not to be confused with the addition $+_{\mathbb{K}}$ of $\mathbb{K}$),
- a map $\cdot\ :\ \mathbb{K} \times M \to M$ (called "*scaling*", and not to be confused with the multiplication $\cdot_{\mathbb{K}}$ of $\mathbb{K}$), and
- an element $0_M \in M$ (called "*zero vector*" or "zero", and not to be confused with the zero of $\mathbb{K}$)

satisfying the following axioms:

- **(a)** We have $a + b = b + a$ for all $a, b \in M$.
- **(b)** We have $a + (b + c) = (a + b) + c$ for all $a, b, c \in M$.
- **(c)** We have $a + 0_M = 0_M + a = a$ for all $a \in M$.
- **(d)** Each $a \in M$ has an additive inverse (i.e., there is an $a' \in M$ such that $a + a' = a' + a = 0_M$).
- **(e)** We have $\lambda (a + b) = \lambda a + \lambda b$ for all $\lambda \in \mathbb{K}$ and $a, b \in M$. Here and in the following, we use the notation "λc" (or, equivalently, "$\lambda \cdot c$") for the image of a pair $(\lambda, c) \in \mathbb{K} \times M$ under the "scaling" map $\cdot$ (similarly to how we write ab for the image of a pair $(a, b) \in \mathbb{K} \times \mathbb{K}$ under the "multiplication" map $\cdot$).
- **(f)** We have $(\lambda + \mu) a = \lambda a + \mu a$ for all $\lambda, \mu \in \mathbb{K}$ and $a \in M$.
- **(g)** We have $0a = 0_M$ for all $a \in M$.
- **(h)** We have $(\lambda\mu) a = \lambda (\mu a)$ for all $\lambda, \mu \in \mathbb{K}$ and $a \in M$.
- **(i)** We have $1a = a$ for all $a \in M$.
- **(j)** We have $\lambda \cdot 0_M = 0_M$ for all $\lambda \in \mathbb{K}$.

These ten axioms are called the *module axioms*.

A $\mathbb{K}$-module is often called a "module over $\mathbb{K}$".

The axioms "$\lambda (a+b) = \lambda a + \lambda b$" and "$(\lambda + \mu) a = \lambda a + \mu a$" are known as the *distributivity laws for modules*. The axiom "$(\lambda \mu) a = \lambda (\mu a)$" is known as the *associativity law for modules*.

Definition 6.3.2. If $\mathbb{K}$ is a commutative ring and M is a $\mathbb{K}$-module, then the elements of M are called *vectors*, while the elements of $\mathbb{K}$ are called *scalars*. If $\lambda \in \mathbb{K}$ and $a \in M$, then λa (that is, the image of (λ, a) under the scaling map $\cdot : \mathbb{K} \times M \to M$) will be called the result of *scaling* the vector a by the scalar λ.

Definition 6.3.3. If $\mathbb{K}$ is a field, then $\mathbb{K}$-modules are called $\mathbb{K}$-*vector spaces*. (When $\mathbb{K} = \mathbb{R}$, these are the usual real vector spaces known from undergraduate linear algebra classes.)

6.4. Examples of $\mathbb{K}$-modules

Thus, any vector space you have seen in linear algebra is an example of a module. Let us see some other examples:

Example 6.4.1. Let $\mathbb{K}$ be a commutative ring. Then, $\mathbb{K}$ itself is a $\mathbb{K}$-module (with the addition given by the addition $+_{\mathbb{K}}$ of $\mathbb{K}$, and with the scaling given by the multiplication $\cdot_{\mathbb{K}}$ of $\mathbb{K}$, and with the zero vector given by the zero $0_{\mathbb{K}}$ of $\mathbb{K}$).

Example 6.4.2. Let $\mathbb{K}$ be a commutative ring. Let $n \in \mathbb{N}$. Equip the set $\mathbb{K}^n$ (that is, the set of all n-tuples of elements of $\mathbb{K}$) with entrywise addition (that is, a binary operation $+$ on $\mathbb{K}^n$ defined by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

for all $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \mathbb{K}^n$) and entrywise scaling (that is, a map $\cdot : \mathbb{K} \times \mathbb{K}^n \to \mathbb{K}^n$ defined by

$$\lambda (a_1, a_2, \ldots, a_n) = (\lambda a_1, \lambda a_2, \ldots, \lambda a_n)$$

for all $\lambda \in \mathbb{K}$ and $(a_1, a_2, \ldots, a_n) \in \mathbb{K}^n$) and the zero vector $(0, 0, \ldots, 0) \in \mathbb{K}^n$. Then, $\mathbb{K}^n$ becomes a $\mathbb{K}$-module.

Example 6.4.3. Let $\mathbb{K}$ be a commutative ring. Let $n, m \in \mathbb{N}$. Equip the set $\mathbb{K}^{n \times m}$ (that is, the set of all $n \times m$-matrices over $\mathbb{K}$) with the addition defined in Definition 5.8.7 **(a)** and the scaling defined in Definition 5.8.7 **(c)** and the zero vector $0_{n \times m}$. Then, $\mathbb{K}^{n \times m}$ becomes a $\mathbb{K}$-module.

Example 6.4.4. Let $\mathbb{K}$ be a commutative ring. The one-element set $\{0\}$ is a $\mathbb{K}$-module (with $+$ and $\cdot$ and zero vector defined in the only possible way). This is called the *zero module*. It is often called 0.

Example 6.4.5. Let n be an integer. Then:

(a) The set $\mathbb{Z}/n$ is a $\mathbb{Z}$-module, if you equip it with the addition and the scaling that we defined above (in Definition 3.4.12 and Definition 3.4.18) and with the zero vector $[0]_n$.

(b) The set $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\} = \{\text{all multiples of } n\}$ is a $\mathbb{Z}$-module (again equipped with the usual addition as addition, and the usual multiplication as scaling, and the integer 0 as zero vector).

Example 6.4.6. **(a)** The set $\mathbb{Q}$ (equipped with the usual addition, and with a scaling defined by the usual multiplication, and the zero vector 0) is a $\mathbb{Z}$-module.

(b) For every $q \in \mathbb{Q}$, the subset $q\mathbb{Z} := \{qz \mid z \in \mathbb{Z}\}$ of $\mathbb{Q}$ (again equipped with the usual $+$ and $\cdot$ and 0) is a $\mathbb{Z}$-module. For example, $\frac{1}{2}\mathbb{Z} = \{\ldots, -2, -1.5, -1, -0.5, 0, 0.5, 1, 1.5, 2, \ldots\}$ is a $\mathbb{Z}$-module. Note that $\frac{1}{2}\mathbb{Z}$ is **not** a ring (at least not with the usual $\cdot$ as multiplication), since $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \notin \frac{1}{2}\mathbb{Z}$.

(c) What other $\mathbb{Z}$-modules can we find inside $\mathbb{Q}$? Quite a few, it turns out. Here is a more exotic one: Let us call an integer n *squarefree* if it is not divisible by any perfect square other than 1. It is easy to see that an integer n is squarefree if and only if n is a product of **distinct** primes (or, equivalently, $v_p(n) \leq 1$ for each prime p). Thus, the squarefree integers are $1, 2, 3, 5, 6, 7, 10, 11, 13, \ldots$ and their negatives. Now, let $\mathbb{Q}_{\text{sqf}}$ be the subset

$$\left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ with } b \text{ squarefree} \right\}$$

of $\mathbb{Q}$. Then, $\mathbb{Q}_{\text{sqf}}$ (equipped with the usual addition as addition, the usual multiplication as scaling, and the usual 0 as zero vector) is a $\mathbb{Z}$-module. (Check this!)

6.5. Cartesian products of $\mathbb{K}$-modules

Instead of giving further examples, let us show a way of constructing new $\mathbb{K}$-modules from old (analogous to Definition 5.7.3):

Definition 6.5.1. Let $\mathbb{K}$ be a commutative ring. Let $M_1, M_2, \ldots, M_n$ be n many $\mathbb{K}$-modules. Consider the set $M_1 \times M_2 \times \cdots \times M_n$, whose elements are n-tuples $(m_1, m_2, \ldots, m_n)$ with $m_i \in M_i$.

We define a binary operation $+$ on $M_1 \times M_2 \times \cdots \times M_n$ by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n),$$

and we define a "scaling" map $\cdot : \mathbb{K} \times (M_1 \times M_2 \times \cdots \times M_n) \to M_1 \times M_2 \times \cdots \times M_n$ by

$$\lambda \cdot (a_1, a_2, \ldots, a_n) = (\lambda a_1, \lambda a_2, \ldots, \lambda a_n).$$

Proposition 6.5.2. Let $\mathbb{K}$ be a commutative ring. Let $M_1, M_2, \ldots, M_n$ be n many $\mathbb{K}$-modules. The set $M_1 \times M_2 \times \cdots \times M_n$, endowed with the operation $+$ and the map $\cdot$ we just defined and with the zero vector $(0, 0, \ldots, 0)$, is a $\mathbb{K}$-module.

Proof of Proposition 6.5.2. Similar to the proof of Proposition 5.7.2. □

Definition 6.5.3. The $\mathbb{K}$-module $M_1 \times M_2 \times \cdots \times M_n$ constructed in Proposition 6.5.2 is called the *Cartesian product* (or *direct product*) of the $\mathbb{K}$-modules $M_1, M_2, \ldots, M_n$.

The $\mathbb{K}$-module $\mathbb{K}^n$ introduced in Example 6.4.2 is actually a particular case of Definition 6.5.3; in fact, it is precisely the Cartesian product $\underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ times}}$ of the $\mathbb{K}$-modules $\mathbb{K}, \mathbb{K}, \ldots, \mathbb{K}$ (that is, n copies of the $\mathbb{K}$-module $\mathbb{K}$ defined in Example 6.4.1).

6.6. Features and rules

Again, we shall follow the PEMDAS convention for addition and scaling. For example, the expression "$a + \lambda b$" shall mean $a + (\lambda b)$.

Proposition 6.6.1. Axioms **(g)** and **(j)** in Definition 6.3.1 follow from the others.

Proof of Proposition 6.6.1. Assume that all axioms in Definition 6.3.1 are satisfied except for axioms **(g)** and **(j)**. We must now show that axioms **(g)** and **(j)** are also satisfied.

*Proof of axiom **(g)**:* Let $a \in M$. Then, axiom **(f)** (applied to $\lambda = 0$ and $\mu = 0$) yields

$$(0+0)\,a = 0a + 0a.$$

This rewrites as $0a = 0a + 0a$ (since $0 + 0 = 0$). We can cancel $0a$ from this equation by adding an additive inverse of $0a$ to both sides (such an inverse exists because of axiom **(d)**); we thus get $0_M = 0a$. In other words, $0a = 0_M$. This proves axiom **(g)**.

The proof of axiom **(j)** is analogous, with use of axiom **(e)** instead of axiom **(f)**. □

Proposition 6.6.2. Axiom **(d)** in Definition 6.3.1 follows from the others.

Proof of Proposition 6.6.2. Assume that all axioms in Definition 6.3.1 are satisfied except for axiom **(d)**. We must now show that axiom **(d)** is also satisfied.

Let $a \in M$. We must prove that a has an additive inverse.

Axiom **(f)** in Definition 6.3.1 (applied to $\lambda = 1$ and $\mu = -1$) yields $(1 + (-1))\,a = \underbrace{1a}_{\substack{=a \\ \text{(by axiom (i))}}} + (-1)\,a = a + (-1)\,a$. Hence,

$$a + (-1)\,a = \underbrace{(1 + (-1))}_{=0}\,a = 0a = 0_M \qquad \text{(by axiom (g))}.$$

Also, axiom **(a)** yields $a + (-1)\,a = (-1)\,a + a$, so that $a + (-1)\,a = (-1)\,a + a = 0_M$. Thus, $(-1)\,a$ is an additive inverse of a. Hence, a has an additive inverse. Thus, axiom **(d)** is proven. □

Note that Proposition 6.6.1 and Proposition 6.6.2 cannot be merged: If we omit all three axioms **(d)**, **(g)** and **(j)**, then we cannot recover these axioms any more. (Indeed, our proof of axiom **(d)** relied on axiom **(g)** and vice versa.)

What can you do when you have a $\mathbb{K}$-module?

Convention 6.6.3. For the rest of this section, we fix a **commutative** ring $\mathbb{K}$, and we fix a $\mathbb{K}$-module M. We shall denote the zero vector 0_M of M by 0. (More generally, it is common to denote the zero vector of any $\mathbb{K}$-module by 0 as long as you are not afraid of confusion.)

Just as in a ring, elements of a module have unique additive inverses:

Theorem 6.6.4. Let $a \in M$. Then:

(a) The element a has exactly one additive inverse.

(b) This additive inverse is $(-1)\,a$.

Proof of Theorem 6.6.4. **(a)** Same as the proof of Theorem 5.4.2.

(b) This was shown in the proof of Proposition 6.6.2. □

We can now make the following definition, which copies Definition 5.4.4 almost verbatim:

Definition 6.6.5. **(a)** If $a \in M$, then the additive inverse of a will be called $-a$. (This is well-defined, since Theorem 6.6.4 **(a)** shows that this additive inverse is unique.)

(b) If $a \in M$ and $b \in M$, then we define the *difference* $a - b$ to be the element $a + (-b)$ of M. This new binary operation $-$ on M is called *"subtraction"*.

Remark 6.6.6. The subtraction we just defined (in Definition 6.6.5 **(b)**) for an arbitrary $\mathbb{K}$-module generalizes both

- the subtraction of matrices (when the $\mathbb{K}$-module is $\mathbb{K}^{n\times m}$), and
- the subtraction in $\mathbb{Z}/n$ (when $\mathbb{K} = \mathbb{Z}$ and the $\mathbb{K}$-module is $\mathbb{Z}/n$).

Remark 6.6.6 is easy to prove, but we delay the proof until later, since it will become even easier after Proposition 6.6.7 has been proven.

Using Definition 6.6.5 **(a)**, we can rewrite Theorem 6.6.4 **(b)** as follows:

$$-a = (-1)\,a \qquad \text{for each } a \in M. \tag{199}$$

Additive inverses and subtraction satisfy certain rules that should not surprise you:

Proposition 6.6.7. Let $a, b, c \in M$.

(a) We have $a - b = c$ if and only if $a = b + c$. (Roughly speaking, this means that subtraction undoes addition.)

(b) We have $-(a + b) = (-a) + (-b)$.

(c) We have $-0 = 0$.

(d) We have $0 - a = -a$.

(e) We have $-(-a) = a$.

(f) We have $-(\lambda a) = (-\lambda) a = \lambda (-a)$ for all $\lambda \in \mathbb{K}$.

(g) We have $a - b - c = a - (b + c)$. (Here and in the following, "$a - b - c$" should be read as "$(a - b) - c$".)

(h) We have $\lambda (b - c) = \lambda b - \lambda c$ and $(\lambda - \mu) a = \lambda a - \mu a$ for all $\lambda, \mu \in \mathbb{K}$.

(i) We have $-(a - b) = b - a$.

(j) We have $a - (-b) = a + b$.

(k) We have $(-1) a = -a$. (Here, the "1" on the left hand side means the unity of $\mathbb{K}$.)

(l) If $-a = -b$, then $a = b$.

Proof of Proposition 6.6.7. Same as for Proposition 5.4.5. □

Again, Proposition 6.6.7 shows that certain expressions (such as "$-\lambda a$" for $\lambda \in \mathbb{K}$ and $a \in M$) are unambiguous.

Proof of Remark 6.6.6. Let us prove that the subtraction we defined (in Definition 6.6.5 **(b)**) for an arbitrary $\mathbb{K}$-module generalizes the subtraction of matrices (when the $\mathbb{K}$-module is $\mathbb{K}^{n\times m}$).

The rough idea of the proof is "this is true, because both of these subtractions undo the same addition". Here is the argument in detail: Let $n, m \in \mathbb{N}$. Let M be the $\mathbb{K}$-module $\mathbb{K}^{n\times m}$. Let $A, B \in M$. Our goal is then to show that the difference $A - B$ defined as in Definition 6.6.5 **(b)** equals the difference $A - B$ defined as in Definition 5.8.7 **(b)**. Let us denote the former difference by D_1 and the latter difference by D_2. Our goal is thus to prove that $D_1 = D_2$.

We know that D_1 is the difference $A - B$ defined as in Definition 6.6.5 **(b)**. In other words, $A - B = D_1$, where the minus sign refers to the subtraction defined in Definition 6.6.5 **(b)**.

But Proposition 6.6.7 **(a)** (applied to $a = A$, $b = B$ and $c = D_1$) shows that we have $A - B = D_1$ if and only if $A = B + D_1$, where the minus sign refers to the subtraction defined in Definition 6.6.5 **(b)**. Hence, $A = B + D_1$ (since $A - B = D_1$). Note that the plus sign is unambiguous here: We have defined subtraction on M in two different ways (and still have to prove that these two definitions are equivalent), but we have defined addition on M only once.

But Theorem 5.8.10 **(i)** (applied to $C = D_1$) yields that we have the equivalence $(A - B = D_1) \iff (A = B + D_1)$, where the minus sign refers to the subtraction defined in Definition 5.8.7 **(b)**. Hence, we have $A - B = D_1$ (since we have $A = B + D_1$), where the minus sign refers to the subtraction defined in Definition 5.8.7 **(b)**. In other words, D_1 is the difference $A - B$ defined as in Definition 5.8.7 **(b)**.

In other words, we have $D_1 = D_2$ (since D_2 was defined to be the difference $A - B$ defined as in Definition 5.8.7 **(b)**). This is precisely what we set out to prove.

Thus, we have shown that the subtraction we defined (in Definition 6.6.5 **(b)**) for an arbitrary $\mathbb{K}$-module generalizes the subtraction of matrices (when the $\mathbb{K}$-module is $\mathbb{K}^{n\times m}$). A similar argument (but using Theorem 3.4.23 **(i)** instead of Theorem 5.8.10 **(i)**) shows that the former subtraction generalizes the subtraction in $\mathbb{Z}/n$ (when $\mathbb{K} = \mathbb{Z}$ and the $\mathbb{K}$-module is $\mathbb{Z}/n$). Thus, Remark 6.6.6 is proven. □

Theorem 5.4.6 holds for the $\mathbb{K}$-module M just as it holds for the ring $\mathbb{K}$. Thus, we have a notion of finite sums of elements of M; it behaves exactly like finite sums of elements of $\mathbb{K}$ do. But Theorem 5.4.7 has no analogue for $\mathbb{K}$-modules. (However, you can get something similar to Theorem 5.4.7 **(b)** by defining finite products of the form $\lambda_1\lambda_2\cdots\lambda_k a$ with $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}$ and $a \in M$.)

Definition 5.4.8 can be extended to modules by simply replacing $\mathbb{K}$ with M:

Definition 6.6.8. Let $a \in M$ and $n \in \mathbb{Z}$. Then, we define an element na of M by

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{a + a + \cdots + a}_{-n \text{ times}}\right), & \text{if } n < 0 \end{cases}.$$

We cannot define a^n for $a \in M$ and $n \in \mathbb{N}$.

Proposition 5.4.9 has an analogue for a $\mathbb{K}$-module; namely, we have the following:

Proposition 6.6.9. We have

$$(n+m)\,a = na + ma \qquad \text{for all } a \in M \text{ and } n, m \in \mathbb{Z}; \tag{200}$$

$$n\,(a+b) = na + nb \qquad \text{for all } a, b \in M \text{ and } n \in \mathbb{Z}; \tag{201}$$

$$-\,(na) = (-n)\,a = n\,(-a) \qquad \text{for all } a \in M \text{ and } n \in \mathbb{Z}; \tag{202}$$

$$(nm)\,a = n\,(ma) \qquad \text{for all } a \in M \text{ and } n, m \in \mathbb{Z}; \tag{203}$$

$$n\,(\lambda a) = (n\lambda)\,a = \lambda\,(na) \qquad \text{for all } a \in M \text{ and } \lambda \in \mathbb{K} \text{ and } n \in \mathbb{Z}; \tag{204}$$

$$n0_M = 0_M \qquad \text{for all } n \in \mathbb{Z}; \tag{205}$$

$$1a = a \qquad \text{for all } a \in M; \tag{206}$$

$$0a = 0_M \qquad \text{for all } a \in M; \tag{207}$$

$$(-1)\,a = -a \qquad \text{for all } a \in M. \tag{208}$$

(Here, "1" stands for the integer $1 \in \mathbb{Z}$, not for the scalar $1 \in \mathbb{K}$. Likewise, the "0" in "$0a$", and the "-1" in "$(-1)\,a$" stand for integers.) In particular, these equalities show that certain expressions (like "nma" and "$n\lambda a$") are unambiguous.

Proof of Proposition 6.6.9. This is analogous to the proof of Proposition 5.4.9. □

Upshot: All the rules relating to addition that we know from rings are still true for $\mathbb{K}$-modules. Some basic rules relating to multiplication can be salvaged (i.e., made to work for $\mathbb{K}$-modules) by replacing multiplication by scaling.

6.7. Submodules

> **Convention 6.7.1.** For the rest of Chapter 6, we fix a **commutative** ring $\mathbb{K}$, and we denote its addition, multiplication, zero and unity by $+$, $\cdot$, 0 and 1.

In Section 5.3, we have defined the notion of a subring of a ring. Similarly, we shall now define a submodule of a $\mathbb{K}$-module. For example, the $\mathbb{Z}$-modules $q\mathbb{Z}$ and $\mathbb{Q}_{\text{sqf}}$ from Example 6.4.6 will fall under this concept. The idea is the same as for subrings: A submodule of a $\mathbb{K}$-module N is a $\mathbb{K}$-module M that is a subset of N and has "the same" addition, scaling and zero vector. Here is the formal definition (analogous to Definition 5.3.1):

> **Definition 6.7.2.** Let M and N be two $\mathbb{K}$-modules. We say that M is a *$\mathbb{K}$-submodule* (or, for short, *submodule*) of N if and only if it satisfies the following four requirements:
>
> - the set M is a subset of N;
> - the addition of M is a restriction of the addition of N (that is, we have $a_1 +_M a_2 = a_1 +_N a_2$ for all $a_1, a_2 \in M$);
> - the scaling of M is a restriction of the scaling of N (that is, we have $\lambda \cdot_M a = \lambda \cdot_N a$ for all $\lambda \in \mathbb{K}$ and $a \in M$);
> - the zero vector of M is the zero vector of N (that is, we have $0_M = 0_N$).

Thus, according to this definition:

- the $\mathbb{Z}$-modules $n\mathbb{Z}$ from Example 6.4.5 **(b)** are $\mathbb{Z}$-submodules of $\mathbb{Z}$;
- the $\mathbb{Z}$-modules $q\mathbb{Z}$ and $\mathbb{Q}_{\text{sqf}}$ from Example 6.4.6 are $\mathbb{Z}$-submodules of $\mathbb{Q}$;
- every $\mathbb{K}$-module M is a $\mathbb{K}$-submodule of itself.

Again, you can find examples of two $\mathbb{K}$-modules M and N for which the set M is a **subset** of N yet the $\mathbb{K}$-module M is **not a $\mathbb{K}$-submodule** of N. For example, $\mathbb{C}$ becomes a $\mathbb{C}$-module in the usual way (with addition playing the role of addition, and multiplication playing the role of scaling); but you can also define a second "scaling" operation $\overline{\cdot} : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ by setting

$$\alpha \mathbin{\overline{\cdot}} \beta = \overline{\alpha}\beta \qquad \text{for all } \alpha, \beta \in \mathbb{C}.$$

Then, we can turn the set $\mathbb{C}$ into a $\mathbb{C}$-module by endowing it with the usual addition, the unusual scaling operation $\bar{\cdot}$ and the zero vector 0. This new $\mathbb{C}$-module may be called $\overline{\mathbb{C}}$, and is useful in studying Hermitian forms. The $\mathbb{C}$-modules $\mathbb{C}$ and $\overline{\mathbb{C}}$ are equal as sets, but neither is a $\mathbb{C}$-submodule of the other.

Definition 6.7.3. If $\mathbb{K}$ is a field, then $\mathbb{K}$-submodules are also known as $\mathbb{K}$-*vector subspaces* (or, short, $\mathbb{K}$-*subspaces*).

When we have two $\mathbb{K}$-modules M and N such that $M \subseteq N$ as sets (or, more generally, such that M and N have elements in common), we generally need to be careful using the symbol "$+$": This symbol may mean both the addition of M and the addition of N, and these additions might not be the same. Thus it is prudent to disambiguate its meaning by attaching a subscript "$_M$" or "$_N$" to it. The same applies to the symbols "$\cdot$" and "0" and expressions like "λa" (which have an implicit scaling sign). However, when M is a $\mathbb{K}$-submodule of N, we do not need to take this precaution; in this case, the meaning of expressions like "$a + b$" does not depend on whether you read "$+$" as the addition of M or as the addition of N.

The following is analogous to Proposition 5.3.4:

Proposition 6.7.4. Let N be a $\mathbb{K}$-module. Let S be a subset of N that satisfies the following three conditions:[176]

- We have $0 \in S$.
- The subset S is *closed under addition*. (This means that all $a, b \in S$ satisfy $a + b \in S$.)
- The subset S is *closed under scaling*. (This means that all $\lambda \in \mathbb{K}$ and $a \in S$ satisfy $\lambda a \in S$.)

Then, the set S itself becomes a $\mathbb{K}$-module if we endow it with:

- an addition operation $+$ which is defined as the restriction of the addition operation of the $\mathbb{K}$-module N;
- a scaling map $\cdot : \mathbb{K} \times S \to S$ which is defined as the restriction of the scaling map of the $\mathbb{K}$-module N,

and the zero vector 0. Furthermore, this $\mathbb{K}$-module S is a $\mathbb{K}$-submodule of N.

Proof of Proposition 6.7.4. Similar to the proof of Proposition 5.3.4, except that we now need to argue that each $a \in S$ satisfies $-a \in S$. (But this is easy: Since S is closed under scaling, we have $(-1) a \in S$, and thus $-a = (-1) a \in S$.) □

[176] In this proposition, the symbols "$+$", "$\cdot$" and "0" mean the addition, the scaling and the zero vector of N.

Definition 6.7.5. Let N be a $\mathbb{K}$-module. Let S be a subset of N that satisfies the three conditions of Proposition 6.7.4. Then, we shall say that "S is a $\mathbb{K}$-submodule of N". Technically speaking, this is premature, since S is so far just a subset of N without the structure of a $\mathbb{K}$-module; however, Proposition 6.7.4 shows that there is an obvious way of turning S into a $\mathbb{K}$-module (viz.: define an operation $+$ by restricting the corresponding operation of N, define a map $\cdot$ similarly, and steal the zero vector from N), and we shall automatically regard S as becoming a $\mathbb{K}$-module in this way (unless we say otherwise). We say that the addition operation $+$ on S (obtained by restricting the corresponding operation on N) and the scaling map $\cdot$ of S and the zero vector of S are *inherited from N*.

Thus, finding $\mathbb{K}$-submodules of a $\mathbb{K}$-module N boils down to finding subsets that contain its 0 and are closed under addition and under scaling; the module axioms don't need to be re-checked.

Thus, in particular, when $\mathbb{K}$ is a field, the vector subspaces of $\mathbb{K}^{n\times 1}$ (as in Definition 6.1.3) are precisely the $\mathbb{K}$-submodules of $\mathbb{K}^{n\times 1}$. Many examples of $\mathbb{K}$-submodules can thus be found in textbooks on linear algebra. If M is any $\mathbb{K}$-module, then both M and the one-element subset $\{0_M\}$ are $\mathbb{K}$-submodules of M (this is easily checked); the more interesting submodules are the ones that lie in between these two extremes.

6.8. Linear maps, aka module homomorphisms

Recall Definition 5.9.1. In a similar way, we define $\mathbb{K}$-*module homomorphisms*, also known as $\mathbb{K}$-*linear maps*:

Definition 6.8.1. Let M and N be two $\mathbb{K}$-modules. A $\mathbb{K}$-*module homomorphism* from M to N means a map $f : M \to N$ that satisfies the following three axioms:

- **(a)** We have $f(a+b) = f(a) + f(b)$ for all $a, b \in M$. (This is called "f respects addition" or "f preserves addition".)
- **(b)** We have $f(0) = 0$. (This, of course, means $f(0_M) = 0_N$.)
- **(c)** We have $f(\lambda a) = \lambda f(a)$ for all $\lambda \in \mathbb{K}$ and $a \in M$. (This is called "f respects scaling" or "f preserves scaling".)

Instead of "$\mathbb{K}$-module homomorphism", we can also say "$\mathbb{K}$-*linear map*" or just "*linear map*" (when $\mathbb{K}$ is clear).

Remark 6.8.2. The axiom **(b)** in Definition 6.8.1 is redundant – it follows from axiom **(a)**.

Proof. Same argument as for Remark 5.9.3. □

Some authors (for example, Hefferon in [Heffer17, Chapter Three, Definition II.1.1], and the authors of [LaNaSc16, Definition 6.1.1]) omit the axiom **(b)** when they define $\mathbb{K}$-linear maps. This does not change the concept, as Remark 6.8.2 shows.

What are some examples of module homomorphisms?

Example 6.8.3. Let M be a $\mathbb{K}$-module.

(a) The identity map $\operatorname{id} : M \to M$ is $\mathbb{K}$-linear.

(b) For any $\lambda \in \mathbb{K}$, the map $L_\lambda : M \to M,\ a \mapsto \lambda a$ is $\mathbb{K}$-linear.

(c) If $M = \mathbb{K}$ (specifically, the $\mathbb{K}$-module $\mathbb{K}$ defined in Example 6.4.1), then the maps L_λ (for $\lambda \in \mathbb{K}$) that we just defined are the only $\mathbb{K}$-linear maps from M to M.

Proof of Example 6.8.3. **(b)** Let $\lambda \in \mathbb{K}$. We must prove that the map $L_\lambda : M \to M,\ a \mapsto \lambda a$ is $\mathbb{K}$-linear. Thus, we must prove that it satisfies the three axioms **(a)**, **(b)** and **(c)** of Definition 6.8.1. In other words, we must prove the following:

> *Claim 1:* We have $L_\lambda(a+b) = L_\lambda(a) + L_\lambda(b)$ for all $a, b \in M$.
>
> *Claim 2:* We have $L_\lambda(0) = 0$.
>
> *Claim 3:* We have $L_\lambda(\mu a) = \mu L_\lambda(a)$ for all $\mu \in \mathbb{K}$ and $a \in M$. (Note that we are using the letter "μ" for what was called "λ" in Definition 6.8.1, since the letter "λ" is already taken.)

[*Proof of Claim 1:* Let $a, b \in M$. Then, the definition of L_λ yields $L_\lambda(a+b) = \lambda(a+b)$ and $L_\lambda(a) = \lambda a$ and $L_\lambda(b) = \lambda b$. But axiom **(e)** in Definition 6.3.1 yields $\lambda(a+b) = \lambda a + \lambda b$. Hence,

$$L_\lambda(a+b) = \lambda(a+b) = \underbrace{\lambda a}_{=L_\lambda(a)} + \underbrace{\lambda b}_{=L_\lambda(b)} = L_\lambda(a) + L_\lambda(b).$$

This proves Claim 1.]

[*Proof of Claim 2:* We leave this proof to the reader.]

[*Proof of Claim 3:* Let $\mu \in \mathbb{K}$ and $a \in M$. Now, axiom **(h)** in Definition 6.3.1 yields $(\lambda\mu)a = \lambda(\mu a)$. The same argument (with the roles of λ and μ swapped) yields $(\mu\lambda)a = \mu(\lambda a)$. But $\mathbb{K}$ is commutative; thus, $\lambda\mu = \mu\lambda$. Now, the definition of L_λ yields $L_\lambda(a) = \lambda a$. Furthermore, the definition of L_λ yields

$$L_\lambda(\mu a) = \lambda(\mu a) = \underbrace{(\lambda\mu)}_{=\mu\lambda} a = (\mu\lambda)a = \mu \underbrace{(\lambda a)}_{=L_\lambda(a)} = \mu L_\lambda(a).$$

This proves Claim 3.]

Thus, all three Claims 1, 2 and 3 have been proven. Hence, the map $L_\lambda : M \to M,\ a \mapsto \lambda a$ is $\mathbb{K}$-linear; this completes the proof of Example 6.8.3 **(b)**.

(a) In Example 6.8.3 **(b)**, we have defined a map $L_\lambda : M \to M,\ a \mapsto \lambda a$ for each $\lambda \in \mathbb{K}$. Applying this to $\lambda = 1$, we obtain a map $L_1 : M \to M,\ a \mapsto 1a$. This map

$L_1 : M \to M$ is $\mathbb{K}$-linear (by Example 6.8.3 **(b)**, applied to $\lambda = 1$). But each $a \in M$ satisfies

$$\begin{aligned} L_1(a) &= 1a && \text{(by the definition of } L_1\text{)} \\ &= a && \text{(by axiom } \textbf{(i)} \text{ in Definition 6.3.1)} \\ &= \operatorname{id}(a). \end{aligned}$$

In other words, $L_1 = \operatorname{id}$. Hence, the map $\operatorname{id} : M \to M$ is $\mathbb{K}$-linear (since the map $L_1 : M \to M$ is $\mathbb{K}$-linear). This proves Example 6.8.3 **(a)**.

(c) Assume that $M = \mathbb{K}$ (specifically, the $\mathbb{K}$-module $\mathbb{K}$ defined in Example 6.4.1). We must prove that the maps L_λ (for $\lambda \in \mathbb{K}$) that we just defined are the only $\mathbb{K}$-linear maps from M to M. We already have shown that these maps L_λ are $\mathbb{K}$-linear (see Example 6.8.3 **(b)**); thus, it remains to prove that there are no other $\mathbb{K}$-linear maps from M to M. In other words, it remains to prove that if f is a $\mathbb{K}$-linear map from M to M, then $f = L_\lambda$ for some $\lambda \in \mathbb{K}$.

So let f be a $\mathbb{K}$-linear map from M to M. Set $\rho = f(1)$. Then, $\rho \in M = \mathbb{K}$. Thus, a map $L_\rho : M \to M$ is well-defined.

Recall that our $\mathbb{K}$-module M is $\mathbb{K}$ itself, and its scaling map is exactly the multiplication operation of $\mathbb{K}$.

Now, let $a \in M$. Then, $a \in M = \mathbb{K}$, so that $a = a \cdot 1$ (by the "Neutrality of one" axiom in the ring $\mathbb{K}$). Hence,

$$\begin{aligned} f(a) = f(a \cdot 1) = a \cdot \underbrace{f(1)}_{=\rho} \qquad & \left(\begin{array}{c}\text{by the axiom } \textbf{(c)} \text{ in Definition 6.8.1,} \\ \text{applied to } a \text{ and } 1 \text{ instead of } \lambda \text{ and } a\end{array}\right) \\ = a \cdot \rho = \rho \cdot a \qquad & \\ \left(\begin{array}{c}\text{since both } a \text{ and } \rho \text{ are elements of } \mathbb{K}\text{, and since } \mathbb{K} \text{ is commutative} \\ \text{(and since the scaling map of } M \text{ is the multiplication operation of } \mathbb{K}\text{)}\end{array}\right) & \\ = L_\rho(a) \qquad & \end{aligned}$$

(since the definition of L_ρ yields $L_\rho(a) = \rho \cdot a$).

Now, forget that we fixed a. We thus have proven that $f(a) = L_\rho(a)$ for each $a \in M$. In other words, $f = L_\rho$. Hence, $f = L_\lambda$ for some $\lambda \in \mathbb{K}$ (namely, for $\lambda = \rho$). As we said, this proves Example 6.8.3 **(c)**. □

Next comes a less basic example:

Theorem 6.8.4. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be an $n \times m$-matrix. Define a map

$$\begin{aligned} L_A : \mathbb{K}^{m \times 1} &\to \mathbb{K}^{n \times 1}, \\ v &\mapsto Av. \end{aligned}$$

This map L_A is a $\mathbb{K}$-module homomorphism from $\mathbb{K}^{m \times 1}$ to $\mathbb{K}^{n \times 1}$.

Proof of Theorem 6.8.4. We just need to check that the three axioms **(a)**, **(b)** and **(c)** in Definition 6.8.1 are satisfied for $M = \mathbb{K}^{m\times 1}$, $N = \mathbb{K}^{n\times 1}$ and $f = L_A$.

*Proof of axiom **(a)**:* We must prove that $L_A(a+b) = L_A(a) + L_A(b)$ for all $a, b \in \mathbb{K}^{m\times 1}$. Indeed: If $a, b \in \mathbb{K}^{m\times 1}$, then we can compare the equalities

$$\begin{aligned} L_A(a+b) &= A(a+b) && \text{(by the definition of } L_A\text{)} \\ &= Aa + Ab && \text{(by Theorem 5.8.10 \textbf{(g)})} \end{aligned}$$

and

$$\underbrace{L_A(a)}_{\substack{=Aa \\ \text{(by the definition of } L_A\text{)}}} + \underbrace{L_A(b)}_{\substack{=Ab \\ \text{(by the definition of } L_A\text{)}}} = Aa + Ab,$$

and thus obtain $L_A(a+b) = L_A(a) + L_A(b)$. Thus, axiom **(a)** has been verified.

The axioms **(b)** and **(c)** are proven similarly (details are left to the reader). □

Proposition 6.8.5. Let $n, m \in \mathbb{N}$. Each $\mathbb{K}$-module homomorphism from $\mathbb{K}^{m\times 1}$ to $\mathbb{K}^{n\times 1}$ has the form L_A for a unique $A \in \mathbb{K}^{n\times m}$ (where L_A is defined as in Theorem 6.8.4).

We shall delay the proof of this proposition until we have shown some auxiliary results. First, we define a specific kind of column vectors:

Definition 6.8.6. Let $m \in \mathbb{N}$. For each $j \in \{1, 2, \ldots, m\}$, we let $e_j \in \mathbb{K}^{m\times 1}$ be the column vector

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = (0, 0, \ldots, 0, 1, 0, 0, \ldots, 0)^T$$

where the 1 is at the j-th position. (Strictly speaking, we should denote it by $e_{j,m}$ rather than e_j, since it depends on m and not just on j; but the m will always be clear from the context.)

These column vectors $e_1, e_2, \ldots, e_m$ are called the *standard basis vectors* of $\mathbb{K}^{m\times 1}$.

For example, if $m = 3$, then $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and $e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

Lemma 6.8.7. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be an $n \times m$-matrix.

(a) We have $Ae_j = (\text{the } j\text{-th column of } A)$ for all $j \in \{1, 2, \ldots, m\}$.

(b) Consider the map L_A defined in Theorem 6.8.4. Then,

$$L_A\left(e_j\right) = (\text{the } j\text{-th column of } A) \qquad \text{for all } j \in \{1, 2, \ldots, m\}.$$

Proof of Lemma 6.8.7. **(a)** Let $j \in \{1, 2, \ldots, m\}$. Then, Ae_j is a column vector in $\mathbb{K}^{n \times 1}$. For each $i \in \{1, 2, \ldots, n\}$, we have

$$\begin{aligned}
&\left(\text{the } i\text{-th entry of the column vector } Ae_j\right) \\
&= \left(\text{the } (i,1)\text{-th entry of the matrix } Ae_j\right) \\
&= \sum_{k=1}^{m} (\text{the } (i,k)\text{-th entry of } A) \cdot \underbrace{\left(\text{the } (k,1)\text{-th entry of } e_j\right)}_{\substack{= \begin{cases} 1, & \text{if } k = j; \\ 0, & \text{if } k \neq j \end{cases} \\ \text{(by the definition of } e_j\text{)}}} \\
&\qquad \text{(by the definition of multiplication of matrices)} \\
&= \sum_{k=1}^{m} (\text{the } (i,k)\text{-th entry of } A) \cdot \begin{cases} 1, & \text{if } k = j; \\ 0, & \text{if } k \neq j \end{cases} \\
&= (\text{the } (i,j)\text{-th entry of } A) \cdot \underbrace{\begin{cases} 1, & \text{if } j = j; \\ 0, & \text{if } j \neq j \end{cases}}_{\substack{=1 \\ \text{(since } j=j\text{)}}} \\
&\qquad + \sum_{\substack{k \in \{1,2,\ldots,m\}; \\ k \neq j}} (\text{the } (i,k)\text{-th entry of } A) \cdot \underbrace{\begin{cases} 1, & \text{if } k = j; \\ 0, & \text{if } k \neq j \end{cases}}_{\substack{=0 \\ \text{(since } k \neq j\text{)}}} \\
&\qquad \text{(here, we have split off the addend for } k = j \text{ from the sum)} \\
&= (\text{the } (i,j)\text{-th entry of } A) + \underbrace{\sum_{\substack{k \in \{1,2,\ldots,m\}; \\ k \neq j}} (\text{the } (i,k)\text{-th entry of } A) \cdot 0}_{=0} \\
&= (\text{the } (i,j)\text{-th entry of } A) = (\text{the } i\text{-th entry of the } j\text{-th column of } A).
\end{aligned}$$

Hence, $Ae_j = (\text{the } j\text{-th column of } A)$. This proves Lemma 6.8.7 **(a)**.

(b) Let $j \in \{1, 2, \ldots, m\}$. The definition of L_A yields

$$L_A\left(e_j\right) = Ae_j = (\text{the } j\text{-th column of } A)$$

(by Lemma 6.8.7 **(a)**). This proves Lemma 6.8.7 **(b)**. □

Proposition 6.8.8. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a $\mathbb{K}$-linear map.

(a) We have $f(\lambda a + \mu b) = \lambda f(a) + \mu f(b)$ for all $\lambda, \mu \in \mathbb{K}$ and $a, b \in M$.

(b) Let $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}$ and $a_1, a_2, \ldots, a_k \in M$. Then,

$$f\left(\sum_{i=1}^{k} \lambda_i a_i\right) = \sum_{i=1}^{k} \lambda_i f(a_i).$$

(In words: f "preserves linear combinations".)

Proof of Proposition 6.8.8. The map f is $\mathbb{K}$-linear, and thus satisfies the axioms **(a)**, **(b)** and **(c)** of Definition 6.8.1. We shall use these axioms in the following.

(a) Let $\lambda, \mu \in \mathbb{K}$ and $a, b \in M$. Then,

$$\begin{aligned} f(\lambda a + \mu b) &= \underbrace{f(\lambda a)}_{\substack{=\lambda f(a) \\ \text{(by axiom (c))}}} + \underbrace{f(\mu b)}_{\substack{=\mu f(b) \\ \text{(by axiom (c))}}} \qquad \text{(by axiom (a))} \\ &= \lambda f(a) + \mu f(b). \end{aligned}$$

This proves Proposition 6.8.8 **(a)**.

(b) This is proven by induction on k. The induction base (i.e., the case $k = 0$) follows from axiom **(b)**; the induction step uses Proposition 6.8.8 **(a)** (or axioms **(a)** and **(c)**, if you wish). Details are left to the reader. □

Proposition 6.8.8 **(a)** has a converse:

Proposition 6.8.9. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a map. Assume that

$$f(\lambda a + \mu b) = \lambda f(a) + \mu f(b) \qquad \text{for all } \lambda, \mu \in \mathbb{K} \text{ and } a, b \in M. \tag{209}$$

Then, f is $\mathbb{K}$-linear.

Proof of Proposition 6.8.9. We must prove that the three axioms **(a)**, **(b)** and **(c)** of Definition 6.8.1 are satisfied.

*Proof of axiom **(a)**:* Let $a, b \in M$. Then, (209) (applied to $\lambda = 1$ and $\mu = 1$) yields $f(1a + 1b) = 1f(a) + 1f(b)$. This quickly simplifies to $f(a + b) = f(a) + f(b)$. Thus, axiom **(a)** has been verified.

*Proof of axiom **(b)**:* Applying (209) to $\lambda = 0$, $\mu = 0$, $a = 0_M$ and $b = 0_M$, we obtain $f(0 \cdot 0_M + 0 \cdot 0_M) = \underbrace{0f(0_M)}_{=0_N} + \underbrace{0f(0_M)}_{=0_N} = 0_N$. In view of $0 \cdot 0_M + 0 \cdot 0_M = 0_M$, we can rewrite this as $f(0_M) = 0_N$. Thus, axiom **(b)** has been verified.

*Proof of axiom **(c)**:* Let $\lambda \in \mathbb{K}$ and $a \in M$. Applying (209) to $\mu = 0$ and $b = 0_M$, we obtain $f(\lambda a + 0 \cdot 0_M) = \lambda f(a) + \underbrace{0f(0_M)}_{=0_N} = \lambda f(a)$. In view of $\lambda a + \underbrace{0 \cdot 0_M}_{=0_M} = \lambda a + 0_M = \lambda a$, this rewrites as $f(\lambda a) = \lambda f(a)$. Thus, axiom **(c)** has been verified. □

Some authors use the axiom (209) as their definition of what it means for a map $f : M \to N$ between two $\mathbb{K}$-modules M and N to be $\mathbb{K}$-linear. This definition is equivalent to ours (due to Proposition 6.8.9 and Proposition 6.8.8 **(a)**).

Lemma 6.8.10. Let $m \in \mathbb{N}$, and let N be a $\mathbb{K}$-module. For each $j \in \{1, 2, \ldots, m\}$, we let define a column vector $e_j \in \mathbb{K}^{m\times 1}$ as in Definition 6.8.6.

Let $f, g : \mathbb{K}^{m\times 1} \to N$ be two $\mathbb{K}$-linear maps. Assume that $f\left(e_j\right) = g\left(e_j\right)$ for all $j \in \{1, 2, \ldots, m\}$. Then, $f = g$.

Proof of Lemma 6.8.10. Let $v \in \mathbb{K}^{m\times 1}$. Write v as $(v_1, v_2, \ldots, v_m)^T$, where $v_1, v_2, \ldots, v_m \in \mathbb{K}$. Then,

$$\begin{aligned} v &= (v_1, v_2, \ldots, v_m)^T \\ &= \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ \vdots \\ v_m \end{pmatrix} = \underbrace{\begin{pmatrix} v_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{=v_1e_1} + \underbrace{\begin{pmatrix} 0 \\ v_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{=v_2e_2} + \underbrace{\begin{pmatrix} 0 \\ 0 \\ v_3 \\ \vdots \\ 0 \end{pmatrix}}_{=v_3e_3} + \cdots + \underbrace{\begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ v_m \end{pmatrix}}_{=v_me_m} \\ &\qquad \text{(since matrices are added entrywise)} \\ &= v_1e_1 + v_2e_2 + v_3e_3 + \cdots + v_me_m = \sum_{i=1}^{m} v_ie_i. \end{aligned}$$

Hence,

$$\begin{aligned} f(v) &= f\left(\sum_{i=1}^{m} v_ie_i\right) = \sum_{i=1}^{m} v_i f(e_i) \qquad \text{(by Proposition 6.8.8 } \textbf{(b)}\text{)} \\ &= \sum_{j=1}^{m} v_j f\left(e_j\right) \qquad \text{(here, we have renamed the summation index } i \text{ as } j\text{)} \end{aligned}$$

and similarly $g(v) = \sum\limits_{j=1}^{m} v_j g\left(e_j\right)$. Now, the right hand sides of these two equalities are equal, since we assumed that $f\left(e_j\right) = g\left(e_j\right)$ for all $j \in \{1, 2, \ldots, m\}$. Hence, the left hand sides are equal, too. In other words, $f(v) = g(v)$. Since we have proven this for every $v \in \mathbb{K}^{m\times 1}$, we thus conclude that $f = g$. This proves Lemma 6.8.10. □

We are now ready to prove Proposition 6.8.5:

Proof of Proposition 6.8.5. Let f be a $\mathbb{K}$-module homomorphism from $\mathbb{K}^{m\times 1}$ to $\mathbb{K}^{n\times 1}$. We must prove that $f = L_A$ for a unique $A \in \mathbb{K}^{n\times m}$.

For each $j \in \{1, 2, \ldots, m\}$, we let define a column vector $e_j \in \mathbb{K}^{m\times 1}$ as in Definition 6.8.6.

Now, let F be the $n \times m$-matrix whose columns are the m column vectors $f\left(e_1\right), f\left(e_2\right), \ldots, f\left(e_m\right)$. We claim that $f = L_F$.

Indeed, both f and L_F are $\mathbb{K}$-module homomorphisms from $\mathbb{K}^{m\times 1}$ to $\mathbb{K}^{n\times 1}$. That is, they are $\mathbb{K}$-linear maps from $\mathbb{K}^{m\times 1}$ to $\mathbb{K}^{n\times 1}$. Furthermore, for each $j \in \{1,2,\ldots,m\}$, we have

$$\begin{aligned} f\left(e_j\right) &= \left(\text{the } j\text{-th column of } F\right) && \left(\text{by the definition of } F\right) \\ &= L_F\left(e_j\right) && \left(\begin{array}{c}\text{since Lemma 6.8.7 \textbf{(b)} (applied to } A = F\text{)} \\ \text{yields } L_F\left(e_j\right) = \left(\text{the } j\text{-th column of } F\right)\end{array}\right). \end{aligned}$$

Hence, Lemma 6.8.10 (applied to $N = \mathbb{K}^{n\times 1}$ and $g = L_F$) shows that $f = L_F$. This shows that $f = L_A$ for **some** $A \in \mathbb{K}^{n\times m}$ (namely, for $A = F$).

How to prove that this A is unique? The idea is that A can be reconstructed from L_A, because $\left(\text{the } j\text{-th column of } A\right) = L_A\left(e_j\right)$ for each $j \in \{1,2,\ldots,m\}$ (by Lemma 6.8.7 **(b)**). □

Definition 6.8.11. Let M and N be two $\mathbb{K}$-modules.

(a) Let $\operatorname{Hom}(M,N)$ be the set of all $\mathbb{K}$-module homomorphisms (= linear maps) from M to N. We shall now turn this set into a $\mathbb{K}$-module.

(b) We define an addition $+$ on $\operatorname{Hom}(M,N)$ as follows: If $f,g \in \operatorname{Hom}(M,N)$, then $f+g \in \operatorname{Hom}(M,N)$ is defined by

$$(f+g)(v) = f(v) + g(v) \qquad \text{for all } v \in M.$$

(That is, the addition is pointwise. This is well-defined by Proposition 6.8.12 **(a)** below.)

(c) We define a scaling $\cdot$ on $\operatorname{Hom}(M,N)$ as follows: If $\lambda \in \mathbb{K}$ and $f \in \operatorname{Hom}(M,N)$, then $\lambda f \in \operatorname{Hom}(M,N)$ is defined by

$$(\lambda f)(v) = \lambda \cdot f(v) \qquad \text{for all } v \in M.$$

(That is, the scaling is pointwise. This is well-defined by Proposition 6.8.12 **(b)** below.)

(d) We define a map $0_{M\to N} : M \to N$ by setting

$$0_{M\to N}(v) = 0 \qquad \text{for all } v \in M.$$

(e) We equip $\operatorname{Hom}(M,N)$ with the addition $+$, the scaling $\cdot$ and the zero vector $0_{M\to N}$ we have just defined. This yields a $\mathbb{K}$-module (by Proposition 6.8.12 **(d)** below).

Proposition 6.8.12. **(a)** The addition $+$ defined in Definition 6.8.11 **(b)** is well-defined (i.e., we have $f+g \in \operatorname{Hom}(M,N)$ for all $f,g \in \operatorname{Hom}(M,N)$).

(b) The scaling $\cdot$ defined in Definition 6.8.11 **(c)** is well-defined (i.e., we have $\lambda f \in \operatorname{Hom}(M,N)$ for all $\lambda \in \mathbb{K}$ and $f \in \operatorname{Hom}(M,N)$).

(c) The map $0_{M \to N}$ defined in Definition 6.8.11 **(d)** belongs to $\operatorname{Hom}(M, N)$.

(d) The set $\operatorname{Hom}(M, N)$, equipped with the addition $+$, the scaling $\cdot$ and the zero vector $0_{M \to N}$, is a $\mathbb{K}$-module.

Proof of Proposition 6.8.12. **(a)** Let $f, g \in \operatorname{Hom}(M, N)$. We must prove that $f + g \in \operatorname{Hom}(M, N)$. In other words, we must prove that $f + g$ is a $\mathbb{K}$-module homomorphism from M to N (by the definition of $\operatorname{Hom}(M, N)$). In other words, we must prove that the map $f + g$ is $\mathbb{K}$-linear (because a $\mathbb{K}$-module homomorphism is the same as a $\mathbb{K}$-linear map).

We know two ways of proving that a given map (between two $\mathbb{K}$-modules) is $\mathbb{K}$-linear: One way is by checking the three axioms in Definition 6.8.1; the other is through Proposition 6.8.9. Of course, these two ways boil down to the same thing, but the second one tends to give a shorter proof. So let us go with the second one.

Fix $\lambda, \mu \in \mathbb{K}$ and $a, b \in M$. We shall prove that $(f + g)(\lambda a + \mu b) = \lambda (f + g)(a) + \mu (f + g)(b)$.

We have $f \in \operatorname{Hom}(M, N)$. In other words, f is a $\mathbb{K}$-module homomorphism from M to N (by the definition of $\operatorname{Hom}(M, N)$). In other words, the map $f : M \to N$ is $\mathbb{K}$-linear. Thus, Proposition 6.8.8 **(a)** yields $f(\lambda a + \mu b) = \lambda f(a) + \mu f(b)$. The same argument (applied to g instead of f) yields $g(\lambda a + \mu b) = \lambda g(a) + \mu g(b)$. Now, the definition of $f + g$ yields $(f + g)(a) = f(a) + g(a)$ and $(f + g)(b) = f(b) + g(b)$ and $(f + g)(\lambda a + \mu b) = f(\lambda a + \mu b) + g(\lambda a + \mu b)$. Hence,

$$\begin{aligned}(f+g)(\lambda a+\mu b) &= \underbrace{f(\lambda a+\mu b)}_{=\lambda f(a)+\mu f(b)} + \underbrace{g(\lambda a+\mu b)}_{=\lambda g(a)+\mu g(b)} \\ &= \lambda f(a) + \underbrace{\mu f(b) + \lambda g(a)}_{\substack{=\lambda g(a)+\mu f(b) \\ \text{(by axiom (a) in} \\ \text{Definition 6.3.1)}}} + \mu g(b) \\ &= \lambda f(a) + \lambda g(a) + \mu f(b) + \mu g(b).\end{aligned}$$

Comparing this with

$$\begin{aligned}\lambda \underbrace{(f+g)(a)}_{=f(a)+g(a)} + \mu \underbrace{(f+g)(b)}_{=f(b)+g(b)} &= \underbrace{\lambda(f(a)+g(a))}_{\substack{=\lambda f(a)+\lambda g(a) \\ \text{(by axiom (e) in} \\ \text{Definition 6.3.1)}}} + \underbrace{\mu(f(b)+g(b))}_{\substack{=\mu f(b)+\mu g(b) \\ \text{(by axiom (e) in} \\ \text{Definition 6.3.1)}}} \\ &= \lambda f(a) + \lambda g(a) + \mu f(b) + \mu g(b),\end{aligned}$$

we obtain $(f + g)(\lambda a + \mu b) = \lambda (f + g)(a) + \mu (f + g)(b)$.

Now, forget that we fixed λ, μ and a, b. We thus have shown that

$$(f+g)(\lambda a+\mu b) = \lambda (f+g)(a) + \mu (f+g)(b) \qquad \text{for all } \lambda, \mu \in \mathbb{K} \text{ and } a, b \in M.$$

Hence, Proposition 6.8.9 (applied to $f + g$ instead of f) shows that $f + g$ is $\mathbb{K}$-linear. As we know, this completes the proof of Proposition 6.8.12 **(a)**.

(b) The proof of Proposition 6.8.12 **(b)** is analogous to the above proof of Proposition 6.8.12 **(a)**. The details are left to the reader. (For notational reasons, I recommend renaming the variable λ as ν in the statement "$\lambda f \in \operatorname{Hom}(M,N)$ for all $\lambda \in \mathbb{K}$ and $f \in \operatorname{Hom}(M,N)$", since otherwise the letter "λ" would stand for two different things.)

(c) The proof of Proposition 6.8.12 **(c)** is analogous to the above proof of Proposition 6.8.12 **(a)**. Again, the reader can easily fill in the details.

(d) This proof is a series of straightforward verifications: We have to prove that $\operatorname{Hom}(M,N)$ satisfies all the ten module axioms from Definition 6.3.1 (with M replaced by $\operatorname{Hom}(M,N)$). I will only show the proof of axiom **(e)**:

[*Proof of axiom **(e)**:* Let $\lambda \in \mathbb{K}$ and $a,b \in \operatorname{Hom}(M,N)$. We need to prove that $\lambda(a+b) = \lambda a + \lambda b$.

Fix $v \in M$. Then, the definition of the map $a+b$ yields $(a+b)(v) = a(v) + b(v)$. Likewise, the definition of the map $\lambda a + \lambda b$ yields

$$(\lambda a + \lambda b)(v) = \underbrace{(\lambda a)(v)}_{\substack{=\lambda \cdot a(v) \\ \text{(by the definition} \\ \text{of the map } \lambda a)}} + \underbrace{(\lambda b)(v)}_{\substack{=\lambda \cdot b(v) \\ \text{(by the definition} \\ \text{of the map } \lambda b)}} = \lambda \cdot a(v) + \lambda \cdot b(v).$$

But the definition of the map $\lambda(a+b)$ yields

$$(\lambda(a+b))(v) = \lambda \cdot \underbrace{(a+b)(v)}_{=a(v)+b(v)} = \lambda \cdot (a(v) + b(v)) = \lambda \cdot a(v) + \lambda \cdot b(v)$$

(because N is a $\mathbb{K}$-module, and thus satisfies the ten module axioms, in particular axiom **(e)**). Comparing these two equalities, we obtain $(\lambda(a+b))(v) = (\lambda a + \lambda b)(v)$.

Now, forget that we fixed v. We thus have proven that $(\lambda(a+b))(v) = (\lambda a + \lambda b)(v)$ for each $v \in M$. In other words, we have $\lambda(a+b) = \lambda a + \lambda b$. Thus, axiom **(e)** (with M replaced by $\operatorname{Hom}(M,N)$) is proven.]

The remaining nine module axioms can be proven similarly (and the reader will have no trouble doing so). Thus, Proposition 6.8.12 **(d)** follows. □

Proposition 6.8.13. Let M, N and P be three $\mathbb{K}$-modules. Let $f : M \to N$ and $g : N \to P$ be two $\mathbb{K}$-module homomorphisms. Then, the composition $g \circ f : M \to P$ is also a $\mathbb{K}$-module homomorphism.

Proof of Proposition 6.8.13. This is straightforward (and very similar to the proof of Proposition 5.9.15). We leave the details to the reader. □

Note the analogy between Proposition 6.8.13 and Proposition 5.9.15.

We shall follow PEMDAS-style conventions when writing expressions involving addition and composition of $\mathbb{K}$-linear maps (where we treat composition as a multiplication-like operation). For example, the expression "$f \circ h + g \circ h$" (where f, g, h are three $\mathbb{K}$-linear maps) is to be understood as $(f \circ h) + (g \circ h)$.

The following rules hold for addition, multiplication and scaling of module homomorphisms (similarly to Theorem 5.8.10):

Theorem 6.8.14. Let N, M, P, Q be $\mathbb{K}$-modules.

(a) We have $f + g = g + f$ for any $f, g \in \operatorname{Hom}(M, N)$.

(b) We have $f + (g + h) = (f + g) + h$ for any $f, g, h \in \operatorname{Hom}(M, N)$.

(c) We have $f + 0_{M \to N} = 0_{M \to N} + f = f$ for any $f \in \operatorname{Hom}(M, N)$.

(d) We have $f \circ \operatorname{id}_M = \operatorname{id}_N \circ f = f$ for any $f \in \operatorname{Hom}(M, N)$.

(e) In general, we **do not** have $f \circ g = g \circ f$. In fact, it can happen that one of $f \circ g$ and $g \circ f$ is defined and the other is not; but even if both are defined, they can be distinct.

(f) We have $f \circ (g \circ h) = (f \circ g) \circ h$ for any $f \in \operatorname{Hom}(P, Q)$, $g \in \operatorname{Hom}(N, P)$ and $h \in \operatorname{Hom}(M, N)$.

(g) We have $f \circ (g + h) = f \circ g + f \circ h$ for any $f \in \operatorname{Hom}(N, P)$ and $g, h \in \operatorname{Hom}(M, N)$.

We have $(f + g) \circ h = f \circ h + g \circ h$ for any $f, g \in \operatorname{Hom}(N, P)$ and $h \in \operatorname{Hom}(M, N)$.

(h) We have $f \circ 0_{P \to M} = 0_{P \to N}$ and $0_{N \to P} \circ f = 0_{M \to P}$ for any $f \in \operatorname{Hom}(M, N)$.

(j) We have $r(f + g) = rf + rg$ for any $r \in \mathbb{K}$ and $f, g \in \operatorname{Hom}(M, N)$.

(k) We have $(r + s) f = rf + sf$ for any $r, s \in \mathbb{K}$ and $f \in \operatorname{Hom}(M, N)$.

(l) We have $r(sf) = (rs) f$ for any $r, s \in \mathbb{K}$ and $f \in \operatorname{Hom}(M, N)$.

(m) We have $r(f \circ g) = (rf) \circ g = f \circ (rg)$ for any $r \in \mathbb{K}$ and $f \in \operatorname{Hom}(N, P)$ and $g \in \operatorname{Hom}(M, N)$.

(o) We have $1f = f$ for any $f \in \operatorname{Hom}(M, N)$.

(The above list is skipping a few letters since we have not defined subtraction yet; nevertheless, subtraction exists and satisfies the appropriate rules. See below for the details.)

Proof of Theorem 6.8.14. Most of these claims are trivial and hold not just for $\mathbb{K}$-linear maps, but for arbitrary maps. Only the first part of **(g)**, the first part of **(h)**, and the second equality sign in **(m)** do not hold for arbitrary maps. So let us prove the first part of **(g)** (and leave the rest to the reader):

Let $f \in \operatorname{Hom}(N, P)$ and $g, h \in \operatorname{Hom}(M, N)$. We must prove that

$$f \circ (g + h) = f \circ g + f \circ h.$$

So let $v \in M$. The map $f : N \to P$ is $\mathbb{K}$-linear (because $f \in \operatorname{Hom}(N, P)$). The definition of $g + h$ yields $(g + h)(v) = g(v) + h(v)$. Now, comparing

$$\begin{aligned}(f \circ (g + h))(v) &= f\left(\underbrace{(g + h)(v)}_{= g(v) + h(v)}\right) = f(g(v) + h(v)) \\ &= f(g(v)) + f(h(v)) \qquad \text{(since } f \text{ is } \mathbb{K}\text{-linear)}\end{aligned}$$

with

$$(f \circ g + f \circ h)(v) = \underbrace{(f \circ g)(v)}_{=f(g(v))} + \underbrace{(f \circ h)(v)}_{=f(h(v))} = f(g(v)) + f(h(v)),$$

we obtain $(f \circ (g+h))(v) = (f \circ g + f \circ h)(v)$. Since we have proven this for **all** $v \in M$, we thus conclude that $f \circ (g+h) = f \circ g + f \circ h$. This finishes the proof of the first half of **(g)**.

The rest is equally straightforward. □

So far, we have not defined a subtraction operation $-$ on $\operatorname{Hom}(M,N)$ (where M and N are two $\mathbb{K}$-modules). But this does not mean that such an operation does not exist; we simply don't want to waste our time defining it "manually" when we can trivially obtain it from general principles. Namely: We know that $\operatorname{Hom}(M,N)$ is a $\mathbb{K}$-module, but Definition 6.6.5 shows that every $\mathbb{K}$-module automatically has a subtraction operation. Thus, we get a subtraction operation on $\operatorname{Hom}(M,N)$ for free. This subtraction is precisely the pointwise subtraction: i.e., it is given by

$$(f-g)(v) = f(v) - g(v) \qquad \text{for all } f,g \in \operatorname{Hom}(M,N) \text{ and } v \in M \tag{210}$$

[177].

Proposition 6.6.7 shows that the subtraction operation on $\operatorname{Hom}(M,N)$ (for arbitrary $\mathbb{K}$-modules M and N) has almost all the properties that one would expect. The only rule that we do not automatically obtain from these general principles is

$$-(f \circ g) = (-f) \circ g = f \circ (-g) \qquad \text{for all } f \in \operatorname{Hom}(N,P) \text{ and } g \in \operatorname{Hom}(M,P)$$

(where M, N and P are three $\mathbb{K}$-modules). But this rule is easily verified by direct comparison (using (210)).

Corollary 6.8.15. Let M be a $\mathbb{K}$-module. The set $\operatorname{Hom}(M,M)$ of all $\mathbb{K}$-linear maps from M to M (endowed with the addition $+$, the multiplication $\circ$, the zero $0_{M\to M}$ and the unity id_M) is a ring. This ring is called the *endomorphism ring* of M, and is denoted by $\operatorname{End} M$; its elements (i.e., the $\mathbb{K}$-linear maps $M \to M$) are called the *endomorphisms* of M.

So the multiplication of the ring $\operatorname{End} M$ is composition of maps. This ring $\operatorname{End} M$ is, in general, not commutative.

Note that $\operatorname{End} M = \operatorname{Hom}(M,M)$ as sets, and the additions of $\operatorname{End} M$ and of $\operatorname{Hom}(M,M)$ are the same. But $\operatorname{End} M$ is a ring (thus has no scaling), whereas $\operatorname{Hom}(M,M)$ is a $\mathbb{K}$-module (thus has no multiplication).

[177] *Proof of (210):* Let $f,g \in \operatorname{Hom}(M,N)$ and $v \in M$. Then, $f-g$ has the property that $f = (f-g)+g$ (by Proposition 6.6.7 **(a)**). Applying both sides of this equality to v, we obtain

$$f(v) = ((f-g)+g)(v) = (f-g)(v) + g(v) \qquad \text{(by the definition of } (f-g)+g\text{)};$$

but this yields $(f-g)(v) = f(v) - g(v)$. This proves (210).

6.9. $\mathbb{K}$-algebras

There is a notion which combines both the structure of a ring and the structure of a $\mathbb{K}$-module (so it has both multiplication and scaling); this is the notion of a $\mathbb{K}$-*algebra*. It is defined as follows:

> **Definition 6.9.1.** A $\mathbb{K}$-*algebra* is a set M endowed with two binary operations $+$ and $\cdot$ as well as a scaling map $\cdot : \mathbb{K} \times M \to M$ (not to be confused with the multiplication map, which is also denoted by $\cdot$) and two elements $0, 1 \in M$ that satisfy all the ring axioms (with $\mathbb{K}$ replaced by M) as well as all the module axioms (where the zero vector 0_M is taken to be the element $0 \in M$) and also the following axiom:
>
> - **Scale-invariance of multiplication:** We have $\lambda (ab) = (\lambda a) \cdot b = a \cdot (\lambda b)$ for all $\lambda \in \mathbb{K}$ and $a, b \in M$. Here, as usual, we omit the "$\cdot$" sign both for the multiplication operation $\cdot$ (that is, we write "uv" for "$u \cdot v$" when $u, v \in M$) and for the scaling map $\cdot$ (that is, we write "λu" for "$\lambda \cdot u$" when $\lambda \in \mathbb{K}$ and $u \in M$).

It seems somewhat confusing that both the multiplication map $M \times M \to M$ and the scaling map $\mathbb{K} \times M \to M$ are denoted by the same symbol $\cdot$; but in practice, this does not cause any trouble, since it is (almost) always clear from the context which one is being applied (just check if the first argument belongs to M or to $\mathbb{K}$).

So, roughly speaking, a $\mathbb{K}$-*algebra* is a $\mathbb{K}$-module that is also a ring, with the same addition and 0 and satisfying the "Scale-invariance of multiplication" axiom. In other words, you get the definition of a $\mathbb{K}$-algebra by throwing the definitions of a ring and of a $\mathbb{K}$-module together, requiring the two additions $+$ to be the same map, requiring the zero of the ring to coincide with the zero vector of the $\mathbb{K}$-module, and requiring the multiplication to be "nice to the scaling" (in the sense that the "Scale-invariance of multiplication" axiom holds).

Examples of $\mathbb{K}$-algebras include the following:

- The commutative ring $\mathbb{K}$ itself is a $\mathbb{K}$-algebra (with both multiplication and scaling being the usual multiplication $\cdot$ of $\mathbb{K}$).
- If M is any $\mathbb{K}$-module, then the endomorphism ring $\operatorname{End} M$ becomes a $\mathbb{K}$-algebra. (Its multiplication is composition of maps, whereas its scaling is the scaling on $\operatorname{Hom}(M, M)$.)
- The matrix ring $\mathbb{K}^{n \times n}$ is a $\mathbb{K}$-algebra for any $n \in \mathbb{N}$.
- The ring $\mathbb{C}$ is an $\mathbb{R}$-algebra.
- The ring $\mathbb{R}$ is a $\mathbb{Q}$-algebra.

- More generally: If a commutative ring $\mathbb{K}$ is a subring of a commutative ring $\mathbb{L}$, then $\mathbb{L}$ becomes a $\mathbb{K}$-algebra in a natural way[178].
- The polynomial ring $\mathbb{K}[x]$ (introduced in Definition 7.4.10) is a $\mathbb{K}$-algebra.

Particularly common are the $\mathbb{Z}$-algebras: In fact, every ring $\mathbb{K}$ is a $\mathbb{Z}$-algebra in a natural way! To see this, we just need to equip every ring $\mathbb{K}$ with a scaling map $\cdot : \mathbb{Z} \times \mathbb{K} \to \mathbb{K}$ that satisfies the module axioms and the "Scale-invariance of multiplication" axiom. This is done as follows:

> **Example 6.9.2.** Let $\mathbb{K}$ be any ring. Consider the map $\cdot : \mathbb{Z} \times \mathbb{K} \to \mathbb{K}$ sending each pair $(n, a) \in \mathbb{Z} \times \mathbb{K}$ to the element $na \in \mathbb{K}$ defined in Definition 5.4.8. (This map $\cdot$ is not the multiplication operation of $\mathbb{K}$ (unless $\mathbb{K} = \mathbb{Z}$), but we still use the same notation for it, since both of these maps are "multiplications" in a wide sense.) Then, the set $\mathbb{K}$, equipped with the binary operations $+$ and $\cdot$ (the multiplication operation of $\mathbb{K}$), the scaling map $\cdot$ we just defined, and the elements $0_{\mathbb{K}}$ and $1_{\mathbb{K}}$ is a $\mathbb{Z}$-algebra.

Proof of Example 6.9.2. We must prove that $\mathbb{K}$ satisfies the ring axioms, the module axioms and the "Scale-invariance of multiplication" axiom (but we need to be careful, since the roles of the $\mathbb{K}$ and the M in Definition 6.9.1 are now being played by $\mathbb{Z}$ and $\mathbb{K}$). Let us do this:

- The ring axioms are clearly satisfied, since $\mathbb{K}$ is a ring.
- The module axioms are satisfied. In fact, the axioms **(a)**, **(b)**, **(c)** and **(d)** in Definition 6.3.1 are satisfied because $\mathbb{K}$ is a ring; the axiom **(e)** follows from (167); the axiom **(f)** follows from (166); the axiom **(g)** follows from (173); the axiom **(h)** follows from (169); the axiom **(i)** follows from (172); the axiom **(j)** follows from (171).
- The "Scale-invariance of multiplication" axiom is satisfied, because of (170).

Thus, $\mathbb{K}$ is a $\mathbb{Z}$-algebra. This proves Example 6.9.2. □

> **Convention 6.9.3.** If M is a $\mathbb{K}$-algebra, then M automatically becomes a ring (by forgetting the scaling map) and a $\mathbb{K}$-module (by forgetting the multiplication operation and the unity, and declaring the element 0 to be the zero vector). We shall automatically treat any $\mathbb{K}$-algebra both as a ring and as a $\mathbb{K}$-module when

[178] Namely:

- We define the scaling of the $\mathbb{K}$-module $\mathbb{L}$ to be the restriction of the multiplication of the ring $\mathbb{L}$ to $\mathbb{K} \times \mathbb{L}$. (Thus, $\lambda \cdot a = \lambda \cdot a$ for all $\lambda \in \mathbb{K}$ and $a \in \mathbb{L}$, where the "$\cdot$" sign on the left hand side stands for scaling and where the "$\cdot$" sign on the right hand side stands for multiplication.)
- We define the zero vector of $\mathbb{L}$ to be the zero of the ring $\mathbb{L}$.

needed: For example, if M and N are two $\mathbb{K}$-algebras, and we speak of a "ring homomorphism from M to N", then we mean a ring homomorphism from the ring M to the ring N, where M and N become rings in the way we just explained.

There is also a notion of a $\mathbb{K}$-*subalgebra* of a $\mathbb{K}$-algebra, which can be easily defined as follows:

Definition 6.9.4. Let A and B be two $\mathbb{K}$-algebras. We say that A is a $\mathbb{K}$-*subalgebra* (or, for short, *subalgebra*) of B if and only if it satisfies the following six requirements:

- the set A is a subset of B;
- the addition of A is a restriction of the addition of B (that is, we have $a_1 +_A a_2 = a_1 +_B a_2$ for all $a_1, a_2 \in A$);
- the multiplication of A is a restriction of the multiplication of B (that is, we have $a_1 \cdot_A a_2 = a_1 \cdot_B a_2$ for all $a_1, a_2 \in A$);
- the zero of A is the zero of B (that is, we have $0_A = 0_B$);
- the unity of A is the unity of B (that is, we have $1_A = 1_B$);
- the scaling of A is a restriction of the scaling of B (that is, we have $\lambda \cdot_A a = \lambda \cdot_B a$ for all $\lambda \in \mathbb{K}$ and $a \in A$).

Equivalently, A is a $\mathbb{K}$-subalgebra of B if and only if A is simultaneously a subring of B and a $\mathbb{K}$-submodule of B. (Here, we are treating $\mathbb{K}$-algebras as rings and as $\mathbb{K}$-modules, as explained in Convention 6.9.3.)

Similarly, there is a notion of a $\mathbb{K}$-algebra homomorphism:

Definition 6.9.5. Let A and B be two $\mathbb{K}$-algebras. A $\mathbb{K}$-*algebra homomorphism* from A to B means a map $f : A \to B$ that is simultaneously a ring homomorphism from A to B and a $\mathbb{K}$-module homomorphism from A to B. (That is, it means a map $f : A \to B$ that respects addition, respects multiplication, respects scaling, sends 0_A to 0_B, and sends 1_A to 1_B.)

Definition 6.9.6. We say that a $\mathbb{K}$-algebra is *commutative* if the underlying ring is commutative (i.e., if we have $ab = ba$ for each two elements a and b of this $\mathbb{K}$-algebra).

The following property of $\mathbb{K}$-algebras is easy to check but quite useful:

Proposition 6.9.7. Let A be a $\mathbb{K}$-algebra. Let $k \in \mathbb{N}$.

(a) Any $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}$ and $a_1, a_2, \ldots, a_k \in A$ satisfy

$$(\lambda_1 a_1)(\lambda_2 a_2) \cdots (\lambda_k a_k) = (\lambda_1 \lambda_2 \cdots \lambda_k)(a_1 a_2 \cdots a_k).$$

(b) Any $\lambda \in \mathbb{K}$ and $a \in A$ satisfy $(\lambda a)^k = \lambda^k a^k$.

Proof of Proposition 6.9.7. **(a)** This can easily be proven by induction on k. (The induction base boils down to the obvious fact that $1_A = 1_{\mathbb{K}} \cdot 1_A$. The induction step uses the identity

$$(\lambda a)(\mu b) = (\lambda \mu)(ab) \qquad \text{for all } \lambda, \mu \in \mathbb{K} \text{ and } a, b \in A;$$

this identity can be easily proven using "Scale-invariance of multiplication" and axiom **(h)** from Definition 6.3.1.)

(b) This is a particular case of Proposition 6.9.7 **(a)**. □

6.10. Module isomorphisms

In analogy to Definition 5.10.1, we define:

Definition 6.10.1. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a map. Then, f is called a $\mathbb{K}$-*module isomorphism* if and only if f is invertible (i.e., bijective) and both f and f^{-1} are $\mathbb{K}$-module homomorphisms.

Example 6.10.2. Let M be a $\mathbb{K}$-module. The identity map $\operatorname{id} : M \to M$ is a $\mathbb{K}$-module isomorphism.

Proof of Example 6.10.2. We already know that the map $\operatorname{id} : M \to M$ is a $\mathbb{K}$-module homomorphism. Furthermore, it is invertible, and its inverse id^{-1} is id itself. Hence, this inverse id^{-1} is also a $\mathbb{K}$-module homomorphism (since id is a $\mathbb{K}$-module homomorphism). Thus, the map id is invertible and both id and id^{-1} are $\mathbb{K}$-module homomorphisms. In other words, id is a $\mathbb{K}$-module isomorphism (by Definition 6.10.1). This proves Example 6.10.2. □

More generally:

Example 6.10.3. Let M be a $\mathbb{K}$-submodule of a $\mathbb{K}$-module N. Let $\iota : M \to N$ be the map that sends each $a \in M$ to a itself. (This map is called the *inclusion map* from M to N.)

(a) Then, the map ι is a $\mathbb{K}$-module homomorphism.

(b) It is an isomorphism if and only if $M = N$.

Proof of Example 6.10.3. LTTR. □

Proposition 5.10.5 has an analogue for $\mathbb{K}$-module isomorphisms:

Proposition 6.10.4. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be an invertible $\mathbb{K}$-module homomorphism. Then, f is a $\mathbb{K}$-module isomorphism.

Proof of Proposition 6.10.4. Similar to the proof of Proposition 5.10.5. □

The Chinese Remainder Theorem already brought us an example of a ring isomorphism (Example 5.10.7); we can also turn it into an example of a module isomorphism:

Example 6.10.5. Let m and n be two coprime positive integers. Then, $(\mathbb{Z}/m) \times (\mathbb{Z}/n)$ is a $\mathbb{Z}$-module (according to Definition 6.5.3). Theorem 3.6.2 says that the map

$$S_{m,n} : \mathbb{Z}/\left(mn\right) \to \left(\mathbb{Z}/m\right) \times \left(\mathbb{Z}/n\right), \\ \alpha \mapsto \left(\pi_{mn,m}\left(\alpha\right), \pi_{mn,n}\left(\alpha\right)\right)$$

is well-defined and is a bijection. This map $S_{m,n}$ is furthermore a $\mathbb{Z}$-module isomorphism.

Proof of Example 6.10.5. Similar to the proof of Example 5.10.7. □

Definition 6.10.6. Let M and N be two $\mathbb{K}$-modules. We say that the $\mathbb{K}$-modules M and N are *isomorphic* if there exists a $\mathbb{K}$-module isomorphism $f : M \to N$.

We write "$M \cong N$ (as $\mathbb{K}$-modules)" to say that the $\mathbb{K}$-modules M and N are isomorphic.

Keep in mind that one and the same symbol can stand both for a ring and for a $\mathbb{K}$-module. Thus, when saying something like "$M \cong N$", you should clarify whether you mean "$M \cong N$ (as rings)" or "$M \cong N$ (as $\mathbb{K}$-modules)". For example, $\mathbb{C}$ and $\mathbb{R} \times \mathbb{R}$ are both rings and $\mathbb{R}$-modules[179]. We do have $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$ as $\mathbb{R}$-modules, but we don't have $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$ as rings (since $\mathbb{C}$ is a field, but $\mathbb{R} \times \mathbb{R}$ is not a field). So an unqualified statement like "$\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$" would be dangerous.

Example 6.10.7. Let $n, m \in \mathbb{N}$. Then, the map

$$\mathbb{K}^{n \times m} \to \mathbb{K}^{m \times n}, \\ A \mapsto A^T$$

is a $\mathbb{K}$-module isomorphism.

Proof of Example 6.10.7. By Proposition 6.10.4, it suffices to prove that this map is

[179] Indeed:

- The set $\mathbb{C}$ becomes an $\mathbb{R}$-module by defining scaling as multiplication (and addition as addition, and the zero vector as 0), whereas
- the set $\mathbb{R} \times \mathbb{R}$ becomes an $\mathbb{R}$-module according to Definition 6.5.3 (so its scaling is defined entrywise: that is, $\lambda\left(u, v\right) = \left(\lambda u, \lambda v\right)$ for all $\lambda \in \mathbb{R}$ and $\left(u, v\right) \in \mathbb{R} \times \mathbb{R}$).

$\mathbb{K}$-linear and invertible. The $\mathbb{K}$-linearity follows from the formulas

$$\begin{aligned}(A+B)^T &= A^T + B^T; \\ (0_{n\times m})^T &= 0_{m\times n}; \\ (\lambda A)^T &= \lambda A^T,\end{aligned}$$

which hold for arbitrary $A, B \in \mathbb{K}^{n\times m}$ and $\lambda \in \mathbb{K}$ (see [Grinbe15, Exercise 6.5]). The invertibility follows by constructing its inverse, which is the map

$$\begin{aligned}\mathbb{K}^{m\times n} &\to \mathbb{K}^{n\times m}, \\ A &\mapsto A^T.\end{aligned}$$

□

Example 6.10.8. Let $n \in \mathbb{N}$. Then, the map

$$\begin{aligned}\mathbb{K}^{n\times 1} &\to \mathbb{K}^n, \\ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} &\mapsto (a_1, a_2, \ldots, a_n)\end{aligned}$$

is a $\mathbb{K}$-module isomorphism.

Proof. Easy. □

The previous two examples show that

$$\mathbb{K}^{1\times n} \cong \mathbb{K}^{n\times 1} \cong \mathbb{K}^n \qquad \text{as } \mathbb{K}\text{-modules.}$$

Example 6.10.9. Let $n, m \in \mathbb{N}$. Then, we define a map

$$\begin{aligned}\operatorname{vec} : \mathbb{K}^{n\times m} &\to \mathbb{K}^{nm}, \\ (a_{i,j})_{1\leq i\leq n,\ 1\leq j\leq m} &\mapsto (a_{1,1}, a_{1,2}, \ldots, a_{1,m}, a_{2,1}, a_{2,2}, \ldots, a_{2,m}, \ldots, a_{n,1}, a_{n,2}, \ldots, a_{n,m}).\end{aligned}$$

For example, if $n = 2$ and $m = 3$, then

$$\operatorname{vec}\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} = (a, b, c, d, e, f).$$

This map vec is called *row reading* or *row vectorization*.

This map vec is a $\mathbb{K}$-module isomorphism.

Proof of Example 6.10.9. The map vec is $\mathbb{K}$-linear (since addition and scaling are defined entrywise on both $\mathbb{K}^{n\times m}$ and $\mathbb{K}^{nm}$) and invertible. Thus, Proposition 6.10.4 shows that it is a $\mathbb{K}$-module isomorphism. □

Example 6.10.10. Let M be any $\mathbb{K}$-module. Let $\lambda \in \mathbb{K}$. Define the map

$$\begin{aligned} L_\lambda : M &\to M, \\ a &\mapsto \lambda a. \end{aligned}$$

(This is called "scaling by λ".) As we know from Example 6.8.3 **(b)**, this map L_λ is $\mathbb{K}$-linear, i.e., a $\mathbb{K}$-module homomorphism. When is it an isomorphism?

(a) If $\lambda \in \mathbb{K}$ is invertible, then L_λ is a $\mathbb{K}$-module isomorphism.

(b) If $M = \mathbb{K}$ and L_λ is a $\mathbb{K}$-module isomorphism, then λ is invertible.

(c) If $\mathbb{K} = \mathbb{Z}$ and $M = \mathbb{Z}/n$ for some integer n, then L_λ is a $\mathbb{K}$-module isomorphism whenever $\lambda \perp n$.

Proof of Example 6.10.10. **(a)** If $\lambda \in \mathbb{K}$ is invertible, then the map $L_{\lambda^{-1}}$ is inverse to L_λ. (Actually, we have rules like $L_{\lambda\mu} = L_\lambda \circ L_\mu$ and $L_{\lambda+\mu} = L_\lambda + L_\mu$; see Remark 6.10.11 below.)

(b) LTTR.

(c) Let $\mathbb{K} = \mathbb{Z}$ and $M = \mathbb{Z}/n$ for some integer n. Assume that $\lambda \perp n$. Then, λ has a modular inverse μ modulo n. It is now easy to check that the map L_μ is inverse to L_λ; thus, L_λ is invertible and therefore a $\mathbb{K}$-module isomorphism (since we already know that L_λ is a $\mathbb{K}$-module homomorphism). □

Remark 6.10.11. Fix any $\mathbb{K}$-module M. Then, the map

$$\begin{aligned} \mathbb{K} &\to \operatorname{End} M, \\ \lambda &\mapsto L_\lambda \end{aligned}$$

is a ring homomorphism.

Proof. Straightforward. □

We talked for a while about the meaning and use of ring isomorphisms. The same can be said about $\mathbb{K}$-module isomorphisms. So, in particular, two isomorphic $\mathbb{K}$-modules can be viewed as being "the same $\mathbb{K}$-module up to renaming its elements", and any property of one can be transferred to the other. For example, two isomorphic $\mathbb{K}$-modules must have the same size; their endomorphism rings must be isomorphic; etc.

Proposition 6.10.12. Let $n, m \in \mathbb{N}$. The map

$$\begin{aligned} \mathbb{K}^{n\times m} &\to \operatorname{Hom}\left(\mathbb{K}^{m\times 1}, \mathbb{K}^{n\times 1}\right), \\ A &\mapsto L_A \end{aligned}$$

(where L_A is defined as in Theorem 6.8.4) is a $\mathbb{K}$-module isomorphism.

Proof of Proposition 6.10.12. This map is $\mathbb{K}$-linear (due to easily proven statements like $L_{A+B} = L_A + L_B$ and $L_{\lambda A} = \lambda L_A$) and invertible (since Proposition 6.8.5 shows that it is bijective). □

So $\mathbb{K}^{n\times m} \cong \operatorname{Hom}\left(\mathbb{K}^{m\times 1}, \mathbb{K}^{n\times 1}\right)$ as $\mathbb{K}$-modules whenever $n, m \in \mathbb{N}$. This means that **$\mathbb{K}$-linear maps between $\mathbb{K}^{m\times 1}$ and $\mathbb{K}^{n\times 1}$ are "the same as" $n \times m$-matrices**. This says that the "matrix" way of doing linear algebra can be embedded into the "$\mathbb{K}$-module" way of doing linear algebra.

Multiplication of matrices is directly connected to composition of linear maps:

Proposition 6.10.13. Let $n, m, p \in \mathbb{N}$. Let $A \in \mathbb{K}^{n\times m}$ and $B \in \mathbb{K}^{m\times p}$. Then, $L_{AB} = L_A \circ L_B$.

Proof of Proposition 6.10.13. For any $C \in \mathbb{K}^{p\times 1}$, we have $L_{AB}(C) = (L_A \circ L_B)(C)$ (this follows by comparing the equalities $L_{AB}(C) = (AB)C = ABC$ and $(L_A \circ L_B)(C) = L_A(L_B(C)) = A(BC) = ABC$). □

Corollary 6.10.14. Let $n \in \mathbb{N}$. The map

$$\begin{aligned} \mathbb{K}^{n\times n} &\to \operatorname{End}\left(\mathbb{K}^{n\times 1}\right), \\ A &\mapsto L_A \end{aligned}$$

(where L_A is defined as in Theorem 6.8.4 for $m = n$) is a ring isomorphism.

Proof of Corollary 6.10.14. This map respects addition (since $L_{A+B} = L_A + L_B$ for all $A, B \in \mathbb{K}^{n\times n}$) and respects multiplication (by Proposition 6.10.13); furthermore, it sends the zero matrix $0_{n\times n}$ to the zero map $0 \in \operatorname{End}\left(\mathbb{K}^{n\times 1}\right)$ (this is easy to see) and sends the identity matrix I_n to the identity endomorphism $\operatorname{id} \in \operatorname{End}\left(\mathbb{K}^{n\times 1}\right)$ (this follows from observing that $I_n C = C$ for each $C \in \mathbb{K}^{n\times 1}$). Hence, it is a ring homomorphism. Furthermore, it is invertible[180]. Thus, it is a ring isomorphism (by Proposition 5.10.5). □

6.11. Linear independence, spans, bases

Now, let us generalize Definition 6.1.4 to arbitrary $\mathbb{K}$-modules (where $\mathbb{K}$ is still an arbitrary commutative ring):

Definition 6.11.1. Let M be a $\mathbb{K}$-module. Let $v_1, v_2, \ldots, v_k$ be some vectors in M.

(a) A *linear combination* of $v_1, v_2, \ldots, v_k$ means a vector of the form

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k, \qquad \text{with } \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}. \tag{211}$$

[180] The easiest way to see this is to notice that it is the same map as the map from Proposition 6.10.12 (applied to $m = n$), because $\operatorname{End}\left(\mathbb{K}^{n\times 1}\right) = \operatorname{Hom}\left(\mathbb{K}^{n\times 1}, \mathbb{K}^{n\times 1}\right)$ as sets. Hence, the invertibility of this map follows from Proposition 6.10.12.

(b) The *span* of $v_1, v_2, \ldots, v_k$ is defined to be the subset

$$\begin{aligned}&\{\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k \mid \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}\} \\ &= \{\text{linear combinations of } v_1, v_2, \ldots, v_k\}\end{aligned}$$

of M. This span is a $\mathbb{K}$-submodule of M. (This is easy to check.)

(c) The vectors $v_1, v_2, \ldots, v_k$ are said to be *linearly independent* if the only k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k = 0$ is $\left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$.

(d) Let U be a $\mathbb{K}$-submodule of M. We say that $v_1, v_2, \ldots, v_k$ form a *basis* of U (or, more formally, $(v_1, v_2, \ldots, v_k)$ is a basis of U) if and only if the vectors $v_1, v_2, \ldots, v_k$ are linearly independent and their span is U.

(e) Let U be a $\mathbb{K}$-submodule of M. We say that the list $(v_1, v_2, \ldots, v_k)$ *spans* U if and only if the span of $v_1, v_2, \ldots, v_k$ is U. (More informally, instead of saying "the list $(v_1, v_2, \ldots, v_k)$ *spans* U", we can say "the vectors $v_1, v_2, \ldots, v_k$ *span* U"; of course, this is not the same as saying that each of these k vectors on its own spans U.)

(f) All the terminology we have just introduced depends on $\mathbb{K}$. Whenever the ring $\mathbb{K}$ is not clear from the context, you can insert it into this terminology to make it unambiguous: e.g., say "$\mathbb{K}$-linear combination" instead of "linear combination", and "$\mathbb{K}$-span" instead of "span".

The following proposition gives an equivalent criterion for a list of vectors to be a basis of a $\mathbb{K}$-module:

Proposition 6.11.2. Let M be a $\mathbb{K}$-module. Let $v_1, v_2, \ldots, v_k$ be some vectors in M. Then, $(v_1, v_2, \ldots, v_k)$ is a basis of M if and only if each vector in M can be **uniquely** written in the form (211).[181]

Proof of Proposition 6.11.2. The following proof is long, but not much is happening in it (and you may already have seen this argument in a good Linear Algebra class).

$\Longrightarrow$: Assume that $(v_1, v_2, \ldots, v_k)$ is a basis of M. We must prove that each vector in M can be **uniquely** written in the form (211).

We have assumed that $(v_1, v_2, \ldots, v_k)$ is a basis of M. In other words, the vectors $v_1, v_2, \ldots, v_k$ are linearly independent and their span is M (by the definition of "basis").

Now, let $v \in M$ be any vector. Then, v lies in M. In other words, v lies in the span of the vectors $v_1, v_2, \ldots, v_k$ (since the span of these vectors $v_1, v_2, \ldots, v_k$ is M). In other words,

$$v \in \{\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k \mid \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}\}$$

[181] We say that a vector $v \in M$ can be **uniquely** written in the form (211) if there is a **unique** k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$.

(by the definition of the span). In other words, v can be written in the form (211). We shall now show that this way of writing v is unique.

Let $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $(\beta_1, \beta_2, \ldots, \beta_k)$ be two k-tuples $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$. We will show that $(\alpha_1, \alpha_2, \ldots, \alpha_k) = (\beta_1, \beta_2, \ldots, \beta_k)$.

Indeed, $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ is a k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$. In other words, $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ is a k-tuple of elements of $\mathbb{K}$ such that $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k$. Similarly, $(\beta_1, \beta_2, \ldots, \beta_k)$ is a k-tuple of elements of $\mathbb{K}$ such that $v = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k$. Now, multiple uses of the distributivity law yield

$$\begin{aligned}
&(\alpha_1 - \beta_1) v_1 + (\alpha_2 - \beta_2) v_2 + \cdots + (\alpha_k - \beta_k) v_k \\
&= (\alpha_1 v_1 - \beta_1 v_1) + (\alpha_2 v_2 - \beta_2 v_2) + \cdots + (\alpha_k v_k - \beta_k v_k) \\
&= \underbrace{(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k)}_{=v} - \underbrace{(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k)}_{=v} \\
&= v - v = 0. \qquad (212)
\end{aligned}$$

But the only k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k = 0$ is $\left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$ (since the vectors $v_1, v_2, \ldots, v_k$ are linearly independent). Hence, the k-tuple $(\alpha_1 - \beta_1, \alpha_2 - \beta_2, \ldots, \alpha_k - \beta_k) \in \mathbb{K}^k$ must be $\left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$ (since this k-tuple satisfies (212)). In other words, $\alpha_i - \beta_i = 0$ for each $i \in \{1, 2, \ldots, k\}$. In other words, $\alpha_i = \beta_i$ for each $i \in \{1, 2, \ldots, k\}$. In other words, $(\alpha_1, \alpha_2, \ldots, \alpha_k) = (\beta_1, \beta_2, \ldots, \beta_k)$.

Now, forget that we fixed $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $(\beta_1, \beta_2, \ldots, \beta_k)$. We thus have shown that if $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $(\beta_1, \beta_2, \ldots, \beta_k)$ are two k-tuples $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$, then $(\alpha_1, \alpha_2, \ldots, \alpha_k) = (\beta_1, \beta_2, \ldots, \beta_k)$. In other words, there is at most one such k-tuple. In other words, v can be written in the form (211) in at most one way. Thus, v can be **uniquely** written in the form (211) (because we have previously shown that v can be written in this from). This proves the "$\Longrightarrow$" direction of Proposition 6.11.2.

$\Longleftarrow$: Assume that each vector in M can be **uniquely** written in the form (211). We must prove that $(v_1, v_2, \ldots, v_k)$ is a basis of M.

We have assumed that each vector in M can be **uniquely** written in the form (211). Thus, in particular, each vector in M can be written in this form. In other words, for each $v \in M$, there exist $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}$ such that $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$. In other words, each $v \in M$ is a linear combination of the vectors $v_1, v_2, \ldots, v_k$. In other words, each $v \in M$ belongs to the span of the vectors $v_1, v_2, \ldots, v_k$ (by the definition of a span). In other words, M is a subset of the span of the vectors $v_1, v_2, \ldots, v_k$. Hence, the span of the vectors $v_1, v_2, \ldots, v_k$ is M (since this span is clearly a subset of M).

On the other hand, we have assumed that each vector in M can be **uniquely** written in the form (211). Thus, if $v \in M$, then v can be **uniquely** written in this form; thus, in particular, any two ways of writing v in this form must be identical. In other words, if $v \in M$, and if $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $(\beta_1, \beta_2, \ldots, \beta_k)$ are two k-tuples $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$, then

$$(\alpha_1, \alpha_2, \ldots, \alpha_k) = (\beta_1, \beta_2, \ldots, \beta_k). \tag{213}$$

Now, let us prove that the vectors $v_1, v_2, \ldots, v_k$ are linearly independent. Indeed, let $(\rho_1, \rho_2, \ldots, \rho_k) \in \mathbb{K}^k$ be a k-tuple satisfying $\rho_1 v_1 + \rho_2 v_2 + \cdots + \rho_k v_k = 0$. We shall show that $(\rho_1, \rho_2, \ldots, \rho_k) = \left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$.

We notice that $(\rho_1, \rho_2, \ldots, \rho_k)$ and $\left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$ are two k-tuples $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $0 = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$ (since $\rho_1 v_1 + \rho_2 v_2 + \cdots + \rho_k v_k = 0$ and $0 v_1 + 0 v_2 + \cdots + 0 v_k = 0$). Hence, (213) (applied to $v = 0$, $(\alpha_1, \alpha_2, \ldots, \alpha_k) = (\rho_1, \rho_2, \ldots, \rho_k)$ and $(\beta_1, \beta_2, \ldots, \beta_k) = \left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$) yields

$$(\rho_1, \rho_2, \ldots, \rho_k) = \left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right).$$

Now, forget that we fixed $(\rho_1, \rho_2, \ldots, \rho_k)$. We thus have shown that if $(\rho_1, \rho_2, \ldots, \rho_k) \in \mathbb{K}^k$ is any k-tuple satisfying $\rho_1 v_1 + \rho_2 v_2 + \cdots + \rho_k v_k = 0$, then $(\rho_1, \rho_2, \ldots, \rho_k) = \left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$. In other words, the only k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k = 0$ is $\left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$. In other words, the vectors $v_1, v_2, \ldots, v_k$ are linearly independent (by the definition of "linearly independent").

Now we know that the vectors $v_1, v_2, \ldots, v_k$ are linearly independent and their span is M. In other words, $(v_1, v_2, \ldots, v_k)$ is a basis of M (by the definition of "basis"). This proves the "$\Longleftarrow$" direction of Proposition 6.11.2. □

Definition 6.11.3. Let M be a $\mathbb{K}$-module. Then, we say that M is *finitely generated* if there exists a $k \in \mathbb{N}$ and k vectors $v_1, v_2, \ldots, v_k$ that span M.

Finitely generated $\mathbb{K}$-modules are a generalization of finite-dimensional $\mathbb{K}$-vector spaces. A classical result from linear algebra says the following:

Theorem 6.11.4. If $\mathbb{K}$ is a field, then every finitely generated $\mathbb{K}$-module (= $\mathbb{K}$-vector space) has a basis.

Proof. See [ConradD, Theorem 1], for example.[182] □

A version of Theorem 6.11.4 exists for vector spaces that are not finitely generated; however, stating it would require us to define a more general notion of "basis" that would allow for infinite bases (and even then, this version would require the Axiom of Choice).

Theorem 6.11.4 fails horribly when $\mathbb{K}$ is not a field. For example, the $\mathbb{Z}$-module $\mathbb{Z}/2$ has no basis. Indeed, the only $\mathbb{Z}$-linearly independent list of vectors in $\mathbb{Z}/2$ is the empty list $()$, since any vector in $\mathbb{Z}/2$ becomes 0 when scaled by the nonzero integer 2. More generally, if $\mathbb{K}$ is not a field, then there is a $\mathbb{K}$-module spanned by a single vector that has no basis.

Submodules of $\mathbb{K}^{1\times n}$ fare only somewhat better than arbitrary $\mathbb{K}$-modules in terms of having bases. It can be shown that every $\mathbb{Z}$-submodule of $\mathbb{Z}^{1\times n}$ (or, more generally, of a $\mathbb{Z}$-module that has a basis) must have a basis; thus, Theorem 6.1.5 **(a)** does hold for $\mathbb{K} = \mathbb{Z}$. Theorem 6.1.5 **(a)** also holds for $\mathbb{K} = \mathbb{Z}[i]$. (These facts are particular cases of [ConradS, Theorem 2.1].) However, Theorem 6.1.5 **(a)** does not hold for $\mathbb{K} = \mathbb{Z}\left[\sqrt{-3}\right]$ or for $\mathbb{K} = \mathbb{Z}/4$; in both of these cases, we can find $\mathbb{K}$-submodules **of $\mathbb{K}$ itself** that have no basis[183].

Thus, Theorem 6.1.5 **(a)** becomes false when $\mathbb{K}$ is allowed to be an arbitrary ring. The same can be said of parts **(d)** and **(e)** of Theorem 6.1.5; indeed, they become false even for $\mathbb{K} = \mathbb{Z}$, $n = 1$ and $U = \mathbb{Z}^{1\times 1}$. Here are examples of their failure (where, for the sake of simplicity, we are working not in the $\mathbb{Z}$-module $\mathbb{Z}^{1\times 1}$, but in the $\mathbb{Z}$-module $\mathbb{Z}$, which is isomorphic to it):

- The 1-element list (2) of vectors in the $\mathbb{Z}$-module $\mathbb{Z}$ (consisting of just the single vector $2 \in \mathbb{Z}$) is $\mathbb{Z}$-linearly independent (because if $\lambda_1 \in \mathbb{Z}$ satisfies $\lambda_1 \cdot 2 = 0$, then $\lambda_1 = 0$); but you cannot extend it to a basis of $\mathbb{Z}$ (since adding any further vector to it would break linear independence). Thus, Theorem 6.1.5 **(d)** fails for $\mathbb{K} = \mathbb{Z}$, $n = 1$ and $U = \mathbb{Z}^{1\times 1}$.

- The integers 2 and 3 are coprime. Hence, Bezout's theorem says that 1 is a $\mathbb{Z}$-linear combination of 2 and 3. (This can be proven more directly: $1 = 1 \cdot 3 + (-1) \cdot 2$.) This entails that **every** integer is a $\mathbb{Z}$-linear combination of 2 and 3. In other words, the span of the 2-element list $(2, 3)$ of vectors in $\mathbb{Z}$ is

[182] Note that in the (otherwise excellent) note [ConradD], Conrad follows the inane convention that an empty list $()$ cannot be a basis. This forces him to make the unnatural requirement "$V \neq \{0\}$" in [ConradD, Theorem 1]. You should ignore this special treatment (or, rather, non-treatment) of empty lists when you read the note.

[183] If $\mathbb{K} = \mathbb{Z}/4$, then this is easy: Just take the $\mathbb{K}$-submodule $2\mathbb{K} = \{[0]_4, [2]_4\}$ of $\mathbb{K}$; it has no basis, since scaling by 2 sends all of its elements to 0.

If $\mathbb{K} = \mathbb{Z}\left[\sqrt{-3}\right]$, then the subset $\left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z} \text{ satisfying } a \equiv b \mod 2\right\}$ of $\mathbb{K}$ is a $\mathbb{K}$-submodule having no basis. This is closely connected to the fact that division with remainder and unique factorization into primes do not work in the ring $\mathbb{Z}\left[\sqrt{-3}\right]$.

$\mathbb{Z}$. But neither of these two vectors alone suffices: The span of the 1-element list (2) is just $\{\text{multiples of } 2\}$, whereas the span of the 1-element list (3) is just $\{\text{multiples of } 3\}$. So the 2-element list $(2,3)$ spans the $\mathbb{Z}$-module $\mathbb{Z}$, but cannot be "shrunk" to a basis of $\mathbb{Z}$. Therefore, Theorem 6.1.5 **(e)** fails for $\mathbb{K} = \mathbb{Z}$, $n = 1$ and $U = \mathbb{Z}^{1\times 1}$.

Does Theorem 6.1.5 **(b)** survive the generalization from fields to commutative rings? Literally speaking, the answer is "no". Indeed, if $\mathbb{K}$ is the zero ring, then there is only one $\mathbb{K}$-module (namely, $\{0\}$), but it has bases of all sizes (indeed, for each $n \in \mathbb{N}$, the n-element list $(0,0,\ldots,0)$ is a basis of this $\mathbb{K}$-module). So two bases of this module can have different sizes.

However, surprisingly, this turns out to be the only counterexample for Theorem 6.1.5 **(b)**! More precisely, Theorem 6.1.5 **(b)** holds whenever the ring $\mathbb{K}$ has more than one element. More generally, we have:

Theorem 6.11.5. Let $\mathbb{K}$ be a commutative ring with $|\mathbb{K}| > 1$. Let U be a $\mathbb{K}$-module. Then, any two bases of U have the same size.

This is much harder to prove than the analogue for fields! There is an argument using determinants.

More generally, Theorem 6.1.5 **(c)** also holds over commutative rings $\mathbb{K}$ such that $|\mathbb{K}| > 1$.

These results and counterexamples illustrate the fact that $\mathbb{K}$-modules (where $\mathbb{K}$ is a commutative ring) are a much richer structure than just $\mathbb{K}^{n\times 1}$'s for $n \in \mathbb{N}$.

6.12. $\mathbb{K}$-submodules from linear maps

We defined the kernel of a matrix; we can similarly define the kernel of a linear map, and a slightly more general notion:

Proposition 6.12.1. Let $\mathbb{K}$ be a commutative ring. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a $\mathbb{K}$-module homomorphism (i.e., a $\mathbb{K}$-linear map).

(a) The set

$$\{v \in M \mid f(v) = 0\}$$

is a $\mathbb{K}$-submodule of M. This set is called the *kernel* of f, and is written $\operatorname{Ker} f$ (or $\ker f$).

(b) Let V be a $\mathbb{K}$-submodule of N. Then, the set

$$\{v \in M \mid f(v) \in V\}$$

is a $\mathbb{K}$-submodule of M. This set is called the *preimage of V under f*, and is written $f^{-1}(V)$.

Proof of Proposition 6.12.1. **(b)** Let us denote the subset $\{v \in M \mid f(v) \in V\}$ of M by $f^{-1}(V)$. We must prove that this subset $f^{-1}(V)$ is a $\mathbb{K}$-submodule of M.

According to Definition 6.7.5, we can achieve this by proving that this subset contains 0, is closed under addition and is closed under scaling.

Let us first prove that it contains 0. Indeed, since f is $\mathbb{K}$-linear, we have $f\left(0\right) = 0 \in V$ (since V is a $\mathbb{K}$-submodule of N). Thus, $0 \in f^{-1}\left(V\right)$ (by the definition of $f^{-1}\left(V\right)$). In other words, the subset $f^{-1}\left(V\right)$ contains 0.

Next, let us show that $f^{-1}\left(V\right)$ is closed under addition. Indeed, let $a, b \in f^{-1}\left(V\right)$; we must then prove that $a + b \in f^{-1}\left(V\right)$.

From $a \in f^{-1}\left(V\right)$, we obtain $f\left(a\right) \in V$ (by the definition of $f^{-1}\left(V\right)$). Similarly, $f\left(b\right) \in V$. But V is a $\mathbb{K}$-submodule of N and therefore closed under addition; hence, from $f\left(a\right) \in V$ and $f\left(b\right) \in V$, we conclude that $f\left(a\right) + f\left(b\right) \in V$. But the map f is $\mathbb{K}$-linear; thus, $f\left(a+b\right) = f\left(a\right) + f\left(b\right) \in V$. In other words, $a + b \in f^{-1}\left(V\right)$ (by the definition of $f^{-1}\left(V\right)$).

Now, forget that we fixed a, b. We thus have proven that all $a, b \in f^{-1}\left(V\right)$ satisfy $a + b \in f^{-1}\left(V\right)$. In other words, the subset $f^{-1}\left(V\right)$ is closed under addition.

A similar argument shows that $f^{-1}\left(V\right)$ is closed under scaling.

Thus, $f^{-1}\left(V\right)$ is a $\mathbb{K}$-submodule of M (according to Definition 6.7.5). This proves Proposition 6.12.1 **(b)**.

(a) It is easy to see that the one-element set $\left\{0_N\right\}$ is a $\mathbb{K}$-submodule of N (since $0_N + 0_N = 0_N$ and $\lambda \cdot 0_N = 0_N$ for each $\lambda \in \mathbb{K}$). Hence, Proposition 6.12.1 **(b)** (applied to $V = \left\{0_N\right\}$) yields that the set $\left\{v \in M \mid f\left(v\right) \in \left\{0_N\right\}\right\}$ is a $\mathbb{K}$-submodule of M. But this set is precisely $\left\{v \in M \mid f\left(v\right) = 0\right\}$ (since the condition "$f\left(v\right) \in \left\{0_N\right\}$" on a vector $v \in M$ is equivalent to "$f\left(v\right) = 0$"). Hence, we conclude that $\left\{v \in M \mid f\left(v\right) = 0\right\}$ is a $\mathbb{K}$-submodule of M. This proves Proposition 6.12.1 **(a)**. □

A second way to construct $\mathbb{K}$-submodules out of linear maps generalizes the column space of a matrix:

Proposition 6.12.2. Let $\mathbb{K}$ be a commutative ring. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a $\mathbb{K}$-module homomorphism (i.e., a $\mathbb{K}$-linear map).

(a) The set $f\left(M\right) = \left\{f\left(v\right) \mid v \in M\right\}$ is a $\mathbb{K}$-submodule of N. This is called the *image* of f.

(b) Let U be a $\mathbb{K}$-submodule of M. Then, the set $f\left(U\right) = \left\{f\left(v\right) \mid v \in U\right\}$ is a $\mathbb{K}$-submodule of N. This is called the *image of U under f*.

Proof of Proposition 6.12.2. This is somewhat similar to the proof of Proposition 6.12.1, and left to the reader. □

How do the kernel and the image of a linear map generalize the kernel and the column space of a matrix? Again, this comes from the correspondence between matrices and linear maps:

Remark 6.12.3. Let $\mathbb{K}$ be a commutative ring. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be an $n \times m$-matrix. Consider the $\mathbb{K}$-linear map L_A defined in Theorem 6.8.4. Then:

(a) The kernel of the map L_A is the kernel of the matrix A.

(b) The image of the map L_A is the column space of the matrix A.

(Here, we are defining the kernel and the column space of a matrix as we did in Definition 6.1.12 and Definition 6.1.8, but without requiring $\mathbb{K}$ to be a field.)

Proof of Remark 6.12.3. Follows directly from the definitions. □

The reader may wonder, after we have stressed certain parallels between rings and $\mathbb{K}$-modules a few times, whether kernels and images can be defined for ring homomorphisms in the same way as we have defined them for $\mathbb{K}$-module homomorphisms. The answer is "yes", of course (after all, rings also have a 0, just as modules do), but the outcome is perhaps somewhat surprising. First, let us show the analogue of Proposition 6.12.2 for rings:

Proposition 6.12.4. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism.

(a) The set $f(\mathbb{K}) = \{f(v) \mid v \in \mathbb{K}\}$ is a subring of $\mathbb{L}$. This is called the *image* of f.

(b) Let $\mathbb{U}$ be a subring of $\mathbb{K}$. Then, the set $f(\mathbb{U}) = \{f(v) \mid v \in \mathbb{U}\}$ is a subring of $\mathbb{L}$. This is called the *image of* $\mathbb{U}$ *under* f.

Proof of Proposition 6.12.4. This is similar to the proof of Proposition 6.12.2. □

Next, we can define the kernel of a ring homomorphism by imitating Proposition 6.12.1; but this kernel will almost never be a subring (as it will almost never contain 1). Instead, it will be a special sort of subset of $\mathbb{K}$: a so-called *ideal*. Let us define ideals:

Definition 6.12.5. Let $\mathbb{K}$ be a ring. An *ideal* of $\mathbb{K}$ is defined to be a subset I of $\mathbb{K}$ that satisfies the following four conditions:

- The subset I is closed under addition (i.e., we have $a + b \in I$ for all $a \in I$ and $b \in I$).
- The subset I contains $0_{\mathbb{K}}$.
- We have $\lambda a \in I$ for all $\lambda \in \mathbb{K}$ and $a \in I$.
- We have $a\lambda \in I$ for all $\lambda \in \mathbb{K}$ and $a \in I$.

It is easy to see that any ring $\mathbb{K}$ is an ideal of itself; furthermore, the 1-element subset $\{0_{\mathbb{K}}\}$ of $\mathbb{K}$ is an ideal of $\mathbb{K}$ as well. But there can be many further ideals:

Example 6.12.6. Let $\mathbb{K}$ be a commutative ring. Let $u \in \mathbb{K}$. Then, the subset

$$u\mathbb{K} := \{uz \mid z \in \mathbb{K}\}$$

of $\mathbb{K}$ is an ideal of $\mathbb{K}$. Such an ideal is called a *principal ideal*. Note that $\{0_{\mathbb{K}}\}$ is a principal ideal (since $\{0_{\mathbb{K}}\} = 0\mathbb{K}$), and $\mathbb{K}$ itself is a principal ideal (since $\mathbb{K} = 1\mathbb{K}$).

Let us see what this results in for some specific rings $\mathbb{K}$:

- The principal ideals of the ring $\mathbb{Z}$ are the subsets $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\} = \{\text{all multiples of } n\}$ with $n \in \mathbb{Z}$. For example, $2\mathbb{Z} = \{\text{all even numbers}\}$ is an ideal of $\mathbb{Z}$. It is not hard to show that all ideals of $\mathbb{Z}$ are principal ideals.
- It can also be shown that all ideals of $\mathbb{Z}[i]$ are principal ideals. The same holds for $\mathbb{D}$ (the ring of dual numbers), for $\mathbb{Z}\left[\sqrt{-2}\right]$ (the ring of "2-Gaussian integers"), and $\mathbb{Q}[x]$ (the ring of polynomials with rational coefficients, to be formally defined in Definition 7.4.10 below).
- However, there exist some rings that have non-principal ideals as well. For example, if $\mathbb{K}$ is the ring $\mathbb{Z}\left[\sqrt{-3}\right]$, then the subset $\left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z} \text{ satisfying } a \equiv b \mod 2\right\}$ of $\mathbb{K}$ is an ideal but not a principal ideal. For another example, if $\mathbb{K}$ is the ring $\mathbb{Z}[x]$ (the ring of polynomials with integer coefficients, to be formally defined in Definition 7.4.10 below), then the subset of $\mathbb{K}$ consisting of all polynomials with even constant term is an ideal but not a principal ideal.

When $\mathbb{K}$ is a commutative ring, the third and fourth conditions in Definition 6.12.5 actually say the same thing (because $\lambda a = a\lambda$ for all $\lambda \in \mathbb{K}$ and $a \in \mathbb{K}$). From this, it is not hard to see the following:

Proposition 6.12.7. Let $\mathbb{K}$ be a commutative ring. Then, an ideal of $\mathbb{K}$ is the same thing as a $\mathbb{K}$-submodule of $\mathbb{K}$. (Remember that $\mathbb{K}$ itself is a $\mathbb{K}$-module!).

Proof of Proposition 6.12.7. LTTR. □

Now, we can state an analogue of Proposition 6.12.1 is the following:

Proposition 6.12.8. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism.

(a) The set
$$\{v \in \mathbb{K} \mid f(v) = 0\}$$
is an ideal of $\mathbb{K}$. This set is called the *kernel* of f, and is written $\operatorname{Ker} f$ (or $\ker f$).

(b) Let V be an ideal of $\mathbb{L}$. Then, the set
$$\{v \in \mathbb{K} \mid f(v) \in V\}$$
is an ideal of $\mathbb{K}$. This set is called the *preimage of V under f*, and is written $f^{-1}(V)$.

Proof of Proposition 6.12.8. LTTR. □

So the kernel of a ring homomorphism is always an ideal. (And conversely, every ideal can be written as the kernel of a ring homomorphism; this will follow from Proposition 8.2.6 **(g)** further below.)

Kernels can also help in checking whether a ring homomorphism or a module homomorphism is injective. To wit, for ring homomorphisms, the following criterion for injectivity holds:

Proposition 6.12.9. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism. Then, f is injective if and only if $\operatorname{Ker} f = \{0_{\mathbb{K}}\}$.

Proof of Proposition 6.12.9. $\Longrightarrow$: Assume that f is injective. We must prove that $\operatorname{Ker} f = \{0_{\mathbb{K}}\}$.

Recall that f is a ring homomorphism. Thus, $f(0) = 0$ (by the definition of a ring homomorphism).

Let $a \in \operatorname{Ker} f$. Then, $a \in \operatorname{Ker} f = \{v \in \mathbb{K} \mid f(v) = 0\}$ (by the definition of $\operatorname{Ker} f$). In other words, $a \in \mathbb{K}$ and $f(a) = 0$. Comparing this with $f(0) = 0$, we obtain $f(a) = f(0)$. Since f is injective, we can thus conclude that $a = 0 = 0_{\mathbb{K}} \in \{0_{\mathbb{K}}\}$.

Now, forget that we fixed a. We thus have proven that $a \in \{0_{\mathbb{K}}\}$ for each $a \in \operatorname{Ker} f$. In other words, $\operatorname{Ker} f \subseteq \{0_{\mathbb{K}}\}$.

On the other hand, $f(0_{\mathbb{K}}) = f(0) = 0$, so that $0_{\mathbb{K}} \in \operatorname{Ker} f$ (by the definition of $\operatorname{Ker} f$), so that $\{0_{\mathbb{K}}\} \subseteq \operatorname{Ker} f$. Combining this with $\operatorname{Ker} f \subseteq \{0_{\mathbb{K}}\}$, we obtain $\operatorname{Ker} f = \{0_{\mathbb{K}}\}$. This proves the "$\Longrightarrow$" direction of Proposition 6.12.9.

$\Longleftarrow$: Assume that $\operatorname{Ker} f = \{0_{\mathbb{K}}\}$. We must prove that f is injective.

Let a and b be two elements of $\mathbb{K}$ satisfying $f(a) = f(b)$. Then, Proposition 5.9.14 **(c)** yields $f(a-b) = f(a) - f(b) = 0$ (since $f(a) = f(b)$). Hence, $a - b \in \mathbb{K}$ and $f(a-b) = 0$. In other words, $a - b \in \operatorname{Ker} f$ (by the definition of $\operatorname{Ker} f$). Thus, $a - b \in \operatorname{Ker} f = \{0_{\mathbb{K}}\}$, so that $a - b = 0_{\mathbb{K}}$ and thus $a = b$.

Now, forget that we fixed a and b. We thus have shown that if a and b are two elements of $\mathbb{K}$ satisfying $f(a) = f(b)$, then $a = b$. In other words, the map f is injective. This proves the "$\Longleftarrow$" direction of Proposition 6.12.9. □

An analogous statement holds for $\mathbb{K}$-module homomorphisms:

Proposition 6.12.10. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a $\mathbb{K}$-module homomorphism (i.e., a $\mathbb{K}$-linear map). Then, f is injective if and only if $\operatorname{Ker} f = \{0_M\}$.

Proof of Proposition 6.12.10. This is proven analogously to Proposition 6.12.9; the main difference is that instead of applying Proposition 5.9.14 **(c)**, we have to apply the analogue of Proposition 5.9.14 **(c)** for $\mathbb{K}$-module homomorphisms (which we have not stated, but is proven in the same way). □

A curious (and useful) consequence of Proposition 6.12.9 is the following property of fields:

Corollary 6.12.11. Let $\mathbb{K}$ be a field, and let $\mathbb{L}$ be a ring such that $\mathbb{L}$ is not trivial (i.e., we have $|\mathbb{L}| > 1$). Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism. Then, f is injective.

Proof of Corollary 6.12.11. Due to Proposition 6.12.9, it suffices to show that $\operatorname{Ker} f = \{0_{\mathbb{K}}\}$. So let us prove this.

Let $a \in \operatorname{Ker} f$. Thus, $a \in \mathbb{K}$ and $f(a) = 0$ (by the definition of $\operatorname{Ker} f$). We are going to prove that $a = 0_{\mathbb{K}}$.

Indeed, assume the contrary. Thus, $a \neq 0_{\mathbb{K}}$. Hence, the element a of $\mathbb{K}$ is nonzero. But every nonzero element of $\mathbb{K}$ is invertible (since $\mathbb{K}$ is a field). Hence, a is invertible (since a is a nonzero element of $\mathbb{K}$). Thus, Proposition 5.9.14 **(b)** shows that $f(a) \in \mathbb{L}$ is also invertible, and that we have $f\left(a^{-1}\right) = (f(a))^{-1}$.

Thus, comparing $f(a) \cdot (f(a))^{-1} = 1_{\mathbb{L}}$ with $\underbrace{f(a)}_{=0} \cdot (f(a))^{-1} = 0$, we obtain $1_{\mathbb{L}} = 0$. Hence, each $b \in \mathbb{L}$ satisfies $b = b \cdot \underbrace{1_{\mathbb{L}}}_{=0} = 0 \in \{0\}$. Thus, $\mathbb{L} \subseteq \{0\}$, so that $|\mathbb{L}| \leq |\{0\}| = 1$. This contradicts $|\mathbb{L}| > 1$. This contradiction shows that our assumption is wrong. Hence, $a = 0_{\mathbb{K}}$ is proven. Therefore, $a \in \{0_{\mathbb{K}}\}$.

Now, forget that we fixed a. We thus have shown that $a \in \{0_{\mathbb{K}}\}$ for each $a \in \operatorname{Ker} f$. In other words, $\operatorname{Ker} f \subseteq \{0_{\mathbb{K}}\}$. From this, we can easily deduce that $\operatorname{Ker} f = \{0_{\mathbb{K}}\}$ (by the same argument that we used in our proof of the "$\Longrightarrow$" direction of Proposition 6.12.9). Thus, Proposition 6.12.9 shows that f is injective. This proves Corollary 6.12.11. □

7. Polynomials and formal power series

7.1. Motivation

Back in our proof of Theorem 2.17.14, we have used a vague notion of polynomials. Let us try and formalize this notion. While at that, we shall also try to generalize it from polynomials with rational coefficients to polynomials with coefficients in an arbitrary commutative ring.

The most "naive" notion of polynomials is that of a polynomial function:

Definition 7.1.1. Let $\mathbb{K}$ be a commutative ring. A function $f : \mathbb{K} \to \mathbb{K}$ is said to be a *polynomial function* if there exist some elements $a_0, a_1, \ldots, a_n \in \mathbb{K}$ such that every $u \in \mathbb{K}$ satisfies

$$f(u) = a_0 u^0 + a_1 u^1 + \cdots + a_n u^n.$$

For example, the function

$$\mathbb{R} \to \mathbb{R}, \qquad u \mapsto 6u^3 - \frac{1}{2}u + \sqrt{3}$$

is a polynomial function.

Definition 7.1.1 has its uses. In particular, when you are working with real or complex numbers, it is sufficient for most of what you would want from a polynomial. (This is why numerous authors, particularly with backgrounds in analysis, simply define a polynomial to be a polynomial function.) But when we want polynomials with coefficients from other rings, this definition starts showing weaknesses. In what sense?

Here is an example. In Section 5.6, we constructed a field with 4 elements by adjoining a j satisfying $j^2 = j + 1$ to $\mathbb{Z}/2$. In other words, we adjoined a root of "the polynomial $x^2 - x - 1$" (whatever this may mean) to $\mathbb{Z}/2$. It would be helpful to generalize this: How can we adjoin a root of a polynomial to a ring? In particular, if we can do this with polynomials of higher degree than 2, we may hope to be able to construct larger finite fields. For example, how do we find a field of size 8 ? We would hope to get it by adjoining to $\mathbb{Z}/2$ a root of a degree-3 polynomial.

So we need a notion of polynomials over $\mathbb{Z}/2$, and we need there to be infinitely many of them, ideally at least one of each degree. With polynomial functions, we cannot get this. In fact, there are only 4 functions from $\mathbb{Z}/2$ to $\mathbb{Z}/2$.

Even for our above construction of a field with 4 elements, polynomial functions are not suited. In fact, the polynomial function

$$\mathbb{Z}/2 \to \mathbb{Z}/2, \qquad x \mapsto x^2 - x - 1$$

is actually just the constant-1 function. So when we adjoined a root of this polynomial, did we just adjoin a root of 1 ? Hardly. (A root of 1 would be a j satisfying $1 = 0$; "adjoining" such a thing would yield the zero ring, not a field with 4 elements.)

The moral of the story for now is that when we adjoin a root of a polynomial to a field, we certainly are not adjoining a root of a polynomial function. So we have at least one reason to want a concept of polynomials that is finer than that of polynomial functions.

Here is another reason: Polynomial functions from $\mathbb{K}$ to $\mathbb{K}$ can only be applied to elements of $\mathbb{K}$ (because they are defined as functions from $\mathbb{K}$), but we want a notion of polynomials that can be applied to more general things (such as square matrices or other polynomials).

For example, in linear algebra, it is extremely useful to apply polynomials to square matrices. With polynomial functions, this makes no sense: A polynomial function over $\mathbb{R}$ is defined only on $\mathbb{R}$, so how can you apply it to a 2×2-matrix? Once again, the discrepancy becomes the most obvious over a finite field: The two polynomial functions $\mathbb{Z}/2 \to \mathbb{Z}/2$, $x \mapsto x^2$ and $\mathbb{Z}/2 \to \mathbb{Z}/2$, $x \mapsto x$ are identical (since $x^2 = x$ for all $x \in \mathbb{Z}/2$); but the matrix $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in (\mathbb{Z}/2)^{2\times 2}$ does not satisfy $A^2 = A$. So if there was a way to apply these two identical polynomial functions to A, then we should obtain two different results, which is absurd. Thus, it makes no sense to apply a polynomial function $\mathbb{Z}/2 \to \mathbb{Z}/2$ to a square matrix over $\mathbb{Z}/2$.

Hence, we need a finer definition of a polynomial which doesn't just remember its values on the elements of $\mathbb{K}$, but remembers all its coefficients. So we need to bake the coefficients into the definition.

We already gave a hint of such a definition in Subsection 2.17.3, where we said that a polynomial (in 1 variable x, with rational coefficients) is an "expression" (whatever this means) of the form $a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$, where $a_k, a_{k-1}, \ldots, a_0$ are (fixed) rational numbers and where x is an "indeterminate" (a symbol that itself does not stand for a number, but we can substitute a number for). This was vague (what exactly is an "expression"?) but a step in the right direction. We can, of course, generalize this informal definition to an arbitrary commutative ring $\mathbb{K}$ by replacing "rational numbers" by "elements of $\mathbb{K}$". But how do we make the notion of "expression" rigorous?

The idea is to forget (at first) about the specific form of the expression $a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ and simply store the coefficients $a_0, a_1, \ldots, a_k$ appearing in it in a list.

For example, let us consider polynomials of degree ≤ 1 over $\mathbb{R}$. These always have the form $a_0 + a_1 x$ (with $a_0, a_1 \in \mathbb{R}$), so we can simply define them as **pairs** (a_0, a_1) of real numbers a_0 and a_1. (This is analogous to Definition 4.1.1, where we defined complex numbers as pairs of real numbers rather than trying to treat them as "expressions involving i".) Next, we define an addition operation $+$ on polynomials of degree ≤ 1 by setting

$$(a_0, a_1) + (b_0, b_1) = (a_0 + b_0, a_1 + b_1),$$

which of course imitates the informal computation

$$(a_0 + a_1 x) + (b_0 + b_1 x) = (a_0 + b_0) + (a_1 + b_1) x.$$

Furthermore, we define a multiplication on these polynomials by setting

$$(a_0, a_1) \cdot (b_0, b_1) = (a_0 b_0, a_0 b_1 + a_1 b_0, a_1 b_1),$$

which imitates the "FOIL" rule

$$(a_0 + a_1 x) \cdot (b_0 + b_1 x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + a_1 b_1 x^2.$$

However, this multiplication yields a triple, not a pair, so it is not a binary operation. So our polynomials of degree ≤ 1 do not form a ring; their multiplication takes us out of their set.

We can likewise consider polynomials of degree ≤ 2, which can be defined as triples (a_0, a_1, a_2), but then multiplication yields a 5-tuple rather than a triple.

More generally: For each $n \in \mathbb{N}$, we can define polynomials of degree $\leq n$ as $(n+1)$-tuples $(a_0, a_1, \ldots, a_n)$, and define addition and multiplication on them, but the multiplication will result in $(2n+1)$-tuples rather than $(n+1)$-tuples.

Hence, if we want to define polynomials in such a way that they form a ring, we should define them not as pairs or triples or $(n+1)$-tuples, but rather as infinite sequences. In other words, we should define a polynomial as an infinite sequence $(a_0, a_1, a_2, \ldots)$, which will encode the "expression" $a_0 + a_1 x + a_2 x^2 + \cdots$. However, not every sequence stands for a polynomial; after all, we want polynomials to be **finite** expressions, so the sum $a_0 + a_1 x + a_2 x^2 + \cdots$ needs to be finite (in the sense that all but finitely many of its addends are 0) in order for it to qualify as a polynomial. Thus, our polynomials should be defined as infinite sequences $(a_0, a_1, a_2, \ldots)$ that have only finitely many nonzero entries.

An upside of this strategy is that with such a definition, we get a second object for free: the *formal power series*. Those are just going to be **all** infinite sequences $(a_0, a_1, a_2, \ldots)$, including the ones that have infinitely many nonzero entries. We will see that the same rules by which we define addition and multiplication of polynomials can be used to define these operations on formal power series.

7.2. The definition of formal power series and polynomials

Let us now explicitly state the definitions we have been working towards. We shall only define polynomials (and formal power series) in 1 indeterminate; there is a version that involves multiple indeterminates, but for now we restrict ourselves to one.

Convention 7.2.1. For the rest of this chapter, we fix a commutative ring $\mathbb{K}$.

Definition 7.2.2. (a) A *formal power series* (in 1 indeterminate over $\mathbb{K}$) is defined to be a sequence $(a_0, a_1, a_2, \ldots) = (a_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ of elements of $\mathbb{K}$.

We abbreviate the words "formal power series" as "*FPS*".

We let $\mathbb{K}[[x]]$ be the set of all FPSs.

(b) A *polynomial* (in 1 indeterminate over $\mathbb{K}$) is defined to be an FPS $(a_0, a_1, a_2, \ldots)$ such that

$$\text{all but finitely many } i \in \mathbb{N} \text{ satisfy } a_i = 0$$

(that is, only finitely many $i \in \mathbb{N}$ satisfy $a_i \neq 0$).

We let $\mathbb{K}[x]$ be the set of all polynomials.

So far, our FPSs are just sequences, with no other meaning. We will later see why they can be viewed as "power series", what the x in "$\mathbb{K}[[x]]$" means, and why we can write a sequence $(a_0, a_1, a_2, \ldots)$ as $a_0 + a_1 x + a_2 x^2 + \cdots$.

First, let us give two examples to illustrate the above definition:

Example 7.2.3. In this example, let $\mathbb{K} = \mathbb{Z}$.

(a) The sequence $(1, 2, 3, 4, 5, \ldots)$ is an FPS, but not a polynomial. We will later write this FPS as $1 + 2x + 3x^2 + 4x^3 + 5x^4 + \cdots$.

(b) The sequence $\left(3, 0, 2, 5, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}}\right)$ is a polynomial. We will later write this polynomial as $3 + 2x^2 + 5x^3$.

Definition 7.2.4. The goal of this definition is to make $\mathbb{K}[[x]]$ into a $\mathbb{K}$-algebra.

(a) We define a binary operation $+$ (called *addition*) on $\mathbb{K}[[x]]$ by

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots).$$

(That is, we define an entrywise addition.)

(b) We define a scaling map $\cdot : \mathbb{K} \times \mathbb{K}[[x]] \to \mathbb{K}[[x]]$ by

$$\lambda (a_0, a_1, a_2, \ldots) = (\lambda a_0, \lambda a_1, \lambda a_2, \ldots).$$

(That is, we define an entrywise scaling.)

(c) We define a binary operation $\cdot$ (called *multiplication*) on $\mathbb{K}[[x]]$ by

$$(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots),$$

where

$$c_n = \sum_{i=0}^{n} a_i b_{n-i} = \sum_{\substack{i,j \in \mathbb{N};\\ i+j=n}} a_i b_j = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 \qquad \text{for all } n \in \mathbb{N}.$$

(d) For each $a \in \mathbb{K}$, we define an FPS $\underline{a} \in \mathbb{K}[[x]]$ by

$$\underline{a} = \left(a, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right).$$

This is called a *constant* FPS.

For example,

$$\begin{aligned}
(0, 1, 2, 3, 4, \ldots) + (1, 1, 1, 1, 1, \ldots) &= (1, 2, 3, 4, 5, \ldots) && \text{and} \\
(1, 1, 1, 1, 1, \ldots) + (1, 1, 1, 1, 1, \ldots) &= (2, 2, 2, 2, 2, \ldots) && \text{and} \\
8 \cdot (1, 1, 1, 1, 1, \ldots) &= (8, 8, 8, 8, 8, \ldots) && \text{and} \\
(1, 1, 1, 1, 1, \ldots) \cdot (1, 1, 1, 1, 1, \ldots) &= (1, 2, 3, 4, 5, \ldots) && \text{and} \\
\left(1, -1, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) \cdot (1, 1, 1, 1, 1, \ldots) &= \left(1, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) = \underline{1}. && (214)
\end{aligned}$$

Theorem 7.2.5. **(a)** Equip the set $\mathbb{K}[[x]]$ with the addition $+$ defined in Definition 7.2.4 **(a)**, the multiplication $\cdot$ defined in Definition 7.2.4 **(c)**, the scaling $\cdot$ defined in Definition 7.2.4 **(b)**, the zero $\underline{0}$ and the unity $\underline{1}$. Then, $\mathbb{K}[[x]]$ is a $\mathbb{K}$-algebra, a commutative ring and a $\mathbb{K}$-module.

(b) The subtraction $-$ that comes from the $\mathbb{K}$-algebra structure on $\mathbb{K}[[x]]$ is entrywise; in other words, any two FPSs $(a_0, a_1, a_2, \ldots)$ and $(b_0, b_1, b_2, \ldots)$ satisfy

$$(a_0, a_1, a_2, \ldots) - (b_0, b_1, b_2, \ldots) = (a_0 - b_0, a_1 - b_1, a_2 - b_2, \ldots).$$

(c) We have

$$\lambda \mathbf{a} = \underline{\lambda} \cdot \mathbf{a} \qquad \text{for each } \lambda \in \mathbb{K} \text{ and } \mathbf{a} \in \mathbb{K}[[x]].$$

(d) Consider the map

$$\iota : \mathbb{K} \to \mathbb{K}[[x]], \\ a \mapsto \underline{a}$$

(sending each element $a \in \mathbb{K}$ to the corresponding constant FPS $\underline{a} = \left(a, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right)$). This map ι is a $\mathbb{K}$-algebra homomorphism[184].

Before we outline a proof of this theorem, let us introduce a helpful notation (used often in enumerative combinatorics):

Definition 7.2.6. Let $n \in \mathbb{N}$. Let $\mathbf{a} = (a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]]$. Then, we define an element $[x^n]\, \mathbf{a} \in \mathbb{K}$ by

$$[x^n]\, \mathbf{a} = a_n.$$

This element $[x^n]\, \mathbf{a}$ is called *the coefficient of x^n in* $\mathbf{a}$, or the *n-th coefficient* of $\mathbf{a}$. (The letter "x" is so far considered just as a symbolic part of this notation, with no standalone meaning.)

Be careful with this notation: What you would normally call "the first entry" of the sequence $(a_0, a_1, a_2, \ldots)$ is called its 0-th (not 1-st) coefficient.

Example 7.2.7. We have $\left[x^0\right](1, 2, 3, 4, 5, \ldots) = 1$ and $\left[x^3\right](1, 2, 3, 4, 5, \ldots) = 4$.

Definition 7.2.6 has a tautological consequence: Each FPS $\mathbf{a}$ satisfies

$$\mathbf{a} = \left(\left[x^0\right] \mathbf{a}, \left[x^1\right] \mathbf{a}, \left[x^2\right] \mathbf{a}, \ldots\right). \tag{215}$$

[184] Recall that the notion of a $\mathbb{K}$-algebra homomorphism was introduced in Definition 6.9.5; it means "map that is a ring homomorphism and a $\mathbb{K}$-module homomorphism at the same time".

Thus, an FPS $\mathbf{a}$ is uniquely determined by its coefficients $\left[x^0\right]\mathbf{a}$, $\left[x^1\right]\mathbf{a}$, $\left[x^2\right]\mathbf{a}, \ldots$. Hence, if two FPSs $\mathbf{a}$ and $\mathbf{b}$ satisfy $[x^n]\,\mathbf{a} = [x^n]\,\mathbf{b}$ for all $n \in \mathbb{N}$, then $\mathbf{a} = \mathbf{b}$.

The definition of the sum of two FPSs (Definition 7.2.4 **(a)**) rewrites as follows:

$$[x^n](\mathbf{a}+\mathbf{b}) = [x^n]\,\mathbf{a} + [x^n]\,\mathbf{b} \qquad \text{for all } \mathbf{a},\mathbf{b} \in \mathbb{K}[[x]] \text{ and } n \in \mathbb{N}. \tag{216}$$

(Here, the expression "$[x^n]\,\mathbf{a} + [x^n]\,\mathbf{b}$" should be read as "$([x^n]\,\mathbf{a}) + ([x^n]\,\mathbf{b})$".) Furthermore, the definition of scaling on FPSs (Definition 7.2.4 **(b)**) rewrites as follows:

$$[x^n](\lambda\mathbf{a}) = \lambda \cdot [x^n]\,\mathbf{a} \qquad \text{for all } \lambda \in \mathbb{K} \text{ and } \mathbf{a} \in \mathbb{K}[[x]] \text{ and } n \in \mathbb{N}. \tag{217}$$

Moreover, the definition of the product of two FPSs (Definition 7.2.4 **(c)**) rewrites as follows:

$$\begin{aligned}
[x^n](\mathbf{ab}) &= \sum_{i=0}^{n}\left(\left[x^i\right]\mathbf{a}\right)\cdot\left(\left[x^{n-i}\right]\mathbf{b}\right) && (218)\\
&= \sum_{\substack{i,j\in\mathbb{N};\\ i+j=n}}\left(\left[x^i\right]\mathbf{a}\right)\cdot\left(\left[x^j\right]\mathbf{b}\right) && (219)\\
&= \left(\left[x^0\right]\mathbf{a}\right)\cdot([x^n]\,\mathbf{b}) + \left(\left[x^1\right]\mathbf{a}\right)\cdot\left(\left[x^{n-1}\right]\mathbf{b}\right) + \cdots + ([x^n]\,\mathbf{a})\cdot\left(\left[x^0\right]\mathbf{b}\right)\\
&\qquad \text{for all } \mathbf{a},\mathbf{b} \in \mathbb{K}[[x]] \text{ and } n \in \mathbb{N}.
\end{aligned}$$

Thus, any $\mathbf{a},\mathbf{b} \in \mathbb{K}[[x]]$ and $n \in \mathbb{N}$ satisfy

$$\begin{aligned}
[x^n](\mathbf{ab}) &= \sum_{i=0}^{n}\left(\left[x^i\right]\mathbf{a}\right)\cdot\left(\left[x^{n-i}\right]\mathbf{b}\right)\\
&= \sum_{j=0}^{n}\left(\left[x^{n-j}\right]\mathbf{a}\right)\cdot\left(\left[x^j\right]\mathbf{b}\right) && (220)
\end{aligned}$$

(here, we have substituted $n-j$ for i in the sum). Applying (218) to $n=0$, we conclude that

$$\begin{aligned}
\left[x^0\right](\mathbf{ab}) &= \sum_{i=0}^{0}\left(\left[x^i\right]\mathbf{a}\right)\cdot\left(\left[x^{0-i}\right]\mathbf{b}\right) = \left(\left[x^0\right]\mathbf{a}\right)\cdot\left(\left[x^{0-0}\right]\mathbf{b}\right)\\
&= \left(\left[x^0\right]\mathbf{a}\right)\cdot\left(\left[x^0\right]\mathbf{b}\right) && (221)
\end{aligned}$$

for all $\mathbf{a},\mathbf{b} \in \mathbb{K}[[x]]$. (But of course, $[x^n](\mathbf{ab})$ is not generally equal to $([x^n]\,\mathbf{a}) \cdot ([x^n]\,\mathbf{b})$ when $n > 0$.)

Finally, using the Iverson bracket notation (introduced in Exercise 2.17.2), we can rewrite the definition of the constant FPSs $\underline{a}$ (Definition 7.2.4 **(d)**) as follows:

$$\begin{aligned}\left[x^n\right]\left(\underline{a}\right) &= \begin{cases} a, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases} \qquad (222)\\ &= \underbrace{\begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases}}_{=[n=0]} \cdot a \\ &= [n = 0] \cdot a \qquad \text{for all } a \in \mathbb{K} \text{ and } n \in \mathbb{N}. \qquad (223)\end{aligned}$$

We are now ready to prove Theorem 7.2.5:

Proof of Theorem 7.2.5. **(c)** Let $\lambda \in \mathbb{K}$ and $\mathbf{a} \in \mathbb{K}[[x]]$. We must prove that $\lambda\mathbf{a} = \underline{\lambda} \cdot \mathbf{a}$.

Recall that $\underline{\lambda} = (\lambda, 0, 0, 0, 0, \ldots)$, where all entries beyond the first one are zeroes. In other words,

$$\left[x^0\right]\underline{\lambda} = \lambda,$$

and

$$\left[x^n\right]\underline{\lambda} = 0 \qquad \text{for each positive integer } n. \qquad (224)$$

Now, let $n \in \mathbb{N}$. Then, (218) (applied to $\underline{\lambda}$ and $\mathbf{a}$ instead of $\mathbf{a}$ and $\mathbf{b}$) yields

$$\begin{aligned}\left[x^n\right]\left(\underline{\lambda} \cdot \mathbf{a}\right) &= \sum_{i=0}^{n} \left(\left[x^i\right]\underline{\lambda}\right) \cdot \left(\left[x^{n-i}\right]\mathbf{a}\right) \\ &= \underbrace{\left(\left[x^0\right]\underline{\lambda}\right)}_{=\lambda} \cdot \underbrace{\left(\left[x^{n-0}\right]\mathbf{a}\right)}_{=[x^n]\mathbf{a}} + \sum_{i=1}^{n} \underbrace{\left(\left[x^i\right]\underline{\lambda}\right)}_{\substack{=0 \\ \text{(by (224),} \\ \text{applied to } i \text{ instead of } n)}} \cdot \left(\left[x^{n-i}\right]\mathbf{a}\right) \\ &\qquad \left(\text{here, we have split off the addend for } i = 0 \text{ from the sum}\right) \\ &= \lambda \cdot \left[x^n\right]\mathbf{a} + \underbrace{\sum_{i=1}^{n} 0 \cdot \left(\left[x^{n-i}\right]\mathbf{a}\right)}_{=0} = \lambda \cdot \left[x^n\right]\mathbf{a} = \left[x^n\right]\left(\lambda\mathbf{a}\right) \qquad \left(\text{by (217)}\right).\end{aligned}$$

Since we have proven this for each $n \in \mathbb{N}$, we conclude that $\underline{\lambda} \cdot \mathbf{a} = \lambda\mathbf{a}$. This proves Theorem 7.2.5 **(c)**.

(a) We need to verify:

- the ring axioms,
- the module axioms,
- the "Scale-invariance of multiplication" axiom from Definition 6.9.1;
- the "Commutativity of multiplication" axiom.

Most of these verifications are easy and straightforward.[185] Let us only check associativity of multiplication (since this is the hardest one):

Let $\mathbf{a},\mathbf{b},\mathbf{c} \in \mathbb{K}\left[\left[x\right]\right]$. We must prove that $\mathbf{a}\left(\mathbf{bc}\right) = \left(\mathbf{ab}\right)\mathbf{c}$. In order to do so, we shall prove that $\left[x^n\right]\left(\mathbf{a}\left(\mathbf{bc}\right)\right) = \left[x^n\right]\left(\left(\mathbf{ab}\right)\mathbf{c}\right)$ for each $n \in \mathbb{N}$. (This is sufficient, because an FPS is uniquely determined by its coefficients.)

Let $n \in \mathbb{N}$. Consider the two equalities

$$\begin{aligned}\left[x^n\right]\left(\mathbf{a}\left(\mathbf{bc}\right)\right) &= \sum_{i=0}^{n} \left(\left[x^i\right]\mathbf{a}\right) \cdot \underbrace{\left(\left[x^{n-i}\right]\left(\mathbf{bc}\right)\right)}_{\substack{=\sum_{j=0}^{n-i}\left(\left[x^{n-i-j}\right]\mathbf{b}\right)\cdot\left(\left[x^j\right]\mathbf{c}\right) \\ \text{(by (220), applied to } n-j\text{, } \mathbf{b} \text{ and } \mathbf{c} \\ \text{instead of } n\text{, } \mathbf{a} \text{ and } \mathbf{b}\text{)}}} \\ &\qquad \left(\text{by (218), applied to } \mathbf{bc} \text{ instead of } \mathbf{b}\right) \\ &= \sum_{i=0}^{n} \left(\left[x^i\right]\mathbf{a}\right) \cdot \sum_{j=0}^{n-i} \left(\left[x^{n-i-j}\right]\mathbf{b}\right) \cdot \left(\left[x^j\right]\mathbf{c}\right) \\ &= \sum_{i=0}^{n}\sum_{j=0}^{n-i} \left(\left[x^i\right]\mathbf{a}\right) \cdot \left(\left[x^{n-i-j}\right]\mathbf{b}\right) \cdot \left(\left[x^j\right]\mathbf{c}\right)\end{aligned}$$

and

$$\begin{aligned}\left[x^n\right]\left(\left(\mathbf{ab}\right)\mathbf{c}\right) &= \sum_{j=0}^{n} \underbrace{\left(\left[x^{n-j}\right]\left(\mathbf{ab}\right)\right)}_{\substack{=\sum_{i=0}^{n-j}\left(\left[x^i\right]\mathbf{a}\right)\cdot\left(\left[x^{n-j-i}\right]\mathbf{b}\right) \\ \text{(by (218), applied to } n-j \\ \text{instead of } n\text{)}}} \cdot \left(\left[x^j\right]\mathbf{c}\right) \\ &\qquad \left(\text{by (220), applied to } \mathbf{ab} \text{ and } \mathbf{c} \text{ instead of } \mathbf{a} \text{ and } \mathbf{b}\right) \\ &= \sum_{j=0}^{n}\sum_{i=0}^{n-j} \left(\left[x^i\right]\mathbf{a}\right) \cdot \left(\left[x^{n-j-i}\right]\mathbf{b}\right) \cdot \left(\left[x^j\right]\mathbf{c}\right).\end{aligned}$$

The right hand sides of these two equalities are equal, since we have the following equality of summation signs:

$$\sum_{i=0}^{n}\sum_{j=0}^{n-i} = \sum_{\substack{i,j\in\mathbb{N};\\ i+j\leq n}} = \sum_{j=0}^{n}\sum_{i=0}^{n-j} \tag{225}$$

[186] (and since we have $n-i-j = n-j-i$ for all $i,j \in \mathbb{N}$). Thus, the left hand sides of these two equalities are equal as well. In other words, $\left[x^n\right]\left(\mathbf{a}\left(\mathbf{bc}\right)\right) = \left[x^n\right]\left(\left(\mathbf{ab}\right)\mathbf{c}\right)$.

[185] Theorem 7.2.5 **(c)** helps in proving the "Annihilation" and "neutrality of one" axioms.

[186] An "equality of summation signs" is a statement of the form "$A = B$", where A and B are "summation operators" (i.e., summation signs or compositions of several summation signs). It

Forget that we fixed n. Thus, we have shown that $[x^n]\left(\mathbf{a}\left(\mathbf{bc}\right)\right) = [x^n]\left(\left(\mathbf{ab}\right)\mathbf{c}\right)$ for each $n \in \mathbb{N}$. In other words, $\mathbf{a}\left(\mathbf{bc}\right) = \left(\mathbf{ab}\right)\mathbf{c}$.

Thus, associativity of multiplication is proven for $\mathbb{K}[[x]]$. All the remaining axioms to be proven are easier but follow from similar reasoning. The "Existence of additive inverses" axiom follows by recognizing $(-a_0, -a_1, -a_2, \ldots)$ as the additive inverse of the FPS $(a_0, a_1, a_2, \ldots)$. Thus, Theorem 7.2.5 **(a)** is proven.

(b) This follows easily from the fact (noticed in the proof of part **(a)**) that $(-a_0, -a_1, -a_2, \ldots)$ is the additive inverse of any FPS $(a_0, a_1, a_2, \ldots)$.

(d) We need to prove that

$$\underline{a} + \underline{b} = \underline{a+b} \qquad \text{and} \qquad \underline{a} \cdot \underline{b} = \underline{ab} \qquad \text{for all } a, b \in \mathbb{K},$$

that $\lambda \underline{a} = \underline{\lambda a}$ for all $\lambda \in \mathbb{K}$ and $a \in \mathbb{K}$, and that $\underline{0} = 0_{\mathbb{K}[[x]]}$ and $\underline{1} = 1_{\mathbb{K}[[x]]}$. Most of these claims follow easily from the definitions. The $\underline{a} \cdot \underline{b} = \underline{ab}$ claim follows easily from Theorem 7.2.5 **(c)** (applied to $\lambda = a$ and $\mathbf{a} = \underline{b}$). □

Convention 7.2.8. From now on, we shall identify each $a \in \mathbb{K}$ with the FPS $\underline{a} = (a, 0, 0, 0, \ldots) \in \mathbb{K}[[x]]$.

This identification is harmless, due to Theorem 7.2.5 **(d)** and to the fact that the map

$$\begin{aligned} \iota : \mathbb{K} &\to \mathbb{K}[[x]], \\ a &\mapsto \underline{a} \end{aligned}$$

has to be understood as claiming that the summation signs A and B have "the same effect" (i.e., whatever family of elements of $\mathbb{K}$ you apply them to, you will get the same result by applying A as you will get by applying B). For instance, the equality (225) is claiming that if $a_{i,j}$ is an element of $\mathbb{K}$ for each pair $(i,j) \in \mathbb{N}^2$ satisfying $i + j \leq n$, then

$$\sum_{i=0}^{n}\sum_{j=0}^{n-i} a_{i,j} = \sum_{\substack{i,j\in\mathbb{N};\\ i+j\leq n}} a_{i,j} = \sum_{j=0}^{n}\sum_{i=0}^{n-j} a_{i,j}.$$

(And this is fairly easy to prove: The first equality sign follows from

$$\begin{aligned} \sum_{\substack{i,j\in\mathbb{N};\\ i+j\leq n}} a_{i,j} &= \sum_{i\in\mathbb{N}} \sum_{\substack{j\in\mathbb{N};\\ i+j\leq n}} a_{i,j} = \sum_{i=0}^{n} \underbrace{\sum_{\substack{j\in\mathbb{N};\\ i+j\leq n}}}_{=\sum_{j=0}^{n-i}} a_{i,j} + \sum_{i=n+1}^{\infty} \underbrace{\sum_{\substack{j\in\mathbb{N};\\ i+j\leq n}} a_{i,j}}_{\substack{=(\text{empty sum})\\ (\text{since there exists no } j\in\mathbb{N}\\ \text{satisfying } i+j\leq n \text{ (because } i>n))}} \\ &= \sum_{i=0}^{n}\sum_{j=0}^{n-i} a_{i,j} + \sum_{i=n+1}^{\infty} \underbrace{(\text{empty sum})}_{=0} = \sum_{i=0}^{n}\sum_{j=0}^{n-i} a_{i,j} + \underbrace{\sum_{i=n+1}^{\infty} 0}_{=0} = \sum_{i=0}^{n}\sum_{j=0}^{n-i} a_{i,j}. \end{aligned}$$

The second equality sign follows from a similar argument, but with the roles of i and j swapped.)

is injective (since $a = \left[x^0\right]\left(\underline{a}\right)$ for all $a \in \mathbb{K}$). Note that if $a \in \mathbb{K}$, then the FPS $\underline{a}$ is actually a polynomial (since $\underline{a} = (a, 0, 0, 0, 0, \ldots)$ has at most one nonzero entry), i.e., belongs to $\mathbb{K}[x]$.

The identification we have made in Convention 7.2.8 turns $\mathbb{K}$ into a subset of $\mathbb{K}[[x]]$, and more precisely into a $\mathbb{K}$-subalgebra of $\mathbb{K}[[x]]$ (by Theorem 7.2.5 **(d)**).

Theorem 7.2.5 shows that $\mathbb{K}[[x]]$ is a $\mathbb{K}$-algebra and a commutative ring, so that differences, powers, finite sums, and finite products of FPSs are well-defined. But more can be said. Indeed, sometimes, infinite sums of FPSs make sense. For example, it is reasonable to write

$$\begin{aligned}
&\ (1, 1, 1, 1, 1, \ldots) \\
&+ (0, 1, 1, 1, 1, \ldots) \\
&+ (0, 0, 1, 1, 1, \ldots) \\
&+ (0, 0, 0, 1, 1, \ldots) \\
&+ (0, 0, 0, 0, 1, \ldots) \\
&+ \cdots \\
&= (1, 2, 3, 4, 5, \ldots),
\end{aligned}$$

even though the sum on the left hand side has infinitely many nonzero[187] addends! The addition of $\mathbb{K}[[x]]$ is entrywise, so it stands to reason that infinite sums of FPSs should be defined entrywise as well, and whenever such entrywise sums are well-defined, it makes sense to call them the sum of the FPSs. Thus, we make the following definition:

Definition 7.2.9. A (possibly infinite) family $(\mathbf{a}_i)_{i \in I}$ of FPSs (where I is an arbitrary set) is called *summable* if for each $n \in \mathbb{N}$, the following requirement holds:

$$\text{only finitely many } i \in I \text{ satisfy } \left[x^n\right](\mathbf{a}_i) \neq 0. \tag{226}$$

In this case, the *sum* $\sum\limits_{i \in I} \mathbf{a}_i$ of the family $(\mathbf{a}_i)_{i \in I}$ is defined as the FPS whose coefficients are given by

$$\left[x^n\right]\left(\sum_{i \in I} \mathbf{a}_i\right) = \sum_{i \in I} \left[x^n\right](\mathbf{a}_i) \qquad \text{for all } n \in \mathbb{N}.$$

(The sum on the right hand side of this equality is well-defined in $\mathbb{K}$, since it is a sum with only finitely many nonzero addends.)

We notice that the condition (226) is **not** equivalent to saying "infinitely many $i \in I$ satisfy $\left[x^n\right](\mathbf{a}_i) = 0$".

[187] As usual, "nonzero" means "different from $0_{\mathbb{K}[[x]]} = (0, 0, 0, 0, \ldots)$".

Remark 7.2.10. If you work in constructive logic, you should read the condition (226) as "all but finitely many $i \in I$ satisfy $[x^n](\mathbf{a}_i) = 0$" (that is, "there exists a finite subset S of I such that each $i \in I \setminus S$ satisfies $[x^n](\mathbf{a}_i) = 0$").

Proposition 7.2.11. Sums of summable families of FPSs satisfy the usual rules for summation, as long as all families involved are summable. For example:

- If $(\mathbf{a}_i)_{i\in I}$ and $(\mathbf{b}_i)_{i\in I}$ are two summable families of FPSs, then the family $(\mathbf{a}_i + \mathbf{b}_i)_{i\in I}$ is summable as well and its sum is
$$\sum_{i\in I} (\mathbf{a}_i + \mathbf{b}_i) = \sum_{i\in I} \mathbf{a}_i + \sum_{i\in I} \mathbf{b}_i.$$
- If $(\mathbf{a}_i)_{i\in I}$ is a summable family of FPSs, and if J is a subset of I, then the families $(\mathbf{a}_i)_{i\in J}$ and $(\mathbf{a}_i)_{i\in I\setminus J}$ are summable as well and we have
$$\sum_{i\in I} \mathbf{a}_i = \sum_{i\in J} \mathbf{a}_i + \sum_{i\in I\setminus J} \mathbf{a}_i.$$
- The family $(0)_{i\in I}$ (where 0 stands for the FPS $0_{\mathbb{K}[[x]]}$) is always summable (no matter how large I is), and its sum is $\sum_{i\in I} 0 = 0$.
- If $(\mathbf{a}_{i,j})_{(i,j)\in I\times J}$ is a summable family of FPSs indexed by **pairs** $(i,j) \in I \times J$, then
$$\sum_{i\in I} \sum_{j\in J} \mathbf{a}_{i,j} = \sum_{(i,j)\in I\times J} \mathbf{a}_{i,j} = \sum_{j\in J} \sum_{i\in I} \mathbf{a}_{i,j}. \qquad (227)$$

Remark 7.2.12. Caveat: The equality (227) implies, in particular, that the summation signs $\sum\limits_{i\in I}$ and $\sum\limits_{j\in J}$ can be interchanged. However, the condition that the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is summable is needed for this! If we drop this condition, and merely require the (weaker!) condition that all the families $\left(\mathbf{a}_{i,j}\right)_{j\in J}$ (for each fixed i), $\left(\mathbf{a}_{i,j}\right)_{i\in I}$ (for each fixed j), $\left(\sum\limits_{j\in J}\mathbf{a}_{i,j}\right)_{i\in I}$ and $\left(\sum\limits_{i\in I}\mathbf{a}_{i,j}\right)_{j\in J}$ are summable, then the equality

$$\sum_{i\in I}\sum_{j\in J}\mathbf{a}_{i,j}=\sum_{j\in J}\sum_{i\in I}\mathbf{a}_{i,j} \qquad (228)$$

may be false. For an example where it is false, consider the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ with $I=\{1,2,3,\ldots\}$ and $J=\{1,2,3,\ldots\}$ and $\mathbf{a}_{i,j}$ given by the following table:

$\mathbf{a}_{i,j}$	1	2	3	4	5	$\cdots$
1	1	-1				$\cdots$
2		1	-1			$\cdots$
3			1	-1		$\cdots$
4				1	-1	$\cdots$
5					1	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

(where all the entries not shown are 0). Note that the elements of this family belong to $\mathbb{K}$, and thus can be considered as FPSs via Convention 7.2.8. For this specific family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$, the equality (228) rewrites as $0=1$, which is not a good sign. But this does not contradict the rule (227), since the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is not summable (it contains infinitely many 1's).

The upshot of this caveat is that if you want to interchange two summation signs as in (228), you must check not only that the sums involved are all well-defined, but also that the sum $\sum\limits_{(i,j)\in I\times J}\mathbf{a}_{i,j}$ is well-defined (i.e., the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is summable). This is automatically satisfied when the sets I and J are finite, but in the case of infinite sets can be a serious restriction as we have just seen.

Proof of Proposition 7.2.11 (sketched). This is boring yet fairly straightforward: Each of these rules can be derived from the analogous rule for **finite** sums, once you fix an $n\in\mathbb{N}$ and look at the x^n-coefficients on both sides of the rule.

For example, let us prove the rule (227). Assume that $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is a summable family of FPSs indexed by **pairs** $(i,j)\in I\times J$. Fix $n\in\mathbb{N}$. Then, only finitely many $(i,j)\in I\times J$

satisfy $[x^n]\left(\mathbf{a}_{i,j}\right) \neq 0$ (since the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is summable). In other words, there exists a finite subset S of $I \times J$ such that

$$\text{all } (i,j) \in (I\times J) \setminus S \text{ satisfy } [x^n]\left(\mathbf{a}_{i,j}\right) = 0. \tag{229}$$

Consider this S. (Note that S can depend on n.)

Let I' be the subset $\{i \mid (i,j) \in S\}$ of I. Let J' be the subset $\{j \mid (i,j) \in S\}$ of J. Both of these subsets I' and J' are finite (since S is finite). Moreover, $I' \times J' \subseteq I \times J$ (since $I' \subseteq I$ and $J' \subseteq J$) and $S \subseteq I' \times J'$ [188]. Thus, if a pair $(i,j) \in I \times J$ satisfies $(i,j) \notin I' \times J'$, then it must also satisfy $(i,j) \notin S$ [189] and therefore $(i,j) \in (I\times J)\setminus S$ (since $(i,j) \in I \times J$ and $(i,j) \notin S$) and therefore

$$[x^n]\left(\mathbf{a}_{i,j}\right) = 0 \tag{230}$$

(by (229)).

The sets I' and J' are finite. Hence, Fubini's theorem for finite sums (see, e.g., [Grinbe15, §1.4.2, "Fubini's theorem"]) yields

$$\sum_{i\in I'}\sum_{j\in J'} [x^n]\left(\mathbf{a}_{i,j}\right) = \sum_{(i,j)\in I'\times J'} [x^n]\left(\mathbf{a}_{i,j}\right) = \sum_{j\in J'}\sum_{i\in I'} [x^n]\left(\mathbf{a}_{i,j}\right). \tag{231}$$

The sum $\sum\limits_{(i,j)\in I\times J} [x^n]\left(\mathbf{a}_{i,j}\right)$ is well-defined (since only finitely many $(i,j) \in I \times J$ satisfy $[x^n]\left(\mathbf{a}_{i,j}\right) \neq 0$). Hence,

$$\begin{aligned}
\sum_{(i,j)\in I\times J} [x^n]\left(\mathbf{a}_{i,j}\right) &= \underbrace{\sum_{\substack{(i,j)\in I\times J;\\ (i,j)\in I'\times J'}}}_{\substack{=\sum\limits_{(i,j)\in I'\times J'} \\ (\text{since } I'\times J'\subseteq I\times J)}} [x^n]\left(\mathbf{a}_{i,j}\right) + \sum_{\substack{(i,j)\in I\times J;\\ (i,j)\notin I'\times J'}} \underbrace{[x^n]\left(\mathbf{a}_{i,j}\right)}_{\substack{=0\\ (\text{by } (230))}} \\
&\qquad \left(\begin{array}{c}\text{since each } (i,j)\in I\times J \text{ satisfies either } (i,j)\in I'\times J' \\ \text{or } (i,j)\notin I'\times J' \text{ (but never both at the same time)}\end{array}\right) \\
&= \sum_{(i,j)\in I'\times J'} [x^n]\left(\mathbf{a}_{i,j}\right) + \underbrace{\sum_{\substack{(i,j)\in I\times J;\\ (i,j)\notin I'\times J'}} 0}_{=0} = \sum_{(i,j)\in I'\times J'} [x^n]\left(\mathbf{a}_{i,j}\right) \\
&= \sum_{i\in I'}\sum_{j\in J'} [x^n]\left(\mathbf{a}_{i,j}\right)
\end{aligned} \tag{232}$$

(by (231)).

[188] *Proof.* Let $s \in S$. Then, $s \in S \subseteq I \times J$; thus, we can write s in the form $s = (u,v)$ for some $u \in I$ and $v \in J$. Consider these u and v. We have $(u,v) = s \in S$. Hence, u has the form i for some $(i,j) \in S$ (namely, for $(i,j) = (u,v)$). Thus, $u \in \{i \mid (i,j) \in S\} = I'$ (since I' was defined as $\{i \mid (i,j) \in S\}$). Similarly, $v \in J'$. From $u \in I'$ and $v \in J'$, we obtain $(u,v) \in I' \times J'$. Hence, $s = (u,v) \in I' \times J'$.

Now, forget that we fixed s. We thus have shown that $s \in I' \times J'$ for each $s \in S$. In other words, $S \subseteq I' \times J'$.

[189] since otherwise, it would satisfy $(i,j) \in S \subseteq I' \times J'$, which would contradict $(i,j) \notin I' \times J'$

Moreover, if $i \in I$, then the sum $\sum\limits_{j \in J} [x^n] \left(\mathbf{a}_{i,j}\right)$ is well-defined and satisfies

$$\sum_{j \in J} [x^n] \left(\mathbf{a}_{i,j}\right) = \sum_{j \in J'} [x^n] \left(\mathbf{a}_{i,j}\right). \tag{233}$$

[*Proof:* Let $i \in I$. If $j \in J$ satisfies $j \notin J'$, then $(i,j) \notin I' \times J'$ (since $j \notin J'$) and thus $[x^n] \left(\mathbf{a}_{i,j}\right) = 0$ (by (230)). Thus, all but finitely many $j \in J$ satisfy $[x^n] \left(\mathbf{a}_{i,j}\right) = 0$ (since all but finitely many $j \in J$ satisfy $j \notin J'$ (because the set J' is finite)). In other words, only finitely many $j \in J$ satisfy $[x^n] \left(\mathbf{a}_{i,j}\right) \neq 0$. Therefore, the sum $\sum\limits_{j \in J} [x^n] \left(\mathbf{a}_{i,j}\right)$ is well-defined (having only finitely many nonzero addends). Moreover, each $j \in J$ satisfies either $j \in J'$ or $j \notin J'$ (but not both at once); thus,

$$\begin{aligned}\sum_{j \in J} [x^n] \left(\mathbf{a}_{i,j}\right) &= \underbrace{\sum_{\substack{j \in J; \\ j \in J'}}}_{\substack{= \sum\limits_{j \in J'} \\ (\text{since } J' \subseteq J)}} [x^n] \left(\mathbf{a}_{i,j}\right) + \sum_{\substack{j \in J; \\ j \notin J'}} \underbrace{[x^n] \left(\mathbf{a}_{i,j}\right)}_{\substack{=0 \\ (\text{by (230) (since } j \notin J' \\ \text{leads to } (i,j) \notin I' \times J'))}} = \sum_{j \in J'} [x^n] \left(\mathbf{a}_{i,j}\right) + \underbrace{\sum_{\substack{j \in J; \\ j \notin J'}} 0}_{=0} \\ &= \sum_{j \in J'} [x^n] \left(\mathbf{a}_{i,j}\right).\end{aligned}$$

This proves (233).]

Furthermore, if $i \in I$ satisfies $i \notin I'$, then

$$\sum_{j \in J} \underbrace{[x^n] \left(\mathbf{a}_{i,j}\right)}_{\substack{=0 \\ (\text{by (230) (since } i \notin I' \\ \text{leads to } (i,j) \notin I' \times J'))}} = \sum_{j \in J} 0 = 0.$$

Thus, all but finitely many $i \in I$ satisfy $\sum\limits_{j \in J} [x^n] \left(\mathbf{a}_{i,j}\right) = 0$ (since all but finitely many $i \in I$ satisfy $i \notin I'$ (because the set I' is finite)). In other words, only finitely many $i \in I$ satisfy $\sum\limits_{j \in J} [x^n] \left(\mathbf{a}_{i,j}\right) \neq 0$. Therefore, the sum $\sum\limits_{i \in I} \sum\limits_{j \in J} [x^n] \left(\mathbf{a}_{i,j}\right)$ is well-defined (having only finitely many nonzero addends). Moreover, each $i \in I$ satisfies either $i \in I'$ or $i \notin I'$ (but not both at once); thus,

$$\begin{aligned}\sum_{i \in I} \sum_{j \in J} [x^n] \left(\mathbf{a}_{i,j}\right) &= \underbrace{\sum_{\substack{i \in I; \\ i \in I'}}}_{\substack{= \sum\limits_{i \in I'} \\ (\text{since } I' \subseteq I)}} \underbrace{\sum_{j \in J} [x^n] \left(\mathbf{a}_{i,j}\right)}_{\substack{= \sum\limits_{j \in J'} [x^n]\left(\mathbf{a}_{i,j}\right) \\ (\text{by (233)})}} + \sum_{\substack{i \in I; \\ i \notin I'}} \sum_{j \in J} \underbrace{[x^n] \left(\mathbf{a}_{i,j}\right)}_{\substack{=0 \\ (\text{by (230) (since } i \notin I' \\ \text{leads to } (i,j) \notin I' \times J'))}} \\ &= \sum_{i \in I'} \sum_{j \in J'} [x^n] \left(\mathbf{a}_{i,j}\right) + \underbrace{\sum_{\substack{i \in I; \\ i \notin I'}} \sum_{j \in J} 0}_{=0} = \sum_{i \in I'} \sum_{j \in J'} [x^n] \left(\mathbf{a}_{i,j}\right).\end{aligned}$$

Comparing this with (232), we obtain

$$\sum_{i \in I} \sum_{j \in J} [x^n] \left(\mathbf{a}_{i,j}\right) = \sum_{(i,j) \in I \times J} [x^n] \left(\mathbf{a}_{i,j}\right). \tag{234}$$

Now, forget that we fixed n. We thus have proven the equality (234) for each $n \in \mathbb{N}$. We have also proven that all the sums appearing in this equality are well-defined (having only finitely many nonzero addends).

It is now easy to see that for each $i \in I$, the family $\left(\mathbf{a}_{i,j}\right)_{j\in J}$ of FPSs is summable[190], and therefore the sum $\sum\limits_{j\in J} \mathbf{a}_{i,j}$ is well-defined. Moreover, the family $\left(\sum\limits_{j\in J} \mathbf{a}_{i,j}\right)_{i\in I}$ of FPSs is summable[191]. Hence, the sum $\sum\limits_{i\in I}\sum\limits_{j\in J} \mathbf{a}_{i,j}$ is well-defined. Finally, recall that the sum of a summable family of FPSs is defined entrywise; thus, for each $n \in \mathbb{N}$, we have

$$\begin{aligned}\left[x^n\right]\left(\sum_{i\in I}\sum_{j\in J}\mathbf{a}_{i,j}\right) &= \sum_{i\in I}\underbrace{\left[x^n\right]\left(\sum_{j\in J}\mathbf{a}_{i,j}\right)}_{=\sum\limits_{j\in J}\left[x^n\right]\left(\mathbf{a}_{i,j}\right)} = \sum_{i\in I}\sum_{j\in J}\left[x^n\right]\left(\mathbf{a}_{i,j}\right) = \sum_{(i,j)\in I\times J}\left[x^n\right]\left(\mathbf{a}_{i,j}\right) \qquad \text{(by (234))}\\ &= \left[x^n\right]\left(\sum_{(i,j)\in I\times J}\mathbf{a}_{i,j}\right).\end{aligned}$$

In other words, each entry of the FPS $\sum\limits_{i\in I}\sum\limits_{j\in J}\mathbf{a}_{i,j}$ equals the corresponding entry of the FPS $\sum\limits_{(i,j)\in I\times J}\mathbf{a}_{i,j}$. Thus, these two FPSs are identical. In other words, $\sum\limits_{i\in I}\sum\limits_{j\in J}\mathbf{a}_{i,j} = \sum\limits_{(i,j)\in I\times J}\mathbf{a}_{i,j}$. This proves the first equality sign of (227). The second equality sign of (227) is proven similarly (but with the roles of I and J interchanged). □

We shall use standard notations for infinite sums over certain subsets of $\mathbb{Z}$. For instance, the summation sign "$\sum\limits_{i=0}^{\infty}$" shall mean "$\sum\limits_{i\in\mathbb{N}}$"; more generally, if $a \in \mathbb{Z}$, then the summation sign "$\sum\limits_{i=a}^{\infty}$" shall mean "$\sum\limits_{i\in\{a,a+1,a+2,\ldots\}}$". Also, the summation sign "$\sum\limits_{i>0}$" shall mean "$\sum\limits_{i=1}^{\infty}$", which is the same as "$\sum\limits_{i\in\{1,2,3,\ldots\}}$".

[190] *Proof.* Fix $i \in I$. For each $n \in \mathbb{N}$, the sum $\sum\limits_{j\in J}\left[x^n\right]\left(\mathbf{a}_{i,j}\right)$ has only finitely many nonzero addends (as we have proven above). In other words, for each $n \in \mathbb{N}$, only finitely many $j \in J$ satisfy $\left[x^n\right]\left(\mathbf{a}_{i,j}\right) \neq 0$. In other words, the family $\left(\mathbf{a}_{i,j}\right)_{j\in J}$ of FPSs is summable (by the definition of "summable").

[191] *Proof.* For each $n \in \mathbb{N}$, only finitely many $i \in I$ satisfy $\sum\limits_{j\in J}\left[x^n\right]\left(\mathbf{a}_{i,j}\right) \neq 0$ (as we have proven above). In other words, for each $n \in \mathbb{N}$, only finitely many $i \in I$ satisfy $\left[x^n\right]\left(\sum\limits_{j\in J}\mathbf{a}_{i,j}\right) \neq 0$ (since $\left[x^n\right]\left(\sum\limits_{j\in J}\mathbf{a}_{i,j}\right) = \sum\limits_{j\in J}\left[x^n\right]\left(\mathbf{a}_{i,j}\right)$). In other words, the family $\left(\sum\limits_{j\in J}\mathbf{a}_{i,j}\right)_{i\in I}$ of FPSs is summable (by the definition of "summable").

Definition 7.2.13. We let x denote the FPS $\left(0, 1, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}}\right)$.

Thus, we have

$$\left[x^1\right] x = 1, \qquad \text{and} \tag{235}$$

$$\left[x^n\right] x = 0 \qquad \text{for all } n \in \mathbb{N} \text{ satisfying } n \neq 1. \tag{236}$$

In other words, for all $n \in \mathbb{N}$, we have

$$\left[x^n\right] x = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n \neq 1 \end{cases} \tag{237}$$

$$= \underbrace{\begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n \neq 1 \end{cases}}_{=[n=1]} \cdot 1_{\mathbb{K}} = [n = 1] \cdot 1_{\mathbb{K}} \tag{238}$$

(using the Iverson bracket notation).

Lemma 7.2.14. Let $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]]$ be an FPS. Then,

$$x (a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots).$$

In other words, Lemma 7.2.14 says that multiplying an FPS by x shifts all entries of the FPS to the right by 1 step, while filling the now-empty 0-th slot with a 0.

Proof of Lemma 7.2.14. We have $x = \left(0, 1, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}}\right)$ and therefore

$$x (a_0, a_1, a_2, \ldots) = \left(0, 1, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}}\right) (a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots),$$

where the last equality sign can easily be obtained from the definition of the multiplication on $\mathbb{K}[[x]]$.

Here is a more rigorous way of writing down this argument: Applying (236) to $n = 0$, we find $\left[x^0\right] x = 0$ (since $0 \neq 1$). Applying (218) to $n = 0$, $\mathbf{a} = x$ and $\mathbf{b} = (a_0, a_1, a_2, \ldots)$, we obtain

$$\begin{aligned} \left[x^0\right] (x (a_0, a_1, a_2, \ldots)) &= \sum_{i=0}^{0} \left(\left[x^i\right] x\right) \cdot \left(\left[x^{0-i}\right] (a_0, a_1, a_2, \ldots)\right) \\ &= \underbrace{\left(\left[x^0\right] x\right)}_{=0} \cdot \left(\left[x^{0-0}\right] (a_0, a_1, a_2, \ldots)\right) = 0. \end{aligned}$$

In other words, the first entry of the sequence $x\left(a_0, a_1, a_2, \ldots\right)$ is 0. Moreover, if n is a positive integer, then (218) (applied to $\mathbf{a} = x$ and $\mathbf{b} = \left(a_0, a_1, a_2, \ldots\right)$) yields

$$\begin{aligned}
&\left[x^n\right]\left(x\left(a_0, a_1, a_2, \ldots\right)\right) \\
&= \sum_{i=0}^{n} \left(\left[x^i\right] x\right) \cdot \underbrace{\left(\left[x^{n-i}\right]\left(a_0, a_1, a_2, \ldots\right)\right)}_{\substack{=a_{n-i} \\ \text{(by the definition of } \left[x^{n-i}\right]\mathbf{a} \text{ for } \mathbf{a} \in \mathbb{K}[[x]])}} = \sum_{i=0}^{n} \left(\left[x^i\right] x\right) \cdot a_{n-i} \\
&= \underbrace{\left(\left[x^1\right] x\right)}_{\substack{=1 \\ \text{(by (235))}}} \cdot a_{n-1} + \sum_{\substack{i \in \{0,1,\ldots,n\}; \\ i \neq 1}} \underbrace{\left(\left[x^i\right] x\right)}_{\substack{=0 \\ \text{(by (236) (applied} \\ \text{to } i \text{ instead of } n\text{), since } i \neq 1)}} \cdot a_{n-i} \\
&\qquad \left(\begin{array}{c} \text{here, we have split off the addend for } i = 1 \\ \text{from the sum, since } 1 \in \{0, 1, \ldots, n\} \end{array}\right) \\
&= a_{n-1} + \underbrace{\sum_{\substack{i \in \{0,1,\ldots,n\}; \\ i \neq 1}} 0 \cdot a_{n-i}}_{=0} = a_{n-1}.
\end{aligned}$$

In other words, the entries of the sequence $x\left(a_0, a_1, a_2, \ldots\right)$ after the first entry are $a_0, a_1, a_2, \ldots$. Since we already know that the first entry of this sequence is 0, we thus conclude that

$$x\left(a_0, a_1, a_2, \ldots\right) = \left(0, a_0, a_1, a_2, \ldots\right).$$

Thus, Lemma 7.2.14 is proven. □

Proposition 7.2.15. For each $k \in \mathbb{N}$, we have

$$x^k = \left(\underbrace{0, 0, \ldots, 0}_{k \text{ zeroes}}, 1, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}}\right).$$

Proof of Proposition 7.2.15. Induction on k. The induction base follows by observing that $x^0 = 1_{\mathbb{K}[[x]]} = \underline{1} = (1, 0, 0, 0, \ldots)$.

The induction step uses Lemma 7.2.14 and the equality $x^k = xx^{k-1}$ (which holds for all $k > 0$). □

Proposition 7.2.15 can be restated as follows:

$$\left[x^n\right]\left(x^k\right) = \begin{cases} 1, & \text{if } n = k; \\ 0, & \text{if } n \neq k \end{cases} \qquad \text{for all } n, k \in \mathbb{N}. \tag{239}$$

Corollary 7.2.16. Let $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]]$ be any FPS. Then, the family $(a_k x^k)_{k \in \mathbb{N}}$ is summable, so that the sum $\sum\limits_{k \in \mathbb{N}} a_k x^k$ is well-defined. Moreover,

$$(a_0, a_1, a_2, \ldots) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots = \sum_{k \in \mathbb{N}} a_k x^k.$$

Proof of Corollary 7.2.16. For each $k \in \mathbb{N}$, we have

$$x^k = \left(\underbrace{0, 0, \ldots, 0}_{k \text{ zeroes}}, 1, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}} \right) \qquad \text{(by Proposition 7.2.15)}$$

and thus

$$\begin{aligned} a_k x^k &= a_k \left(\underbrace{0, 0, \ldots, 0}_{k \text{ zeroes}}, 1, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}} \right) \\ &= \left(\underbrace{a_k \cdot 0, a_k \cdot 0, \ldots, a_k \cdot 0}_{k \text{ times}}, a_k \cdot 1, \underbrace{a_k \cdot 0, a_k \cdot 0, a_k \cdot 0, a_k \cdot 0, \ldots}_{\infty \text{ times}} \right) \\ &= \left(\underbrace{0, 0, \ldots, 0}_{k \text{ zeroes}}, a_k, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}} \right) \end{aligned} \tag{240}$$

(since $a_k \cdot 0 = 0$ and $a_k \cdot 1 = a_k$). Hence, for any $k \in \mathbb{N}$ and $n \in \mathbb{N}$, we have $[x^n](a_k x^k) = 0$ unless $k = n$. Thus, for each $n \in \mathbb{N}$, only finitely many $k \in \mathbb{N}$ satisfy $[x^n](a_k x^k) \neq 0$ (namely, only $k = n$ can satisfy this). In other words, the family $(a_k x^k)_{k \in \mathbb{N}}$ is summable (by the definition of "summable"). Hence, the sum

$\sum_{k\in\mathbb{N}} a_k x^k$ is well-defined. Let us now compute this sum:

$$\begin{aligned}
\sum_{k\in\mathbb{N}} \underbrace{a_k x^k}_{\substack{=\left(\underbrace{0,0,\ldots,0}_{k\text{ zeroes}},a_k,\underbrace{0,0,0,0,\ldots}_{\text{zeroes}}\right)\\ \text{(by (240))}}}
&= \sum_{k\in\mathbb{N}} \left(\underbrace{0,0,\ldots,0}_{k\text{ zeroes}},a_k,\underbrace{0,0,0,0,\ldots}_{\text{zeroes}}\right)\\
&= (a_0,0,0,0,0,\ldots)\\
&+ (0,a_1,0,0,0,\ldots)\\
&+ (0,0,a_2,0,0,\ldots)\\
&+ (0,0,0,a_3,0,\ldots)\\
&+ \cdots\\
&= (a_0,a_1,a_2,a_3,\ldots)
\end{aligned}$$

(since addition of FPSs is entrywise). Therefore,

$$\begin{aligned}
(a_0,a_1,a_2,\ldots) = \sum_{k\in\mathbb{N}} a_k x^k &= a_0 x^0 + a_1 x^1 + a_2 x^2 + a_3 x^3 + \cdots\\
&= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots
\end{aligned}$$

(since $a_0 \underbrace{x^0}_{=1} = a_0$ and $a_1 \underbrace{x^1}_{=x} = a_1 x$). Combining these, we conclude that Corollary 7.2.16 holds. □

So now we are justified in computing "formally" with FPSs as if they were infinite sums of powers of x times scalars, because we have now constructed a ring with an actual element x in it and we have shown that these infinite sums are well-defined and just encode the sequences of their coefficients. This is the rigorous answer to the question "what is an indeterminate in a polynomial or FPS". This also explains why we refer to the entries of an FPS $(a_0, a_1, a_2, \ldots)$ as its "coefficients".

Exercise 7.2.1. Let $\mathbf{b} \in \mathbb{K}[[x]]$ and $u, v \in \mathbb{N}$. Prove the following:
(a) If $u \geq v$, then $[x^u](x^v \mathbf{b}) = [x^{u-v}]\mathbf{b}$.
(b) If $u < v$, then $[x^u](x^v \mathbf{b}) = 0$.

Solution to Exercise 7.2.1. **(a)** Assume that $u \geq v$. Then, $v \leq u$, so that $v \in \{0, 1, \ldots, u\}$ (since

$v \in \mathbb{N}$). Now, (218) (applied to $n = u$ and $\mathbf{a} = x^v$) yields

$$\begin{aligned}
\left[x^u\right]\left(x^v \mathbf{b}\right) &= \sum_{i=0}^{u} \underbrace{\left(\left[x^i\right]\left(x^v\right)\right)}_{\substack{=\begin{cases}1, & \text{if } i=v;\\ 0, & \text{if } i \neq v\end{cases}\\ \text{(by (239), applied to } n=i \text{ and } k=v)}} \cdot \left(\left[x^{u-i}\right]\mathbf{b}\right) = \sum_{i=0}^{u} \begin{cases}1, & \text{if } i=v;\\ 0, & \text{if } i \neq v\end{cases} \cdot \left(\left[x^{u-i}\right]\mathbf{b}\right) \\
&= \underbrace{\begin{cases}1, & \text{if } v=v;\\ 0, & \text{if } v \neq v\end{cases}}_{\substack{=1\\ \text{(since } v=v)}} \cdot \left(\left[x^{u-v}\right]\mathbf{b}\right) + \sum_{\substack{i\in\{0,1,\ldots,u\};\\ i\neq v}} \underbrace{\begin{cases}1, & \text{if } i=v;\\ 0, & \text{if } i \neq v\end{cases}}_{\substack{=0\\ \text{(since } i\neq v)}} \cdot \left(\left[x^{u-i}\right]\mathbf{b}\right) \\
&\qquad \left(\begin{array}{c}\text{here, we have split off the addend for } i=v \text{ from the sum,}\\ \text{since } v\in\{0,1,\ldots,u\}\end{array}\right) \\
&= \left[x^{u-v}\right]\mathbf{b} + \underbrace{\sum_{\substack{i\in\{0,1,\ldots,u\};\\ i\neq v}} 0 \cdot \left(\left[x^{u-i}\right]\mathbf{b}\right)}_{=0} = \left[x^{u-v}\right]\mathbf{b}.
\end{aligned}$$

This solves Exercise 7.2.1 **(a)**.

(b) Assume that $u < v$. Then, each $i \in \{0,1,\ldots,u\}$ satisfies $i \neq v$ (since each $i \in \{0,1,\ldots,u\}$ satisfies $i \leq u < v$ and thus $i \neq v$) and therefore

$$\begin{cases}1, & \text{if } i=v;\\ 0, & \text{if } i \neq v\end{cases} = 0. \tag{241}$$

Now, (218) (applied to $n = u$ and $\mathbf{a} = x^v$) yields

$$\begin{aligned}
\left[x^u\right]\left(x^v \mathbf{b}\right) &= \sum_{i=0}^{u} \underbrace{\left(\left[x^i\right]\left(x^v\right)\right)}_{\substack{=\begin{cases}1, & \text{if } i=v;\\ 0, & \text{if } i \neq v\end{cases}\\ \text{(by (239), applied to } n=i \text{ and } k=v)}} \cdot \left(\left[x^{u-i}\right]\mathbf{b}\right) = \sum_{i=0}^{u} \underbrace{\begin{cases}1, & \text{if } i=v;\\ 0, & \text{if } i \neq v\end{cases}}_{\substack{=0\\ \text{(by (241))}}} \cdot \left(\left[x^{u-i}\right]\mathbf{b}\right) \\
&= \sum_{i=0}^{u} 0 \cdot \left(\left[x^{u-i}\right]\mathbf{b}\right) = 0.
\end{aligned}$$

This solves Exercise 7.2.1 **(b)**. □

7.3. Inverses in the ring $\mathbb{K}[[x]]$

7.3.1. The invertibility criterion for power series

The equation (214) is not just an example of multiplying two FPSs. It is also an example of a multiplicative inverse in the ring $\mathbb{K}[[x]]$. Indeed, we can rewrite it as

$$(1-x)\cdot\left(1+x+x^2+x^3+\cdots\right) = \underline{1}$$

(since $\left(1, -1, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) = 1 - x$ and $(1, 1, 1, 1, 1, \ldots) = 1 + x + x^2 + x^3 + \cdots$). Since the ring $\mathbb{K}[[x]]$ is commutative, we also have $(1-x) \cdot \left(1 + x + x^2 + x^3 + \cdots\right) = \left(1 + x + x^2 + x^3 + \cdots\right) \cdot (1-x)$. Thus,

$$(1-x) \cdot \left(1 + x + x^2 + x^3 + \cdots\right) = \left(1 + x + x^2 + x^3 + \cdots\right) \cdot (1-x) = \underline{1}.$$

Since $\underline{1}$ is the unity $1_{\mathbb{K}[[x]]}$ of the ring $\mathbb{K}[[x]]$, we thus conclude that the FPS $1 + x + x^2 + x^3 + \cdots$ is a multiplicative inverse of $1 - x$. Thus, the FPS $1 - x$ is invertible, and its multiplicative inverse is

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots .$$

This, of course, looks exactly like the well-known geometric series formula from analysis, which states that $\dfrac{1}{1-r} = 1 + r + r^2 + r^3 + \cdots$ for each real $r \in (-1, 1)$. But keep in mind that our x is an indeterminate over an arbitrary commutative ring, while the r in the latter formula is a real number between -1 and 1; there are ways to transfer identities between these two worlds, but they are not a-priori the same.

Thus we have seen that $1 - x$ is an invertible FPS. Let us ask a more general question: When is an FPS invertible? Quite often, as it turns out:

Theorem 7.3.1. Let $\mathbf{a} \in \mathbb{K}[[x]]$. Then, $\mathbf{a}$ is invertible (in the ring $\mathbb{K}[[x]]$) if and only if the coefficient $\left[x^0\right] \mathbf{a}$ is invertible in $\mathbb{K}$.

Proof of Theorem 7.3.1. $\Longrightarrow$: Assume that $\mathbf{a}$ is invertible (in the ring $\mathbb{K}[[x]]$). We must prove that the coefficient $\left[x^0\right] \mathbf{a}$ is invertible in $\mathbb{K}$.

The FPS $\mathbf{a}^{-1}$ is well-defined (since $\mathbf{a}$ is invertible) and satisfies $\mathbf{a}\mathbf{a}^{-1} = 1_{\mathbb{K}[[x]]} = \underline{1}$. But (221) (applied to $\mathbf{b} = \mathbf{a}^{-1}$) yields

$$\left[x^0\right] \left(\mathbf{a}\mathbf{a}^{-1}\right) = \left(\left[x^0\right] \mathbf{a}\right) \cdot \left(\left[x^0\right] \left(\mathbf{a}^{-1}\right)\right).$$

Hence,

$$\left(\left[x^0\right] \mathbf{a}\right) \cdot \left(\left[x^0\right] \left(\mathbf{a}^{-1}\right)\right) = \left[x^0\right] \left(\underbrace{\mathbf{a}\mathbf{a}^{-1}}_{=\underline{1}}\right) = \left[x^0\right] \underline{1} = 1.$$

Thus, the element $\left[x^0\right] \left(\mathbf{a}^{-1}\right)$ of $\mathbb{K}$ is a multiplicative inverse of $\left[x^0\right] \mathbf{a}$ (since $\mathbb{K}$ is commutative, so we only need to check the product in one order). Therefore, the element $\left[x^0\right] \mathbf{a}$ of $\mathbb{K}$ has a multiplicative inverse, i.e., is invertible. This proves the "$\Longrightarrow$" direction of Theorem 7.3.1.

$\Longleftarrow$: Assume that the coefficient $\left[x^0\right] \mathbf{a}$ is invertible in $\mathbb{K}$. We must prove that $\mathbf{a}$ is invertible (in the ring $\mathbb{K}[[x]]$).

Write the FPS $\mathbf{a}$ in the form $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ with $a_0, a_1, a_2, \ldots \in \mathbb{K}$. Then, the definition of $\left[x^0\right] \mathbf{a}$ yields $\left[x^0\right] \mathbf{a} = a_0$. Hence, a_0 is invertible in $\mathbb{K}$ (since $\left[x^0\right] \mathbf{a}$ is invertible in $\mathbb{K}$). Thus, we can divide elements of $\mathbb{K}$ by a_0.

Now, we want to find a multiplicative inverse $\mathbf{b}$ of $\mathbf{a}$ in $\mathbb{K}\left[\left[x\right]\right]$.

Let $\mathbf{b} = (b_0, b_1, b_2, \ldots) \in \mathbb{K}\left[\left[x\right]\right]$. We want to see when $\mathbf{b}$ is a multiplicative inverse of $\mathbf{a}$.

From $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ and $\mathbf{b} = (b_0, b_1, b_2, \ldots)$, we obtain

$$\begin{aligned}\mathbf{ab} &= (a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) \\ &= (a_0b_0, \quad a_0b_1 + a_1b_0, \quad a_0b_2 + a_1b_1 + a_2b_0, \quad a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0, \quad \ldots)\end{aligned} \tag{242}$$

(by the definition of the product of two FPSs). On the other hand, the definition of $\underline{1}$ yields

$$\underline{1} = (1, 0, 0, 0, 0, \ldots). \tag{243}$$

Now, by the definition of a multiplicative inverse, we have the following chain of logical equivalences:

$$\begin{aligned}&(\mathbf{b} \text{ is a multiplicative inverse of } \mathbf{a}) \\ \iff &\left(\mathbf{ab} = \mathbf{ba} = 1_{\mathbb{K}[[x]]}\right) \iff (\mathbf{ab} = \mathbf{ba} = \underline{1}) \qquad \left(\text{since } 1_{\mathbb{K}[[x]]} = \underline{1}\right) \\ \iff &(\mathbf{ab} = \underline{1}) \qquad \left(\begin{array}{c}\text{since } \mathbf{ab} = \mathbf{ba} \text{ holds automatically} \\ \text{(because } \mathbb{K}\left[\left[x\right]\right] \text{ is commutative)}\end{array}\right) \\ \iff &((a_0b_0, \quad a_0b_1 + a_1b_0, \quad a_0b_2 + a_1b_1 + a_2b_0, \quad a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0, \quad \ldots) \\ &\qquad = (1, 0, 0, 0, 0, \ldots)) \qquad \text{(by (242) and (243))} \\ \iff &\left(\begin{cases} a_0b_0 = 1; \\ a_0b_1 + a_1b_0 = 0; \\ a_0b_2 + a_1b_1 + a_2b_0 = 0; \\ a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 = 0; \\ \ldots\ldots\ldots\ldots \end{cases}\right).\end{aligned} \tag{244}$$

But if we treat the coefficients $b_0, b_1, b_2, \ldots$ as unknowns[192], then the statement

$$\begin{cases} a_0b_0 = 1; \\ a_0b_1 + a_1b_0 = 0; \\ a_0b_2 + a_1b_1 + a_2b_0 = 0; \\ a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 = 0; \\ \ldots\ldots\ldots\ldots \end{cases} \tag{245}$$

is a system of infinitely many linear equations in these unknowns, and this system can be solved recursively by elimination (thanks to the fact that a_0 is invertible!) as follows:

[192] while $a_0, a_1, a_2, \ldots$, of course, remain givens

- First, solve the first equation $a_0 b_0 = 1$ for b_0, thus obtaining a unique value of b_0 (namely, a_0^{-1}).
- Next, solve the second equation $a_0 b_1 + a_1 b_0 = 0$ for b_1, thus obtaining a unique value of b_1 (namely, $-a_0^{-1}(a_1 b_0)$).
- Next, solve the third equation $a_0 b_2 + a_1 b_1 + a_2 b_0 = 0$ for b_2, thus obtaining a unique value of b_2 (namely, $-a_0^{-1}(a_1 b_1 + a_2 b_0)$).
- And so on, obtaining a value for each of $b_0, b_1, b_2, \ldots$ eventually.

We thus have found a sequence $(b_0, b_1, b_2, \ldots)$ of elements of $\mathbb{K}$ satisfying the statement (245). Now, define the FPS $\mathbf{b}$ to be this sequence. Then, the statement (245) holds. In other words, $\mathbf{b}$ is a multiplicative inverse of $\mathbf{a}$ (because of the equivalence (244)). Thus, the FPS $\mathbf{a}$ has a multiplicative inverse (namely, $\mathbf{b}$). In other words, $\mathbf{a}$ is invertible (in the ring $\mathbb{K}[[x]]$). This proves the "$\Longleftarrow$" direction of Theorem 7.3.1. □

7.3.2. Newton's binomial formula

In Definition 4.1.19, we have defined negative powers (i.e., powers of the form α^n with n being a negative integer) of any nonzero complex number α. All that we needed from α in that definition was that α has a multiplicative inverse α^{-1}. Thus, we can straightforwardly extend this definition to any invertible element α of any ring:

> **Definition 7.3.2.** Let $\mathbb{L}$ be a ring. Let $\alpha \in \mathbb{L}$ be invertible. For any negative $n \in \mathbb{Z}$, we define an element $\alpha^n \in \mathbb{L}$ (called the *n-th power of α*) by $\alpha^n = \left(\alpha^{-1}\right)^{-n}$. (This is well-defined, since $\left(\alpha^{-1}\right)^{-n}$ is already defined by Definition 5.4.10 (because n is negative and thus $-n \in \mathbb{N}$).)

When the ring $\mathbb{L}$ is commutative, the powers of its elements satisfy the same rules as the powers of complex numbers (see Proposition 4.1.20), except that we have to replace "nonzero" by "invertible" (since negative powers are defined only for invertible elements of $\mathbb{L}$). For example, if $\mathbb{L}$ is a commutative ring, then

$$(\alpha\beta)^n = \alpha^n \beta^n \qquad \text{for all invertible } \alpha, \beta \in \mathbb{L} \text{ and all } n \in \mathbb{Z}.$$

We can apply this to $\mathbb{L} = \mathbb{K}[[x]]$ (which is a commutative ring). Recall that the FPS $1 - x$ is invertible, and its multiplicative inverse is

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots = \sum_{k \in \mathbb{N}} x^k.$$

A similar argument shows that the FPS $1 + x$ is invertible, and its multiplicative inverse is

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 \pm \cdots = \sum_{k \in \mathbb{N}} (-1)^k x^k.$$

Thus, negative powers of $1 + x$ are well-defined. We can explicitly compute not just the multiplicative inverse of $1 + x$ (as we just did), but also all powers of $1 + x$. As far as the nonnegative powers are concerned (that is, $(1+x)^u$ for $u \in \mathbb{N}$), this can easily be done by the binomial formula, and the result can be written either as $\sum\limits_{k=0}^{u} \dbinom{u}{k} x^k$ or as the infinite sum $\sum\limits_{k \in \mathbb{N}} \dbinom{u}{k} x^k$. (The second sum differs from the first sum only in the presence of addends for $k > u$; but all these addends are 0, and thus do not actually affect the sum.) Interestingly, however, the formula

$$(1+x)^u = \sum_{k \in \mathbb{N}} \binom{u}{k} x^k$$

is also valid for negative integers u – even though there is no binomial formula for negative exponents any more! This result is called *Newton's (generalized) binomial theorem for integers*; let us state it as follows:

Theorem 7.3.3. (a) The FPS $1 + x$ is invertible (in $\mathbb{K}[[x]]$). Thus, $(1+x)^u$ is defined for each $u \in \mathbb{Z}$ (by Definition 7.3.2).

(b) In the ring $\mathbb{K}[[x]]$, we have

$$(1+x)^u = \sum_{k \in \mathbb{N}} \binom{u}{k} x^k \qquad \text{for each } u \in \mathbb{Z}.$$

In particular, the sum $\sum\limits_{k \in \mathbb{N}} \dbinom{u}{k} x^k$ is well-defined (i.e., the family $\left(\dbinom{u}{k} x^k \right)_{k \in \mathbb{N}}$ is summable) for each $u \in \mathbb{Z}$.

To prove this, we begin by showing a simple corollary of the binomial formula:

Lemma 7.3.4. Let $u \in \mathbb{N}$. Let $\mathbb{K}$ be any ring, and let $a \in \mathbb{K}$. Then,

$$(1+a)^u = \sum_{k \in \mathbb{N}} \binom{u}{k} a^k.$$

(Here, the sum $\sum\limits_{k \in \mathbb{N}} \dbinom{u}{k} a^k$ is well-defined, since it has only finitely many nonzero addends.)

Proof of Lemma 7.3.4. For each $k \in \{u+1, u+2, u+3, \ldots\}$, we have $k \geq u + 1 > u$ and thus

$$\binom{u}{k} = 0 \tag{246}$$

(by Theorem 2.17.4, applied to $n = u$). Hence, all of the addends of the sum $\sum\limits_{k \in \mathbb{N}} \dbinom{u}{k} a^k$ with $k \geq u + 1$ are 0. Therefore, this sum has only finitely many nonzero addends, and thus is well-defined.

Now, $a \cdot 1 = a = 1 \cdot a$. Hence, (183) (applied to $b = 1$ and $n = u$) yields

$$(a+1)^u = \sum_{k=0}^{u} \binom{u}{k} a^k \underbrace{1^{u-k}}_{=1} = \sum_{k=0}^{u} \binom{u}{k} a^k.$$

Thus,

$$\left(\underbrace{1+a}_{=a+1} \right)^u = (a+1)^u = \sum_{k=0}^{u} \binom{u}{k} a^k.$$

Comparing this with

$$\sum_{k \in \mathbb{N}} \binom{u}{k} a^k = \sum_{k=0}^{u} \binom{u}{k} a^k + \sum_{k=u+1}^{\infty} \underbrace{\binom{u}{k}}_{\substack{=0 \\ \text{(by (246))}}} a^k = \sum_{k=0}^{u} \binom{u}{k} a^k + \underbrace{\sum_{k=u+1}^{\infty} 0 a^k}_{=0} = \sum_{k=0}^{u} \binom{u}{k} a^k,$$

we obtain $(1+a)^u = \sum_{k \in \mathbb{N}} \binom{u}{k} a^k$. This proves Lemma 7.3.4. □

Lemma 7.3.4 easily implies that Theorem 7.3.3 **(b)** holds for $u \in \mathbb{N}$; but proving Theorem 7.3.3 **(b)** for negative integers u requires more work. Here is ours:

Proof of Theorem 7.3.3. Let $u \in \mathbb{Z}$. Define N_u to be the FPS

$$\left(\binom{u}{0}, \binom{u}{1}, \binom{u}{2}, \ldots \right) \in \mathbb{K}\left[\left[x\right]\right].$$

(To be more precise, we mean the FPS $\left(\binom{u}{0} \cdot 1_{\mathbb{K}}, \binom{u}{1} \cdot 1_{\mathbb{K}}, \binom{u}{2} \cdot 1_{\mathbb{K}}, \ldots \right)$, because the binomial coefficients $\binom{u}{0}, \binom{u}{1}, \binom{u}{2}, \ldots$ by themselves are integers, not elements of $\mathbb{K}$. But we shall abuse notation and drop the "$\cdot 1_{\mathbb{K}}$"; thus, if r is any integer, then we will also denote the corresponding element $r \cdot 1_{\mathbb{K}}$ of $\mathbb{K}$ by r, as long as it is clear from the context that we mean an element of $\mathbb{K}$.)

Corollary 7.2.16 (applied to $a_i = \binom{u}{i}$) shows that the family $\left(\binom{u}{k} x^k \right)_{k \in \mathbb{N}}$ is summable, so that the sum $\sum_{k \in \mathbb{N}} \binom{u}{k} x^k$ is well-defined, and furthermore

$$\left(\binom{u}{0}, \binom{u}{1}, \binom{u}{2}, \ldots \right) = \binom{u}{0} + \binom{u}{1} x + \binom{u}{2} x^2 + \binom{u}{3} x^3 + \cdots = \sum_{k \in \mathbb{N}} \binom{u}{k} x^k.$$

Thus,

$$N_u = \left(\binom{u}{0}, \binom{u}{1}, \binom{u}{2}, \ldots \right) = \sum_{k \in \mathbb{N}} \binom{u}{k} x^k. \tag{247}$$

Now, forget that we fixed u. Thus, for each $u \in \mathbb{Z}$, we have defined an FPS N_u and showed that it satisfies (247), and, in particular, the sum $\sum_{k\in\mathbb{N}} \binom{u}{k} x^k$ is well-defined (i.e., the family $\left(\binom{u}{k} x^k\right)_{k\in\mathbb{N}}$ is summable).

Next, let us prove the following:

Claim 1: We have $N_n = (1+x) N_{n-1}$ for each $n \in \mathbb{Z}$.

[*Proof of Claim 1:* Let $n \in \mathbb{Z}$. Then, (247) (applied to $u = n-1$) yields $N_{n-1} = \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k$. Multiplying both sides of this equality with $1+x$, we find

$$\begin{aligned}(1+x) N_{n-1} &= (1+x) \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k \\ &= \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k + x \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k. \qquad (248)\end{aligned}$$

But

$$\begin{aligned}x \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k &= \sum_{k\in\mathbb{N}} \binom{n-1}{k} x x^k = \sum_{k=1}^{\infty} \binom{n-1}{k-1} \underbrace{x x^{k-1}}_{=x^k} \\ &\qquad \text{(here, we have substituted } k-1 \text{ for } k \text{ in the sum)} \\ &= \sum_{k=1}^{\infty} \binom{n-1}{k-1} x^k.\end{aligned}$$

Comparing this with

$$\begin{aligned}\sum_{k\in\mathbb{N}} \binom{n-1}{k-1} x^k &= \underbrace{\binom{n-1}{0-1}}_{\substack{=0 \\ \text{(by Definition 2.17.1 (b),} \\ \text{since } 0-1=-1\notin\mathbb{N})}} x^0 + \sum_{k=1}^{\infty} \binom{n-1}{k-1} x^k \\ &\qquad \text{(here, we have split off the addend for } k=0 \text{ from the sum)} \\ &= \sum_{k=1}^{\infty} \binom{n-1}{k-1} x^k,\end{aligned}$$

we obtain

$$x \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k = \sum_{k\in\mathbb{N}} \binom{n-1}{k-1} x^k.$$

Thus, (248) becomes

$$(1+x)\,N_{n-1} = \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k + \underbrace{x \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k}_{=\sum_{k\in\mathbb{N}} \binom{n-1}{k-1} x^k} = \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k + \sum_{k\in\mathbb{N}} \binom{n-1}{k-1} x^k$$

$$= \sum_{k\in\mathbb{N}} \underbrace{\left(\binom{n-1}{k} + \binom{n-1}{k-1}\right)}_{\substack{=\binom{n}{k} \\ \text{(by Theorem 2.17.8)}}} x^k = \sum_{k\in\mathbb{N}} \binom{n}{k} x^k.$$

Comparing this with

$$N_n = \sum_{k\in\mathbb{N}} \binom{n}{k} x^k \qquad \text{(by (247), applied to } u = n\text{)},$$

we obtain $N_n = (1+x)\,N_{n-1}$. This proves Claim 1.]

Also, (247) (applied to $u = 0$) yields

$$N_0 = \sum_{k\in\mathbb{N}} \binom{0}{k} x^k = \underbrace{\binom{0}{0}}_{=1} \underbrace{x^0}_{=1_{\mathbb{K}[[x]]}} + \sum_{k=1}^{\infty} \underbrace{\binom{0}{k}}_{\substack{=0 \\ \text{(by Theorem 2.17.4} \\ \text{(applied to } n=0\text{), since } k>0\text{)}}} x^k = 1_{\mathbb{K}[[x]]} + \underbrace{\sum_{k=1}^{\infty} 0x^k}_{=0}$$

$$= 1_{\mathbb{K}[[x]]}.$$

But Claim 1 (applied to $n = 0$) yields $N_0 = (1+x)\,N_{0-1} = (1+x)\,N_{-1}$. Hence, $(1+x)\,N_{-1} = N_0 = 1_{\mathbb{K}[[x]]}$, so that $N_{-1}(1+x) = (1+x)\,N_{-1} = 1_{\mathbb{K}[[x]]}$. Thus, $(1+x)\,N_{-1} = N_{-1}(1+x) = 1_{\mathbb{K}[[x]]}$. In other words, the FPS N_{-1} is a multiplicative inverse of $1+x$. Hence, the FPS $1+x$ has a multiplicative inverse, i.e., is invertible. This proves Theorem 7.3.3 **(a)**.

Next, we claim the following:

Claim 2: We have $(1+x)^{-n} = N_{-n}$ for each $n \in \mathbb{N}$.

[*Proof of Claim 2:* We shall prove Claim 2 by induction on n:

Induction base: We have $(1+x)^{-0} = (1+x)^0 = 1_{\mathbb{K}[[x]]} = N_{-0}$ (since $N_{-0} = N_0 = 1_{\mathbb{K}[[x]]}$). In other words, Claim 2 holds for $n = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume that Claim 2 holds for $n = m$. We must prove that Claim 2 holds for $n = m+1$.

We have assumed that Claim 2 holds for $n = m$. In other words, we have $(1+x)^{-m} = N_{-m}$.

But Claim 1 (applied to $n = -m$) yields

$$N_{-m} = (1+x)\, N_{-m-1} = (1+x)\, N_{-(m+1)} = N_{-(m+1)} \cdot (1+x)\,.$$

But $-(m+1) = (-m) + (-1)$, so that

$$\begin{aligned}(1+x)^{-(m+1)} &= (1+x)^{(-m)+(-1)} = \underbrace{\underbrace{(1+x)^{-m}}_{=N_{-m}}}_{=N_{-(m+1)}\cdot(1+x)} \cdot (1+x)^{-1} \\ &\qquad \text{(by the basic rules of exponents)} \\ &= N_{-(m+1)} \cdot \underbrace{(1+x)\cdot(1+x)^{-1}}_{=1_{\mathbb{K}[[x]]}} = N_{-(m+1)}.\end{aligned}$$

In other words, Claim 2 holds for $n = m+1$. This completes the induction step. Thus, Claim 2 is proven by induction.]

(b) Let $u \in \mathbb{Z}$. We have already checked that the sum $\sum\limits_{k\in\mathbb{N}} \binom{u}{k} x^k$ is well-defined (i.e., the family $\left(\binom{u}{k} x^k\right)_{k\in\mathbb{N}}$ is summable). It remains to prove that $(1+x)^u = \sum\limits_{k\in\mathbb{N}} \binom{u}{k} x^k$.

We are in one of the following two cases:

Case 1: We have $u \geq 0$.

Case 2: We have $u < 0$.

Let us first consider Case 1. In this case, we have $u \geq 0$. Thus, $u \in \mathbb{N}$. Hence, Lemma 7.3.4 (applied to $\mathbb{K}[[x]]$ and x instead of $\mathbb{K}$ and a) yields

$$(1+x)^u = \sum_{k\in\mathbb{N}} \binom{u}{k} x^k.$$

Thus, Theorem 7.3.3 **(b)** is proven in Case 1.

Let us now consider Case 2. In this case, we have $u < 0$. Hence, $-u > 0$, so that $-u \in \mathbb{N}$ (since $u \in \mathbb{Z}$). Thus, Claim 2 (applied to $n = -u$) yields

$$(1+x)^{-(-u)} = N_{-(-u)} = N_u = \sum_{k\in\mathbb{N}} \binom{u}{k} x^k \qquad \text{(by (247))}\,.$$

In view of $-(-u) = u$, this rewrites as

$$(1+x)^u = \sum_{k\in\mathbb{N}} \binom{u}{k} x^k.$$

Thus, Theorem 7.3.3 **(b)** is proven in Case 2.

We have now proven Theorem 7.3.3 **(b)** in both Cases 1 and 2. Hence, Theorem 7.3.3 **(b)** always holds. □

7.4. Polynomials and their degrees

Recall that polynomials have been defined as a special case of FPSs: Namely, a polynomial is just an FPS with only finitely many nonzero entries (= coefficients). But polynomials are, in many ways, better behaved than arbitrary FPSs; in particular, polynomials (unlike FPSs) can be evaluated at elements of $\mathbb{K}$ (by plugging these elements for the "x" in the polynomial), and even at more general things, whereas FPSs don't (in general).

We shall now study polynomials in more detail. To that aim, it helps to look a bit closer and define some smaller classes of polynomials. Namely, we know that each polynomial has only finitely many nonzero coefficients; we can thus ask what its last nonzero coefficient is. This leads to the following definition:

Definition 7.4.1. **(a)** For each $n \in \mathbb{Z}$, we define a subset $\mathbb{K}[x]_{\leq n}$ of $\mathbb{K}[[x]]$ by

$$\begin{aligned} \mathbb{K}[x]_{\leq n} &= \{(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]] \mid a_k = 0 \text{ for all } k > n\} & (249) \\ &= \left\{\mathbf{a} \in \mathbb{K}[[x]] \mid \left[x^k\right] \mathbf{a} = 0 \text{ for all } k > n\right\}. & (250) \end{aligned}$$

(Here, of course, "for all $k > n$" means "for all $k \in \mathbb{N}$ satisfying $k > n$".)

(b) Let $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ be a polynomial. Then, all but finitely many $i \in \mathbb{N}$ satisfy $a_i = 0$ (by the definition of a polynomial); in other words, only finitely many $i \in \mathbb{N}$ satisfy $a_i \neq 0$. The *degree* of $\mathbf{a}$ is defined to be the largest $i \in \mathbb{N}$ such that $a_i \neq 0$. (If no such i exists, then we define it to be $-\infty$, which is a symbolic quantity that is understood to be smaller than every integer and to satisfy $(-\infty) + m = -\infty$ for all m.)

The degree of the polynomial $\mathbf{a}$ will be denoted $\deg \mathbf{a}$.

Example 7.4.2. **(a)** We have

$$\begin{aligned} \mathbb{K}[x]_{\leq 0} &= \{(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]] \mid a_k = 0 \text{ for all } k > 0\} \\ &= \{(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]] \mid a_1 = a_2 = a_3 = \cdots = 0\} \\ &= \left\{ \left(a_0, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}} \right) \mid a_0 \in \mathbb{K} \right\} \\ &= \left\{ \left(a, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}} \right) \mid a \in \mathbb{K} \right\} \\ &= \{\underline{a} \mid a \in \mathbb{K}\} \qquad \left(\text{since } \left(a, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}} \right) = \underline{a} \text{ for each } a \in \mathbb{K} \right). \end{aligned}$$

This is the set of all constant FPSs; these are also known as the *constant polynomials*. Convention 7.2.8 lets us identify these constant polynomials to the elements of $\mathbb{K}$; thus, $\mathbb{K}[x]_{\leq 0}$ simply is $\mathbb{K}$.

(b) We have

$$\begin{aligned}\mathbb{K}\left[x\right]_{\leq 1} &= \left\{\left(a_0, a_1, a_2, \ldots\right) \in \mathbb{K}\left[\left[x\right]\right] \ \mid\ a_k = 0 \text{ for all } k > 1\right\} \\ &= \left\{\left(a_0, a_1, a_2, \ldots\right) \in \mathbb{K}\left[\left[x\right]\right] \ \mid\ a_2 = a_3 = a_4 = \cdots = 0\right\} \\ &= \left\{\left(a_0, a_1, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) \ \mid\ a_0, a_1 \in \mathbb{K}\right\} \\ &= \left\{a_0 + a_1 x \ \mid\ a_0, a_1 \in \mathbb{K}\right\}.\end{aligned}$$

The elements of this set are called the *linear polynomials* (at least in one sense of this word).

(c) If $n \in \mathbb{Z}$ is negative, then

$$\begin{aligned}\mathbb{K}\left[x\right]_{\leq n} &= \left\{\left(a_0, a_1, a_2, \ldots\right) \in \mathbb{K}\left[\left[x\right]\right] \ \mid\ a_k = 0 \text{ for all } k > n\right\} \\ &= \left\{\left(a_0, a_1, a_2, \ldots\right) \in \mathbb{K}\left[\left[x\right]\right] \ \mid\ a_0 = a_1 = a_2 = \cdots = 0\right\} \\ &= \left\{\left(0, 0, 0, \ldots\right)\right\} = \left\{\underline{0}\right\}.\end{aligned}$$

(d) The FPS $\left(3, 0, 2, 5, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}}\right)$ is a polynomial of degree 3.

Parts **(a)** and **(b)** of Definition 7.4.1 are essentially two different ways to look at the same thing (viz., at what point the coefficients of a polynomial become 0); the precise relation is captured by the following lemma:

Lemma 7.4.3. Let $n \in \mathbb{Z}$. Let $\mathbf{a} \in \mathbb{K}\left[\left[x\right]\right]$ be an FPS. Then:

(a) We have the following equivalence:

$$\left(\mathbf{a} \in \mathbb{K}\left[x\right]_{\leq n}\right) \iff \left(\left[x^k\right] \mathbf{a} = 0 \text{ for all } k > n\right).$$

(b) We have the following equivalence:

$$\left(\mathbf{a} \text{ is a polynomial of degree } \leq n\right) \iff \left(\mathbf{a} \in \mathbb{K}\left[x\right]_{\leq n}\right).$$

Note that n is allowed to be negative in Lemma 7.4.3; in this case, Lemma 7.4.3 **(b)** is simply saying that $\mathbf{a}$ is a polynomial of degree $-\infty$ if and only if all its coefficients $a_0, a_1, a_2, \ldots$ are 0 (because the only negative degree that a polynomial can have is $-\infty$).

Lemma 7.4.3 is an easy consequence of Definition 7.4.1, but the proof grows long on paper:

Proof of Lemma 7.4.3. **(a)** This follows directly from (250).

(b) Write the FPS $\mathbf{a}$ in the form $\mathbf{a} = (a_0, a_1, a_2, \ldots)$. Then, we have the following equivalence:

$$\left(\mathbf{a} \in \mathbb{K}[x]_{\leq n}\right) \iff (a_k = 0 \text{ for all } k > n) \qquad (251)$$

(by (249)).

Now, we shall prove the equivalence

$$(\mathbf{a} \text{ is a polynomial of degree } \leq n) \iff (a_k = 0 \text{ for all } k > n). \qquad (252)$$

In order to do so, let us prove the "$\Longrightarrow$" and "$\Longleftarrow$" directions of the equivalence (252) separately:

$\Longrightarrow$: Assume that $\mathbf{a}$ is a polynomial of degree $\leq n$. We must prove that $(a_k = 0 \text{ for all } k > n)$.

If all $i \in \mathbb{N}$ satisfy $a_i = 0$, then this is clearly satisfied. Thus, WLOG assume that not all $i \in \mathbb{N}$ satisfy $a_i = 0$. Hence, there exists an $i \in \mathbb{N}$ such that $a_i \neq 0$. Moreover, there exist only finitely many such i (since $\mathbf{a}$ is a polynomial). Thus, there exists a **largest** such i (since a finite nonempty set of integers always has a largest element). Let d denote this largest i. Then, d is the degree of $\mathbf{a}$ (since this is how the degree of $\mathbf{a}$ was defined). Thus, $d \leq n$ (since $\mathbf{a}$ is a polynomial of degree $\leq n$). In other words, $n \geq d$.

But d is the largest $i \in \mathbb{N}$ such that $a_i \neq 0$. Thus, every larger $i \in \mathbb{N}$ must satisfy $a_i = 0$. In other words, we have $a_i = 0$ for all $i > d$. Hence, $a_i = 0$ for all $i > n$ (because if $i > n$, then $i > n \geq d$). Renaming the index i as k in this statement, we obtain $(a_k = 0 \text{ for all } k > n)$. This proves the "$\Longrightarrow$" direction of the equivalence (252).

$\Longleftarrow$: Assume that $(a_k = 0 \text{ for all } k > n)$. We must prove that $\mathbf{a}$ is a polynomial of degree $\leq n$.

If all $i \in \mathbb{N}$ satisfy $a_i = 0$, then this is clearly satisfied (because in this case, the degree of $\mathbf{a}$ is defined to be $-\infty$, and we have $-\infty \leq n$). Thus, WLOG assume that not all $i \in \mathbb{N}$ satisfy $a_i = 0$. In other words, there exists some $i \in \mathbb{N}$ such that $a_i \neq 0$.

We have assumed that $a_k = 0$ for all $k > n$. Renaming the index k as i in this statement, we obtain $(a_i = 0 \text{ for all } i > n)$. Hence, all but finitely many $i \in \mathbb{N}$ satisfy $a_i = 0$ (since all but finitely many $i \in \mathbb{N}$ satisfy $i > n$). In other words, $\mathbf{a}$ is a polynomial (by the definition of a polynomial).

The set $\{i \in \mathbb{N} \mid a_i \neq 0\}$ is finite (since all but finitely many $i \in \mathbb{N}$ satisfy $a_i = 0$) and nonempty (since there exists some $i \in \mathbb{N}$ such that $a_i \neq 0$). Thus, it has a largest element (since a finite nonempty set of integers always has a largest element). Let d denote this largest i. Then, d is the degree of $\mathbf{a}$ (since this is how the degree of $\mathbf{a}$ was defined). Moreover, d is an $i \in \mathbb{N}$ satisfying $a_i \neq 0$ (since d belongs to the set $\{i \in \mathbb{N} \mid a_i \neq 0\}$). In other words, $d \in \mathbb{N}$ and $a_d \neq 0$. If we had $d > n$, then we would have $a_d = 0$ (since $a_k = 0$ for all $k > n$), which would contradict $a_d \neq 0$. Hence, we cannot have $d > n$. Thus, we have $d \leq n$. In other words, the degree of $\mathbf{a}$ is $\leq n$ (since d is the degree of $\mathbf{a}$). Thus, $\mathbf{a}$ is a polynomial of degree $\leq n$. This proves the "$\Longleftarrow$" direction of the equivalence (252).

We have now proven both directions of the equivalence (252); thus, this equivalence holds. Now, the equivalence (252) becomes

$$(\mathbf{a} \text{ is a polynomial of degree } \leq n) \iff (a_k = 0 \text{ for all } k > n) \iff \left(\mathbf{a} \in \mathbb{K}[x]_{\leq n}\right)$$

(by (251)). This proves Lemma 7.4.3 **(b)**. □

Remark 7.4.4. If you work in constructive logic, then Lemma 7.4.3 **(b)** cannot be proven. In fact, in constructive logic, you cannot prove that each polynomial has a well-defined degree (since you cannot generally prove that each $i \in \mathbb{N}$ satisfies either $a_i = 0$ or $a_i \neq 0$). Thus, the notion of "the degree of a polynomial" is not well-behaved in constructive mathematics. It is also not well-behaved in other ways – e.g., it is not preserved by ring homomorphisms, and leads to nuisances when $\mathbb{K}$ is a trivial ring, as witnessed in Theorem 7.4.11 **(d)** below. Thus, I shall avoid this notion wherever I can help it, and instead use the notion of $\mathbb{K}[x]_{\leq n}$ (where $n \in \mathbb{Z}$). This is a bit less familiar but hopefully more "philosophically right" (while being essentially equivalent to the notion of degree under classical logic, because of Lemma 7.4.3 **(b)**). (The notion of a degree does become useful again when $\mathbb{K}$ is a field, but I will first study a more general setup.)

Corollary 7.2.16 has shown that we can write each FPS as an infinite sum; likewise, we can write each polynomial as a finite sum:

Theorem 7.4.5. Let $n \in \mathbb{Z}$. Let $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]_{\leq n}$. Then,

$$(a_0, a_1, a_2, \ldots) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{k=0}^{n} a_k x^k.$$

Note that n is allowed to be negative in Theorem 7.4.5; in this case, the sum $\sum_{k=0}^{n} a_k x^k$ is empty (and thus equals $0_{\mathbb{K}[[x]]}$), and this should not be surprising (because in this case, we have $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]_{\leq n} = \{\underline{0}\}$ (by Example 7.4.2 **(c)**), so that $(a_0, a_1, a_2, \ldots) = \underline{0} = (\text{empty sum})$).

Proof of Theorem 7.4.5. We have $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]_{\leq n}$. Equivalently,

$$a_k = 0 \qquad \text{for all } k > n \tag{253}$$

(indeed, this is equivalent to $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]_{\leq n}$, because of (249)). Now, Corollary 7.2.16 yields

$$\begin{aligned}(a_0, a_1, a_2, \ldots) &= \sum_{k \in \mathbb{N}} a_k x^k = \sum_{k=0}^{n} a_k x^k + \sum_{k=n+1}^{\infty} \underbrace{a_k}_{\substack{=0 \\ \text{(by (253))}}} x^k = \sum_{k=0}^{n} a_k x^k + \underbrace{\sum_{k=n+1}^{\infty} 0 x^k}_{=0} \\ &= \sum_{k=0}^{n} a_k x^k = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n \\ &= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n\end{aligned}$$

(since $a_0 \underbrace{x^0}_{=1} = a_0$ and $a_1 \underbrace{x^1}_{=x} = a_1 x$). This proves Theorem 7.4.5. □

Exercise 7.4.1. Let $n \in \mathbb{N}$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Prove the following:
(a) If $[x^n]\,\mathbf{a} = 0$, then $\mathbf{a} \in \mathbb{K}[x]_{\leq n-1}$.
(b) If $[x^n]\,\mathbf{a} \neq 0$, then $\deg \mathbf{a} = n$.
(c) We have $\deg \mathbf{a} = n$ if and only if $[x^n]\,\mathbf{a} \neq 0$.

Solution to Exercise 7.4.1. Lemma 7.4.3 **(a)** shows that we have the equivalence $\left(\mathbf{a} \in \mathbb{K}[x]_{\leq n}\right) \iff \left(\left[x^k\right]\mathbf{a} = 0 \text{ for all } k > n\right)$. Hence, we have

$$\left[x^k\right]\mathbf{a} = 0 \text{ for all } k > n \tag{254}$$

(since we have $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$).

(a) Assume that $[x^n]\,\mathbf{a} = 0$. The equality $\left[x^k\right]\mathbf{a} = 0$ holds for all $k > n$ (by (254)), but also holds for $k = n$ (since $[x^n]\,\mathbf{a} = 0$). Hence, this equality holds for all $k \geq n$. In other words, it holds for all $k > n-1$ (since the $k \in \mathbb{N}$ satisfying $k \geq n$ are precisely the $k \in \mathbb{N}$ satisfying $k > n-1$). Thus, we have proven that $\left[x^k\right]\mathbf{a} = 0$ for all $k > n-1$.

But Lemma 7.4.3 **(a)** (applied to $n-1$ instead of n) shows that we have the equivalence $\left(\mathbf{a} \in \mathbb{K}[x]_{\leq n-1}\right) \iff \left(\left[x^k\right]\mathbf{a} = 0 \text{ for all } k > n-1\right)$. Hence, we have $\mathbf{a} \in \mathbb{K}[x]_{\leq n-1}$ (since we have $\left[x^k\right]\mathbf{a} = 0$ for all $k > n-1$). This solves Exercise 7.4.1 **(a)**.

(b) Assume that $[x^n]\,\mathbf{a} \neq 0$. Then, we have $[x^n]\,\mathbf{a} \neq 0$, but $\left[x^k\right]\mathbf{a} = 0$ for all $k > n$ (by (254)). Hence, n is the **largest** $i \in \mathbb{N}$ satisfying $\left[x^i\right]\mathbf{a} \neq 0$.

But $\mathbf{a} = \left(\left[x^0\right]\mathbf{a}, \left[x^1\right]\mathbf{a}, \left[x^2\right]\mathbf{a}, \ldots\right)$. Hence, the degree of the polynomial $\mathbf{a}$ is the largest $i \in \mathbb{N}$ satisfying $\left[x^i\right]\mathbf{a} \neq 0$ (because this is how the degree of $\mathbf{a}$ was defined). Thus, this degree is n (since we have shown that n is the largest $i \in \mathbb{N}$ satisfying $\left[x^i\right]\mathbf{a} \neq 0$). In other words, $\deg \mathbf{a} = n$. This solves Exercise 7.4.1 **(b)**.

(c) $\Longleftarrow$: The "$\Longleftarrow$" direction of Exercise 7.4.1 **(c)** follows immediately from Exercise 7.4.1 **(b)**.

$\Longrightarrow$: Assume that $\deg \mathbf{a} = n$. We must prove that $[x^n]\,\mathbf{a} \neq 0$.

Indeed, assume the contrary. Thus, $[x^n]\,\mathbf{a} = 0$. Hence, Exercise 7.4.1 **(a)** yields $\mathbf{a} \in \mathbb{K}[x]_{\leq n-1}$. But Lemma 7.4.3 **(b)** (applied to $n-1$ instead of n) yields the equivalence

$$\left(\mathbf{a} \text{ is a polynomial of degree } \leq n-1\right) \iff \left(\mathbf{a} \in \mathbb{K}[x]_{\leq n-1}\right).$$

Hence, $\mathbf{a}$ is a polynomial of degree $\leq n-1$ (since we have $\mathbf{a} \in \mathbb{K}[x]_{\leq n-1}$). Thus, $\deg \mathbf{a} \leq n-1 < n$. This contradicts $\deg \mathbf{a} = n$. This contradiction shows that our assumption was wrong. Hence, $[x^n]\,\mathbf{a} \neq 0$. This solves the "$\Longrightarrow$" direction of Exercise 7.4.1 **(c)**. □

Next, let us prove some basic properties of $\mathbb{K}[x]_{\leq n}$:

Lemma 7.4.6. Let $n \in \mathbb{Z}$.
(a) We have $\underline{0} \in \mathbb{K}[x]_{\leq n}$.
(b) If $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]_{\leq n}$, then $\mathbf{a} + \mathbf{b} \in \mathbb{K}[x]_{\leq n}$.
(c) If $\lambda \in \mathbb{K}$ and $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$, then $\lambda\mathbf{a} \in \mathbb{K}[x]_{\leq n}$.
(d) The subset $\mathbb{K}[x]_{\leq n}$ of $\mathbb{K}[[x]]$ is a $\mathbb{K}$-submodule of $\mathbb{K}[[x]]$.
(e) Any finite sum of elements of $\mathbb{K}[x]_{\leq n}$ belongs to $\mathbb{K}[x]_{\leq n}$.
(f) If $i \in \mathbb{N}$ satisfies $i \leq n$, then $x^i \in \mathbb{K}[x]_{\leq n}$.

Proof of Lemma 7.4.6. **(b)** Let $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]_{\leq n}$.

Lemma 7.4.3 **(a)** shows that we have the equivalence

$$\left(\mathbf{a} \in \mathbb{K}[x]_{\leq n}\right) \iff \left(\left[x^k\right] \mathbf{a} = 0 \text{ for all } k > n\right).$$

Hence, we have

$$\left[x^k\right] \mathbf{a} = 0 \text{ for all } k > n \tag{255}$$

(since $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$). Similarly,

$$\left[x^k\right] \mathbf{b} = 0 \text{ for all } k > n. \tag{256}$$

Now, for each $k \in \mathbb{N}$ satisfying $k > n$, we have

$$\begin{aligned}\left[x^k\right](\mathbf{a}+\mathbf{b}) &= \underbrace{\left[x^k\right]\mathbf{a}}_{\substack{=0 \\ \text{(by (255))}}} + \underbrace{\left[x^k\right]\mathbf{b}}_{\substack{=0 \\ \text{(by (256))}}} \qquad \text{(by (216))} \\ &= 0+0 = 0.\end{aligned}$$

In other words, $\left[x^k\right](\mathbf{a}+\mathbf{b}) = 0$ for all $k > n$. But Lemma 7.4.3 **(a)** (applied to $\mathbf{a}+\mathbf{b}$ instead of $\mathbf{a}$) shows that we have the equivalence

$$\left(\mathbf{a}+\mathbf{b} \in \mathbb{K}[x]_{\leq n}\right) \iff \left(\left[x^k\right](\mathbf{a}+\mathbf{b}) = 0 \text{ for all } k > n\right).$$

Thus, $\mathbf{a}+\mathbf{b} \in \mathbb{K}[x]_{\leq n}$ (since $\left[x^k\right](\mathbf{a}+\mathbf{b}) = 0$ for all $k > n$). This proves Lemma 7.4.6 **(b)**.

(a) This is trivial.

(c) This is like Lemma 7.4.6 **(b)**, but easier.

(d) The subset $\mathbb{K}[x]_{\leq n}$ of $\mathbb{K}[[x]]$ contains the zero vector $\underline{0}$ (by Lemma 7.4.6 **(a)**) and is closed under addition (by Lemma 7.4.6 **(b)**) and closed under scaling (by Lemma 7.4.6 **(c)**). Hence, it is a $\mathbb{K}$-submodule of $\mathbb{K}[[x]]$. This proves Lemma 7.4.6 **(d)**.

(e) This follows from Lemma 7.4.6 **(d)**. (A more down-to-earth way to prove this is to proceed by induction on the size of the sum; the induction base uses Lemma 7.4.6 **(a)**, while the induction step uses Lemma 7.4.6 **(b)**.)

(f) Let $i \in \mathbb{N}$ be such that $i \leq n$. We must prove that $x^i \in \mathbb{K}[x]_{\leq n}$.

Lemma 7.4.3 **(a)** (applied to $\mathbf{a} = x^i$) shows that we have the equivalence

$$\left(x^i \in \mathbb{K}[x]_{\leq n}\right) \iff \left(\left[x^k\right]\left(x^i\right) = 0 \text{ for all } k > n\right).$$

Thus, it remains to show that $\left[x^k\right]\left(x^i\right) = 0$ for all $k > n$. So let us fix a $k \in \mathbb{N}$ satisfying $k > n$. Then, $k > n \geq i$ (since $i \leq n$). Hence, (239) (applied to k and i instead of n and k) yields $\left[x^k\right]\left(x^i\right) = 0$. This is precisely what we wanted to show. Hence, Lemma 7.4.6 **(f)** is proven. □

Lemma 7.4.6 yields the following converse of Theorem 7.4.5:

Exercise 7.4.2. Let $n \in \mathbb{Z}$. Let $a_0, a_1, \ldots, a_n \in \mathbb{K}$. Prove that $\sum\limits_{k=0}^{n} a_k x^k \in \mathbb{K}[x]_{\leq n}$.

Solution to Exercise 7.4.2. If $k \in \{0, 1, \ldots, n\}$, then $x^k \in \mathbb{K}[x]_{\leq n}$ (by Lemma 7.4.6 **(f)**, applied to $i = k$) and therefore $a_k x^k \in \mathbb{K}[x]_{\leq n}$ (by Lemma 7.4.6 **(c)**, applied to $\lambda = a_k$ and $\mathbf{a} = x^k$). Hence, $\sum\limits_{k=0}^{n} a_k x^k$ is a finite sum of elements of $\mathbb{K}[x]_{\leq n}$. Because of Lemma 7.4.6 **(e)**, this entails that $\sum\limits_{k=0}^{n} a_k x^k$ belongs to $\mathbb{K}[x]_{\leq n}$. This solves Exercise 7.4.2. □

Combining Lemma 7.4.6 with Exercise 7.4.1 **(a)**, we obtain a simple fact: If two polynomials in $\mathbb{K}[x]_{\leq n}$ have the same coefficient of x^n, then their difference belongs to $\mathbb{K}[x]_{\leq n-1}$ (since the subtraction "cancels their leading terms"[193]). This fact is highly useful in induction proofs (specifically, it helps prove properties of polynomials by induction on the degree of a polynomial); let us state it as an exercise:

Exercise 7.4.3. Let $n \in \mathbb{N}$. Let $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]_{\leq n}$ be such that $[x^n]\,\mathbf{a} = [x^n]\,\mathbf{b}$. Then, $\mathbf{a} - \mathbf{b} \in \mathbb{K}[x]_{\leq n-1}$.

Solution to Exercise 7.4.3. Lemma 7.4.6 **(c)** (applied to -1 and $\mathbf{b}$ instead of λ and $\mathbf{a}$) shows that $(-1)\,\mathbf{b} \in \mathbb{K}[x]_{\leq n}$. Hence, Lemma 7.4.6 **(b)** (applied to $(-1)\,\mathbf{b}$ instead of $\mathbf{b}$) shows that $\mathbf{a} + (-1)\,\mathbf{b} \in \mathbb{K}[x]_{\leq n}$. Moreover, (216) (applied to $(-1)\,\mathbf{b}$ instead of $\mathbf{b}$) shows that

$$[x^n]\,(\mathbf{a} + (-1)\,\mathbf{b}) = \underbrace{[x^n]\,\mathbf{a}}_{=[x^n]\mathbf{b}} + \underbrace{[x^n]\,((-1)\,\mathbf{b})}_{\substack{=(-1)\cdot[x^n]\mathbf{b} \\ \text{(by (217), applied to } -1 \text{ and } \mathbf{b} \\ \text{instead of } \lambda \text{ and } \mathbf{a})}} = [x^n]\,\mathbf{b} + (-1)\cdot[x^n]\,\mathbf{b} = 0.$$

Hence, Exercise 7.4.1 **(a)** (applied to $\mathbf{a} + (-1)\,\mathbf{b}$ instead of $\mathbf{a}$) yields $\mathbf{a} + (-1)\,\mathbf{b} \in \mathbb{K}[x]_{\leq n-1}$. In view of

$$\mathbf{a} - \mathbf{b} = \mathbf{a} + \underbrace{(-\mathbf{b})}_{\substack{=(-1)\mathbf{b} \\ \text{(by (199), applied to } M=\mathbb{K}[[x]] \\ \text{and } a=\mathbf{b})}} = \mathbf{a} + (-1)\,\mathbf{b},$$

this rewrites as $\mathbf{a} - \mathbf{b} \in \mathbb{K}[x]_{\leq n-1}$. This solves Exercise 7.4.3. □

Theorem 7.4.7. **(a)** If $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$ satisfy $u \leq v$, then $\mathbb{K}[x]_{\leq u} \subseteq \mathbb{K}[x]_{\leq v}$.

(b) If $n \in \mathbb{Z}$, then $\mathbb{K}[x]_{\leq n}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$.

(c) If $\mathbf{a} \in \mathbb{K}[x]$, then there exists some $n \in \mathbb{N}$ such that $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$.

(d) If $a \in \mathbb{K}$, then $\underline{a} \in \mathbb{K}[x]_{\leq 0}$.

[193] I am putting this in quotation marks because I am trying to avoid the notion of "leading term". (The *leading term* of a nonzero polynomial $\mathbf{a} = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ of degree n is defined to be $a_n x^n$. But beware that if $\mathbf{a} = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ is merely in $\mathbb{K}[x]_{\leq n}$, then $\deg \mathbf{a}$ may be smaller than n, in which case its leading term is not $a_n x^n$ but rather $a_i x^i$ for $i = \deg \mathbf{a}$. Thus there is a discrepancy between the definition of "leading term" and what we typically want to say when we use this word.)

(e) We have $x \in \mathbb{K}[x]_{\leq 1}$.

(f) Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$ and $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$. Then, $\mathbf{a} + \mathbf{b} \in \mathbb{K}[x]_{\leq \max\{n,m\}}$ and $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$.

We shall prove Theorem 7.4.7 in Exercise 7.4.4 below. The hardest part of this theorem is the claim $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$ in its part **(f)**; we can strengthen this part as follows:

Lemma 7.4.8. Let $n, m \in \mathbb{N}$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$ and $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$. Then:

(a) We have $\left[x^{n+i}\right](\mathbf{ab}) = ([x^n]\,\mathbf{a}) \cdot \left(\left[x^i\right]\mathbf{b}\right)$ for each integer $i \geq m$.

(b) We have $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$.

(c) We have $[x^{n+m}](\mathbf{ab}) = ([x^n]\,\mathbf{a}) \cdot ([x^m]\,\mathbf{b})$.

Proof of Lemma 7.4.8. Lemma 7.4.3 **(a)** shows that we have the equivalence

$$\left(\mathbf{a} \in \mathbb{K}[x]_{\leq n}\right) \iff \left(\left[x^k\right]\mathbf{a} = 0 \text{ for all } k > n\right).$$

Hence, we have

$$\left[x^k\right]\mathbf{a} = 0 \text{ for all } k > n \tag{257}$$

(since $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$). Similarly,

$$\left[x^k\right]\mathbf{b} = 0 \text{ for all } k > m. \tag{258}$$

(a) Let i be an integer such that $i \geq m$. Thus, $i \geq m \geq 0$. For each $j \in \{0, 1, \ldots, i-1\}$, we have $j \leq i - 1 < i$ and thus $n + i - \underbrace{j}_{<i} > n + i - i = n$ and thus

$$\left[x^{n+i-j}\right]\mathbf{a} = 0 \tag{259}$$

(by (257), applied to $k = n + i - j$). For each $j \in \{i+1, i+2, \ldots, n+i\}$, we have $j \geq i + 1 > i \geq m$ and thus

$$\left[x^j\right]\mathbf{b} = 0 \tag{260}$$

(by (258), applied to $k = j$).

The equality (220) (applied to $n+i$ instead of n) yields

$$\begin{aligned}
\left[x^{n+i}\right](\mathbf{ab}) &= \sum_{j=0}^{n+i}\left(\left[x^{n+i-j}\right]\mathbf{a}\right)\cdot\left(\left[x^{j}\right]\mathbf{b}\right) \\
&= \sum_{j=0}^{i}\left(\left[x^{n+i-j}\right]\mathbf{a}\right)\cdot\left(\left[x^{j}\right]\mathbf{b}\right) + \sum_{j=i+1}^{n+i}\left(\left[x^{n+i-j}\right]\mathbf{a}\right)\cdot\underbrace{\left(\left[x^{j}\right]\mathbf{b}\right)}_{\substack{=0\\ \text{(by (260))}}} \\
&\qquad \left(\text{since } 0\leq i\leq n+i\right) \\
&= \sum_{j=0}^{i}\left(\left[x^{n+i-j}\right]\mathbf{a}\right)\cdot\left(\left[x^{j}\right]\mathbf{b}\right) + \underbrace{\sum_{j=i+1}^{n+i}\left(\left[x^{n+i-j}\right]\mathbf{a}\right)\cdot 0}_{=0} \\
&= \sum_{j=0}^{i}\left(\left[x^{n+i-j}\right]\mathbf{a}\right)\cdot\left(\left[x^{j}\right]\mathbf{b}\right) \\
&= \sum_{j=0}^{i-1}\underbrace{\left(\left[x^{n+i-j}\right]\mathbf{a}\right)}_{\substack{=0\\ \text{(by (259))}}}\cdot\left(\left[x^{j}\right]\mathbf{b}\right) + \underbrace{\left(\left[x^{n+i-i}\right]\mathbf{a}\right)}_{=[x^n]\mathbf{a}}\cdot\left(\left[x^{i}\right]\mathbf{b}\right) \\
&\qquad \left(\text{here, we have split off the addend for } j=i \text{ from the sum}\right) \\
&= \underbrace{\sum_{j=0}^{i-1}0\cdot\left(\left[x^{j}\right]\mathbf{b}\right)}_{=0} + \left(\left[x^{n}\right]\mathbf{a}\right)\cdot\left(\left[x^{i}\right]\mathbf{b}\right) = \left(\left[x^{n}\right]\mathbf{a}\right)\cdot\left(\left[x^{i}\right]\mathbf{b}\right).
\end{aligned}$$

This proves Lemma 7.4.8 **(a)**.

(b) Let $k\in\mathbb{N}$ be such that $k>n+m$. Hence, $k-n>m\geq 0$, so that $k-n\in\mathbb{N}$. Thus, (258) (applied to $k-n$ instead of k) yields $\left[x^{k-n}\right]\mathbf{b}=0$ (since $k-n>m$).

Again, we have $k-n>m$; thus, Lemma 7.4.8 **(a)** (applied to $i=k-n$) yields

$$\left[x^{n+(k-n)}\right](\mathbf{ab}) = \left(\left[x^{n}\right]\mathbf{a}\right)\cdot\underbrace{\left(\left[x^{k-n}\right]\mathbf{b}\right)}_{=0} = 0.$$

In other words, $\left[x^{k}\right](\mathbf{ab})=0$ (since $n+(k-n)=k$).

Now, forget that we fixed k. Thus we have seen that $\left[x^{k}\right](\mathbf{ab})=0$ for all $k>n+m$.

But Lemma 7.4.3 **(a)** (applied to $n+m$ and $\mathbf{ab}$ instead of n and $\mathbf{a}$) shows that we have the equivalence

$$\left(\mathbf{ab}\in\mathbb{K}\left[x\right]_{\leq n+m}\right) \iff \left(\left[x^{k}\right](\mathbf{ab})=0 \text{ for all } k>n+m\right).$$

Hence, $\mathbf{ab}\in\mathbb{K}\left[x\right]_{\leq n+m}$ (since $\left[x^{k}\right](\mathbf{ab})=0$ for all $k>n+m$). This proves Lemma 7.4.8 **(b)**.

(c) This follows from applying Lemma 7.4.8 **(a)** to $i=m$. □

▌ **Exercise 7.4.4.** Prove Theorem 7.4.7.

Proof of Theorem 7.4.7. **(a)** Let $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$ be such that $u \leq v$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq u}$. We shall prove that $\mathbf{a} \in \mathbb{K}[x]_{\leq v}$.

We have $u \leq v$, thus $v \geq u$. Lemma 7.4.3 **(a)** (applied to $n = u$) shows that we have the equivalence

$$\left(\mathbf{a} \in \mathbb{K}[x]_{\leq u}\right) \iff \left(\left[x^k\right] \mathbf{a} = 0 \text{ for all } k > u\right).$$

Hence, we have $\left[x^k\right] \mathbf{a} = 0$ for all $k > u$ (since $\mathbf{a} \in \mathbb{K}[x]_{\leq u}$). Therefore, $\left[x^k\right] \mathbf{a} = 0$ for all $k > v$ (since each $k \in \mathbb{N}$ satisfying $k > v$ must also satisfy $k > v \geq u$).

But Lemma 7.4.3 **(a)** (applied to $n = v$) shows that we have the equivalence $\left(\mathbf{a} \in \mathbb{K}[x]_{\leq v}\right) \iff \left(\left[x^k\right] \mathbf{a} = 0 \text{ for all } k > v\right)$. Hence, we have $\mathbf{a} \in \mathbb{K}[x]_{\leq v}$ (since we have $\left[x^k\right] \mathbf{a} = 0$ for all $k > v$).

Now, forget that we fixed $\mathbf{a}$. We thus have shown that $\mathbf{a} \in \mathbb{K}[x]_{\leq v}$ for each $\mathbf{a} \in \mathbb{K}[x]_{\leq u}$. In other words, $\mathbb{K}[x]_{\leq u} \subseteq \mathbb{K}[x]_{\leq v}$. This proves Theorem 7.4.7 **(a)**.

(b) Let $n \in \mathbb{Z}$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. We shall show that $\mathbf{a} \in \mathbb{K}[x]$.

Write the FPS $\mathbf{a}$ as $\mathbf{a} = (a_0, a_1, a_2, \ldots)$. Thus, $(a_0, a_1, a_2, \ldots) = \mathbf{a} \in \mathbb{K}[x]_{\leq n}$. According to (249), this means that $a_k = 0$ for all $k > n$. Renaming k as i in this statement, we conclude the following: $a_i = 0$ for all $i > n$. Hence, all but finitely many $i \in \mathbb{N}$ satisfy $a_i = 0$ (since all but finitely many $i \in \mathbb{N}$ satisfy $i > n$). In other words, the FPS $(a_0, a_1, a_2, \ldots)$ is a polynomial (by the definition of a polynomial). In other words, $\mathbf{a}$ is a polynomial (since $\mathbf{a} = (a_0, a_1, a_2, \ldots)$). In other words, $\mathbf{a} \in \mathbb{K}[x]$ (since $\mathbb{K}[x]$ is the set of all polynomials).

Forget that we fixed $\mathbf{a}$. We thus have shown that $\mathbf{a} \in \mathbb{K}[x]$ for each $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. In other words, $\mathbb{K}[x]_{\leq n}$ is a subset of $\mathbb{K}[x]$.

Furthermore, this subset $\mathbb{K}[x]_{\leq n}$ contains the zero vector $\underline{0}$ (by Lemma 7.4.6 **(a)**) and is closed under addition (by Lemma 7.4.6 **(b)**) and closed under scaling (by Lemma 7.4.6 **(c)**). Hence, it is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$. This proves Theorem 7.4.7 **(b)**.

(c) Let $\mathbf{a} \in \mathbb{K}[x]$. In other words, $\mathbf{a}$ is a polynomial (since $\mathbb{K}[x]$ is the set of all polynomials).

Write the FPS $\mathbf{a}$ as $\mathbf{a} = (a_0, a_1, a_2, \ldots)$. Then, $(a_0, a_1, a_2, \ldots) = \mathbf{a}$ is a polynomial. In other words, all but finitely many $i \in \mathbb{N}$ satisfy $a_i = 0$ (by the definition of a polynomial). In other words, there is a finite subset S of $\mathbb{N}$ such that

$$\text{every } i \in \mathbb{N} \setminus S \text{ satisfies } a_i = 0. \tag{261}$$

Consider this S.

The subset $S \cup \{0\}$ of $\mathbb{N}$ is finite (since it is the union of the two finite sets S and $\{0\}$) and nonempty (since it contains 0); thus, it has a maximum (since any finite nonempty subset of $\mathbb{N}$ is finite). Let n be this maximum. Then,

$$\text{every } t \in S \cup \{0\} \text{ satisfies } n \geq t \tag{262}$$

(since n is the maximum of $S \cup \{0\}$).

If $k \in \mathbb{N}$ satisfies $k > n$, then $a_k = 0$ [194]. In other words, $(a_k = 0 \text{ for all } k > n)$. In view of (249), this rewrites as $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]_{\leq n}$. Thus, $\mathbf{a} = (a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]_{\leq n}$.

[194] *Proof.* Let $k \in \mathbb{N}$ be such that $k > n$. We must prove that $a_k = 0$.

If we had $k \in S$, then we would have $k \in S \subseteq S \cup \{0\}$ and therefore $n \geq k$ (by (262), applied to $t = k$); but this would contradict $k > n$. Hence, we cannot have $k \in S$. Thus, $k \notin S$. Combining this with $k \in \mathbb{N}$, we obtain $k \in \mathbb{N} \setminus S$. Hence, (261) (applied to $i = k$) yields $a_k = 0$. Qed.

Hence, we have found an $n \in \mathbb{N}$ such that $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Thus, such an n exists. This proves Theorem 7.4.7 **(c)**.

(d) Lemma 7.4.6 **(f)** (applied to $i = 0$ and $n = 0$) yields $x^0 \in \mathbb{K}[x]_{\leq 0}$. Thus, Lemma 7.4.6 **(c)** (applied to $n = 0$, $\lambda = a$ and $\mathbf{a} = x^0$) yields $ax^0 \in \mathbb{K}[x]_{\leq 0}$. But

$$a \underbrace{x^0}_{=1_{\mathbb{K}[[x]]}=\underline{1}} = a\underline{1} = a\left(1, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) = \left(a, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) = \underline{a}.$$

Thus, $\underline{a} = ax^0 \in \mathbb{K}[x]_{\leq 0}$. This proves Theorem 7.4.7 **(d)**.

(e) Lemma 7.4.6 **(f)** (applied to $i = 1$ and $n = 1$) yields $x^1 \in \mathbb{K}[x]_{\leq 1}$. Thus, $x = x^1 \in \mathbb{K}[x]_{\leq 1}$. This proves Theorem 7.4.7 **(e)**.

(f) Let $j = \max\{n, m\}$. Then, $n \leq \max\{n, m\} = j$ and similarly $m \leq j$.

But Theorem 7.4.7 **(a)** (applied to $u = n$ and $v = j$) yields $\mathbb{K}[x]_{\leq n} \subseteq \mathbb{K}[x]_{\leq j}$ (since $n \leq j$). Hence, $\mathbf{a} \in \mathbb{K}[x]_{\leq n} \subseteq \mathbb{K}[x]_{\leq j}$. Similarly, $\mathbf{b} \in \mathbb{K}[x]_{\leq j}$. Hence, Lemma 7.4.6 **(b)** (applied to j instead of n) yields $\mathbf{a} + \mathbf{b} \in \mathbb{K}[x]_{\leq j} = \mathbb{K}[x]_{\leq \max\{n,m\}}$ (since $j = \max\{n, m\}$). Furthermore, Lemma 7.4.8 **(b)** yields $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$. Thus, Theorem 7.4.7 **(f)** is proven. □

Corollary 7.4.9. **(a)** The subset $\mathbb{K}[x]$ of $\mathbb{K}[[x]]$ is a $\mathbb{K}$-subalgebra of $\mathbb{K}[[x]]$.

(b) We have $x \in \mathbb{K}[x]$.

(c) We have

$$\mathbb{K}[x] = \bigcup_{n \in \mathbb{N}} \mathbb{K}[x]_{\leq n}.$$

Here, $\bigcup_{n \in \mathbb{N}} \mathbb{K}[x]_{\leq n}$ means the union of the sets $\mathbb{K}[x]_{\leq n}$ over all $n \in \mathbb{N}$ (in other words,

$$\begin{aligned}\bigcup_{n \in \mathbb{N}} \mathbb{K}[x]_{\leq n} &= \mathbb{K}[x]_{\leq 0} \cup \mathbb{K}[x]_{\leq 1} \cup \mathbb{K}[x]_{\leq 2} \cup \cdots \\ &= \left\{\mathbf{a} \mid \text{there exists some } n \in \mathbb{N} \text{ such that } \mathbf{a} \in \mathbb{K}[x]_{\leq n}\right\}\end{aligned}$$

).

Exercise 7.4.5. Prove Corollary 7.4.9.

Proof of Corollary 7.4.9. Theorem 7.4.7 **(b)** (applied to $n = 1$) yields that $\mathbb{K}[x]_{\leq 1}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$. Thus, $\mathbb{K}[x]_{\leq 1} \subseteq \mathbb{K}[x]$. But Theorem 7.4.7 **(e)** yields $x \in \mathbb{K}[x]_{\leq 1} \subseteq \mathbb{K}[x]$. This proves Corollary 7.4.9 **(b)**.

(a) Theorem 7.4.7 **(b)** (applied to $n = 0$) yields that $\mathbb{K}[x]_{\leq 0}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$. Thus, $\mathbb{K}[x]_{\leq 0} \subseteq \mathbb{K}[x]$.

Theorem 7.4.7 **(e)** yields $\underline{0} \in \mathbb{K}[x]_{\leq 0} \subseteq \mathbb{K}[x]$ and $\underline{1} \in \mathbb{K}[x]_{\leq 0} \subseteq \mathbb{K}[x]$.

Now, let $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$. Then, there exists some $n \in \mathbb{N}$ such that $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$ (by Theorem 7.4.7 **(c)**). Similarly, there exists some $m \in \mathbb{N}$ such that $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$. Consider these n and m.

Theorem 7.4.7 **(f)** yields that $\mathbf{a} + \mathbf{b} \in \mathbb{K}[x]_{\leq \max\{n,m\}}$ and $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$. But Theorem 7.4.7 **(b)** (applied to $\max\{n, m\}$ instead of n) yields that $\mathbb{K}[x]_{\leq \max\{n,m\}}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$. Thus, $\mathbb{K}[x]_{\leq \max\{n,m\}} \subseteq \mathbb{K}[x]$. Hence,

$$\mathbf{a} + \mathbf{b} \in \mathbb{K}[x]_{\leq \max\{n,m\}} \subseteq \mathbb{K}[x]. \tag{263}$$

Furthermore, Theorem 7.4.7 **(b)** (applied to $n+m$ instead of n) yields that $\mathbb{K}[x]_{\leq n+m}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$. Thus, $\mathbb{K}[x]_{\leq n+m} \subseteq \mathbb{K}[x]$. Hence,

$$\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m} \subseteq \mathbb{K}[x]. \tag{264}$$

Now, forget that we fixed $\mathbf{a}$ and $\mathbf{b}$. We thus have proven (263) and (264) for every $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$.

Thus, in particular, $\mathbf{a}+\mathbf{b} \in \mathbb{K}[x]$ for every $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$. In other words, the subset $\mathbb{K}[x]$ of $\mathbb{K}[[x]]$ is closed under addition.

Furthermore, $\mathbf{ab} \in \mathbb{K}[x]$ for every $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$ (since we have proven (264) for every $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$). In other words, the subset $\mathbb{K}[x]$ of $\mathbb{K}[[x]]$ is closed under multiplication.

If $\lambda \in \mathbb{K}$ and if $\mathbf{a} \in \mathbb{K}[x]$, then $\lambda\mathbf{a} \in \mathbb{K}[x]$ [195]. In other words, the subset $\mathbb{K}[x]$ of $\mathbb{K}[[x]]$ is closed under scaling.

The subset $\mathbb{K}[x]$ of $\mathbb{K}[[x]]$ contains $0_{\mathbb{K}[[x]]}$ (since $0_{\mathbb{K}[[x]]} = \underline{0} \in \mathbb{K}[x]$) and is closed under addition and closed under scaling. Thus, this subset $\mathbb{K}[x]$ is a $\mathbb{K}$-submodule of $\mathbb{K}[[x]]$.

The subset $\mathbb{K}[x]$ of $\mathbb{K}[[x]]$ contains $0_{\mathbb{K}[[x]]}$ and contains $1_{\mathbb{K}[[x]]}$ (since $1_{\mathbb{K}[[x]]} = \underline{1} \in \mathbb{K}[x]$) and is closed under addition and closed under multiplication. Thus, this subset $\mathbb{K}[x]$ is a subring of $\mathbb{K}[[x]]$.

Now, the subset $\mathbb{K}[x]$ is both a subring and a $\mathbb{K}$-submodule of $\mathbb{K}[[x]]$. In other words, $\mathbb{K}[x]$ is a $\mathbb{K}$-subalgebra of $\mathbb{K}[[x]]$. This proves Corollary 7.4.9 **(a)**.

(c) If $n \in \mathbb{N}$, then $\mathbb{K}[x]_{\leq n}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$ (by Theorem 7.4.7 **(b)**), and thus satisfies $\mathbb{K}[x]_{\leq n} \subseteq \mathbb{K}[x]$. Hence,

$$\bigcup_{n\in\mathbb{N}} \underbrace{\mathbb{K}[x]_{\leq n}}_{\subseteq \mathbb{K}[x]} \subseteq \bigcup_{n\in\mathbb{N}} \mathbb{K}[x] \subseteq \mathbb{K}[x]. \tag{265}$$

On the other hand, let $\mathbf{a} \in \mathbb{K}[x]$. Then, Theorem 7.4.7 **(c)** shows that there exists some $n \in \mathbb{N}$ such that $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. In other words, we have $\mathbf{a} \in \bigcup\limits_{n\in\mathbb{N}} \mathbb{K}[x]_{\leq n}$. Now, forget that we fixed $\mathbf{a}$. We thus have shown that $\mathbf{a} \in \bigcup\limits_{n\in\mathbb{N}} \mathbb{K}[x]_{\leq n}$ for each $\mathbf{a} \in \mathbb{K}[x]$. In other words, $\mathbb{K}[x] \subseteq \bigcup\limits_{n\in\mathbb{N}} \mathbb{K}[x]_{\leq n}$. Combining this with (265), we obtain $\mathbb{K}[x] = \bigcup\limits_{n\in\mathbb{N}} \mathbb{K}[x]_{\leq n}$. This proves Corollary 7.4.9 **(c)**. □

Definition 7.4.10. Corollary 7.4.9 **(a)** yields that $\mathbb{K}[x]$ is a $\mathbb{K}$-algebra. This $\mathbb{K}$-algebra is called the *polynomial ring over* $\mathbb{K}$ *in the indeterminate* x (or the *algebra of polynomials in* x *over* $\mathbb{K}$).

Exercise 7.4.6. Let $n \in \{-1, 0, 1, \ldots\}$. Theorem 7.4.7 **(b)** shows that $\mathbb{K}[x]_{\leq n}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$. Prove that the list $(x^0, x^1, \ldots, x^n)$ is a basis of this $\mathbb{K}$-submodule $\mathbb{K}[x]_{\leq n}$. (See Definition 6.11.1 **(d)** for the definition of a basis of a $\mathbb{K}$-submodule.)

[195] *Proof.* Let $\lambda \in \mathbb{K}$ and let $\mathbf{a} \in \mathbb{K}[x]$. We must prove that $\lambda\mathbf{a} \in \mathbb{K}[x]$.

There exists some $n \in \mathbb{N}$ such that $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$ (by Theorem 7.4.7 **(c)**). Consider this n. Then, Lemma 7.4.6 **(c)** yields $\lambda\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. On the other hand, Theorem 7.4.7 **(b)** yields that $\mathbb{K}[x]_{\leq n}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$. Thus, $\mathbb{K}[x]_{\leq n} \subseteq \mathbb{K}[x]$. Hence, $\lambda\mathbf{a} \in \mathbb{K}[x]_{\leq n} \subseteq \mathbb{K}[x]$. Qed.

Solution to Exercise 7.4.6. Each $i \in \{0, 1, \ldots, n\}$ satisfies $i \in \mathbb{N}$ and $i \leq n$ (since $i \in \{0, 1, \ldots, n\}$) and thus $x^i \in \mathbb{K}[x]_{\leq n}$ (by Lemma 7.4.6 **(f)**). In other words, the $n+1$ vectors $x^0, x^1, \ldots, x^n$ all belong to $\mathbb{K}[x]_{\leq n}$.

Hence, Proposition 6.11.2 (applied to $\mathbb{K}[x]_{\leq n}$, $n+1$ and $\left(x^0, x^1, \ldots, x^n\right)$ instead of M, k and $(v_1, v_2, \ldots, v_k)$) shows that $\left(x^0, x^1, \ldots, x^n\right)$ is a basis of $\mathbb{K}[x]_{\leq n}$ if and only if each vector in $\mathbb{K}[x]_{\leq n}$ can be **uniquely** written in the form

$$\lambda_1 x^0 + \lambda_2 x^1 + \cdots + \lambda_{n+1} x^n, \qquad \text{with } \lambda_1, \lambda_2, \ldots, \lambda_{n+1} \in \mathbb{K}. \tag{266}$$

We are now going to prove that each vector in $\mathbb{K}[x]_{\leq n}$ can be uniquely written in this form.

Indeed, let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. We are going to show that $\mathbf{a}$ can be uniquely written in the form (266). In order to show this, we must prove the following two claims:

> *Claim 1:* There exists **at least** one $(n+1)$-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1}) \in \mathbb{K}^{n+1}$ such that $\mathbf{a} = \lambda_1 x^0 + \lambda_2 x^1 + \cdots + \lambda_{n+1} x^n$.
>
> *Claim 2:* There exists **at most** one $(n+1)$-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1}) \in \mathbb{K}^{n+1}$ such that $\mathbf{a} = \lambda_1 x^0 + \lambda_2 x^1 + \cdots + \lambda_{n+1} x^n$.

[*Proof of Claim 1:* Write the FPS $\mathbf{a}$ in the form $\mathbf{a} = (a_0, a_1, a_2, \ldots)$. Then, $(a_0, a_1, a_2, \ldots) = \mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Hence, Theorem 7.4.5 shows that

$$(a_0, a_1, a_2, \ldots) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{k=0}^{n} a_k x^k.$$

Thus,

$$\mathbf{a} = \sum_{k=0}^{n} a_k x^k = a_0 x^0 + a_1 x^1 + \cdots + a_n x^n.$$

Thus, there exists **at least** one $(n+1)$-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1}) \in \mathbb{K}^{n+1}$ such that $\mathbf{a} = \lambda_1 x^0 + \lambda_2 x^1 + \cdots + \lambda_{n+1} x^n$ (namely, $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1}) = (a_0, a_1, \ldots, a_n)$). This proves Claim 1.]

[*Proof of Claim 2:* Let $(u_0, u_1, \ldots, u_n)$ and $(v_0, v_1, \ldots, v_n)$ be two $(n+1)$-tuples $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1}) \in \mathbb{K}^{n+1}$ such that $\mathbf{a} = \lambda_1 x^0 + \lambda_2 x^1 + \cdots + \lambda_{n+1} x^n$. We shall show that $(u_0, u_1, \ldots, u_n) = (v_0, v_1, \ldots, v_n)$.

Indeed, $(u_0, u_1, \ldots, u_n)$ is an $(n+1)$-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1}) \in \mathbb{K}^{n+1}$ such that $\mathbf{a} = \lambda_1 x^0 + \lambda_2 x^1 + \cdots + \lambda_{n+1} x^n$. In other words, $(u_0, u_1, \ldots, u_n)$ is an $(n+1)$-tuple in $\mathbb{K}^{n+1}$ and satisfies $\mathbf{a} = u_0 x^0 + u_1 x^1 + \cdots + u_n x^n$. Extend this $(n+1)$-tuple to an infinite sequence $(u_0, u_1, u_2, \ldots)$ by setting

$$u_k = 0 \qquad \text{for all integers } k > n. \tag{267}$$

Then, $(u_0, u_1, u_2, \ldots)$ is an FPS. Corollary 7.2.16 (applied to $a_i = u_i$) thus shows that the family $\left(u_k x^k\right)_{k \in \mathbb{N}}$ is summable, so that the sum $\sum_{k \in \mathbb{N}} u_k x^k$ is well-defined, and moreover,

$$(u_0, u_1, u_2, \ldots) = u_0 + u_1 x + u_2 x^2 + u_3 x^3 + \cdots = \sum_{k \in \mathbb{N}} u_k x^k.$$

Hence,

$$\begin{aligned}(u_0, u_1, u_2, \ldots) &= \sum_{k\in\mathbb{N}} u_k x^k = \sum_{k=0}^{n} u_k x^k + \sum_{k=n+1}^{\infty} \underbrace{u_k}_{\substack{=0 \\ \text{(by (267),} \\ \text{since } k\geq n+1>n)}} x^k \\ &= \sum_{k=0}^{n} u_k x^k + \underbrace{\sum_{k=n+1}^{\infty} 0x^k}_{=0} = \sum_{k=0}^{n} u_k x^k = u_0 x^0 + u_1 x^1 + \cdots + u_n x^n.\end{aligned}$$

Comparing this with $\mathbf{a} = u_0 x^0 + u_1 x^1 + \cdots + u_n x^n$, we obtain $\mathbf{a} = (u_0, u_1, u_2, \ldots)$. Hence, each $k \in \mathbb{N}$ satisfies $\left[x^k\right] \mathbf{a} = u_k$ (by the definition of $\left[x^k\right] \mathbf{a}$). Thus, in particular, each $k \in \{0, 1, \ldots, n\}$ satisfies

$$\left[x^k\right] \mathbf{a} = u_k. \tag{268}$$

The same argument (applied to $(v_0, v_1, \ldots, v_n)$ instead of $(u_0, u_1, \ldots, u_n)$) yields that each $k \in \{0, 1, \ldots, n\}$ satisfies

$$\left[x^k\right] \mathbf{a} = v_k. \tag{269}$$

Hence, each $k \in \{0, 1, \ldots, n\}$ satisfies

$$\begin{aligned} u_k &= \left[x^k\right] \mathbf{a} \qquad \text{(by (268))} \\ &= v_k \qquad \text{(by (269))}. \end{aligned}$$

In other words, $(u_0, u_1, \ldots, u_n) = (v_0, v_1, \ldots, v_n)$.

Now, forget that we fixed $(u_0, u_1, \ldots, u_n)$ and $(v_0, v_1, \ldots, v_n)$. We thus have shown that if $(u_0, u_1, \ldots, u_n)$ and $(v_0, v_1, \ldots, v_n)$ are two $(n+1)$-tuples $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1}) \in \mathbb{K}^{n+1}$ such that $\mathbf{a} = \lambda_1 x^0 + \lambda_2 x^1 + \cdots + \lambda_{n+1} x^n$, then $(u_0, u_1, \ldots, u_n) = (v_0, v_1, \ldots, v_n)$. In other words, there exists **at most** one $(n+1)$-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1}) \in \mathbb{K}^{n+1}$ such that $\mathbf{a} = \lambda_1 x^0 + \lambda_2 x^1 + \cdots + \lambda_{n+1} x^n$. This proves Claim 2.]

Combining Claim 1 and Claim 2, we now conclude that there exists a **unique** $(n+1)$-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1}) \in \mathbb{K}^{n+1}$ such that $\mathbf{a} = \lambda_1 x^0 + \lambda_2 x^1 + \cdots + \lambda_{n+1} x^n$. In other words, $\mathbf{a}$ can be uniquely written in the form (266).

Now, forget that we fixed $\mathbf{a}$. We thus have shown that each $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$ can be uniquely written in the form (266). In other words, each vector in $\mathbb{K}[x]_{\leq n}$ can be **uniquely** written in the form (266). Thus, the list $\left(x^0, x^1, \ldots, x^n\right)$ is a basis of $\mathbb{K}[x]_{\leq n}$ (because we have seen that the list $\left(x^0, x^1, \ldots, x^n\right)$ is a basis of $\mathbb{K}[x]_{\leq n}$ if and only if each vector in $\mathbb{K}[x]_{\leq n}$ can be **uniquely** written in the form (266)). This solves Exercise 7.4.6. □

We can restate some of Theorem 7.4.7 in terms of degrees:

Theorem 7.4.11. **(a)** If $a \in \mathbb{K}$, then $\underline{a} \in \mathbb{K}[x]$ and $\deg \underline{a} \leq 0$.

(b) If $a \in \mathbb{K}$ is nonzero, then $\deg \underline{a} = 0$.

(c) We have $x \in \mathbb{K}[x]$ and $\deg x \leq 1$.

(d) If $|\mathbb{K}| > 1$, then $\deg x = 1$.

(e) If $\mathbf{a}$ and $\mathbf{b}$ are two polynomials, then $\mathbf{a}+\mathbf{b}$ and $\mathbf{ab}$ are two polynomials satisfying

$$\deg\left(\mathbf{a}+\mathbf{b}\right) \leq \max\left\{\deg\mathbf{a}, \deg\mathbf{b}\right\} \qquad \text{and} \qquad \deg\left(\mathbf{ab}\right) \leq \deg\mathbf{a}+\deg\mathbf{b}.$$

(f) If $\mathbb{K}$ is a field, and if $\mathbf{a}$ and $\mathbf{b}$ are two polynomials, then $\deg\left(\mathbf{ab}\right) = \deg\mathbf{a} + \deg\mathbf{b}$.

We shall prove this in Exercise 7.4.7. The condition "$|\mathbb{K}| > 1$" in Theorem 7.4.11 **(d)** is a homage to the possibility that $\mathbb{K}$ may be a trivial ring (i.e., a ring with only one element). If $\mathbb{K}$ is a trivial ring, then all coefficients of the polynomial x are 0 (because all elements of $\mathbb{K}$ are 0), and thus $\deg x = -\infty$ rather than $\deg x = 1$. The zero ring is generally responsible for lots of exceptions in rules about degrees; thus it is better to speak of "polynomials of degree $\leq n$" than of the exact degree of a polynomial.

Note also that Theorem 7.4.11 **(f)** would not be true without the "$\mathbb{K}$ is a field" requirement. For example, if $\mathbb{K} = \mathbb{Z}/4$ and $\mathbf{a} = 1+2x$ and $\mathbf{b} = 1+2x$ (using the standard shorthand notations $1 = [1]_4$ and $2 = [2]_4$ etc.), then the polynomial

$$\mathbf{ab} = (1+2x)(1+2x) = 1 + \underbrace{4x+4x^2}_{\substack{=0 \\ \text{(since } 4=0 \text{ in } \mathbb{K})}} = 1 \qquad (270)$$

has degree < 2.

Our next lemma is a generalization of Theorem 7.4.11 **(f)**: Instead of requiring $\mathbb{K}$ to be a field, we will merely require that the coefficient $[x^m]\,\mathbf{b}$ of $\mathbf{b}$ be invertible (which is automatically satisfied when $\mathbb{K}$ is a field and $m = \deg\mathbf{b}$).

Lemma 7.4.12. Let $m \in \mathbb{N}$. Let $\mathbf{a}$ and $\mathbf{b}$ be two polynomials with $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$. Assume that $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible. Then, $\deg\left(\mathbf{ab}\right) = \deg\mathbf{a} + m$.

Exercise 7.4.7. Prove Theorem 7.4.11 and Lemma 7.4.12.

Proof of Lemma 7.4.12. If $\mathbf{a} = \underline{0}$, then the claim that we have to prove boils down to $-\infty = (-\infty) + m$ (since both polynomials $\underbrace{\mathbf{a}}_{=\underline{0}}\mathbf{b} = \underline{0}\mathbf{b}$ and $\mathbf{a}$ equal $\underline{0}$ and thus have degree $-\infty$), which is a consequence of the rules we stipulated for the symbol $-\infty$. Thus, WLOG assume that $\mathbf{a} \neq \underline{0}$. Hence, $\deg\mathbf{a} \in \mathbb{N}$. Define $n \in \mathbb{N}$ by $n = \deg\mathbf{a}$.

Now, $\deg\mathbf{a} = n \leq n$. Hence, $\mathbf{a}$ is a polynomial of degree $\leq n$. According to Lemma 7.4.3 **(b)**, this entails that $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Hence, Lemma 7.4.8 **(b)** yields that $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$. Furthermore, Lemma 7.4.8 **(c)** yields $[x^{n+m}]\left(\mathbf{ab}\right) = \left([x^n]\,\mathbf{a}\right)\cdot\left([x^m]\,\mathbf{b}\right)$.

But Exercise 7.4.1 **(c)** yields that we have $\deg\mathbf{a} = n$ if and only if $[x^n]\,\mathbf{a} \neq 0$. Hence, $[x^n]\,\mathbf{a} \neq 0$ (since $\deg\mathbf{a} = n$).

Assume (for the sake of contradiction) that $[x^{n+m}]\left(\mathbf{ab}\right) = 0$. Then, $0 = [x^{n+m}]\left(\mathbf{ab}\right) = \left([x^n]\,\mathbf{a}\right)\cdot\left([x^m]\,\mathbf{b}\right)$. We can divide both sides of this equality by $[x^m]\,\mathbf{b}$ (since $[x^m]\,\mathbf{b}$ is invertible), and thus obtain $0 = [x^n]\,\mathbf{a} \neq 0$. This is absurd. This contradiction shows that our assumption was wrong. Hence, $[x^{n+m}]\left(\mathbf{ab}\right) \neq 0$. Thus, Exercise 7.4.1 **(b)** (applied to $\mathbf{ab}$

and $n+m$ instead of $\mathbf{a}$ and n) yields $\deg(\mathbf{ab}) = n+m$ (since $\deg(\mathbf{ab}) \leq n+m$). In view of $n = \deg \mathbf{a}$, this rewrites as $\deg(\mathbf{ab}) = \deg \mathbf{a} + m$. This proves Lemma 7.4.12. □

Proof of Theorem 7.4.11. **(a)** Let $a \in \mathbb{K}$. Theorem 7.4.7 **(d)** yields $\underline{a} \in \mathbb{K}[x]_{\leq 0}$. But Lemma 7.4.3 **(b)** (applied to $\mathbf{a} = \underline{a}$ and $n = 0$) shows that we have the following equivalence:

$$(\underline{a} \text{ is a polynomial of degree } \leq 0) \iff \left(\underline{a} \in \mathbb{K}[x]_{\leq 0}\right).$$

Hence, $\underline{a}$ is a polynomial of degree ≤ 0 (since $\underline{a} \in \mathbb{K}[x]_{\leq 0}$). In other words, $\underline{a} \in \mathbb{K}[x]$ and $\deg \underline{a} \leq 0$. This proves Theorem 7.4.11 **(a)**.

(b) Let $a \in \mathbb{K}$ be nonzero. Theorem 7.4.7 **(d)** yields $\underline{a} \in \mathbb{K}[x]_{\leq 0}$. Moreover, $\left[x^0\right](\underline{a}) = a \neq 0$ (since a is nonzero). Hence, Exercise 7.4.1 **(b)** (applied to $n = 0$ and $\mathbf{a} = \underline{a}$) yields $\deg \underline{a} = 0$. This proves Theorem 7.4.11 **(b)**.

(c) Theorem 7.4.7 **(e)** yields $x \in \mathbb{K}[x]_{\leq 1}$. But Lemma 7.4.3 **(b)** (applied to $\mathbf{a} = x$ and $n = 1$) shows that we have the following equivalence:

$$(x \text{ is a polynomial of degree } \leq 1) \iff \left(x \in \mathbb{K}[x]_{\leq 1}\right).$$

Hence, x is a polynomial of degree ≤ 1 (since $x \in \mathbb{K}[x]_{\leq 1}$). In other words, $x \in \mathbb{K}[x]$ and $\deg x \leq 1$. This proves Theorem 7.4.11 **(c)**.

(d) Assume that $|\mathbb{K}| > 1$. Then, $1 \neq 0$ in $\mathbb{K}$ (that is, $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$) [196]. Now, Theorem 7.4.7 **(e)** yields $x \in \mathbb{K}[x]_{\leq 1}$. Moreover, $\left[x^1\right](x) = 1 \neq 0$. Hence, Exercise 7.4.1 **(b)** (applied to $n = 1$ and $\mathbf{a} = x$) yields $\deg x = 1$. This proves Theorem 7.4.11 **(d)**.

(e) Let $\mathbf{a}$ and $\mathbf{b}$ be two polynomials. We must prove that $\mathbf{a}+\mathbf{b}$ and $\mathbf{ab}$ are two polynomials satisfying

$$\deg(\mathbf{a}+\mathbf{b}) \leq \max\{\deg \mathbf{a}, \deg \mathbf{b}\} \qquad \text{and} \qquad \deg(\mathbf{ab}) \leq \deg \mathbf{a} + \deg \mathbf{b}.$$

If $\mathbf{a} = \underline{0}$, then this is all obvious (because in this case, we have $\mathbf{a}+\mathbf{b} = \mathbf{b}$ and $\mathbf{ab} = \underline{0}$ and $\deg \underline{0} = -\infty$). Thus, for the rest of this proof, we WLOG assume that $\mathbf{a} \neq \underline{0}$. For a similar reason, we WLOG assume that $\mathbf{b} \neq \underline{0}$. Now, $\deg \mathbf{a}$ is a well-defined nonnegative integer (since $\mathbf{a} \neq \underline{0}$). Similarly, $\deg \mathbf{b}$ is a well-defined nonnegative integer.

Define $n \in \mathbb{N}$ by $n = \deg \mathbf{a}$. Define $m \in \mathbb{N}$ by $m = \deg \mathbf{b}$. Lemma 7.4.3 **(b)** shows that we have the following equivalence:

$$(\mathbf{a} \text{ is a polynomial of degree } \leq n) \iff \left(\mathbf{a} \in \mathbb{K}[x]_{\leq n}\right).$$

Hence, $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$ (since $\mathbf{a}$ is a polynomial of degree $\leq n$ (since $n = \deg \mathbf{a}$)). Similarly, $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$.

Now, $\mathbf{a}$ is a polynomial of degree $\deg \mathbf{a} = n \leq \max\{n, m\}$. But Lemma 7.4.3 **(b)** (applied to $\max\{n, m\}$ instead of n) shows that we have the following equivalence:

$$(\mathbf{a} \text{ is a polynomial of degree } \leq \max\{n, m\}) \iff \left(\mathbf{a} \in \mathbb{K}[x]_{\leq \max\{n,m\}}\right).$$

Hence, $\mathbf{a} \in \mathbb{K}[x]_{\leq \max\{n,m\}}$ (since $\mathbf{a}$ is a polynomial of degree $\leq \max\{n, m\}$). Similarly, $\mathbf{b} \in \mathbb{K}[x]_{\leq \max\{n,m\}}$. Thus, Lemma 7.4.6 **(b)** (applied to $\max\{n, m\}$ instead of n) shows that

[196] *Proof:* Let us recall how this is proven: If we had $1 = 0$ in $\mathbb{K}$, then we would have $a = a \cdot \underbrace{1}_{=0} = a \cdot 0 = 0$ for each $a \in \mathbb{K}$, and therefore we would have $\mathbb{K} \subseteq \{0\}$ and thus $|\mathbb{K}| \leq |\{0\}| = 1$, which would contradict $|\mathbb{K}| > 1$. Hence, we cannot have $1 = 0$ in $\mathbb{K}$. Thus, $1 \neq 0$ in $\mathbb{K}$.

$\mathbf{a}+\mathbf{b} \in \mathbb{K}[x]_{\leq \max\{n,m\}}$. But Lemma 7.4.3 **(b)** (applied to $\max\{n,m\}$ and $\mathbf{a}+\mathbf{b}$ instead of n and $\mathbf{a}$) shows that we have the following equivalence:

$$(\mathbf{a}+\mathbf{b} \text{ is a polynomial of degree } \leq \max\{n,m\}) \iff \left(\mathbf{a}+\mathbf{b} \in \mathbb{K}[x]_{\leq \max\{n,m\}}\right).$$

Hence, $\mathbf{a}+\mathbf{b}$ is a polynomial of degree $\leq \max\{n,m\}$ (since $\mathbf{a}+\mathbf{b} \in \mathbb{K}[x]_{\leq \max\{n,m\}}$). In other words, $\mathbf{a}+\mathbf{b}$ is a polynomial satisfying $\deg(\mathbf{a}+\mathbf{b}) \leq \max\{n,m\}$.

Lemma 7.4.8 **(b)** yields $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$. But Lemma 7.4.3 **(b)** (applied to $n+m$ and $\mathbf{ab}$ instead of n and $\mathbf{a}$) shows that we have the following equivalence:

$$(\mathbf{ab} \text{ is a polynomial of degree } \leq n+m) \iff \left(\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}\right).$$

Hence, $\mathbf{ab}$ is a polynomial of degree $\leq n+m$ (since $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$). In other words, $\mathbf{ab}$ is a polynomial satisfying $\deg(\mathbf{ab}) \leq n+m$.

So we have shown that $\mathbf{a}+\mathbf{b}$ and $\mathbf{ab}$ are two polynomials, and we have

$$\deg(\mathbf{a}+\mathbf{b}) \leq \max\left\{\underbrace{n}_{=\deg\mathbf{a}}, \underbrace{m}_{=\deg\mathbf{b}}\right\} = \max\{\deg\mathbf{a}, \deg\mathbf{b}\} \qquad \text{and}$$
$$\deg(\mathbf{ab}) \leq \underbrace{n}_{=\deg\mathbf{a}} + \underbrace{m}_{=\deg\mathbf{b}} = \deg\mathbf{a} + \deg\mathbf{b}.$$

This completes the proof of Theorem 7.4.11 **(e)**.

(f) Assume that $\mathbb{K}$ is a field. Let $\mathbf{a}$ and $\mathbf{b}$ be two polynomials. We must prove that $\deg(\mathbf{ab}) = \deg\mathbf{a} + \deg\mathbf{b}$. If $\mathbf{a} = \underline{0}$, then this is obvious (because in this case, we have $\mathbf{ab} = \underline{0}$ and $\deg\underline{0} = -\infty$). Thus, for the rest of this proof, we WLOG assume that $\mathbf{a} \neq \underline{0}$. For a similar reason, we WLOG assume that $\mathbf{b} \neq \underline{0}$.

Define $m \in \mathbb{N}$ by $m = \deg\mathbf{b}$. (We can do this, since $\mathbf{b} \neq \underline{0}$.) Then, $\deg\mathbf{b} \leq m$. In other words, $\mathbf{b}$ is a polynomial of degree $\leq m$. Exercise 7.4.1 **(c)** (applied to m and $\mathbf{b}$ instead of n and $\mathbf{a}$) yields that we have $\deg\mathbf{b} = m$ if and only if $[x^m]\,\mathbf{b} \neq 0$. Hence, $[x^m]\,\mathbf{b} \neq 0$ (since $\deg\mathbf{b} = m$). Thus, the element $[x^m]\,\mathbf{b} \in \mathbb{K}$ is nonzero and therefore invertible (since $\mathbb{K}$ is a field, and thus every nonzero element of $\mathbb{K}$ is invertible). Therefore, Lemma 7.4.12 shows that $\deg(\mathbf{ab}) = \deg\mathbf{a} + \underbrace{m}_{=\deg\mathbf{b}} = \deg\mathbf{a} + \deg\mathbf{b}$. This proves Theorem 7.4.11 **(f)**. □

Proposition 7.4.13. Let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k \in \mathbb{K}[x]$.

(a) Then,

$$\deg(\mathbf{a}_1\mathbf{a}_2\cdots\mathbf{a}_k) \leq \deg(\mathbf{a}_1) + \deg(\mathbf{a}_2) + \cdots + \deg(\mathbf{a}_k).$$

(b) If $\mathbb{K}$ is a field, then this is an equality.

Proof of Proposition 7.4.13. **(a)** Proceed by induction on k. The base case ($k = 0$) follows from Theorem 7.4.11 **(a)** (applied to $a = 1$), since the empty product of polynomials in $\mathbb{K}[x]$ is $1_{\mathbb{K}[x]} = \underline{1}$. The induction step relies on Theorem 7.4.11 **(e)** (specifically, the inequality $\deg(\mathbf{ab}) \leq \deg\mathbf{a} + \deg\mathbf{b}$).

(b) Again, proceed by induction on k. The base case ($k = 0$) follows from Theorem 7.4.11 **(b)** (applied to $a = 1$), since the empty product of polynomials in $\mathbb{K}[x]$ is $1_{\mathbb{K}[x]} = \underline{1}$. The induction step relies on Theorem 7.4.11 **(f)**. □

The following exercise will be useful to us later on:

Exercise 7.4.8. Let $m \in \mathbb{N}$. Let $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ be such that $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible. Let $\mathbf{q} \in \mathbb{K}[x]$ be such that $\mathbf{qb} \in \mathbb{K}[x]_{\leq m-1}$. Prove that $\mathbf{q} = \underline{0}$.

Solution to Exercise 7.4.8. This can be easily solved using classical logic: Assume the contrary. Thus, $\mathbf{q} \neq \underline{0}$. Hence, $\deg \mathbf{q}$ is a well-defined nonnegative integer. Thus, $\deg \mathbf{q} \geq 0$. Now, Lemma 7.4.12 (applied to $\mathbf{a} = \mathbf{q}$) yields $\deg(\mathbf{qb}) = \underbrace{\deg \mathbf{q}}_{\geq 0} + m \geq m$. But Lemma 7.4.3 **(b)** (applied to $n = m-1$ and $\mathbf{a} = \mathbf{qb}$) shows that we have the following equivalence:

$$(\mathbf{qb} \text{ is a polynomial of degree } \leq m-1) \iff \left(\mathbf{qb} \in \mathbb{K}[x]_{\leq m-1}\right).$$

Hence, $\mathbf{qb}$ is a polynomial of degree $\leq m-1$ (since $\mathbf{qb} \in \mathbb{K}[x]_{\leq m-1}$). Hence, $\deg(\mathbf{qb}) \leq m-1 < m$. This contradicts $\deg(\mathbf{qb}) \geq m$. This contradiction shows that our assumption was false. Thus, the exercise is solved.

Here is a constructive solution: Theorem 7.4.7 **(c)** (applied to $\mathbf{a} = \mathbf{q}$) shows that there exists some $n \in \mathbb{N}$ such that $\mathbf{q} \in \mathbb{K}[x]_{\leq n}$. Consider this n. We now claim that

$$\mathbf{q} \in \mathbb{K}[x]_{\leq n-d} \qquad \text{for each } d \in \{0,1,\ldots,n+1\}. \tag{271}$$

[*Proof of (271):* We shall prove (271) by induction on d:

Induction base: We have $\mathbf{q} \in \mathbb{K}[x]_{\leq n} = \mathbb{K}[x]_{\leq n-0}$ (since $n = n-0$). In other words, (271) holds for $d = 0$. This completes the induction base.

Induction step: Let $p \in \{0,1,\ldots,n\}$. Assume that (271) holds for $d = p$. We must prove that (271) holds for $d = p+1$.

Note that $p \in \{0,1,\ldots,n\}$, thus $p \leq n$, hence $n-p \geq 0$ and thus $n-p \in \mathbb{N}$. Hence, $(n-p)+m \in \mathbb{N}$ (since $m \in \mathbb{N}$). Furthermore, $\underbrace{(n-p)}_{\geq 0} + m \geq m > m-1$.

We have assumed that (271) holds for $d = p$. In other words, we have $\mathbf{q} \in \mathbb{K}[x]_{\leq n-p}$. Also, $n-p \in \mathbb{N}$ and $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$. Hence, Lemma 7.4.8 **(c)** (applied to $n-p$ and $\mathbf{q}$ instead of n and $\mathbf{a}$) yields

$$\left[x^{(n-p)+m}\right](\mathbf{qb}) = \left(\left[x^{n-p}\right]\mathbf{q}\right) \cdot \left([x^m]\,\mathbf{b}\right). \tag{272}$$

Lemma 7.4.3 **(a)** (applied to $\mathbf{qb}$ and $m-1$ instead of $\mathbf{a}$ and n) shows that we have the following equivalence:

$$\left(\mathbf{qb} \in \mathbb{K}[x]_{\leq m-1}\right) \iff \left(\left[x^k\right](\mathbf{qb}) = 0 \text{ for all } k > m-1\right).$$

Hence, we have $\left[x^k\right](\mathbf{qb}) = 0$ for all $k > m-1$ (since $\mathbf{qb} \in \mathbb{K}[x]_{\leq m-1}$). Applying this to $k = (n-p)+m$, we obtain $\left[x^{(n-p)+m}\right](\mathbf{qb}) = 0$ (since $(n-p)+m > m-1$). Comparing this with (272), we obtain $\left(\left[x^{n-p}\right]\mathbf{q}\right) \cdot \left([x^m]\,\mathbf{b}\right) = 0$. We can divide both sides of this equality by $[x^m]\,\mathbf{b}$ (since $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible). As a result, we obtain $\left[x^{n-p}\right]\mathbf{q} = 0$.

Now, we know that $\mathbf{q} \in \mathbb{K}[x]_{\leq n-p}$ and $\left[x^{n-p}\right]\mathbf{q} = 0$. Hence, Exercise 7.4.1 **(a)** (applied to $n-p$ and $\mathbf{q}$ instead of n and $\mathbf{a}$) yields $\mathbf{q} \in \mathbb{K}[x]_{\leq n-p-1} = \mathbb{K}[x]_{\leq n-(p+1)}$ (since $n-p-1 = n-(p+1)$). In other words, (271) holds for $d = p+1$. This completes the induction step. Thus, (271) is proven by induction.]

Now that we have proven (271), we can apply (271) to $d = n + 1$. As a result, we obtain

$$\begin{aligned}\mathbf{q} \in \mathbb{K}[x]_{\leq n-(n+1)} &= \mathbb{K}[x]_{\leq -1} \qquad (\text{since } n - (n+1) = -1) \\ &= \{\underline{0}\}\end{aligned}$$

(by Example 7.4.2 **(c)** (applied to -1 instead of n), since -1 is negative). In other words, $\mathbf{q} = \underline{0}$. Thus, Exercise 7.4.8 is solved again (constructively this time). □

7.5. Division with remainder

7.5.1. The general case

Polynomials, in many senses, are like numbers. In particular, we can study their divisibility, congruence and remainder classes just as we did with integers and Gaussian integers. We will not go deeply into this, but we shall see some of the very basic properties.

The first basic fact is a version of division with remainder for polynomials (compare with Theorem 2.6.1 and Theorem 4.2.26):

Theorem 7.5.1. Let $m \in \mathbb{N}$. Let $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ be such that $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible. Let $\mathbf{a} \in \mathbb{K}[x]$ be any polynomial.

(a) Then, there exists a **unique** pair $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{qb} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$.

(b) Moreover, if $n \in \mathbb{N}$ satisfies $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$, then this pair satisfies $\mathbf{q} \in \mathbb{K}[x]_{\leq n-m}$.

We shall give an example for Theorem 7.5.1 in a moment (and then prove the theorem after a while); but first, let us comment on the condition that $[x^m]\,\mathbf{b}$ be invertible. Indeed, if $\mathbb{K}$ is a field, then this condition is equivalent to the requirement that $[x^m]\,\mathbf{b}$ be nonzero; and this latter requirement is equivalent to requiring that $\deg \mathbf{b} = m$ (by Exercise 7.4.1 **(c)**). Hence, if $\mathbb{K}$ is a field, then Theorem 7.5.1 can be applied to any nonzero polynomial $\mathbf{b} \in \mathbb{K}[x]$ (as long as m is chosen to be $\deg \mathbf{b}$). Thus, if $\mathbf{b}$ is a nonzero polynomial over a field $\mathbb{K}$, then any polynomial $\mathbf{a}$ can be uniquely divided with remainder by $\mathbf{b}$ (in such a way that the remainder will have degree $< \deg \mathbf{b}$). But if $\mathbb{K}$ is not a field, then not every polynomial can play the role of $\mathbf{b}$ in Theorem 7.5.1. For example, the polynomial $1 + 2x$ over $\mathbb{K} = \mathbb{Z}$ cannot, because its coefficient of x^1 is not invertible (it equals 2). And unsurprisingly, many polynomials over $\mathbb{Z}$ cannot be divided with remainder by $1 + 2x$ (for example, x^2 cannot – unless you allow remainders of degree > 1).

Example 7.5.2. For this example, set $\mathbb{K} = \mathbb{Z}$ and $m = 2$ and $\mathbf{b} = x^2 + x + 1$. Then, $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$.

Let $n = 4$ and $\mathbf{a} = x^4 - x^2$; thus, $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Then, Theorem 7.5.1 **(a)** says that there exists a **unique** pair $(\mathbf{q}, \mathbf{r})$ of polynomials such that

$$\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r} \qquad \left(\text{that is, } x^4 - x^2 = \mathbf{q} \cdot \left(x^2 + x + 1\right) + \mathbf{r}\right) \qquad \text{and}$$

$$\mathbf{r} \in \mathbb{K}[x]_{\leq m-1} \qquad \left(\text{that is, } \deg \mathbf{r} \leq \underbrace{m}_{=2} - 1 = 1\right).$$

Theorem 7.5.1 **(b)** says that this pair satisfies

$$\mathbf{q} \in \mathbb{K}[x]_{\leq n-m} \qquad \left(\text{that is, } \deg \mathbf{q} \leq \underbrace{n}_{=4} - \underbrace{m}_{=2} = 2\right).$$

How can we find this pair?

Consider this, so far unknown, pair. Comparing the coefficients of x^4 in the equality

$$x^4 - x^2 = \mathbf{q} \cdot \left(x^2 + x + 1\right) + \mathbf{r} = \left(x^2 + x + 1\right) \mathbf{q} + \mathbf{r}, \tag{273}$$

we obtain $1 = 1 \cdot \left[x^2\right] \mathbf{q}$ (because $\deg \mathbf{r} \leq 1$ and $\deg \mathbf{q} \leq 2$, so the only contribution to the coefficient of x^4 on the right hand side of (273) comes from picking the "x^2" from the "$x^2 + x + 1$" factor and the "$\left(\left[x^2\right] \mathbf{q}\right) x^2$" from the expansion of $\mathbf{q}$). Hence, $\left[x^2\right] \mathbf{q} = 1$. Since $\deg \mathbf{q} \leq 2$, we can thus write $\mathbf{q}$ in the form

$$\mathbf{q} = x^2 + \mathbf{q}_1 \qquad \text{for some polynomial } \mathbf{q}_1 \text{ with } \deg \mathbf{q}_1 \leq 1.$$

Consider this $\mathbf{q}_1$. Now, (273) can be transformed as follows:

$$\begin{aligned}
&\left(x^4 - x^2 = \left(x^2 + x + 1\right) \underbrace{\mathbf{q}}_{=x^2+\mathbf{q}_1} + \mathbf{r}\right) \\
\Longleftrightarrow\ &\left(x^4 - x^2 = \underbrace{\left(x^2 + x + 1\right)\left(x^2 + \mathbf{q}_1\right)}_{=(x^2+x+1)x^2+(x^2+x+1)\mathbf{q}_1} + \mathbf{r}\right) \\
\Longleftrightarrow\ &\left(x^4 - x^2 = \left(x^2 + x + 1\right) x^2 + \left(x^2 + x + 1\right) \mathbf{q}_1 + \mathbf{r}\right) \\
\Longleftrightarrow\ &\left(\underbrace{x^4 - x^2 - \left(x^2 + x + 1\right) x^2}_{=-x^3-2x^2} = \left(x^2 + x + 1\right) \mathbf{q}_1 + \mathbf{r}\right) \\
\Longleftrightarrow\ &\left(-x^3 - 2x^2 = \left(x^2 + x + 1\right) \mathbf{q}_1 + \mathbf{r}\right).
\end{aligned} \tag{274}$$

Comparing the coefficients of x^3 in the last equality here, we obtain $-1 = 1 \cdot \left[x^1\right] \mathbf{q}_1$ (because $\deg \mathbf{r} \leq 1$ and $\deg \mathbf{q}_1 \leq 1$). Hence, $\left[x^1\right] \mathbf{q}_1 = -1$. Since $\deg \mathbf{q}_1 \leq 1$, we can thus write $\mathbf{q}_1$ in the form

$$\mathbf{q}_1 = -x + \mathbf{q}_2 \qquad \text{for some polynomial } \mathbf{q}_2 \text{ with } \deg \mathbf{q}_2 \leq 0.$$

Consider this $\mathbf{q}_2$. Now, the last equality of (274) can be transformed as follows:

$$\begin{aligned}
&\left(-x^3 - 2x^2 = \left(x^2+x+1\right) \underbrace{\mathbf{q}_1}_{=-x+\mathbf{q}_2} + \mathbf{r}\right) \\
\Longleftrightarrow\ &\left(-x^3 - 2x^2 = \underbrace{\left(x^2+x+1\right)\left(-x+\mathbf{q}_2\right)}_{=(x^2+x+1)(-x)+(x^2+x+1)\mathbf{q}_2} + \mathbf{r}\right) \\
\Longleftrightarrow\ &\left(-x^3 - 2x^2 = \left(x^2+x+1\right)(-x) + \left(x^2+x+1\right)\mathbf{q}_2 + \mathbf{r}\right) \\
\Longleftrightarrow\ &\left(\underbrace{-x^3 - 2x^2 - \left(x^2+x+1\right)(-x)}_{=-x^2+x} = \left(x^2+x+1\right)\mathbf{q}_2 + \mathbf{r}\right) \\
\Longleftrightarrow\ &\left(-x^2 + x = \left(x^2+x+1\right)\mathbf{q}_2 + \mathbf{r}\right). \qquad (275)
\end{aligned}$$

Comparing the coefficients of x^2 in the last equality here, we obtain $-1 = 1 \cdot \left[x^0\right] \mathbf{q}_2$ (because $\deg \mathbf{r} \leq 1$ and $\deg \mathbf{q}_2 \leq 0$). Hence, $\left[x^0\right] \mathbf{q}_2 = -1$. Since $\deg \mathbf{q}_2 \leq 0$, we can thus write $\mathbf{q}_2$ in the form

$$\mathbf{q}_2 = -1 + \mathbf{q}_3 \qquad \text{for some polynomial } \mathbf{q}_3 \text{ with } \deg \mathbf{q}_3 \leq -1.$$

Consider this $\mathbf{q}_3$. Of course, $\mathbf{q}_3$ must be the zero polynomial (that is, $\underline{0} = 0_{\mathbb{K}[x]}$), since $\deg \mathbf{q}_3 \leq -1$. Now that we have found $\mathbf{q}_3$, we can recover $\mathbf{q}_2, \mathbf{q}_1, \mathbf{q}$ by back-substitution:

$$\begin{aligned}
\mathbf{q}_2 &= -1 + \underbrace{\mathbf{q}_3}_{=\underline{0}} = -1; \\
\mathbf{q}_1 &= -x + \underbrace{\mathbf{q}_2}_{=-1} = -x - 1; \\
\mathbf{q} &= x^2 + \underbrace{\mathbf{q}_1}_{=-x-1} = x^2 - x - 1.
\end{aligned}$$

Finally, we can find $\mathbf{r}$, for instance, by solving the last equality (275):

$$\mathbf{r} = -x^2 + x - \left(x^2+x+1\right) \underbrace{\mathbf{q}_2}_{=-1} = -x^2 + x - \left(x^2+x+1\right)(-1) = 2x + 1.$$

Hence, we have found the pair $(\mathbf{q},\mathbf{r})$. And we can check that this pair $(\mathbf{q},\mathbf{r})$ does indeed satisfy $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$: Indeed,

$$\underbrace{\mathbf{q}}_{=x^2-x-1}\ \underbrace{\mathbf{b}}_{=x^2+x+1} + \underbrace{\mathbf{r}}_{=2x+1} = \left(x^2-x-1\right)\cdot\left(x^2+x+1\right) + (2x+1) = x^4 - x^2 = \mathbf{a}.$$

Our next goal is to prove Theorem 7.5.1. You may have already spotted a proof idea in Example 7.5.2; we will essentially follow this idea when proving the "existence" part of Theorem 7.5.1 **(a)**, while the "uniqueness" part will be proven by a direct argument using Exercise 7.4.8.

Let us first combine the "existence" part of Theorem 7.5.1 **(a)** with Theorem 7.5.1 **(b)** in order to prove both simultaneously:

Lemma 7.5.3. Let $m \in \mathbb{N}$. Let $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ be such that $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible. Let $n \in \{-1,0,1,\ldots\}$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Then, there exist $\mathbf{q} \in \mathbb{K}[x]_{\leq n-m}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$.

Proof of Lemma 7.5.3. We shall prove Lemma 7.5.3 by strong induction on n (while keeping m and $\mathbf{b}$ fixed).

So let $N \in \{-1,0,1,\ldots\}$. We assume (as the induction hypothesis) that Lemma 7.5.3 holds whenever $n < N$. We must now prove that Lemma 7.5.3 holds for $n = N$.

We have assumed that Lemma 7.5.3 holds whenever $n < N$. In other words, the following claim holds:

Claim 1: Let $n \in \{-1,0,1,\ldots\}$ be such that $n < N$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Then, there exist $\mathbf{q} \in \mathbb{K}[x]_{\leq n-m}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$.

(We did not have to write "Let $m \in \mathbb{N}$" and "Let $\mathbf{b}$ be a polynomial..." here, since m and $\mathbf{b}$ are fixed.)

We must prove that Lemma 7.5.3 holds for $n = N$. In other words, we must prove the following claim:

Claim 2: Let $\mathbf{a} \in \mathbb{K}[x]_{\leq N}$. Then, there exist $\mathbf{q} \in \mathbb{K}[x]_{\leq N-m}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$.

[*Proof of Claim 2:* If $N < m$, then Claim 2 clearly holds (just take $\mathbf{q} = \underline{0}$ and $\mathbf{r} = \mathbf{a}$) [197]. Hence, for the rest of this proof of Claim 2, we WLOG assume that

[197] *Proof.* Assume that $N < m$. Then, $N \leq m-1$ (since N and m are integers). Hence, Theorem 7.4.7 **(a)** (applied to $u = N$ and $v = m-1$) yields $\mathbb{K}[x]_{\leq N} \subseteq \mathbb{K}[x]_{\leq m-1}$. Hence, $\mathbf{a} \in \mathbb{K}[x]_{\leq N} \subseteq \mathbb{K}[x]_{\leq m-1}$. Furthermore, $\underline{0} \in \mathbb{K}[x]_{\leq N-m}$ (by Lemma 7.4.6 **(a)**, applied to $n = N-m$). Finally, $\mathbf{a} = \underline{0}\cdot\mathbf{b} + \mathbf{a}$ (obviously). Thus, there exist $\mathbf{q} \in \mathbb{K}[x]_{\leq N-m}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ (namely, $\mathbf{q} = \underline{0}$ and $\mathbf{r} = \mathbf{a}$). In other words, Claim 2 holds. So we have shown that Claim 2 holds under the assumption that $N < m$.

we don't have $N < m$. Hence, $N \geq m$. Thus, $N - m \geq 0$, so that $N - m \in \mathbb{N}$. Also, $N \geq m \geq 0$ (since $m \in \mathbb{N}$), so that $N \in \mathbb{N}$ and therefore $N - 1 \in \{-1, 0, 1, \ldots\}$.

Define two elements a_N and b_m of $\mathbb{K}$ by $a_N = \left[x^N\right] \mathbf{a}$ and $b_m = [x^m] \mathbf{b}$. (These are well-defined, since $N \geq 0$ and $m \geq 0$.) Note that $b_m = [x^m] \mathbf{b}$ is invertible (by an assumption in Lemma 7.5.3).

Define an element $\lambda \in \mathbb{K}$ by $\lambda = \dfrac{a_N}{b_m}$. (This is well-defined, since b_m is invertible.)

Recall that $N - m \in \mathbb{N}$ and $N - m \leq N - m$. Hence, Lemma 7.4.6 **(f)** (applied to $N - m$ and $N - m$ instead of n and i) yields that $x^{N-m} \in \mathbb{K}[x]_{\leq N-m}$. Thus, Lemma 7.4.6 **(c)** (applied to $N - m$ and x^{N-m} instead of n and $\mathbf{a}$) yields that $\lambda x^{N-m} \in \mathbb{K}[x]_{\leq N-m}$. Recall also that $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$. Hence, Lemma 7.4.8 **(b)** (applied to $N - m$ and λx^{N-m} instead of n and $\mathbf{a}$) yields that $\lambda x^{N-m}\mathbf{b} \in \mathbb{K}[x]_{\leq (N-m)+m} = \mathbb{K}[x]_{\leq N}$ (since $(N - m) + m = N$). But we also know that $\mathbf{a} \in \mathbb{K}[x]_{\leq N}$.

We have $N \in \mathbb{N}$ and $N - m \in \mathbb{N}$ and $N \geq N - m$ (since $m \geq 0$). Hence, Exercise 7.2.1 **(a)** (applied to $u = N$ and $v = N - m$) yields

$$\begin{aligned}\left[x^N\right]\left(x^{N-m}\mathbf{b}\right) &= \left[x^{N-(N-m)}\right]\mathbf{b} = [x^m]\,\mathbf{b} \qquad (\text{since } N - (N-m) = m) \\ &= b_m \qquad (\text{by the definition of } b_m).\end{aligned}$$

Furthermore, (217) (applied to N and $x^{N-m}\mathbf{b}$ instead of n and $\mathbf{a}$) yields

$$\left[x^N\right]\left(\lambda x^{N-m}\mathbf{b}\right) = \underbrace{\lambda}_{=\frac{a_N}{b_m}} \cdot \underbrace{\left[x^N\right]\left(x^{N-m}\mathbf{b}\right)}_{=b_m} = \frac{a_N}{b_m} \cdot b_m = a_N = \left[x^N\right]\mathbf{a}$$

(by the definition of a_N); in other words, $\left[x^N\right]\mathbf{a} = \left[x^N\right]\left(\lambda x^{N-m}\mathbf{b}\right)$. Hence, Exercise 7.4.3 (applied to N and $\lambda x^{N-m}\mathbf{b}$ instead of n and $\mathbf{b}$) yields that $\mathbf{a} - \lambda x^{N-m}\mathbf{b} \in \mathbb{K}[x]_{\leq N-1}$. Hence, Claim 1 (applied to $N - 1$ and $\mathbf{a} - \lambda x^{N-m}\mathbf{b}$ instead of n and $\mathbf{a}$) yields that there exist $\mathbf{q} \in \mathbb{K}[x]_{\leq N-1-m}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ such that $\mathbf{a} - \lambda x^{N-m}\mathbf{b} = \mathbf{q}\mathbf{b} + \mathbf{r}$ (since $N - 1 < N$). Consider these $\mathbf{q}$ and $\mathbf{r}$, and denote them by $\mathbf{q}_0$ and $\mathbf{r}_0$. Thus, $\mathbf{q}_0 \in \mathbb{K}[x]_{\leq N-1-m}$ and $\mathbf{r}_0 \in \mathbb{K}[x]_{\leq m-1}$ satisfy $\mathbf{a} - \lambda x^{N-m}\mathbf{b} = \mathbf{q}_0\mathbf{b} + \mathbf{r}_0$.

From $\mathbf{a} - \lambda x^{N-m}\mathbf{b} = \mathbf{q}_0\mathbf{b} + \mathbf{r}_0$, we obtain

$$\mathbf{a} = \lambda x^{N-m}\mathbf{b} + \mathbf{q}_0\mathbf{b} + \mathbf{r}_0 = \left(\lambda x^{N-m} + \mathbf{q}_0\right)\mathbf{b} + \mathbf{r}_0. \qquad (276)$$

We shall next show that $\lambda x^{N-m} + \mathbf{q}_0 \in \mathbb{K}[x]_{\leq N-m}$. Indeed, $N - 1 - m \leq N - m$; hence, Theorem 7.4.7 **(a)** (applied to $u = N - 1 - m$ and $v = N - m$) yields $\mathbb{K}[x]_{\leq N-1-m} \subseteq \mathbb{K}[x]_{\leq N-m}$. Thus, $\mathbf{q}_0 \in \mathbb{K}[x]_{\leq N-1-m} \subseteq \mathbb{K}[x]_{\leq N-m}$. Furthermore, $\lambda x^{N-m} \in \mathbb{K}[x]_{\leq N-m}$ (as we already know). Thus, Lemma 7.4.6 **(c)** (applied to $N - m$, λx^{N-m} and $\mathbf{q}_0$ instead of n, $\mathbf{a}$ and $\mathbf{b}$) yields $\lambda x^{N-m} + \mathbf{q}_0 \in \mathbb{K}[x]_{\leq N-m}$.

Altogether, we now know that $\lambda x^{N-m} + \mathbf{q}_0 \in \mathbb{K}[x]_{\leq N-m}$ and $\mathbf{r}_0 \in \mathbb{K}[x]_{\leq m-1}$ and $\mathbf{a} = \left(\lambda x^{N-m} + \mathbf{q}_0\right)\mathbf{b} + \mathbf{r}_0$ (by (276)). Hence, there exist $\mathbf{q} \in \mathbb{K}[x]_{\leq N-m}$ and

$\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ (namely, $\mathbf{q} = \lambda x^{N-m} + \mathbf{q}_0$ and $\mathbf{r} = \mathbf{r}_0$). This proves Claim 2.]

Now, we have proven Claim 2; in other words, Lemma 7.5.3 holds for $n = N$. This completes the induction step. Thus, Lemma 7.5.3 is proven by induction. □

Proof of Theorem 7.5.1. **(a)** Theorem 7.4.7 **(c)** shows that there exists some $n \in \mathbb{N}$ such that $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Consider this n.

Now, Lemma 7.5.3 yields that there exist $\mathbf{q} \in \mathbb{K}[x]_{\leq n-m}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$. Consider these $\mathbf{q}$ and $\mathbf{r}$, and denote them by $\mathbf{q}_0$ and $\mathbf{r}_0$. Thus, $\mathbf{q}_0 \in \mathbb{K}[x]_{\leq n-m}$ and $\mathbf{r}_0 \in \mathbb{K}[x]_{\leq m-1}$ satisfy $\mathbf{a} = \mathbf{q}_0\mathbf{b} + \mathbf{r}_0$.

Now, $\mathbf{q}_0 \in \mathbb{K}[x]_{\leq n-m} \subseteq \mathbb{K}[x]$ (since Theorem 7.4.7 **(b)** (applied to $n-m$ instead of n) shows that $\mathbb{K}[x]_{\leq n-m}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$). In other words, $\mathbf{q}_0$ is a polynomial. Similarly, $\mathbf{r}_0$ is a polynomial. Hence, $(\mathbf{q}_0, \mathbf{r}_0)$ is a pair of polynomials. As we know, this pair satisfies $\mathbf{a} = \mathbf{q}_0\mathbf{b} + \mathbf{r}_0$ and $\mathbf{r}_0 \in \mathbb{K}[x]_{\leq m-1}$. Thus, there exists a pair $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ (namely, $(\mathbf{q}, \mathbf{r}) = (\mathbf{q}_0, \mathbf{r}_0)$).

It remains to prove that this pair is unique. In other words, it remains to prove that any two such pairs $(\mathbf{q}, \mathbf{r})$ must be equal. In other words, it remains to prove the following:

> *Claim 1:* If $(\mathbf{q}_1, \mathbf{r}_1)$ and $(\mathbf{q}_2, \mathbf{r}_2)$ are two pairs $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$, then $(\mathbf{q}_1, \mathbf{r}_1) = (\mathbf{q}_2, \mathbf{r}_2)$.

[*Proof of Claim 1:* Let $(\mathbf{q}_1, \mathbf{r}_1)$ and $(\mathbf{q}_2, \mathbf{r}_2)$ be two pairs $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$. We must prove that $(\mathbf{q}_1, \mathbf{r}_1) = (\mathbf{q}_2, \mathbf{r}_2)$.

We have assumed that $(\mathbf{q}_1, \mathbf{r}_1)$ is a pair $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$. In other words, $(\mathbf{q}_1, \mathbf{r}_1)$ is a pair of polynomials satisfying $\mathbf{a} = \mathbf{q}_1\mathbf{b} + \mathbf{r}_1$ and $\mathbf{r}_1 \in \mathbb{K}[x]_{\leq m-1}$. Similarly, $(\mathbf{q}_2, \mathbf{r}_2)$ is a pair of polynomials satisfying $\mathbf{a} = \mathbf{q}_2\mathbf{b} + \mathbf{r}_2$ and $\mathbf{r}_2 \in \mathbb{K}[x]_{\leq m-1}$.

From $\mathbf{r}_1 \in \mathbb{K}[x]_{\leq m-1}$ and $\mathbf{r}_2 \in \mathbb{K}[x]_{\leq m-1}$, we easily obtain $\mathbf{r}_2 - \mathbf{r}_1 \in \mathbb{K}[x]_{\leq m-1}$ [198].

Comparing the equalities $\mathbf{a} = \mathbf{q}_1\mathbf{b} + \mathbf{r}_1$ and $\mathbf{a} = \mathbf{q}_2\mathbf{b} + \mathbf{r}_2$, we obtain $\mathbf{q}_1\mathbf{b} + \mathbf{r}_1 = \mathbf{q}_2\mathbf{b} + \mathbf{r}_2$. In other words, $\mathbf{q}_1\mathbf{b} - \mathbf{q}_2\mathbf{b} = \mathbf{r}_2 - \mathbf{r}_1$. Hence,

$$(\mathbf{q}_1 - \mathbf{q}_2)\,\mathbf{b} = \mathbf{q}_1\mathbf{b} - \mathbf{q}_2\mathbf{b} = \mathbf{r}_2 - \mathbf{r}_1 \in \mathbb{K}[x]_{\leq m-1}.$$

Hence, Exercise 7.4.8 (applied to $\mathbf{q} = \mathbf{q}_1 - \mathbf{q}_2$) yields $\mathbf{q}_1 - \mathbf{q}_2 = \underline{0} = 0_{\mathbb{K}[[x]]}$. In other words, $\mathbf{q}_1 = \mathbf{q}_2$. Now, comparing the equalities

$$\mathbf{a} = \underbrace{\mathbf{q}_1}_{=\mathbf{q}_2}\mathbf{b} + \mathbf{r}_1 = \mathbf{q}_2\mathbf{b} + \mathbf{r}_1 \qquad \text{and} \qquad \mathbf{a} = \mathbf{q}_2\mathbf{b} + \mathbf{r}_2,$$

[198] *Proof.* Lemma 7.4.6 **(c)** (applied to $m-1$, -1 and $\mathbf{r}_1$ instead of n, λ and $\mathbf{a}$) yields $(-1)\,\mathbf{r}_1 \in \mathbb{K}[x]_{\leq m-1}$ (since $\mathbf{r}_1 \in \mathbb{K}[x]_{\leq m-1}$). Hence, Lemma 7.4.6 **(b)** (applied to $m-1$, $\mathbf{r}_2$ and $(-1)\,\mathbf{r}_1$ instead of n, $\mathbf{a}$ and $\mathbf{b}$) yields $\mathbf{r}_2 + (-1)\,\mathbf{r}_1 \in \mathbb{K}[x]_{\leq m-1}$ (since $\mathbf{r}_2 \in \mathbb{K}[x]_{\leq m-1}$). Thus, $\mathbf{r}_2 - \mathbf{r}_1 = \mathbf{r}_2 + (-1)\,\mathbf{r}_1 \in \mathbb{K}[x]_{\leq m-1}$.

we obtain $\mathbf{q}_2\mathbf{b} + \mathbf{r}_1 = \mathbf{q}_2\mathbf{b} + \mathbf{r}_2$. Thus, $\mathbf{r}_1 = \mathbf{r}_2$. Combining $\mathbf{q}_1 = \mathbf{q}_2$ with $\mathbf{r}_1 = \mathbf{r}_2$, we obtain $(\mathbf{q}_1, \mathbf{r}_1) = (\mathbf{q}_2, \mathbf{r}_2)$. This proves Claim 1.]

As we said, Claim 1 was the only thing that remained for us to prove in order to obtain Theorem 7.5.1 **(a)**. Thus, having just proven Claim 1, we have finished the proof of Theorem 7.5.1 **(a)**.

(b) Let $n \in \mathbb{N}$ be such that $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Let $(\mathbf{u}, \mathbf{v})$ be the pair $(\mathbf{q}, \mathbf{r})$ whose existence is claimed by Theorem 7.5.1 **(a)**. (We don't want to call it $(\mathbf{q}, \mathbf{r})$ just yet, since we want to keep the letters $\mathbf{q}$ and $\mathbf{r}$ free for other uses.) We shall show that $\mathbf{u} \in \mathbb{K}[x]_{\leq n-m}$.

Indeed, Lemma 7.5.3 yields that there exist $\mathbf{q} \in \mathbb{K}[x]_{\leq n-m}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$. Consider these $\mathbf{q}$ and $\mathbf{r}$, and denote them by $\mathbf{q}_0$ and $\mathbf{r}_0$. Thus, $\mathbf{q}_0 \in \mathbb{K}[x]_{\leq n-m}$ and $\mathbf{r}_0 \in \mathbb{K}[x]_{\leq m-1}$ satisfy $\mathbf{a} = \mathbf{q}_0\mathbf{b} + \mathbf{r}_0$.

Now, $(\mathbf{q}_0, \mathbf{r}_0)$ is a pair of polynomials[199]. As we know, this pair satisfies $\mathbf{a} = \mathbf{q}_0\mathbf{b} + \mathbf{r}_0$ and $\mathbf{r}_0 \in \mathbb{K}[x]_{\leq m-1}$. Thus, $(\mathbf{q}_0, \mathbf{r}_0)$ is a pair $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$. But $(\mathbf{u}, \mathbf{v})$ also is a pair $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ (because this is how $(\mathbf{u}, \mathbf{v})$ was defined). Now, recall the Claim 1 that we stated (and proved) during our proof of Theorem 7.5.1 **(a)**. We can apply this Claim to $(\mathbf{q}_1, \mathbf{r}_1) = (\mathbf{u}, \mathbf{v})$ and $(\mathbf{q}_2, \mathbf{r}_2) = (\mathbf{q}_0, \mathbf{r}_0)$ (since $(\mathbf{u}, \mathbf{v})$ and $(\mathbf{q}_0, \mathbf{r}_0)$ are two pairs $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$). As a result, we obtain $(\mathbf{u}, \mathbf{v}) = (\mathbf{q}_0, \mathbf{r}_0)$. In other words, $\mathbf{u} = \mathbf{q}_0$ and $\mathbf{v} = \mathbf{r}_0$. Thus, $\mathbf{u} = \mathbf{q}_0 \in \mathbb{K}[x]_{\leq n-m}$.

Now, forget that we introduced $(\mathbf{u}, \mathbf{v})$. We thus have shown that if $(\mathbf{u}, \mathbf{v})$ is the pair $(\mathbf{q}, \mathbf{r})$ whose existence is claimed by Theorem 7.5.1 **(a)**, then $\mathbf{u} \in \mathbb{K}[x]_{\leq n-m}$. Renaming $(\mathbf{u}, \mathbf{v})$ as $(\mathbf{q}, \mathbf{r})$ in this statement, we obtain the following: The pair $(\mathbf{q}, \mathbf{r})$ whose existence is claimed by Theorem 7.5.1 **(a)** satisfies $\mathbf{q} \in \mathbb{K}[x]_{\leq n-m}$. This proves Theorem 7.5.1 **(b)**. □

7.5.2. The case of a field

When $\mathbb{K}$ is a field, every nonzero polynomial $\mathbf{b} \in \mathbb{K}[x]$ has an invertible leading coefficient (i.e., if $m = \deg \mathbf{b}$, then $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible). Thus, Theorem 7.5.1 **(a)** shows that we can divide (with remainder) any polynomial $\mathbf{a}$ by any nonzero polynomial $\mathbf{b}$ when $\mathbb{K}$ is a field. More precisely, the following holds:

Theorem 7.5.4. Let $\mathbb{K}$ be a field. Let $\mathbf{a}$ and $\mathbf{b} \neq \underline{0}$ be polynomials in $\mathbb{K}[x]$. Then, there exist polynomials $\mathbf{q}$ and $\mathbf{r}$ in $\mathbb{K}[x]$ such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ and $\deg \mathbf{r} < \deg \mathbf{b}$.

Proof of Theorem 7.5.4. Let $m = \deg \mathbf{b}$. Then, $m \in \mathbb{N}$ (since $\mathbf{b} \neq \underline{0}$) and $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ (since $\deg \mathbf{b} = m$). The coefficient $[x^m]\,\mathbf{b} \in \mathbb{K}$ is nonzero (since $\deg \mathbf{b} = m$), and thus invertible (since any nonzero element of $\mathbb{K}$ is invertible[200]). Thus, Theorem 7.5.1 **(a)** shows that there exists a **unique** pair $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$. In other words, there exists a **unique** pair $(\mathbf{q}, \mathbf{r})$ of

[199] This can be shown just as in the proof of Theorem 7.5.1 **(a)** above.

[200] because $\mathbb{K}$ is a field

polynomials such that $\mathbf{a} = \mathbf{qb} + \mathbf{r}$ and $\deg \mathbf{r} < \deg \mathbf{b}$ (because for a polynomial $\mathbf{r} \in \mathbb{K}[x]$, the condition "$\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$" is equivalent to the condition "$\deg \mathbf{r} < \deg \mathbf{b}$" [201]). Hence, in particular, there exist polynomials $\mathbf{q}$ and $\mathbf{r}$ in $\mathbb{K}[x]$ such that $\mathbf{a} = \mathbf{qb} + \mathbf{r}$ and $\deg \mathbf{r} < \deg \mathbf{b}$. This proves Theorem 7.5.4. □

I have deliberately stated Theorem 7.5.4 in the above form (omitting the uniqueness of the pair $(\mathbf{q}, \mathbf{r})$, which I could have stated but did not) in order to evoke a deja-vu; indeed, in this form, Theorem 7.5.4 is obviously an analogue of Theorem 4.2.26. This analogy can be taken much further. When $\mathbb{K}$ is a field, the ring $\mathbb{K}[x]$ shares many properties with $\mathbb{Z}$ and $\mathbb{Z}[i]$. In particular, there is a good theory of divisibility, congruence, common divisors and gcds in this ring, which parallels the corresponding theory for Gaussian integers. The degree of a polynomial plays the same role in $\mathbb{K}[x]$ that the norm of a Gaussian integer plays in $\mathbb{Z}[i]$; in particular, it can be used for purposes of induction.

In defining the gcd of two polynomials over a field $\mathbb{K}$, we are faced with the same difficulty as in the case of $\mathbb{Z}[i]$: The gcd is not unique on the nose, but only unique up to unit-equivalence. However, for polynomials there is a natural choice: Out of all possible gcds of two polynomials, we pick the gcd whose leading coefficient is 1. (The "leading coefficient" of a polynomial means the coefficient of x^n, where n is the degree of the polynomial.)

There is a Euclidean algorithm for finding gcd's: For example, if $\mathbb{K} = \mathbb{Q}$, then

$$\begin{aligned}
&\gcd\left(x^2-1, x^3-1\right) \\
&= \gcd\left(x^2-1, \underbrace{\left(x^3-1\right) \% \left(x^2-1\right)}_{=x-1}\right) \\
&= \gcd\left(x^2-1, x-1\right) = \gcd\left(x-1, x^2-1\right) \\
&= \gcd\left(x-1, \underbrace{\left(x^2-1\right) \% (x-1)}_{=0}\right) = \gcd(x-1, 0) \\
&= \gcd(x-1) = x-1.
\end{aligned}$$

Here, of course, the notation $\mathbf{a}\%\mathbf{b}$ for a remainder is defined for polynomials in the same way as for integers (after all, the $\mathbf{q}$ and $\mathbf{r}$ in Theorem 7.5.4 are unique, even if we didn't say so!).

[201] Indeed, if $\mathbf{r} \in \mathbb{K}[x]$ is any polynomial, then we have the following chain of equivalences:

$$\begin{aligned}
\left(\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}\right) &\iff (\deg \mathbf{r} \leq m-1) \iff (\deg \mathbf{r} < m) \qquad (\text{since } m \in \mathbb{Z} \text{ and } \deg \mathbf{r} \in \mathbb{Z} \cup \{-\infty\}) \\
&\iff (\deg \mathbf{r} < \deg \mathbf{b}) \qquad (\text{since } m = \deg \mathbf{b}).
\end{aligned}$$

7.6. Evaluating polynomials

So far, polynomials have just been sequences of scalars. But recall that the most useful thing about polynomials should be the ability of evaluating them (at numbers, matrices, other polynomials). So how do we evaluate our polynomials?

Definition 7.6.1. Let U be a $\mathbb{K}$-algebra. Let $u \in U$.

Let $\mathbf{a} = (a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]$ be a polynomial over $\mathbb{K}$. (Thus, $\mathbf{a} = \sum\limits_{k\in\mathbb{N}} a_k x^k$.)

Then, we define

$$\mathbf{a}[u] := \sum_{k\in\mathbb{N}} a_k u^k \in U.$$

This sum is well-defined, since all but finitely many of its addends are zero (indeed, $(a_0, a_1, a_2, \ldots)$ is a polynomial, and thus all but finitely many $k \in \mathbb{N}$ satisfy $a_k = 0$).

We shall call $\mathbf{a}[u]$ the *value* of $\mathbf{a}$ at u. This is commonly denoted by $\mathbf{a}(u)$, but that notation is problematic, since expressions like "$\mathbf{a}(x+1)$" could mean different things depending on whether they are interpreted as values or as products. (That said, be careful with the notation "$\mathbf{a}[u]$" as well: The expression "$\mathbf{a}\left[x^2\right]\mathbf{b}$" can mean either $\mathbf{a}$ times the coefficient $\left[x^2\right]\mathbf{b}$ or the value $\mathbf{a}\left[x^2\right]$ times $\mathbf{b}$. Disambiguate such expressions using parentheses or dots.)

Example 7.6.2. Let $\mathbf{a} = (a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]$ be a polynomial.

(a) Taking $U = \mathbb{K}$ and $u = 0$ in Definition 7.6.1, we obtain

$$\mathbf{a}[0] = \sum_{k\in\mathbb{N}} a_k 0^k = a_0 \underbrace{0^0}_{=1} + \sum_{k>0} a_k \underbrace{0^k}_{\substack{=0 \\ (\text{since } k>0)}} = a_0 = \left[x^0\right]\mathbf{a}.$$

(b) Taking $U = \mathbb{K}$ and $u = 1$ in Definition 7.6.1, we obtain

$$\mathbf{a}[1] = \sum_{k\in\mathbb{N}} a_k \underbrace{1^k}_{=1} = \sum_{k\in\mathbb{N}} a_k = a_0 + a_1 + a_2 + \cdots.$$

This is the sum of all coefficients of $\mathbf{a}$.

(c) Taking $U = \mathbb{K}[x]$ and $u = x$ in Definition 7.6.1, we obtain

$$\mathbf{a}[x] = \sum_{k\in\mathbb{N}} a_k x^k = (a_0, a_1, a_2, \ldots) = \mathbf{a}.$$

So $\mathbf{a}[x]$ is another way of saying "$\mathbf{a}$".

(d) Furthermore,

$$\mathbf{a}[-x] = \sum_{k\in\mathbb{N}} a_k \underbrace{(-x)^k}_{=(-1)^k x^k} = \sum_{k\in\mathbb{N}} (-1)^k a_k x^k = (a_0, -a_1, a_2, -a_3, a_4, \ldots).$$

(e) Furthermore,

$$\mathbf{a}\left[x^2\right] = \sum_{k\in\mathbb{N}} a_k \left(x^2\right)^k = \sum_{k\in\mathbb{N}} a_k x^{2k} = (a_0, 0, a_1, 0, a_2, 0, a_3, 0, \ldots).$$

In Definition 7.6.1, we have rigorously defined the value $\mathbf{a}[u]$ of a polynomial $\mathbf{a}$ at an element u of a $\mathbb{K}$-algebra. In practice, this value is best understood through the following slogan:

> *Substitution slogan:* Let U be a $\mathbb{K}$-algebra, and let $u \in U$. Let $\mathbf{a} \in \mathbb{K}[x]$ be a polynomial. Then, $\mathbf{a}[u]$ is, roughly speaking, the result of "substituting u for x" into $\mathbf{a}$.

For example,

$$\left(1+3x+8x^2\right)[u] = 1+3u+8u^2 \qquad \text{and} \tag{277}$$

$$\left(x^9-2x\right)[u] = u^9-2u \qquad \text{and} \tag{278}$$

$$\left(x^4-(x-1)^2(x+1)^2\right)[u] = u^4-(u-1)^2(u+1)^2. \tag{279}$$

However, strictly speaking, this is not all obvious at this point yet. While (277) and (278) can easily be checked using Definition 7.6.1[202], it is not so clear how to obtain (279) from Definition 7.6.1 without multiplying out both sides[203]. Definition 7.6.1 only justifies the Substitution slogan when the substitution happens in the **expanded form** of $\mathbf{a}$ (that is, in the form $\mathbf{a} = a_0x^0 + a_1x^1 + a_2x^2 + \cdots$), but not

[202] Namely: Write the polynomial $1+3x+8x^2$ in the form $(a_0, a_1, a_2, \ldots)$ for some $a_0, a_1, a_2, \ldots \in \mathbb{K}$. Then, $a_0 = 1$ and $a_1 = 3$ and $a_2 = 8$ and $a_k = 0$ for all $k > 2$. But Definition 7.6.1 (applied to $\mathbf{a} = 1+3x+8x^2$) yields

$$\begin{aligned}\left(1+3x+8x^2\right)[u] &= \sum_{k\in\mathbb{N}} a_k u^k = \underbrace{a_0}_{=1}\underbrace{u^0}_{=1} + \underbrace{a_1}_{=3}\underbrace{u^1}_{=u} + \underbrace{a_2}_{=8}u^2 + \sum_{k>2}\underbrace{a_k}_{=0}u^k \\ &= 1+3u+8u^2 + \underbrace{\sum_{k>2} 0u^k}_{=0} = 1+3u+8u^2.\end{aligned}$$

This proves (277). A similar argument can be used to prove (278).

[203] Of course, if you multiply them out, then (279) becomes obvious: We have $x^4-(x-1)^2(x+1)^2 = 2x^2-1$, so that

$$\left(x^4-(x-1)^2(x+1)^2\right)[u] = \left(2x^2-1\right)[u] = 2u^2-1$$

(this follows from Definition 7.6.1 in the same way as (277) did). Comparing this with

$$u^4-(u-1)^2(u+1)^2 = 2u^2-1,$$

we obtain $\left(x^4-(x-1)^2(x+1)^2\right)[u] = u^4-(u-1)^2(u+1)^2$, and thus (279) is proven.

But multiplying out is not always viable. Let's say we want to prove that

$$\left(x^{2n}-(x-1)^n(x+1)^n\right)[u] = u^{2n}-(u-1)^n(u+1)^n$$

for all $n \in \mathbb{N}$. This can no longer be proven as easily, since the coefficients of the polynomial $x^{2n}-(x-1)^n(x+1)^n$ will grow more complicated as n grows larger.

when it happens in some other form like $(1+x)(1-x)$ or $x^2 - (x-1)^2$. We shall soon convince ourselves that the Substitution slogan is true for the latter forms as well. First, we need to prove some basic properties of values of polynomials:

Theorem 7.6.3. Let U be a $\mathbb{K}$-algebra. Let $u \in U$.

(a) Any $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$ satisfy

$$(\mathbf{a}+\mathbf{b})[u] = \mathbf{a}[u] + \mathbf{b}[u] \qquad \text{and} \qquad (\mathbf{ab})[u] = \mathbf{a}[u] \cdot \mathbf{b}[u].$$

(b) Any $\lambda \in \mathbb{K}$ and $\mathbf{a} \in \mathbb{K}[x]$ satisfy

$$(\lambda\mathbf{a})[u] = \lambda \cdot \mathbf{a}[u].$$

(c) Any $a \in \mathbb{K}$ satisfies $\underline{a}[u] = a \cdot 1_U$. (This is often written as "$\underline{a}[u] = a$", but keep in mind that the "a" on the right hand side of this equality is understood to be "coerced into U", so it actually means "the element of U corresponding to a", which is $a \cdot 1_U$.)

(d) We have $x[u] = u$.

(e) We have $x^i[u] = u^i$ for each $i \in \mathbb{N}$.

Proof of Theorem 7.6.3. For each $\mathbf{a} \in \mathbb{K}[x]$, we have $\mathbf{a} = \left([x^0]\mathbf{a}, [x^1]\mathbf{a}, [x^2]\mathbf{a}, \ldots\right)$ (by (215)) and therefore

$$\mathbf{a}[u] = \sum_{k\in\mathbb{N}} \left(\left[x^k\right]\mathbf{a}\right) u^k. \tag{280}$$

(e) Let $i \in \mathbb{N}$. Then, (280) (applied to $\mathbf{a} = x^i$) yields

$$\begin{aligned}
x^i[u] &= \sum_{k\in\mathbb{N}} \underbrace{\left(\left[x^k\right]\left(x^i\right)\right)}_{\substack{=\begin{cases}1, & \text{if } k=i;\\ 0, & \text{if } k\neq i\end{cases} \\ \text{(by (239), applied} \\ \text{to } k \text{ and } i \text{ instead of } n \text{ and } k)}} u^k = \sum_{k\in\mathbb{N}} \begin{cases}1, & \text{if } k=i;\\ 0, & \text{if } k\neq i\end{cases} u^k \\
&= \underbrace{\begin{cases}1, & \text{if } i=i;\\ 0, & \text{if } i\neq i\end{cases}}_{\substack{=1 \\ \text{(since } i=i)}} u^i + \sum_{\substack{k\in\mathbb{N};\\ k\neq i}} \underbrace{\begin{cases}1, & \text{if } k=i;\\ 0, & \text{if } k\neq i\end{cases}}_{\substack{=0 \\ \text{(since } k\neq i)}} u^k \\
&\qquad \text{(here, we have split off the addend for } k=i \text{ from the sum)} \\
&= u^i + \underbrace{\sum_{\substack{k\in\mathbb{N};\\ k\neq i}} 0u^k}_{=0} = u^i.
\end{aligned}$$

This proves Theorem 7.6.3 **(e)**.

(d) Theorem 7.6.3 **(e)** (applied to $i = 1$) yields $x^1 [u] = u^1 = u$. In view of $x^1 = x$, this rewrites as $x [u] = u$. This proves Theorem 7.6.3 **(d)**.

(c) Let $a \in \mathbb{K}$. Then, (280) (applied to $\mathbf{a} = \underline{a}$) yields

$$\begin{aligned}
\underline{a}[u] &= \sum_{k\in\mathbb{N}} \underbrace{\left(\left[x^k\right](\underline{a})\right)}_{\substack{=\begin{cases} a, & \text{if } k=0; \\ 0, & \text{if } k\neq 0 \end{cases} \\ \text{(by (222), applied to } n=k)}} u^k = \sum_{k\in\mathbb{N}} \begin{cases} a, & \text{if } k=0; \\ 0, & \text{if } k\neq 0 \end{cases} u^k \\
&= \underbrace{\begin{cases} a, & \text{if } 0=0; \\ 0, & \text{if } 0\neq 0 \end{cases}}_{\substack{=a \\ \text{(since } 0=0)}} \underbrace{u^0}_{=1_U} + \sum_{\substack{k\in\mathbb{N}; \\ k\neq 0}} \underbrace{\begin{cases} a, & \text{if } k=0; \\ 0, & \text{if } k\neq 0 \end{cases}}_{\substack{=0 \\ \text{(since } k\neq 0)}} u^k \\
&\qquad \text{(here, we have split off the addend for } k=0 \text{ from the sum)} \\
&= a\cdot 1_U + \underbrace{\sum_{\substack{k\in\mathbb{N}; \\ k\neq 0}} 0u^k}_{=0} = a\cdot 1_U.
\end{aligned}$$

This proves Theorem 7.6.3 **(c)**.

(c) This is easy and left to the reader.

(a) Let $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$. It is easy to see that $(\mathbf{a}+\mathbf{b})[u] = \mathbf{a}[u] + \mathbf{b}[u]$.

It remains to prove that $(\mathbf{ab})[u] = \mathbf{a}[u] \cdot \mathbf{b}[u]$.

Write $\mathbf{a}$ and $\mathbf{b}$ as $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ and $\mathbf{b} = (b_0, b_1, b_2, \ldots)$. Then, the definition of multiplication on $\mathbb{K}[[x]]$ yields

$$\mathbf{ab} = (c_0, c_1, c_2, \ldots), \qquad \text{where } c_n = \sum_{\substack{i,j\in\mathbb{N}; \\ i+j=n}} a_i b_j.$$

Hence,

$$\begin{aligned}
\left(\mathbf{ab}\right)[u] &= \sum_{k\in\mathbb{N}} c_k u^k = \sum_{n\in\mathbb{N}} \underbrace{c_n}_{\substack{=\sum\limits_{\substack{i,j\in\mathbb{N};\\ i+j=n}} a_i b_j}} u^n = \sum_{n\in\mathbb{N}} \sum_{\substack{i,j\in\mathbb{N};\\ i+j=n}} a_i b_j \underbrace{u^n}_{\substack{=u^{i+j}\\ \text{(since } n=i+j\text{)}}} \\
&= \underbrace{\sum_{n\in\mathbb{N}} \sum_{\substack{i,j\in\mathbb{N};\\ i+j=n}}}_{\substack{=\sum\limits_{i,j\in\mathbb{N}}\\ =\sum\limits_{i\in\mathbb{N}}\sum\limits_{j\in\mathbb{N}}}} a_i b_j \underbrace{u^{i+j}}_{=u^i u^j} = \sum_{i\in\mathbb{N}} \sum_{j\in\mathbb{N}} a_i b_j u^i u^j = \sum_{i\in\mathbb{N}} a_i u^i \sum_{j\in\mathbb{N}} b_j u^j \\
&= \underbrace{\left(\sum_{i\in\mathbb{N}} a_i u^i\right)}_{\substack{=\sum\limits_{k\in\mathbb{N}} a_k u^k\\ =\mathbf{a}[u]}} \underbrace{\left(\sum_{j\in\mathbb{N}} b_j u^j\right)}_{\substack{=\sum\limits_{k\in\mathbb{N}} b_k u^k\\ =\mathbf{b}[u]}} = \mathbf{a}[u]\cdot\mathbf{b}[u].
\end{aligned}$$

(These manipulations with infinite sums are all kosher, because only finitely many pairs $(i, j) \in \mathbb{N}\times\mathbb{N}$ satisfy $a_i b_j \neq 0$.) This completes our proof of Theorem 7.6.3 **(a)**. □

Corollary 7.6.4. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. Then, the map

$$\begin{aligned}
\operatorname{ev}_u : \mathbb{K}[x] &\to U, \\
\mathbf{a} &\mapsto \mathbf{a}[u]
\end{aligned}$$

is a $\mathbb{K}$-algebra homomorphism.

Proof of Corollary 7.6.4. We must prove that ev_u is a $\mathbb{K}$-algebra homomorphism. In other words, we must prove that ev_u is a ring homomorphism and a $\mathbb{K}$-module homomorphism (by the definition of a $\mathbb{K}$-algebra homomorphism).

In order to prove that ev_u is a ring homomorphism, we must prove the following four claims:

Claim 1: We have $\operatorname{ev}_u(\mathbf{a}+\mathbf{b}) = \operatorname{ev}_u(\mathbf{a}) + \operatorname{ev}_u(\mathbf{b})$ for all $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$.

Claim 2: We have $\operatorname{ev}_u(0) = 0$.

Claim 3: We have $\operatorname{ev}_u(\mathbf{ab}) = \operatorname{ev}_u(\mathbf{a})\operatorname{ev}_u(\mathbf{b})$ for all $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$.

Claim 4: We have $\operatorname{ev}_u(1) = 1$.

Indeed, these four claims are the axioms in the definition of a ring homomorphism.

In order to prove that ev_u is a $\mathbb{K}$-module homomorphism, we must prove the following four claims:

Claim 5: We have $\operatorname{ev}_u(\mathbf{a}+\mathbf{b}) = \operatorname{ev}_u(\mathbf{a}) + \operatorname{ev}_u(\mathbf{b})$ for all $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$.

Claim 6: We have $\operatorname{ev}_u(0) = 0$.

Claim 7: We have $\operatorname{ev}_u(\lambda\mathbf{a}) = \lambda \operatorname{ev}_u(\mathbf{a})$ for all $\lambda \in \mathbb{K}$ and $\mathbf{a} \in \mathbb{K}[x]$.

Indeed, these three claims are the axioms in the definition of a $\mathbb{K}$-module homomorphism.

Let us first prove Claim 3:

[*Proof of Claim 3:* Let $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$. We must prove that $\operatorname{ev}_u(\mathbf{ab}) = \operatorname{ev}_u(\mathbf{a}) \cdot \operatorname{ev}_u(\mathbf{b})$. But the definition of ev_u yields $\operatorname{ev}_u(\mathbf{ab}) = (\mathbf{ab})[u]$ and $\operatorname{ev}_u(\mathbf{a}) = \mathbf{a}[u]$ and $\operatorname{ev}_u(\mathbf{b}) = \mathbf{b}[u]$. Hence, proving that $\operatorname{ev}_u(\mathbf{ab}) = \operatorname{ev}_u(\mathbf{a}) \cdot \operatorname{ev}_u(\mathbf{b})$ is tantamount to proving that $(\mathbf{ab})[u] = \mathbf{a}[u] \cdot \mathbf{b}[u]$. But the latter equality follows from Theorem 7.6.3 **(a)**. Hence, $\operatorname{ev}_u(\mathbf{ab}) = \operatorname{ev}_u(\mathbf{a}) \cdot \operatorname{ev}_u(\mathbf{b})$ is proven. This proves Claim 3.]

Claim 1 is proven in the same way as Claim 3. Claims 2 and 4 follow easily from Theorem 7.6.3 **(c)**. Claims 5 and 6 are just Claims 1 and 2, repeated. Claim 7 follows easily from Theorem 7.6.3 **(b)**. Thus, we have proven all seven Claims 1, 2, ..., 7. As we explained, this shows that ev_u is a $\mathbb{K}$-algebra homomorphism. Thus, Corollary 7.6.4 holds. □

The map ev_u in Corollary 7.6.4 is called an *evaluation homomorphism* (specifically, the *evaluation homomorphism at u*), since it "evaluates" each polynomial at u.

Corollary 7.6.5. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. Then:

(a) We have $(-\mathbf{a})[u] = -\mathbf{a}[u]$ for each $\mathbf{a} \in \mathbb{K}[x]$.

(b) We have $(\mathbf{a}-\mathbf{b})[u] = \mathbf{a}[u] - \mathbf{b}[u]$ for each $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$.

(c) We have $\left(\sum\limits_{s\in S} \mathbf{a}_s\right)[u] = \sum\limits_{s\in S} (\mathbf{a}_s[u])$ whenever S is a finite set and $\mathbf{a}_s \in \mathbb{K}[x]$ for all $s \in S$.

(d) We have $(\mathbf{a}_1\mathbf{a}_2\cdots\mathbf{a}_k)[u] = \mathbf{a}_1[u] \cdot \mathbf{a}_2[u] \cdot \cdots \cdot \mathbf{a}_k[u]$ whenever $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k \in \mathbb{K}[x]$.

(e) If the ring U is commutative, then $\left(\prod\limits_{s\in S} \mathbf{a}_s\right)[u] = \prod\limits_{s\in S} (\mathbf{a}_s[u])$ whenever S is a finite set and $\mathbf{a}_s \in \mathbb{K}[x]$ for all $s \in S$.

(f) We have $\mathbf{a}^n[u] = (\mathbf{a}[u])^n$ for each $\mathbf{a} \in \mathbb{K}[x]$ and each $n \in \mathbb{N}$.

(g) We have $(n\mathbf{a})[u] = n \cdot \mathbf{a}[u]$ for each $\mathbf{a} \in \mathbb{K}[x]$ and each $n \in \mathbb{Z}$.

Proof of Corollary 7.6.5. Consider the map ev_u in Corollary 7.6.4. This map is a $\mathbb{K}$-algebra homomorphism (by Corollary 7.6.4), and thus is a ring homomorphism. Hence, each part of Corollary 7.6.5 follows from a corresponding part of Proposition 5.9.14 (applied to $\mathbb{K}[x]$, U and ev_u instead of $\mathbb{K}$, $\mathbb{L}$ and f). For example, let us show how Corollary 7.6.5 **(d)** follows from Proposition 5.9.14 **(f)**:

(d) Let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k \in \mathbb{K}[x]$. Then, Proposition 5.9.14 **(f)** (applied to $\mathbb{K}[x]$, U, ev_u and $\mathbf{a}_i$ instead of $\mathbb{K}$, $\mathbb{L}$, f and a_i) yields

$$\operatorname{ev}_u(\mathbf{a}_1\mathbf{a}_2\cdots\mathbf{a}_k) = \operatorname{ev}_u(\mathbf{a}_1)\operatorname{ev}_u(\mathbf{a}_2)\cdots\operatorname{ev}_u(\mathbf{a}_k).$$

Since each $\mathbf{b} \in \mathbb{K}[x]$ satisfies $\operatorname{ev}_u(\mathbf{b}) = \mathbf{b}[u]$ (by the definition of ev_u), this equality rewrites as

$$(\mathbf{a}_1\mathbf{a}_2 \cdots \mathbf{a}_k)[u] = \mathbf{a}_1[u] \cdot \mathbf{a}_2[u] \cdot \cdots \cdot \mathbf{a}_k[u].$$

This proves Corollary 7.6.5 **(d)**. As we said, all the other parts of Corollary 7.6.5 follow similarly from other parts of Proposition 5.9.14. □

Theorem 7.6.3 and Corollary 7.6.5 (or, more abstractly, Corollary 7.6.4) justify the Substitution slogan in general. For example, we can now prove (279) directly, without multiplying out anything, as follows:

$$\begin{aligned}
&\left(x^4 - (x-1)^2(x+1)^2\right)[u] \\
&= \underbrace{x^4[u]}_{\substack{=(x[u])^4 \\ \text{(by Corollary 7.6.5 (f))}}} - \underbrace{\left((x-1)^2(x+1)^2\right)[u]}_{\substack{=(x-1)^2[u]\cdot(x+1)^2[u] \\ \text{(by the second equality of} \\ \text{Theorem 7.6.3 (a))}}} \qquad \text{(by Corollary 7.6.5 (b))} \\
&= \Bigg(\underbrace{x[u]}_{\substack{=u \\ \text{(by Theorem 7.6.3 (d))}}}\Bigg)^4 - \underbrace{(x-1)^2[u]}_{\substack{=((x-1)[u])^2 \\ \text{(by Corollary 7.6.5 (f))}}} \cdot \underbrace{(x+1)^2[u]}_{\substack{=((x+1)[u])^2 \\ \text{(by Corollary 7.6.5 (f))}}} \\
&= u^4 - \Bigg(\underbrace{(x-1)[u]}_{\substack{=x[u]-1[u] \\ \text{(by Corollary 7.6.5 (b))}}}\Bigg)^2 \cdot \Bigg(\underbrace{(x+1)[u]}_{\substack{=x[u]+1[u] \\ \text{(by the first equality of} \\ \text{Theorem 7.6.3 (a))}}}\Bigg)^2 \\
&= u^4 - (x[u] - 1[u])^2 \cdot (x[u] + 1[u])^2 \\
&= u^4 - \Bigg(\underbrace{x[u]}_{\substack{=u \\ \text{(by Theorem 7.6.3 (d))}}} - \underbrace{\underline{1}[u]}_{\substack{=1 \\ \text{(by Theorem 7.6.3 (c))}}}\Bigg)^2 \cdot \Bigg(\underbrace{x[u]}_{\substack{=u \\ \text{(by Theorem 7.6.3 (d))}}} + \underbrace{\underline{1}[u]}_{\substack{=1 \\ \text{(by Theorem 7.6.3 (c))}}}\Bigg)^2 \\
&\qquad \text{(since our "1" here really means "}\underline{1}\text{")} \\
&= u^4 - (u-1)^2(u+1)^2.
\end{aligned}$$

This argument was completely straightforward (despite its length); all we did was "opening the parentheses"[204] using whatever part of Theorem 7.6.3 or Corollary 7.6.5 would let us do that.

[204] more formally: rewriting an expression of the form "(something complicated) $[u]$" in terms of one or several expressions of the form "(something simpler) $[u]$"

Thanks to Corollary 7.6.4 (or the Substitution slogan), the polynomial ring $\mathbb{K}[x]$ is a sort of "forge" for identities that concern an arbitrary element u of an arbitrary $\mathbb{K}$-algebra U. For example, if you want to prove the identity

$$u^3 - u = u(u-1)(u+1) \qquad \text{for any } \mathbb{K}\text{-algebra } U \text{ and any } u \in U,$$

then it suffices to prove the identity

$$x^3 - x = x(x-1)(x+1) \qquad \text{in } \mathbb{K}[x]$$

and then apply ev_u to both sides of it (or, less formally, take the values of both sides at u, and simplify them using the Substitution slogan). Indeed, the map ev_u sends x to u and is a $\mathbb{K}$-algebra homomorphism, whence it also sends $x^3 - x$ to $u^3 - u$ and sends $x(x-1)(x+1)$ to $u(u-1)(u+1)$. The Substitution slogan is saying this at a more concrete level: Indeed, applying the map ev_u is tantamount to "substituting u for x" in a polynomial.

Remark 7.6.6. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. We have defined $\mathbf{a}[u]$ for $\mathbf{a} \in \mathbb{K}[x]$. We can try to define it for arbitrary $\mathbf{a} = (a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]]$ as well. But in general, this will not work, since the sum $\sum_{k\in\mathbb{N}} a_k u^k$ may not be well-defined. However, if u itself is a FPS (that is, $u \in \mathbb{K}[[x]]$) and satisfies $[x^0]\, u = 0$, then the family $(a_k u^k)_{k\in\mathbb{N}}$ is summable (because in this case, we have

$$\left[x^0\right]\left(u^k\right) = \left[x^1\right]\left(u^k\right) = \cdots = \left[x^{k-1}\right]\left(u^k\right) = 0$$

for all $k \in \mathbb{N}$), and therefore $\mathbf{a}[u]$ is well-defined. For example, $\mathbf{a}[x^2]$ is well-defined, and more generally, $\mathbf{a}[x^k]$ is well-defined for every positive integer k; but $\mathbf{a}[1]$ is not well-defined.

We now define the concept of a root of a polynomial:

Definition 7.6.7. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. Let $\mathbf{a} \in \mathbb{K}[x]$.

We say that u is a *root* of $\mathbf{a}$ if $\mathbf{a}[u] = 0$.

This is a very general notion of "root" that we have just defined. You may be used to the idea that a polynomial $\mathbf{a} \in \mathbb{K}[x]$ can have roots in the ring $\mathbb{K}$ itself, but we are allowing roots in any arbitrary $\mathbb{K}$-algebra (e.g., in a matrix algebra $\mathbb{K}^{n\times n}$ or even in the polynomial ring $\mathbb{K}[x]$ itself). For example, the roots of the polynomial $x(x-1)$ in a $\mathbb{K}$-algebra U are the idempotent elements of U, because for any element $u \in U$, we have the following equivalence:

$$\begin{aligned} & (u \text{ is a root of } x(x-1)) \\ \Longleftrightarrow\ & \left(\underbrace{(x(x-1))[u]}_{=x[u]\cdot(x-1)[u]} = 0 \right) \Longleftrightarrow \left(\underbrace{x[u]}_{=u} \cdot \underbrace{(x-1)[u]}_{=u-1} = 0 \right) \\ \Longleftrightarrow\ & \left(\underbrace{u \cdot (u-1)}_{=u^2-u} = 0 \right) \Longleftrightarrow \left(u^2 - u = 0 \right) \Longleftrightarrow \left(u^2 = u \right) \\ \Longleftrightarrow\ & (u \text{ is idempotent}). \end{aligned}$$

If U is a field, then the only idempotent elements of U are 0 and 1 (because $u \cdot (u-1) = 0$ implies that u or $u-1$ is 0). Otherwise, there can be more idempotent elements; for example, $\mathbb{Z}/6$ has the four idempotent elements $[0]_6, [1]_6, [3]_6, [4]_6$.

We now define divisibility of polynomials in the same way as we defined divisibility of integers (Definition 2.2.1) and divisibility of Gaussian integers (Definition 4.2.17):

Definition 7.6.8. Let $\mathbf{a}$ and $\mathbf{b}$ be two polynomials in $\mathbb{K}[x]$. We say that $\mathbf{a} \mid \mathbf{b}$ (or, more precisely, "$\mathbf{a} \mid \mathbf{b}$ in $\mathbb{K}[x]$") if there exists a $\mathbf{c} \in \mathbb{K}[x]$ such that $\mathbf{b} = \mathbf{ac}$.

Be aware that this is a somewhat slippery notion, as its meaning depends on $\mathbb{K}$, which is not reflected in the notation "$\mathbf{a} \mid \mathbf{b}$". For example, the two polynomials $1 + x$ and $2 + 2x$ satisfy $2 + 2x \mid 1 + x$ when $\mathbb{K} = \mathbb{Q}$ (since $1 + x = (2 + 2x) \cdot \dfrac{1}{2}$), but not when $\mathbb{K} = \mathbb{Z}$. Thus, when ambiguity is possible, $\mathbb{K}$ should be specified (i.e., you should write "$\mathbf{a} \mid \mathbf{b}$ in $\mathbb{K}[x]$" rather than just "$\mathbf{a} \mid \mathbf{b}$").

The roots of a polynomial $\mathbf{a} \in \mathbb{K}[x]$ are closely connected to divisors of $\mathbf{a}$ – specifically, ones of the form $x - u$:

Proposition 7.6.9. Let $\mathbf{a}$ be a polynomial in $\mathbb{K}[x]$. Let $u \in \mathbb{K}$. Then,

$$(u \text{ is a root of } \mathbf{a}) \Longleftrightarrow (x - u \mid \mathbf{a}).$$

(Of course, $x - u$ means $x - \underline{u}$.)

Proof of Proposition 7.6.9. $\Longrightarrow$: Assume that u is a root of $\mathbf{a}$. We must prove that $x - u \mid \mathbf{a}$.

We have $x - u \in \mathbb{K}[x]_{\leq 1}$, and the coefficient $[x^1](x-u) \in \mathbb{K}$ is invertible (since this coefficient is 1). Thus, Theorem 7.5.1 **(a)** (applied to $m = 1$ and $\mathbf{b} = x - u$) shows that there exists a **unique** pair $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{q} \cdot (x-u) + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq 1-1}$. Consider this pair.

Now,

$$\begin{aligned} \mathbf{r} \in \mathbb{K}[x]_{\leq 1-1} = \mathbb{K}[x]_{\leq 0} = \{\underline{a} \mid a \in \mathbb{K}\} \qquad & \text{(by Example 7.4.2 **(a)**)} \\ = \{\underline{b} \mid b \in \mathbb{K}\}. \end{aligned}$$

In other words, $\mathbf{r} = \underline{b}$ for some $b \in \mathbb{K}$. Consider this b. Thus, $\mathbf{a} = \mathbf{q} \cdot (x - u) + \underbrace{\mathbf{r}}_{=\underline{b}} = \mathbf{q} \cdot (x - u) + \underline{b}$.

We can substitute u for x in this equation (i.e., apply the $\mathbb{K}$-algebra homomorphism ev_u to both sides of it), and obtain

$$\mathbf{a}[u] = (\mathbf{q} \cdot (x-u) + \underline{b})[u] = \mathbf{q}[u] \cdot \underbrace{(x-u)[u]}_{=u-u=0} + \underbrace{\underline{b}[u]}_{=b} = \underbrace{\mathbf{q}[u] \cdot 0}_{=0} + b = b.$$

Thus, $b = \mathbf{a}[u] = 0$ (since u is a root of $\mathbf{a}$). Hence, $\underline{b} = \underline{0}$, so that

$$\mathbf{a} = \mathbf{q} \cdot (x-u) + \underbrace{\underline{b}}_{=\underline{0}} = \mathbf{q} \cdot (x-u), \qquad \text{and thus } x - u \mid \mathbf{a}.$$

Thus, the "$\Longrightarrow$" direction of Proposition 7.6.9 is proven.

$\Longleftarrow$: Assume that $x - u \mid \mathbf{a}$. We must prove that u is a root of $\mathbf{a}$.

We have $x - u \mid \mathbf{a}$. In other words, $\mathbf{a} = (x-u) \cdot \mathbf{c}$ for some polynomial $\mathbf{c}$. Substituting u for x in this equation, we obtain

$$\mathbf{a}[u] = \underbrace{(u-u)}_{=0} \cdot \mathbf{c}[u] = 0,$$

so that u is a root of $\mathbf{a}$. Thus, the "$\Longleftarrow$" direction of Proposition 7.6.9 is proven. □

> **Example 7.6.10.** Let $\mathbb{K} = \mathbb{Z}/6$ and $\mathbf{a} = x^2 - x$. Then, the roots of $\mathbf{a}$ in $\mathbb{K}$ are precisely the idempotent elements of $\mathbb{K}$; these are $0, 1, 3, 4$. So the previous proposition yields that $x - 0$, $x - 1$, $x - 3$ and $x - 4$ all divide $\mathbf{a}$. However, this does not mean that the product $(x-0)(x-1)(x-3)(x-4)$ divides $\mathbf{a}$. Instead, we have
>
> $$\mathbf{a} = (x-0)(x-1) = (x-3)(x-4) \qquad \text{in } \mathbb{K}[x].$$

If this example appears weird, keep in mind that $\mathbb{Z}/6$ is not a field. When $\mathbb{K}$ is a field, the polynomial ring $\mathbb{K}[x]$ behaves very much like $\mathbb{Z}$ or $\mathbb{Z}[i]$: We have division with remainder by any nonzero polynomial; we have gcds; we have a notion of "primes" (which are called irreducible polynomials); and every nonzero polynomial has a unique factorization into primes (up to units, which are the nonzero constant polynomials). But when $\mathbb{K}$ is merely a commutative ring, this can all break down; in particular, Example 7.6.10 shows that the factorization into primes (when it exists) is not unique.

The following theorem is often called the "*easy half of the Fundamental Theorem of Algebra*":

> **Theorem 7.6.11.** Let $\mathbb{K}$ be a field. Let $n \in \mathbb{N}$. Then, any nonzero polynomial $\mathbf{a} \in \mathbb{K}[x]$ of degree $\leq n$ has at most n roots in $\mathbb{K}$. (We are not counting the roots with multiplicity here.)

Proof of Theorem 7.6.11. Induction on n.

The base case ($n = 0$) is obvious, since a nonzero constant polynomial has no roots.

Induction step: Let n be a positive integer. Assume (as induction hypothesis) that any nonzero polynomial of degree $\leq n-1$ has at most $n-1$ roots in $\mathbb{K}$. We must prove the analogous fact for n.

Let $\mathbf{a} \in \mathbb{K}[x]$ be a nonzero polynomial of degree $\leq n$. We must prove that $\mathbf{a}$ has at most n roots in $\mathbb{K}$. If $\mathbf{a}$ has no roots at all, then we are done. So WLOG assume that $\mathbf{a}$ has a root $u \in \mathbb{K}$. Then, $x - u \mid \mathbf{a}$ (by Proposition 7.6.9). Hence,

$$\mathbf{a} = (x-u) \cdot \mathbf{c} \qquad \text{for some } \mathbf{c} \in \mathbb{K}[x].$$

Consider this $\mathbf{c}$. From $\mathbf{a} = (x-u) \cdot \mathbf{c}$, we obtain

$$\begin{aligned} \deg \mathbf{a} &= \deg\left((x-u) \cdot \mathbf{c}\right) = \underbrace{\deg(x-u)}_{=1} + \deg \mathbf{c} \qquad \text{(since } \mathbb{K} \text{ is a field)} \\ &= 1 + \deg \mathbf{c}, \end{aligned}$$

so that $\deg \mathbf{c} = \underbrace{\deg \mathbf{a}}_{\leq n} - 1 \leq n-1$. Thus, $\mathbf{c}$ is a polynomial of degree $\leq n-1$, and thus has at most $n-1$ roots in $\mathbb{K}$ (by the induction hypothesis).

Next, we claim that every root of $\mathbf{a}$ other than u must be a root of $\mathbf{c}$.

[*Proof:* Let v be a root of $\mathbf{a}$ other than u. We must prove that v is a root of $\mathbf{c}$.

By definition of v, we have $v \neq u$ and $\mathbf{a}[v] = 0$. From $v \neq u$, we obtain $v - u \neq 0$, and thus $v - u \in \mathbb{K}$ is invertible (since $\mathbb{K}$ is a field). But substituting v for x in $\mathbf{a} = (x-u) \cdot \mathbf{c}$, we obtain

$$\mathbf{a}[v] = (v-u) \cdot \mathbf{c}[v].$$

Thus, $(v-u) \cdot \mathbf{c}[v] = \mathbf{a}[v] = 0$. We can divide this equation by $v-u$ (since $v-u$ is invertible), and thus obtain $\mathbf{c}[v] = 0$. In other words, v is a root of $\mathbf{c}$. As we claimed.]

The claim that we just proved shows that $\mathbf{a}$ has at most one more root than $\mathbf{c}$. Thus, $\mathbf{a}$ has at most n roots (since $\mathbf{c}$ has at most $n-1$ roots). This completes the induction step. Hence, Theorem 7.6.11 is proven. □

When $\mathbb{K}$ is just an arbitrary field, the number of roots of a degree-n nonzero polynomial over $\mathbb{K}$ can be much smaller than n. For example, the polynomial $x^2 + 1 \in \mathbb{R}[x]$ has 0 roots in $\mathbb{R}$ (but it has 2 roots in $\mathbb{C}$). The "hard half" of the Fundamental Theorem of Algebra says that a nonzero polynomial $\mathbf{a} \in \mathbb{C}[x]$ of degree n has exactly n roots in $\mathbb{C}$, counted with multiplicity. As I said before, this is not a theorem of algebra, since it relies on the fact that $\mathbb{C}$ has a topology and is closed in this topology.

Next comes a little potpourri of properties of polynomials:

Proposition 7.6.12. Let $\mathbf{a}$ and $\mathbf{b}$ be two nonzero polynomials in $\mathbb{K}[x]$.
(a) We have $\deg(\mathbf{a}[\mathbf{b}]) \leq \deg \mathbf{a} \cdot \deg \mathbf{b}$.
(b) If $\mathbb{K}$ is a field, then this inequality is an equality.

Proof of Proposition 7.6.12. Easy. □

Proposition 7.6.13. Let U and V be two $\mathbb{K}$-algebras. Let $f : U \to V$ be a $\mathbb{K}$-algebra homomorphism. Let $u \in U$ and $\mathbf{a} \in \mathbb{K}[x]$. Then,

$$f(\mathbf{a}[u]) = \mathbf{a}[f(u)].$$

Proof of Proposition 7.6.13. For example, if $\mathbf{a} = x^3 + 2x + 5$, then this is saying

$$f\left(u^3 + 2u + 5\right) = (f(u))^3 + 2f(u) + 5$$

(because $\mathbf{a}[u] = u^3 + 2u + 5$ and $\mathbf{a}[f(u)] = (f(u))^3 + 2f(u) + 5$ in this case). But this equality is true, since f preserves addition, multiplication, scaling, zero and unity (because f is a $\mathbb{K}$-algebra homomorphism).

The proof of Proposition 7.6.13 in the general case follows this example. Here are the details:

First we notice that f is a ring homomorphism (since f is a $\mathbb{K}$-algebra homomorphism). Thus,

$$f\left(u^k\right) = (f(u))^k \qquad \text{for all } k \in \mathbb{N} \tag{281}$$

(by Proposition 5.9.14 **(h)**, applied to U, V, u and k instead of $\mathbb{K}$, $\mathbb{L}$, a and n). Now, write the polynomial $\mathbf{a} \in \mathbb{K}[x]$ in the form $\mathbf{a} = (a_0, a_1, a_2, \ldots)$. Then, the definition of $\mathbf{a}[u]$ yields

$$\mathbf{a}[u] = \sum_{k\in\mathbb{N}} a_k u^k, \tag{282}$$

whereas the definition of $\mathbf{a}[f(u)]$ yields

$$\mathbf{a}[f(u)] = \sum_{k\in\mathbb{N}} a_k (f(u))^k. \tag{283}$$

Now, applying the map f to both sides of the equality (282), we find

$$f(\mathbf{a}[u]) = f\left(\sum_{k\in\mathbb{N}} a_k u^k\right) = \sum_{k\in\mathbb{N}} f\left(a_k u^k\right). \tag{284}$$

Here, the last equality sign needs a bit of a justification. It is tempting to say that this equality sign follows from Proposition 5.9.14 **(e)**, but this is not quite precise: The set S in Proposition 5.9.14 **(e)** is required to be finite, while the set $\mathbb{N}$, which the sums in (284) are ranging over, is infinite. However, $\mathbf{a}$ is a polynomial; in other words, all but finitely many $i \in \mathbb{N}$ satisfy $a_i = 0$ (by the definition of a polynomial). In other words, there exists a finite subset S of $\mathbb{Z}$ such that

$$\text{all } i \in \mathbb{N} \setminus S \text{ satisfy } a_i = 0. \tag{285}$$

Consider this S. Now, each $k \in \mathbb{N}$ satisfies either $k \in S$ or $k \notin S$ (but not both at once); hence,

$$\begin{aligned}\sum_{k\in\mathbb{N}} a_k u^k &= \sum_{\underbrace{\substack{k\in\mathbb{N};\\ k\in S}}_{\substack{=\sum\limits_{k\in S}\\ (\text{since } S\subseteq\mathbb{N})}}} a_k u^k + \sum_{\underbrace{\substack{k\in\mathbb{N};\\ k\notin S}}_{=\sum\limits_{k\in\mathbb{N}\setminus S}}} a_k u^k = \sum_{k\in S} a_k u^k + \sum_{k\in\mathbb{N}\setminus S} \underbrace{a_k}_{\substack{=0\\ (\text{by (285),}\\ \text{applied to } i=k)}} u^k \\ &= \sum_{k\in S} a_k u^k + \underbrace{\sum_{k\in\mathbb{N}\setminus S} 0u^k}_{=0} = \sum_{k\in S} a_k u^k.\end{aligned}$$

Applying the map f to both sides of this equality, we find

$$f\left(\sum_{k\in\mathbb{N}} a_k u^k\right) = f\left(\sum_{k\in S} a_k u^k\right) = \sum_{k\in S} f\left(a_k u^k\right) \qquad (286)$$

(by Proposition 5.9.14 **(e)**, since the set S is finite). But if $k \in \mathbb{N} \setminus S$, then $a_k = 0$ (by (285), applied to $i = k$) and thus $\underbrace{a_k}_{=0} u^k = 0$ and thus

$$f\left(\underbrace{a_k u^k}_{=0}\right) = f(0) = 0 \qquad (287)$$

(since f is a $\mathbb{K}$-linear map[205]). Now, again, recall that each $k \in \mathbb{N}$ satisfies either $k \in S$ or $k \notin S$ (but not both at once); hence,

$$\begin{aligned}\sum_{k\in\mathbb{N}} f\left(a_k u^k\right) &= \sum_{\underbrace{\substack{k\in\mathbb{N};\\ k\in S}}_{\substack{=\sum\limits_{k\in S}\\ (\text{since } S\subseteq\mathbb{N})}}} f\left(a_k u^k\right) + \sum_{\underbrace{\substack{k\in\mathbb{N};\\ k\notin S}}_{=\sum\limits_{k\in\mathbb{N}\setminus S}}} f\left(a_k u^k\right) = \sum_{k\in S} f\left(a_k u^k\right) + \sum_{k\in\mathbb{N}\setminus S} \underbrace{f\left(a_k u^k\right)}_{\substack{=0\\ (\text{by (287)})}} \\ &= \sum_{k\in S} f\left(a_k u_k\right).\end{aligned}$$

Comparing this with (286), we obtain $f\left(\sum\limits_{k\in\mathbb{N}} a_k u^k\right) = \sum\limits_{k\in\mathbb{N}} f\left(a_k u^k\right)$. Thus, the last equality sign in (284) has been justified. (This sort of straightforward argument is commonly left unsaid when working with polynomials, because it is almost completely automatic; the main idea is "reduce the infinite sum to a finite sum by throwing out vanishing addends".)

Now that (284) is proven, we can move on. The map f is $\mathbb{K}$-linear (since it is a $\mathbb{K}$-algebra homomorphism). Hence, for each $k \in \mathbb{N}$, we have

$$f\left(a_k u^k\right) = a_k \underbrace{f\left(u^k\right)}_{\substack{=(f(u))^k\\ (\text{by (281)})}} = a_k \left(f(u)\right)^k.$$

[205] because f is a $\mathbb{K}$-algebra homomorphism

Hence, (284) rewrites as

$$f\left(\mathbf{a}\left[u\right]\right) = \sum_{k\in\mathbb{N}} a_k \left(f\left(u\right)\right)^k .$$

Comparing this with (283), we obtain $f\left(\mathbf{a}\left[u\right]\right) = \mathbf{a}\left[f\left(u\right)\right]$. Thus, Proposition 7.6.13 is proven. □

Proposition 7.6.14. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. Let $\mathbf{a}, \mathbf{b} \in \mathbb{K}\left[x\right]$. Then,

$$\mathbf{a}\left[\mathbf{b}\left[u\right]\right] = \left(\mathbf{a}\left[\mathbf{b}\right]\right)\left[u\right].$$

Proof of Proposition 7.6.14. The map $\operatorname{ev}_u : \mathbb{K}\left[x\right] \to U$ is a $\mathbb{K}$-algebra homomorphism (by Corollary 7.6.4). Hence, Proposition 7.6.13 (applied to $\mathbb{K}\left[x\right]$, U, ev_u and $\mathbf{b}$ instead of U, V, f and u) yields $\operatorname{ev}_u\left(\mathbf{a}\left[\mathbf{b}\right]\right) = \mathbf{a}\left[\operatorname{ev}_u\left(\mathbf{b}\right)\right]$. But the definition of ev_u yields $\operatorname{ev}_u\left(\mathbf{b}\right) = \mathbf{b}\left[u\right]$ and $\operatorname{ev}_u\left(\mathbf{a}\left[\mathbf{b}\right]\right) = \left(\mathbf{a}\left[\mathbf{b}\right]\right)\left[u\right]$. Hence, $\left(\mathbf{a}\left[\mathbf{b}\right]\right)\left[u\right] = \operatorname{ev}_u\left(\mathbf{a}\left[\mathbf{b}\right]\right) = \mathbf{a}\left[\underbrace{\operatorname{ev}_u\left(\mathbf{b}\right)}_{=\mathbf{b}\left[u\right]}\right] = \mathbf{a}\left[\mathbf{b}\left[u\right]\right]$. This proves Proposition 7.6.14. □

One more notation is needed for the next section.

Definition 7.6.15. Let $\mathbb{L}$ be a ring that contains $\mathbb{Q}$ as a subring. (For example, $\mathbb{L}$ can be $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{Q}\left[x\right]$.)

Recall that in Definition 2.17.1, we have defined the binomial coefficient $\dbinom{n}{k}$ for all $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$. We extend the very same definition to all $n \in \mathbb{L}$.

Thus, in particular, we have a polynomial $\dbinom{x}{k} \in \mathbb{Q}\left[x\right]$ for each $k \in \mathbb{Q}$. This polynomial $\dbinom{x}{k}$ is explicitly given by

$$\binom{x}{k} = \frac{x\left(x-1\right)\left(x-2\right)\cdots\left(x-k+1\right)}{k!} \qquad \text{when } k \in \mathbb{N} \tag{288}$$

(and equals 0 when $k \notin \mathbb{N}$). More generally, for each polynomial $\mathbf{a} \in \mathbb{Q}\left[x\right]$ and each $k \in \mathbb{N}$, we have a polynomial

$$\binom{\mathbf{a}}{k} = \frac{\mathbf{a}\left(\mathbf{a}-1\right)\left(\mathbf{a}-2\right)\cdots\left(\mathbf{a}-k+1\right)}{k!}. \tag{289}$$

The following is easy:

Corollary 7.6.16. Let $k \in \mathbb{N}$.

(a) Then, $\dbinom{x}{k}$ is a polynomial of degree k.

(b) For each $u \in \mathbb{Q}$, we have $\dbinom{x}{k}[u] = \dbinom{u}{k}$.

(c) For each $\mathbf{a} \in \mathbb{Q}[x]$ and $u \in \mathbb{Q}$, we have $\dbinom{\mathbf{a}}{k}[u] = \dbinom{\mathbf{a}[u]}{k}$.

Proof of Corollary 7.6.16. **(a)** This follows from (288) and Proposition 7.4.13 **(b)** (applied to $\mathbf{a}_i = x - i + 1$).

(b) Let $u \in \mathbb{Q}$. Evaluating both sides of the equality (288) at u (that is, applying the evaluation homomorphism $\operatorname{ev}_u : \mathbb{Q}[x] \to \mathbb{Q}$ to this equality), we obtain

$$\begin{aligned}
\binom{x}{k}[u] &= \frac{x(x-1)(x-2)\cdots(x-k+1)}{k!}[u] \\
&= \frac{(x[u])(x[u]-1[u])(x[u]-2[u])\cdots(x[u]-(k-1)[u])}{k!} \\
&\qquad (\text{since } \operatorname{ev}_u \text{ is a } \mathbb{Q}\text{-algebra homomorphism}) \\
&= \frac{u(u-1)(u-2)\cdots(u-k+1)}{k!} \\
&\qquad (\text{since } x[u] = u \text{ and } i[u] = i \text{ for all integers } i) \\
&= \binom{u}{k} \qquad \left(\text{by the definition of } \binom{u}{k}\right).
\end{aligned}$$

This proves Corollary 7.6.16 **(b)**.

(c) Let $\mathbf{a} \in \mathbb{Q}[x]$ and $u \in \mathbb{Q}$. Evaluating both sides of the equality (289) at u (that is, applying the evaluation homomorphism $\operatorname{ev}_u : \mathbb{Q}[x] \to \mathbb{Q}$ to this equality), we obtain

$$\begin{aligned}
\binom{\mathbf{a}}{k}[u] &= \frac{\mathbf{a}(\mathbf{a}-1)(\mathbf{a}-2)\cdots(\mathbf{a}-k+1)}{k!}[u] \\
&= \frac{(\mathbf{a}[u])(\mathbf{a}[u]-1[u])(\mathbf{a}[u]-2[u])\cdots(\mathbf{a}[u]-(k-1)[u])}{k!} \\
&\qquad (\text{since } \operatorname{ev}_u \text{ is a } \mathbb{Q}\text{-algebra homomorphism}) \\
&= \frac{(\mathbf{a}[u])(\mathbf{a}[u]-1)(\mathbf{a}[u]-2)\cdots(\mathbf{a}[u]-k+1)}{k!} \\
&\qquad (\text{since } i[u] = i \text{ for all integers } i) \\
&= \binom{\mathbf{a}[u]}{k} \qquad \left(\text{by the definition of } \binom{\mathbf{a}[u]}{k}\right).
\end{aligned}$$

This proves Corollary 7.6.16 **(c)**. □

7.7. The polynomial identity trick

Convention 7.7.1. For this whole section, let $\mathbb{K}$ be a field.

7.7.1. Enough equal values make polynomials equal

Corollary 7.7.2. Let $\mathbf{a}$ and $\mathbf{b}$ be two polynomials of degree $\leq n$ over the field $\mathbb{K}$. Assume that at least $n+1$ many elements $u \in \mathbb{K}$ satisfy $\mathbf{a}[u] = \mathbf{b}[u]$. Then, $\mathbf{a} = \mathbf{b}$.

Proof of Corollary 7.7.2. Clearly, $\mathbf{a} - \mathbf{b}$ is a polynomial of degree $\leq n$.

Moreover, at least $n+1$ many elements $u \in \mathbb{K}$ satisfy $(\mathbf{a} - \mathbf{b})[u] = 0$ (since this is what $\mathbf{a}[u] = \mathbf{b}[u]$ means). In other words, the polynomial $\mathbf{a} - \mathbf{b}$ must have at least $n+1$ roots in $\mathbb{K}$.

But Theorem 7.6.11 (applied to $\mathbf{a} - \mathbf{b}$ instead of $\mathbf{a}$) yields that if $\mathbf{a} - \mathbf{b}$ is nonzero, then $\mathbf{a} - \mathbf{b}$ has at most n roots in $\mathbb{K}$. This would contradict the preceding sentence. So $\mathbf{a} - \mathbf{b}$ cannot be nonzero. In other words, $\mathbf{a} - \mathbf{b} = \underline{0}$. In other words, $\mathbf{a} = \mathbf{b}$. This proves Corollary 7.7.2. □

I like to refer to the following corollary as "the *polynomial identity trick*":

Corollary 7.7.3. Let $\mathbf{a}$ and $\mathbf{b}$ be two polynomials over the field $\mathbb{K}$. Assume that infinitely many elements $u \in \mathbb{K}$ satisfy $\mathbf{a}[u] = \mathbf{b}[u]$. Then, $\mathbf{a} = \mathbf{b}$.

Proof of Corollary 7.7.3. Choose an $n \in \mathbb{N}$ such that $\mathbf{a}$ and $\mathbf{b}$ have degree $\leq n$. Then, apply Corollary 7.7.2. □

Example 7.7.4. Corollary 7.7.3 can be false when $\mathbb{K}$ is not a field. For an example, pick any infinite set S, and let $\mathbb{K}$ be the commutative ring $(\mathcal{P}(S), \triangle, \cap, \varnothing, S)$ constructed in Section 5.2. Let $n = 2$, $\mathbf{a} = x^2 - x$ and $\mathbf{b} = \underline{0}$. Then, **each** $u \in \mathbb{K}$ satisfies $\mathbf{a}[u] = \mathbf{b}[u]$ (because $\mathbf{a}[u] = u^2 - u = \underbrace{u \cap u}_{=u} - u = u - u = \varnothing = 0_{\mathbb{K}} = \underline{0}[u] = \mathbf{b}[u]$); thus, in particular, infinitely many elements $u \in \mathbb{K}$ satisfy $\mathbf{a}[u] = \mathbf{b}[u]$. But it is not true that $\mathbf{a} = \mathbf{b}$.

We can now prove Proposition 2.17.16:

Proof of Proposition 2.17.16. The polynomials P and Q are polynomials over the field $\mathbb{Q}$. We have assumed that infinitely many $u \in \mathbb{Q}$ satisfy $P(u) = Q(u)$. In other words, infinitely many $u \in \mathbb{Q}$ satisfy $P[u] = Q[u]$ (since we are now using the notation $\mathbf{a}[u]$ for what we previously denoted by $\mathbf{a}(u)$). Hence, Corollary 7.7.3 (applied to $\mathbb{K} = \mathbb{Q}$, $\mathbf{a} = P$ and $\mathbf{b} = Q$) yields $P = Q$. This proves Proposition 2.17.16. □

We can now finish our proof of Theorem 2.17.14 by putting on solid ground everything we used about polynomials in that proof:

Finishing touches to our proof of Theorem 2.17.14. In the proof of Lemma 2.17.17, we defined two polynomials P and Q by (85) and (86). Both of these P and Q are well-defined polynomials in $\mathbb{Q}[x]$, due to Corollary 7.6.16. Moreover, substituting u for x into these polynomials works exactly as we claimed in our proof of Lemma 2.17.17 (i.e., for example, we have $P(u) = \dbinom{u+b}{n}$), due to parts **(b)** and **(c)** of Corollary 7.6.16. The same holds for the polynomials P and Q defined in the proof of Lemma 2.17.18. But these two lemmas were the only places in which polynomials were used in our above proof of Theorem 2.17.14. Hence, our proof of Theorem 2.17.14 is now on solid ground. □

7.7.2. Lagrange interpolation

Corollary 7.7.2 shows that for any $n \in \mathbb{N}$, a polynomial of degree $\leq n$ over a field $\mathbb{K}$ is uniquely determined by its values on any $n+1$ (given) distinct elements of $\mathbb{K}$. There is a matching existence claim to this uniqueness claim: To any choice of values at any $n+1$ given distinct elements of $\mathbb{K}$, you can find excatly one polynomial of degree $\leq n$ over $\mathbb{K}$ that takes these values at these elements. This polynomial can even be determined explicitly, as the following theorem shows:

Theorem 7.7.5. Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_{n+1}$ be $n+1$ distinct elements of a field $\mathbb{K}$. Let $b_1, b_2, \ldots, b_{n+1}$ be $n+1$ arbitrary elements of $\mathbb{K}$.

(a) There is a unique polynomial $\mathbf{f} \in \mathbb{K}[x]_{\leq n}$ satisfying

$$\left(\mathbf{f}[a_i] = b_i \qquad \text{for all } i \in \{1, 2, \ldots, n+1\}\right). \tag{290}$$

(b) This polynomial $\mathbf{f}$ is given by

$$\mathbf{f} = \sum_{j=1}^{n+1} b_j \frac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)}$$

(where the "$\prod\limits_{k \neq j}$" signs mean "$\prod\limits_{\substack{k \in \{1,2,\ldots,n+1\};\\ k \neq j}}$").

Theorem 7.7.5 is known as the *Lagrange interpolation theorem*. Before we prove it, let us remark that it generalizes (and concretizes) Proposition 1.6.6 (which is its particular case for $n = 2$ and $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{R}$). After proving it, we will discuss how it helps make Shamir's Secret Sharing Scheme work. We also notice that Theorem 7.7.5 requires $\mathbb{K}$ to be a field; when $\mathbb{K}$ is merely a commutative ring, both the "existence" and "uniqueness" parts of Theorem 7.7.5 **(a)** may fail, and the fractions appearing in Theorem 7.7.5 **(b)** may fail to be well-defined (since their denominators $a_j - a_k$ may fail to be invertible). We have already witnessed the failure of the "existence" part of Theorem 7.7.5 **(a)** in the case when $\mathbb{K} = \mathbb{Z}$:

Indeed, if we set

$$\begin{array}{llll} n = 2, & a_1 = 0, & a_2 = 1, & a_3 = 2, \\ & b_1 = 0, & b_2 = 0, & b_3 = 1, \end{array}$$

then there exists no polynomial $\mathbf{f} \in \mathbb{Z}[x]_{\leq 2}$ satisfying $\mathbf{f}[a_i] = b_i$ for all $i \in \{1, 2, 3\}$. (The polynomial $\dbinom{x}{2}$ would satisfy this, but it is not a polynomial in $\mathbb{Z}[x]_{\leq 2}$, since its coefficients are not integers. We have already observed this in Example 2.17.24 **(a)**.)

Proof of Theorem 7.7.5. Define a polynomial $\mathbf{g} \in \mathbb{K}[x]$ by

$$\mathbf{g} = \sum_{j=1}^{n+1} b_j \frac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)} \tag{291}$$

(where the "$\prod\limits_{k \neq j}$" signs mean "$\prod\limits_{\substack{k \in \{1,2,\ldots,n+1\};\\ k \neq j}}$"). Note that $\mathbf{g}$ is well-defined; indeed, all the differences $a_j - a_k$ appearing in the denominators are nonzero (because $a_1, a_2, \ldots, a_{n+1}$ are distinct) and thus invertible (since $\mathbb{K}$ is a field).

Each of the $n+1$ addends $b_j \dfrac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)}$ on the right hand side of (291) belongs to $\mathbb{K}[x]_{\leq n}$ [206]. Hence, their sum must belong to $\mathbb{K}[x]_{\leq n}$ as well (since $\mathbb{K}[x]_{\leq n}$ is a $\mathbb{K}$-module). In other words, $\mathbf{g}$ belongs to $\mathbb{K}[x]_{\leq n}$ (since (291) shows that the sum of these $n+1$ addends is $\mathbf{g}$). In other words, $\mathbf{g} \in \mathbb{K}[x]_{\leq n}$.

If $i \in \{1, 2, \ldots, n+1\}$ and $j \in \{1, 2, \ldots, n+1\}$ satisfy $j \neq i$, then we have

$$\prod_{k \neq j} (a_i - a_k) = 0 \tag{292}$$

(because in this case, the product $\prod\limits_{k \neq j} (a_i - a_k)$ contains the factor $a_i - a_i$ (since $i \neq j$), but this factor is 0, and therefore the whole product is 0).

[206] *Proof.* Let $j \in \{1, 2, \ldots, n+1\}$. We must prove that $b_j \dfrac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)} \in \mathbb{K}[x]_{\leq n}$.

Indeed, the product $\prod\limits_{k \neq j} (x - a_k)$ has exactly n factors, each of which is a polynomial of degree 1. Thus, this product has degree $\leq n$ (by Proposition 7.4.13 **(a)**), i.e., belongs to $\mathbb{K}[x]_{\leq n}$. The polynomial $b_j \dfrac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)}$ is obtained by scaling this product by $\dfrac{b_j}{\prod\limits_{k \neq j} (a_j - a_k)} \in \mathbb{K}$; thus, it also belongs to $\mathbb{K}[x]_{\leq n}$ (since $\mathbb{K}[x]_{\leq n}$ is a $\mathbb{K}$-module). Qed.

For each $i \in \{1, 2, \ldots, n+1\}$, we have

$$\begin{aligned}
\mathbf{g}[a_i] &= \left(\sum_{j=1}^{n+1} b_j \dfrac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)} \right) [a_i] \qquad \text{(by the definition of } \mathbf{g}\text{)} \\
&= \sum_{j=1}^{n+1} b_j \dfrac{\prod\limits_{k \neq j} (a_i - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)} \\
&= b_i \underbrace{\dfrac{\prod\limits_{k \neq i} (a_i - a_k)}{\prod\limits_{k \neq i} (a_i - a_k)}}_{=1} + \sum_{\substack{j \in \{1,2,\ldots,n+1\}; \\ j \neq i}} b_j \underbrace{\dfrac{\prod\limits_{k \neq j} (a_i - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)}}_{\substack{=0 \\ \text{(by (292))}}} \\
&\qquad \text{(here, we have split off the addend for } j = i \text{ from the sum)} \\
&= b_i + \underbrace{\sum_{\substack{j \in \{1,2,\ldots,n+1\}; \\ j \neq i}} b_j 0}_{=0} = b_i .
\end{aligned}$$

Hence, $\mathbf{g}$ is a polynomial $\mathbf{f} \in \mathbb{K}[x]_{\leq n}$ satisfying (290) (since we already know that $\mathbf{g} \in \mathbb{K}[x]_{\leq n}$).

(a) We need to prove that there is a unique polynomial $\mathbf{f} \in \mathbb{K}[x]_{\leq n}$ satisfying (290). We already know that such an $\mathbf{f}$ exists (because we have just shown that $\mathbf{g}$ is such an $\mathbf{f}$); thus, it remains to prove its uniqueness. In other words, we need to prove the following claim:

> *Claim 1:* Let $\mathbf{f}_1$ and $\mathbf{f}_2$ be two polynomials $\mathbf{f} \in \mathbb{K}[x]_{\leq n}$ satisfying (290). Then, $\mathbf{f}_1 = \mathbf{f}_2$.

[*Proof of Claim 1:* We have assumed that $\mathbf{f}_1$ is a polynomial $\mathbf{f} \in \mathbb{K}[x]_{\leq n}$ satisfying (290). In other words, $\mathbf{f}_1 \in \mathbb{K}[x]_{\leq n}$ is a polynomial and satisfies

$$\mathbf{f}_1[a_i] = b_i \qquad \text{for all } i \in \{1, 2, \ldots, n+1\}. \tag{293}$$

Similarly, $\mathbf{f}_2 \in \mathbb{K}[x]_{\leq n}$ is a polynomial and satisfies

$$\mathbf{f}_2[a_i] = b_i \qquad \text{for all } i \in \{1, 2, \ldots, n+1\}. \tag{294}$$

The polynomials $\mathbf{f}_1$ and $\mathbf{f}_2$ belong to $\mathbb{K}[x]_{\leq n}$; in other words, they have degree $\leq n$. Moreover, each $i \in \{1, 2, \ldots, n+1\}$ satisfies $\mathbf{f}_1[a_i] = \mathbf{f}_2[a_i]$ (as we can see by comparing (293) with (294)). Thus, at least $n+1$ many elements $u \in \mathbb{K}$ satisfy $\mathbf{f}_1[u] = \mathbf{f}_2[u]$ (namely, the $n+1$ elements $a_1, a_2, \ldots, a_{n+1}$ satisfy this[207]). Hence,

[207] Recall that $a_1, a_2, \ldots, a_{n+1}$ are distinct (by assumption), so they actually do constitute $n+1$ many elements $u \in \mathbb{K}$.

Corollary 7.7.2 (applied to $\mathbf{a} = \mathbf{f}_1$ and $\mathbf{b} = \mathbf{f}_2$) shows that $\mathbf{f}_1 = \mathbf{f}_2$. This proves Claim 1.]

Now, our proof of Theorem 7.7.5 **(a)** is complete.

(b) In our above proof of Theorem 7.7.5 **(a)**, we have shown not just that there is a unique polynomial $\mathbf{f} \in \mathbb{K}[x]_{\leq n}$ satisfying (290); we have also shown that $\mathbf{g}$ is such a polynomial. But since this $\mathbf{f}$ is unique, this means that $\mathbf{g}$ is the **only** such polynomial. This proves Theorem 7.7.5 **(b)**. □

7.7.3. Application: Curve fitting

Theorem 7.7.5 has multiple applications.

The most obvious one is to treat Theorem 7.7.5 as an interpolation theorem: Roughly speaking, it says that $n+1$ values (at distinct points) in a field can always be fit by a unique polynomial of degree $\leq n$. See the Wikipedia pages for Lagrange polynomials and polynomial interpolation, but beware that this is not the kind of interpolation that is a good choice for curve-fitting practical datasets (which rarely follow a polynomial rule). It is best suited for interpolating functions when you can freely choose the points at which you sample (i.e., the a_i in Theorem 7.7.5); certain choices of a_i fare much better than others. Thus, Lagrange interpolation can also be used in designing numerical quadrature rules. See [Trefet11] for details.

7.7.4. Application: Shamir's Secret Sharing Scheme

Here is another application of Theorem 7.7.5. Shamir's Secret Sharing Scheme (as presented in Subsection 1.6.7 and fixed in Remark 5.6.3) can now finally be implemented concretely. Indeed, consider the setting of Section 1.6 with general n and k, and assume that the secret $\mathbf{a}$ that we want to distribute is a bitstring of length N. As in Remark 5.6.3, we pick a prime p such that both $p \geq 2^N$ and $p > n$, and we encode $\mathbf{a}$ as a residue class $\alpha \in \mathbb{Z}/p$. Pick $k-1$ uniformly random elements $\beta_1, \beta_2, \ldots, \beta_{k-1}$ of $\mathbb{Z}/p$, and define the polynomial

$$\mathbf{f} = \beta_{k-1}x^{k-1} + \beta_{k-2}x^{k-2} + \cdots + \beta_1 x^1 + \alpha \in (\mathbb{Z}/p)[x]_{\leq k-1}.$$

Reveal to each person $i \in \{1, 2, \ldots, n\}$ the value $\mathbf{f}\left[[i]_p\right]$. Then, Theorem 7.7.5 (applied to $k-1$ instead of n) shows that any k of the n people can uniquely reconstruct $\mathbf{f}$ (since they know the values of $\mathbf{f}$ at k distinct elements of $\mathbb{Z}/p$ [208]), whereas $k-1$ of the n people cannot gain any knowledge about the secret $\mathbf{a}$ (since they only know the values of $\mathbf{f}$ at $k-1$ nonzero elements of $\mathbb{Z}/p$ [209], and these values could be combined with any possible value at $[0]_p$ to form a valid polynomial in $(\mathbb{Z}/p)[x]_{\leq k-1}$). Thus, both Requirements 1 and 2 from Section 1.6 are satisfied. This is Shamir's Secret Sharing Scheme in its final form.

[208] Here we are using the fact that the elements $[1]_p, [2]_p, \ldots, [n]_p$ of $\mathbb{Z}/p$ are distinct (since $p > n$).

[209] Here we are using the fact that the elements $[1]_p, [2]_p, \ldots, [n]_p$ of $\mathbb{Z}/p$ are nonzero (since $p > n$).

Instead of $\mathbb{Z}/p$ we could have used any finite field $\mathbb{F}$ whose size is $\geq 2^N$ and $> n$, but we would need to be careful, since the elements $[1]_p, [2]_p, \ldots, [n]_p$ would no longer necessarily be distinct and nonzero. Thus, we would have to use n distinct nonzero elements of $\mathbb{F}$ instead.

7.7.5. Application: Reed–Solomon codes

Finally, here is a far more important application of Theorem 7.7.5.

Assume that you want to send digital data over a noisy channel (e.g., radio). "Noisy" means that the transmission will introduce errors, and you expect (e.g.) that every bit you send has a small probability p of getting corrupted on its way[210]. You want to ensure that the recepient gets the correct bits that you sent him.[211] How can you do this?

Of course, you cannot guarantee this with complete surety. But there are several schemes that you can use to make it rather likely. They are called *error-correcting codes*.

- For instance, let us assume you have agreed with your recepient that you will be sending each bit **twice** in a row. Then, if the recepient gets two different bits when they expect the same bit sent twice, he can immediately tell that a bit got corrupted on its way. He cannot tell which bit you meant to send him – but at least he knows that he cannot trust the ones he got.[212] Of course, there is a probability that he got the wrong bit twice, in which case he is clueless about it being wrong; but this probability is p^2, which is a lot smaller than p. This is called *error detection*.

- An even better scheme is to send each bit **thrice** in a row. This way, your recipient can not only tell if some bit was corrupted (with an even smaller probability of falsely believing that everything went right – namely, p^3); he can also try to guess which bit is the right one, by the "majority rule" (i.e., among the 3 bits he obtained, he chooses the one that appears more often). This is called *error correction*.

- But sending each bit multiple times is not the only thing you can do; you can also mix several bits together. For example, you can follow every four bits a, b, c, d that you are sending with the three bits

$$a+b+d, \qquad a+c+d, \qquad b+c+d,$$

[210] "Corrupted" means that the recepient will receive a 0 instead of 1, or a 1 instead of a 0. For simplicity, we assume that bits will not be lost, and the order in which they are received is the order in which they are sent (so, e.g., messenger pigeons are not the kind of channel we are considering).

[211] Another, mostly equivalent, version of this problem is long-term storage of data on a medium (e.g., a hard drive, a DVD, paper or a scroll) that gradually decays. Here, the sender is you when you are storing the data; the recepient is you (or whoever wants to read it) in the future. That's a noisy channel!

[212] If he can talk back to you, this means he can ask you to resend the correct one.

where you are regarding bits as elements of $\mathbb{Z}/2$ (so that, for example, $1 + 1 + 1 = 1$). Thus, you are sending 7 bits instead of 4 bits, but the transmission has become a lot safer, because:

- If at most 2 of the 7 bits get corrupted along the way, the recepient will be able to tell that something went wrong. (In the language of coding theory, this is saying that your code *detects up to* 2 *errors*.)
- If at most 1 of the 7 bits gets corrupted along the way, the recepient will be able to guess the bits you intended to send[213]. (In the language of coding theory, this is saying that your code *corrects up to* 1 *error*.)

This scheme is called the Hamming$(7,4)$ code, and was invented by Richard W. Hamming in 1950 as a tool to make error-prone punch card readers less likely to fail.

- Here is yet another error-correcting code, which makes use of finite fields. Fix two integers $d, e \in \mathbb{N}$ such that $d < e$, as well as a finite field $\mathbb{K}$ and e distinct elements $a_1, a_2, \ldots, a_e$ of $\mathbb{K}$. (You have to agree on these in advance with your recepient. Of course, the field must satisfy $|\mathbb{K}| \geq e$.) Now, instead of transmitting bits, you transmit elements of $\mathbb{K}$. (This does not require a different kind of channel; you can always, under the hood, re-encode your elements of $\mathbb{K}$ into bitstrings and send those as bits via the channel that you have.[214]) Now, when you want to send $d+1$ elements $u_0, u_1, \ldots, u_d$ of $\mathbb{K}$ over the channel, you instead form the polynomial

$$\mathbf{f} = u_0 + u_1 x + \cdots + u_d x^d \in \mathbb{K}[x]_{\leq d},$$

and transmit the e values $\mathbf{f}[a_1], \mathbf{f}[a_2], \ldots, \mathbf{f}[a_e]$ of this polynomial. The recepient will then receive e values of the polynomial $\mathbf{f}$. If all of these values have been transmitted correctly, then he will be able to pick any $d+1$ of these values[215] and use them to reconstruct $\mathbf{f}$ (and therefore, your messages $u_0, u_1, \ldots, u_d$) via Theorem 7.7.5. If at most $e - d - 1$ of these e values get corrupted along the way, he will be able to recognize that something is wrong[216]. Thus, this code detects up to $e - d - 1$ errors. It furthermore corrects up to $\left\lfloor \dfrac{e-d-1}{2} \right\rfloor$ errors (i.e., there is a way in which the recepient can guess your original messages, and if no more than $\left\lfloor \dfrac{e-d-1}{2} \right\rfloor$ of your e values have gotten corrupted, then his guess will be right).

[213] without having to ask you to re-send them

[214] Of course, an element of $\mathbb{K}$ is more likely to get corrupted along the way than a single bit (if $|\mathbb{K}| > 2$), because it will be encoded as several bits (and each of them can get corrupted). But this is par for the course: After all, an element of $\mathbb{K}$ carries more information than a bit, too.

[215] He can do this, since $e \geq d+1$.

[216] e.g., by attempting to recover $\mathbf{f}$ using some $d+1$ of the values, and then checking whether the resulting polynomial also fits the remaining $e - d - 1$ values

This is called a *Reed–Solomon code*; such codes were used by the Voyager spacecraft and later in the storage of data on CDs and DVDs (as said above, storing data on a decaying medium is transmitting it through a noisy channel).

See [Childs00, Chapter 29] for more about these codes, and see textbooks on coding theory (e.g., [Garret07]) for much more.[217]

7.8. Generating functions

7.8.1. A binomial identity

Let me show a further application of the "polynomial identity trick", which is interesting in that it uses polynomials in two different ways.

Among many properties of Pascal's triangle, one rather famous one is that the sum of all entries in the n-th row is 2^n. That is,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \qquad \text{for each } n \in \mathbb{N}.$$

This is, in fact, the direct result of applying Theorem 2.17.13 to $x = 1$ and $y = 1$. Likewise, we can apply Theorem 2.17.13 to $x = -1$ and $y = 1$, and conclude that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0^n = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases} \qquad \text{for each } n \in \mathbb{N}.$$

In other words, the alternating sum of all entries in the n-th row of Pascal's triangle is 0, unless $n = 0$ (in which case it is 1).

One may wonder what happens if we start summing higher powers of the entries of a row of Pascal's triangle. For example, the sum of their squares has a nice formula:

Proposition 7.8.1. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

Proof of Proposition 7.8.1. We have

$$\sum_{k=0}^{n} \underbrace{\binom{n}{k}^2}_{=\binom{n}{k}\binom{n}{k}} = \sum_{k=0}^{n} \binom{n}{k} \underbrace{\binom{n}{k}}_{\substack{=\binom{n}{n-k} \\ \text{(by Theorem 2.17.6)}}} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}.$$

[217] Be aware that there are several different ways of defining Reed–Solomon codes; the one in [Garret07] is not the same as ours.

Comparing this with

$$\binom{2n}{n} = \binom{n+n}{n} = \sum_{k=0}^{n} \binom{n}{k} \binom{n}{n-k} \qquad \left(\begin{array}{c} \text{by Theorem 2.17.14,} \\ \text{applied to } x = n \text{ and } y = n \end{array} \right),$$

we obtain $\sum\limits_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$. This proves Proposition 7.8.1. □

Now, what about the alternating sum of the squares of the elements of the n-th row of Pascal's triangle? Here, the formula turns out to be just as neat, apart from having two cases to distinguish:

Proposition 7.8.2. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}^2 = \begin{cases} (-1)^{n/2} \dbinom{n}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

Just as we derived Proposition 7.8.1 from Theorem 2.17.14, we are going to derive Proposition 7.8.2 from the following fact:

Theorem 7.8.3. Let $u \in \mathbb{Q}$ and $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} (-1)^k \binom{u}{k} \binom{u}{n-k} = \begin{cases} (-1)^{n/2} \dbinom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

Theorem 7.8.3 can be proven in an elementary, computational way (see [Grinbe15, Second solution to Exercise 3.22] for this proof). Let us, however, prove it by applying polynomials strategically (this argument is [Grinbe15, First solution to Exercise 3.22], and is folklore). First, we prove the particular case of Theorem 7.8.3 for $u \in \mathbb{N}$:

Lemma 7.8.4. Let $u \in \mathbb{N}$ and $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} (-1)^k \binom{u}{k} \binom{u}{n-k} = \begin{cases} (-1)^{n/2} \dbinom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

Proof of Lemma 7.8.4. Let $\mathbb{K}$ be the polynomial ring $\mathbb{Q}[x]$. We have

$$(1-x)^u (1+x)^u = \Bigg(\underbrace{(1-x)(1+x)}_{=1-x^2=1+(-x^2)}\Bigg)^u = \left(1+\left(-x^2\right)\right)^u = \sum_{k\in\mathbb{N}} \binom{u}{k} \underbrace{\left(-x^2\right)^k}_{=(-1)^k x^{2k}}$$

$$\left(\text{by Lemma 7.3.4, applied to } a = -x^2\right)$$

$$= \sum_{k\in\mathbb{N}} (-1)^k \binom{u}{k} x^{2k}.$$

Hence,

$$[x^n]\left((1-x)^u (1+x)^u\right) = [x^n]\left(\sum_{k\in\mathbb{N}} (-1)^k \binom{u}{k} x^{2k}\right) = \begin{cases} (-1)^{n/2} \dbinom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}. \tag{295}$$

Let us now compute the left hand side in a different way, using (218). Namely,

$$\Bigg(\underbrace{1-x}_{=1+(-x)}\Bigg)^u = (1+(-x))^u = \sum_{k\in\mathbb{N}} \binom{u}{k} \underbrace{(-x)^k}_{=(-1)^k x^k}$$

$$(\text{by Lemma 7.3.4, applied to } a = -x)$$

$$= \sum_{k\in\mathbb{N}} (-1)^k \binom{u}{k} x^k.$$

Hence, each $i \in \mathbb{N}$ satisfies

$$\left[x^i\right]\left((1-x)^u\right) = \left[x^i\right]\left(\sum_{k\in\mathbb{N}} (-1)^k \binom{u}{k} x^k\right) = (-1)^i \binom{u}{i}. \tag{296}$$

A similar argument (without the "-1") shows that each $i \in \mathbb{N}$ satisfies

$$\left[x^i\right]\left((1+x)^u\right) = \binom{u}{i}. \tag{297}$$

Now, (218) (applied to $\mathbf{a} = (1-x)^u$ and $\mathbf{b} = (1+x)^u$) yields

$$\begin{aligned} \left[x^n\right]\left((1-x)^u(1+x)^u\right) &= \sum_{i=0}^{n} \underbrace{\left(\left[x^i\right]\left((1-x)^u\right)\right)}_{\substack{=(-1)^i\binom{u}{i} \\ \text{(by (296))}}} \cdot \underbrace{\left(\left[x^{n-i}\right]\left((1+x)^u\right)\right)}_{\substack{=\binom{u}{n-i} \\ \text{(by (297), applied to } n-i \\ \text{instead of } i)}} \\ &= \sum_{i=0}^{n}(-1)^i\binom{u}{i}\binom{u}{n-i} = \sum_{k=0}^{n}(-1)^k\binom{u}{k}\binom{u}{n-k} \end{aligned}$$

(here, we have renamed the summation index i as k). Comparing this with (295), we obtain

$$\sum_{k=0}^{n}(-1)^k\binom{u}{k}\binom{u}{n-k} = \begin{cases} (-1)^{n/2}\dbinom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

This proves Lemma 7.8.4. □

Our proof of Lemma 7.8.4 is an example of the use of "generating functions": We have proven that two sequences $(a_0, a_1, a_2, \ldots)$ and $(b_0, b_1, b_2, \ldots)$ of numbers were equal[218] by showing that the two FPSs $\sum\limits_{k\in\mathbb{N}} a_k x^k$ and $\sum\limits_{k\in\mathbb{N}} b_k x^k$ are equal. (In our case, these two FPSs were actually the polynomials $\left(1-x^2\right)^u$ and $(1-x)^u(1+x)^u$. But they don't have to be polynomials in order for the technique of generating functions to be applicable.) This technique is central to enumerative combinatorics, and also has many uses in pure algebra. See [Loehr11, Chapters 7 and 8] and [Wilf94] for (a lot) more about this technique.

We still need to prove Theorem 7.8.3, which generalizes Lemma 7.8.4 from $u \in \mathbb{N}$ to $u \in \mathbb{Q}$. Here, polynomials come useful once again (in the same way as they came useful when we were generalizing Lemma 2.17.15 to Lemma 2.17.17):

Proof of Theorem 7.8.3. Forget that we fixed u. Define the two polynomials

$$\mathbf{a} = \sum_{k=0}^{n}(-1)^k\binom{x}{k}\binom{x}{n-k} \qquad \text{and}$$

$$\mathbf{b} = \begin{cases} (-1)^{n/2}\dbinom{x}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}$$

[218] In our case, the two sequences are given by $a_n = \sum\limits_{k=0}^{n}(-1)^k\binom{u}{k}\binom{u}{n-k}$ and $b_n = \begin{cases} (-1)^{n/2}\dbinom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}$ for all $n \in \mathbb{N}$.

in 1 variable over the field $\mathbb{Q}$. For each $u \in \mathbb{Q}$, we have

$$\mathbf{a}[u] = \sum_{k=0}^{n} (-1)^k \binom{u}{k} \binom{u}{n-k} \qquad \text{and} \tag{298}$$

$$\mathbf{b}[u] = \begin{cases} (-1)^{n/2} \dbinom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases} \tag{299}$$

(since the evaluation map ev_u is a $\mathbb{Q}$-algebra homomorphism and satisfies Corollary 7.6.16 **(b)**). Thus, for each $u \in \mathbb{N}$, we have

$$\begin{aligned} \mathbf{a}[u] &= \sum_{k=0}^{n} (-1)^k \binom{u}{k} \binom{u}{n-k} \qquad (\text{by (298)}) \\ &= \begin{cases} (-1)^{n/2} \dbinom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases} \qquad (\text{by Lemma 7.8.4}) \\ &= \mathbf{b}[u] \qquad (\text{by (299)}). \end{aligned}$$

Hence, infinitely many elements $u \in \mathbb{Q}$ satisfy $\mathbf{a}[u] = \mathbf{b}[u]$ (since infinitely many elements $u \in \mathbb{Q}$ satisfy $u \in \mathbb{N}$). Thus, Corollary 7.7.3 (applied to $\mathbb{K} = \mathbb{Q}$) yields $\mathbf{a} = \mathbf{b}$. Thus, each $u \in \mathbb{Q}$ satisfies

$$\begin{aligned} \sum_{k=0}^{n} (-1)^k \binom{u}{k} \binom{u}{n-k} &= \underbrace{\mathbf{a}}_{=\mathbf{b}}[u] \qquad (\text{by (298)}) \\ &= \mathbf{b}[u] = \begin{cases} (-1)^{n/2} \dbinom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases} \qquad (\text{by (299)}). \end{aligned}$$

This proves Theorem 7.8.3. □

Proof of Proposition 7.8.2. We have

$$\begin{aligned} \sum_{k=0}^{n} (-1)^k \underbrace{\binom{n}{k}^2}_{=\binom{n}{k}\binom{n}{k}} &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} \underbrace{\binom{n}{k}}_{\substack{=\binom{n}{n-k} \\ (\text{by Theorem 2.17.6})}} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{n}{n-k} \\ &= \begin{cases} (-1)^{n/2} \dbinom{n}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases} \end{aligned}$$

(by Theorem 7.8.3, or just Lemma 7.8.4, applied to $u = n$). This proves Proposition 7.8.2. □

Remark 7.8.5. We now know

- the sum of all entries of the n-th row of Pascal's triangle (it is 2^n);
- the alternating sum of all entries of the n-th row of Pascal's triangle (it is 0 if $n \neq 0$, and 1 otherwise);
- the sum of the squares of all entries of the n-th row of Pascal's triangle (it is $\dbinom{2n}{n}$);
- the alternating sum of the squares of all entries of the n-th row of Pascal's triangle (see Proposition 7.8.2).

How does this pattern continue? We may ask for the sum $\sum\limits_{k=0}^{n} \dbinom{n}{k}^3$ of all cubes of all entries of the n-th row of Pascal's triangle, as well as their alternating sum.

The numbers $\sum\limits_{k=0}^{n} \dbinom{n}{k}^3$ are known as the *Franel numbers* (OEIS sequence A000172); no explicit (sum-less) formula for them is known (unlike for the sums of squares).

As for the alternating sum, however, there is a nice formula:

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}^3 = \begin{cases} (-1)^{n/2} \dfrac{(3n/2)!}{(n/2)!^3}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases} \qquad \text{for all } n \in \mathbb{N}.$$

In the case when n is odd, this formula is easy to check (indeed, in the sum $\sum\limits_{k=0}^{n} (-1)^k \dbinom{n}{k}^3$, the addend for $k = u$ cancels the addend for $k = n - u$). In the case when n is even, it is a particular case of what is known as *Dixon's identity* (see, e.g., [Ward91]). The sequence of these alternating sums is OEIS sequence A245086.

Higher powers are even more complicated. For example, as far as fourth powers are concerned, neither $\sum\limits_{k=0}^{n} \dbinom{n}{k}^4$ nor $\sum\limits_{k=0}^{n} (-1)^k \dbinom{n}{k}^4$ has a known explicit form (see OEIS sequences A005260 and A228304).

7.8.2. Proving Lucas's congruence

Recall Lucas's congruence (Theorem 2.17.20), which we have left unproven back when we were studying binomial coefficients. Let us now outline how it can be proven using polynomials and FPSs. We first shall prove a particular case:

Lemma 7.8.6. Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Then, we have the four congruences

$$\binom{2a}{2b} \equiv \binom{a}{b} \bmod 2; \qquad \binom{2a}{2b+1} \equiv 0 \bmod 2;$$
$$\binom{2a+1}{2b} \equiv \binom{a}{b} \bmod 2; \qquad \binom{2a+1}{2b+1} \equiv \binom{a}{b} \bmod 2.$$

Lemma 7.8.6 is a very particular case of Theorem 2.17.20 – namely, the one when $p = 2$ and $a \in \mathbb{N}$ and $b \in \mathbb{N}$. (The four congruences correspond to the four different options for the pair $(c, d) \in \{0, 1, \ldots, p-1\}^2$.) Nevertheless, it is already the reason for a curious pattern: If you plot the first 2^n rows of Pascal's triangle (for some $n \in \mathbb{N}$), and color all odd entries black and all even entries white, then you obtain an (approximation to) Sierpinski's triangle (the fractal). Lemma 7.8.6 can be used to prove this (by induction on n).

Proof of Lemma 7.8.6 (sketched). Work in the polynomial ring $(\mathbb{Z}/2)[x]$ over $\mathbb{Z}/2$. In this ring, we have

$$(1+x)^2 = 1 + \underbrace{2x}_{\substack{=0 \\ \text{(since } 2=0 \text{ in } \mathbb{Z}/2)}} + x^2 = 1 + x^2.$$

Lemma 7.3.4 (applied to $(\mathbb{Z}/2)[x]$, a and x^2 instead of $\mathbb{K}$, u and a) yields

$$\begin{aligned}
\left(1+x^2\right)^a &= \sum_{k\in\mathbb{N}} \binom{a}{k} \underbrace{\left(x^2\right)^k}_{=x^{2k}} \qquad (300)\\
&= \sum_{k\in\mathbb{N}} \binom{a}{k} x^{2k} = \binom{a}{0}x^0 + \binom{a}{1}x^2 + \binom{a}{2}x^4 + \binom{a}{3}x^6 + \cdots .
\end{aligned}$$

Now,

$$\begin{aligned}
(1+x)^{2a+1} &= \underbrace{(1+x)^{2a}}_{=\left((1+x)^2\right)^a} (1+x) = \left(\underbrace{(1+x)^2}_{=1+x^2}\right)^a (1+x)\\
&= \underbrace{\left(1+x^2\right)^a}_{=\binom{a}{0}x^0+\binom{a}{1}x^2+\binom{a}{2}x^4+\binom{a}{3}x^6+\cdots\cdots} (1+x)\\
&= \left(\binom{a}{0}x^0 + \binom{a}{1}x^2 + \binom{a}{2}x^4 + \binom{a}{3}x^6 + \cdots\right)(1+x)\\
&= \left(\binom{a}{0}x^0 + \binom{a}{1}x^2 + \binom{a}{2}x^4 + \binom{a}{3}x^6 + \cdots\right)\\
&\qquad + \left(\binom{a}{0}x^0 + \binom{a}{1}x^2 + \binom{a}{2}x^4 + \binom{a}{3}x^6 + \cdots\right)x\\
&= \binom{a}{0}x^0 + \binom{a}{0}x^1 + \binom{a}{1}x^2 + \binom{a}{1}x^3 + \binom{a}{2}x^4 + \binom{a}{2}x^5 + \cdots\\
&= \sum_{k\in\mathbb{N}} \binom{a}{k//2} x^k \qquad (301)
\end{aligned}$$

(where we are using Definition 2.6.2).

Comparing this to

$$(1+x)^{2a+1} = \sum_{k\in\mathbb{N}} \binom{2a+1}{k} x^k \qquad (302)$$

$$\left(\begin{array}{c}\text{by Lemma 7.3.4, applied to } (\mathbb{Z}/2)[x], 2a+1 \text{ and } x\\ \text{instead of } \mathbb{K}, u \text{ and } a\end{array}\right),$$

we obtain

$$\sum_{k\in\mathbb{N}} \binom{2a+1}{k} x^k = \sum_{k\in\mathbb{N}} \binom{a}{k//2} x^k. \qquad (303)$$

This is an equality of FPSs (actually, polynomials). But recall that FPSs are just sequences of elements of $\mathbb{K}$ (where in our case, $\mathbb{K} = \mathbb{Z}/2$). Hence, if two FPSs are equal, then the coefficients in x^n in these two FPSs are equal (whenever $n \in \mathbb{N}$). Hence, from (303), we conclude that

$$[x^n]\left(\sum_{k\in\mathbb{N}} \binom{2a+1}{k} x^k\right) = [x^n]\left(\sum_{k\in\mathbb{N}} \binom{a}{k//2} x^k\right)$$

for each $n \in \mathbb{N}$. In view of

$$[x^n]\left(\sum_{k\in\mathbb{N}} \binom{2a+1}{k} x^k\right) = \binom{2a+1}{n} \qquad (304)$$

(by the definition of $[x^n]\,\mathbf{a}$ for an FPS $\mathbf{a}$) and

$$[x^n]\left(\sum_{k\in\mathbb{N}} \binom{a}{k//2} x^k\right) = \binom{a}{n//2}, \qquad (305)$$

this rewrites as

$$\binom{2a+1}{n} = \binom{a}{n//2}. \qquad (306)$$

Thus, we have proven (306) for each $n \in \mathbb{N}$. Applying (306) to $n = 2b$, we obtain

$$\binom{2a+1}{2b} = \binom{a}{(2b)//2} = \binom{a}{b} \qquad \left(\text{since } (2b)//2 = b\right).$$

This proves the third of the four congruences that are claimed in Lemma 7.8.6... except that something is amiss: Why did we get an equality rather than a congruence? As an equality between two integers, $\binom{2a+1}{2b} = \binom{a}{b}$ is clearly wrong (e.g., if $a = 1$ and $b = 1$, then it claims that $3 = 1$). What did we do wrong?

The culprit is our abuse of notation which lets us use the same symbol for an integer w and the corresponding element $w \cdot 1_{\mathbb{Z}/2} = [w]_2$ of $\mathbb{Z}/2$. For example, the coefficients of the FPS $\sum\limits_{k\in\mathbb{N}} \dbinom{2a+1}{k} x^k$ on the left hand side of (305) are not the **integers** $\dbinom{2a+1}{k}$, but rather the corresponding elements $\dbinom{2a+1}{k} \cdot 1_{\mathbb{Z}/2}$ of $\mathbb{Z}/2$ (since $\lambda x^k = (\lambda \cdot 1_{\mathbb{Z}/2}) \cdot x^k$ for each $\lambda \in \mathbb{Z}$). Thus, the "$\dbinom{2a+1}{n}$" on the right hand side of (305) should be understood not as the **integer** $\dbinom{2a+1}{n}$, but rather as the corresponding element $\dbinom{2a+1}{n} \cdot 1_{\mathbb{Z}/2}$ of $\mathbb{Z}/2$. Hence, the equality (306) that we obtained is not actually an equality between integers (despite looking like one), but rather an equality between the corresponding elements of $\mathbb{Z}/2$, namely

$$\binom{2a+1}{n} \cdot 1_{\mathbb{Z}/2} = \binom{a}{n//2} \cdot 1_{\mathbb{Z}/2}. \tag{307}$$

Such an equality can be translated into a congruence modulo 2 between the integers: Indeed, if u and v are two integers satisfying $u \cdot 1_{\mathbb{Z}/2} = v \cdot 1_{\mathbb{Z}/2}$, then $[u]_2 = u \cdot 1_{\mathbb{Z}/2} = v \cdot 1_{\mathbb{Z}/2} = [v]_2$ and thus $u \equiv v \bmod 2$. Hence, (307) yields

$$\binom{2a+1}{n} \equiv \binom{a}{n//2} \bmod 2.$$

By applying this to $n = 2b$, we obtain the third of the four congruences that are claimed in Lemma 7.8.6. Likewise, we can apply it to $n = 2b+1$, and thus obtain the fourth of these four congruences.

In order to prove the first two of these four congruences, we have to consider $(1+x)^{2a}$ instead of $(1+x)^{2a+1}$. Thus, the computation (301) is replaced by

$$\begin{aligned}
(1+x)^{2a} &= \left(\underbrace{(1+x)^2}_{=1+x^2}\right)^a = \left(1+x^2\right)^a \\
&= \binom{a}{0}x^0 + \binom{a}{1}x^2 + \binom{a}{2}x^4 + \binom{a}{3}x^6 + \cdots \\
&= \binom{a}{0}x^0 + 0x^1 + \binom{a}{1}x^2 + 0x^3 + \binom{a}{2}x^4 + 0x^5 + \cdots \\
&= \sum_{k\in\mathbb{N}} \begin{cases} \dbinom{a}{k//2}, & \text{if } k \text{ is even;} \\ 0, & \text{if } k \text{ is odd} \end{cases} x^k.
\end{aligned}$$

The rest of the argument is similar to the argument we used above to prove the third and fourth congruences; we leave this to the reader. Thus, Lemma 7.8.6 is proven. □

Now, how can we extend this proof to a full proof of Theorem 2.17.20? As we know, Lemma 7.8.6 is the particular case of Theorem 2.17.20 for $p = 2$ and $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Thus, we need to lift the three restrictions $p = 2$, $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Here is a rough plan:

- To lift the restriction $b \in \mathbb{N}$, we simply observe that Theorem 2.17.20 is trivial in the case when $b \in \mathbb{Z}$ is negative. Indeed, if $b \in \mathbb{Z}$ is negative, then both $pb + d$ and b are negative (since $d \in \{0, 1, \ldots, p-1\}$ yields $d < p$, but $b < 0$ yields $pb \leq -p$), and therefore Theorem 2.17.20 boils down to the obvious congruence $0 \equiv 0 \dbinom{c}{d} \mod p$.

- To lift the restriction $a \in \mathbb{N}$, we have to tweak our above proof so that it works for negative a as well. Of course, the first step is to use FPSs instead of polynomials. There are only two places in our proof where we have used the nonnegativity of a – namely, the two places where we applied Lemma 7.3.4. The first place was (300); the second was (302). So we have to prove (300) and (302) without using the requirement that $a \in \mathbb{N}$. But this is easy using Newton's binomial theorem. In fact, (302) follows directly from Theorem 7.3.3 **(b)** (applied to $u = 2a + 1$), whereas (300) follows by first applying Theorem 7.3.3 **(b)** to $u = a$ and then substituting x^2 for x. (As we explained in Remark 7.6.6, not every element of a $\mathbb{K}$-algebra can be substituted into an FPS; but x^2 can always be substituted into an FPS, and the usual properties of substitution – such as it being a $\mathbb{K}$-algebra homomorphism – are satisfied.)

- Finally, how can we lift the restriction that p be a prime? Recall that we used the identity $(1 + x)^2 = 1 + x^2$ (in $(\mathbb{Z}/2)[x]$) in our above proof. This has to be replaced by the identity

  $$(1 + x)^p = 1 + x^p \qquad \text{in } (\mathbb{Z}/p)[x].$$

  This identity is a consequence of Theorem 5.11.1 (applied to $\mathbb{K} = (\mathbb{Z}/p)[x]$, $a = 1$ and $b = x$), since $p \cdot 1_{(\mathbb{Z}/p)[x]} = 0$.

Thus, we obtain the following proof of Theorem 2.17.20 in full generality:

Proof of Theorem 2.17.20 (sketched). If $b < 0$, then both $pb + d$ and b are negative[219], and therefore both $\dbinom{pa+c}{pb+d}$ and $\dbinom{a}{b}$ equal 0. Thus, if $b < 0$, then the claim of Theorem 2.17.20 rewrites as $0 \equiv 0 \dbinom{c}{d} \mod p$, which is obvious. Hence, for the rest of this proof, we WLOG assume that we don't have $b < 0$. Thus, $b \geq 0$, so that $b \in \mathbb{N}$ and therefore $pb + d \in \mathbb{N}$.

[219] The proof of this is left to the reader. (**Hint:** From $b < 0$, we obtain $b \leq -1$ and thus $pb \leq -p$; but from $d \in \{0, 1, \ldots, p-1\}$, we obtain $d \leq p - 1 < p$.)

Let us work in the ring $(\mathbb{Z}/p)[[x]]$. In this ring, we have

$$p \cdot \underbrace{1_{(\mathbb{Z}/p)[[x]]}}_{=1_{\mathbb{Z}/p}\cdot 1_{(\mathbb{Z}/p)[[x]]}} = \underbrace{p \cdot 1_{\mathbb{Z}/p}}_{=[p]_p=[0]_p=0} \cdot 1_{(\mathbb{Z}/p)[[x]]} = 0 \cdot 1_{(\mathbb{Z}/p)[[x]]} = 0.$$

Thus, Theorem 5.11.1 (applied to $\mathbb{K} = (\mathbb{Z}/p)[[x]]$, $a = 1$ and $b = x$) yields

$$(1+x)^p = \underbrace{1^p}_{=1} + x^p = 1 + x^p \qquad \text{in } (\mathbb{Z}/p)[[x]]. \tag{308}$$

Theorem 7.3.3 **(b)** (applied to $\mathbb{K} = \mathbb{Z}/p$ and $u = a$) yields

$$(1+x)^a = \sum_{k\in\mathbb{N}} \binom{a}{k} x^k.$$

We can substitute x^p for x in this equality[220], and thus obtain

$$\begin{aligned}(1+x^p)^a &= \sum_{k\in\mathbb{N}} \binom{a}{k} \underbrace{(x^p)^k}_{=x^{pk}=x^{kp}} = \sum_{k\in\mathbb{N}} \binom{a}{k} x^{kp} \\ &= \sum_{q\in\mathbb{N}} \binom{a}{q} x^{qp} \end{aligned} \tag{309}$$

(here, we have renamed the summation index k as q).

On the other hand, $c \in \{0, 1, \ldots, p-1\}$ and thus $c \leq p - 1 < p$. Hence, for each $k \in \{p, p+1, p+2, \ldots\}$, we have $k \geq p > c$ and thus

$$\binom{c}{k} = 0 \tag{310}$$

(by Theorem 2.17.4, applied to $n = c$). Now, Theorem 7.3.3 **(b)** (applied to $\mathbb{K} = \mathbb{Z}/p$

[220] Rigorously speaking, this means that we apply the map

$$\begin{aligned}\mathbb{K}[[x]] &\to \mathbb{K}[[x]], \\ \mathbf{a} &\mapsto \mathbf{a}[x^p]\end{aligned}$$

to both sides of this equality. This map is well-defined because of Remark 7.6.6 (since p is a positive integer), and it is not hard to see that this map is a $\mathbb{K}$-algebra homomorphism (this is proven just as Corollary 7.6.4 was proven, except that we are now working with FPSs instead of polynomials) that furthermore respects not just finite sums but also infinite sums (of summable families). Thus, applying this map to $(1+x)^a$ yields $(1+x^p)^a$ (because it is a ring homomorphism), and applying it to $\sum_{k\in\mathbb{N}} \binom{a}{k} x^k$ yields $\sum_{k\in\mathbb{N}} \binom{a}{k} (x^p)^k$ (because it respects infinite sums of summable families).

and $u = c$) yields

$$(1+x)^c = \sum_{k\in\mathbb{N}} \binom{c}{k} x^k = \sum_{k=0}^{p-1} \binom{c}{k} x^k + \sum_{k=p}^{\infty} \underbrace{\binom{c}{k}}_{\substack{=0 \\ \text{(by (310))}}} x^k = \sum_{k=0}^{p-1} \binom{c}{k} x^k + \underbrace{\sum_{k=p}^{\infty} 0x^k}_{=0}$$
$$= \sum_{k=0}^{p-1} \binom{c}{k} x^k = \sum_{r=0}^{p-1} \binom{c}{r} x^r \tag{311}$$

(here, we have renamed the summation index k as r).

Now,

$$(1+x)^{pa+c} = \underbrace{(1+x)^{pa}}_{=\left((1+x)^p\right)^a} (1+x)^c = \left(\underbrace{(1+x)^p}_{\substack{=1+x^p \\ \text{(by (308))}}} \right)^a (1+x)^c = \underbrace{(1+x^p)^a}_{\substack{=\sum_{q\in\mathbb{N}} \binom{a}{q} x^{qp} \\ \text{(by (309))}}} \underbrace{(1+x)^c}_{\substack{=\sum_{r=0}^{p-1} \binom{c}{r} x^r \\ \text{(by (311))}}}$$
$$= \left(\sum_{q\in\mathbb{N}} \binom{a}{q} x^{qp} \right) \left(\sum_{r=0}^{p-1} \binom{c}{r} x^r \right) = \sum_{q\in\mathbb{N}} \sum_{r=0}^{p-1} \binom{a}{q} \binom{c}{r} x^{qp} x^r .$$

Comparing this with

$$\sum_{k\in\mathbb{N}} \binom{a}{k//p} \binom{c}{k\%p} x^k$$
$$= \underbrace{\sum_{(q,r)\in\mathbb{N}\times\{0,1,\ldots,p-1\}}}_{=\sum_{q\in\mathbb{N}} \sum_{r\in\{0,1,\ldots,p-1\}}} \binom{a}{(qp+r)//p} \binom{c}{(qp+r)\%p} \underbrace{x^{qp+r}}_{=x^{qp}x^r}$$
$$\left(\begin{array}{c} \text{here, we have substituted } qp+r \text{ for } k \text{ in the sum, since} \\ \text{the map } \mathbb{N}\times\{0,1,\ldots,p-1\} \to \mathbb{N},\ (q,r) \mapsto qp+r \text{ is a} \\ \text{bijection (by Exercise 2.6.4 \textbf{(b)}, applied to } n=p) \end{array} \right)$$
$$= \sum_{q\in\mathbb{N}} \underbrace{\sum_{r\in\{0,1,\ldots,p-1\}}}_{=\sum_{r=0}^{p-1}} \underbrace{\binom{a}{(qp+r)//p}}_{\substack{=\binom{a}{q} \\ \text{(since Exercise 2.6.4 \textbf{(c)}} \\ \text{(applied to } n=p) \\ \text{yields } (qp+r)//p=q)}} \underbrace{\binom{c}{(qp+r)\%p}}_{\substack{=\binom{c}{r} \\ \text{(since Exercise 2.6.4 \textbf{(d)}} \\ \text{(applied to } n=p) \\ \text{yields } (qp+r)\%p=r)}} x^{qp} x^r$$
$$= \sum_{q\in\mathbb{N}} \sum_{r=0}^{p-1} \binom{a}{q} \binom{c}{r} x^{qp} x^r ,$$

we obtain

$$(1+x)^{pa+c} = \sum_{k\in\mathbb{N}} \binom{a}{k//p}\binom{c}{k\%p} x^k. \tag{312}$$

But Theorem 7.3.3 **(b)** (applied to $\mathbb{K} = \mathbb{Z}/p$ and $u = pa+c$) yields

$$(1+x)^{pa+c} = \sum_{k\in\mathbb{N}} \binom{pa+c}{k} x^k.$$

Comparing this with (312), we find

$$\sum_{k\in\mathbb{N}} \binom{pa+c}{k} x^k = \sum_{k\in\mathbb{N}} \binom{a}{k//p}\binom{c}{k\%p} x^k.$$

Thus, for each $n \in \mathbb{N}$, we have

$$\begin{aligned} \left[x^n\right]\left(\sum_{k\in\mathbb{N}} \binom{pa+c}{k} x^k\right) &= \left[x^n\right]\left(\sum_{k\in\mathbb{N}} \binom{a}{k//p}\binom{c}{k\%p} x^k\right) \\ &= \binom{a}{n//p}\binom{c}{n\%p} \cdot 1_{\mathbb{Z}/p} \end{aligned} \tag{313}$$

(by the definition of $[x^n]\,\mathbf{a}$ for an FPS $\mathbf{a}$). Here, the "$1_{\mathbb{Z}/p}$" factor on the right hand side stems from the fact that our FPSs are over $\mathbb{Z}/p$, so their coefficients are not the integers they seem to be but rather the corresponding elements of $\mathbb{Z}/p$. On the other hand, for each $n \in \mathbb{N}$, we have

$$\left[x^n\right]\left(\sum_{k\in\mathbb{N}} \binom{pa+c}{k} x^k\right) = \binom{pa+c}{n} \cdot 1_{\mathbb{Z}/p} \tag{314}$$

(by the definition of $[x^n]\,\mathbf{a}$ for an FPS $\mathbf{a}$). Comparing this with (313), we conclude that

$$\binom{a}{n//p}\binom{c}{n\%p} \cdot 1_{\mathbb{Z}/p} = \binom{pa+c}{n} \cdot 1_{\mathbb{Z}/p}$$

for each $n \in \mathbb{N}$. In other words,

$$\binom{a}{n//p}\binom{c}{n\%p} \equiv \binom{pa+c}{n} \operatorname{mod} p \tag{315}$$

for each $n \in \mathbb{N}$ (because if u and v are two integers satisfying $u \cdot 1_{\mathbb{Z}/p} = v \cdot 1_{\mathbb{Z}/p}$, then $[u]_p = u \cdot 1_{\mathbb{Z}/p} = v \cdot 1_{\mathbb{Z}/p} = [v]_p$ and thus $u \equiv v \operatorname{mod} p$).

We can apply this to $n = pb + d$. Thus, we obtain

$$\binom{a}{(pb+d)//p}\binom{c}{(pb+d)\%p} \equiv \binom{pa+c}{pb+d} \operatorname{mod} p.$$

Hence,

$$\begin{aligned}
\binom{pa+c}{pb+d} &\equiv \underbrace{\binom{a}{(pb+d)\,//\,p}}_{\substack{=\binom{a}{(bp+d)\,//\,p}=\binom{a}{b} \\ \text{(since Exercise 2.6.4 }\textbf{(c)} \\ \text{(applied to } n=p,\ q=b \text{ and } r=d\text{)} \\ \text{yields } (bp+d)//p=b\text{)}}} \quad \underbrace{\binom{c}{(pb+d)\,\%p}}_{\substack{=\binom{c}{(bp+d)\,\%p}=\binom{c}{d} \\ \text{(since Exercise 2.6.4 }\textbf{(d)} \\ \text{(applied to } n=p,\ q=b \text{ and } r=d\text{)} \\ \text{yields } (bp+d)\%p=d\text{)}}} \\
&= \binom{a}{b}\binom{c}{d} \bmod p.
\end{aligned}$$

This proves Theorem 2.17.20. □

7.9. Invertible and nilpotent polynomials

In Subsection 7.3.1, we have seen when an FPS $\mathbf{a} \in \mathbb{K}[[x]]$ is invertible in the ring $\mathbb{K}[[x]]$. When is a polynomial $\mathbf{a} \in \mathbb{K}[x]$ invertible in the ring $\mathbb{K}[x]$?

The first hint that the answer is different comes from the example of $1+x$. As we know, the FPS $1+x$ is invertible in $\mathbb{K}[[x]]$. Since this FPS is actually a polynomial, we might wonder whether it is invertible in $\mathbb{K}[x]$ as well. The answer is "no", unless the ring $\mathbb{K}$ is trivial.[221] More generally, we can easily characterize the invertible elements of $\mathbb{K}[x]$ when $\mathbb{K}$ is a field:

Proposition 7.9.1. Let $\mathbb{K}$ be a field. Let $\mathbf{a} \in \mathbb{K}[x]$ be a polynomial. Then, $\mathbf{a}$ is invertible in $\mathbb{K}[x]$ if and only if $\deg \mathbf{a} = 0$ (that is, $\mathbf{a}$ is a nonzero constant polynomial).

Proof of Proposition 7.9.1 (sketched). $\Longleftarrow$: Assume that $\deg \mathbf{a} = 0$. Then, $\mathbf{a} = \underline{a}$ for some $a \in \mathbb{K}$. This a is nonzero (since otherwise, we would have $\mathbf{a} = \underline{0}$ and thus $\deg \mathbf{a} = -\infty$, which contradicts $\deg \mathbf{a} = 0$), and thus invertible (since $\mathbb{K}$ is a field). Now, it is easy to see that $\underline{a^{-1}}$ is a multiplicative inverse of $\mathbf{a}$ in $\mathbb{K}[x]$. Hence, $\mathbf{a}$ is invertible in $\mathbb{K}[x]$. This proves the "$\Longleftarrow$" direction of Proposition 7.9.1.

$\Longrightarrow$: Assume that $\mathbf{a}$ is invertible in $\mathbb{K}[x]$. Then, $\mathbf{a}$ has a multiplicative inverse $\mathbf{a}^{-1} \in \mathbb{K}[x]$. Clearly, $\mathbf{a}\mathbf{a}^{-1} = 1_{\mathbb{K}[x]} = \underline{1}$, so that $\deg\left(\mathbf{a}\mathbf{a}^{-1}\right) = 0$. Also, from $\mathbf{a}\mathbf{a}^{-1} = \underline{1} \neq 0$, we conclude that $\mathbf{a}$ and $\mathbf{a}^{-1}$ are nonzero. Thus, $\deg \mathbf{a}$ and $\deg\left(\mathbf{a}^{-1}\right)$ are nonnegative integers. Theorem 7.4.11 **(f)** (applied to $\mathbf{b} = \mathbf{a}^{-1}$) yields $\deg\left(\mathbf{a}\mathbf{a}^{-1}\right) = \deg \mathbf{a} + \underbrace{\deg\left(\mathbf{a}^{-1}\right)}_{\geq 0} \geq \deg \mathbf{a}$, thus $\deg \mathbf{a} \leq \deg\left(\mathbf{a}\mathbf{a}^{-1}\right) = 0$. Hence, $\deg \mathbf{a} = 0$ (since $\deg \mathbf{a}$ is a nonnegative integer). This proves the "$\Longrightarrow$" direction of Proposition 7.9.1. □

[221] Indeed, if it was invertible in $\mathbb{K}[x]$, then its multiplicative inverse in $\mathbb{K}[x]$ would also be its multiplicative inverse in $\mathbb{K}[[x]]$; but we already know that the latter is $1 - x + x^2 - x^3 \pm \cdots$ and therefore does not belong to $\mathbb{K}[x]$ unless $\mathbb{K}$ is trivial.

If the ring $\mathbb{K}$ is not a field, the situation becomes more interesting: As we have already seen, the polynomial $1 + 2x$ is invertible when $\mathbb{K} = \mathbb{Z}/4$, despite its degree not being 0, so Proposition 7.9.1 would no longer hold here. Instead, we can give a necessary and sufficient criterion based on the notion of *nilpotent elements*. Let us define this notion:

Definition 7.9.2. Let $\mathbb{L}$ be a ring. Let $a \in \mathbb{L}$. We say that a is *nilpotent* if there exists an $r \in \mathbb{N}$ satisfying $a^r = 0$.

In other words, an element a of a ring $\mathbb{L}$ is nilpotent if one of its powers is 0.

For example:

- The element 0 of any ring $\mathbb{L}$ is nilpotent, since $0^r = 0$ holds for $r = 1$.
- If $m \in \mathbb{Z}$ and $k \in \mathbb{N}$, then the element $[m]_{m^k}$ of $\mathbb{Z}/m^k$ is nilpotent, since its k-th power is $\left[m^k\right]_{m^k} = 0$.
- The nilpotent elements of a matrix ring $\mathbb{K}^{n \times n}$ are exactly the nilpotent $n \times n$-matrices. It is well-known that any nilpotent $n \times n$-matrix A over a field $\mathbb{K}$ satisfies $A^n = 0$; but this is not always true when $\mathbb{K}$ is not a field.

If $\mathbb{K}$ is a field, then the only nilpotent element of $\mathbb{K}$ is 0 (this can be easily proven using Exercise 5.5.2).

Let us state two basic and simple properties of nilpotent elements:

Proposition 7.9.3. Let $\mathbb{L}$ be a ring. Let a and b be two nilpotent elements of $\mathbb{L}$ such that $ab = ba$. Then, $a + b$ is also nilpotent.

The requirement $ab = ba$ in Proposition 7.9.3 cannot be removed: e.g., the two matrices $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ in $\mathbb{Q}^{2\times 2}$ are nilpotent, but their sum $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is not.

Proof of Proposition 7.9.3. We know that a is nilpotent. In other words, there exists a $p \in \mathbb{N}$ satisfying $a^p = 0$ (by the definition of "nilpotent"). Similarly, there exists a $q \in \mathbb{N}$ such that $b^q = 0$ (since b is nilpotent). Consider these p and q.

Now, every $k \in \{0, 1, \ldots, p\}$ satisfies

$$b^{p+q-k} = 0. \tag{316}$$

[*Proof of (316):* Let $k \in \{0, 1, \ldots, p\}$. Then, $k \leq p$, so that $p - k \in \mathbb{N}$. Now, $p + q - k = q + (p - k)$, so that

$$\begin{aligned} b^{p+q-k} &= b^{q+(p-k)} = \underbrace{b^q}_{=0} b^{p-k} \qquad (\text{since } p - k \in \mathbb{N}) \\ &= 0 b^{p-k} = 0. \end{aligned}$$

This proves (316).]

Furthermore, every $k \in \{p+1, p+2, \ldots, p+q\}$ satisfies

$$a^k = 0. \tag{317}$$

[*Proof of (317):* Let $k \in \{p+1, p+2, \ldots, p+q\}$. Then, $k \geq p+1 \geq p$, so that $k - p \in \mathbb{N}$. Now, $k = p + (k-p)$, so that

$$\begin{aligned} a^k &= a^{p+(k-p)} = \underbrace{a^p}_{=0} a^{k-p} \qquad \left(\text{since } k-p \in \mathbb{N}\right) \\ &= 0a^{k-p} = 0. \end{aligned}$$

This proves (317).]

Now, $ab = ba$. Thus, (183) (applied to $\mathbb{K} = \mathbb{L}$ and $n = p+q$) yields

$$\begin{aligned} (a+b)^{p+q} &= \sum_{k=0}^{p+q} \binom{n}{k} a^k b^{p+q-k} = \sum_{k=0}^{p} \binom{n}{k} a^k \underbrace{b^{p+q-k}}_{\substack{=0 \\ \text{(by (316))}}} + \sum_{k=p+1}^{p+q} \binom{n}{k} \underbrace{a^k}_{\substack{=0 \\ \text{(by (317))}}} b^{p+q-k} \\ &= \underbrace{\sum_{k=0}^{p} \binom{n}{k} a^k 0}_{=0} + \underbrace{\sum_{k=p+1}^{p+q} \binom{n}{k} 0 b^{p+q-k}}_{=0} = 0. \end{aligned}$$

Thus, there exists an $r \in \mathbb{N}$ satisfying $(a+b)^r = 0$ (namely, $r = p+q$). In other words, $a+b$ is nilpotent (by the definition of "nilpotent"). This proves Proposition 7.9.3. □

Proposition 7.9.4. Let $\mathbb{L}$ be a ring. Let u be an invertible element of $\mathbb{L}$. Let a be a nilpotent element of $\mathbb{L}$ such that $ua = au$. Then, the element $u - a$ of $\mathbb{L}$ is invertible.

Proof of Proposition 7.9.4 (sketched). The element u is invertible. Thus, it has a multiplicative inverse $u^{-1} \in \mathbb{L}$. We have $uu^{-1} = 1_{\mathbb{L}} = u^{-1}u$.

We know that a is nilpotent. In other words, there exists an $r \in \mathbb{N}$ satisfying $a^r = 0$ (by the definition of "nilpotent"). Consider this r.

Applying (182) to $\mathbb{K} = \mathbb{L}$, $a = u$, $b = u^{-1}$ and $n = r$, we obtain $\left(uu^{-1}\right)^r = u^r \left(u^{-1}\right)^r$ (since $uu^{-1} = u^{-1}u$). Thus, $u^r \left(u^{-1}\right)^r = \left(\underbrace{uu^{-1}}_{=1_{\mathbb{L}}}\right)^r = \left(1_{\mathbb{L}}\right)^r = 1_{\mathbb{L}}$.

Furthermore, $ua = au$. Hence, Proposition 5.4.11 **(d)** (applied to $\mathbb{L}$, u, a and r instead of $\mathbb{K}$, a, b and n) yields

$$u^r - a^r = (u-a)\left(u^{r-1} + u^{r-2}a + \cdots + ua^{r-2} + a^{r-1}\right).$$

Comparing this with $u^r - \underbrace{a^r}_{=0} = u^r$, we obtain

$$(u-a)\left(u^{r-1} + u^{r-2}a + \cdots + ua^{r-2} + a^{r-1}\right) = u^r.$$

Multiplying both sides of this equality with $\left(u^{-1}\right)^r$, we obtain

$$(u-a)\left(u^{r-1} + u^{r-2}a + \cdots + ua^{r-2} + a^{r-1}\right)\left(u^{-1}\right)^r = u^r\left(u^{-1}\right)^r = 1_{\mathbb{L}}.$$

A similar argument (but using products in the opposite order[222]) shows that

$$\left(u^{-1}\right)^r\left(u^{r-1} + u^{r-2}a + \cdots + ua^{r-2} + a^{r-1}\right)(u-a) = 1_{\mathbb{L}}.$$

Hence, Exercise 5.5.3 (applied to $\mathbb{L}$, $\left(u^{-1}\right)^r\left(u^{r-1} + u^{r-2}a + \cdots + ua^{r-2} + a^{r-1}\right)$, $u - a$ and $\left(u^{r-1} + u^{r-2}a + \cdots + ua^{r-2} + a^{r-1}\right)\left(u^{-1}\right)^r$ instead of $\mathbb{K}$, a, b and c) shows that the element $u-a$ is invertible and its multiplicative inverse satisfies

$$\begin{aligned}(u-a)^{-1} &= \left(u^{-1}\right)^r\left(u^{r-1} + u^{r-2}a + \cdots + ua^{r-2} + a^{r-1}\right)\\ &= \left(u^{r-1} + u^{r-2}a + \cdots + ua^{r-2} + a^{r-1}\right)\left(u^{-1}\right)^r.\end{aligned}$$

This proves Proposition 7.9.4. □

Now, when is a polynomial $\mathbf{a} \in \mathbb{K}[x]$ invertible in $\mathbb{K}[x]$? The answer is given by the following result:

Theorem 7.9.5. Let $\mathbf{a} \in \mathbb{K}[x]$ (where $\mathbb{K}$, still, is a commutative ring). Then, $\mathbf{a}$ is invertible in $\mathbb{K}[x]$ if and only if

- its coefficient $\left[x^0\right]\mathbf{a}$ is invertible in $\mathbb{K}$, **and**
- its coefficients $[x^n]\,\mathbf{a}$ are nilpotent for all positive integers n.

For example, the polynomial $\mathbf{a} = 1 + 2x$ over $\mathbb{K} = \mathbb{Z}/4$ satisfies this condition, since its coefficient $\left[x^0\right]\mathbf{a} = [1]_4$ is invertible in $\mathbb{Z}/4$ whereas its other coefficients (which are $[2]_4, [0]_4, [0]_4, [0]_4, \ldots$) are nilpotent.

[222] and, accordingly, relying on a variant of Proposition 5.4.11 **(d)** that says

$$a^n - b^n = \left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right)(a-b)$$

instead of

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right)$$

We will not prove Theorem 7.9.5 here. We only notice that its "$\Longleftarrow$" direction is fairly easy (using Proposition 7.9.3 and Proposition 7.9.4), while its "$\Longrightarrow$" direction is proven in `https://math.stackexchange.com/a/392604/` .

Note the stark contrast between Theorem 7.9.5 and Theorem 7.3.1.

Now that we have introduced nilpotent elements, we might also wonder when a polynomial is nilpotent. This can also be answered:

Theorem 7.9.6. Let $\mathbf{a} \in \mathbb{K}[x]$ (where $\mathbb{K}$, still, is a commutative ring). Then, $\mathbf{a}$ is nilpotent if and only if its coefficients $[x^n]\,\mathbf{a}$ are nilpotent for all $n \in \mathbb{N}$.

Again, we omit the proof of this theorem.

Note that Theorem 7.9.6 has no analogue for FPSs: An FPS can fail to be nilpotent even if all its coefficients are nilpotent.

Let us briefly note that the non-invertibility of most polynomials over a field can be amended: We can introduce formal fractions of polynomials over a field in the same way as formal fractions of integers (also known as "rational numbers") were defined. These fractions are called *rational functions*[223].

7.10. Functoriality of power series and polynomial rings

The polynomial ring $\mathbb{K}[x]$, and the ring $\mathbb{K}[[x]]$ of FPSs, are defined for every ring $\mathbb{K}$. How do they depend on $\mathbb{K}$? For example, does $\mathbb{Z}[x]$ lie in $\mathbb{Q}[x]$ in the same way $\mathbb{Z}$ lies in $\mathbb{Q}$? The answer is a "yes", for fairly simple reasons:

Proposition 7.10.1. Let $\mathbb{K}$ be a subring of a commutative ring $\mathbb{L}$. Then:

(a) The polynomial ring $\mathbb{K}[x]$ is a subring of $\mathbb{L}[x]$.

(b) The ring $\mathbb{K}[[x]]$ is a subring of $\mathbb{L}[[x]]$.

Proof of Proposition 7.10.1 (sketched). **(b)** This is easy: The elements of $\mathbb{K}[[x]]$ are sequences of elements of $\mathbb{K}$. But any sequence of elements of $\mathbb{K}$ is a sequence of elements of $\mathbb{L}$ (since $\mathbb{K} \subseteq \mathbb{L}$), and thus belongs to $\mathbb{L}[[x]]$. Hence, $\mathbb{K}[[x]] \subseteq \mathbb{L}[[x]]$. The rest of the proof is straightforward.

(a) LTTR. □

So being a subring is "inherited" to polynomial rings and rings of FPSs.

Does a homomorphism between two commutative rings also yield a homomorphism between their polynomial rings or a homomorphism between their FPS rings? The next theorem shows that the answer is "yes" to both questions:

Theorem 7.10.2. Let $\mathbb{K}$ and $\mathbb{L}$ be two commutative rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism.

[223] This is a confusing name, because polynomials are not functions. It is an artifact of the history of the subject.

(a) Then, the map

$$\mathbb{K}[[x]] \to \mathbb{L}[[x]],$$
$$(a_0, a_1, a_2, \ldots) \mapsto (f(a_0), f(a_1), f(a_2), \ldots)$$

is a ring homomorphism.

(b) Its restriction to $\mathbb{K}[x]$ is a ring homomorphism from $\mathbb{K}[x]$ to $\mathbb{L}[x]$.

Proof of Theorem 7.10.2. **(a)** Let us denote this map by F. We must then prove that F is a ring homomorphism.

Let us only prove that $F(\mathbf{ab}) = F(\mathbf{a}) F(\mathbf{b})$ for all $\mathbf{a}, \mathbf{b} \in \mathbb{K}[[x]]$. (This is axiom **(c)** in Definition 5.9.1; the other three axioms are proven similarly.)

Let $\mathbf{a}, \mathbf{b} \in \mathbb{K}[[x]]$. Write the FPSs $\mathbf{a}$ and $\mathbf{b}$ as $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ and $\mathbf{b} = (b_0, b_1, b_2, \ldots)$. Then, their images $F(\mathbf{a})$ and $F(\mathbf{b})$ under F are

$$F(\mathbf{a}) = (f(a_0), f(a_1), f(a_2), \ldots) \qquad \text{and} \qquad F(\mathbf{b}) = (f(b_0), f(b_1), f(b_2), \ldots)$$

(by the definition of F). Hence, the definition of the multiplication on $\mathbb{L}[[x]]$ yields

$$F(\mathbf{a}) F(\mathbf{b}) = (d_0, d_1, d_2, \ldots), \tag{318}$$

where

$$d_n = \sum_{i=0}^{n} f(a_i) f(b_{n-i}) \qquad \text{for all } n \in \mathbb{N}. \tag{319}$$

Consider these d_n.

On the other hand, $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ and $\mathbf{b} = (b_0, b_1, b_2, \ldots)$. Hence, the definition of the multiplication on $\mathbb{K}[[x]]$ yields

$$\mathbf{ab} = (c_0, c_1, c_2, \ldots), \tag{320}$$

where

$$c_n = \sum_{i=0}^{n} a_i b_{n-i} \qquad \text{for all } n \in \mathbb{N}. \tag{321}$$

Consider these c_n. From (320), we obtain

$$F(\mathbf{ab}) = (f(c_0), f(c_1), f(c_2), \ldots) \qquad \text{(by the definition of } F\text{)}. \tag{322}$$

But for each $n \in \mathbb{N}$, we have

$$\begin{aligned} f(c_n) &= f\left(\sum_{i=0}^{n} a_i b_{n-i}\right) && \text{(by (321))} \\ &= \sum_{i=0}^{n} \underbrace{f(a_i b_{n-i})}_{\substack{= f(a_i) f(b_{n-i}) \\ \text{(since } f \text{ is a ring} \\ \text{homomorphism)}}} && \text{(by Proposition 5.9.14 (e))} \\ &= \sum_{i=0}^{n} f(a_i) f(b_{n-i}) = d_n && \text{(by (319))}. \end{aligned}$$

Hence, $(f(c_0), f(c_1), f(c_2), \ldots) = (d_0, d_1, d_2, \ldots)$. Thus, the right hand sides of the equalities (322) and (318) are equal. Hence, their left hand sides are equal as well. In other words, we have $F(\mathbf{ab}) = F(\mathbf{a}) F(\mathbf{b})$. Thus, the map F satisfies axiom **(c)** in Definition 5.9.1. As we have said, the other three axioms are proven similarly; thus, F is a ring homomorphism. This proves Theorem 7.10.2 **(a)**.

(b) LTTR. □

8. Quotient constructions

8.1. Residue classes in commutative rings

8.1.1. The general case

We have previously defined

- what it means for an **integer** to divide an integer (Definition 2.2.1);
- what it means for a **Gaussian integer** to divide a Gaussian integer (Definition 4.2.17);
- what it means for a **polynomial** to divide a polynomial (Definition 7.6.8).

These definitions differed only in what kind of "numbers" we were using. So let us generalize them all together:

> **Definition 8.1.1.** Let $\mathbb{L}$ be a commutative ring. Let a and b be two elements of $\mathbb{L}$. We say that $a \mid b$ *in* $\mathbb{L}$ (or "*a divides b in* $\mathbb{L}$" or "b is *divisible by a in* $\mathbb{L}$" or "b is a *multiple* of *a in* $\mathbb{L}$") if there exists a $c \in \mathbb{L}$ such that $b = ac$.
>
> We furthermore say that $a \nmid b$ *in* $\mathbb{L}$ if a does not divide b *in* $\mathbb{L}$.

We shall omit the words "in $\mathbb{L}$" whenever $\mathbb{L}$ is clear. But keep in mind that $\mathbb{L}$ matters. For example, $2 \nmid 1$ in $\mathbb{Z}$, but $2 \mid 1$ in $\mathbb{Q}$ (since $1 = 2 \cdot \dfrac{1}{2}$). Of course, when we speak of divisibility between integers, we mean "in $\mathbb{Z}$", since divisibility in $\mathbb{Q}$ is boring[224].

Most of the standard properties of divisibility still work for any commutative ring $\mathbb{L}$. For example:

- we have $a \mid a$ for all $a \in \mathbb{L}$;
- if $a, b, c \in \mathbb{L}$ satisfy $a \mid b$ and $b \mid c$, then $a \mid c$,

[224] More generally: If $\mathbb{F}$ is any field, then divisibility in $\mathbb{F}$ is boring (because $a \mid b$ holds for any $a, b \in \mathbb{F}$ unless we have $a = 0$ and $b \neq 0$).

and so on. (But, for example, the obvious generalization of Exercise 2.2.3 does not work: In general, we cannot conclude $a \mid b$ from $ac \mid bc$ even if $c \neq 0$.)

We can furthermore generalize the concept of congruence (Definition 2.3.1 and Definition 4.2.21) to arbitrary commutative rings:

Definition 8.1.2. Let $\mathbb{L}$ be a commutative ring. Let $w, a, b \in \mathbb{L}$. We say that *a is congruent to b modulo w (in $\mathbb{L}$)* if and only if $w \mid a - b$. We shall use the notation "$a \equiv b \mod w$" for "a is congruent to b modulo w".

We furthermore shall use the notation "$a \not\equiv b \mod w$" for "a is not congruent to b modulo w".

Again, the standard properties of congruence all hold. For example, the following analogue of Proposition 2.3.4 holds (and is proven in the same way as Proposition 2.3.4):

Proposition 8.1.3. Let $\mathbb{L}$ be a commutative ring. Let $w \in \mathbb{L}$.

(a) We have $a \equiv a \mod w$ for every $a \in \mathbb{L}$.

(b) If $a, b, c \in \mathbb{L}$ satisfy $a \equiv b \mod w$ and $b \equiv c \mod w$, then $a \equiv c \mod w$.

(c) If $a, b \in \mathbb{L}$ satisfy $a \equiv b \mod w$, then $b \equiv a \mod w$.

(d) If $a_1, a_2, b_1, b_2 \in \mathbb{L}$ satisfy $a_1 \equiv b_1 \mod w$ and $a_2 \equiv b_2 \mod w$, then

$$a_1 + a_2 \equiv b_1 + b_2 \mod w; \tag{323}$$

$$a_1 - a_2 \equiv b_1 - b_2 \mod w; \tag{324}$$

$$a_1 a_2 \equiv b_1 b_2 \mod w. \tag{325}$$

(e) Let $m \in \mathbb{L}$ be such that $m \mid w$. If $a, b \in \mathbb{L}$ satisfy $a \equiv b \mod w$, then $a \equiv b \mod m$.

Now, we can define the straightforward generalization of residue classes (Definition 3.4.2 and Definition 3.4.3) and of the standard operations (addition, multiplication and scaling) on them (Definition 3.4.12 and Definition 3.4.18):

Definition 8.1.4. Fix a commutative ring $\mathbb{L}$ and an element $w \in \mathbb{L}$.

(a) Define a relation $\underset{w}{\equiv}$ on the set $\mathbb{L}$ by

$$\left(a \underset{w}{\equiv} b\right) \iff (a \equiv b \mod w) .$$

This $\underset{w}{\equiv}$ is an equivalence relation. (The proof of this is analogous to the proof of Example 3.2.5.)

(b) A *residue class modulo w* means an equivalence class of the relation $\underset{w}{\equiv}$.

(c) If $a \in \mathbb{L}$, then we denote the residue class $[a]_{\underset{w}{\equiv}}$ by $[a]_w$.

(d) The set $\mathbb{L} / \underset{w}{\equiv}$ of all residue classes modulo w is called $\mathbb{L}/w$.

(e) We define a binary operation $+$ on $\mathbb{L}/w$ (called *addition*) by setting

$$[a]_w + [b]_w = [a+b]_w \qquad \text{for all } a, b \in \mathbb{L}.$$

This is well-defined, because of Theorem 8.1.5 **(a)** below.

(f) We define a binary operation $\cdot$ on $\mathbb{L}/w$ (called *multiplication*) by setting

$$[a]_w \cdot [b]_w = [a \cdot b]_w \qquad \text{for all } a, b \in \mathbb{L}.$$

This is well-defined, because of Theorem 8.1.5 **(a)** below.

(g) Fix $r \in \mathbb{L}$. For any $\alpha \in \mathbb{L}/w$, we define a residue class $r\alpha \in \mathbb{L}/w$ by setting

$$\left(r\,[a]_w = [ra]_w \qquad \text{for any } a \in \mathbb{L}\right).$$

(In other words, for any $\alpha \in \mathbb{L}/w$, we let $r\alpha = [ra]_w$, where a is an element of $\mathbb{L}$ satisfying $\alpha = [a]_w$.) This is well-defined, because of Theorem 8.1.5 **(a)** below.

We shall also write $r \cdot \alpha$ instead of $r\alpha$. The map $\mathbb{L} \times (\mathbb{L}/w) \to \mathbb{L}/w,\ (r, \alpha) \mapsto r\alpha$ will be called *scaling*.

If we set $\mathbb{L} = \mathbb{Z}$ in Definition 8.1.4, and let w be an integer n, then we recover our old definitions of residue classes modulo n and of their set $\mathbb{Z}/n$. Note that we are not defining a subtraction on $\mathbb{L}/w$ this time, because we will get it for free once we recognize $\mathbb{L}/w$ as a ring.

Theorem 8.1.5. Fix a commutative ring $\mathbb{L}$ and an element $w \in \mathbb{L}$.

(a) The operations $+$ and $\cdot$ and the "scaling map" $\cdot$ in Definition 8.1.4 are well-defined.

(b) The set $\mathbb{L}/w$, equipped with the addition $+$ (defined in Definition 8.1.4 **(e)**), the multiplication $\cdot$ (defined in Definition 8.1.4 **(f)**) and the zero $[0]_w$ and the unity $[1]_w$, is a commutative ring.

(c) The set $\mathbb{L}/w$, equipped with the addition $+$ (defined in Definition 8.1.4 **(e)**), the scaling $\cdot$ (defined in Definition 8.1.4 **(g)**) and the zero vector $[0]_w$, is an $\mathbb{L}$-module.

(d) The set $\mathbb{L}/w$, equipped with all of these items, is a commutative $\mathbb{L}$-algebra.

(e) The map

$$\begin{aligned} \pi_w : \mathbb{L} &\to \mathbb{L}/w, \\ a &\mapsto [a]_w \end{aligned}$$

is an $\mathbb{L}$-algebra homomorphism.

Proof of Theorem 8.1.5. All of this is analogous to the proofs we did for integers (but $\mathbb{Z}$ and n have to become $\mathbb{L}$ and w). To be more specific:

- The proof of Theorem 8.1.5 **(a)** is analogous to the proof of Proposition 3.4.13 and Proposition 3.4.19 **(a)**.
- The proof of Theorem 8.1.5 **(b)** boils down to checking the ring axioms and the "commutativity of multiplication" axiom. This is analogous to our proof of Theorem 3.4.23, except that the representatives of our residue classes are now elements of $\mathbb{L}$ rather than integers.

- The proof of Theorem 8.1.5 **(c)** boils down to checking the module axioms. This is analogous to our proof of Theorem 3.4.23.
- The proof of Theorem 8.1.5 **(d)** boils down to checking the "Scale-invariance of multiplication" axiom (since all remaining axioms have already been checked when we proved parts **(b)** and **(c)** of this theorem). This is analogous to our proof of Theorem 3.4.23 **(m)**.
- The proof of Theorem 8.1.5 **(e)** follows straightforwardly from the definition of the operations $+$ and $\cdot$ and the scaling map on $\mathbb{L}/w$.

□

Definition 8.1.6. Consider the setting of Theorem 8.1.5.

The commutative $\mathbb{L}$-algebra $\mathbb{L}/w$ constructed in Theorem 8.1.5 **(d)** is called "$\mathbb{L}$ *modulo* w" or "$\mathbb{L}$ *divided by* w" or "$\mathbb{L}$ *quotiented by* w". Whenever we speak of "the $\mathbb{L}$-algebra $\mathbb{L}/w$", we shall mean this precise $\mathbb{L}$-algebra.

The reader can easily check the following:

- If we have $w = 0$ in Theorem 8.1.5, then the map π_w is an $\mathbb{L}$-algebra isomorphism, so that $\mathbb{L}/0 \cong \mathbb{L}$ as rings and as $\mathbb{L}$-modules.
- If we have $w = 1$ in Theorem 8.1.5, then the ring $\mathbb{L}/w = \mathbb{L}/1$ is trivial. More generally, if $w \in \mathbb{L}$ is invertible, then the ring $\mathbb{L}/w$ is trivial.

8.1.2. The case of a polynomial ring

The commutative $\mathbb{L}$-algebra $\mathbb{L}/w$ constructed in Theorem 8.1.5 **(d)** generalizes not just the $\mathbb{Z}$-algebras $\mathbb{Z}/n$, but also the $\mathbb{Z}[i]$-algebras $\mathbb{Z}[i]/\alpha$ (where α is a Gaussian integer). But we can apply this construction to other rings $\mathbb{L}$ as well. It will prove particularly useful to apply it to $\mathbb{L} = \mathbb{K}[x]$, where $\mathbb{K}$ is a commutative ring. In particular, this will help us adjoin a root of a polynomial to a commutative ring $\mathbb{K}$. First, let us introduce some standard conventions:

Convention 8.1.7. Let $\mathbb{K}$ be a commutative ring.

(a) Any $\mathbb{K}[x]$-module automatically becomes a $\mathbb{K}$-module: In fact, let M be a $\mathbb{K}[x]$-module. Then, $\mathbf{a}m$ is defined for each $\mathbf{a} \in \mathbb{K}[x]$ and each $m \in M$. But we have identified each element $a \in \mathbb{K}$ with the corresponding constant polynomial $\underline{a} \in \mathbb{K}[x]$. Thus, am is also defined for each $a \in \mathbb{K}$ and each $m \in M$ (because we can treat a as a constant polynomial); explicitly speaking, it is defined by the equality

$$am = \underline{a}m \qquad \text{for all } a \in \mathbb{K} \text{ and } m \in M.$$

Thus, a "scaling" map $\cdot : \mathbb{K} \times M \to M$ is defined. This "scaling" map (along with the addition and the zero vector that M is already equipped with) makes M a $\mathbb{K}$-module. Thus, every $\mathbb{K}[x]$-module M automatically becomes a $\mathbb{K}$-module.

(b) In this way, any $\mathbb{K}[x]$-algebra becomes a $\mathbb{K}$-algebra (because we just explained how it becomes a $\mathbb{K}$-module, and it is easy to see that this $\mathbb{K}$-module structure harmonizes with the ring structure in a way that yields a $\mathbb{K}$-algebra[225]).

(c) Any $\mathbb{K}[x]$-module homomorphism is automatically a $\mathbb{K}$-module homomorphism. (This is easy to check.)

(d) Any $\mathbb{K}[x]$-algebra homomorphism is automatically a $\mathbb{K}$-algebra homomorphism. (This is easy to check.)

Thus, in particular, if $\mathbf{b} \in \mathbb{K}[x]$ is any polynomial, then the $\mathbb{K}[x]$-algebra $\mathbb{K}[x]/\mathbf{b}$ automatically becomes a $\mathbb{K}$-algebra as well.

Proposition 8.1.8. Let $\mathbb{K}$ be a commutative ring. Let $\mathbf{b} \in \mathbb{K}[x]$ be a polynomial.

(a) The projection map

$$\pi_{\mathbf{b}} : \mathbb{K}[x] \to \mathbb{K}[x]/\mathbf{b},$$
$$\mathbf{a} \mapsto [\mathbf{a}]_{\mathbf{b}}$$

is a $\mathbb{K}[x]$-algebra homomorphism and thus a $\mathbb{K}$-algebra homomorphism.

(b) The map

$$\mathbb{K} \to \mathbb{K}[x]/\mathbf{b},$$
$$a \mapsto [\underline{a}]_{\mathbf{b}}$$

is a $\mathbb{K}$-algebra homomorphism.

(c) We have $\mathbf{a}[[x]_{\mathbf{b}}] = [\mathbf{a}]_{\mathbf{b}}$ for any $\mathbf{a} \in \mathbb{K}[x]$.

(d) The element $[x]_{\mathbf{b}} \in \mathbb{K}[x]/\mathbf{b}$ is a root of $\mathbf{b}$.

Proof of Proposition 8.1.8. **(a)** This is a particular case of Theorem 8.1.5 **(e)** (applied to $\mathbb{L} = \mathbb{K}[x]$ and $w = \mathbf{b}$).

(b) This map is a composition of the projection map $\pi_{\mathbf{b}}$ from Proposition 8.1.8 **(a)** with the map $\mathbb{K} \to \mathbb{K}[x]$, $a \mapsto \underline{a}$. Since both of the maps we are composing are $\mathbb{K}$-algebra homomorphisms, their composition is therefore a $\mathbb{K}$-algebra homomorphism as well.

(c) The projection map

$$\pi_{\mathbf{b}} : \mathbb{K}[x] \to \mathbb{K}[x]/\mathbf{b},$$
$$\mathbf{a} \mapsto [\mathbf{a}]_{\mathbf{b}}$$

is a $\mathbb{K}$-algebra homomorphism (by Proposition 8.1.8 **(a)**). Now, let $\mathbf{a} \in \mathbb{K}[x]$. The definition of $\pi_{\mathbf{b}}$ yields $\pi_{\mathbf{b}}(x) = [x]_{\mathbf{b}}$ and $\pi_{\mathbf{b}}(\mathbf{a}) = [\mathbf{a}]_{\mathbf{b}}$. But Proposition 7.6.13

[225] i.e., the "Scale-invariance of multiplication" axiom is satisfied

(applied to $\mathbb{K}[x]$, $\mathbb{K}[x]/\mathbf{b}$, $\pi_{\mathbf{b}}$ and x instead of U, V, f and u) yields

$$\begin{aligned} \pi_{\mathbf{b}}(\mathbf{a}[x]) &= \mathbf{a}\left[\underbrace{\pi_{\mathbf{b}}(x)}_{=[x]_{\mathbf{b}}}\right] \qquad \text{(since } \pi_{\mathbf{b}} \text{ is a } \mathbb{K}\text{-algebra homomorphism)} \\ &= \mathbf{a}\left[[x]_{\mathbf{b}}\right]. \end{aligned}$$

Hence,

$$\mathbf{a}\left[[x]_{\mathbf{b}}\right] = \pi_{\mathbf{b}}\left(\underbrace{\mathbf{a}[x]}_{=\mathbf{a}}\right) = \pi_{\mathbf{b}}(\mathbf{a}) = [\mathbf{a}]_{\mathbf{b}}.$$

This proves Proposition 8.1.8 **(c)**.

(d) We must prove that $\mathbf{b}\left[[x]_{\mathbf{b}}\right] = 0_{\mathbb{K}[x]/\mathbf{b}}$.

Applying Proposition 8.1.8 **(c)** to $\mathbf{a} = \mathbf{b}$, we obtain

$$\begin{aligned} \mathbf{b}\left[[x]_{\mathbf{b}}\right] &= [\mathbf{b}]_{\mathbf{b}} = [0]_{\mathbf{b}} \qquad (\text{since } \mathbf{b} \equiv 0 \bmod \mathbf{b}) \\ &= 0_{\mathbb{K}[x]/\mathbf{b}}, \end{aligned}$$

and this shows that $[x]_{\mathbf{b}}$ is a root of $\mathbf{b}$. This proves Proposition 8.1.8 **(d)**. □

Theorem 8.1.9. Let $\mathbb{K}$ be a commutative ring.

Let $m \in \mathbb{N}$. Let $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ be such that $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible. Then:

(a) Each element of $\mathbb{K}[x]/\mathbf{b}$ can be uniquely written in the form

$$\lambda_0\left[x^0\right]_{\mathbf{b}} + \lambda_1\left[x^1\right]_{\mathbf{b}} + \cdots + \lambda_{m-1}\left[x^{m-1}\right]_{\mathbf{b}} \qquad \text{with } \lambda_0, \lambda_1, \ldots, \lambda_{m-1} \in \mathbb{K}.$$

(b) The m vectors $\left[x^0\right]_{\mathbf{b}}, \left[x^1\right]_{\mathbf{b}}, \ldots, \left[x^{m-1}\right]_{\mathbf{b}}$ form a basis of the $\mathbb{K}$-module $\mathbb{K}[x]/\mathbf{b}$. (See Definition 6.11.1 **(d)** for what "basis" means.)

(c) Assume that $m > 0$. Then, the $\mathbb{K}$-algebra homomorphism

$$\begin{aligned} \mathbb{K} &\to \mathbb{K}[x]/\mathbf{b}, \\ a &\mapsto [\underline{a}]_{\mathbf{b}} \end{aligned}$$

is injective. Thus, $\mathbb{K}$ can be viewed as a $\mathbb{K}$-subalgebra of $\mathbb{K}[x]/\mathbf{b}$ if we identify each $a \in \mathbb{K}$ with the $[\underline{a}]_{\mathbf{b}} \in \mathbb{K}[x]/\mathbf{b}$.

Proof of Theorem 8.1.9. **(a)** Let $\alpha \in \mathbb{K}[x]/\mathbf{b}$. Then, $\alpha = [\mathbf{a}]_{\mathbf{b}}$ for **some** polynomial $\mathbf{a} \in \mathbb{K}[x]$. Consider this $\mathbf{a}$. Theorem 7.5.1 **(a)** yields that there is a unique pair $(\mathbf{q}, \mathbf{r})$ of polynomials with $\mathbf{a} = \mathbf{qb} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$. Consider this pair $(\mathbf{q}, \mathbf{r})$. Then, $\mathbf{a} = \underbrace{\mathbf{qb}}_{\equiv 0 \bmod \mathbf{b}} + \mathbf{r} \equiv \mathbf{r} \bmod \mathbf{b}$, so that $[\mathbf{a}]_{\mathbf{b}} = [\mathbf{r}]_{\mathbf{b}}$.

Write $\mathbf{r}$ in the form $\mathbf{r} = r_0x^0 + r_1x^1 + \cdots + r_{m-1}x^{m-1}$ with $r_0, r_1, \ldots, r_{m-1} \in \mathbb{K}$ (this can be done, since $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$). Then,

$$\begin{aligned}\alpha = [\mathbf{a}]_{\mathbf{b}} = [\mathbf{r}]_{\mathbf{b}} &= \left[r_0x^0 + r_1x^1 + \cdots + r_{m-1}x^{m-1}\right]_{\mathbf{b}} \\ &\qquad \left(\text{since } \mathbf{r} = r_0x^0 + r_1x^1 + \cdots + r_{m-1}x^{m-1}\right) \\ &= r_0\left[x^0\right]_{\mathbf{b}} + r_1\left[x^1\right]_{\mathbf{b}} + \cdots + r_{m-1}\left[x^{m-1}\right]_{\mathbf{b}}.\end{aligned}$$

So we have found a way to write α in the form

$$\lambda_0\left[x^0\right]_{\mathbf{b}} + \lambda_1\left[x^1\right]_{\mathbf{b}} + \cdots + \lambda_{m-1}\left[x^{m-1}\right]_{\mathbf{b}} \qquad \text{with } \lambda_0, \lambda_1, \ldots, \lambda_{m-1} \in \mathbb{K}$$

(namely, with $(\lambda_0, \lambda_1, \ldots, \lambda_{m-1}) = (r_0, r_1, \ldots, r_{m-1})$).

It remains to prove that this way is unique. This can easily be done using the uniqueness part of Theorem 7.5.1 **(a)**.[226] Thus, Theorem 8.1.9 **(a)** is proven.

[226] Here is the argument in detail:

Let $(\mu_0, \mu_1, \ldots, \mu_{m-1})$ and $(\rho_0, \rho_1, \ldots, \rho_{m-1})$ be two m-tuples $(\lambda_0, \lambda_1, \ldots, \lambda_{m-1}) \in \mathbb{K}^m$ satisfying $\alpha = \lambda_0\left[x^0\right]_{\mathbf{b}} + \lambda_1\left[x^1\right]_{\mathbf{b}} + \cdots + \lambda_{m-1}\left[x^{m-1}\right]_{\mathbf{b}}$. We shall show that $(\mu_0, \mu_1, \ldots, \mu_{m-1}) = (\rho_0, \rho_1, \ldots, \rho_{m-1})$.

Define a polynomial $\mathbf{m} \in \mathbb{K}[x]$ by $\mathbf{m} = \mu_0x^0 + \mu_1x^1 + \cdots + \mu_{m-1}x^{m-1}$. Then, $\mathbf{m} \in \mathbb{K}[x]_{\leq m-1}$ and

$$\left[x^i\right]\mathbf{m} = \mu_i \qquad \text{for each } i \in \{0, 1, \ldots, m-1\}. \tag{326}$$

We know that $(\mu_0, \mu_1, \ldots, \mu_{m-1})$ is an m-tuple $(\lambda_0, \lambda_1, \ldots, \lambda_{m-1}) \in \mathbb{K}^m$ satisfying $\alpha = \lambda_0\left[x^0\right]_{\mathbf{b}} + \lambda_1\left[x^1\right]_{\mathbf{b}} + \cdots + \lambda_{m-1}\left[x^{m-1}\right]_{\mathbf{b}}$. In other words, $(\mu_0, \mu_1, \ldots, \mu_{m-1})$ is an m-tuple in $\mathbb{K}^m$ and satisfies $\alpha = \mu_0\left[x^0\right]_{\mathbf{b}} + \mu_1\left[x^1\right]_{\mathbf{b}} + \cdots + \mu_{m-1}\left[x^{m-1}\right]_{\mathbf{b}}$. Thus, from $\alpha = [\mathbf{a}]_{\mathbf{b}}$, we obtain

$$[\mathbf{a}]_{\mathbf{b}} = \alpha = \mu_0\left[x^0\right]_{\mathbf{b}} + \mu_1\left[x^1\right]_{\mathbf{b}} + \cdots + \mu_{m-1}\left[x^{m-1}\right]_{\mathbf{b}} = \left[\mu_0x^0 + \mu_1x^1 + \cdots + \mu_{m-1}x^{m-1}\right]_{\mathbf{b}} = [\mathbf{m}]_{\mathbf{b}}$$

(since $\mu_0x^0 + \mu_1x^1 + \cdots + \mu_{m-1}x^{m-1} = \mathbf{m}$). In other words, $\mathbf{a} \equiv \mathbf{m} \mod \mathbf{b}$. In other words, $\mathbf{b} \mid \mathbf{a} - \mathbf{m}$.In other words, there exists a polynomial $\mathbf{c} \in \mathbb{K}[x]$ such that $\mathbf{a} - \mathbf{m} = \mathbf{bc}$. Consider this $\mathbf{c}$. From $\mathbf{a} - \mathbf{m} = \mathbf{bc}$, we obtain $\mathbf{a} = \mathbf{m} + \mathbf{bc} = \mathbf{cb} + \mathbf{m}$.

Now, recall that $(\mathbf{q}, \mathbf{r})$ was defined as the **unique** pair $(\mathbf{q}, \mathbf{r})$ of polynomials with $\mathbf{a} = \mathbf{qb} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$. Thus, in particular, it is the only such pair. In other words, if $(\widetilde{\mathbf{q}}, \widetilde{\mathbf{r}})$ is a pair of polynomials with $\mathbf{a} = \widetilde{\mathbf{q}}\mathbf{b} + \widetilde{\mathbf{r}}$ and $\widetilde{\mathbf{r}} \in \mathbb{K}[x]_{\leq m-1}$, then $(\widetilde{\mathbf{q}}, \widetilde{\mathbf{r}}) = (\mathbf{q}, \mathbf{r})$. We can apply this fact to $(\widetilde{\mathbf{q}}, \widetilde{\mathbf{r}}) = (\mathbf{c}, \mathbf{m})$ (since $\mathbf{a} = \mathbf{cb} + \mathbf{m}$ and $\mathbf{m} \in \mathbb{K}[x]_{\leq m-1}$), and thus obtain $(\mathbf{c}, \mathbf{m}) = (\mathbf{q}, \mathbf{r})$. In other words, $\mathbf{c} = \mathbf{q}$ and $\mathbf{m} = \mathbf{r}$. Now, for each $i \in \{0, 1, \ldots, m-1\}$, we have

$$\begin{aligned}\mu_i &= \left[x^i\right]\underbrace{\mathbf{m}}_{=\mathbf{r}} \qquad (\text{by } (326)) \\ &= \left[x^i\right]\mathbf{r}.\end{aligned} \tag{327}$$

The same argument (applied to $(\rho_0, \rho_1, \ldots, \rho_{m-1})$ instead of $(\mu_0, \mu_1, \ldots, \mu_{m-1})$) shows that for each $i \in \{0, 1, \ldots, m-1\}$, we have

$$\rho_i = \left[x^i\right]\mathbf{r}.$$

Comparing this with (327), we conclude that for each $i \in \{0, 1, \ldots, m-1\}$, we have $\mu_i = \rho_i$. In other words, $(\mu_0, \mu_1, \ldots, \mu_{m-1}) = (\rho_0, \rho_1, \ldots, \rho_{m-1})$.

(b) Proposition 6.11.2 shows that Theorem 8.1.9 **(b)** is a restatement of Theorem 8.1.9 **(a)**. Thus, Theorem 8.1.9 **(b)** holds.

(c) We already know (from Proposition 8.1.8 **(b)**) that the map

$$\begin{aligned} \mathbb{K} &\to \mathbb{K}[x]/\mathbf{b}, \\ a &\mapsto [\underline{a}]_{\mathbf{b}} \end{aligned}$$

is a $\mathbb{K}$-algebra homomorphism. We just need to show that it is injective. In other words, we need to show that if $a, b \in \mathbb{K}$ satisfy $[\underline{a}]_{\mathbf{b}} = [\underline{b}]_{\mathbf{b}}$, then $a = b$.

So let $a, b \in \mathbb{K}$ satisfy $[\underline{a}]_{\mathbf{b}} = [\underline{b}]_{\mathbf{b}}$. Note that

$$\begin{aligned} [\underline{a}]_{\mathbf{b}} &= \left[ax^0\right]_{\mathbf{b}} \qquad \left(\text{since } \underline{a} = a \cdot \underbrace{\underline{1}}_{=x^0} = ax^0\right) \\ &= a\left[x^0\right]_{\mathbf{b}}, \end{aligned}$$

and similarly $[\underline{b}]_{\mathbf{b}} = b\left[x^0\right]_{\mathbf{b}}$. Hence, the equality $[\underline{a}]_{\mathbf{b}} = [\underline{b}]_{\mathbf{b}}$ rewrites as

$$a\left[x^0\right]_{\mathbf{b}} = b\left[x^0\right]_{\mathbf{b}}.$$

Thus, define an element $\alpha \in \mathbb{K}[x]/\mathbf{b}$ by $\alpha = a\left[x^0\right]_{\mathbf{b}} = b\left[x^0\right]_{\mathbf{b}}$. Then, we have found two ways of representing the element $\alpha \in \mathbb{K}[x]/\mathbf{b}$ in the form

$$\lambda_0\left[x^0\right]_{\mathbf{b}} + \lambda_1\left[x^1\right]_{\mathbf{b}} + \cdots + \lambda_{m-1}\left[x^{m-1}\right]_{\mathbf{b}} \qquad \text{with } \lambda_0, \lambda_1, \ldots, \lambda_{m-1} \in \mathbb{K}:$$

one way uses $\lambda_0 = a$ and $\lambda_i = 0$ for all $i > 0$; the other way uses $\lambda_0 = b$ and $\lambda_i = 0$ for all $i > 0$. But the "uniqueness" statement in Theorem 8.1.9 **(a)** yields that there is only one way to represent an element in this form. Hence, these two ways must be equal. Therefore, $a = b$. □

Note that Theorem 8.1.9 **(c)** really requires m to be > 0 (otherwise, $\mathbb{K}[x]/\mathbf{b}$ is a trivial ring) and $[x^m]\,\mathbf{b}$ to be invertible (we will see an example below where $[x^m]\,\mathbf{b}$ is not invertible, and $\mathbb{K}$ does not inject into $\mathbb{K}[x]/\mathbf{b}$).

We now understand the quotient rings $\mathbb{K}[x]/\mathbf{b}$ well enough at least in the case when the leading coefficient of $\mathbf{b}$ is invertible. Let us use this to see some examples:

Now, forget that we fixed $(\mu_0, \mu_1, \ldots, \mu_{m-1})$ and $(\rho_0, \rho_1, \ldots, \rho_{m-1})$. We thus have shown that if $(\mu_0, \mu_1, \ldots, \mu_{m-1})$ and $(\rho_0, \rho_1, \ldots, \rho_{m-1})$ are two m-tuples $(\lambda_0, \lambda_1, \ldots, \lambda_{m-1}) \in \mathbb{K}^m$ satisfying $\alpha = \lambda_0\left[x^0\right]_{\mathbf{b}} + \lambda_1\left[x^1\right]_{\mathbf{b}} + \cdots + \lambda_{m-1}\left[x^{m-1}\right]_{\mathbf{b}}$, then $(\mu_0, \mu_1, \ldots, \mu_{m-1}) = (\rho_0, \rho_1, \ldots, \rho_{m-1})$. In other words, any two m-tuples $(\lambda_0, \lambda_1, \ldots, \lambda_{m-1}) \in \mathbb{K}^m$ satisfying $\alpha = \lambda_0\left[x^0\right]_{\mathbf{b}} + \lambda_1\left[x^1\right]_{\mathbf{b}} + \cdots + \lambda_{m-1}\left[x^{m-1}\right]_{\mathbf{b}}$ must be identical. In other words, there exists at most one such m-tuple. In other words, there is at most one way to write α in the form

$$\lambda_0\left[x^0\right]_{\mathbf{b}} + \lambda_1\left[x^1\right]_{\mathbf{b}} + \cdots + \lambda_{m-1}\left[x^{m-1}\right]_{\mathbf{b}} \qquad \text{with } \lambda_0, \lambda_1, \ldots, \lambda_{m-1} \in \mathbb{K}.$$

Since we already know that such a way exists, we thus conclude that such a way is unique.

Example 8.1.10. We have $\mathbb{C} \cong \mathbb{R}[x] \,/\, (x^2+1)$ (as rings).

Indeed, the map

$$\begin{aligned} \mathbb{C} &\to \mathbb{R}[x] \,/\, \left(x^2+1\right), \\ (a,b) = a + bi &\mapsto [a+bx]_{x^2+1} \end{aligned}$$

is a ring homomorphism, and is invertible, with inverse

$$\begin{aligned} \mathbb{R}[x] \,/\, \left(x^2+1\right) &\to \mathbb{C}, \\ [\mathbf{a}]_{x^2+1} &\mapsto \mathbf{a}[i]. \end{aligned}$$

To see that the latter inverse is well-defined, you have to check that if $\mathbf{a}$ and $\mathbf{b}$ are two polynomials in $\mathbb{R}[x]$ satisfying $\mathbf{a} \equiv \mathbf{b} \bmod x^2+1$, then $\mathbf{a}[i] = \mathbf{b}[i]$. (LTTR.)

Example 8.1.11. We have $\mathbb{Z}[i] \cong \mathbb{Z}[x] \,/\, (x^2+1)$ (as rings).

Example 8.1.12. Recall the dual numbers $\mathbb{D}$ from homework set #4 exercise 3. Each dual number has the form $(a,b) = a + b\varepsilon$ for a unique pair (a,b) of real numbers, and the multiplication of $\mathbb{D}$ satisfies $\varepsilon^2 = 0$.

We have $\mathbb{D} \cong \mathbb{R}[x] \,/ x^2$ (as rings). More precisely, the map

$$\begin{aligned} \mathbb{D} &\to \mathbb{R}[x] \,/ x^2, \\ (a,b) = a + b\varepsilon &\mapsto [a+bx]_{x^2} \end{aligned}$$

is a ring isomorphism.

Moreover, we also have $\mathbb{D} \cong \mathbb{R}[[x]] \,/ x^2$ as rings.

Note, however, that this is unusual: Normally, if $\mathbf{a} \in \mathbb{K}[x]$ is a polynomial, then $\mathbb{K}[[x]] \,/ \mathbf{a}$ is not isomorphic to $\mathbb{K}[x] \,/ \mathbf{a}$. For example, the ring $\mathbb{R}[x] \,/\, (x^2+1)$ is isomorphic to $\mathbb{C}$ (as we have seen above), whereas the ring $\mathbb{R}[[x]] \,/\, (x^2+1)$ is trivial (since the FPS x^2+1 is invertible, and thus any two FPSs are congruent to each other modulo x^2+1).

Example 8.1.13. In Section 5.6, we constructed a field with 4 elements by adjoining a j satisfying $j^2 = j+1$ to $\mathbb{Z}/2$. This field is isomorphic to

$$(\mathbb{Z}/2)[x] \,/\, \left(x^2 - x - 1\right).$$

Example 8.1.14. Let $m \in \mathbb{Z}$ be nonzero. On midterm #2 exercise 1, we defined R_m to be the set of all m-integers (= rational numbers that can be turned into integers by multiplying with m often enough). We proved that R_m is a ring. Each element of R_m can be written in the form $\dfrac{a}{m^k}$ for some $a \in \mathbb{Z}$ and some

$k \in \mathbb{N}$ (but these a and k are not unique, since $\dfrac{a}{m^k} = \dfrac{am}{m^{k+1}} = \dfrac{am^2}{m^{k+2}} = \cdots$).

This ring R_m is isomorphic to the ring $\mathbb{Z}[x] / (mx-1)$. Indeed, we have a ring homomorphism

$$\mathbb{Z}[x] / (mx-1) \to R_m, \\ [\mathbf{a}]_{mx-1} \mapsto \mathbf{a}\left[\frac{1}{m}\right],$$

and this is invertible, with inverse

$$R_m \to \mathbb{Z}[x] / (mx-1), \\ \frac{a}{m^k} \mapsto \left[ax^k\right]_{mx-1} \qquad (\text{for } a \in \mathbb{Z} \text{ and } k \in \mathbb{N})$$

(you have to check that this is well-defined).

Note that Theorem 8.1.9 does not apply here (unless $m \in \{1, -1\}$), and the $\mathbb{Z}$-module R_m has no basis (again, unless $m \in \{1, -1\}$).

Note that R_m (the ring of m-integers) is commonly called $\mathbb{Z}\left[\dfrac{1}{m}\right]$, in analogy to $\mathbb{Z}[i]$.

Example 8.1.15. We have a ring isomorphism

$$(\mathbb{Z}/6)[x] / (2x+1) \cong \mathbb{Z}/3.$$

Thus, if we adjoin a root of $2x+1$ to the ring $\mathbb{Z}/6$, then we get a smaller ring (namely, $\mathbb{Z}/3$). In particular, there is no injective map from $\mathbb{Z}/6$ to the result of this adjunction!

This is no surprise, since $\left[x^1\right](2x+1) = [2]_6$ is not invertible in $\mathbb{Z}/6$, and thus Theorem 8.1.9 does not apply here.

This is similar to how dividing by 0 makes all numbers equal:

$$\mathbb{Z}[x] / (0x-1) \cong \{0\}.$$

Let us summarize: We can always adjoin a root of a polynomial $\mathbf{b}$ to a commutative ring $\mathbb{K}$ by forming the ring $\mathbb{K}[x] / \mathbf{b}$. This latter ring will always be a commutative ring; moreover, if $\mathbf{b}$ is "nice" (that is, there is a positive integer m such that $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ and such that $[x^m]\,\mathbf{b}$ is invertible), then Theorem 8.1.9 **(c)** shows that this latter ring will contain $\mathbb{K}$ as a subring (at least if we make a natural identification). If $\mathbf{b}$ is not as "nice", then the ring $\mathbb{K}[x] / \mathbf{b}$ may fail to contain $\mathbb{K}$ as a subring (though it is always a $\mathbb{K}$-algebra), and may be smaller than $\mathbb{K}$ and even trivial.

If $\mathbb{K}$ itself is a field, then $\mathbf{b}$ will always be "nice" (unless $\mathbf{b} = 0$), but the ring

$\mathbb{K}[x]/\mathbf{b}$ may and may not be a field. What must a polynomial $\mathbf{b}$ satisfy in order for $\mathbb{K}[x]/\mathbf{b}$ to be a field?

Definition 8.1.16. Let $\mathbb{F}$ be a field.

A polynomial $\mathbf{a} \in \mathbb{F}[x]$ is said to be *irreducible* if $\deg \mathbf{a} > 0$ and there exist no two polynomials $\mathbf{b}, \mathbf{c} \in \mathbb{F}[x]$ with $\mathbf{a} = \mathbf{bc}$ and $\deg \mathbf{b} > 0$ and $\deg \mathbf{c} > 0$.

In other words, a polynomial $\mathbf{a} \in \mathbb{F}[x]$ is said to be *irreducible* if it is non-constant but cannot be written as a product of two non-constant polynomials. (Indeed, the non-constant polynomials are precisely the polynomials having degree > 0.)

Irreducible polynomials over a field $\mathbb{F}$ are an analogue of prime numbers (or, to be more precise, of integers of the form $\pm p$ where p is a prime).

Theorem 8.1.17. Let $\mathbb{F}$ be a field. Let $\mathbf{a} \in \mathbb{F}[x]$ be a polynomial.

Then, the ring $\mathbb{F}[x]/\mathbf{a}$ is a field if and only if $\mathbf{a}$ is irreducible.

So, for example, the irreducible polynomial x^2+1 over $\mathbb{R}$ yields the field $\mathbb{R}[x]/\left(x^2+1\right)$ (which is $\cong \mathbb{C}$), but the non-irreducible polynomial x^2 over $\mathbb{R}$ yields the non-field $\mathbb{R}[x]/x^2$ (which is $\cong \mathbb{D}$).

Proof of Theorem 8.1.17 (sketched). In Subsection 7.5.2, we have already explained that there is an analogy between polynomials in $\mathbb{F}[x]$ and Gaussian integers in $\mathbb{Z}[i]$ (although we denoted the field by $\mathbb{K}$ rather than $\mathbb{F}$ in that Subsection). In particular, the degree of a polynomial is analogous to the norm of a Gaussian integer. The nonzero constant polynomials in $\mathbb{F}[x]$ (that is, the polynomials of degree 0) are precisely the units of the ring $\mathbb{F}[x]$ (that is, the invertible elements of $\mathbb{F}[x]$) [227], and thus play the same role in $\mathbb{F}[x]$ that the units $1, -1, i, -i$ play in $\mathbb{Z}[i]$. Theorem 7.5.4 serves as an analogue of Theorem 4.2.26, and can be used to prove an analogue of Bezout's theorem for polynomials in $\mathbb{F}[x]$. This lets us define an analogue of gcds. Irreducible polynomials in $\mathbb{F}[x]$ are an analogue of Gaussian primes. This analogy between $\mathbb{Z}[i]$ and $\mathbb{F}[x]$ is not perfect[228]; but it suffices to prove $\mathbb{F}[x]$-analogues of all the fundamental results such as Theorem 2.9.12, Theorem 2.9.15, Theorem 2.10.6, Theorem 2.10.7, Theorem 2.10.8, Proposition 2.13.4, Proposition 2.13.5 and Theorem 2.13.6.[229] As a consequence, we can prove an $\mathbb{F}[x]$-analogue of Theorem 5.5.8. This latter analogue shows that if $\mathbf{n} \in \mathbb{F}[x]$ is a polynomial of degree $\deg \mathbf{n} > 0$, then the ring $\mathbb{F}[x]/\mathbf{n}$ is a field if and only if $\mathbf{n}$ is irreducible. Applying this to $\mathbf{n} = \mathbf{a}$, we obtain Theorem 8.1.17 (after first dealing with the easy case when $\deg \mathbf{a} \leq 0$). □

[227] This follows from Proposition 7.9.1.

[228] For example: If $n \in \mathbb{N}$, then there are only finitely many Gaussian integers $\alpha \in \mathbb{Z}[i]$ having norm n, but there are often infinitely many polynomials $\mathbf{a} \in \mathbb{F}[x]$ having degree n.

[229] The analogue of Proposition 2.13.4 states that if $\mathbf{p} \in \mathbb{F}[x]$ is an irreducible polynomial, then every polynomial $\mathbf{i} \in \mathbb{F}[x]$ with degree $\deg \mathbf{i} \in \{1, 2, \ldots, \deg \mathbf{p} - 1\}$ is coprime to $\mathbf{p}$.

8.2. Quotients modulo ideals

8.2.1. Congruence and quotients modulo ideals

The notion of "congruence modulo w" introduced in Definition 8.1.2 was a generalization of "congruence modulo n" from number theory; but it can be generalized further. Namely, we can replace w by an ideal I of $\mathbb{L}$. (See Definition 6.12.5 for the definition of an ideal.) Here is how this general notion is defined:

Definition 8.2.1. Let $\mathbb{L}$ be a ring. Let I be an ideal of $\mathbb{L}$. Let $a, b \in \mathbb{L}$. We say that *a is congruent to b modulo I (in $\mathbb{L}$)* if and only if $a - b \in I$. We shall use the notation "$a \equiv b \mod I$" for "a is congruent to b modulo I".

We furthermore shall use the notation "$a \not\equiv b \mod I$" for "a is not congruent to b modulo I".

Why is this a generalization of "congruence modulo w"? Because congruence modulo w is recovered if we take I to be the principal ideal[230] $w\mathbb{L}$. More precisely, the following holds:

Proposition 8.2.2. Let $\mathbb{L}$ be a commutative ring. Let $w \in \mathbb{L}$. Let $a, b \in \mathbb{L}$. Consider the principal ideal $w\mathbb{L}$ of $\mathbb{L}$, defined as in Example 6.12.6 (that is, by $w\mathbb{L} = \{wz \mid z \in \mathbb{L}\}$). Then, $a \equiv b \mod w$ holds if and only if $a \equiv b \mod w\mathbb{L}$.

Proof of Proposition 8.2.2. The definition of $w\mathbb{L}$ yields $w\mathbb{L} = \{wz \mid z \in \mathbb{L}\}$. Now, We have the following chain of equivalences:

$$\begin{aligned}
(a \equiv b \mod w) &\iff (w \mid a - b) \qquad \text{(by Definition 8.1.2)} \\
&\iff (a - b = wz \text{ for some } z \in \mathbb{L}) \\
&\qquad \text{(by Definition 8.1.1)} \\
&\iff \left(a - b \in \underbrace{\{wz \mid z \in \mathbb{L}\}}_{= w\mathbb{L}} \right) \iff (a - b \in w\mathbb{L}) \\
&\iff (a \equiv b \mod w\mathbb{L}) \qquad \text{(by Definition 8.2.1)}.
\end{aligned}$$

Thus, Proposition 8.2.2 is proven. □

Knowing that "congruence modulo I" is a generalization of "congruence modulo w" and of "congruence modulo n", we can play the usual game in which we recall properties of the latter and check whether they still hold for the former. For example, the following generalization of Proposition 8.1.3 holds:

Proposition 8.2.3. Let $\mathbb{L}$ be a ring. Let I be an ideal of $\mathbb{L}$.

(a) We have $a \equiv a \mod I$ for every $a \in \mathbb{L}$.

(b) If $a, b, c \in \mathbb{L}$ satisfy $a \equiv b \mod I$ and $b \equiv c \mod I$, then $a \equiv c \mod I$.

[230] See Example 6.12.6 for the definition of principal ideals.

(c) If $a, b \in \mathbb{L}$ satisfy $a \equiv b \mod I$, then $b \equiv a \mod I$.

(d) If $a_1, a_2, b_1, b_2 \in \mathbb{L}$ satisfy $a_1 \equiv b_1 \mod I$ and $a_2 \equiv b_2 \mod I$, then

$$a_1 + a_2 \equiv b_1 + b_2 \mod I; \tag{328}$$

$$a_1 - a_2 \equiv b_1 - b_2 \mod I; \tag{329}$$

$$a_1 a_2 \equiv b_1 b_2 \mod I. \tag{330}$$

(e) Let J be an ideal of $\mathbb{L}$ such that $I \subseteq J$. If $a, b \in \mathbb{L}$ satisfy $a \equiv b \mod I$, then $a \equiv b \mod J$.

Note how the "$I \subseteq J$" assumption in Proposition 8.2.3 **(e)** is the correct generalization of the "$m \mid w$" assumption in Proposition 8.1.3, because of the following fact:

Proposition 8.2.4. Let $\mathbb{L}$ be a commutative ring. Let $m, w \in \mathbb{L}$. Then, $w\mathbb{L} \subseteq m\mathbb{L}$ holds if and only if $m \mid w$. (Here, the principal ideals $w\mathbb{L}$ and $m\mathbb{L}$ are defined as in Example 6.12.6).

This proposition is so easy it barely needs proof, but it illustrates a useful point of view: Divisibility of elements of $\mathbb{L}$ can be rewritten as containment of ideals of $\mathbb{L}$.

Proof of Proposition 8.2.4. $\Longrightarrow$: Assume that $w\mathbb{L} \subseteq m\mathbb{L}$. We must prove that $m \mid w$.

The definition of $w\mathbb{L}$ yields $w\mathbb{L} = \{wz \mid z \in \mathbb{L}\}$. Now, $w = w \cdot 1$; hence, the element w has the form wz for some $z \in \mathbb{L}$ (namely, for $z = 1$). Thus,

$$w \in \{wz \mid z \in \mathbb{L}\} = w\mathbb{L} \subseteq m\mathbb{L} = \{mz \mid z \in \mathbb{L}\}$$

(by the definition of $m\mathbb{L}$). In other words, $w = mz$ for some $z \in \mathbb{L}$. In other words, $m \mid w$ (by Definition 8.1.1). Thus, the "$\Longrightarrow$" part of Proposition 8.2.4 is proven.

$\Longleftarrow$: Assume that $m \mid w$. We must prove that $w\mathbb{L} \subseteq m\mathbb{L}$.

We have assumed that $m \mid w$. In other words, $w = mc$ for some $c \in \mathbb{L}$. Consider this c.

The definition of $m\mathbb{L}$ yields $m\mathbb{L} = \{mz \mid z \in \mathbb{L}\} = \{ma \mid a \in \mathbb{L}\}$ (here, we have renamed the index z as a).

Now, let $g \in w\mathbb{L}$. Hence, $g \in w\mathbb{L} = \{wz \mid z \in \mathbb{L}\}$ (by the definition of $w\mathbb{L}$). In other words, $g = wz$ for some $z \in \mathbb{L}$. Consider this z. Then, $g = \underbrace{w}_{=mc} z = mcz$. Hence, $g = ma$ for some $a \in \mathbb{L}$ (namely, for $a = cz$). In other words, $g \in \{ma \mid a \in \mathbb{L}\} = m\mathbb{L}$.

Forget that we fixed g. We thus have shown that $g \in m\mathbb{L}$ for some $g \in w\mathbb{L}$. In other words, $w\mathbb{L} \subseteq m\mathbb{L}$. Thus, the "$\Longleftarrow$" part of Proposition 8.2.4 is proven. □

Proof of Proposition 8.2.3. We know that I is an ideal of $\mathbb{L}$. Thus, I satisfies the four conditions in Definition 6.12.5 (applied to $\mathbb{L}$ instead of $\mathbb{K}$). In other words, the following holds:

- The subset I is closed under addition (i.e., we have $a+b \in I$ for all $a \in I$ and $b \in I$).

- The subset I contains $0_{\mathbb{L}}$.

- We have
$$\lambda a \in I \qquad \text{for all } \lambda \in \mathbb{L} \text{ and } a \in I. \tag{331}$$

- We have
$$a\lambda \in I \qquad \text{for all } \lambda \in \mathbb{L} \text{ and } a \in I. \tag{332}$$

(a) Let $a \in \mathbb{L}$. We know that I contains $0_{\mathbb{L}}$. Thus, $0_{\mathbb{L}} \in I$. Now, $a - a = 0_{\mathbb{L}} \in I$. This rewrites as $a \equiv a \bmod I$ (by Definition 8.2.1). This proves Proposition 8.2.3 **(a)**.

(b) Let $a, b, c \in \mathbb{L}$ satisfy $a \equiv b \bmod I$ and $b \equiv c \bmod I$. Then, $a \equiv b \bmod I$, so that $a - b \in I$ (by Definition 8.2.1). Similarly, $b - c \in I$. But we know that I is closed under addition. Hence, from $a - b \in I$ and $b - c \in I$, we obtain $\underbrace{(a-b)}_{\in I} + \underbrace{(b-c)}_{\in I} \in I$. Hence, $a - c = (a-b) + (b-c) \in I$. In other words, $a \equiv c \bmod I$ (by Definition 8.2.1). This proves Proposition 8.2.3 **(b)**.

(c) Let $a, b \in \mathbb{L}$ satisfy $a \equiv b \bmod I$. Thus, $a - b \in I$ (by Definition 8.2.1). Hence, (331) (applied to -1 and $a - b$ instead of λ and a) yields $(-1)(a-b) \in I$. Hence, $b - a = (-1)(a-b) \in I$. In other words, $b \equiv a \bmod I$ (by Definition 8.2.1). This proves Proposition 8.2.3 **(c)**.

(d) Let $a_1, a_2, b_1, b_2 \in \mathbb{L}$ satisfy $a_1 \equiv b_1 \bmod I$ and $a_2 \equiv b_2 \bmod I$. We have $a_1 \equiv b_1 \bmod I$ and thus $a_1 - b_1 \in I$ (by Definition 8.2.1). But we know that I is closed under addition. Hence, from $a_1 - b_1 \in I$ and $a_2 - b_2 \in I$, we obtain $\underbrace{(a_1 - b_1)}_{\in I} + \underbrace{(a_2 - b_2)}_{\in I} \in I$. Hence,
$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in I.$$
In other words, $a_1 + a_2 \equiv b_1 + b_2 \bmod I$ (by Definition 8.2.1).

Recall that $a_2 - b_2 \in I$. Hence, (331) (applied to -1 and $a_2 - b_2$ instead of λ and a) yields $(-1)(a_2 - b_2) \in I$. Hence, $b_2 - a_2 = (-1)(a_2 - b_2) \in I$. Recall again that I is closed under addition. Hence, from $a_1 - b_1 \in I$ and $b_2 - a_2 \in I$, we obtain $\underbrace{(a_1 - b_1)}_{\in I} + \underbrace{(b_2 - a_2)}_{\in I} \in I$. Hence,
$$(a_1 - a_2) - (b_1 - b_2) = (a_1 - b_1) + (b_2 - a_2) \in I.$$
In other words, $a_1 - a_2 \equiv b_1 - b_2 \bmod I$ (by Definition 8.2.1).

It remains to prove that $a_1 a_2 \equiv b_1 b_2 \bmod I$.

Let us first show that $a_1 a_2 \equiv a_1 b_2 \bmod I$. Indeed, $a_1 a_2 - a_1 b_2 = a_1 (a_2 - b_2) \in I$ (by (331), applied to a_1 and $a_2 - b_2$ instead of λ and a), because $a_2 - b_2 \in I$. In other words, $a_1 a_2 \equiv a_1 b_2 \bmod I$.

Next, we shall show that $a_1 b_2 \equiv b_1 b_2 \bmod I$. Indeed, $a_1 b_2 - b_1 b_2 = (a_1 - b_1) b_2 \in I$ (by (332), applied to b_2 and $a_1 - b_1$ instead of λ and a), because $a_1 - b_1 \in I$. In other words, $a_1 b_2 \equiv b_1 b_2 \bmod I$.

Now, we have $a_1 a_2 \equiv a_1 b_2 \bmod I$ and $a_1 b_2 \equiv b_1 b_2 \bmod I$. Hence, Proposition 8.2.3 **(b)** (applied to $a = a_1 a_2$, $b = a_1 b_2$ and $c = b_1 b_2$) yields $a_1 a_2 \equiv b_1 b_2 \bmod I$. This completes the proof of Proposition 8.2.3 **(d)**.

(e) Let $a, b \in \mathbb{L}$ satisfy $a \equiv b \bmod I$. Thus, $a - b \in I$ (by Definition 8.2.1). Hence, $a - b \in I \subseteq J$. In other words, $a \equiv b \bmod J$ (by Definition 8.2.1). This proves Proposition 8.2.3 **(e)**. □

The following definition generalizes Definition 8.1.4 (and thus also generalizes our construction of $\mathbb{Z}/n$ for $n \in \mathbb{Z}$):

Definition 8.2.5. Fix a ring $\mathbb{L}$ and an ideal I of $\mathbb{L}$.

(a) Define a relation $\underset{I}{\equiv}$ on the set $\mathbb{L}$ by

$$\left(a \underset{I}{\equiv} b \right) \iff (a \equiv b \bmod I) .$$

This $\underset{I}{\equiv}$ is an equivalence relation. (The proof of this is analogous to the proof of Example 3.2.5.)

(b) A *residue class modulo I* means an equivalence class of the relation $\underset{I}{\equiv}$.

(c) If $a \in \mathbb{L}$, then we denote the residue class $[a]_{\underset{I}{\equiv}}$ by $[a]_I$.

(d) The set $\mathbb{L} / \underset{I}{\equiv}$ of all residue classes modulo I is called $\mathbb{L}/I$.

(e) We define a binary operation $+$ on $\mathbb{L}/I$ (called *addition*) by setting

$$[a]_I + [b]_I = [a+b]_I \qquad \text{for all } a, b \in \mathbb{L}.$$

This is well-defined, because of Theorem 8.2.6 **(a)** below.

(f) We define a binary operation $\cdot$ on $\mathbb{L}/I$ (called *multiplication*) by setting

$$[a]_I \cdot [b]_I = [a \cdot b]_I \qquad \text{for all } a, b \in \mathbb{L}.$$

This is well-defined, because of Theorem 8.2.6 **(a)** below.

(g) Fix $r \in \mathbb{L}$. For any $\alpha \in \mathbb{L}/I$, we define a residue class $r\alpha \in \mathbb{L}/I$ by setting

$$\left(r [a]_I = [ra]_I \qquad \text{for any } a \in \mathbb{L} \right) .$$

(In other words, for any $\alpha \in \mathbb{L}/I$, we let $r\alpha = [ra]_I$, where a is an element of $\mathbb{L}$ satisfying $\alpha = [a]_I$.) This is well-defined, because of Theorem 8.2.6 **(a)** below.

We shall also write $r \cdot \alpha$ instead of $r\alpha$. The map $\mathbb{L} \times (\mathbb{L}/I) \to \mathbb{L}/I$, $(r, \alpha) \mapsto r\alpha$ will be called *scaling*.

Theorem 8.2.6. Fix a ring $\mathbb{L}$ and an ideal I of $\mathbb{L}$.

(a) The operations $+$ and $\cdot$ and the "scaling map" $\cdot$ in Definition 8.2.5 are well-defined.

(b) The set $\mathbb{L}/I$, equipped with the addition $+$ (defined in Definition 8.2.5 **(e)**), the multiplication $\cdot$ (defined in Definition 8.2.5 **(f)**) and the zero $[0]_I$ and the unity $[1]_I$, is a commutative ring.

(c) The set $\mathbb{L}/I$, equipped with the addition $+$ (defined in Definition 8.2.5 **(e)**), the scaling $\cdot$ (defined in Definition 8.2.5 **(g)**) and the zero vector $[0]_I$, is an $\mathbb{L}$-module when $\mathbb{L}$ is commutative.

(d) The set $\mathbb{L}/I$, equipped with all of these items, is an $\mathbb{L}$-algebra when $\mathbb{L}$ is commutative.

(e) The map

$$\pi_I : \mathbb{L} \to \mathbb{L}/I,$$
$$a \mapsto [a]_I$$

is an $\mathbb{L}$-algebra homomorphism.

(f) If the ring $\mathbb{L}$ is commutative, then the ring $\mathbb{L}/I$ is a commutative $\mathbb{L}$-algebra.

(g) The kernel of the $\mathbb{L}$-algebra homomorphism π_I is $\operatorname{Ker}(\pi_I) = I$. (See Proposition 6.12.8 **(a)** for the definition of a kernel.)

Proof of Theorem 8.2.6. Parts **(a)**, **(b)**, **(c)**, **(d)** and **(e)** of this theorem are proven in the same way as the corresponding parts of Theorem 8.1.5. Part **(f)** is easy.

(g) The map π_I is an $\mathbb{L}$-algebra homomorphism (by Theorem 8.2.6 **(e)**), thus a ring homomorphism.

For each $a \in \mathbb{L}$, we have the following chain of equivalences:

$$\begin{aligned}
& (\pi_I(a) = 0_{\mathbb{L}/I}) \\
\iff & ([a]_I = [0]_I) \\
& \qquad (\text{since } \pi_I(a) = [a]_I \text{ (by the definition of } \pi_I) \text{ and } 0_{\mathbb{L}/I} = [0]_I) \\
\iff & \left([a]_{\underset{I}{\equiv}} = [0]_{\underset{I}{\equiv}}\right) \\
& \qquad \left(\text{since Definition 8.2.5 } \textbf{(c)} \text{ yields } [a]_I = [a]_{\underset{I}{\equiv}} \text{ and } [0]_I = [0]_{\underset{I}{\equiv}}\right) \\
\iff & \left(a \underset{I}{\equiv} 0\right) \qquad \left(\begin{array}{c}\text{since Proposition 3.3.5 } \textbf{(e)} \text{ yields that} \\ \text{we have } a \underset{I}{\equiv} 0 \text{ if and only if } [a]_{\underset{I}{\equiv}} = [0]_{\underset{I}{\equiv}}\end{array}\right) \\
\iff & (a \equiv 0 \bmod I) \qquad (\text{by Definition 8.2.5 } \textbf{(a)}) \\
\iff & (a - 0 \in I) \qquad (\text{by Definition 8.2.1}) \\
\iff & (a \in I) \qquad (\text{since } a - 0 = a).
\end{aligned}$$

Hence,

$$\{a \in \mathbb{L} \mid \pi_I(a) = 0_{\mathbb{L}/I}\} = \{a \in \mathbb{L} \mid a \in I\} = I$$

(since $I \subseteq \mathbb{L}$). Now, the definition of $\operatorname{Ker}(\pi_I)$ yields

$$\begin{aligned} \operatorname{Ker}(\pi_I) &= \left\{v \in \mathbb{L} \mid \pi_I(v) = 0_{\mathbb{L}/I}\right\} = \left\{a \in \mathbb{L} \mid \pi_I(a) = 0_{\mathbb{L}/I}\right\} \\ &\qquad \text{(here, we have renamed the index } v \text{ as } a\text{)} \\ &= I. \end{aligned}$$

This proves Theorem 8.2.6 **(g)**. □

Proposition 8.2.2 shows that Definition 8.2.5 generalizes Definition 8.1.4: Namely, if $\mathbb{L}$ is a commutative ring, and if the ideal I in Definition 8.2.5 is a principal ideal $w\mathbb{L}$ (for some $w \in \mathbb{L}$), then the relation $\underset{I}{\equiv}$ and the ring $\mathbb{L}/I$ are precisely the relation $\underset{w}{\equiv}$ and the ring $\mathbb{L}/w$ defined in Definition 8.1.4. Thus, if w is any element of a commutative ring $\mathbb{L}$, then

$$\mathbb{L}/w = \mathbb{L}/w\mathbb{L}.$$

Thus, in particular, $\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z}$ for any $n \in \mathbb{Z}$. Most authors prefer the notation $\mathbb{Z}/n\mathbb{Z}$ to our notation $\mathbb{Z}/n$ (since it is an instance of the more general construction $\mathbb{L}/I$).

9. Epilogue (UMN Fall 2019 Math 4281)

Here ends our one-semester course on abstract algebra (Fall 2019 at UMN). I will now tie up some loose ends and point into a few directions for further study.

9.1. Roads not taken

During the course of the past semester, we have learned new things about old concepts (such as the integers) as well as new concepts – both concrete (such as the Gaussian integers) and abstract (such as arbitrary rings and fields).

A one-semester course on abstract algebra always has to decide between many things of roughly equal importance; not everything can get its day[231]. The main topics we missed are:

- **Groups** (and monoids, and group homomorphisms, and subgroups, etc.). Many algebra classes **start** with this topic, since much of it can be done with almost no prerequisites. I have kept delaying this topic and, in the end, did not get to it at all. My main excuse is that it would have taken me afield – we haven't needed groups in what we did above (though they would have simplified a few of our proofs). Nevertheless, groups are worth learning about. Readable introductions into groups include [Siksek15], [GalQua17, §4.1–§4.2], [Goodma16, Chapters 1–5] and [Pinter10, Chapter 1–16]; other sources are

[231] The alternative is to skimp on proofs; I consider this the worst option.

[Armstr18, Abstract Algebra I] (with a historical perspective), [Artin10, Chapter 2], [Bosch18, Chapter 1], [Carrel17, Chapter 2], [Elman18, Chapters III–IV], [Knapp16a, Chapter IV], [Loehr11, Chapter 9], [Milne17].

Only a few dozen pages of basic properties of groups will get you ready for the proof of Theorem 3.9.5, which we left unproved. See [GalQua17, §4.1–§4.2] or [Conrad*, "Cyclicity of $(\mathbf{Z}/(p))^{\times}$"] (for the case $n = p$).

- **Permutations**. The basics of this subject are extremely important throughout mathematics; in particular, the notion of the **sign** of a permutation is needed for the study of determinants of matrices and of signed volumes in geometry. Concerning this notion, see [Strick13, Appendix B] for a quick "from-scratch" introduction, and [Conrad*, "The sign of a permutation"] for an approach using group theory.

  You can learn more about permutations from a textbook on enumerative combinatorics (such as [Loehr11]) or on permutation puzzles (such as [Bump02], [Joyner08] or [Mulhol16]). The latter texts focus on permutation-related puzzles such as Rubik's cube and the 15-game; but in doing so, they motivate and introduce the properties of permutations and even the basics of group theory.

- **Determinants**. Determinants belong equally to combinatorics, abstract algebra and linear algebra. As a consequence, none of these courses covers them well; usually, only the most basic properties are stated, and their proofs outlined as best. Strickland, in [Strick13, §12 and Appendix B], gives a short but rigorous and honest treatment of the fundamentals. Other good introductions are found in Day's [Day16, Chapter 6], Mate's [Mate14], Walker's [Walker87, §5.4], and Pinkham's [Pinkha15, Chapter 11] (but they all limit themselves to the basics). In [Grinbe15, Chapter 6], I prove a variety of results (including some nonstandard ones) in much detail (probably too much). The "bible" on determinants is [MuiMet60] (and, for the particularly bold, [Muir30] is a goldmine of forgotten results).

  The determinant used to be one of the central notions in mathematics, and even predated the notion of matrices! (Determinants first appear in a 1693 letter of Leibniz. The word "matrix" was coined in 1850 by J. J. Sylvester, as a "womb" (this is what "matrix" means in Latin) from which determinants spring out.) Determinants have become less central since, thanks to abstract algebra incorporating many ideas that were first stated in their language. Nevertheless, they are still one of the strongest tools on the algebraic side of mathematics.

- **Multivariate polynomials** (i.e., polynomials in several variables). This is a highly useful topic, but it is rarely done justice in one-semester courses on algebra, since it takes some amount of notational work. For example, $3 + 2x + 3x^2y + 6y^2$ is a polynomial in the two variables x, y over the ring $\mathbb{Q}$. To define such polynomials rigorously, we recall that we defined FPSs in one variable as infinite sequences of elements of our ring $\mathbb{K}$. Likewise, we can define FPSs in two variables as infinite "2-dimensional sequences" of elements of $\mathbb{K}$, where a "2-dimensional sequence" is a family $\left(a_{i,j}\right)_{(i,j)\in\mathbb{N}^2}$ of elements of $\mathbb{K}$ indexed by pairs of nonnegative integers.[232] Such an FPS is called a polynomial if the family has only finitely many nonzero entries. Then, x is defined to be the family $\left(a_{i,j}\right)_{(i,j)\in\mathbb{N}^2}$ whose only nonzero entry is $a_{1,0} = 1$, and y is defined to be the family $\left(a_{i,j}\right)_{(i,j)\in\mathbb{N}^2}$ whose only nonzero entry is $a_{0,1} = 1$. The theory of polynomials (and FPSs) in two variables can thus be built up in analogy to our 1-variable theory; details can be found in [Hunger03, Chapter III, §5], [Loehr11, §7.16], [GalQua18, §30.2] and [AmaEsc05, §I.8].

Eventually, the theory of multivariate polynomials becomes more complicated than the 1-variable theory. The first point where it significantly differs is division with remainder: There is no analogue of Theorem 7.5.1; instead there is a rich and highly useful theory of *Gröbner bases* ([CoLiOs15]). Also, a polynomial f in two variables x and y can be evaluated at two elements u and v of a $\mathbb{K}$-algebra U only if u and v commute (that is, $uv = vu$).

- **Galois theory** (i.e., the theory of field extensions and roots of polynomials). This is the study of *field extensions*. In the simplest case, this is about how a field $\mathbb{K}$ grows when a root of some polynomial is adjoined to it. We saw a small bit of it when we constructed $\mathbb{C}$, or finite fields of size p^2, by adjoining roots of quadratic polynomials; but the game can be played in greater generality. When a field $\mathbb{K}$ is a subring of a field $\mathbb{L}$, the pair $(\mathbb{K}, \mathbb{L})$ is called a *field extension* (and is often written as $\mathbb{L}/\mathbb{K}$, a notation that has nothing to do with quotients despite its look). The Galois theory proper studies the $\mathbb{K}$-algebra isomorphisms from $\mathbb{L}$ to $\mathbb{L}$. (For example, there are two $\mathbb{R}$-algebra homomorphisms from $\mathbb{C}$ to $\mathbb{C}$; one of them is simply the identity map, while the other is the conjugation map $z \mapsto \overline{z}$. The dimension of the $\mathbb{R}$-vector space $\mathbb{C}$ also happens to be 2. Coincidence?)

  A one-semester class on Galois theory usually covers only the very basics, but undergraduate-level introductions to the theory exist. Two of them are [Stewar15] and [Tignol01]. Some algebra texts centered on Galois theory are [Armstr18], [Goodma16] and [Bosch18].

- **Finite fields** (also known as Galois fields). We have started exploring them by

[232] You can think of such a "2-dimensional sequence" as an infinite table

$$\begin{array}{cccc} a_{0,0} & a_{0,1} & a_{0,2} & \cdots \\ a_{1,0} & a_{1,1} & a_{1,2} & \cdots \\ a_{2,0} & a_{2,1} & a_{2,2} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{array}.$$

defining the ones of size p and p^2 (for p prime). But as I already mentioned, there exists a finite field of any prime-power size, and it is unique up to isomorphism. Most algebra textbooks that go deeper than a one-semester course will prove this and perhaps say more – Galois theory texts in particular. But there are also books specifically devoted to finite fields, such as [Wan11] and [LidNie97].

Then, there are deeper topics such as representation theory, algebraic number theory and algebraic geometry, which we have grazed at best (see, e.g., [DumFoo04], [Knapp16a] and [Knapp16b]).

9.2. A quick history of algebraic equations

Algebraic equations (i.e., equations of the form $P(x) = 0$, where P is a given polynomial) were the historical origin of much of abstract algebra. Thus, I am going to say a few words about them, even though they eventually lead into topics (like Galois theory and algebraic geometry) which have not been the subject of this course.

The Babylonians knew the quadratic formula: The solutions to a quadratic equation $ax^2 + bx + c = 0$ (say, over $\mathbb{C}$) are $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. (Of course, the Babylonians did not know $\mathbb{C}$; even the negative numbers only appeared during the Chinese Han Dynasty and took a long time to propagate into the West. But the idea was there.)

The question of solving cubic equations ($ax^3 + bx^2 + cx + d = 0$) and equations of higher degree has puzzled people for centuries, until the case of the cubic was solved by Scipione del Ferro and Niccolò Tartaglia (and written up by Girolamo Cardano) in the early 16th Century. The history of their solution has been amply discussed and dramatized in the literature (even over-dramatized, as if the truth wasn't interesting enough!); see the lecture slides

```
https://cs.uwaterloo.ca/~cbruni/CO480Resources/lectures/CO480MayAug2017/lecture11.pdf
```

for a highly readable chronology, and see [Rothma15] for some pop-science claims debunked (including some from the slides).

The formula they found is surprising in its practical uselessness. Consider the case of a "depressed" cubic polynomial; this is a polynomial of the form $x^3 + px + q$ (so the coefficient of x^2 is 0). In this particular case, the Cardano formula[233] says that the roots of this polynomial are

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

[233] The attentive reader will have noticed that this is another instance of an object named for its first expositor, not for its original discoverer. There is a moral here.

The cubic roots here are understood to be *complex* cubic roots[234], which is why you get not 1 but 3 roots[235]. Note that $\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ may be non-real, even if the polynomial has a real root! Ironically, this happens precisely in the case when the cubic polynomial has 3 real roots (which is the maximum possible number); thus, it qualifies as an explicit formula only if we tolerate the presence of cubic roots of complex numbers inside it.

Worse yet: Even if the Cardano formula does not involve any non-real numbers, it is still far from the expression you might be looking for. For instance, let us try to find the roots of the polynomial x^3+3x-4 using this formula. By plugging in $p=3$ and $q=-4$, we get the expression

$$\sqrt[3]{2+\sqrt{4+1}}+\sqrt[3]{2-\sqrt{4+1}}=\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}$$

for its roots. To find the real root, we take the usual (i.e., non-complex) cubic roots. Thus we conclude that $\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}$ is a root of the polynomial x^3+3x-4. But a bit of numerical computation suggests that this root is actually the number 1. And this is indeed the case, as you can easily verify by evaluating the polynomial x^3+3x-4 at 1; but how could you have guessed this from the cube-root formula? So the Cardano formula gave us a complicated expression for the number 1, and no way to simplify it![236]

Nevertheless, the discovery of the Cardano formula has proven highly useful, as it forced the introduction of complex numbers! While complex numbers already appear as solutions of **quadratic** equations, this has not convinced anyone to define them, because everyone would content themselves with the answer "no solutions". But cubic equations like $x^3-x+1=0$ tease you with their 3 real roots which, nevertheless, cannot be expressed through $\sqrt[3]{}$ and $\sqrt{}$ signs until complex numbers are defined. Thus, it was the cubic equation that made complex numbers accepted.[237]

Cardano went on and solved the general quartic equation $ax^4+bx^3+cx^2+dx+e=0$ with an even longer formula. The proofs of these formulas have remained tricky and computational (see, e.g., [Armstr18, Week 1] for the case of the cubic), even as some of the tricks have since been explained using abstract algebra.

[234] If $z\in\mathbb{C}$ is a complex number, then the *complex cubic roots* of z are the complex numbers w satisfying $w^3=z$. There are three of them (unless $z=0$), and (in terms of the Argand diagram) they form the vertices of an equilateral triangle with center at 0.

[235] Actually, you get 9 roots if you are not careful (because there are two $\sqrt[3]{}$ signs in the formula). When picking complex cubic roots of $-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ and $-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$, you should choose not all $3\cdot 3=9$ combinations, but only the ones whose product is $-\frac{1}{3}p$.

[236] Actually, you can prove that $\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}=1$ by showing that $\sqrt[3]{2+\sqrt{5}}=\frac{1}{2}\left(1+\sqrt{5}\right)$ and $\sqrt[3]{2-\sqrt{5}}=\frac{1}{2}\left(1-\sqrt{5}\right)$. But how would you have found these two identities?

[237] There may be a moral here as well.

For three more centuries, the quintic equation $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$ stumped mathematicians. Finally, in 1824, Niels Henrik Abel (based on work by Paolo Ruffini) showed that a general formula for the roots of a degree-5 polynomial (using $+$, $-$, $\cdot$, $/$ and $\sqrt{}$ signs only) does not exist (not even an impractical one like Cardano's). A real understanding of the reasons behind this emerged when Évariste Galois introduced the notion of groups, and what later became known as Galois groups, in 1832. This formed the beginning of Galois theory (for which see the references in Section 9.1).

From a modern viewpoint, the question of finding explicit formulas for roots of polynomials appears arbitrary and inconsequential. After all, why exactly are we allowing $\sqrt{}$ signs in these formulas, if computing $\sqrt[n]{a}$ is already tantamount to finding a root of a polynomial (namely, $x^n - a$) ? Why do some roots count as explicit, but the ones we are looking for don't? In the case of quadratic polynomials, at least the formula ends up quite useful; for higher degrees, this is almost never the case. Expressions involving third (and higher) roots are hard to work with (recall our difficulties recognizing $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$ as 1!), and if one wants numerical results, the standard numerical methods (such as Newton's) are much simpler. Algebraists generally want to compute precisely, but they don't care for the arbitrary limitations of $+$, $-$, $\cdot$, $/$ and $\sqrt{}$ signs; thus, much of the time, they end up formally adjoining their roots (using the $\mathbb{K}[x] / \mathbf{b}$ construction in Theorem 8.1.9) and computing in the resulting rings. Thus, despite giving birth to some of the algebra we know and love, Cardano's formulas eventually became historical footnotes.

9.3. Irreducible polynomials over finite fields

I have told you that there exists a field of any prime-power size; but I only showed this for the sizes p and p^2 (where p is a prime). Let me go one step further and prove this for size p^3 as well, just to illustrate the use of the $\mathbb{K}[x] / \mathbf{b}$ construction from Theorem 8.1.9. More generally, I claim the following:

Lemma 9.3.1. Let $\mathbb{F}$ be a finite field.
(a) There exists an irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 2.
(b) There exists an irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 3.

Proof of Lemma 9.3.1 (sketched). If $n \in \mathbb{N}$, then a polynomial $\mathbf{a} \in \mathbb{F}[x]$ is said to be *monic of degree n* if and only if $\mathbf{a} \in \mathbb{F}[x]_{\leq n}$ and $[x^n]\,\mathbf{a} = 1$. Thus, a polynomial is monic of degree n if and only if it can be written in the form $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0x^0$ for some $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$. In particular, the monic polynomials of degree 1 have the form $x + b$ for $b \in \mathbb{F}$, while the monic polynomials of degree 2 have the form $x^2 + bx + c$ for $b, c \in \mathbb{F}$. It is clear that for each $n \in \mathbb{N}$, we have

$$|\{\text{monic polynomials } \mathbf{a} \in \mathbb{F}[x] \text{ of degree } n\}| = |\mathbb{F}|^n \qquad (333)$$

(because in order to choose a monic polynomial $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 x^0$, we just have to choose the n coefficients $a_0, a_1, \ldots, a_{n-1}$, and we have $|\mathbb{F}|$ options for each of these coefficients).

It is easy to see that if $n \in \mathbb{N}$ and if $\mathbf{a} \in \mathbb{F}[x]$ has degree n, then

$$\text{there exists some } \lambda \in \mathbb{F} \text{ such that } \lambda\mathbf{a} \text{ is monic of degree } n. \qquad (334)$$

(Indeed, it suffices to choose $\lambda = \dfrac{1}{[x^n]\,\mathbf{a}}$; then, $[x^n](\lambda\mathbf{a}) = 1$, and therefore $\lambda\mathbf{a}$ is monic of degree n.)

(a) Assume the contrary. Thus, there exists no irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 2.

As a consequence, I claim the following:

> *Claim 1:* Each monic polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 2 has the form $(x+b)(x+c)$ for some $b, c \in \mathbb{F}$.

[*Proof of Claim 1:* Let $\mathbf{a} \in \mathbb{F}[x]$ be a monic polynomial of degree 2. Then, $[x^2]\,\mathbf{a} = 1$. But we know that $\mathbf{a}$ is not irreducible (since we assumed that there exists no irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 2). In other words, $\mathbf{a}$ can be written in the form $\mathbf{a} = \mathbf{bc}$ for two polynomials $\mathbf{b}$ and $\mathbf{c}$ with $\deg\mathbf{b} > 0$ and $\deg\mathbf{c} > 0$. Consider these $\mathbf{b}$ and $\mathbf{c}$. From $\mathbf{a} = \mathbf{bc}$, we obtain $\deg\mathbf{a} = \deg(\mathbf{bc}) = \deg\mathbf{b} + \deg\mathbf{c}$ and thus $\deg\mathbf{b} + \deg\mathbf{c} = \deg\mathbf{a} = 2$. In view of $\deg\mathbf{b} > 0$ and $\deg\mathbf{c} > 0$, this leads to $\deg\mathbf{b} = 1$ and $\deg\mathbf{c} = 1$. Hence, (334) (applied to 1 and $\mathbf{b}$ instead of n and $\mathbf{a}$) shows that there exists some $\lambda \in \mathbb{F}$ such that $\lambda\mathbf{b}$ is monic of degree 1. Similarly, there exists some $\mu \in \mathbb{F}$ such that $\mu\mathbf{c}$ is monic of degree 1. Consider these λ and μ. Now, $\lambda\mathbf{b} = x + b$ for some $b \in \mathbb{F}$ (since $\lambda\mathbf{b}$ is monic of degree 1), and $\mu\mathbf{c} = x + c$ for some $c \in \mathbb{F}$ (similarly). Consider these b and c. Now,

$$\lambda\mu \underbrace{\mathbf{a}}_{=\mathbf{bc}} = \lambda\mu\mathbf{bc} = \underbrace{(\lambda\mathbf{b})}_{=x+b}\underbrace{(\mu\mathbf{c})}_{=x+c} = (x+b)(x+c).$$

Comparing the coefficients of x^2 on both sides of this equality, we find $\lambda\mu = 1$ (because the coefficient of x^2 in $\lambda\mu\mathbf{a}$ is $\lambda\mu \underbrace{[x^2]\,\mathbf{a}}_{=1} = \lambda\mu$, but the coefficient of x^2 in $(x+b)(x+c)$ is 1). Thus, $\lambda\mu\mathbf{a} = (x+b)(x+c)$ rewrites as $\mathbf{a} = (x+b)(x+c)$. Hence, we have written our polynomial $\mathbf{a}$ in the form $(x+b)(x+c)$ for some $b, c \in \mathbb{F}$. This proves Claim 1.]

Claim 1 shows that the map

$$\mathbb{F} \times \mathbb{F} \to \{\text{monic polynomials } \mathbf{a} \in \mathbb{F}[x] \text{ of degree } 2\},$$
$$(b, c) \mapsto (x+b)(x+c)$$

is surjective. But this is a map between two finite sets of equal sizes (because $|\mathbb{F} \times \mathbb{F}| = |\mathbb{F}|^2$, but (333) (applied to $n = 2$) shows that

$\left|\left\{\text{monic polynomials } \mathbf{a} \in \mathbb{F}[x] \text{ of degree } 2\right\}\right| = |\mathbb{F}|^2$ as well). Thus, the Pigeonhole Principle for Surjections shows that this map is bijective. Thus, in particular, this map is injective. But this is absurd, because it sends the two different pairs $(0,1)$ and $(1,0)$ to one and the same polynomial $(x+0)(x+1) = (x+1)(x+0)$. This contradiction shows that our assumption was wrong. Hence, Lemma 9.3.1 **(a)** is proven.

(b) This is similar to our proof of Lemma 9.3.1 **(a)**, with just one more little twist. Here are the details:

Assume the contrary. Thus, there exists no irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 3. As a consequence, I claim the following:

Claim 2: Each monic polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 3 has the form $(x+b)\left(x^2+cx+d\right)$ for some $b,c,d \in \mathbb{F}$.

[*Proof of Claim 2:* Let $\mathbf{a} \in \mathbb{F}[x]$ be a monic polynomial of degree 3. Then, $\left[x^3\right]\mathbf{a} = 1$. But we know that $\mathbf{a}$ is not irreducible (since we assumed that there exists no irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 3). In other words, $\mathbf{a}$ can be written in the form $\mathbf{a} = \mathbf{bc}$ for two polynomials $\mathbf{b}$ and $\mathbf{c}$ with $\deg \mathbf{b} > 0$ and $\deg \mathbf{c} > 0$. Consider these $\mathbf{b}$ and $\mathbf{c}$. From $\mathbf{a} = \mathbf{bc}$, we obtain $\deg \mathbf{a} = \deg(\mathbf{bc}) = \deg \mathbf{b} + \deg \mathbf{c}$ and thus $\deg \mathbf{b} + \deg \mathbf{c} = \deg \mathbf{a} = 3$. In view of $\deg \mathbf{b} > 0$ and $\deg \mathbf{c} > 0$, this shows that we have **either** ($\deg \mathbf{b} = 1$ and $\deg \mathbf{c} = 2$) **or** ($\deg \mathbf{b} = 2$ and $\deg \mathbf{c} = 1$). We WLOG assume that we are in the first of these two cases (since otherwise, we can simply swap $\mathbf{b}$ with $\mathbf{c}$). Thus, $\deg \mathbf{b} = 1$ and $\deg \mathbf{c} = 2$. Hence, (334) (applied to 1 and $\mathbf{b}$ instead of n and $\mathbf{a}$) shows that there exists some $\lambda \in \mathbb{F}$ such that $\lambda\mathbf{b}$ is monic of degree 1. Similarly, there exists some $\mu \in \mathbb{F}$ such that $\mu\mathbf{c}$ is monic of degree 2. Consider these λ and μ. Now, $\lambda\mathbf{b} = x + b$ for some $b \in \mathbb{F}$ (since $\lambda\mathbf{b}$ is monic of degree 1), and $\mu\mathbf{c} = x^2 + cx + d$ for some $c, d \in \mathbb{F}$ (since $\mu\mathbf{c}$ is monic of degree 2). Consider these b, c, d. Now,

$$\lambda\mu \underbrace{\mathbf{a}}_{=\mathbf{bc}} = \lambda\mu\mathbf{bc} = \underbrace{(\lambda\mathbf{b})}_{=x+b} \underbrace{(\mu\mathbf{c})}_{=x^2+cx+d} = (x+b)\left(x^2+cx+d\right).$$

Comparing the coefficients of x^3 on both sides of this equality, we find $\lambda\mu = 1$ (because the coefficient of x^3 in $\lambda\mu\mathbf{a}$ is $\lambda\mu \underbrace{\left[x^3\right]\mathbf{a}}_{=1} = \lambda\mu$, but the coefficient of x^3 in $(x+b)\left(x^2+cx+d\right)$ is 1). Thus, $\lambda\mu\mathbf{a} = (x+b)\left(x^2+cx+d\right)$ rewrites as $\mathbf{a} = (x+b)\left(x^2+cx+d\right)$. Hence, we have written our polynomial $\mathbf{a}$ in the form $(x+b)\left(x^2+cx+d\right)$ for some $b,c,d \in \mathbb{F}$. This proves Claim 2.]

Claim 2 shows that the map

$$\begin{aligned} \mathbb{F} \times \mathbb{F} \times \mathbb{F} &\to \left\{\text{monic polynomials } \mathbf{a} \in \mathbb{F}[x] \text{ of degree } 3\right\}, \\ (b,c,d) &\mapsto (x+b)\left(x^2+cx+d\right) \end{aligned}$$

is surjective. But this is a map between two finite sets of equal sizes (because $|\mathbb{F} \times \mathbb{F} \times \mathbb{F}| = |\mathbb{F}|^3$, but (333) (applied to $n = 3$) shows that $\left|\left\{\text{monic polynomials } \mathbf{a} \in \mathbb{F}[x] \text{ of degree } 3\right\}\right| = |\mathbb{F}|^3$ as well). Thus, the Pigeonhole Principle for Surjections shows that this map is bijective. Thus, in particular, this map is injective. But this is absurd, because it sends the two different triples $(0,2,1)$ and $(1,1,0)$ to one and the same polynomial $(x+0)\left(x^2+2x+1\right) = (x+1)\left(x^2+1x+0\right)$. This contradiction shows that our assumption was wrong. Hence, Lemma 9.3.1 **(b)** is proven. □

Note that we could not use the same argument to prove the existence of an irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 4. Indeed, if we tried, we would have to deal with the two substantially different possibilities $(\deg \mathbf{b} = 1$ and $\deg \mathbf{c} = 3)$ and $(\deg \mathbf{b} = 2$ and $\deg \mathbf{c} = 2)$, which would prevent us from obtaining a surjective map from $\mathbb{F} \times \mathbb{F} \times \mathbb{F} \times \mathbb{F}$ to $\{$monic polynomials $\mathbf{a} \in \mathbb{F}[x]$ of degree $4\}$.

Corollary 9.3.2. Let $\mathbb{F}$ be a finite field, and let $q = |\mathbb{F}|$. Then, there exist finite fields of sizes q^2 and q^3.

Proof of Corollary 9.3.2 (sketched). Lemma 9.3.1 **(a)** shows that there exists an irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 2. Consider this $\mathbf{a}$. Then, Theorem 8.1.17 shows that the ring $\mathbb{F}[x]/\mathbf{a}$ is a field. Moreover, $\mathbf{a}$ is a monic polynomial of degree 2; thus, $\mathbf{a} \in \mathbb{F}[x]_{\leq 2}$, and the coefficient $[x^2]\,\mathbf{a} = 1$ is invertible. Hence, Theorem 8.1.9 **(a)** (applied to $\mathbb{K} = \mathbb{F}$, $m = 2$ and $\mathbf{b} = \mathbf{a}$) shows that each element of $\mathbb{F}[x]/\mathbf{a}$ can be uniquely written in the form

$$\lambda_0 \left[x^0\right]_{\mathbf{a}} + \lambda_1 \left[x^1\right]_{\mathbf{a}} \qquad \text{with } \lambda_0, \lambda_1 \in \mathbb{F}.$$

Therefore, the number of elements of $\mathbb{F}[x]/\mathbf{a}$ is $|\mathbb{F}|^2$ (since there are $|\mathbb{F}|$ many choices for λ_0, and $|\mathbb{F}|$ many choices for λ_1). In other words, the field $\mathbb{F}[x]/\mathbf{a}$ has size $|\mathbb{F}|^2$. In other words, the field $\mathbb{F}[x]/\mathbf{a}$ has size q^2 (since $|\mathbb{F}| = q$). Thus, there exists a finite field of size q^2.

A similar argument (using Lemma 9.3.1 **(b)** instead of Lemma 9.3.1 **(a)**) shows that there exists a finite field of size q^3. Thus, Corollary 9.3.2 is proven. □

Now, if p is a prime, then Corollary 9.3.2 (applied to $\mathbb{F} = \mathbb{Z}/p$ and $q = p$) shows that there exist finite fields of sizes p^2 and p^3. Moreover, by applying Corollary 9.3.2 twice, we can see that there exists a finite field of size $\left(p^2\right)^2 = p^4$. However, this method fails at proving that there exists a finite field of size p^5.

For a proper proof of the existence of a finite field of size p^n (for any prime p and integer $n \geq 1$), see [LidNie97, Theorem 2.5], [Knapp16a, Theorem 9.14], [Loehr11, Exercise 12.126], [ConradF, Theorem 2.2], [Hunger14, Corollary 11.26], [Hunger03, Chapter V, Proposition 5.6], [Stewar15, Theorem 19.3], [Walker87, Theorem 6.2.11] or [Escofi01, 14.5.1] or [Grinbe19b]. However, each of these proofs, except for the one in [Grinbe19b], uses at least something we have not seen so far. (The proof in [Grinbe19b], on the other hand, is fairly long.)

10. Solutions to the exercises

10.1. Solution to Exercise 2.2.1

Solution to Exercise 2.2.1. The definition of $|a|$ shows that $|a|$ equals either a or $-a$. In other words, $|a|$ equals either $1a$ or $(-1)\,a$. In other words, $|a| = qa$ for some $q \in \{1, -1\}$.

Consider this q. Clearly, q is an integer. Now, from $|a| = qa = aq$, we conclude that $a \mid |a|$ (since q is an integer). This solves Exercise 2.2.1 **(a)**.

(b) From $q \in \{1, -1\}$, we obtain $q^2 \in \left\{1^2, (-1)^2\right\} = \{1, 1\} = \{1\}$, so that $q^2 = 1$. Now, multiplying the equality $|a| = qa$ by q, we obtain $q\,|a| = \underbrace{qq}_{=q^2=1} a = a$. Hence, $a = q\,|a| = |a| \cdot q$. Thus, $|a| \mid a$ (since q is an integer). This solves Exercise 2.2.1 **(b)**. □

10.2. Solution to Exercise 2.2.2

Solution to Exercise 2.2.2. We are in one of the following two cases:

Case 1: We have $b \neq 0$.

Case 2: We have $b = 0$.

Let us first consider Case 1. In this case, we have $b \neq 0$. Thus, Proposition 2.2.3 **(b)** yields $|a| \leq |b|$ (since $a \mid b$).

We have $a \mid b$. In other words, there exists an integer c such that $b = ac$. Consider this c. If we had $a = 0$, then we would have $b = \underbrace{a}_{=0} c = 0$, which would contradict $b \neq 0$. Thus, we cannot have $a = 0$. Hence, $a \neq 0$. Thus, Proposition 2.2.3 **(b)** (applied to b and a instead of a and b) yields $|b| \leq |a|$ (since $b \mid a$). Combining this with $|a| \leq |b|$, we obtain $|a| = |b|$. Thus, Exercise 2.2.2 is solved in Case 1.

Let us now consider Case 2. In this case, we have $b = 0$. But we have $b \mid a$. In other words, there exists an integer c such that $a = bc$. Consider this c. Hence, $a = \underbrace{b}_{=0} c = 0c = 0 = b$ (since $b = 0$). Thus, $|a| = |b|$. Hence, Exercise 2.2.2 is solved in Case 2.

Now, we have solved Exercise 2.2.2 in both Cases 1 and 2. Hence, Exercise 2.2.2 always holds. □

10.3. Solution to Exercise 2.2.3

Solution to Exercise 2.2.3. $\Longrightarrow$: Assume that $a \mid b$ holds. We must prove that $ac \mid bc$.

It is easy to do this straight from the definition of divisibility, but here is a shorter argument: Proposition 2.2.4 **(a)** (applied to c instead of a) yields $c \mid c$. Also, $a \mid b$. Hence, Proposition 2.2.4 **(c)** (applied to $a_1 = a$, $b_1 = b$, $a_2 = c$ and $b_2 = c$) yields $ac \mid bc$. This proves the "$\Longrightarrow$" direction of Exercise 2.2.3.

$\Longleftarrow$: Assume that $ac \mid bc$ holds. We must prove that $a \mid b$.

We have $ac \mid bc$. In other words, there exists an integer d such that $bc = (ac)\,d$ (by Definition 2.2.1). Consider this d. We have $bc = (ac)\,d = adc$. We can divide both sides of this equality by c (since $c \neq 0$), and thus obtain $b = ad$. Thus, there exists an integer e such that $b = ae$ (namely, $e = d$). In other words, $a \mid b$ (by Definition 2.2.1). This proves the "$\Longleftarrow$" direction of Exercise 2.2.3. □

10.4. Solution to Exercise 2.2.4

Solution to Exercise 2.2.4. We have $b - a \geq 0$ (since $a \leq b$), thus $b - a \in \mathbb{N}$. Hence, n^{b-a} is a well-defined integer. Now, $n^b = n^a n^{b-a}$ (since $n^a n^{b-a} = n^{a+(b-a)} = n^b$). Hence, there exists an integer c such that $n^b = n^a c$ (namely, $c = n^{b-a}$). In other words, $n^a \mid n^b$ (by the definition of divisibility). This solves Exercise 2.2.4. □

10.5. Solution to Exercise 2.2.5

First solution to Exercise 2.2.5. Assume the contrary. Thus, $g \neq 1$. But Proposition 2.2.3 **(b)** (applied to g and 1 instead of a and b) yields $|g| \leq |1|$ (since $g \mid 1$ and $1 \neq 0$). But g is nonnegative; hence, $|g| = g$, so that $g = |g| \leq |1| = 1$. Combining this with $g \neq 1$, we obtain $g < 1$. Hence, $g = 0$ (since g is a nonnegative integer).

But $g \mid 1$. In other words, there exists an integer c such that $1 = gc$ (by Definition 2.2.1). Consider this c. Now, $1 = \underbrace{g}_{=0} c = 0c = 0$. This contradicts $1 \neq 0$. This contradiction shows that our assumption was wrong. Hence, Exercise 2.2.5 is solved. □

Second solution to Exercise 2.2.5. We have $g = 1g$. Hence, there exists an integer c such that $g = 1c$ (namely, $c = g$). In other words, $1 \mid g$ (by the definition of divisibility). But we also have $g \mid 1$ (by assumption). Hence, Exercise 2.2.2 (applied to $a = g$ and $b = 1$) yields $|g| = |1| = 1$. But g is nonnegative; thus, $|g| = g$. Hence, $g = |g| = 1$. Hence, Exercise 2.2.5 is solved. □

10.6. Solution to Exercise 2.2.6

Solution to Exercise 2.2.6. We have $a \mid b$. In other words, there exists an integer d such that $b = ad$ (by Definition 2.2.1). Consider this d. Clearly, d^k is an integer (since d is an integer and $k \in \mathbb{N}$). From $b = ad$, we obtain $b^k = (ad)^k = a^k d^k$. Hence, there exists an integer c such that $b^k = a^k c$ (namely, $c = d^k$). In other words, $a^k \mid b^k$ (by Definition 2.2.1). This solves Exercise 2.2.6. □

10.7. Solution to Exercise 2.3.1

Solution to Exercise 2.3.1. According to Definition 2.3.1, we have $a + b \equiv a - b \mod 2$ if and only if $2 \mid (a + b) - (a - b)$. Thus, it remains to prove that $2 \mid (a + b) - (a - b)$. But this follows immediately from $(a + b) - (a - b) = 2b$. Thus Exercise 2.3.1 is solved. □

10.8. Solution to Exercise 2.3.2

Solution to Exercise 2.3.2. There are many such examples. Here is one:

$$n = 8, \qquad a_1 = 10, \qquad a_2 = 2, \qquad b_1 = 10, \qquad b_2 = 10.$$

These satisfy $a_1 \equiv b_1 \mod n$ and $a_2 \equiv b_2 \mod n$ but neither $a_1 / a_2 \equiv b_1 / b_2 \mod n$ nor $a_1^{a_2} \equiv b_1^{b_2} \mod n$.

It is much easier to find examples which fail only one of the two congruences $a_1 / a_2 \equiv b_1 / b_2 \mod n$ and $a_1^{a_2} \equiv b_1^{b_2} \mod n$. □

10.9. Solution to Exercise 2.3.3

Solution to Exercise 2.3.3. We have $a \equiv b \mod n$. In other words, $n \mid a - b$ (by the definition of congruence). Note that all of a/d, b/d and n/d are integers (since d divides each of a, b, n). Hence, $(a-b)/d = a/d - b/d$ is an integer as well. Hence, Exercise 2.2.3 (applied to n/d, $(a-b)/d$ and d instead of a, b and c) shows that $n/d \mid (a-b)/d$ holds if and only if $(n/d)\,d \mid ((a-b)/d)\,d$. Since $(n/d)\,d \mid ((a-b)/d)\,d$ does hold (indeed, this is just a complicated way to say $n \mid a - b$), we thus conclude that $n/d \mid (a-b)/d$ holds. In other words, $n/d \mid a/d - b/d$ (since $(a-b)/d = a/d - b/d$). In other words, $a/d \equiv b/d \mod n/d$ (by the definition of congruence). This solves Exercise 2.3.3. □

10.10. Solution to Exercise 2.3.4

First solution to Exercise 2.3.4. We want to prove that

$$a^k \equiv b^k \mod n \qquad \text{for each } k \in \mathbb{N}. \tag{335}$$

We shall prove this by induction on k:

Induction base: Proposition 2.3.4 **(a)** yields $1 \equiv 1 \mod n$. In view of $a^0 = 1$ and $b^0 = 1$, this rewrites as $a^0 \equiv b^0 \mod n$. In other words, (335) holds for $k = 0$. This completes the induction base.

Induction step: Let $\ell \in \mathbb{N}$. Assume that (335) holds for $k = \ell$. We must prove that (335) holds for $k = \ell + 1$.

We have assumed that (335) holds for $k = \ell$. In other words, we have $a^\ell \equiv b^\ell \mod n$. Also, recall that $a \equiv b \mod n$. Hence, (6) (applied to $c = a^\ell$ and $d = b^\ell$) yields $aa^\ell \equiv bb^\ell \mod n$. In other words, $a^{\ell+1} \equiv b^{\ell+1} \mod n$ (since $aa^\ell = a^{\ell+1}$ and $bb^\ell = b^{\ell+1}$). In other words, (335) holds for $k = \ell + 1$. This completes the induction step. Thus, (335) is proven by induction. Therefore, Exercise 2.3.4 is solved. □

Second solution to Exercise 2.3.4. Recall that

$$(a-b)\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}\right) = a^k - b^k \tag{336}$$

for every $k \in \mathbb{N}$. (This is a well-known identity, and it appears (with k renamed as n) as the first half of Exercise 1 on homework set #0.)

Now, let $k \in \mathbb{N}$. We have assumed that $a \equiv b \mod n$. In other words, $n \mid a - b$. In other words, there exists an integer c such that $a - b = nc$. Consider this c. Now, (336) yields

$$\begin{aligned} a^k - b^k &= \underbrace{(a-b)}_{=nc}\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}\right) \\ &= nc\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}\right). \end{aligned}$$

The right hand side of this equality is clearly divisible by n. Hence, so is the left hand side. In other words, $n \mid a^k - b^k$. In other words, $a^k \equiv b^k \mod n$. Hence, Exercise 2.3.4 is solved again. □

10.11. Solution to Exercise 2.3.5

Solution to Exercise 2.3.5. **(a)** We shall solve Exercise 2.3.5 **(a)** by induction on $|S|$:

Induction base: Exercise 2.3.5 **(a)** holds whenever $|S| = 0$ [238]. This completes the induction base.

Induction step: Fix $k \in \mathbb{N}$. Assume that Exercise 2.3.5 **(a)** holds whenever $|S| = k$. We must prove that Exercise 2.3.5 **(a)** holds whenever $|S| = k + 1$.

We have assumed that Exercise 2.3.5 **(a)** holds whenever $|S| = k$. In other words, the following statement is true:

> *Statement 1:* Let n, S, a_s and b_s be as in Exercise 2.3.5. Assume that $|S| = k$. Then, $\sum\limits_{s \in S} a_s \equiv \sum\limits_{s \in S} b_s \mod n$.

Now, we must prove that Exercise 2.3.5 **(a)** holds whenever $|S| = k + 1$. In other words, we must prove the following statement:

> *Statement 2:* Let n, S, a_s and b_s be as in Exercise 2.3.5. Assume that $|S| = k + 1$. Then, $\sum\limits_{s \in S} a_s \equiv \sum\limits_{s \in S} b_s \mod n$.

[*Proof of Statement 2:* We have $|S| = k + 1 > k \geq 0$; thus, the set S is nonempty. Hence, there exists some $t \in S$. Pick such a t. Thus, $|S \setminus \{t\}| = |S| - 1 = k$ (since $|S| = k + 1$). Moreover, from (7), we immediately obtain that

$$a_s \equiv b_s \mod n \qquad \text{for each } s \in S \setminus \{t\}$$

(since each $s \in S \setminus \{t\}$ belongs to S). Hence, we can apply Statement 1 to $S \setminus \{t\}$ instead of S. We thus obtain

$$\sum_{s \in S \setminus \{t\}} a_s \equiv \sum_{s \in S \setminus \{t\}} b_s \mod n.$$

Also, we have

$$a_t \equiv b_t \mod n$$

(by (7), applied to $s = t$). Adding these two congruences together, we obtain

$$\sum_{s \in S \setminus \{t\}} a_s + a_t \equiv \sum_{s \in S \setminus \{t\}} b_s + b_t \mod n.$$

In view of

$$\sum_{s \in S} a_s = \sum_{s \in S \setminus \{t\}} a_s + a_t \qquad \left(\begin{array}{c}\text{here, we have split off the addend} \\ \text{for } s = t \text{ from the sum}\end{array}\right)$$

[238] *Proof.* Let n, S, a_s and b_s be as in Exercise 2.3.5, and assume that $|S| = 0$. Then, the set S is empty (since $|S| = 0$), and thus we have $\sum\limits_{s \in S} a_s = (\text{empty sum}) = 0$. Similarly, $\sum\limits_{s \in S} b_s = 0$. Now, Proposition 2.3.4 **(a)** yields $0 \equiv 0 \mod n$. In view of $\sum\limits_{s \in S} a_s = 0$ and $\sum\limits_{s \in S} b_s = 0$, this rewrites as $\sum\limits_{s \in S} a_s \equiv \sum\limits_{s \in S} b_s \mod n$. Thus, Exercise 2.3.5 **(a)** holds in our case.

So we have shown that Exercise 2.3.5 **(a)** holds whenever $|S| = 0$.

and

$$\sum_{s\in S} b_s = \sum_{s\in S\setminus\{t\}} b_s + b_t \qquad \left(\begin{array}{c}\text{here, we have split off the addend}\\ \text{for } s=t \text{ from the sum}\end{array}\right),$$

this can be rewritten as

$$\sum_{s\in S} a_s \equiv \sum_{s\in S} b_s \operatorname{mod} n.$$

This proves Statement 2.]

We have now proven Statement 2; this means that Exercise 2.3.5 **(a)** holds whenever $|S| = k+1$. This completes the induction step; thus, Exercise 2.3.5 **(a)** is solved.

(b) The solution to Exercise 2.3.5 **(b)** is analogous to the one we gave above for Exercise 2.3.5 **(a)**; the main difference is that we have to replace sums by products (and 0 by 1). □

10.12. Solution to Exercise 2.3.6

Solution to Exercise 2.3.6. No, it is not true. For example, $a_1 = 1$, $a_2 = 1$, $b_1 = 1$, $b_2 = 0$, $n_1 = 0$ and $n_2 = 1$ yield a counterexample. □

10.13. Solution to Exercise 2.3.7

Solution to Exercise 2.3.7. If $a \equiv b \operatorname{mod} n$, then $b \equiv a \operatorname{mod} n$ (by Proposition 2.3.4 **(c)**). In other words, the implication $(a \equiv b \operatorname{mod} n) \Longrightarrow (b \equiv a \operatorname{mod} n)$ holds. The same argument (but with the roles of a and b swapped) shows that the implication $(b \equiv a \operatorname{mod} n) \Longrightarrow (a \equiv b \operatorname{mod} n)$ holds. Combining these two implications, we obtain the logical equivalence $(a \equiv b \operatorname{mod} n) \Longleftrightarrow (b \equiv a \operatorname{mod} n)$. Thus, we have the following chain of logical equivalences:

$$\begin{aligned}
(a \equiv b \operatorname{mod} n) &\Longleftrightarrow (b \equiv a \operatorname{mod} n)\\
&\Longleftrightarrow (n \mid b-a) \qquad \text{(by the definition of congruence)}\\
&\Longleftrightarrow (\text{there exists an integer } d \text{ such that } b-a=nd)\\
&\qquad \text{(by the definition of divisibility)}\\
&\Longleftrightarrow (\text{there exists an integer } d \text{ such that } b=a+nd)
\end{aligned}$$

(since the equation $b-a=nd$ for an integer d is equivalent to $b=a+nd$). In other words, $a \equiv b \operatorname{mod} n$ if and only if there exists some $d \in \mathbb{Z}$ such that $b = a+nd$. This solves Exercise 2.3.7. □

10.14. Solution to Exercise 2.3.8

Solution to Exercise 2.3.8. We have $a-b \equiv c \operatorname{mod} n$ if and only if $n \mid (a-b)-c$ (by the definition of congruence). Thus, we have the logical equivalence

$$(a-b \equiv c \operatorname{mod} n) \Longleftrightarrow (n \mid (a-b)-c). \tag{337}$$

On the other hand, we have $a \equiv b+c \operatorname{mod} n$ if and only if $n \mid a-(b+c)$ (by the definition of congruence). Thus, we have the logical equivalence

$$(a \equiv b+c \operatorname{mod} n) \Longleftrightarrow (n \mid a-(b+c)). \tag{338}$$

Now, we have the following chain of logical equivalences:

$$\begin{aligned}(a-b\equiv c\operatorname{mod}n) &\iff \left(n\mid \underbrace{(a-b)-c}_{=a-(b+c)}\right) \qquad \text{(by (337))}\\ &\iff (n\mid a-(b+c)) \iff (a\equiv b+c\operatorname{mod}n) \qquad \text{(by (338))}.\end{aligned}$$

In other words, we have $a-b\equiv c\operatorname{mod}n$ if and only if $a\equiv b+c\operatorname{mod}n$. This solves Exercise 2.3.8. □

10.15. Solution to Exercise 2.3.9

Solution to Exercise 2.3.9. Let us first prove the logical implication

$$(a\equiv b\operatorname{mod}n) \implies (a\equiv b\operatorname{mod}-n). \tag{339}$$

[*Proof of (339):* Assume that $a\equiv b\operatorname{mod}n$. We must show that $a\equiv b\operatorname{mod}-n$.

We have $n=(-n)(-1)$. Since -1 is an integer, this shows that $-n\mid n$ (by the definition of divisibility). Thus, Proposition 2.3.4 **(e)** (applied to $m=-n$) yields $a\equiv b\operatorname{mod}-n$. This proves (339).]

So we have proven the logical implication (339). The same reasoning (applied to $-n$ instead of n) yields the logical implication

$$(a\equiv b\operatorname{mod}-n) \implies (a\equiv b\operatorname{mod}-(-n)).$$

Since $-(-n)=n$, this rewrites as follows:

$$(a\equiv b\operatorname{mod}-n) \implies (a\equiv b\operatorname{mod}n).$$

Combining this implication with the implication (339), we obtain the equivalence

$$(a\equiv b\operatorname{mod}n) \iff (a\equiv b\operatorname{mod}-n).$$

This solves Exercise 2.3.9. □

10.16. Solution to Exercise 2.5.1

Solution to Exercise 2.5.1. We have $3^{2n+1}=\left(\underbrace{3^2}_{=9\equiv 2\operatorname{mod}7}\right)^n\cdot 3\equiv 2^n\cdot 3\operatorname{mod}7$. (This follows from the PSC, in its extended form that allows k-th powers in the expression A. Alternatively, you can argue by hand as follows: We have $3^2=9\equiv 2\operatorname{mod}7$. Thus, Exercise 2.3.4 (applied to 7, 3^2, 2 and n instead of n, a, b and k) yields $(3^2)^n\equiv 2^n\operatorname{mod}7$. Multiplying this congruence by the obvious congruence $3\equiv 3\operatorname{mod}7$, we obtain $(3^2)^n\cdot 3\equiv 2^n\cdot 3\operatorname{mod}7$. Thus, $3^{2n+1}=(3^2)^n\cdot 3\equiv 2^n\cdot 3\operatorname{mod}7$.)

Hence, again using the PSC, we obtain

$$\underbrace{3^{2n+1}}_{\equiv 2^n\cdot 3\operatorname{mod}7}+\underbrace{2^{n+2}}_{=2^n\cdot 2^2=2^n\cdot 4}\equiv 2^n\cdot 3+2^n\cdot 4=2^n\cdot\underbrace{(3+4)}_{=7}=2^n\cdot 7\equiv 0\operatorname{mod}7$$

(since $2^n \cdot 7$ is clearly divisible by 7). In other words, $7 \mid 3^{2n+1} + 2^{n+2}$. This solves Exercise 2.5.1.

[*Remark:* Here is a sketch of a different solution: If we set $a_n = 3^{2n+1} + 2^{n+2}$ for each $n \in \mathbb{N}$, then we must prove that $7 \mid a_n$ for all $n \in \mathbb{N}$. But a straightforward computation reveals that

$$a_n = 11a_{n-1} - 18a_{n-2} \qquad \text{for each } n \geq 2. \tag{340}$$

Thus, once we check that $7 \mid a_0$ and $7 \mid a_1$, we can use a straightforward strong induction on n to see that $7 \mid a_n$ for all $n \in \mathbb{N}$, which is exactly the claim of Exercise 2.5.1. Of course, **finding** the relation (340) was the main trick in this solution; it becomes somewhat natural once you know the theory of linear recurrences (such as the Fibonacci sequence).] □

10.17. Solution to Exercise 2.6.1

Solution to Exercise 2.6.1. $\Longrightarrow$: Assume that $u \equiv v \mod n$. We must prove that $u\%n = v\%n$.

Corollary 2.6.9 **(a)** yields that $u\%n \in \{0, 1, \ldots, n-1\}$ and $u\%n \equiv u \mod n$. Hence, $u\%n \equiv u \equiv v \mod n$.

But Corollary 2.6.9 **(c)** (applied to v instead of u) yields that if $c \in \{0, 1, \ldots, n-1\}$ is such that $c \equiv v \mod n$, then $c = v\%n$. Applying this to $c = u\%n$, we obtain $u\%n = v\%n$ (since $u\%n \in \{0, 1, \ldots, n-1\}$ and $u\%n \equiv v \mod n$). This proves the "$\Longrightarrow$" direction of Exercise 2.6.1.

$\Longleftarrow$: Assume that $u\%n = v\%n$. We must prove that $u \equiv v \mod n$.

Corollary 2.6.9 **(a)** yields that $u\%n \in \{0, 1, \ldots, n-1\}$ and $u\%n \equiv u \mod n$. Corollary 2.6.9 **(a)** (applied to v instead of u) yields that $v\%n \in \{0, 1, \ldots, n-1\}$ and $v\%n \equiv v \mod n$.

From $u\%n \equiv u \mod n$, we obtain $u \equiv u\%n = v\%n \equiv v \mod n$. Thus, we have proven $u \equiv v \mod n$. This proves the "$\Longleftarrow$" direction of Exercise 2.6.1. □

10.18. Solution to Exercise 2.6.2

Solution to Exercise 2.6.2. **(a)** Theorem 2.6.1 shows that there exists a unique pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$. Consider this pair (q, r), and denote it by (s, t). Thus, $(s, t) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ is a pair satisfying $u = sn + t$. From $(s, t) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$, we obtain $s \in \mathbb{Z}$ and $t \in \{0, 1, \ldots, n-1\} \subseteq \mathbb{Z}$.

We are in one of the following two cases:

Case 1: We have $t \leq n/2$.

Case 2: We have $t > n/2$.

Let us first consider Case 1. In this case, we have $t \leq n/2$. But t is nonnegative (since $t \in \{0, 1, \ldots, n-1\}$); thus, $|t| = t \leq n/2$. So we have $(s, t) \in \mathbb{Z} \times \mathbb{Z}$ (since $s \in \mathbb{Z}$ and $t \in \mathbb{Z}$) and $u = sn + t$ and $|t| \leq n/2$. Hence, there exists a pair $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ such that $u = qn + r$ and $|r| \leq n/2$ (namely, $(q, r) = (s, t)$). Thus, Exercise 2.6.2 **(a)** is solved in Case 1.

Let us now consider Case 2. In this case, we have $t > n/2$. But $t \in \{0, 1, \ldots, n-1\}$, thus $t \leq n - 1 \leq n$. Hence, $t - n \leq 0$. Hence, $|t - n| = -(t - n) = n - \underbrace{t}_{> n/2} < n - n/2 = n/2$. Therefore, $|t - n| \leq n/2$. Furthermore, $t - n \in \mathbb{Z}$ (since $t \in \mathbb{Z}$ and $n \in \mathbb{Z}$) and $s + 1 \in \mathbb{Z}$ (since $s \in \mathbb{Z}$). So we have $(s + 1, t - n) \in \mathbb{Z} \times \mathbb{Z}$ (since $s + 1 \in \mathbb{Z}$ and $t - n \in \mathbb{Z}$) and $u = (s + 1) n + (t - n)$ (since $(s + 1) n + (t - n) = sn + t = u$) and $|t - n| \leq n/2$. Hence, there exists a pair $(q,r) \in \mathbb{Z} \times \mathbb{Z}$ such that $u = qn + r$ and $|r| \leq n/2$ (namely, $(q,r) = (s+1, t-n)$). Thus, Exercise 2.6.2 **(a)** is solved in Case 2.

We have now solved Exercise 2.6.2 **(a)** in each of the two Cases 1 and 2. Since these two Cases cover all possibilities, we thus conclude that Exercise 2.6.2 **(a)** always holds.

(b) For example, if $n = 2$ and $u = 5$, then both $(2,1)$ and $(3,-1)$ are pairs $(q,r) \in \mathbb{Z} \times \mathbb{Z}$ such that $u = qn + r$ and $|r| \leq n/2$.

More generally: If $n = 2k$ for some positive integer k, and if $u \equiv k \mod n$, then both $((u-k)/n, k)$ and $((u+k)/n, -k)$ are pairs $(q,r) \in \mathbb{Z} \times \mathbb{Z}$ such that $u = qn + r$ and $|r| \leq n/2$.

[It is not hard to see that these are the **only** cases in which the pair (q,r) from Exercise 2.6.2 **(a)** is not unique.] □

10.19. Solution to Exercise 2.6.3

Solution to Exercise 2.6.3. **(a)** Corollary 2.6.9 **(a)** yields that $u\%n \in \{0,1,\ldots,n-1\}$ and $u\%n \equiv u \mod n$. From $u\%n \in \{0,1,\ldots,n-1\}$, we conclude that $u\%n$ is an integer satisfying $0 \leq u\%n \leq n-1$.

Corollary 2.6.9 **(a)** (applied to v instead of u) yields that $v\%n \in \{0,1,\ldots,n-1\}$ and $v\%n \equiv v \mod n$. From $v\%n \in \{0,1,\ldots,n-1\}$, we conclude that $v\%n$ is an integer satisfying $0 \leq v\%n \leq n-1$.

Corollary 2.6.9 **(a)** (applied to $u+v$ instead of u) yields that $(u+v)\%n \in \{0,1,\ldots,n-1\}$ and $(u+v)\%n \equiv u+v \mod n$. From $(u+v)\%n \in \{0,1,\ldots,n-1\}$, we conclude that $(u+v)\%n$ is an integer satisfying $0 \leq (u+v)\%n \leq n-1$.

Adding the congruences $u\%n \equiv u \mod n$ and $v\%n \equiv v \mod n$ together, we obtain $u\%n + v\%n \equiv u+v \mod n$. Subtracting the congruence $(u+v)\%n \equiv u+v \mod n$ from this congruence, we obtain $u\%n + v\%n - (u+v)\%n \equiv (u+v) - (u+v) = 0 \mod n$. By Proposition 2.3.3 (applied to $a = u\%n + v\%n - (u+v)\%n$), this entails $n \mid u\%n + v\%n - (u+v)\%n$. In other words, there exists an integer c such that $u\%n + v\%n - (u+v)\%n = nc$. Consider this c.

Hence,

$$nc = \underbrace{u\%n}_{\leq n-1 < n} + \underbrace{v\%n}_{\leq n-1 < n} - \underbrace{(u+v)\%n}_{\geq 0} < n + n - 0 = 2n = n \cdot 2.$$

We can divide this inequality by n (since n is positive). We thus obtain $c < 2$. Hence, $c \leq 1$ (since c is an integer).

On the other hand,

$$nc = \underbrace{u\%n}_{\geq 0} + \underbrace{v\%n}_{\geq 0} - \underbrace{(u+v)\%n}_{\leq n-1 < n} > 0 + 0 - n = -n = n \cdot (-1).$$

We can divide this inequality by n (since n is positive). We thus obtain $c > -1$. Hence, $c \geq 0$ (since c is an integer).

Combining $c \geq 0$ with $c \leq 1$, we obtain $c \in \{0,1\}$ (since c is an integer). In other words, we have $c = 0$ or $c = 1$. Hence, we have $nc = n \cdot 0 = 0$ or $nc = n \cdot 1 = n$. In other words, $nc \in \{0,n\}$. Now, recall that $u\%n + v\%n - (u+v)\%n = nc \in \{0,n\}$. This solves Exercise 2.6.3 **(a)**.

(b) Exercise 2.6.3 **(a)** yields $u\%n + v\%n - (u+v)\%n \in \{0,n\}$.

The integer n is positive and thus nonzero. Corollary 2.6.9 **(d)** yields $u = (u//n)\, n + (u\%n)$. Solving this equation for $u//n$, we find

$$u//n = \frac{u - u\%n}{n} \tag{341}$$

(since n is nonzero). The same argument (applied to v instead of u) yields

$$v//n = \frac{v - v\%n}{n}. \tag{342}$$

Finally, the same argument that we used to prove (341) can be applied to $u+v$ instead of u, and thus we obtain

$$(u+v)\,//n = \frac{(u+v) - (u+v)\,\%n}{n}. \tag{343}$$

Now,

$$\begin{aligned}
&\underbrace{(u+v)\,//n}_{\substack{=\dfrac{(u+v)-(u+v)\,\%n}{n} \\ \text{(by (343))}}} - \underbrace{u//n}_{\substack{=\dfrac{u-u\%n}{n} \\ \text{(by (341))}}} - \underbrace{v//n}_{\substack{=\dfrac{v-v\%n}{n} \\ \text{(by (342))}}} \\
&= \frac{(u+v)-(u+v)\,\%n}{n} - \frac{u-u\%n}{n} - \frac{v-v\%n}{n} \\
&= \frac{1}{n} \underbrace{\left(\left((u+v)-(u+v)\,\%n\right) - (u-u\%n) - (v-v\%n)\right)}_{=u\%n+v\%n-(u+v)\%n} \\
&= \frac{1}{n}\left(u\%n + v\%n - (u+v)\,\%n\right) \\
&\in \left\{\frac{1}{n}0, \frac{1}{n}n\right\} \qquad \left(\text{since } u\%n + v\%n - (u+v)\,\%n \in \{0, n\}\right) \\
&= \{0, 1\} \qquad \left(\text{since } \frac{1}{n}0 = 0 \text{ and } \frac{1}{n}n = 1\right).
\end{aligned}$$

This solves Exercise 2.6.3 **(b)**. □

10.20. Solution to Exercise 2.6.4

Solution to Exercise 2.6.4. **(a)** The map

$$\begin{aligned}
\mathbb{Z} \times \{0, 1, \ldots, n-1\} &\to \mathbb{Z}, \\
(q, r) &\mapsto qn + r
\end{aligned}$$

is clearly well-defined. Let us denote this map by A. Then, in order to solve Exercise 2.6.4 **(a)**, we must prove that this map A is a bijection.

We shall achieve this by showing that A is injective and surjective:

[*Proof of the injectivity of A:* Let x and y be two elements of $\mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $A(x) = A(y)$. We shall show that $x = y$.

Define a $u \in \mathbb{Z}$ by $u = A(x)$. Then, $u = A(x) = A(y)$.

Now, x is an element of $\mathbb{Z} \times \{0, 1, \ldots, n-1\}$. In other words, x is a pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$. Moreover, if we write x in the form $x = (q, r)$ for some $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$, then

$$u = A\left(\underbrace{x}_{=(q,r)}\right) = A((q,r)) = qn + r \qquad \text{(by the definition of } A\text{)}.$$

Hence, x is a pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$. Similarly, y is a pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$ (since $u = A(y)$).

But Lemma 2.6.5 shows that there exists **at most one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$. Hence, any two such pairs (q, r) must be equal. Thus, x and y must be equal (since x and y are two pairs $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$). In other words, $x = y$.

Now, forget that we fixed x and y. We thus have shown that if x and y are two elements of $\mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $A(x) = A(y)$, then $x = y$. In other words, the map A is injective.]

[*Proof of the surjectivity of A:* Let $u \in \mathbb{Z}$. We shall find an $x \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = A(x)$.

Indeed, Lemma 2.6.4 shows that there exists **at least one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$. Consider this (q, r). Now, the definition of A yields $A((q, r)) = qn + r = u$. Hence, $u = A((q, r))$. Thus, there exists an $x \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = A(x)$ (namely, $x = (q, r)$).

Now, forget that we fixed u. We thus have shown that for each $u \in \mathbb{Z}$, there exists an $x \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = A(x)$. In other words, the map A is surjective.]

We have now shown that the map A is injective and surjective. Hence, A is bijective. In other words, A is a bijection. As we explained above, this solves Exercise 2.6.4 **(a)**.

(b) The map

$$\begin{aligned} \mathbb{N} \times \{0, 1, \ldots, n-1\} &\to \mathbb{N}, \\ (q, r) &\mapsto qn + r \end{aligned}$$

is clearly well-defined[239]. Let us denote this map by B. Then, in order to solve Exercise 2.6.4 **(b)**, we must prove that this map B is a bijection.

We shall achieve this by showing that B is injective and surjective:

[*Proof of the injectivity of B:* In our solution to Exercise 2.6.4 **(a)**, we have defined a map A and proven that this map A is injective. The very same argument (with A replaced by B, and $\mathbb{Z}$ replaced by $\mathbb{N}$) shows that the map B is injective.]

[*Proof of the surjectivity of B:* Let $u \in \mathbb{N}$. We shall find an $x \in \mathbb{N} \times \{0, 1, \ldots, n-1\}$ such that $u = B(x)$.

Indeed, Lemma 2.6.4 shows that there exists **at least one** pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$. Consider this (q, r). From $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$, we obtain $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. From $r \in \{0, 1, \ldots, n-1\}$, we obtain $r \leq n - 1 < n$, so that $u = qn + \underbrace{r}_{<n} < qn + n = (q+1)n$. Thus, $(q+1)n > u \geq 0$ (since $u \in \mathbb{N}$). But if we had $q + 1 \leq 0$, then we would have $\underbrace{(q+1)}_{\leq 0} n \leq 0$ (since n is positive), which would contradict

[239] since $qn + r \in \mathbb{N}$ for each $(q, r) \in \mathbb{N} \times \{0, 1, \ldots, n-1\}$ (because n is positive)

$(q+1)\,n > 0$. Thus, we cannot have $q+1 \leq 0$. Hence, we have $q+1 > 0$, and therefore $q+1 \geq 1$ (since $q+1$ is an integer), so that $q \geq 0$. In other words, $q \in \mathbb{N}$. Combining this with $r \in \{0,1,\ldots,n-1\}$, we obtain $(q,r) \in \mathbb{N} \times \{0,1,\ldots,n-1\}$. Thus, $B\left((q,r)\right)$ is well-defined. The definition of B yields $B\left((q,r)\right) = qn + r = u$. Hence, $u = B\left((q,r)\right)$. Thus, there exists an $x \in \mathbb{N} \times \{0,1,\ldots,n-1\}$ such that $u = B\left(x\right)$ (namely, $x = (q,r)$).

Now, forget that we fixed u. We thus have shown that for each $u \in \mathbb{N}$, there exists an $x \in \mathbb{N} \times \{0,1,\ldots,n-1\}$ such that $u = B\left(x\right)$. In other words, the map B is surjective.]

We have now shown that the map B is injective and surjective. Hence, B is bijective. In other words, B is a bijection. As we explained above, this solves Exercise 2.6.4 **(b)**.

(c) Let $a \in \mathbb{Z}$ and $b \in \{0,1,\ldots,n-1\}$. We shall show that $(an+b)\,//n = a$. (This is, of course, the claim of Exercise 2.6.4 **(c)** with q and r renamed as a and b.)

Let $u = an + b$. Then, $u \in \mathbb{Z}$ (since a, n and b are integers). We have $(a,b) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ (since $a \in \mathbb{Z}$ and $b \in \{0,1,\ldots,n-1\}$) and $u = an + b$. Hence, (a,b) is a pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$. But Theorem 2.6.1 shows that there exists a unique pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$. This unique pair (q,r) must be (a,b) (because we have just shown that (a,b) is such a pair). Hence, Definition 2.6.2 **(a)** yields $u//n = a$. In view of $u = an + b$, this rewrites as $(an+b)\,//n = a$.

Now, forget that we fixed a and b. We thus have shown that any $a \in \mathbb{Z}$ and $b \in \{0,1,\ldots,n-1\}$ satisfy $(an+b)\,//n = a$. Renaming a and b as q and r in this statement, we obtain the following: Any $q \in \mathbb{Z}$ and $r \in \{0,1,\ldots,n-1\}$ satisfy $(qn+r)\,//n = q$. This solves Exercise 2.6.4 **(c)**.

(d) Let $a \in \mathbb{Z}$ and $b \in \{0,1,\ldots,n-1\}$. We shall show that $(an+b)\,\%n = b$. (This is, of course, the claim of Exercise 2.6.4 **(d)** with q and r renamed as a and b.)

Let $u = an + b$. Then, $u \in \mathbb{Z}$ (since a, n and b are integers). We have $(a,b) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ (since $a \in \mathbb{Z}$ and $b \in \{0,1,\ldots,n-1\}$) and $u = an + b$. Hence, (a,b) is a pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$. But Theorem 2.6.1 shows that there exists a unique pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$. This unique pair (q,r) must be (a,b) (because we have just shown that (a,b) is such a pair). Hence, Definition 2.6.2 **(b)** yields $u\%n = b$. In view of $u = an + b$, this rewrites as $(an+b)\,\%n = b$.

Now, forget that we fixed a and b. We thus have shown that any $a \in \mathbb{Z}$ and $b \in \{0,1,\ldots,n-1\}$ satisfy $(an+b)\,\%n = b$. Renaming a and b as q and r in this statement, we obtain the following: Any $q \in \mathbb{Z}$ and $r \in \{0,1,\ldots,n-1\}$ satisfy $(qn+r)\,\%n = r$. This solves Exercise 2.6.4 **(d)**. □

10.21. Solution to Exercise 2.7.1

Solution to Exercise 2.7.1. Corollary 2.6.9 **(b)** (applied to $n = 2$) shows that we have $2 \mid u$ if and only if $u\%2 = 0$. In other words, we have the logical equivalence

$$(2 \mid u) \iff (u\%2 = 0)\,. \qquad (344)$$

Corollary 2.6.9 **(a)** (applied to $n = 2$) yields that $u\%2 \in \{0,1,\ldots,2-1\}$ and $u\%2 \equiv u \operatorname{mod} 2$. Thus, in particular, $u\%2 \in \{0,1,\ldots,2-1\} = \{0,1\}$. Hence, $u\%2$ is either 0 or 1. Thus, the number $u\%2$ is 1 if and only if it is not 0. In other words, we have the equivalence

$$(u\%2 = 1) \iff (u\%2 \neq 0)\,. \qquad (345)$$

Proposition 2.3.3 (applied to $a = u$ and $n = 2$) shows that $u \equiv 0 \bmod 2$ if and only if $2 \mid u$. In other words, we have the equivalence

$$(u \equiv 0 \bmod 2) \iff (2 \mid u). \tag{346}$$

(a) We have the following chain of equivalences:

$$\begin{aligned}(u \text{ is even}) &\iff (u \text{ is divisible by } 2) \qquad \text{(by the definition of "even")} \\ &\iff (2 \mid u) \iff (u\%2 = 0) \qquad (\text{by (344)}).\end{aligned}$$

In other words, u is even if and only if $u\%2 = 0$. This solves Exercise 2.7.1 **(a)**.

(b) We have the following chain of equivalences:

$$\begin{aligned}(u \text{ is odd}) &\iff (u \text{ is not divisible by } 2) \qquad \text{(by the definition of "odd")} \\ &\iff (\text{we don't have } 2 \mid u) \iff (\text{we don't have } u\%2 = 0) \\ &\qquad (\text{because of the equivalence } (2 \mid u) \iff (u\%2 = 0)) \\ &\iff (u\%2 \neq 0) \\ &\iff (u\%2 = 1) \qquad (\text{by (345)}).\end{aligned} \tag{347}$$

In other words, u is odd if and only if $u\%2 = 1$. This solves Exercise 2.7.1 **(b)**.

(c) We have the following chain of equivalences:

$$\begin{aligned}(u \text{ is even}) &\iff (u \text{ is divisible by } 2) \qquad \text{(by the definition of "even")} \\ &\iff (2 \mid u) \iff (u \equiv 0 \bmod 2) \qquad (\text{by (346)}).\end{aligned}$$

In other words, u is even if and only if $u \equiv 0 \bmod 2$. This solves Exercise 2.7.1 **(c)**.

(d) $\Longrightarrow$: Assume that u is odd. We must prove that $u \equiv 1 \bmod 2$.

We know that u is odd. In other words, $u\%2 = 1$ (by Exercise 2.7.1 **(b)**). But recall that $u\%2 \equiv u \bmod 2$. Thus, $u \equiv u\%2 = 1 \bmod 2$. This proves the "$\Longrightarrow$" direction of Exercise 2.7.1 **(d)**.

$\Longleftarrow$: Assume that $u \equiv 1 \bmod 2$. We must prove that u is odd.

We have $1 \equiv u \bmod 2$ (since $u \equiv 1 \bmod 2$) and $1 \in \{0, 1, \ldots, 2-1\}$. But Corollary 2.6.9 **(c)** (applied to $n = 2$) says that if $c \in \{0, 1, \ldots, 2-1\}$ satisfies $c \equiv u \bmod 2$, then $c = u\%2$. Applying this to $c = 1$, we find $1 = u\%2$ (since $1 \in \{0, 1, \ldots, 2-1\}$ and $1 \equiv u \bmod 2$). In other words, $u\%2 = 1$. According to Exercise 2.7.1 **(b)**, this means that u is odd. This proves the "$\Longleftarrow$" direction of Exercise 2.7.1 **(d)**.

(e) $\Longrightarrow$: Assume that u is odd. We must prove that $u + 1$ is even.

We have assumed that u is odd. According to Exercise 2.7.1 **(d)**, this means that $u \equiv 1 \bmod 2$. On the other hand, $1 \equiv -1 \bmod 2$ (since $2 \mid 1 - (-1)$). Adding these two congruences together, we find $u + 1 \equiv 1 + (-1) = 0 \bmod 2$.

But Exercise 2.7.1 **(c)** (applied to $u + 1$ instead of u) shows that $u + 1$ is even if and only if $u + 1 \equiv 0 \bmod 2$. Hence, $u + 1$ is even (since $u + 1 \equiv 0 \bmod 2$). This proves the "$\Longrightarrow$" direction of Exercise 2.7.1 **(e)**.

$\Longleftarrow$: Assume that $u + 1$ is even. We must prove that u is odd.

We know that $u + 1$ is even. But Exercise 2.7.1 **(c)** (applied to $u + 1$ instead of u) shows that $u + 1$ is even if and only if $u + 1 \equiv 0 \bmod 2$. Hence, $u + 1 \equiv 0 \bmod 2$ (since $u + 1$ is even). On the other hand, $-1 \equiv 1 \bmod 2$ (since $2 \mid (-1) - 1$). Adding these two congruences together, we obtain $(u + 1) + (-1) \equiv 0 + 1 = 1 \bmod 2$. In view of $(u + 1) + (-1) = u$, this rewrites as $u \equiv 1 \operatorname{mod} 2$. According to Exercise 2.7.1 **(d)**, this means that u is odd. This proves the "$\Longleftarrow$" direction of Exercise 2.7.1 **(e)**.

(f) We have the equivalence $(u \text{ is divisible by } 2) \iff (u \text{ is even})$ (by the definition of "even").

Exercise 2.7.1 **(e)** shows that u is odd if and only if $u+1$ is even. Thus, we have the following chain of equivalences:

$$\begin{aligned} & (u+1 \text{ is even}) \\ \iff & (u \text{ is odd}) \iff (u \text{ is not divisible by } 2) \qquad \text{(by the definition of "odd")} \\ \iff & (u \text{ is not even}) \end{aligned}$$

(because of the equivalence $(u \text{ is divisible by } 2) \iff (u \text{ is even})$). In other words, $u+1$ is even if and only if u is not. In other words, exactly one of the two numbers u and $u+1$ is even. This solves Exercise 2.7.1 **(f)**.

(g) Exercise 2.7.1 **(f)** shows that exactly one of the two numbers u and $u+1$ is even. Thus, in particular, **at least** one of these two numbers is even. Hence, the product $u(u+1)$ has **at least** one even factor. But a product of any even integer with any integer is even[240]. Hence, a product that has at least one even factor is always even. Thus, $u(u+1)$ is even (since $u(u+1)$ is a product that has at least one even factor). In other words, $2 \mid u(u+1)$. In other words, $u(u+1) \equiv 0 \operatorname{mod} 2$. This solves Exercise 2.7.1 **(g)**.

(h) We have $u^2 - (-u) = u^2 + u = u(u+1) \equiv 0 \operatorname{mod} 2$ (by Exercise 2.7.1 **(g)**). In other words, $2 \mid u^2 - (-u)$. In other words, $u^2 \equiv -u \operatorname{mod} 2$.

Also, $2 \mid (-u) - u$ (since $(-u) - u = 2(-u)$ is clearly divisible by 2); in other words, $-u \equiv u \operatorname{mod} 2$. Hence, $u^2 \equiv -u \equiv u \operatorname{mod} 2$. This solves Exercise 2.7.1 **(h)**.

(i) Exercise 2.6.1 (applied to $n = 2$) shows that $u \equiv v \operatorname{mod} 2$ if and only if $u\%2 = v\%2$.

We are in one of the following four cases:

Case 1: We have $u\%2 = 0$ and $v\%2 = 0$.

Case 2: We have $u\%2 = 0$ and $v\%2 \neq 0$.

Case 3: We have $u\%2 \neq 0$ and $v\%2 = 0$.

Case 4: We have $u\%2 \neq 0$ and $v\%2 \neq 0$.

Let us first consider Case 1. In this case, we have $u\%2 = 0$ and $v\%2 = 0$. Thus, $u\%2 = 0 = v\%2$ and therefore $u \equiv v \operatorname{mod} 2$ (since we know that $u \equiv v \operatorname{mod} 2$ if and only if $u\%2 = v\%2$). But recall that $u\%2 = 0$. Equivalently, u is even (because of Exercise 2.7.1 **(a)**). Similarly, from $v\%2 = 0$, we conclude that v is even. Thus, u and v are either both odd or both even (namely, they are both even).

Thus, $u \equiv v \operatorname{mod} 2$ holds if and only if u and v are either both odd or both even (because both statements "$u \equiv v \operatorname{mod} 2$" and "$u$ and v are either both odd or both even" hold). Hence, Exercise 2.7.1 **(i)** is solved in Case 1.

Let us now consider Case 2. In this case, we have $u\%2 = 0$ and $v\%2 \neq 0$. Thus, $u\%2 = 0 \neq v\%2$. In other words, "$u\%2 = v\%2$" is false. Thus, "$u \equiv v \operatorname{mod} 2$" is false as well (since we know that $u \equiv v \operatorname{mod} 2$ if and only if $u\%2 = v\%2$). But recall that $u\%2 = 0$. Equivalently, u is even (because of Exercise 2.7.1 **(a)**). Hence, u is not odd[241]. Thus, u and v are not both odd. Also, Exercise 2.7.1 **(a)** (applied to v instead of u) shows that v is even

[240] *Proof.* We must prove that if a is an even integer, and if b is an integer, then the product ab is even.

So let a be an even integer, and let b be an integer. Then, a is even; in other words, $2 \mid a$ (by the definition of "even"). But $a \mid ab$. Hence, $2 \mid a \mid ab$; in other words, ab is even. Qed.

[241] because an integer is either even or odd (but not both at the same time)

if and only if $v\%2 = 0$. Since we don't have $v\%2 = 0$ (because $v\%2 \neq 0$), we thus conclude that v is not even. Thus, u and v are not both even.

So u and v are neither both odd nor both even. In other words, the statement "u and v are either both odd or both even" is false.

Thus, $u \equiv v \mod 2$ holds if and only if u and v are either both odd or both even (because both statements "$u \equiv v \mod 2$" and "u and v are either both odd or both even" are false). Hence, Exercise 2.7.1 **(i)** is solved in Case 2.

Case 3 is analogous to Case 2 (it differs from Case 2 only in that u and v trade places).

Let us finally consider Case 4. In this case, we have $u\%2 \neq 0$ and $v\%2 \neq 0$. By (347), we have the logical equivalence $(u \text{ is odd}) \iff (u\%2 \neq 0)$. Hence, u is odd (since $u\%2 \neq 0$). Similarly, v is odd. Thus, u and v are both odd. Thus, u and v are either both odd or both even (namely, they are both odd). Moreover, we know that u is odd; equivalently, $u\%2 = 1$ (by Exercise 2.7.1 **(b)**). Similarly, $v\%2 = 1$. Hence, $u\%2 = 1 = v\%2$. Therefore, $u \equiv v \mod 2$ (since we know that $u \equiv v \mod 2$ if and only if $u\%2 = v\%2$).

Thus, $u \equiv v \mod 2$ holds if and only if u and v are either both odd or both even (because both statements "$u \equiv v \mod 2$" and "u and v are either both odd or both even" hold). Hence, Exercise 2.7.1 **(i)** is solved in Case 4.

We have now solved Exercise 2.7.1 **(i)** in all four Cases 1, 2, 3 and 4. Hence, Exercise 2.7.1 **(i)** is solved. □

10.22. Solution to Exercise 2.7.2

Solution to Exercise 2.7.2. **(a)** Let u be an even integer. Thus, u is even. In other words, u is divisible by 2. In other words, there exists some integer c such that $u = 2c$. Consider this c.

From $u = 2c$, we obtain $u^2 = (2c)^2 = 4c^2$, which is clearly divisible by 4. So we have $4 \mid u^2 = u^2 - 0$. In other words, $u^2 \equiv 0 \mod 4$. This solves Exercise 2.7.2 **(a)**.

(b) Let u be an odd integer. Thus, u is odd. Equivalently, $u \equiv 1 \mod 2$ (by Exercise 2.7.1 **(d)**). In other words, $2 \mid u - 1$. In other words, there exists some integer c such that $u - 1 = 2c$. Consider this c.

From $u - 1 = 2c$, we obtain $u = 2c + 1$ and thus $u^2 = (2c+1)^2 = 4c^2 + 4c + 1$. Hence, $u^2 - 1 = 4c^2 + 4c = 4\left(c^2 + c\right)$, which is clearly divisible by 4. So we have $4 \mid u^2 - 1$. In other words, $u^2 \equiv 1 \mod 4$. This solves Exercise 2.7.2 **(b)**.

(c) Let x and y be two integers such that $x^2 + y^2 \equiv 3 \mod 4$. We shall derive a contradiction.

Recall that an integer is always either even or odd. Thus, x is either even or odd. Similarly, y is either even or odd. Thus, we are in one of the following four cases:

Case 1: The integer x is even, and the integer y is even.

Case 2: The integer x is even, and the integer y is odd.

Case 3: The integer x is odd, and the integer y is even.

Case 4: The integer x is odd, and the integer y is odd.

Let us first consider Case 1. In this case, the integer x is even, and the integer y is even. Hence, Exercise 2.7.2 **(a)** (applied to $u = x$) yields $x^2 \equiv 0 \mod 4$ (since x is even). Also, Exercise 2.7.2 **(a)** (applied to $u = y$) yields $y^2 \equiv 0 \mod 4$ (since y is even). Thus, $\underbrace{x^2}_{\equiv 0 \mod 4} + \underbrace{y^2}_{\equiv 0 \mod 4} \equiv 0 + 0 = 0 \mod 4$. Hence, $0 \equiv x^2 + y^2 \equiv 3 \mod 4$. But Exercise 2.6.1 (applied to $n = 4$, $u = 0$ and $v = 3$) shows that $0 \equiv 3 \mod 4$ if and only if $0\%4 = 3\%4$.

Hence, $0\%4 = 3\%4$ (since $0 \equiv 3 \mod 4$). This contradicts the fact that $0\%4 = 0 \neq 3 = 3\%4$. Hence, we have obtained a contradiction in Case 1.

Let us next consider Case 2. In this case, the integer x is even, and the integer y is odd. Hence, Exercise 2.7.2 **(a)** (applied to $u = x$) yields $x^2 \equiv 0 \mod 4$ (since x is even). Also, Exercise 2.7.2 **(b)** (applied to $u = y$) yields $y^2 \equiv 1 \mod 4$ (since y is odd). Thus, $\underbrace{x^2}_{\equiv 0 \mod 4} + \underbrace{y^2}_{\equiv 1 \mod 4} \equiv 0 + 1 = 1 \mod 4$. Hence, $1 \equiv x^2 + y^2 \equiv 3 \mod 4$. But Exercise 2.6.1 (applied to $n = 4$, $u = 1$ and $v = 3$) shows that $1 \equiv 3 \mod 4$ if and only if $1\%4 = 3\%4$. Hence, $1\%4 = 3\%4$ (since $1 \equiv 3 \mod 4$). This contradicts the fact that $1\%4 = 1 \neq 3 = 3\%4$. Hence, we have obtained a contradiction in Case 2.

The arguments in Cases 3 and 4 are completely analogous (in Case 3, we obtain $x^2 + y^2 \equiv 1 \mod 4$ again, whereas in Case 4 we obtain $x^2 + y^2 \equiv 2 \mod 4$). Thus, we have obtained a contradiction in each of the four Cases 1, 2, 3 and 4. Hence, we always have a contradiction.

Now, forget that we fixed x and y. We thus have obtained a contradiction whenever x and y are two integers such that $x^2 + y^2 \equiv 3 \mod 4$. Thus, there are no such two integers. This solves Exercise 2.7.2 **(c)**.

(d) The solution of Exercise 2.7.2 **(d)** is very similar to the above solution of Exercise 2.7.2 **(c)** (indeed, we have to consider the same four cases, but this time we don't get a contradiction in Case 4) and is left to the reader. □

10.23. Solution to Exercise 2.7.3

Solution to Exercise 2.7.3. **(a)** Define two sets A and B by

$$A = \{i \in \mathbb{N} \mid i \text{ is even}\} \tag{348}$$

and

$$B = \{d \in \mathbb{N} \mid d \equiv 1 \mod 4\}. \tag{349}$$

For each $u \in A$, we have $2u + 1 \in B$ [242]. Renaming the variable u as i in this statement, we obtain the following: For each $i \in A$, we have $2i + 1 \in B$. Thus, the map

$$\begin{aligned} A &\to B, \\ i &\mapsto 2i + 1 \end{aligned}$$

is well-defined. Let us denote this map by f.

[242] *Proof.* Let $u \in A$. Thus, $u \in A = \{i \in \mathbb{N} \mid i \text{ is even}\}$. In other words, u is an $i \in \mathbb{N}$ such that i is even. In other words, u is an element of $\mathbb{N}$ and is even. Thus, $u \in \mathbb{N}$, so that $2u + 1 \in \mathbb{N}$. Moreover, u is even; in other words, $u \equiv 0 \mod 2$ (by Exercise 2.7.1 **(c)**). In other words, $2 \mid u - 0$. In other words, there exists an integer c such that $u - 0 = 2c$. Consider this c. Now, $u = u - 0 = 2c$, so that $2 \underbrace{u}_{=2c} = 2 \cdot 2c = 4c \equiv 0 \mod 4$ (since we clearly have $4 \mid 4c$). Hence,

$$\underbrace{2u}_{\equiv 0 \mod 4} + 1 \equiv 0 + 1 = 1 \mod 4.$$

Hence, $2u + 1$ is an element of $\mathbb{N}$ (since $2u + 1 \in \mathbb{N}$) and satisfies $2u + 1 \equiv 1 \mod 4$. In other words, $2u + 1$ is a $d \in \mathbb{N}$ satisfying $d \equiv 1 \mod 4$. In other words, $2u + 1 \in \{d \in \mathbb{N} \mid d \equiv 1 \mod 4\}$. In view of (349), this rewrites as $2u + 1 \in B$. Qed.

For each $v \in B$, we have $(v-1)/2 \in A$ [243]. Hence, the map

$$B \to A,$$
$$v \mapsto (v-1)/2$$

is well-defined. Let us denote this map by g.

We have $f \circ g = \operatorname{id}$ [244] and $g \circ f = \operatorname{id}$ [245]. Thus, the maps f and g are mutually inverse. Hence, the map f is invertible, i.e., bijective. In other words, the map f is a bijection.

So we have proven that the map f is well-defined and is a bijection. In other words, the map

$$A \to B,$$
$$i \mapsto 2i+1$$

is well-defined and is a bijection[246]. Using (348) and (349), we can rewrite this as follows: The map

$$\{i \in \mathbb{N} \mid i \text{ is even}\} \to \{d \in \mathbb{N} \mid d \equiv 1 \operatorname{mod} 4\},$$
$$i \mapsto 2i+1$$

[243] *Proof.* Let $v \in B$. Thus, $v \in B = \{d \in \mathbb{N} \mid d \equiv 1 \operatorname{mod} 4\}$. In other words, v is a $d \in \mathbb{N}$ satisfying $d \equiv 1 \operatorname{mod} 4$. In other words, v is an element of $\mathbb{N}$ and satisfies $v \equiv 1 \operatorname{mod} 4$. Thus, in particular, $v \equiv 1 \operatorname{mod} 4$; in other words, $4 \mid v-1$. In other words, there exists an integer w such that $v - 1 = 4w$. Consider this w. We have $v \geq 0$ (since v is an element of $\mathbb{N}$) and thus $\underbrace{v}_{\geq 0} -1 \geq -1$. If we had $w \leq -1$, then we would have $v - 1 = 4 \underbrace{w}_{\leq -1} \leq 4(-1) = -4 < -1$, which would contradict $v - 1 \geq -1$. Thus, we cannot have $w \leq -1$. Hence, we have $w > -1$. Thus, $w \geq 0$ (since w is an integer), so that $w \in \mathbb{N}$. Hence, $2w \in \mathbb{N}$. Moreover, $2 \mid 2w$ (since w is an integer). Thus, $2w$ is even. Hence, $2w$ is an $i \in \mathbb{N}$ such that i is even (since $2w \in \mathbb{N}$). In other words, $2w \in \{i \in \mathbb{N} \mid i \text{ is even}\}$. In view of (348), this rewrites as $2w \in A$. But $v - 1 = 4w = 2 \cdot 2w$, so that $(v-1)/2 = 2w \in A$. Qed.

[244] *Proof.* Let $v \in B$. Then, the definition of g yields $g(v) = (v-1)/2$. But the definition of f yields $f(g(v)) = 2 \underbrace{g(v)}_{=(v-1)/2} +1 = 2(v-1)/2 + 1 = v = \operatorname{id}(v)$. Comparing this with $f(g(v)) = (f \circ g)(v)$, we obtain $(f \circ g)(v) = \operatorname{id}(v)$.

Now, forget that we fixed v. We thus have proven that $(f \circ g)(v) = \operatorname{id}(v)$ for each $v \in B$. In other words, $f \circ g = \operatorname{id}$.

[245] *Proof.* Let $i \in A$. Then, the definition of f yields $f(i) = 2i+1$. But the definition of g yields $g(f(i)) = \left(\underbrace{f(i)}_{=2i+1} -1\right)/2 = (2i+1-1)/2 = i = \operatorname{id}(i)$. Comparing this with $g(f(i)) = (g \circ f)(i)$, we obtain $(g \circ f)(i) = \operatorname{id}(i)$.

Now, forget that we fixed i. We thus have proven that $(g \circ f)(i) = \operatorname{id}(i)$ for each $i \in A$. In other words, $g \circ f = \operatorname{id}$.

[246] since the map f is the map

$$A \to B,$$
$$i \mapsto 2i+1$$

is well-defined and is a bijection. This solves Exercise 2.7.3 **(a)**.

(b) Define two sets A and B by

$$A = \{i \in \mathbb{N} \mid i \text{ is odd}\} \tag{350}$$

and

$$B = \{d \in \mathbb{N} \mid d \equiv 3 \bmod 4\}. \tag{351}$$

For each $u \in A$, we have $2u + 1 \in B$ [247]. Renaming the variable u as i in this statement, we obtain the following: For each $i \in A$, we have $2i + 1 \in B$. Thus, the map

$$A \to B,$$
$$i \mapsto 2i + 1$$

is well-defined. Let us denote this map by f.

For each $v \in B$, we have $(v-1)/2 \in A$ [248]. Hence, the map

$$B \to A,$$
$$v \mapsto (v-1)/2$$

is well-defined. Let us denote this map by g.

[247] *Proof.* Let $u \in A$. Thus, $u \in A = \{i \in \mathbb{N} \mid i \text{ is odd}\}$. In other words, u is an $i \in \mathbb{N}$ such that i is odd. In other words, u is an element of $\mathbb{N}$ and is odd. Thus, $u \in \mathbb{N}$, so that $2u + 1 \in \mathbb{N}$. Moreover, u is odd; in other words, $u \equiv 1 \bmod 2$ (by Exercise 2.7.1 **(d)**). In other words, $2 \mid u - 1$. In other words, there exists an integer c such that $u - 1 = 2c$. Consider this c. Now, $2u - 2 = 2\underbrace{(u-1)}_{=2c} = 2 \cdot 2c = 4c \equiv 0 \bmod 4$ (since we clearly have $4 \mid 4c$). Hence,

$$2u + 1 = \underbrace{2u - 2}_{\equiv 0 \bmod 4} + 3 \equiv 0 + 3 = 3 \bmod 4.$$

Hence, $2u + 1$ is an element of $\mathbb{N}$ (since $2u + 1 \in \mathbb{N}$) and satisfies $2u + 1 \equiv 3 \bmod 4$. In other words, $2u + 1$ is a $d \in \mathbb{N}$ satisfying $d \equiv 3 \bmod 4$. In other words, $2u + 1 \in \{d \in \mathbb{N} \mid d \equiv 3 \bmod 4\}$. In view of (351), this rewrites as $2u + 1 \in B$. Qed.

[248] *Proof.* Let $v \in B$. Thus, $v \in B = \{d \in \mathbb{N} \mid d \equiv 3 \bmod 4\}$. In other words, v is a $d \in \mathbb{N}$ satisfying $d \equiv 3 \bmod 4$. In other words, v is an element of $\mathbb{N}$ and satisfies $v \equiv 3 \bmod 4$. Thus, in particular, $v \equiv 3 \bmod 4$; in other words, $4 \mid v - 3$. In other words, there exists an integer w such that $v - 3 = 4w$. Consider this w. We have $v \geq 0$ (since v is an element of $\mathbb{N}$) and thus $\underbrace{v}_{\geq 0} - 3 \geq -3$. If we had $w \leq -1$, then we would have $v - 3 = 4\underbrace{w}_{\leq -1} \leq 4(-1) = -4 < -3$, which would contradict $v - 3 \geq -3$. Thus, we cannot have $w \leq -1$. Hence, we have $w > -1$. Thus, $w \geq 0$ (since w is an integer), so that $w \in \mathbb{N}$. Hence, $2w + 1 \in \mathbb{N}$. Moreover, $\underbrace{2}_{\equiv 0 \bmod 2} w + 1 \equiv 0w + 1 = 1 \bmod 2$. But Exercise 2.7.1 **(d)** (applied to $u = 2w + 1$) shows that $2w + 1$ is odd if and only if $2w + 1 \equiv 1 \bmod 2$. Hence, $2w + 1$ is odd (since $2w + 1 \equiv 1 \bmod 2$). Hence, $2w + 1$ is an $i \in \mathbb{N}$ such that i is odd (since $2w + 1 \in \mathbb{N}$). In other words, $2w + 1 \in \{i \in \mathbb{N} \mid i \text{ is odd}\}$. In view of (350), this rewrites as $2w + 1 \in A$. But $v - 1 = \underbrace{v - 3}_{=4w} + 2 = 4w + 2 = 2(2w + 1)$, so that $(v-1)/2 = 2w + 1 \in A$. Qed.

The maps f and g are mutually inverse[249]. Hence, the map f is invertible, i.e., bijective. In other words, the map f is a bijection.

So we have proven that the map f is well-defined and is a bijection. In other words, the map

$$\begin{aligned} A &\to B, \\ i &\mapsto 2i+1 \end{aligned}$$

is well-defined and is a bijection[250]. Using (350) and (351), we can rewrite this as follows: The map

$$\begin{aligned} \{i \in \mathbb{N} \mid i \text{ is odd}\} &\to \{d \in \mathbb{N} \mid d \equiv 3 \operatorname{mod} 4\}, \\ i &\mapsto 2i+1 \end{aligned}$$

is well-defined and is a bijection. This solves Exercise 2.7.3 **(b)**.

[*Remark:* The reader can easily find an alternative solution to Exercise 2.7.3, which proceeds by restricting the bijection from Exercise 2.6.4 **(b)**. We chose to give the above solution instead since it is more explicit.] □

10.24. Solution to Exercise 2.9.1

Solution to Exercise 2.9.1. Assume that $\{b_1, b_2, \ldots, b_k\} = \{c_1, c_2, \ldots, c_\ell\}$.

Let a be an integer. Then, a is a common divisor of $b_1, b_2, \ldots, b_k$ if and only if a satisfies ($a \mid b_i$ for all $i \in \{1, 2, \ldots, k\}$) (by the definition of "common divisor"). Hence, we have the following chain of equivalences:

$$\begin{aligned} & (a \text{ is a common divisor of } b_1, b_2, \ldots, b_k) \\ \Longleftrightarrow\ & (a \mid b_i \text{ for all } i \in \{1, 2, \ldots, k\}) \\ \Longleftrightarrow\ & (a \mid b_1 \text{ and } a \mid b_2 \text{ and } \cdots \text{ and } a \mid b_k) \\ \Longleftrightarrow\ & (a \mid u \text{ for each } u \in \{b_1, b_2, \ldots, b_k\}). \end{aligned}$$

But $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ is the set of all common divisors of $b_1, b_2, \ldots, b_k$. Hence, we have $a \in \operatorname{Div}(b_1, b_2, \ldots, b_k)$ if and only if a is a common divisor of $b_1, b_2, \ldots, b_k$. Thus, we have the following chain of equivalences:

$$\begin{aligned} & (a \in \operatorname{Div}(b_1, b_2, \ldots, b_k)) \\ \Longleftrightarrow\ & (a \text{ is a common divisor of } b_1, b_2, \ldots, b_k) \\ \Longleftrightarrow\ & (a \mid u \text{ for each } u \in \{b_1, b_2, \ldots, b_k\}). \end{aligned} \tag{352}$$

[249] This can be proven in the exact same way as the analogous statement was shown in our above solution to Exercise 2.7.3 **(a)**. In fact, the maps f and g here act in the exact same way as the maps f and g in our solution to Exercise 2.7.3 **(a)**; the only thing that is different are their domains and codomains A and B.

[250] since the map f is the map

$$\begin{aligned} A &\to B, \\ i &\mapsto 2i+1 \end{aligned}$$

The same argument (applied to ℓ and $(c_1, c_2, \ldots, c_\ell)$ instead of k and $(b_1, b_2, \ldots, b_k)$) yields the equivalence

$$\begin{aligned} &(a \in \operatorname{Div}(c_1, c_2, \ldots, c_\ell)) \\ \Longleftrightarrow\ & (a \mid u \text{ for each } u \in \{c_1, c_2, \ldots, c_\ell\}) . \end{aligned} \tag{353}$$

Now, we have the following chain of equivalences:

$$\begin{aligned} &(a \in \operatorname{Div}(b_1, b_2, \ldots, b_k)) \\ \Longleftrightarrow\ & \left(a \mid u \text{ for each } u \in \underbrace{\{b_1, b_2, \ldots, b_k\}}_{=\{c_1,c_2,\ldots,c_\ell\}} \right) \qquad \text{(by (352))} \\ \Longleftrightarrow\ & (a \mid u \text{ for each } u \in \{c_1, c_2, \ldots, c_\ell\}) \\ \Longleftrightarrow\ & (a \in \operatorname{Div}(c_1, c_2, \ldots, c_\ell)) \qquad \text{(by (353))} . \end{aligned}$$

Now, forget that we fixed a. We thus have proven the equivalence

$$(a \in \operatorname{Div}(b_1, b_2, \ldots, b_k)) \iff (a \in \operatorname{Div}(c_1, c_2, \ldots, c_\ell))$$

for each integer a. In other words, an integer a belongs to the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ if and only if it belongs to the set $\operatorname{Div}(c_1, c_2, \ldots, c_\ell)$. In other words, the two sets $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ and $\operatorname{Div}(c_1, c_2, \ldots, c_\ell)$ contain the exact same integers. Since both of these sets consist of integers only, this entails that these two sets are equal. In other words, $\operatorname{Div}(b_1, b_2, \ldots, b_k) = \operatorname{Div}(c_1, c_2, \ldots, c_\ell)$. This solves Exercise 2.9.1. □

10.25. Solution to Exercise 2.9.2

Solution to Exercise 2.9.2. Assume that $\{b_1, b_2, \ldots, b_k\} = \{c_1, c_2, \ldots, c_\ell\}$. Then, Exercise 2.9.1 yields $\operatorname{Div}(b_1, b_2, \ldots, b_k) = \operatorname{Div}(c_1, c_2, \ldots, c_\ell)$. Hence, Lemma 2.9.9 yields $\gcd(b_1, b_2, \ldots, b_k) = \gcd(c_1, c_2, \ldots, c_\ell)$. This solves Exercise 2.9.2. □

10.26. Solution to Exercise 2.9.3

Solution to Exercise 2.9.3. **(a)** Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$ be such that $b \geq a$.

We have $b - a \geq 0$ (since $b \geq a$), hence $b - a \in \mathbb{N}$. Thus, u^{b-a} is an integer. We have

$$\begin{aligned} \left(u^b - 1\right) - (u^a - 1) = u^b - u^a &= \underbrace{u^{(b-a)+a}}_{=u^{b-a}u^a} - u^a \qquad (\text{since } b = (b-a) + a) \\ &= u^{b-a}u^a - u^a = \left(u^{b-a} - 1\right) u^a. \end{aligned}$$

Thus, $u^{b-a} - 1 \mid \left(u^b - 1\right) - (u^a - 1)$ (since u^a is an integer). In other words, $u^b - 1 \equiv u^a - 1 \bmod u^{b-a} - 1$. This solves Exercise 2.9.3 **(a)**.

(b) The following argument will imitate our proof of Lemma 2.9.13 above.

We use strong induction on $a + b$. Thus, we fix an $n \in \mathbb{N}$, and assume (as induction hypothesis) that Exercise 2.9.3 **(b)** holds whenever $a + b < n$. We must now prove that Exercise 2.9.3 **(b)** holds whenever $a + b = n$.

We have assumed that Exercise 2.9.3 **(b)** holds whenever $a + b < n$. In other words, the following statement holds:

> *Statement 1:* Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$ be such that $a+b<n$. Then, $\gcd\left(u^a-1, u^b-1\right) = \left|u^{\gcd(a,b)}-1\right|$.

Now, we must prove that Exercise 2.9.3 **(b)** holds whenever $a+b=n$. Let us first prove this in the case when $b \geq a$:

> *Statement 2:* Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$ be such that $a+b=n$ and $b \geq a$. Then, $\gcd\left(u^a-1, u^b-1\right) = \left|u^{\gcd(a,b)}-1\right|$.

[*Proof of Statement 2:* We are in one of the following two cases:

Case 1: We have $a=0$.

Case 2: We have $a \neq 0$.

Let us first consider Case 1. In this case, we have $a=0$. Hence, $u^a = u^0 = 1$ and thus $u^a - 1 = 0$. Thus,

$$\begin{aligned} \gcd\left(\underbrace{u^a-1}_{=0}, u^b-1\right) &= \gcd\left(0, u^b-1\right) = \gcd\left(u^b-1, 0\right) \\ &\qquad \left(\begin{array}{c}\text{by Proposition 2.9.7 } \textbf{(b)}\text{, applied to } 0 \text{ and } u^b-1 \\ \text{instead of } a \text{ and } b\end{array}\right) \\ &= \left|u^b-1\right| \end{aligned} \tag{354}$$

(since Proposition 2.9.7 **(a)** (applied to u^b-1 instead of a) yields $\gcd\left(u^b-1,0\right) = \gcd\left(u^b-1\right) = \left|u^b-1\right|$).

But Proposition 2.9.7 **(b)** yields $\gcd(a,b) = \gcd\left(b, \underbrace{a}_{=0}\right) = \gcd(b,0)$. Now, Proposition 2.9.7 **(a)** (applied to b instead of a) yields $\gcd(b,0) = \gcd(b) = |b|$. Hence, $\gcd(a,b) = \gcd(b,0) = |b| = b$ (since b is nonnegative). Hence, $\left|u^{\gcd(a,b)}-1\right| = \left|u^b-1\right|$. Comparing this equality with (354), we obtain $\gcd\left(u^a-1,u^b-1\right) = \left|u^{\gcd(a,b)}-1\right|$. Thus, Statement 2 is proven in Case 1.

Let us next consider Case 2. In this case, we have $a \neq 0$. Hence, $a > 0$ (since $a \in \mathbb{N}$), so that $a+b>b$. Hence, $b < a+b = n$.

From $b \geq a$, we obtain $b-a \in \mathbb{N}$. Moreover, $a \in \mathbb{N}$ and $b-a \in \mathbb{N}$ satisfy $a+(b-a) = b < n$. Therefore, we can apply Statement 1 **to** $b-a$ **instead of** b. Thus we obtain that $\gcd\left(u^a-1,u^{b-a}-1\right) = \left|u^{\gcd(a,b-a)}-1\right|$.

But Proposition 2.9.7 **(c)** (applied to $u=-1$) yields $\gcd(a,(-1)a+b) = \gcd(a,b)$. This rewrites as $\gcd(a,b-a) = \gcd(a,b)$ (since $(-1)a+b = b-a$).

Recall that $b-a \in \mathbb{N}$. Also, $b \geq b-a$ (since $a \geq 0$). Hence, Exercise 2.9.3 **(a)** (applied to $b-a$ instead of a) yields $u^b - 1 \equiv u^{b-a}-1 \mod u^{b-(b-a)}-1$. Since $b-(b-a) = a$, this rewrites as $u^b-1 \equiv u^{b-a}-1 \mod u^a-1$. Hence, Proposition 2.9.7 **(d)** (applied to u^a-1, u^b-1 and $u^{b-a}-1$ instead of a, b and c) yields

$$\begin{aligned} \gcd\left(u^a-1,u^b-1\right) &= \gcd\left(u^a-1,u^{b-a}-1\right) = \left|u^{\gcd(a,b-a)}-1\right| \\ &= \left|u^{\gcd(a,b)}-1\right| \qquad (\text{since } \gcd(a,b-a) = \gcd(a,b)). \end{aligned}$$

Thus, Statement 2 is proven in Case 2.

We have now proven Statement 2 in both Cases 1 and 2. Hence, Statement 2 is always proven.]

Now, we can prove that Exercise 2.9.3 **(b)** holds whenever $a+b=n$:

> *Statement 3:* Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$ be such that $a+b=n$. Then, $\gcd\left(u^a-1, u^b-1\right) = \left|u^{\gcd(a,b)}-1\right|$.

[*Proof of Statement 3:* We are in one of the following two cases:

Case 1: We have $b \geq a$.

Case 2: We have $b < a$.

Let us first consider Case 1. In this case, we have $b \geq a$. Hence, Statement 2 shows that $\gcd\left(u^a-1, u^b-1\right) = \left|u^{\gcd(a,b)}-1\right|$. Thus, Statement 3 is proven in Case 1.

Let us next consider Case 2. In this case, we have $b < a$. Hence, $a > b$, so that $a \geq b$. This shows that we can apply Statement 2 **to** b **and** a **instead of** a **and** b. Thus we obtain $\gcd\left(u^b-1, u^a-1\right) = \left|u^{\gcd(b,a)}-1\right|$. But Proposition 2.9.7 **(b)** yields $\gcd(a,b) = \gcd(b,a)$. Moreover, Proposition 2.9.7 **(b)** (applied to u^a-1 and u^b-1 instead of a and b) yields

$$\gcd\left(u^a-1, u^b-1\right) = \gcd\left(u^b-1, u^a-1\right) = \left|u^{\gcd(b,a)}-1\right| = \left|u^{\gcd(a,b)}-1\right|$$

(since $\gcd(b,a) = \gcd(a,b)$). Thus, Statement 3 is proven in Case 2.

We have now proven Statement 3 in both Cases 1 and 2. Hence, Statement 3 is always proven.]

By proving Statement 3, we have shown that Exercise 2.9.3 **(b)** holds whenever $a+b=n$. This completes the induction step. Thus, Exercise 2.9.3 **(b)** is proven by strong induction.

[See also `https://math.stackexchange.com/questions/7473/` for various solutions of Exercise 2.9.3 **(b)**.] □

10.27. Solution to Exercise 2.9.4

Solution to Exercise 2.9.4. Proposition 2.9.7 **(f)** (applied to $a=a_1$ and $b=a_2$) yields that we have $\gcd(a_1,a_2) \mid a_1$ and $\gcd(a_1,a_2) \mid a_2$. Thus, $\gcd(a_1,a_2) \mid a_1 \mid b_1$ and $\gcd(a_1,a_2) \mid a_2 \mid b_2$.

So we know that $\gcd(a_1,a_2) \mid b_1$ and $\gcd(a_1,a_2) \mid b_2$. Hence, Lemma 2.9.16 (applied to $m = \gcd(a_1,a_2)$, $a = b_1$ and $b = b_2$) yields $\gcd(a_1,a_2) \mid \gcd(b_1,b_2)$. This solves Exercise 2.9.4. □

10.28. Solution to Exercise 2.9.5

Solution to Exercise 2.9.5. **(a)** If $b \geq 0$, then $|b| = b$. Hence, if $b \geq 0$, then Exercise 2.9.5 **(a)** holds (since $\gcd\left(a, \underbrace{|b|}_{=b}\right) = \gcd(a,b)$). Thus, for the rest of this solution to Exercise 2.9.5 **(a)**, we WLOG assume that we don't have $b \geq 0$. Hence, we have $b < 0$. Thus, $|b| = -b$ and therefore $\gcd\left(a, \underbrace{|b|}_{=-b}\right) = \gcd(a,-b) = \gcd(a,b)$ (by Proposition 2.9.7 **(h)**). This solves Exercise 2.9.5 **(a)**.

(b) If $a \geq 0$, then $|a| = a$. Hence, if $a \geq 0$, then Exercise 2.9.5 **(b)** holds (since $\gcd\left(\underbrace{|a|}_{=a}, b\right) = \gcd(a,b)$). Thus, for the rest of this solution to Exercise 2.9.5 **(b)**, we WLOG assume that we don't have $a \geq 0$. Hence, we have $a < 0$. Thus, $|a| = -a$ and therefore $\gcd\left(\underbrace{|a|}_{=-a}, b\right) = \gcd(-a,b) = \gcd(a,b)$ (by Proposition 2.9.7 **(g)**). This solves Exercise 2.9.5 **(b)**.

(c) Exercise 2.9.5 **(b)** (applied to $|b|$ instead of b) yields $\gcd(|a|,|b|) = \gcd(a,|b|) = \gcd(a,b)$ (by Exercise 2.9.5 **(a)**). This solves Exercise 2.9.5 **(c)**. □

10.29. Solution to Exercise 2.9.6

Solution to Exercise 2.9.6. Theorem 2.9.20 yields

$$\gcd(sa,sb) = |s|\gcd(a,b). \tag{355}$$

But $\gcd(a,b)$ is a nonnegative integer (by the definition of $\gcd(a,b)$). The equality (3) (applied to $x = s$ and $y = \gcd(a,b)$) yields

$$\begin{aligned} |s\gcd(a,b)| &= |s| \cdot \underbrace{|\gcd(a,b)|}_{\substack{=\gcd(a,b) \\ (\text{since } \gcd(a,b) \text{ is nonnegative})}} = |s|\gcd(a,b) \\ &= \gcd(sa,sb) \qquad (\text{by (355)}). \end{aligned} \tag{356}$$

Now, Theorem 2.9.21 **(d)** (applied to 3 and (a,b,c) instead of k and $(b_1,b_2,\ldots,b_k)$) yields

$$\gcd(a,b,c) = \gcd(\gcd(a,b),c). \tag{357}$$

The same argument (applied to sa, sb, sc instead of a, b, c) yields

$$\begin{aligned} &\gcd(sa,sb,sc) \\ &= \gcd\left(\underbrace{\gcd(sa,sb)}_{\substack{=|s\gcd(a,b)| \\ (\text{by (356)})}}, sc\right) = \gcd(|s\gcd(a,b)|, sc) \\ &= \gcd(s\gcd(a,b), sc) \qquad \left(\begin{array}{c}\text{by Exercise 2.9.5 \textbf{(b)}, applied to } s\gcd(a,b) \\ \text{and } sc \text{ instead of } a \text{ and } b\end{array}\right) \\ &= |s|\underbrace{\gcd(\gcd(a,b),c)}_{\substack{=\gcd(a,b,c) \\ (\text{by (357)})}} \qquad \left(\begin{array}{c}\text{by Theorem 2.9.20, applied to } \gcd(a,b) \\ \text{and } c \text{ instead of } a \text{ and } b\end{array}\right) \\ &= |s|\gcd(a,b,c). \end{aligned}$$

This solves Exercise 2.9.6. □

10.30. Solution to Exercise 2.9.7

Solution to Exercise 2.9.7. We shall show that

$$\gcd\left(sa_1, sa_2, \ldots, sa_i\right) = |s| \gcd\left(a_1, a_2, \ldots, a_i\right) \qquad (358)$$

for each $i \in \{0, 1, \ldots, k\}$.

[*Proof of (358):* We proceed by induction on i:

Induction base: Proposition 2.9.7 **(j)** shows that the greatest common divisor of the empty list of integers is $\gcd() = 0$. Now, comparing $\gcd\left(sa_1, sa_2, \ldots, sa_0\right) = \gcd() = 0$ with $|s| \underbrace{\gcd\left(a_1, a_2, \ldots, a_0\right)}_{=\gcd()=0} = 0$, we obtain $\gcd\left(sa_1, sa_2, \ldots, sa_0\right) = |s| \gcd\left(a_1, a_2, \ldots, a_0\right)$. In other words, (358) holds for $i = 0$. This completes the induction base.

Induction step: Let $j \in \{1, 2, \ldots, k\}$. Assume that (358) holds for $i = j - 1$. We must prove that (358) holds for $i = j$.

We have assumed that (358) holds for $i = j - 1$. In other words, we have

$$\gcd\left(sa_1, sa_2, \ldots, sa_{j-1}\right) = |s| \gcd\left(a_1, a_2, \ldots, a_{j-1}\right). \qquad (359)$$

But $\gcd\left(a_1, a_2, \ldots, a_{j-1}\right)$ is a nonnegative integer (by the definition of $\gcd\left(a_1, a_2, \ldots, a_{j-1}\right)$). The equality (3) (applied to $x = s$ and $y = \gcd\left(a_1, a_2, \ldots, a_{j-1}\right)$) yields

$$\left|s \gcd\left(a_1, a_2, \ldots, a_{j-1}\right)\right| = |s| \cdot \underbrace{\left|\gcd\left(a_1, a_2, \ldots, a_{j-1}\right)\right|}_{\substack{=\gcd\left(a_1, a_2, \ldots, a_{j-1}\right) \\ \text{(since } \gcd\left(a_1, a_2, \ldots, a_{j-1}\right) \text{ is nonnegative)}}} = |s| \gcd\left(a_1, a_2, \ldots, a_{j-1}\right)$$
$$= \gcd\left(sa_1, sa_2, \ldots, sa_{j-1}\right) \qquad \text{(by (359))}. \qquad (360)$$

Theorem 2.9.21 **(d)** (applied to j and a_i instead of k and b_i) yields

$$\gcd\left(a_1, a_2, \ldots, a_j\right) = \gcd\left(\gcd\left(a_1, a_2, \ldots, a_{j-1}\right), a_j\right). \qquad (361)$$

Theorem 2.9.21 **(d)** (applied to j and sa_i instead of k and b_i) yields

$$\begin{aligned}
&\gcd\left(sa_1, sa_2, \ldots, sa_j\right) \\
&= \gcd\left(\underbrace{\gcd\left(sa_1, sa_2, \ldots, sa_{j-1}\right)}_{\substack{=\left|s \gcd\left(a_1, a_2, \ldots, a_{j-1}\right)\right| \\ \text{(by (360))}}}, sa_j\right) \\
&= \gcd\left(\left|s \gcd\left(a_1, a_2, \ldots, a_{j-1}\right)\right|, sa_j\right) \\
&= \gcd\left(s \gcd\left(a_1, a_2, \ldots, a_{j-1}\right), sa_j\right) \\
&\qquad \left(\text{by Exercise 2.9.5 \textbf{(b)}, applied to } s \gcd\left(a_1, a_2, \ldots, a_{j-1}\right) \text{ and } sa_j \text{ instead of } a \text{ and } b\right) \\
&= |s| \underbrace{\gcd\left(\gcd\left(a_1, a_2, \ldots, a_{j-1}\right), a_j\right)}_{\substack{=\gcd\left(a_1, a_2, \ldots, a_j\right) \\ \text{(by (361))}}} \\
&\qquad \left(\text{by Theorem 2.9.20, applied to } \gcd\left(a_1, a_2, \ldots, a_{j-1}\right) \text{ and } a_j \text{ instead of } a \text{ and } b\right) \\
&= |s| \gcd\left(a_1, a_2, \ldots, a_j\right).
\end{aligned}$$

In other words, (358) holds for $i = j$. This completes the induction step. Thus, (358) is proven.]

Now, (358) (applied to $i = k$) yields $\gcd(sa_1, sa_2, \ldots, sa_k) = |s| \gcd(a_1, a_2, \ldots, a_k)$. This solves Exercise 2.9.7. □

10.31. Solution to Exercise 2.10.1

Solution to Exercise 2.10.1. **(a)** We have $1 \mid a$ (since $a = 1 \cdot a$). Thus, Proposition 2.9.7 **(i)** (applied to 1 and a instead of a and b) yields $\gcd(1, a) = |1| = 1$. In other words, $1 \perp a$ (by the definition of "coprime"). This solves Exercise 2.10.1 **(a)**.

(b) Proposition 2.9.7 **(a)** yields $\gcd(a, 0) = \gcd(a) = |a|$. But Proposition 2.9.7 **(b)** (applied to $b = 0$) yields $\gcd(a, 0) = \gcd(0, a)$. Hence, $\gcd(0, a) = \gcd(a, 0) = |a|$. Now, we have the following chain of logical equivalences:

$$\begin{aligned}(0 \perp a) &\iff (\gcd(0, a) = 1) \qquad \text{(by the definition of "coprime")} \\ &\iff (|a| = 1) \qquad \left(\text{since } \gcd(0, a) = |a|\right).\end{aligned}$$

In other words, we have $0 \perp a$ if and only if $|a| = 1$. This solves Exercise 2.10.1 **(b)**. □

10.32. Solution to Exercise 2.10.2

Solution to Exercise 2.10.2. Let us prove that

$$a_1 a_2 \cdots a_i \perp c \qquad \text{for each } i \in \{0, 1, \ldots, k\}. \tag{362}$$

Proof of (362): We shall prove (362) by induction on i:

Induction base: Exercise 2.10.1 **(a)** (applied to $a = c$) yields $1 \perp c$. Now, $a_1 a_2 \cdots a_0 = (\text{empty product}) = 1 \perp c$. Hence, (362) holds for $i = 0$. This completes the induction base.

Induction step: Let $j \in \{1, 2, \ldots, k\}$. Assume that (362) holds for $i = j - 1$. We must now prove that (362) holds for $i = j$.

We have assumed that (362) holds for $i = j - 1$. In other words, $a_1 a_2 \cdots a_{j-1} \perp c$.

We have assumed that each $i \in \{1, 2, \ldots, k\}$ satisfies $a_i \perp c$. Applying this to $i = j$, we find $a_j \perp c$.

Now we know that $a_1 a_2 \cdots a_{j-1} \perp c$ and $a_j \perp c$. Hence, Theorem 2.10.9 (applied to $a = a_1 a_2 \cdots a_{j-1}$ and $b = a_j$) yields $\left(a_1 a_2 \cdots a_{j-1}\right) a_j \perp c$. In other words, $a_1 a_2 \cdots a_j \perp c$ (since $a_1 a_2 \cdots a_j = \left(a_1 a_2 \cdots a_{j-1}\right) a_j$). In other words, (362) holds for $i = j$. This completes the induction step. Thus, (362) is proven by induction.

Now, we can apply (362) to $i = k$. We thus obtain $a_1 a_2 \cdots a_k \perp c$. This proves Exercise 2.10.2. □

10.33. Solution to Exercise 2.10.3

Solution to Exercise 2.10.3. We assumed that the integers $b_1, b_2, \ldots, b_k$ are mutually coprime. In other words, we have

$$b_i \perp b_j \text{ for all } i, j \in \{1, 2, \ldots, k\} \text{ satisfying } i \neq j. \tag{363}$$

Let us prove that

$$b_1 b_2 \cdots b_i \mid c \qquad \text{for each } i \in \{0, 1, \ldots, k\}. \tag{364}$$

Proof of (364): We shall prove (364) by induction on i:

Induction base: We have $b_1 b_2 \cdots b_0 = (\text{empty product}) = 1 \mid c$. Hence, (364) holds for $i = 0$. This completes the induction base.

Induction step: Let $j \in \{1, 2, \ldots, k\}$. Assume that (364) holds for $i = j - 1$. We must now prove that (364) holds for $i = j$.

We have assumed that (364) holds for $i = j - 1$. In other words, $b_1 b_2 \cdots b_{j-1} \mid c$.

We have assumed that each $i \in \{1, 2, \ldots, k\}$ satisfies $b_i \mid c$. Applying this to $i = j$, we find $b_j \mid c$.

For each $i \in \{1, 2, \ldots, j-1\}$, we have $i \leq j - 1 < j$ and thus $i \neq j$ and therefore $b_i \perp b_j$ (by (363)). Hence, Exercise 2.10.3 (applied to $j - 1$, b_j and $(b_1, b_2, \ldots, b_{j-1})$ instead of k, c and $(a_1, a_2, \ldots, a_k)$) yields $b_1 b_2 \cdots b_{j-1} \perp b_j$.

Now we know that $b_1 b_2 \cdots b_{j-1} \mid c$ and $b_j \mid c$ and $b_1 b_2 \cdots b_{j-1} \perp b_j$. Hence, Theorem 2.10.7 (applied to $a = b_1 b_2 \cdots b_{j-1}$ and $b = b_j$) yields $(b_1 b_2 \cdots b_{j-1}) b_j \mid c$. In other words, $b_1 b_2 \cdots b_j \mid c$ (since $b_1 b_2 \cdots b_j = (b_1 b_2 \cdots b_{j-1}) b_j$). In other words, (364) holds for $i = j$. This completes the induction step. Thus, (364) is proven by induction.

Now, we can apply (364) to $i = k$. We thus obtain $b_1 b_2 \cdots b_k \mid c$. This proves Exercise 2.10.3. □

10.34. Solution to Exercise 2.10.4

Solution to Exercise 2.10.4. We have $a \perp b$. Thus, Exercise 2.10.2 (applied to n, b and $\left(\underbrace{a, a, \ldots, a}_{n \text{ times}}\right)$ instead of k, c and $(a_1, a_2, \ldots, a_k)$) yields that $\underbrace{aa \cdots a}_{n \text{ times}} \perp b$. In other words, $a^n \perp b$.

According to Proposition 2.10.4 (applied to a^n instead of a), we have $a^n \perp b$ if and only if $b \perp a^n$. Thus, $b \perp a^n$ (since $a^n \perp b$). Hence, Exercise 2.10.2 (applied to m, a^n and $\left(\underbrace{b, b, \ldots, b}_{m \text{ times}}\right)$ instead of k, c and $(a_1, a_2, \ldots, a_k)$) yields that $\underbrace{bb \cdots b}_{m \text{ times}} \perp a^n$. In other words, $b^m \perp a^n$.

According to Proposition 2.10.4 (applied to a^n and b^m instead of a and b), we have $a^n \perp b^m$ if and only if $b^m \perp a^n$. Hence, $a^n \perp b^m$ (since $b^m \perp a^n$). This solves Exercise 2.10.4. □

10.35. Solution to Exercise 2.10.5

Solution to Exercise 2.10.5. Exercise 2.10.2 and Exercise 2.10.5 say the same thing: They say that if c is a fixed integer, then a product of finitely many integers that are coprime to c will also be coprime to c. The difference between these two exercises is merely how the product is indexed. Thus, deriving Exercise 2.10.5 from Exercise 2.10.2 is merely a matter of bookkeeping. Let us do this bookkeeping:

By assumption, we have

$$b_i \perp c \qquad \text{for each } i \in I. \tag{365}$$

The set I is finite; thus, we can define some $k \in \mathbb{N}$ by $k = |I|$. Consider this k. There exists a bijection $f : \{1, 2, \ldots, k\} \to I$ (since $k = |I|$). Pick such an f. Thus, $f(1), f(2), \ldots, f(k)$ are the k elements of I; hence, $b_{f(1)}, b_{f(2)}, \ldots, b_{f(k)}$ are k integers. Moreover, each $j \in \{1, 2, \ldots, k\}$ satisfies $b_{f(j)} \perp c$ (by (365), applied to $i = f(j)$). Renaming the index j as i in this statement, we obtain: Each $i \in \{1, 2, \ldots, k\}$ satisfies $b_{f(i)} \perp c$. Hence, Exercise 2.10.2 (applied to $a_i = b_{f(i)}$) shows that

$$b_{f(1)} b_{f(2)} \cdots b_{f(k)} \perp c. \tag{366}$$

The map $f : \{1, 2, \ldots, k\} \to I$ is a bijection. Hence, we can substitute $f(j)$ for i in the product $\prod\limits_{i \in I} b_i$. We thus find

$$\prod_{i \in I} b_i = \prod_{j \in \{1,2,\ldots,k\}} b_{f(j)} = \prod_{j=1}^{k} b_{f(j)} = b_{f(1)} b_{f(2)} \cdots b_{f(k)}.$$

Thus, (366) can be rewritten as $\prod\limits_{i \in I} b_i \perp c$. This solves Exercise 2.10.5. □

10.36. Solution to Exercise 2.10.6

Solution to Exercise 2.10.6. Assume that $a \perp c$. But Proposition 2.10.4 (applied to c instead of b) shows that $a \perp c$ if and only if $c \perp a$. Thus, we have $c \perp a$ (since $a \perp c$). In other words, c is coprime to a. In other words, $\gcd(c, a) = 1$ (by the definition of "coprime").

But $a \equiv b \mod c$. Hence, Proposition 2.9.7 **(d)** (applied to c, a and b instead of a, b and c) yields $\gcd(c, a) = \gcd(c, b)$. Hence, $\gcd(c, b) = \gcd(c, a) = 1$. In other words, c is coprime to b. In other words, $c \perp b$. But Proposition 2.10.4 (applied to c instead of a) shows that $c \perp b$ if and only if $b \perp c$. Hence, $b \perp c$ (since $c \perp b$). This solves Exercise 2.10.6. □

10.37. Solution to Exercise 2.10.7

Solution to Exercise 2.10.7. Proposition 2.9.7 **(b)** (applied to $b - a$ instead of a) yields

$$\begin{aligned}
\gcd(b - a, b) &= \gcd\left(b, \underbrace{b - a}_{=1b+(-a)}\right) = \gcd(b, 1b + (-a)) \\
&= \gcd(b, -a) && \left(\begin{array}{c}\text{by Proposition 2.9.7 } \textbf{(c)}\text{,} \\ \text{applied to } b, -a \text{ and } 1 \text{ instead of } a, b \text{ and } u\end{array}\right) \\
&= \gcd(b, a) && \left(\begin{array}{c}\text{by Proposition 2.9.7 } \textbf{(h)}\text{,} \\ \text{applied to } b \text{ and } a \text{ instead of } a \text{ and } b\end{array}\right) \\
&= \gcd(a, b) && (\text{by Proposition 2.9.7 } \textbf{(b)}).
\end{aligned}$$

Now, we have the following chain of logical equivalences:

$$\begin{aligned}
(b - a \perp b) &\iff \left(\underbrace{\gcd(b - a, b)}_{=\gcd(a,b)} = 1\right) && (\text{by the definition of "coprime"}) \\
&\iff (\gcd(a, b) = 1) \iff (a \perp b) && (\text{by the definition of "coprime"}).
\end{aligned}$$

In other words, $b - a \perp b$ holds if and only if $a \perp b$. This solves Exercise 2.10.7. □

10.38. Solution to Exercise 2.10.8

Solution to Exercise 2.10.8. Proposition 2.10.12 yields $1+2+\cdots+n=\dfrac{n(n+1)}{2}$. Thus, we need to prove that

$$\frac{n(n+1)}{2} \mid 1^d+2^d+\cdots+n^d.$$

This is equivalent to

$$n(n+1) \mid 2\left(1^d+2^d+\cdots+n^d\right) \tag{367}$$

(by Exercise 2.2.3, applied to $a=\dfrac{n(n+1)}{2}$, $b=1^d+2^d+\cdots+n^d$ and $c=2$). Hence, it suffices to prove (367).

In order to prove (367), it suffices to show that

$$n \mid 2\left(1^d+2^d+\cdots+n^d\right) \qquad \text{and} \tag{368}$$

$$n+1 \mid 2\left(1^d+2^d+\cdots+n^d\right). \tag{369}$$

Indeed, the integers n and $n+1$ are coprime (by Example 2.10.2 **(c)**, applied to $a=n$); in other words, $n \perp n+1$. Hence, if we can prove (368) and (369), then Theorem 2.10.7 (applied to $a=n$, $b=n+1$ and $c=2\left(1^d+2^d+\cdots+n^d\right)$) will yield $n(n+1) \mid 2\left(1^d+2^d+\cdots+n^d\right)$; this will prove (367) and therefore complete our solution.

We shall prove (369) first:

Proof of (369): We have

$$\begin{aligned}2\left(1^d+2^d+\cdots+n^d\right) &= \left(1^d+2^d+\cdots+n^d\right)+\left(1^d+2^d+\cdots+n^d\right)\\ &= \left(1^d+2^d+\cdots+n^d\right)+\left(n^d+(n-1)^d+\cdots+1^d\right)\\ &= \sum_{k=1}^{n} k^d+\sum_{k=1}^{n}(n+1-k)^d\\ &= \sum_{k=1}^{n}\left(k^d+(n+1-k)^d\right).\end{aligned} \tag{370}$$

But if $k\in\mathbb{Z}$, then Lemma 2.10.11 **(b)** (applied to $x=k$ and $y=n+1-k$) shows that $k^d+(n+1-k)^d$ is divisible by $k+(n+1-k)=n+1$. Hence, each addend in the sum on the right hand side of (370) is divisible by $n+1$. Therefore, the whole sum is divisible by $n+1$ as well. Thus, the left hand side is divisible by $n+1$, too. In other words, $n+1 \mid 2\left(1^d+2^d+\cdots+n^d\right)$. Thus, (369) is proven.

Proof of (368): If $n=0$, then (368) boils down to $0 \mid 2\cdot 0$ (since empty sums are 0); this is obvious. Thus, for the rest of this proof, we WLOG assume that $n\neq 0$. Hence, n is a positive integer, and thus $n-1\in\mathbb{N}$. Therefore, we can apply (369) to $n-1$ instead of n (since we have already proven (369) for each $n\in\mathbb{N}$). We thus obtain

$$n \mid 2\left(1^d+2^d+\cdots+(n-1)^d\right).$$

In other words, $2\left(1^d + 2^d + \cdots + (n-1)^d\right) \equiv 0 \mod n$. Now,

$$\begin{aligned}
&2\left(1^d + 2^d + \cdots + n^d\right) - 2\left(1^d + 2^d + \cdots + (n-1)^d\right) \\
&= 2 \cdot \underbrace{\left(\left(1^d + 2^d + \cdots + n^d\right) - \left(1^d + 2^d + \cdots + (n-1)^d\right)\right)}_{=n^d} \\
&= 2n^d = n \cdot 2n^{d-1} \qquad (\text{since } d \geq 1 \text{ (because } d \text{ is odd))}
\end{aligned}$$

is clearly divisible by n. In other words,

$$2\left(1^d + 2^d + \cdots + n^d\right) \equiv 2\left(1^d + 2^d + \cdots + (n-1)^d\right) \mod n.$$

Hence,

$$2\left(1^d + 2^d + \cdots + n^d\right) \equiv 2\left(1^d + 2^d + \cdots + (n-1)^d\right) \equiv 0 \mod n.$$

That is, $n \mid 2\left(1^d + 2^d + \cdots + n^d\right)$. This proves (368).

We have now proven both (368) and (369). As we have explained, this yields (367), which in turn solves Exercise 2.10.8. □

10.39. Solution to Exercise 2.10.9

Solution to Exercise 2.10.9. Proposition 2.9.28 yields $\gcd(a,b) \mid xa + yb = 1$. But $\gcd(a,b)$ is a nonnegative integer. Hence, Exercise 2.2.5 (applied to $g = \gcd(a,b)$) yields $\gcd(a,b) = 1$ (since $\gcd(a,b) \mid 1$). In other words, a is coprime to b. In other words, $a \perp b$. This solves Exercise 2.10.9. □

10.40. Solution to Exercise 2.10.10

Solution to Exercise 2.10.10. Let $g = \gcd(x,y)$. Then, g is a nonnegative integer (since any gcd is a nonnegative integer); thus, $|g| = g$.

Theorem 2.9.26 (applied to 2, (ux, uy), 2 and (vx, vy) instead of k, $(b_1, b_2, \ldots, b_k)$, ℓ and $(c_1, c_2, \ldots, c_\ell)$) yields

$$\gcd(ux, uy, vx, vy) = \gcd(\gcd(ux, uy), \gcd(vx, vy)). \tag{371}$$

Theorem 2.9.20 (applied to $s = u$, $a = x$ and $b = y$) yields

$$\gcd(ux, uy) = |u| \underbrace{\gcd(x,y)}_{=g} = |u|\, g = g\, |u|.$$

The same argument (applied to v instead of u) yields

$$\gcd(vx, vy) = g\, |v|.$$

Now, (371) becomes

$$\begin{aligned}\gcd(ux,uy,vx,vy) &= \gcd\left(\underbrace{\gcd(ux,uy)}_{=g|u|},\underbrace{\gcd(vx,vy)}_{=g|v|}\right) = \gcd(g|u|,g|v|)\\ &= \underbrace{|g|}_{\substack{=g\\ =\gcd(x,y)}} \underbrace{\gcd(|u|,|v|)}_{\substack{=\gcd(u,v)\\ \text{(by Exercise 2.9.5 (c),}\\ \text{applied to } a=u \text{ and } b=v)}}\\ &\qquad \left(\text{by Theorem 2.9.20, applied to } s=g,\ a=|u| \text{ and } b=|v|\right)\\ &= \gcd(x,y)\cdot\gcd(u,v) = \gcd(u,v)\cdot\gcd(x,y).\end{aligned}$$

This solves Exercise 2.10.10. □

10.41. Solution to Exercise 2.10.11

Solution to Exercise 2.10.11. **(a)** Let $g=\gcd(a,b,c)$. Then, $g=\gcd(a,b,c)\geq 0$ (since any gcd is a nonnegative integer) and thus $|g|=g$. But Exercise 2.9.6 (applied to $s=a$) yields

$$\gcd(aa,ab,ac) = |a|\underbrace{\gcd(a,b,c)}_{=g=|g|} = |a|\cdot|g| = |ag| \tag{372}$$

(since (3) yields $|ag|=|a|\cdot|g|$).

Exercise 2.10.10 (applied to $u=a$, $v=c$, $x=a$ and $y=b$) yields

$$\begin{aligned}&\gcd(a,c)\cdot\gcd(a,b)\\ &= \gcd\left(aa,ab,\underbrace{ca}_{=ac},\underbrace{cb}_{=bc}\right) = \gcd(aa,ab,ac,bc) = \gcd\left(\underbrace{\gcd(aa,ab,ac)}_{\substack{=|ag|\\ \text{(by (372))}}},bc\right)\\ &\qquad \left(\begin{array}{c}\text{by Theorem 2.9.21 (d)}\\ \text{(applied to 4 and } (aa,ab,ac,bc) \text{ instead of } k \text{ and } (b_1,b_2,\ldots,b_k))\end{array}\right)\\ &= \gcd(|ag|,bc) = \gcd(ag,bc)\end{aligned}$$

(by Exercise 2.9.5 **(b)**, applied to ag and bc instead of a and b). In other words, $\gcd(a,b)\cdot\gcd(a,c)=\gcd(ag,bc)$. This solves Exercise 2.10.11 **(a)**.

(b) Assume that $b\perp c$. Thus, $\gcd(b,c)=1$.

Let $g=\gcd(a,b,c)$. Theorem 2.9.26 (applied to 1, (a), 2 and (b,c) instead of k, $(b_1,b_2,\ldots,b_k)$, ℓ and $(c_1,c_2,\ldots,c_\ell)$) yields

$$\gcd(a,b,c) = \gcd\left(\gcd(a),\underbrace{\gcd(b,c)}_{=1}\right) = \gcd(\gcd(a),1) \mid 1$$

(by Proposition 2.9.7 **(f)**, applied to $\gcd(a)$ and 1 instead of a and b). This rewrites as $g\mid 1$ (since $g=\gcd(a,b,c)$).

But $g = \gcd(a,b,c)$ is a nonnegative integer (since any gcd is a nonnegative integer). Hence, Exercise 2.2.5 yields $g = 1$ (since $g \mid 1$). Now, Exercise 2.10.11 **(a)** yields

$$\gcd(a,b) \cdot \gcd(a,c) = \gcd\left(a \underbrace{g}_{=1}, bc\right) = \gcd(a,bc).$$

This solves Exercise 2.10.11 **(b)**. □

10.42. Solution to Exercise 2.10.12

Solution to Exercise 2.10.12. We have assumed that a and b are not both zero. In other words, the two integers a, b are not all zero. Hence, Definition 2.9.6 shows that $\gcd(a,b)$ is defined as the largest element of the set $\operatorname{Div}(a,b)$ and is a positive integer.

Now, $g = \gcd(a,b)$. Hence, g is a positive integer (since $\gcd(a,b)$ is a positive integer). Thus, $|g| = g$. Also, $g \neq 0$ (since g is positive).

Proposition 2.9.7 **(f)** yields $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$. Hence, $g = \gcd(a,b) \mid a$. But Proposition 2.2.3 **(c)** (applied to g and a instead of a and b) shows that $g \mid a$ if and only if $\frac{a}{g} \in \mathbb{Z}$. Hence, we have $\frac{a}{g} \in \mathbb{Z}$ (since $g \mid a$). Similarly, $\frac{b}{g} \in \mathbb{Z}$. Thus, $\frac{a}{g}$ and $\frac{b}{g}$ are integers.

It remains to prove that $\frac{a}{g} \perp \frac{b}{g}$. But Theorem 2.9.20 (applied to g, $\frac{a}{g}$ and $\frac{b}{g}$ instead of s, a and b) shows that

$$\gcd\left(g \cdot \frac{a}{g}, g \cdot \frac{b}{g}\right) = \underbrace{|g|}_{=g} \gcd\left(\frac{a}{g}, \frac{b}{g}\right) = g \gcd\left(\frac{a}{g}, \frac{b}{g}\right).$$

Comparing this with

$$\gcd\left(\underbrace{g \cdot \frac{a}{g}}_{=a}, \underbrace{g \cdot \frac{b}{g}}_{=b}\right) = \gcd(a,b) = g,$$

we obtain $g \gcd\left(\frac{a}{g}, \frac{b}{g}\right) = g$. We can cancel g from this equality (since $g \neq 0$), and thus obtain $\gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$. In other words, $\frac{a}{g} \perp \frac{b}{g}$. Thus, the solution of Exercise 2.10.12 is finished. □

10.43. Solution to Exercise 2.10.13

Solution to Exercise 2.10.13. If $k = 0$, then Exercise 2.10.13 holds[251]. Hence, for the rest of this solution, we WLOG assume that $k \neq 0$. Thus, k is a positive integer (since $k \in \mathbb{N}$); therefore, $0^k = 0$.

[251] *Proof.* Assume that $k = 0$. Thus, $(\gcd(a,b))^k = (\gcd(a,b))^0 = 1$.

If the integers a and b are both zero, then Exercise 2.10.13 holds[252]. Thus, for the rest of this solution, we WLOG assume that a and b are not both zero. Let $g = \gcd(a, b)$. Then, $g \geq 0$ (since any gcd is nonnegative) and therefore $g^k \geq 0$. But Exercise 2.10.12 yields that $\frac{a}{g}$ and $\frac{b}{g}$ are integers satisfying $\frac{a}{g} \perp \frac{b}{g}$. Therefore, Exercise 2.10.4 (applied to $\frac{a}{g}$, $\frac{b}{g}$, k and k instead of a, b, n and m) yields $\left(\frac{a}{g}\right)^k \perp \left(\frac{b}{g}\right)^k$. In other words, $\gcd\left(\left(\frac{a}{g}\right)^k, \left(\frac{b}{g}\right)^k\right) = 1$.

Note that $\left(\frac{a}{g}\right)^k$ and $\left(\frac{b}{g}\right)^k$ are integers (since $\frac{a}{g}$ and $\frac{b}{g}$ are integers). Thus, Theorem 2.9.20 (applied to g^k, $\left(\frac{a}{g}\right)^k$ and $\left(\frac{b}{g}\right)^k$ instead of s, a and b) yields

$$\gcd\left(g^k\left(\frac{a}{g}\right)^k, g^k\left(\frac{b}{g}\right)^k\right) = \underbrace{\left|g^k\right|}_{\substack{=g^k \\ (\text{since } g^k \geq 0)}} \underbrace{\gcd\left(\left(\frac{a}{g}\right)^k, \left(\frac{b}{g}\right)^k\right)}_{=1} = g^k = (\gcd(a, b))^k$$

(since $g = \gcd(a, b)$). Comparing this with

$$\gcd\left(\underbrace{g^k\left(\frac{a}{g}\right)^k}_{=a^k}, \underbrace{g^k\left(\frac{b}{g}\right)^k}_{=b^k}\right) = \gcd\left(a^k, b^k\right),$$

we obtain $\gcd\left(a^k, b^k\right) = (\gcd(a, b))^k$. This solves Exercise 2.10.13. □

10.44. Solution to Exercise 2.10.14

Solution to Exercise 2.10.14. We have $r \in \mathbb{Q}$. In other words, r is a rational number. Thus, r can be written in the form $r = x/y$ for some $x \in \mathbb{Z}$ and some nonzero $y \in \mathbb{Z}$ (by the

But $1 \mid 1$. Thus, Proposition 2.9.7 **(i)** (applied to 1 and 1 instead of a and b) yields $\gcd(1, 1) = |1| = 1$. From $k = 0$, we obtain $\gcd\left(a^k, b^k\right) = \gcd\left(\underbrace{a^0}_{=1}, \underbrace{b^0}_{=1}\right) = \gcd(1, 1) = 1$. Comparing this with $(\gcd(a, b))^k = 1$, we obtain $\gcd\left(a^k, b^k\right) = (\gcd(a, b))^k$. Hence, Exercise 2.10.13 holds (under the assumption that $k = 0$).

[252] *Proof.* Assume that a and b are both zero. In other words, $a = 0$ and $b = 0$. Thus,

$$\gcd\left(a^k, b^k\right) = \gcd\left(\underbrace{0^k}_{=0}, \underbrace{0^k}_{=0}\right) = \gcd(0, 0) = |0|$$

(by Proposition 2.9.7 **(i)**, applied to 0 and 0 instead of a and b). Thus, $\gcd\left(a^k, b^k\right) = |0| = 0$.

But the integers a, b are all zero (since $a = 0$ and $b = 0$). Thus, the definition of gcd yields $\gcd(a, b) = 0$. Hence, $(\gcd(a, b))^k = 0^k = 0$. Comparing this with $\gcd\left(a^k, b^k\right) = 0$, we obtain $\gcd\left(a^k, b^k\right) = (\gcd(a, b))^k$. Hence, Exercise 2.10.13 holds (under the assumption that a and b are both zero).

definition of a rational number). Consider these x and y. The integers x and y are not both zero (since y is nonzero). Let $g = \gcd(x, y)$. Exercise 2.10.12 (applied to $a = x$ and $b = y$) yields that $\dfrac{x}{g}$ and $\dfrac{y}{g}$ are integers satisfying $\dfrac{x}{g} \perp \dfrac{y}{g}$. These two integers $\dfrac{x}{g}$ and $\dfrac{y}{g}$ are coprime (since $\dfrac{x}{g} \perp \dfrac{y}{g}$) and satisfy $r = \dfrac{x}{g} / \dfrac{y}{g}$ (since $\dfrac{x}{g} / \dfrac{y}{g} = x/y = r$). Hence, there exist two **coprime** integers a and b satisfying $r = a/b$ (namely, $a = \dfrac{x}{g}$ and $b = \dfrac{y}{g}$). This solves Exercise 2.10.14. □

10.45. Solution to Exercise 2.10.15

Solution to Exercise 2.10.15. **(a)** Let u be a positive integer that is not a perfect square. We must prove that $\sqrt{u}$ is irrational.

Assume the contrary. Thus, $\sqrt{u}$ is rational. In other words, $\sqrt{u} \in \mathbb{Q}$. Hence, Exercise 2.10.14 (applied to $r = \sqrt{u}$) yields that there exist two **coprime** integers a and b satisfying $\sqrt{u} = a/b$. Consider these a and b.

We have $a \perp b$ (since a and b are coprime). Thus, Exercise 2.10.4 (applied to $n = 2$ and $m = 2$) yields $a^2 \perp b^2$. In other words, $b^2 \perp a^2$ (by Proposition 2.10.4). In other words, $\gcd\left(b^2, a^2\right) = 1$. Also, b^2 is nonnegative (since the square of any real number is nonnegative).

Squaring both sides of the equality $\sqrt{u} = a/b$, we obtain $u = (a/b)^2 = a^2/b^2$, so that $a^2 = b^2 u$. Hence, $b^2 \mid a^2$ (since u is an integer). Thus, Proposition 2.9.7 **(i)** (applied to b^2 and a^2 instead of a and b) yields $\gcd\left(b^2, a^2\right) = \left|b^2\right| = b^2$ (since b^2 is nonnegative). Comparing this with $\gcd\left(b^2, a^2\right) = 1$, we obtain $b^2 = 1$. Hence, $u = a^2 / \underbrace{b^2}_{=1} = a^2$. Thus, u is a perfect square (since a is an integer). This contradicts the fact that u is not a perfect square.

This contradiction shows that our assumption was false. Hence, $\sqrt{u}$ is irrational. This solves Exercise 2.10.15 **(a)**.

(b) Let u and v be two positive integers that are not both perfect squares. We must prove that $\sqrt{u} + \sqrt{v}$ is irrational.

Assume the contrary. Thus, $\sqrt{u} + \sqrt{v}$ is rational. Denote this rational number $\sqrt{u} + \sqrt{v}$ by x. Thus, $x = \sqrt{u} + \sqrt{v}$, so that $x - \sqrt{u} = \sqrt{v}$. Squaring both sides of this equality, we obtain $\left(x - \sqrt{u}\right)^2 = v$. Hence,

$$v = \left(x - \sqrt{u}\right)^2 = x^2 - 2x\sqrt{u} + \left(\sqrt{u}\right)^2 = x^2 - 2x\sqrt{u} + u.$$

Subtracting $x^2 + u$ from both sides of this equation, we obtain

$$v - \left(x^2 + u\right) = -2x\sqrt{u}. \tag{373}$$

But $x = \sqrt{u} + \sqrt{v} > 0$ (since u and v are positive) and thus $x \neq 0$, so that $-2x \neq 0$. Hence, we can solve the equation (373) for $\sqrt{u}$; we thus obtain

$$\sqrt{u} = \frac{v - \left(x^2 + u\right)}{-2x}.$$

Thus, $\sqrt{u}$ is rational (since v, x and u are rational). Therefore, u must be a perfect square (since otherwise, Exercise 2.10.15 **(a)** would yield that $\sqrt{u}$ is irrational). Similarly, v must be a perfect square. This shows that both u and v are perfect squares; but this contradicts the fact that u and v are not both perfect squares.

This contradiction shows that our assumption was false. Hence, $\sqrt{u}+\sqrt{v}$ is irrational. This solves Exercise 2.10.15 **(b)**. □

10.46. Solution to Exercise 2.10.16

Solution to Exercise 2.10.16. A gcd of a list of integers is always a nonnegative integer (by the definition of a gcd). Hence, in particular, $\gcd(a_1, a_2, \ldots, a_k)$ is a nonnegative integer. Thus, we can define a nonnegative integer h by $h = \gcd(a_1, a_2, \ldots, a_k)$. Consider this h. We have $|h| = h$ (since h is nonnegative).

Theorem 2.9.26 (applied to $(a_1x, a_2x, \ldots, a_kx)$, k and $(a_1y, a_2y, \ldots, a_ky)$ instead of $(b_1, b_2, \ldots, b_k)$, ℓ and $(c_1, c_2, \ldots, c_\ell)$) yields

$$\begin{aligned}&\gcd(a_1x, a_2x, \ldots, a_kx, a_1y, a_2y, \ldots, a_ky)\\&= \gcd(\gcd(a_1x, a_2x, \ldots, a_kx), \gcd(a_1y, a_2y, \ldots, a_ky)). \qquad (374)\end{aligned}$$

But $(a_1x, a_2x, \ldots, a_kx) = (xa_1, xa_2, \ldots, xa_k)$ (since $a_ix = xa_i$ for each $i \in \{1, 2, \ldots, k\}$) and thus

$$\begin{aligned}\gcd(a_1x, a_2x, \ldots, a_kx) = \gcd(xa_1, xa_2, \ldots, xa_k) &= |x| \gcd(a_1, a_2, \ldots, a_k)\\&\qquad (\text{by Exercise 2.9.7, applied to } s = x).\end{aligned}$$

Comparing this with

$$\begin{aligned}|xh| &= |x| \cdot \underbrace{|h|}_{=h} \qquad (\text{by (3) (applied to } h \text{ instead of } y))\\&= |x| \cdot \underbrace{h}_{=\gcd(a_1,a_2,\ldots,a_k)} = |x| \gcd(a_1, a_2, \ldots, a_k),\end{aligned}$$

we obtain

$$\gcd(a_1x, a_2x, \ldots, a_kx) = |xh|.$$

The same argument (applied to y instead of x) yields

$$\gcd(a_1y, a_2y, \ldots, a_ky) = |yh|.$$

Thus, (374) becomes

$$\begin{aligned}
&\gcd\left(a_1x, a_2x, \ldots, a_kx, a_1y, a_2y, \ldots, a_ky\right)\\
&= \gcd\left(\underbrace{\gcd\left(a_1x, a_2x, \ldots, a_kx\right)}_{=|xh|}, \underbrace{\gcd\left(a_1y, a_2y, \ldots, a_ky\right)}_{=|yh|}\right) = \gcd\left(|xh|, |yh|\right)\\
&= \gcd\left(\underbrace{xh}_{=hx}, \underbrace{yh}_{=hy}\right) \qquad \left(\begin{array}{c}\text{by Exercise 2.9.5 \textbf{(c)} (applied to } xh \text{ and } yh\\ \text{instead of } a \text{ and } b\text{)}\end{array}\right)\\
&= \gcd\left(hx, hy\right) = \underbrace{|h|}_{=h} \gcd\left(x, y\right) \qquad \left(\begin{array}{c}\text{by Theorem 2.9.20 (applied to } h\text{, } x \text{ and } y\\ \text{instead of } s\text{, } a \text{ and } b\text{)}\end{array}\right)\\
&= \underbrace{h}_{=\gcd(a_1,a_2,\ldots,a_k)} \gcd\left(x, y\right) = \gcd\left(a_1, a_2, \ldots, a_k\right) \cdot \gcd\left(x, y\right).
\end{aligned}$$

This solves Exercise 2.10.16. □

10.47. Solution to Exercise 2.10.17

Solution to Exercise 2.10.17. Theorem 2.9.21 **(d)** (applied to 3 and (x, y, z) instead of k and $(b_1, b_2, \ldots, b_k)$) yields $\gcd(x, y, z) = \gcd(\gcd(x, y), z)$. But Exercise 2.9.5 **(a)** (applied to $\gcd(x, y)$ and z instead of a and b) yields $\gcd(\gcd(x, y), |z|) = \gcd(\gcd(x, y), z)$. Comparing these two equalities, we obtain

$$\gcd\left(\gcd\left(x, y\right), |z|\right) = \gcd\left(x, y, z\right). \tag{375}$$

A gcd of a list of integers is always a nonnegative integer (by the definition of a gcd). Hence, in particular, $\gcd(a_1, a_2, \ldots, a_k)$ is a nonnegative integer. Thus, we can define a nonnegative integer h by $h = \gcd(a_1, a_2, \ldots, a_k)$. Consider this h. We have $|h| = h$ (since h is nonnegative).

Multiplying both sides of the equality $h = \gcd(a_1, a_2, \ldots, a_k)$ by $\gcd(x, y)$, we obtain

$$\begin{aligned}
h \gcd\left(x, y\right) &= \gcd\left(a_1, a_2, \ldots, a_k\right) \cdot \gcd\left(x, y\right)\\
&= \gcd\left(a_1x, a_2x, \ldots, a_kx, a_1y, a_2y, \ldots, a_ky\right)
\end{aligned} \tag{376}$$

(by Exercise 2.10.16).

But $(a_1z, a_2z, \ldots, a_kz) = (za_1, za_2, \ldots, za_k)$ (since $a_iz = za_i$ for each $i \in \{1, 2, \ldots, k\}$) and thus

$$\gcd\left(a_1z, a_2z, \ldots, a_kz\right) = \gcd\left(za_1, za_2, \ldots, za_k\right) = |z| \gcd\left(a_1, a_2, \ldots, a_k\right)$$

(by Exercise 2.9.7, applied to $s = z$). Thus,

$$\gcd\left(a_1z, a_2z, \ldots, a_kz\right) = |z| \underbrace{\gcd\left(a_1, a_2, \ldots, a_k\right)}_{=h} = |z| h = h |z|. \tag{377}$$

Theorem 2.9.26 (applied to $2k$, $(a_1x, a_2x, \ldots, a_kx, a_1y, a_2y, \ldots, a_ky)$, k and $(a_1z, a_2z, \ldots, a_kz)$ instead of k, $(b_1, b_2, \ldots, b_k)$, ℓ and $(c_1, c_2, \ldots, c_\ell)$) yields

$$\begin{aligned}
&\gcd(a_1x, a_2x, \ldots, a_kx, a_1y, a_2y, \ldots, a_ky, a_1z, a_2z, \ldots, a_kz) \\
&= \gcd\left(\underbrace{\gcd(a_1x, a_2x, \ldots, a_kx, a_1y, a_2y, \ldots, a_ky)}_{\substack{=h\gcd(x,y) \\ \text{(by (376))}}}, \underbrace{\gcd(a_1z, a_2z, \ldots, a_kz)}_{\substack{=h|z| \\ \text{(by (377))}}}\right) \\
&= \gcd(h\gcd(x,y), h|z|) = \underbrace{|h|}_{\substack{=h \\ =\gcd(a_1,a_2,\ldots,a_k)}} \underbrace{\gcd(\gcd(x,y), |z|)}_{\substack{=\gcd(x,y,z) \\ \text{(by (375))}}} \\
&\qquad \text{(by Theorem 2.9.20 (applied to } h,\ \gcd(x,y) \text{ and } |z| \text{ instead of } s,\ a \text{ and } b)) \\
&= \gcd(a_1, a_2, \ldots, a_k) \cdot \gcd(x, y, z).
\end{aligned}$$

This solves Exercise 2.10.17. □

10.48. Solution to Exercise 2.10.18

Solution to Exercise 2.10.18. Exercise 2.10.10 (applied to $u = b$, $v = c$, $x = c$ and $y = a$) yields

$$\gcd(b,c) \cdot \gcd(c,a) = \gcd(bc, ba, cc, ca). \tag{378}$$

Multiplying both sides of this equality by $\gcd(a,b)$, we find

$$\begin{aligned}
&\gcd(b,c) \cdot \gcd(c,a) \cdot \gcd(a,b) \\
&= \gcd(bc, ba, cc, ca) \cdot \gcd(a,b) \\
&= \gcd(bca, baa, cca, caa, bcb, bab, ccb, cab)
\end{aligned} \tag{379}$$

(by Exercise 2.10.16, applied to a, b, 4 and (bc, ba, cc, ca) instead of x, y, k and $(a_1, a_2, \ldots, a_k)$).

On the other hand, Exercise 2.10.17 (applied to bc, ca, ab, 3 and (a,b,c) instead of x, y, z, k and $(a_1, a_2, \ldots, a_k)$) yields

$$\begin{aligned}
&\gcd(a,b,c) \cdot \gcd(bc, ca, ab) \\
&= \gcd(abc, bbc, cbc, aca, bca, cca, aab, bab, cab).
\end{aligned} \tag{380}$$

But comparing

$$\begin{aligned}
&\left\{\underbrace{bca}_{=abc}, \underbrace{baa}_{=a^2b}, \underbrace{cca}_{=c^2a}, \underbrace{caa}_{=a^2c}, \underbrace{bcb}_{=b^2c}, \underbrace{bab}_{=b^2a}, \underbrace{ccb}_{=c^2b}, \underbrace{cab}_{=abc}\right\} \\
&= \left\{abc, a^2b, c^2a, a^2c, b^2c, b^2a, c^2b, abc\right\} = \left\{abc, b^2c, c^2b, c^2a, a^2c, a^2b, b^2a\right\}
\end{aligned}$$

with

$$\begin{aligned}
&\left\{abc, \underbrace{bbc}_{=b^2c}, \underbrace{cbc}_{=c^2b}, \underbrace{aca}_{=a^2c}, \underbrace{bca}_{=abc}, \underbrace{cca}_{=c^2a}, \underbrace{aab}_{=a^2b}, \underbrace{bab}_{=b^2a}, \underbrace{cab}_{=abc}\right\} \\
&= \left\{abc, b^2c, c^2b, a^2c, abc, c^2a, a^2b, b^2a, abc\right\} = \left\{abc, b^2c, c^2b, c^2a, a^2c, a^2b, b^2a\right\},
\end{aligned}$$

we obtain

$$\{bca, baa, cca, caa, bcb, bab, ccb, cab\} = \{abc, bbc, cbc, aca, bca, cca, aab, bab, cab\}.$$

Hence, Exercise 2.9.2 (applied to 8, $(bca, baa, cca, caa, bcb, bab, ccb, cab)$, 9 and $(abc, bbc, cbc, aca, bca, cca, aab, bab, cab)$ instead of k, $(b_1, b_2, \ldots, b_k)$, ℓ and $(c_1, c_2, \ldots, c_\ell)$) yields

$$\gcd(bca, baa, cca, caa, bcb, bab, ccb, cab) = \gcd(abc, bbc, cbc, aca, bca, cca, aab, bab, cab).$$

Comparing this with (380), we obtain

$$\gcd(a,b,c) \cdot \gcd(bc, ca, ab) = \gcd(bca, baa, cca, caa, bcb, bab, ccb, cab).$$

Comparing this with (379), we obtain

$$\gcd(b,c) \cdot \gcd(c,a) \cdot \gcd(a,b) = \gcd(a,b,c) \cdot \gcd(bc, ca, ab).$$

This solves Exercise 2.10.18. □

10.49. Solution to Exercise 2.11.1

Solution to Exercise 2.11.1. The lowest common multiple of any set of integers is a nonnegative integer (by Definition 2.11.4). Thus, in particular, $\operatorname{lcm}(a,b)$ and $\operatorname{lcm}(b,a)$ and $\operatorname{lcm}(-a,b)$ are nonnegative integers.

(a) Proposition 2.11.5 **(c)** (applied to b and a instead of a and b) yields $b \mid \operatorname{lcm}(b,a)$ and $a \mid \operatorname{lcm}(b,a)$. Thus, $a \mid \operatorname{lcm}(b,a)$ and $b \mid \operatorname{lcm}(b,a)$. Hence, Lemma 2.11.8 (applied to $m = \operatorname{lcm}(b,a)$) yields $\operatorname{lcm}(a,b) \mid \operatorname{lcm}(b,a)$. The same argument (applied to b and a instead of a and b) yields $\operatorname{lcm}(b,a) \mid \operatorname{lcm}(a,b)$. Hence, Exercise 2.2.2 (applied to $\operatorname{lcm}(a,b)$ and $\operatorname{lcm}(b,a)$ instead of a and b) yields $|\operatorname{lcm}(a,b)| = |\operatorname{lcm}(b,a)| = \operatorname{lcm}(b,a)$ (since $\operatorname{lcm}(b,a)$ is nonnegative). But $\operatorname{lcm}(a,b)$ is nonnegative; thus, $|\operatorname{lcm}(a,b)| = \operatorname{lcm}(a,b)$. Hence, $\operatorname{lcm}(a,b) = |\operatorname{lcm}(a,b)| = \operatorname{lcm}(b,a)$. This solves Exercise 2.11.1 **(a)**.

(b) Proposition 2.11.5 **(c)** (applied to $-a$ instead of a) yields $-a \mid \operatorname{lcm}(-a,b)$ and $b \mid \operatorname{lcm}(-a,b)$. But $a \mid -a$ (since $-a = a \cdot (-1)$). Thus, $a \mid -a \mid \operatorname{lcm}(-a,b)$ and $b \mid \operatorname{lcm}(-a,b)$. Hence, Lemma 2.11.8 (applied to $m = \operatorname{lcm}(-a,b)$) yields $\operatorname{lcm}(a,b) \mid \operatorname{lcm}(-a,b)$. The same argument (applied to $-a$ instead of a) yields $\operatorname{lcm}(-a,b) \mid \operatorname{lcm}(-(-a),b)$. In view of $-(-a) = a$, this rewrites as $\operatorname{lcm}(-a,b) \mid \operatorname{lcm}(a,b)$. Hence, Exercise 2.2.2 (applied to $\operatorname{lcm}(a,b)$ and $\operatorname{lcm}(-a,b)$ instead of a and b) yields $|\operatorname{lcm}(a,b)| = |\operatorname{lcm}(-a,b)| = \operatorname{lcm}(-a,b)$ (since $\operatorname{lcm}(-a,b)$ is nonnegative). But $\operatorname{lcm}(a,b)$ is nonnegative; thus, $|\operatorname{lcm}(a,b)| = \operatorname{lcm}(a,b)$. Hence, $\operatorname{lcm}(a,b) = |\operatorname{lcm}(a,b)| = \operatorname{lcm}(-a,b)$. This solves Exercise 2.11.1 **(b)**.

(c) Exercise 2.11.1 **(a)** (applied to $-b$ instead of b) yields $\operatorname{lcm}(a,-b) = \operatorname{lcm}(-b,a) = \operatorname{lcm}(b,a)$ (by Exercise 2.11.1 **(b)**, applied to b and a instead of a and b). But Exercise 2.11.1 **(a)** yields $\operatorname{lcm}(a,b) = \operatorname{lcm}(b,a) = \operatorname{lcm}(a,-b)$ (since $\operatorname{lcm}(a,-b) = \operatorname{lcm}(b,a)$). This solves Exercise 2.11.1 **(c)**.

(d) Assume that $a \mid b$. Thus, $a \mid b$ and $b \mid b$. Hence, Lemma 2.11.8 (applied to $m = b$) yields $\operatorname{lcm}(a,b) \mid b$. But Proposition 2.11.5 **(c)** yields $a \mid \operatorname{lcm}(a,b)$ and $b \mid \operatorname{lcm}(a,b)$. Hence, Exercise 2.2.2 (applied to b and $\operatorname{lcm}(a,b)$ instead of a and b) yields $|b| = |\operatorname{lcm}(a,b)| = \operatorname{lcm}(a,b)$ (since $\operatorname{lcm}(a,b)$ is nonnegative). In other words, $\operatorname{lcm}(a,b) = |b|$. This solves Exercise 2.11.1 **(d)**.

(e) If $s = 0$, then Exercise 2.11.1 **(e)** holds[253]. Hence, for the rest of this solution, we WLOG assume that $s \neq 0$.

Recall that any lcm is a nonnegative integer. Thus, $\operatorname{lcm}(sa, sb)$ is a nonnegative integer.

Proposition 2.11.5 **(c)** (applied to sa and sb instead of a and b) yields $sa \mid \operatorname{lcm}(sa, sb)$ and $sb \mid \operatorname{lcm}(sa, sb)$. Hence, $s \mid sa \mid \operatorname{lcm}(sa, sb)$. In other words, there exists some integer d such that $\operatorname{lcm}(sa, sb) = sd$. Consider this d.

Now, $as = sa \mid \operatorname{lcm}(sa, sb) = sd = ds$. But Exercise 2.2.3 (applied to a, d and s instead of a, b and c) yields that $a \mid d$ holds if and only if $as \mid ds$. Thus, we have $a \mid d$ (since $as \mid ds$).

Also, $bs = sb \mid \operatorname{lcm}(sa, sb) = sd = ds$. But Exercise 2.2.3 (applied to b, d and s instead of a, b and c) yields that $b \mid d$ holds if and only if $bs \mid ds$. Thus, we have $b \mid d$ (since $bs \mid ds$).

From $a \mid d$ and $b \mid d$, we obtain $\operatorname{lcm}(a, b) \mid d$ (by Lemma 2.11.8, applied to $m = d$). Hence, Proposition 2.2.4 **(c)** (applied to $a_1 = s$, $a_2 = \operatorname{lcm}(a, b)$, $b_1 = s$ and $b_2 = d$) yields $s \operatorname{lcm}(a, b) \mid sd$ (since $s \mid s$). In view of $\operatorname{lcm}(sa, sb) = sd$, this rewrites as $s \operatorname{lcm}(a, b) \mid \operatorname{lcm}(sa, sb)$.

Proposition 2.11.5 **(c)** yields $a \mid \operatorname{lcm}(a, b)$ and $b \mid \operatorname{lcm}(a, b)$. Hence, Proposition 2.2.4 **(c)** (applied to $a_1 = s$, $a_2 = a$, $b_1 = s$ and $b_2 = \operatorname{lcm}(a, b)$) yields $sa \mid s \operatorname{lcm}(a, b)$ (since $s \mid s$ and $a \mid \operatorname{lcm}(a, b)$). Similarly, we obtain $sb \mid s \operatorname{lcm}(a, b)$ (since $s \mid s$ and $b \mid \operatorname{lcm}(a, b)$). Hence, Lemma 2.11.8 (applied to sa, sb and $s \operatorname{lcm}(a, b)$ instead of a, b and m) yields that $\operatorname{lcm}(sa, sb) \mid s \operatorname{lcm}(a, b)$.

Now, we know that $s \operatorname{lcm}(a, b) \mid \operatorname{lcm}(sa, sb)$ and $\operatorname{lcm}(sa, sb) \mid s \operatorname{lcm}(a, b)$. Hence, Exercise 2.2.2 (applied to $s \operatorname{lcm}(a, b)$ and $\operatorname{lcm}(sa, sb)$ instead of a and b) yields $|s \operatorname{lcm}(a, b)| = |\operatorname{lcm}(sa, sb)| = \operatorname{lcm}(sa, sb)$ (since $\operatorname{lcm}(sa, sb)$ is nonnegative). Hence,

$$\begin{aligned} \operatorname{lcm}(sa, sb) &= |s \operatorname{lcm}(a, b)| = |s| \cdot \underbrace{|\operatorname{lcm}(a, b)|}_{\substack{=\operatorname{lcm}(a,b) \\ \text{(since } \operatorname{lcm}(a,b) \\ \text{is nonnegative)}}} \qquad \text{(by (3))} \\ &= |s| \operatorname{lcm}(a, b). \end{aligned}$$

This solves Exercise 2.11.1 **(e)**. □

10.50. Solution to Exercise 2.11.2

First solution to Exercise 2.11.2. Let us prove a more general fact:

> *Claim 1:* Let x, y, z, N be four integers such that $ax = by = cz = N$. Then, $\gcd(a, b, c) \cdot \operatorname{lcm}(x, y, z) = |N|$.

Once we have proven Claim 1, we will immediately obtain Exercise 2.11.2 **(a)** by applying Claim 1 to $x = bc$, $y = ca$, $z = ab$ and $N = abc$; and we will obtain Exercise 2.11.2 **(b)** in a similar way (see below for the details). Thus, let us focus on proving Claim 1.

[253] *Proof.* Assume that $s = 0$. Thus, $\underbrace{s}_{=0} a = 0$. Hence, the integers sa, sb are not all nonzero. Hence, $\operatorname{lcm}(sa, sb) = 0$ (by Definition 2.11.4). Comparing this with $\left|\underbrace{s}_{=0}\right| \operatorname{lcm}(a, b) = \underbrace{|0|}_{=0} \operatorname{lcm}(a, b) = 0$, we obtain $\operatorname{lcm}(sa, sb) = |s| \operatorname{lcm}(a, b)$. Hence, Exercise 2.11.1 **(e)** holds. Qed.

Proof of Claim 1: If the integers x, y, z are not all nonzero, then Claim 1 holds[254]. Thus, for the rest of this proof, we WLOG assume that the integers x, y, z are all nonzero. Hence, $\operatorname{lcm}(x, y, z)$ is the smallest positive element of the set $\operatorname{Mul}(x, y, z)$ (by Definition 2.11.4). Thus, $\operatorname{lcm}(x, y, z)$ is a positive integer.

If the integers a, b, c are all zero, then Claim 1 holds[255]. Hence, for the rest of this proof, we WLOG assume that the integers a, b, c are not all zero. Hence, $\gcd(a, b, c)$ is a positive integer (by Definition 2.9.6). Denote this positive integer by g. Hence, $g = \gcd(a, b, c)$.

Definition 2.9.6 also shows that $\gcd(a, b, c)$ is the largest element of the set $\operatorname{Div}(a, b, c)$ (since a, b, c are not all zero). Hence, $\gcd(a, b, c) \in \operatorname{Div}(a, b, c)$. In other words, $g \in \operatorname{Div}(a, b, c)$ (since $g = \gcd(a, b, c)$). In other words, g is a common divisor of a, b, c (by the definition of $\operatorname{Div}(a, b, c)$). In other words, g is an integer satisfying ($g \mid a$ and $g \mid b$ and $g \mid c$). Thus, $g \mid a \mid ax = N$. In other words, there exists an integer h such that $N = gh$. Consider this h.

It is easy to see that $N \neq 0$ [256]. Now, $gh = N \neq 0$ and thus $h \neq 0$. Hence, $|h|$ is a positive integer (since h is an integer). Denote this positive integer by m. Thus, $m = |h|$.

Also, set $N' = |N|$. Thus, N' is an integer satisfying

$$N' = \left| \underbrace{N}_{=gh} \right| = |gh| = \underbrace{|g|}_{\substack{=g \\ \text{(since } g \text{ is positive)}}} \cdot \underbrace{|h|}_{=m} \qquad \text{(by (3))}$$
$$= gm. \tag{381}$$

Our next goal is to prove that $m = \operatorname{lcm}(x, y, z)$. First, we shall prove that $m \in \operatorname{Mul}(x, y, z)$.

Indeed, we have $h \neq 0$. Hence, Exercise 2.2.3 (applied to g, a and h instead of a, b and c) shows that $g \mid a$ holds if and only if $gh \mid ah$. Hence, $gh \mid ah$ holds (since $g \mid a$ holds). Now, $xa = ax = N = gh \mid ah = ha$. But $a \neq 0$ (since $ax = N \neq 0$). Thus, Exercise 2.2.3 (applied to x, h and a instead of a, b and c) shows that $x \mid h$ holds if and only if $xa \mid ha$. Hence, $x \mid h$ holds (since $xa \mid ha$ holds). But Exercise 2.2.1 **(a)** (applied to h instead

[254] *Proof.* Assume that the integers x, y, z are not all nonzero. In other words, $x = 0$ or $y = 0$ or $z = 0$. We thus WLOG assume that $x = 0$ (since the proofs in the two cases $y = 0$ and $z = 0$ are analogous).

The integers x, y, z are not all nonzero. Hence, Definition 2.11.4 yields that their lowest common multiple is 0. In other words, $\operatorname{lcm}(x, y, z) = 0$.

But $ax = N$, thus $N = a \underbrace{x}_{=0} = 0$. Hence, $|N| = |0| = 0$. Comparing this with $\gcd(a, b, c) \cdot \underbrace{\operatorname{lcm}(x, y, z)}_{=0} = 0$, we obtain $\gcd(a, b, c) \cdot \operatorname{lcm}(x, y, z) = |N|$. Hence, Claim 1 holds, qed.

[255] *Proof.* Assume that the integers a, b, c are all zero. Hence, $\gcd(a, b, c) = 0$ (by Definition 2.9.6). Also, $a = 0$ (since a, b, c are all zero).

But $ax = N$, thus $N = \underbrace{a}_{=0} x = 0$. Hence, $|N| = |0| = 0$. Comparing this with $\underbrace{\gcd(a, b, c)}_{=0} \cdot \operatorname{lcm}(x, y, z) = 0$, we obtain $\gcd(a, b, c) \cdot \operatorname{lcm}(x, y, z) = |N|$. Hence, Claim 1 holds, qed.

[256] *Proof.* Assume the contrary. Thus, $N = 0$. But $x \neq 0$ (since x, y, z are nonzero). Hence, from $ax = N = 0$, we obtain $a = 0$. Similarly, $b = 0$ and $c = 0$. Thus, the integers a, b, c are all zero. This contradicts the fact that the integers a, b, c are not all zero. This contradiction shows that our assumption was wrong, qed.

of a) yields $h \mid |h| = m$. Thus, $x \mid h \mid m$. Similarly, $y \mid m$ and $z \mid m$. Thus, we have ($x \mid m$ and $y \mid m$ and $z \mid m$). In other words, m is a common multiple of x, y, z. In other words, $m \in \operatorname{Mul}(x, y, z)$. So we know that m is a positive element of the set $\operatorname{Mul}(x, y, z)$ (since m is positive).

We shall now show that m is the smallest positive element of this set. Indeed, let w be any positive element of $\operatorname{Mul}(x, y, z)$. We are going to prove that $w \geq m$.

In fact, $w \in \operatorname{Mul}(x, y, z)$. In other words, w is a common multiple of x, y, z. In other words, we have ($x \mid w$ and $y \mid w$ and $z \mid w$). Also, $w \neq 0$ (since w is positive).

We have $wa \neq 0$ (since $w \neq 0$ and $a \neq 0$). Hence, the integers wa, wb, wc are not all zero. Thus, Definition 2.9.6 shows that $\gcd(wa, wb, wc)$ is the largest element of the set $\operatorname{Div}(wa, wb, wc)$.

We have $a \neq 0$. Hence, Exercise 2.2.3 (applied to x, w and a instead of a, b and c) shows that $x \mid w$ holds if and only if $xa \mid wa$. Hence, $xa \mid wa$ holds (since $x \mid w$). Thus, $N = ax = xa \mid wa$. But Exercise 2.2.1 **(b)** (applied to N instead of a) yields $|N| \mid N$. In other words, $N' \mid N$ (since $N' = |N|$). Hence, $N' \mid N \mid wa$. Similarly, $N' \mid wb$ and $N' \mid wc$. Thus, ($N' \mid wa$ and $N' \mid wb$ and $N' \mid wc$). In other words, N' is a common divisor of wa, wb, wc. In other words, $N' \in \operatorname{Div}(wa, wb, wc)$. Hence, $N' \leq \gcd(wa, wb, wc)$ (since $\gcd(wa, wb, wc)$ is the **largest** element of the set $\operatorname{Div}(wa, wb, wc)$). Now, (381) yields

$$\begin{aligned} gm = N' \leq \gcd(wa, wb, wc) &= \underbrace{|w|}_{\substack{=w \\ \text{(since } w \text{ is positive)}}} \underbrace{\gcd(a, b, c)}_{=g} \\ &\qquad \text{(by Exercise 2.9.6 (applied to } s = w\text{))} \\ &= wg = gw. \end{aligned}$$

We can divide both sides of this inequality by g (since g is positive), and thus obtain $m \leq w$. In other words, $w \geq m$.

Now, forget that we fixed w. We thus have proven that each positive element w of the set $\operatorname{Mul}(x, y, z)$ satisfies $w \geq m$. Hence, m is the **smallest** positive element of the set $\operatorname{Mul}(x, y, z)$ (since we already know that m is a positive element of the set $\operatorname{Mul}(x, y, z)$). In other words, m is $\operatorname{lcm}(x, y, z)$ (since $\operatorname{lcm}(x, y, z)$ is the smallest positive element of the set $\operatorname{Mul}(x, y, z)$). In other words, $m = \operatorname{lcm}(x, y, z)$. Hence, (381) becomes

$$N' = \underbrace{g}_{=\gcd(a,b,c)} \underbrace{m}_{=\operatorname{lcm}(x,y,z)} = \gcd(a, b, c) \cdot \operatorname{lcm}(x, y, z).$$

Thus, $\gcd(a, b, c) \cdot \operatorname{lcm}(x, y, z) = N' = |N|$. This proves Claim 1.

We can now solve the actual exercise:

(a) We have $a(bc) = b(ca) = c(ab) = abc$. Hence, Claim 1 (applied to $x = bc$, $y = ca$, $z = ab$ and $N = abc$) yields $\gcd(a, b, c) \cdot \operatorname{lcm}(bc, ca, ab) = |abc|$. This solves Exercise 2.11.2 **(a)**.

(b) We have $(bc)a = (ca)b = (ab)c = abc$. Hence, Claim 1 (applied to bc, ca, ab, a, b, c and abc instead of a, b, c, x, y, z and N) yields $\gcd(bc, ca, ab) \cdot \operatorname{lcm}(a, b, c) = |abc|$. Thus, $\operatorname{lcm}(a, b, c) \cdot \gcd(bc, ca, ab) = \gcd(bc, ca, ab) \cdot \operatorname{lcm}(a, b, c) = |abc|$. This solves Exercise 2.11.2 **(b)**. □

10.51. Solution to Exercise 2.13.1

Solution to Exercise 2.13.1. We have $p \neq q$ (since p and q are distinct). Hence, $p \nmid q$ [257].

But Proposition 2.13.5 (applied to $a = q$) shows that either $p \mid q$ or $p \perp q$. Since $p \mid q$ cannot hold (because we have $p \nmid q$), we thus conclude that $p \perp q$. This solves Exercise 2.13.1. □

10.52. Solution to Exercise 2.13.2

Solution to Exercise 2.13.2. The integer p is positive (since $p > 1 > 0$). Thus, $|p| = p$.

Let d be a positive divisor of p other than 1 and p. We shall derive a contradiction.

We know that d is a divisor of p **other than** 1 and p. Hence, $d \neq 1$ and $d \neq p$.

But d is a divisor of p. In other words, there exists an integer c such that $p = dc$. Consider this c.

The integer d is positive, therefore nonzero. Hence, we can solve the equality $p = dc$ for c; thus we find $c = p/d > 0$ (since both p and d are positive). Thus, the integer c is positive; hence, $c \geq 1$. Also, $d \geq 1$ (since d is a positive integer). Combining this with $d \neq 1$, we obtain $d > 1$.

Since $c > 0$, we can multiply the inequality $d > 1$ by c. We thus find $cd > c \cdot 1 = c$. Hence, $c < cd = dc = p$. Since c is positive, we have $|c| = c < p$. But p is positive; thus, $|p| = p > |c|$ (since $|c| < p$).

Since $d > 0$, we can multiply the inequality $c \geq 1$ by d. We thus find $dc \geq d \cdot 1 = d$. Hence, $d \leq dc = p$. Combining this with $d \neq p$, we obtain $d < p$. Since d is positive, we have $|d| = d < p$. But p is positive; thus, $|p| = p > |d|$ (since $|d| < p$).

We have $p \mid p = dc$. But let us recall that for every $a, b \in \mathbb{Z}$ satisfying $p \mid ab$, we must have $p \mid a$ or $p \mid b$. Applying this to $a = d$ and $b = c$, we conclude that $p \mid d$ or $p \mid c$.

We have $d \neq 0$ (since $d > 0$). Hence, if we had $p \mid d$, then we would have $|p| \leq |d|$ (by Proposition 2.2.3 **(b)**, applied to $a = p$ and $b = d$); but this would contradict $|p| > |d|$. Hence, we cannot have $p \mid d$.

We have $c \neq 0$ (since $c > 0$). Hence, if we had $p \mid c$, then we would have $|p| \leq |c|$ (by Proposition 2.2.3 **(b)**, applied to $a = p$ and $b = c$); but this would contradict $|p| > |c|$. Hence, we cannot have $p \mid c$.

Thus, we have neither $p \mid d$ nor $p \mid c$. This contradicts the fact that $p \mid d$ or $p \mid c$.

Now, forget that we have fixed d. We thus have found a contradiction for each positive divisor d of p other than 1 and p. Thus, there exists no positive divisor d of p other than 1 and p. In other words, each positive divisor of p is either 1 or p. Thus, the only positive divisors of p are 1 and p (since 1 and p are indeed positive divisors of p). In other words, p is prime (by the definition of "prime"). This solves Exercise 2.13.2. □

[257] *Proof.* Assume the contrary. Thus, $p \mid q$. In other words, p is a divisor of q.

But q is a prime. According to the definition of a prime, this means that $q > 1$ and that the only positive divisors of q are 1 and q.

Also, p is a prime; thus, $p > 1$ (by the definition of a prime); hence, $p > 1 > 0$. Thus, p is positive. So we know that p is a positive divisor of q. Hence, p must be either 1 or q (since the only positive divisors of q are 1 and q). Since p cannot be 1 (because $p > 1$), we thus conclude that p must be q. In other words, $p = q$. This contradicts $p \neq q$. This contradiction shows that our assumption was false, qed.

10.53. Solution to Exercise 2.13.3

Solution to Exercise 2.13.3. $\Longrightarrow$: Assume that $a \perp p^k$ holds. We must prove that $p \nmid a$.

Assume the contrary. Thus, $p \mid a$. But $k \geq 1$ (since k is a positive integer), so that $1 \leq k$. Hence, Exercise 2.2.4 (applied to p, 1 and k instead of n, a and b) yields $p^1 \mid p^k$. In other words, $p \mid p^k$ (since $p^1 = p$). Now, Lemma 2.9.16 (applied to $m = p$ and $b = p^k$) yields $p \mid \gcd\left(a, p^k\right)$ (since $p \mid a$ and $p \mid p^k$). But from $a \perp p^k$, we obtain $\gcd\left(a, p^k\right) = 1$. Hence, $p \mid \gcd\left(a, p^k\right) = 1$. But p is prime; hence, $p > 1 > 0$, so that p is nonnegative. Hence, Exercise 2.2.5 (applied to $g = p$) yields $p = 1$ (since $p \mid 1$). This contradicts $p > 1$. This contradiction shows that our assumption was false. Hence, $p \nmid a$ is proven. This concludes the proof of the "$\Longrightarrow$" direction of Exercise 2.13.3.

$\Longleftarrow$: Assume that $p \nmid a$. We must prove that $a \perp p^k$.

Proposition 2.13.5 yields that either $p \mid a$ or $p \perp a$. Since $p \mid a$ does not hold (because $p \nmid a$), we thus conclude that $p \perp a$. But Proposition 2.10.4 (applied to $b = p$) yields that $a \perp p$ if and only if $p \perp a$. Hence, $a \perp p$ (since $p \perp a$). Thus, Exercise 2.10.4 (applied to $b = p$, $n = 1$ and $m = k$) yields $a^1 \perp p^k$. In other words, $a \perp p^k$. This concludes the proof of the "$\Longleftarrow$" direction of Exercise 2.13.3. □

10.54. Solution to Exercise 2.13.4

Solution to Exercise 2.13.4. This exercise can easily be solved by induction on k; but here is a more artful proof:

Let $k \in \mathbb{N}$. We have $p \geq 2$ (since p is an integer and satisfies $p > 1$). Thus, $p - 1 \geq 1$.

Recall the identity (25), which holds for every $a, b \in \mathbb{Q}$. Let us apply this identity to $a = p$ and $b = 1$. We thus obtain

$$(p-1)\left(p^{k-1} + p^{k-2}\cdot 1 + p^{k-3}\cdot 1^2 + \cdots + p\cdot 1^{k-2} + 1^{k-1}\right) = p^k - \underbrace{1^k}_{=1} = p^k - 1.$$

Thus,

$$\begin{aligned} p^k - 1 &= (p-1)\underbrace{\left(p^{k-1} + p^{k-2}\cdot 1 + p^{k-3}\cdot 1^2 + \cdots + p\cdot 1^{k-2} + 1^{k-1}\right)}_{=\sum_{i=0}^{k-1} p^i 1^{k-i}} \\ &= \underbrace{(p-1)}_{\geq 1}\sum_{i=0}^{k-1} p^i 1^{k-i} \geq 1\sum_{i=0}^{k-1} p^i 1^{k-i} \qquad \left(\text{since } \sum_{i=0}^{k-1} p^i 1^{k-i} \text{ is clearly } \geq 0\right) \\ &= \sum_{i=0}^{k-1} \underbrace{p^i 1^{k-i}}_{\substack{=p^i \geq 1^i \\ (\text{since } p \geq 1)}} \geq \sum_{i=0}^{k-1} \underbrace{1^i}_{=1} = \sum_{i=0}^{k-1} 1 = k. \end{aligned}$$

Hence, $p^k \geq k + 1 > k$. This solves Exercise 2.13.4. □

10.55. Solution to Exercise 2.13.5

Solution to Exercise 2.13.5. If $n \geq 0$, then we have $|n| = n$ and thus $v_p(|n|) = v_p(n)$. Hence, if $n \geq 0$, then Exercise 2.13.5 holds. Thus, for the rest of this solution, we WLOG assume that $n < 0$. Hence, $|n| = -n$.

We have $-1 \mid p$ (since $p = (-1) \cdot (-p)$). Thus, Proposition 2.9.7 **(i)** (applied to $a = -1$ and $b = p$) yields $\gcd(-1, p) = |-1| = 1$. In other words, $-1 \perp p$. Also, $-1 = (-1) \cdot p^0$ (since $p^0 = 1$). Thus, Lemma 2.13.27 **(b)** (applied to -1, 0 and 1 instead of n, i and w) yields $v_p(-1) = 0$. Now, Theorem 2.13.28 **(a)** (applied to $a = -1$ and $b = n$) yields $v_p((-1)n) = \underbrace{v_p(-1)}_{=0} + v_p(n) = v_p(n)$. In view of $(-1)n = -n = |n|$, this rewrites as $v_p(|n|) = v_p(n)$. This solves Exercise 2.13.5. □

10.56. Solution to Exercise 2.13.6

Solution to Exercise 2.13.6. Corollary 2.13.29 (applied to $a_i = a$) yields

$$v_p\left(\underbrace{aa\cdots a}_{k\text{ times}}\right) = \underbrace{v_p(a) + v_p(a) + \cdots + v_p(a)}_{k\text{ times}} = kv_p(a).$$

In view of $\underbrace{aa\cdots a}_{k\text{ times}} = a^k$, this rewrites as $v_p\left(a^k\right) = kv_p(a)$. This solves Exercise 2.13.6. □

10.57. Solution to Exercise 2.13.7

Solution to Exercise 2.13.7. For each $i \in \{1, 2, \ldots, u\}$, the number $p_i^{a_i}$ is a well-defined positive integer (since p_i is a prime, and since a_i is a nonnegative integer). Thus, $p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}$ is a product of positive integers, and therefore itself a positive integer.

Now, let p be a prime. Note that $p_1^{a_1}, p_2^{a_2}, \ldots, p_u^{a_u}$ are u integers. Hence, Corollary 2.13.29 (applied to u and $p_j^{a_j}$ instead of k and a_j) yields

$$\begin{aligned} v_p\left(p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}\right) &= v_p\left(p_1^{a_1}\right) + v_p\left(p_2^{a_2}\right) + \cdots + v_p\left(p_u^{a_u}\right) \\ &= \sum_{j=1}^{u} \underbrace{v_p\left(p_j^{a_j}\right)}_{\substack{=a_j v_p(p_j) \\ \text{(by Exercise 2.13.6,} \\ \text{applied to } a=p_j \text{ and } k=a_j)}} = \underbrace{\sum_{j=1}^{u}}_{=\sum_{j\in\{1,2,\ldots,u\}}} a_j \underbrace{v_p(p_j)}_{\substack{=\begin{cases} 1, & \text{if } p_j = p; \\ 0, & \text{if } p_j \neq p \end{cases} \\ \text{(by Theorem 2.13.28 (d),} \\ \text{applied to } q=p_j \\ \text{(since } p_j \text{ is prime))}}} \\ &= \sum_{j\in\{1,2,\ldots,u\}} a_j \begin{cases} 1, & \text{if } p_j = p; \\ 0, & \text{if } p_j \neq p \end{cases}. \end{aligned} \tag{382}$$

Now, forget that we fixed p. We thus have proven the equality (382) for each prime p.

(a) Let $i \in \{1, 2, \ldots, u\}$. Then, p_i is a prime. Hence, (382) (applied to $p = p_i$) yields

$$\begin{aligned} v_p\left(p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}\right) &= \sum_{j\in\{1,2,\ldots,u\}} a_j \begin{cases} 1, & \text{if } p_j = p_i; \\ 0, & \text{if } p_j \neq p_i \end{cases} \\ &= a_i \begin{cases} 1, & \text{if } p_i = p_i; \\ 0, & \text{if } p_i \neq p_i \end{cases} + \sum_{\substack{j\in\{1,2,\ldots,u\}; \\ j\neq i}} a_j \begin{cases} 1, & \text{if } p_j = p_i; \\ 0, & \text{if } p_j \neq p_i \end{cases} \end{aligned} \tag{383}$$

(here, we have split off the addend for $j = i$ from the sum). But if $j \in \{1, 2, \ldots, u\}$ satisfies $j \neq i$, then it must satisfy $p_j \neq p_i$ (since the primes $p_1, p_2, \ldots, p_u$ are distinct) and therefore

$$\begin{cases} 1, & \text{if } p_j = p_i; \\ 0, & \text{if } p_j \neq p_i \end{cases} = 0. \tag{384}$$

Hence, (383) becomes

$$\begin{aligned} v_p\left(p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}\right) &= a_i \underbrace{\begin{cases} 1, & \text{if } p_i = p_i; \\ 0, & \text{if } p_i \neq p_i \end{cases}}_{\substack{=1 \\ \text{(since } p_i = p_i\text{)}}} + \sum_{\substack{j \in \{1,2,\ldots,u\}; \\ j \neq i}} a_j \underbrace{\begin{cases} 1, & \text{if } p_j = p_i; \\ 0, & \text{if } p_j \neq p_i \end{cases}}_{\substack{=0 \\ \text{(by (384))}}} \\ &= a_i 1 + \underbrace{\sum_{\substack{j \in \{1,2,\ldots,u\}; \\ j \neq i}} a_j 0}_{=0} = a_i 1 = a_i. \end{aligned}$$

This solves Exercise 2.13.7 **(a)**.

(b) Let p be a prime satisfying $p \notin \{p_1, p_2, \ldots, p_u\}$. Then, for each $j \in \{1, 2, \ldots, u\}$, we have $p_j \neq p$ (since otherwise, we would have $p_j = p$ and therefore $p = p_j \in \{p_1, p_2, \ldots, p_u\}$, which would contradict $p \notin \{p_1, p_2, \ldots, p_u\}$) and therefore

$$\begin{cases} 1, & \text{if } p_j = p; \\ 0, & \text{if } p_j \neq p \end{cases} = 0. \tag{385}$$

Hence, (382) becomes

$$v_p\left(p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}\right) = \sum_{j \in \{1,2,\ldots,u\}} a_j \underbrace{\begin{cases} 1, & \text{if } p_j = p; \\ 0, & \text{if } p_j \neq p \end{cases}}_{\substack{=0 \\ \text{(by (385))}}} = \sum_{j \in \{1,2,\ldots,u\}} a_j 0 = 0.$$

This solves Exercise 2.13.7 **(b)**. □

10.58. Solution to Exercise 2.13.8

Solution to Exercise 2.13.8. Applying (41) to $p = 2$, we obtain $v_2(n) = v_2(m)$ (since 2 is a prime).

If n is nonzero, then $v_p(n)$ is a nonnegative integer for every prime p (by Definition 2.13.23 **(a)**). Applying this to $p = 2$, we conclude the following: If n is nonzero, then $v_2(n)$ is a nonnegative integer and thus satisfies $v_2(n) \neq \infty$. Thus, we have shown that

$$\text{if } n \text{ is nonzero, then } v_2(n) \neq \infty. \tag{386}$$

The same argument (applied to m instead of n) shows that

$$\text{if } m \text{ is nonzero, then } v_2(m) \neq \infty. \tag{387}$$

We are in one of the following two cases:

Case 1: We have $n = 0$.

Case 2: We have $n \neq 0$.

Let us first consider Case 1. In this case, we have $n = 0$. Thus, $v_2(n) = v_2(0) = \infty$ (by Definition 2.13.23 **(b)**). Comparing this with $v_2(n) = v_2(m)$, we obtain $v_2(m) = \infty$. But if m was nonzero, then we would have $v_2(m) \neq \infty$ (by (387)), which would contradict $v_2(m) = \infty$. Hence, m cannot be nonzero. In other words, m must be 0. Thus, $m = 0$. Comparing this with $n = 0$, we obtain $n = m$. Hence, Exercise 2.13.8 is solved in Case 1.

Let us now consider Case 2. In this case, we have $n \neq 0$. Thus, n is nonzero; hence, $v_2(n) \neq \infty$ (by (386)). If we had $m = 0$, then we would have $v_2(n) = v_2\left(\underbrace{m}_{=0}\right) = v_2(0) = \infty$ (by Definition 2.13.23 **(b)**), which would contradict $v_2(n) \neq \infty$. Thus, we cannot have $m = 0$. Hence, m is nonzero.

The integer n is nonzero and nonnegative; thus, the integer n is positive. Thus, Corollary 2.13.33 yields

$$n = \prod_{p \text{ prime}} \underbrace{p^{v_p(n)}}_{\substack{= p^{v_p(m)} \\ \text{(since (41)} \\ \text{yields } v_p(n) = v_p(m))}} = \prod_{p \text{ prime}} p^{v_p(m)}. \tag{388}$$

The integer m is nonzero and nonnegative; thus, the integer m is positive. Hence, Corollary 2.13.33 (applied to m instead of n) yields

$$m = \prod_{p \text{ prime}} p^{v_p(m)}.$$

Comparing this with (388), we obtain $n = m$. Thus, Exercise 2.13.8 is solved in Case 2.

We have now solved Exercise 2.13.8 in both of the Cases 1 and 2. Hence, Exercise 2.13.8 always holds. □

10.59. Second solution to Exercise 2.11.2

Second solution to Exercise 2.11.2 (sketched). WLOG assume that a, b, c are nonzero (since otherwise, the claim of Exercise 2.11.2 easily reduces to $0 = 0$). Then, abc is nonzero as well. Hence, Corollary 2.13.34 yields

$$|abc| = \prod_{p \text{ prime}} p^{v_p(abc)}.$$

We have

$$\begin{aligned}
&\underbrace{\gcd\left(a,b,c\right)}_{\substack{=\prod\limits_{p \text{ prime}} p^{\min\left\{v_p(a),v_p(b),v_p(c)\right\}} \\ \text{(by Proposition 2.13.40)}}} \cdot \underbrace{\operatorname{lcm}\left(bc,ca,ab\right)}_{\substack{=\prod\limits_{p \text{ prime}} p^{\max\left\{v_p(bc),v_p(ca),v_p(ab)\right\}} \\ \text{(by Proposition 2.13.40)}}} \\
&= \left(\prod_{p \text{ prime}} p^{\min\left\{v_p(a),v_p(b),v_p(c)\right\}}\right) \cdot \left(\prod_{p \text{ prime}} p^{\max\left\{v_p(bc),v_p(ca),v_p(ab)\right\}}\right) \\
&= \prod_{p \text{ prime}} \underbrace{\left(p^{\min\left\{v_p(a),v_p(b),v_p(c)\right\}} p^{\max\left\{v_p(bc),v_p(ca),v_p(ab)\right\}}\right)}_{=p^{\min\left\{v_p(a),v_p(b),v_p(c)\right\}+\max\left\{v_p(bc),v_p(ca),v_p(ab)\right\}}} \\
&= \prod_{p \text{ prime}} p^{\min\left\{v_p(a),v_p(b),v_p(c)\right\}+\max\left\{v_p(bc),v_p(ca),v_p(ab)\right\}}. \qquad (389)
\end{aligned}$$

Let us now fix a prime p, and try to simplify $\min\left\{v_p\left(a\right),v_p\left(b\right),v_p\left(c\right)\right\}+\max\left\{v_p\left(bc\right),v_p\left(ca\right),v_p\left(ab\right)\right\}$. Indeed, set $u = v_p\left(abc\right)$. Note that $u \in \mathbb{N}$ (since abc is nonzero).

Theorem 2.13.28 **(a)** (applied to ca and b instead of a and b) yields $v_p\left(cab\right) = v_p\left(ca\right) + v_p\left(b\right)$. Comparing this with $v_p\left(\underbrace{cab}_{=abc}\right) = v_p\left(abc\right) = u$, we obtain $u = v_p\left(ca\right) + v_p\left(b\right)$. Subtracting $v_p\left(b\right)$ from this equality[258], we obtain $u - v_p\left(b\right) = v_p\left(ca\right)$. Thus, $v_p\left(ca\right) = u - v_p\left(b\right)$. Similarly, $v_p\left(ab\right) = u - v_p\left(c\right)$ and $v_p\left(bc\right) = u - v_p\left(a\right)$. Now,

$$\begin{aligned}
&\min\left\{v_p\left(a\right),v_p\left(b\right),v_p\left(c\right)\right\} + \max\left\{\underbrace{v_p\left(bc\right)}_{=u-v_p(a)}, \underbrace{v_p\left(ca\right)}_{=u-v_p(b)}, \underbrace{v_p\left(ab\right)}_{=u-v_p(c)}\right\} \\
&= \min\left\{v_p\left(a\right),v_p\left(b\right),v_p\left(c\right)\right\} + \underbrace{\max\left\{u-v_p\left(a\right),u-v_p\left(b\right),u-v_p\left(c\right)\right\}}_{\substack{=u-\min\left\{v_p(a),v_p(b),v_p(c)\right\} \\ \text{(since any three reals } x,y,z \\ \text{satisfy } \max\{u-x,u-y,u-z\}=u-\min\{x,y,z\})}} \\
&= \min\left\{v_p\left(a\right),v_p\left(b\right),v_p\left(c\right)\right\} + \left(u - \min\left\{v_p\left(a\right),v_p\left(b\right),v_p\left(c\right)\right\}\right) \\
&= u = v_p\left(abc\right). \qquad (390)
\end{aligned}$$

Now, forget that we fixed p. We thus have proven (390) for each prime p. Thus, (389) becomes

$$\begin{aligned}
&\gcd\left(a,b,c\right)\cdot\operatorname{lcm}\left(bc,ca,ab\right) \\
&= \prod_{p \text{ prime}} \underbrace{p^{\min\left\{v_p(a),v_p(b),v_p(c)\right\}+\max\left\{v_p(bc),v_p(ca),v_p(ab)\right\}}}_{\substack{=p^{v_p(abc)} \\ \text{(by (390))}}} = \prod_{p \text{ prime}} p^{v_p(abc)} = \left|abc\right|.
\end{aligned}$$

This solves Exercise 2.11.2 **(a)** again. Similarly we can re-solve Exercise 2.11.2 **(b)**. □

[258] This is allowed, since $v_p\left(b\right) \in \mathbb{N}$ (because b is nonzero).

Remark 10.59.1. Similarly, we could show that any four integers a, b, c, d satisfy

$$\gcd(a,b,c,d) \cdot \operatorname{lcm}(bcd, cda, dab, abc) = |abcd| \qquad \text{and}$$
$$\operatorname{lcm}(a,b,c,d) \cdot \gcd(bcd, cda, dab, abc) = |abcd| .$$

Indeed, the last equality holds since each prime p satisfies

$$\begin{aligned}
&\min\left\{v_p(a), v_p(b), v_p(c), v_p(d)\right\} \\
&\qquad + \max\left\{ \underbrace{v_p(bcd)}_{=v_p(abcd)-v_p(a)}, \underbrace{v_p(cda)}_{=v_p(abcd)-v_p(b)}, \underbrace{v_p(dab)}_{=v_p(abcd)-v_p(c)}, \underbrace{v_p(abc)}_{=v_p(abcd)-v_p(d)} \right\} \\
&= \min\left\{v_p(a), v_p(b), v_p(c), v_p(d)\right\} \\
&\qquad + \underbrace{\max\left\{v_p(abcd)-v_p(a), v_p(abcd)-v_p(b), v_p(abcd)-v_p(c), v_p(abcd)-v_p(d)\right\}}_{=v_p(abcd)-\min\left\{v_p(a),v_p(b),v_p(c),v_p(d)\right\}} \\
&= \min\left\{v_p(a), v_p(b), v_p(c), v_p(d)\right\} + \left(v_p(abcd) - \min\left\{v_p(a), v_p(b), v_p(c), v_p(d)\right\}\right) \\
&= v_p(abcd)
\end{aligned}$$

(assuming that a, b, c, d are nonzero). Similarly, the first equality holds. You can likewise prove generalizations to k integers.[259]

10.60. Solution to Exercise 2.13.9

First solution to Exercise 2.13.9. We must prove that $a \equiv b \operatorname{mod} n$. If $a = b$, then this is true (because if $a = b$, then $a = b \equiv b \operatorname{mod} n$). Thus, for the rest of this proof, we WLOG assume that we don't have $a = b$. Hence, $a \neq b$, so that $a - b \neq 0$. Thus, $a - b$ is a nonzero integer. Hence, $v_p(a-b) \in \mathbb{N}$ for every prime p.

Let p be any prime. Then, (49) yields $a \equiv b \operatorname{mod} p^{v_p(n)}$. In other words, $p^{v_p(n)} \mid a - b$. But Lemma 2.13.25 (applied to $v_p(n)$ and $a - b$ instead of i and n) yields that $p^{v_p(n)} \mid a - b$ if and only if $v_p(a-b) \geq v_p(n)$. Hence, we have $v_p(a-b) \geq v_p(n)$ (since $p^{v_p(n)} \mid a - b$). In other words, $v_p(n) \leq v_p(a-b)$.

Now, forget that we fixed p. We thus have proven that each prime p satisfies $v_p(n) \leq v_p(a-b)$. But Proposition 2.13.35 (applied to $a - b$ instead of m) shows that $n \mid a - b$ if and only if each prime p satisfies $v_p(n) \leq v_p(a-b)$. Hence, $n \mid a - b$ (since each prime p satisfies $v_p(n) \leq v_p(a-b)$). In other words, $a \equiv b \operatorname{mod} n$. This solves Exercise 2.13.9. □

[259] That said, it is probably better (and easier) to generalize Claim 1 from the first solution of Exercise 2.11.2 to k integers:

> *Claim 2:* Let $k > 0$. Let N be an integer. Let $a_1, a_2, \ldots, a_k$ be k integers, and let $x_1, x_2, \ldots, x_k$ be k integers such that $a_1 x_1 = a_2 x_2 = \cdots = a_k x_k = N$. Then, $\gcd(a_1, a_2, \ldots, a_k) \cdot \operatorname{lcm}(x_1, x_2, \ldots, x_k) = |N|$.

This Claim 2 can be proven either by generalizing the proof of Claim 1 from the solution of Exercise 2.11.2, or (again) using Proposition 2.13.38.

Second solution to Exercise 2.13.9. Define an integer c by $c = a - b$.

We shall show that

$$d \mid c \text{ for every positive divisor } d \text{ of } n. \tag{391}$$

[*Proof of (391):* We shall prove (391) by strong induction on d:

Let e be a positive divisor of n. Assume that (391) holds for all positive divisors d of n satisfying $d < e$. We must prove that (391) holds for $d = e$. In other words, we must prove that $e \mid c$.

We have assumed that (391) holds for all positive divisors d of n satisfying $d < e$. In other words, if d is a positive divisor of n satisfying $d < e$, then

$$d \mid c. \tag{392}$$

Note that the integer e is nonzero (since e is positive); thus, $v_p(e) \in \mathbb{N}$. Also, $v_p(n) \in \mathbb{N}$ (since n is nonzero). We know that $e \mid n$ (since e is a divisor of n). But Proposition 2.13.35 (applied to e and n instead of n and m) shows that $e \mid n$ if and only if each prime p satisfies $v_p(e) \leq v_p(n)$. Hence,

$$\text{each prime } p \text{ satisfies } v_p(e) \leq v_p(n) \tag{393}$$

(since $e \mid n$).

We must prove that $e \mid c$. If $e = 1$, then this follows from the (obvious) fact that $1 \mid c$. Thus, for the rest of this proof, we WLOG assume that $e \neq 1$. Hence, $e > 1$ (since e is a positive integer). Thus, Proposition 2.13.8 (applied to e instead of n) shows that there exists at least one prime p such that $p \mid e$. Consider this p. Theorem 2.13.27 **(a)** (applied to e instead of n) shows that there exists a nonzero integer u such that $u \perp p$ and $e = up^{v_p(e)}$. Consider this u. From $e = up^{v_p(e)}$, we obtain $u = e/p^{v_p(e)}$; therefore, u is positive (since e and $p^{v_p(e)}$ are positive).

Lemma 2.13.25 (applied to 1 and e instead of i and n) shows that $p^1 \mid e$ if and only if $v_p(e) \geq 1$. Hence, $v_p(e) \geq 1$ (since $p^1 = p \mid e$). Hence, $p^{v_p(e)} \geq p^1 = p > 1$. Now, $e = u \underbrace{p^{v_p(e)}}_{>1} > u$ (since u is positive). Thus, $u < e$. Furthermore, $p^{v_p(e)}$ is an integer; hence, the equality $e = up^{v_p(e)}$ yields that $u \mid e$. Thus, $u \mid e \mid n$. Hence, u is a divisor of n. Thus, u is a positive divisor of n (since u is positive). Since $u < e$, we can thus apply (392) to $d = u$. We thus obtain $u \mid c$.

On the other hand, (49) yields $a \equiv b \bmod p^{v_p(n)}$. In other words, $p^{v_p(n)} \mid a - b$. This rewrites as $p^{v_p(n)} \mid c$ (since $c = a - b$). But $v_p(e) \leq v_p(n)$ (by (393)). Hence, Exercise 2.2.4 (applied to p, $v_p(e)$ and $v_p(n)$ instead of n, a and b) yields $p^{v_p(e)} \mid p^{v_p(n)} \mid c$.

Recall that $u \perp p$. Thus, Exercise 2.10.4 (applied to u, p, 1 and $v_p(e)$ instead of a, b, n and m) yields $u^1 \perp p^{v_p(e)}$. In view of $u^1 = u$, this rewrites as $u \perp p^{v_p(e)}$.

Now we know that $u \in \mathbb{Z}$ and $p^{v_p(e)} \in \mathbb{Z}$ and $c \in \mathbb{Z}$ and $u \mid c$ and $p^{v_p(e)} \mid c$ and $u \perp p^{v_p(e)}$. Hence, Theorem 2.10.7 (applied to u and $p^{v_p(e)}$ instead of a and b) yields $up^{v_p(e)} \mid c$. In view of $e = up^{v_p(e)}$, this rewrites as $e \mid c$. In other words, (391) holds for $d = e$. This completes the induction step. Hence, (391) is proven by strong induction.]

Let $n' = |n|$. Then, $n' = |n| > 0$ (since n is nonzero). Moreover, Exercise 2.2.1 **(b)** (applied to n instead of a) yields $|n| \mid n$. Since $n' = |n|$, this rewrites as $n' \mid n$. Hence, n' is a divisor of n. Since n' is positive, we thus conclude that n' is a positive divisor of n. Hence, (391) (applied to $d = n'$) yields $n' \mid c$. But Exercise 2.2.1 **(a)** (applied to n instead of a) yields

$n \mid |n|$. Since $n' = |n|$, this rewrites as $n \mid n'$. Hence, $n \mid n' \mid c = a - b$. In other words, $a \equiv b \mod n$. This solves Exercise 2.13.9 again. □

10.61. Solution to Exercise 2.13.10

Solution to Exercise 2.13.10. **(a)** Forget that we fixed p. We thus must prove that

$$v_p(\gcd(n,m)) = \min\{v_p(n), v_p(m)\} \qquad \text{for each prime } p. \tag{394}$$

We are in one of the following two cases:

Case 1: The integers n and m are both nonzero.

Case 2: The integers n and m are not both nonzero.

Let us first consider Case 1. In this case, the integers n and m are both nonzero. Thus, (50) yields

$$\gcd(n,m) = \prod_{p \text{ prime}} p^{\min\{v_p(n), v_p(m)\}}.$$

In particular, the product $\prod_{p \text{ prime}} p^{\min\{v_p(n), v_p(m)\}}$ is well-defined. In other words:

- The number $\min\{v_p(n), v_p(m)\}$ is a nonnegative integer for each prime p;
- all but finitely many primes p satisfy $\min\{v_p(n), v_p(m)\} = 0$.

(Both of these facts were proven during our proof of Proposition 2.13.38.)

Hence, Corollary 2.13.37 (applied to $\gcd(n,m)$ and $\min\{v_p(n), v_p(m)\}$ instead of n and b_p) shows that

$$v_q(\gcd(n,m)) = \min\{v_q(n), v_q(m)\} \qquad \text{for each prime } q.$$

Renaming q as p in this statement, we obtain

$$v_p(\gcd(n,m)) = \min\{v_p(n), v_p(m)\} \qquad \text{for each prime } p.$$

Thus, (394) is proven in Case 1.

Now, let us consider Case 2. In this case, the integers n and m are not both nonzero. In other words, we have $n = 0$ or $m = 0$. Thus, we can WLOG assume that $m = 0$ (because in the case $n = 0$, we can swap n with m without changing the meaning of our claim, since n and m play symmetric roles[260]). Assume this.

Fix a prime p. Now, $\gcd\left(n, \underbrace{m}_{=0}\right) = \gcd(n,0) = |n|$ (since Proposition 2.9.7 **(a)** (applied to $a = n$) yields $\gcd(n,0) = \gcd(n) = |n|$). Hence,

$$v_p(\gcd(n,m)) = v_p(|n|) = v_p(n) \qquad (\text{by Exercise 2.13.5}).$$

On the other hand, from $m = 0$, we obtain $v_p(m) = v_p(0) = \infty$ (by Definition 2.13.23 **(b)**). Thus,

$$\min\left\{v_p(n), \underbrace{v_p(m)}_{=\infty}\right\} = \min\{v_p(n), \infty\} = v_p(n)$$

[260] Here we are using the fact that $\gcd(n,m) = \gcd(m,n)$ (which follows from Proposition 2.9.7 **(b)**).

(by our rules for the symbol ∞). Comparing this with $v_p(\gcd(n,m)) = v_p(n)$, we obtain $v_p(\gcd(n,m)) = \min\{v_p(n), v_p(m)\}$.

Now, forget that we fixed p. We thus have proven that $v_p(\gcd(n,m)) = \min\{v_p(n), v_p(m)\}$ for each prime p. Thus, (394) is proven in Case 2.

We have now proven (394) in each of the two Cases 1 and 2. Thus, (394) always holds. This solves Exercise 2.13.10 **(a)**.

(b) Forget that we fixed p. We thus must prove that

$$v_p(\operatorname{lcm}(n,m)) = \max\{v_p(n), v_p(m)\} \qquad \text{for each prime } p. \tag{395}$$

We are in one of the following two cases:

Case 1: The integers n and m are both nonzero.

Case 2: The integers n and m are not both nonzero.

Let us first consider Case 1. In this case, the integers n and m are both nonzero. Thus, (51) yields

$$\operatorname{lcm}(n,m) = \prod_{p \text{ prime}} p^{\max\{v_p(n), v_p(m)\}}.$$

In particular, the product $\prod_{p \text{ prime}} p^{\max\{v_p(n), v_p(m)\}}$ is well-defined. In other words:

- The number $\max\{v_p(n), v_p(m)\}$ is a nonnegative integer for each prime p;
- all but finitely many primes p satisfy $\max\{v_p(n), v_p(m)\} = 0$.

(Both of these facts were proven during our proof of Proposition 2.13.38.)

Hence, Corollary 2.13.37 (applied to $\operatorname{lcm}(n,m)$ and $\max\{v_p(n), v_p(m)\}$ instead of n and b_p) shows that

$$v_q(\operatorname{lcm}(n,m)) = \max\{v_q(n), v_q(m)\} \qquad \text{for each prime } q.$$

Renaming q as p in this statement, we obtain

$$v_p(\operatorname{lcm}(n,m)) = \max\{v_p(n), v_p(m)\} \qquad \text{for each prime } p.$$

Thus, (395) is proven in Case 1.

Now, let us consider Case 2. In this case, the integers n and m are not both nonzero. In other words, we have $n = 0$ or $m = 0$. Thus, we can WLOG assume that $m = 0$ (because in the case $n = 0$, we can swap n with m without changing the meaning of our claim, since n and m play symmetric roles[261]). Assume this.

Fix a prime p. The numbers n, m are not all nonzero (since $m = 0$). Hence, $\operatorname{lcm}(n,m) = 0$ (by the definition of $\operatorname{lcm}(n,m)$). Thus,

$$v_p(\operatorname{lcm}(n,m)) = v_p(0) = \infty \qquad (\text{by Definition 2.13.23 } \textbf{(b)}).$$

On the other hand, from $m = 0$, we obtain $v_p(m) = v_p(0) = \infty$ (by Definition 2.13.23 **(b)**). Thus,

$$\max\left\{v_p(n), \underbrace{v_p(m)}_{=\infty}\right\} = \max\{v_p(n), \infty\} = \infty$$

[261] Here we are using the fact that $\operatorname{lcm}(n,m) = \operatorname{lcm}(m,n)$ (which follows from Exercise 2.11.1 **(a)**).

(by our rules for the symbol ∞). Comparing this with $v_p(\operatorname{lcm}(n,m)) = \infty$, we obtain $v_p(\operatorname{lcm}(n,m)) = \max\{v_p(n), v_p(m)\}$.

Now, forget that we fixed p. We thus have proven that $v_p(\operatorname{lcm}(n,m)) = \max\{v_p(n), v_p(m)\}$ for each prime p. Thus, (395) is proven in Case 2.

We have now proven (395) in each of the two Cases 1 and 2. Thus, (395) always holds. This solves Exercise 2.13.10 **(b)**. □

10.62. Solution to Exercise 2.13.11

We shall solve Exercise 2.13.11 in two different ways. The first solution uses p-valuations (and Exercise 2.13.10 in particular) to reduce the claim of the exercise to a simple identity between minima and maxima of sets of numbers. This solution (just as our Second proof of Theorem 2.11.6 above) illustrates how properties of gcds and lcms of integers can be proven in a straightforward way using p-valuations. The second solution (due to Bill Dubuque), in contrast, completely avoids the use of prime numbers.

First solution to Exercise 2.13.11. **(a)** Let us first show an auxiliary claim:

> *Claim 1:* Let $i, j, k \in \mathbb{N} \cup \{\infty\}$ be arbitrary. Then,
>
> $$\min\{i, \max\{j,k\}\} = \max\{\min\{i,j\}, \min\{i,k\}\}.$$

[*Proof of Claim 1:* We have $j \leq k$ or $j \geq k$. Since j and k play symmetric roles in Claim 1, we can always swap j and k; thus, we can WLOG assume that $j \leq k$. Assume this. From $j \leq k$, we obtain $\max\{j,k\} = k$. Moreover, any element of a set must be $\geq$ to the minimum of this set; hence, $i \geq \min\{i,j\}$ and $j \geq \min\{i,j\}$. The minimum $\min\{i,k\}$ must be one of the two elements i and k (since the minimum of a set must always be an element of this set); but both of these elements i and k are $\geq \min\{i,j\}$ (because $i \geq \min\{i,j\}$ and $k \geq j \geq \min\{i,j\}$). Hence, $\min\{i,k\}$ must be $\geq \min\{i,j\}$. Hence, $\max\{\min\{i,j\}, \min\{i,k\}\} = \min\{i,k\}$. Comparing this with $\min\left\{i, \underbrace{\max\{j,k\}}_{=k}\right\} = \min\{i,k\}$, we obtain $\min\{i, \max\{j,k\}\} = \max\{\min\{i,j\}, \min\{i,k\}\}$. This proves Claim 1.]

Now, fix a prime p. Then, Exercise 2.13.10 **(a)** (applied to $n = a$ and $m = \operatorname{lcm}(b,c)$) yields

$$\begin{aligned} v_p(\gcd(a, \operatorname{lcm}(b,c))) &= \min\left\{v_p(a), \underbrace{v_p(\operatorname{lcm}(b,c))}_{\substack{=\max\{v_p(b), v_p(c)\} \\ \text{(by Exercise 2.13.10 (b),} \\ \text{applied to } n=b \text{ and } m=c)}}\right\} \\ &= \min\{v_p(a), \max\{v_p(b), v_p(c)\}\} \\ &= \max\{\min\{v_p(a), v_p(b)\}, \min\{v_p(a), v_p(c)\}\} \end{aligned} \tag{396}$$

(by Claim 1, applied to $i = v_p(a)$, $j = v_p(b)$ and $k = v_p(c)$). On the other hand, Exercise 2.13.10 **(b)** (applied to $n = \gcd(a,b)$ and $m = \gcd(a,c)$) yields

$$v_p(\operatorname{lcm}(\gcd(a,b), \gcd(a,c))) = \max\left\{ \underbrace{v_p(\gcd(a,b))}_{\substack{=\min\{v_p(a),v_p(b)\} \\ \text{(by Exercise 2.13.10 (a),} \\ \text{applied to } n=a \text{ and } m=b)}}, \underbrace{v_p(\gcd(a,c))}_{\substack{=\min\{v_p(a),v_p(c)\} \\ \text{(by Exercise 2.13.10 (a),} \\ \text{applied to } n=a \text{ and } m=c)}} \right\}$$
$$= \max\{\min\{v_p(a), v_p(b)\}, \min\{v_p(a), v_p(c)\}\}.$$

Comparing this with (396), we obtain

$$v_p(\gcd(a, \operatorname{lcm}(b,c))) = v_p(\operatorname{lcm}(\gcd(a,b), \gcd(a,c))).$$

Now, forget that we fixed p. We thus have proven that

$$v_p(\gcd(a, \operatorname{lcm}(b,c))) = v_p(\operatorname{lcm}(\gcd(a,b), \gcd(a,c))) \qquad \text{for every prime } p.$$

Thus, Exercise 2.13.8 (applied to $n = \gcd(a, \operatorname{lcm}(b,c))$ and $m = \operatorname{lcm}(\gcd(a,b), \gcd(a,c))$) yields that $\gcd(a, \operatorname{lcm}(b,c)) = \operatorname{lcm}(\gcd(a,b), \gcd(a,c))$ (since $\gcd(a, \operatorname{lcm}(b,c))$ and $\operatorname{lcm}(\gcd(a,b), \gcd(a,c))$ are nonnegative integers[262]). This solves Exercise 2.13.11 **(a)**.

(b) Exercise 2.13.11 **(b)** can be solved in the same way as we solved Exercise 2.13.11 **(a)** above, after making the obvious changes (i.e., all minima should be replaced by maxima and vice versa; all inequalities in the proof of Claim 1 need to be flipped; all gcds should be replaced by lcms and vice versa). For example, instead of Claim 1, we now need the following claim (with an analogous proof):

Claim 2: Let $i, j, k \in \mathbb{N} \cup \{\infty\}$ be arbitrary. Then,

$$\max\{i, \min\{j,k\}\} = \min\{\max\{i,j\}, \max\{i,k\}\}.$$

□

Second solution to Exercise 2.13.11. **(a)** We are in one of the following two cases:

Case 1: The two integers b, c are all 0.

Case 2: The two integers b, c are not all 0.

Let us first consider Case 1. In this case, the two integers b, c are all 0. In other words, $b = 0$ and $c = 0$. Clearly, $|a| \mid |a|$. Thus, Exercise 2.11.1 **(e)** (applied to $|a|$ and $|a|$ instead of a and b) yields $\operatorname{lcm}(|a|, |a|) = ||a|| = |a|$ (since $|a| \geq 0$).

Proposition 2.9.7 **(a)** yields $\gcd(a, 0) = \gcd(a) = |a|$. Now,

$$\operatorname{lcm}\left(\gcd\left(a, \underbrace{b}_{=0}\right), \gcd\left(a, \underbrace{c}_{=0}\right)\right) = \operatorname{lcm}\left(\underbrace{\gcd(a,0)}_{=|a|}, \underbrace{\gcd(a,0)}_{=|a|}\right) = \operatorname{lcm}(|a|, |a|) = |a|.$$

[262] because any gcd and any lcm is a nonnegative integer

On the other hand, $\operatorname{lcm}\left(\underbrace{b}_{=0}, \underbrace{c}_{=0}\right) = \operatorname{lcm}(0,0) = 0$ (by Definition 2.11.4, because the integers $0, 0$ are not all nonzero). Hence,

$$\gcd\left(a, \underbrace{\operatorname{lcm}(b,c)}_{=0}\right) = \gcd(a,0) = |a|.$$

Comparing this with $\operatorname{lcm}(\gcd(a,b), \gcd(a,c)) = |a|$, we find $\gcd(a, \operatorname{lcm}(b,c)) = \operatorname{lcm}(\gcd(a,b), \gcd(a,c))$. Thus, Exercise 2.13.11 **(a)** is solved in Case 1.

Let us now consider Case 2. In this case, the two integers b, c are not all 0. Thus, $\gcd(b,c)$ is a positive integer (by Definition 2.9.6). Hence, $\gcd(b,c) > 0$, so that $\gcd(b,c) \neq 0$.

Theorem 2.9.20 (applied to a, b and c instead of s, a and b) yields $\gcd(ab, ac) = |a| \gcd(b,c)$. But (3) (applied to $x = a$ and $y = \gcd(b,c)$) yields $|a \gcd(b,c)| = |a| \cdot \underbrace{|\gcd(b,c)|}_{\substack{=\gcd(b,c) \\ (\text{since } \gcd(b,c)>0)}} = |a| \gcd(b,c)$. Comparing this with $\gcd(ab, ac) = |a| \gcd(b,c)$, we obtain

$$|a \gcd(b,c)| = \gcd\left(ab, \underbrace{ac}_{=ca}\right) = \gcd(ab, ca). \tag{397}$$

On the other hand, Theorem 2.11.6 (applied to b and c instead of a and b) yields $\gcd(b,c) \cdot \operatorname{lcm}(b,c) = |bc|$.

Now, Theorem 2.9.20 (applied to $\gcd(b,c)$, a and $\operatorname{lcm}(b,c)$ instead of s, a and b) yields

$$\begin{aligned} \gcd(\gcd(b,c)\, a, \gcd(b,c) \operatorname{lcm}(b,c)) &= \underbrace{|\gcd(b,c)|}_{\substack{=\gcd(b,c) \\ (\text{since } \gcd(b,c)>0)}} \gcd(a, \operatorname{lcm}(b,c)) \\ &= \gcd(b,c) \gcd(a, \operatorname{lcm}(b,c)). \end{aligned}$$

Hence,

$$\begin{aligned} &\gcd(b,c) \gcd(a, \operatorname{lcm}(b,c)) \\ &= \gcd\left(\underbrace{\gcd(b,c)\, a}_{=a\gcd(b,c)}, \underbrace{\gcd(b,c) \operatorname{lcm}(b,c)}_{=\gcd(b,c)\cdot\operatorname{lcm}(b,c)=|bc|}\right) \\ &= \gcd(a \gcd(b,c), |bc|) = \gcd(a \gcd(b,c), bc) \end{aligned} \tag{398}$$

(by Exercise 2.9.5 **(a)**, applied to $a \gcd(b,c)$ and bc instead of a and b).

On the other hand, Exercise 2.9.5 **(b)** (applied to $a \gcd(b,c)$ and bc instead of a and b) yields

$$\gcd(|a \gcd(b,c)|, bc) = \gcd(a \gcd(b,c), bc).$$

Comparing this with (398), we obtain

$$\gcd(b,c) \gcd(a, \operatorname{lcm}(b,c)) = \gcd\left(\underbrace{|a \gcd(b,c)|}_{\substack{=\gcd(ab,ca) \\ (\text{by } (397))}}, bc\right) = \gcd(\gcd(ab, ca), bc).$$

On the other hand, Theorem 2.9.21 **(d)** (applied to 3 and (ab, ca, bc) instead of k and $(b_1, b_2, \ldots, b_k)$) yields

$$\gcd(ab, ca, bc) = \gcd(\gcd(ab, ca), bc).$$

Comparing these two equalities, we obtain

$$\gcd(b, c)\gcd(a, \operatorname{lcm}(b, c)) = \gcd(ab, ca, bc). \tag{399}$$

But $\{bc, ca, ab\} = \{ab, ca, bc\}$. Thus, Exercise 2.9.1 (applied to 3, (bc, ca, ab), 3 and (ab, ca, bc) instead of k, $(b_1, b_2, \ldots, b_k)$, ℓ and $(c_1, c_2, \ldots, c_\ell)$) yields $\gcd(bc, ca, ab) = \gcd(ab, ca, bc)$. Comparing this with (399), we obtain

$$\gcd(b, c)\gcd(a, \operatorname{lcm}(b, c)) = \gcd(bc, ca, ab).$$

We can divide both sides of this equality by $\gcd(b, c)$ (since $\gcd(b, c) \neq 0$); thus we obtain

$$\gcd(a, \operatorname{lcm}(b, c)) = \frac{\gcd(bc, ca, ab)}{\gcd(b, c)}. \tag{400}$$

On the other hand, the three integers a, b, c are not all 0 (since the two integers b, c are not all 0). Thus, $\gcd(a, b, c)$ is a positive integer (by Definition 2.9.6). Hence, $\gcd(a, b, c) > 0$, so that $\gcd(a, b, c) \neq 0$. From $\gcd(a, b, c) \neq 0$ and $\gcd(b, c) \neq 0$, we obtain $\gcd(a, b, c) \cdot \gcd(b, c) \neq 0$.

Recall that a gcd of a finite list of integers is always nonnegative. Hence, the two numbers $\gcd(a, b)$ and $\gcd(a, c)$ are nonnegative. Thus, their product $\gcd(a, b)\gcd(a, c)$ is nonnegative as well.

Now, Theorem 2.11.6 (applied to $\gcd(a, b)$ and $\gcd(a, c)$ instead of a and b) yields

$$\begin{aligned}
&\gcd(\gcd(a, b), \gcd(a, c)) \cdot \operatorname{lcm}(\gcd(a, b), \gcd(a, c)) \\
&= |\gcd(a, b)\gcd(a, c)| = \gcd(a, b) \underbrace{\gcd(a, c)}_{\substack{=\gcd(c,a) \\ \text{(by Proposition 2.9.7 (b),} \\ \text{applied to } c \text{ instead of } b)}} \\
&\qquad (\text{since } \gcd(a, b)\gcd(a, c) \text{ is nonnegative}) \\
&= \gcd(a, b) \cdot \gcd(c, a) = \gcd(c, a) \cdot \gcd(a, b).
\end{aligned} \tag{401}$$

But $\{a, b, a, c\} = \{a, b, c\}$. Hence, Exercise 2.9.1 (applied to 4, (a, b, a, c), 3 and (a, b, c) instead of k, $(b_1, b_2, \ldots, b_k)$, ℓ and $(c_1, c_2, \ldots, c_\ell)$) yields

$$\gcd(a, b, a, c) = \gcd(a, b, c).$$

But Theorem 2.9.26 (applied to 2, (a, b), 2 and (a, c) instead of k, $(b_1, b_2, \ldots, b_k)$, ℓ and $(c_1, c_2, \ldots, c_\ell)$) yields

$$\gcd(a, b, a, c) = \gcd(\gcd(a, b), \gcd(a, c)).$$

Comparing these two equalities, we obtain

$$\gcd(\gcd(a, b), \gcd(a, c)) = \gcd(a, b, c).$$

Now, (401) yields

$$\begin{aligned}\gcd(c,a)\cdot\gcd(a,b) &= \underbrace{\gcd(\gcd(a,b),\gcd(a,c))}_{=\gcd(a,b,c)}\cdot\operatorname{lcm}(\gcd(a,b),\gcd(a,c))\\ &= \gcd(a,b,c)\cdot\operatorname{lcm}(\gcd(a,b),\gcd(a,c)).\end{aligned}$$

Dividing both sides of this equality by $\gcd(a,b,c)$ (we can do this, since $\gcd(a,b,c)\neq 0$), we obtain

$$\frac{\gcd(c,a)\cdot\gcd(a,b)}{\gcd(a,b,c)} = \operatorname{lcm}(\gcd(a,b),\gcd(a,c)). \qquad (402)$$

However, Exercise 2.10.18 yields

$$\gcd(b,c)\cdot\gcd(c,a)\cdot\gcd(a,b) = \gcd(a,b,c)\cdot\gcd(bc,ca,ab).$$

We can divide both sides of this equality by $\gcd(a,b,c)\cdot\gcd(b,c)$ (since $\gcd(a,b,c)\cdot\gcd(b,c)\neq 0$); we thus obtain

$$\frac{\gcd(c,a)\cdot\gcd(a,b)}{\gcd(a,b,c)} = \frac{\gcd(bc,ca,ab)}{\gcd(b,c)}.$$

Comparing this with (402), we find

$$\operatorname{lcm}(\gcd(a,b),\gcd(a,c)) = \frac{\gcd(bc,ca,ab)}{\gcd(b,c)} = \gcd(a,\operatorname{lcm}(b,c))$$

(by (400)). Thus, Exercise 2.13.11 **(a)** is solved in Case 2.

We have now solved Exercise 2.13.11 **(a)** in each of the two Cases 1 and 2. Thus, Exercise 2.13.11 **(a)** is solved in all cases.

[*Remark:* The above solution to Exercise 2.13.11 **(a)** is (an expanded version of) Bill Dubuque's post `https://math.stackexchange.com/a/147992/`. Note that Dubuque uses the notations $(x_1,x_2,\ldots,x_k)$ and $[x_1,x_2,\ldots,x_k]$ for what we call $\gcd(x_1,x_2,\ldots,x_k)$ and $\operatorname{lcm}(x_1,x_2,\ldots,x_k)$.]

(b) We are in one of the following two cases:

Case 1: We have $a=0$.

Case 2: We have $a\neq 0$.

Let us first consider Case 1. In this case, we have $a=0$. Thus, the two integers $a,\gcd(b,c)$ are not all nonzero. Hence, Definition 2.11.4 yields $\operatorname{lcm}(a,\gcd(b,c))=0$. Also, the two integers a,b are not all nonzero (since $a=0$). Hence, $\operatorname{lcm}(a,b)=0$ (again by Definition 2.11.4). Similarly, $\operatorname{lcm}(a,c)=0$. Now,

$$\gcd\left(\underbrace{\operatorname{lcm}(a,b)}_{=0},\underbrace{\operatorname{lcm}(a,c)}_{=0}\right) = \gcd(0,0) = 0$$

(by Definition 2.9.6, since all of the integers $0,0$ are 0). Comparing this with $\operatorname{lcm}(a,\gcd(b,c))=0$, we obtain $\operatorname{lcm}(a,\gcd(b,c)) = \gcd(\operatorname{lcm}(a,b),\operatorname{lcm}(a,c))$. Thus, Exercise 2.13.11 **(b)** is solved in Case 1.

Let us now consider Case 2. In this case, we have $a\neq 0$. Hence, the two integers a,b are not all 0. Thus, $\gcd(a,b)$ is a positive integer (by Definition 2.9.6). Similarly, $\gcd(a,c)$ is a positive integer. Also, the three integers a, b, c are not all 0 (since $a \neq 0$). Thus, $\gcd(a, b, c)$ is a positive integer (by Definition 2.9.6). Hence, $\gcd(a, b, c) \neq 0$.

The numbers $\gcd(a, b)$ and $\gcd(a, c)$ are positive integers. Hence, their product $\gcd(a, b) \cdot \gcd(a, c)$ is a positive integer as well. Let us denote this positive integer by g. Thus,

$$\begin{aligned} g &= \gcd(a, b) \cdot \underbrace{\gcd(a, c)}_{\substack{=\gcd(c,a) \\ \text{(by Proposition 2.9.7 \textbf{(b)},} \\ \text{applied to } c \text{ instead of } b)}} = \gcd(a, b) \cdot \gcd(c, a) \\ &= \gcd(c, a) \cdot \gcd(a, b). \end{aligned} \tag{403}$$

Also, $g \neq 0$ (since g is positive).

Theorem 2.11.6 yields $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = |ab|$. Also, Theorem 2.11.6 (applied to c instead of b) yields $\gcd(a, c) \cdot \operatorname{lcm}(a, c) = |ac|$.

Theorem 2.9.20 (applied to g, $\operatorname{lcm}(a, b)$ and $\operatorname{lcm}(a, c)$ instead of s, a and b) yields

$$\begin{aligned} \gcd(g \operatorname{lcm}(a, b), g \operatorname{lcm}(a, c)) &= \underbrace{|g|}_{\substack{=g \\ \text{(since } g \text{ is positive)}}} \gcd(\operatorname{lcm}(a, b), \operatorname{lcm}(a, c)) \\ &= g \gcd(\operatorname{lcm}(a, b), \operatorname{lcm}(a, c)). \end{aligned}$$

Hence,

$$\begin{aligned} & g \gcd(\operatorname{lcm}(a, b), \operatorname{lcm}(a, c)) \\ &= \gcd\left(\underbrace{g}_{=\gcd(c,a)\cdot\gcd(a,b)} \operatorname{lcm}(a, b), \underbrace{g}_{=\gcd(a,b)\cdot\gcd(a,c)} \operatorname{lcm}(a, c) \right) \\ &= \gcd\left(\gcd(c, a) \cdot \underbrace{\gcd(a, b) \cdot \operatorname{lcm}(a, b)}_{=|ab|}, \gcd(a, b) \cdot \underbrace{\gcd(a, c) \cdot \operatorname{lcm}(a, c)}_{=|ac|} \right) \\ &= \gcd(\gcd(c, a) \cdot |ab|, \gcd(a, b) \cdot |ac|). \end{aligned} \tag{404}$$

On the other hand, Theorem 2.9.20 (applied to ab, c and a instead of s, a and b) yields

$$\gcd(abc, aba) = |ab| \gcd(c, a) = \gcd(c, a) \cdot |ab|. \tag{405}$$

Also, Theorem 2.9.20 (applied to ac, a and b instead of s, a and b) yields

$$\gcd(aca, acb) = |ac| \gcd(a, b) = \gcd(a, b) \cdot |ac|. \tag{406}$$

Also, $\left\{ abc, \underbrace{aba}_{=aab}, aca, \underbrace{acb}_{=abc} \right\} = \{abc, aab, aca, abc\} = \{abc, aca, aab\}$. Hence, Exercise 2.9.1 (applied to 4, (abc, aba, aca, acb), 3 and (abc, aca, aab) instead of k, $(b_1, b_2, \ldots, b_k)$, ℓ and $(c_1, c_2, \ldots, c_\ell)$) yields

$$\gcd(abc, aba, aca, acb) = \gcd(abc, aca, aab) = |a| \gcd(bc, ca, ab)$$

(by Exercise 2.9.7, applied to a, 3 and (bc, ca, ab) instead of s, k and $(a_1, a_2, \ldots, a_k)$). Hence,

$$|a| \gcd(bc, ca, ab) = \gcd(abc, aba, aca, acb) = \gcd\left(\underbrace{\gcd(abc, aba)}_{\substack{=\gcd(c,a)\cdot|ab| \\ \text{(by (405))}}}, \underbrace{\gcd(aca, acb)}_{\substack{=\gcd(a,b)\cdot|ac| \\ \text{(by (406))}}}\right)$$

$$\left(\begin{array}{c}\text{by Theorem 2.9.26, applied to 2, } (abc, aba)\text{, 2 and } (aca, acb) \\ \text{instead of } k,\ (b_1, b_2, \ldots, b_k)\text{, } \ell \text{ and } (c_1, c_2, \ldots, c_\ell)\end{array}\right)$$

$$= \gcd(\gcd(c, a) \cdot |ab|, \gcd(a, b) \cdot |ac|) = g \gcd(\operatorname{lcm}(a, b), \operatorname{lcm}(a, c))$$

(by (404)). We can divide both sides of this equality by g (since $g \neq 0$); thus we obtain

$$\frac{|a| \gcd(bc, ca, ab)}{g} = \gcd(\operatorname{lcm}(a, b), \operatorname{lcm}(a, c)). \qquad (407)$$

Proposition 2.9.7 **(b)** (applied to $\gcd(b, c)$ instead of b) yields $\gcd(a, \gcd(b, c)) = \gcd(\gcd(b, c), a)$. But Theorem 2.9.21 **(d)** (applied to 3 and (b, c, a) instead of k and $(b_1, b_2, \ldots, b_k)$) yields $\gcd(b, c, a) = \gcd(\gcd(b, c), a)$. Comparing these two equalities, we obtain

$$\gcd(a, \gcd(b, c)) = \gcd(b, c, a). \qquad (408)$$

But $\{b, c, a\} = \{a, b, c\}$. Thus, Exercise 2.9.1 (applied to 3, (b, c, a), 3 and (a, b, c) instead of k, $(b_1, b_2, \ldots, b_k)$, ℓ and $(c_1, c_2, \ldots, c_\ell)$) yields $\gcd(b, c, a) = \gcd(a, b, c)$. Thus, (408) becomes

$$\gcd(a, \gcd(b, c)) = \gcd(b, c, a) = \gcd(a, b, c). \qquad (409)$$

The gcd of any list of integers is a nonnegative integer. Thus, $\gcd(b, c)$ is a nonnegative integer. Now, Theorem 2.11.6 (applied to $\gcd(b, c)$ instead of b) yields

$$\begin{aligned} &\gcd(a, \gcd(b, c)) \cdot \operatorname{lcm}(a, \gcd(b, c)) \\ &= |a \gcd(b, c)| = |a| \cdot \underbrace{|\gcd(b, c)|}_{\substack{=\gcd(b,c) \\ \text{(since } \gcd(b,c) \\ \text{is nonnegative)}}} \qquad \text{(by (3), applied to } x = a \text{ and } y = \gcd(b, c)\text{)} \\ &= |a| \gcd(b, c). \end{aligned}$$

In view of (409), this rewrites as

$$\gcd(a, b, c) \cdot \operatorname{lcm}(a, \gcd(b, c)) = |a| \gcd(b, c). \qquad (410)$$

Multiplying both sides of this equality by g, we obtain

$$\begin{aligned} \gcd(a, b, c) \cdot \operatorname{lcm}(a, \gcd(b, c)) \cdot g &= |a| \gcd(b, c) \cdot \underbrace{g}_{\substack{=\gcd(c,a)\cdot\gcd(a,b) \\ \text{(by (403))}}} \\ &= |a| \underbrace{\gcd(b, c) \cdot \gcd(c, a) \cdot \gcd(a, b)}_{\substack{=\gcd(a,b,c)\cdot\gcd(bc,ca,ab) \\ \text{(by Exercise 2.10.18)}}} \\ &= |a| \gcd(a, b, c) \cdot \gcd(bc, ca, ab) \\ &= \gcd(a, b, c) \cdot |a| \gcd(bc, ca, ab). \end{aligned}$$

We can divide both sides of this equality by $\gcd(a,b,c)$ (since $\gcd(a,b,c) \neq 0$); we thus obtain

$$\operatorname{lcm}(a, \gcd(b,c)) \cdot g = |a| \gcd(bc, ca, ab).$$

We can divide both sides of this equality by g (since $g \neq 0$); thus we find

$$\operatorname{lcm}(a, \gcd(b,c)) = \frac{|a| \gcd(bc, ca, ab)}{g} = \gcd(\operatorname{lcm}(a,b), \operatorname{lcm}(a,c))$$

(by (407)). Thus, Exercise 2.13.11 **(b)** is solved in Case 2.

We have now solved Exercise 2.13.11 **(b)** in each of the two Cases 1 and 2. Thus, Exercise 2.13.11 **(b)** is solved in all cases. □

10.63. Solution to Exercise 2.13.12

Solution to Exercise 2.13.12. We have $a^2 \equiv 1 \operatorname{mod} p$. In other words, $p \mid a^2 - 1 = (a-1)(a+1)$. Hence, Theorem 2.13.6 (applied to $a-1$ and $a+1$ instead of a and b) yields that $p \mid a-1$ or $p \mid a+1$. In view of the logical equivalences

$$(p \mid a-1) \iff (a \equiv 1 \operatorname{mod} p)$$

and

$$\left(p \mid \underbrace{a+1}_{=a-(-1)}\right) \iff (p \mid a-(-1)) \iff (a \equiv -1 \operatorname{mod} p),$$

this rewrites as follows: $a \equiv 1 \operatorname{mod} p$ or $a \equiv -1 \operatorname{mod} p$. This solves Exercise 2.13.12. □

10.64. Solution to Exercise 2.13.13

Solution to Exercise 2.13.13. The number p is a prime, and thus is a positive integer. Hence, p^k is a positive integer as well (since $k \in \mathbb{N}$).

For each $i \in \{0,1,\ldots,k\}$, the integer p^i is a nonnegative divisor of p^k [263]. In other words, the integers $p^0, p^1, \ldots, p^k$ are nonnegative divisors of p^k. In other words, we have

$$\left\{p^0, p^1, \ldots, p^k\right\} \subseteq \left\{\text{the nonnegative divisors of } p^k\right\}. \tag{411}$$

Now we shall show that $\left\{\text{the nonnegative divisors of } p^k\right\} \subseteq \left\{p^0, p^1, \ldots, p^k\right\}$.

Indeed, let $d \in \left\{\text{the nonnegative divisors of } p^k\right\}$. Thus, d is a nonnegative divisor of p^k. Hence, in particular, d is a divisor of p^k; thus, $d \mid p^k$. In other words, there exists an integer c such that $p^k = dc$. Consider this c. If we had $d = 0$, then we would have $p^k = \underbrace{d}_{=0} c = 0c = 0$, which would contradict the fact that p^k is positive. Hence, we

[263] *Proof.* Let $i \in \{0,1,\ldots,k\}$. We must show that the integer p^i is a nonnegative divisor of p^k.

The number p is a positive integer. Thus, p^i is a positive integer (since $i \in \{0,1,\ldots,k\} \subseteq \mathbb{N}$). Hence, p^i is a nonnegative integer. Furthermore, $i \leq k$ (since $i \in \{0,1,\ldots,k\}$). Hence, Exercise 2.2.4 (applied to $n = p$, $a = i$ and $b = k$) yields $p^i \mid p^k$. Thus, p^i is a divisor of p^k. Hence, p^i is a nonnegative divisor of p^k (since p^i is nonnegative). Qed.

cannot have $d = 0$. Thus, we have $d \neq 0$. Hence, d is nonzero. Therefore, Lemma 2.13.27 **(a)** (applied to $n = d$) shows that there exists a nonzero integer u such that $u \perp p$ and $d = up^{v_p(d)}$. Consider this u. From $d = up^{v_p(d)}$, we obtain $u = d/p^{v_p(d)}$, and thus u is nonnegative (since d is nonnegative and p is positive).

Let $i = v_p(d)$. Then, $i = v_p(d) \in \mathbb{N}$ (since d is nonzero). Moreover, from $i = v_p(d)$, we obtain $up^i = up^{v_p(d)} = d$ (since $d = up^{v_p(d)}$). Moreover, u is an integer; thus,

$$p^i \mid up^i = d \mid p^k.$$

But Lemma 2.13.25 (applied to $n = p^k$) yields that $p^i \mid p^k$ if and only if $v_p\left(p^k\right) \geq i$. Hence, $v_p\left(p^k\right) \geq i$ (since $p^i \mid p^k$).

However, Theorem 2.13.28 **(d)** (applied to $q = p$) yields $v_p(p) = \begin{cases} 1, & \text{if } p = p; \\ 0, & \text{if } p \neq p \end{cases} = 1$ (since $p = p$). But Exercise 2.13.6 (applied to $a = p$) yields $v_p\left(p^k\right) = k \underbrace{v_p(p)}_{=1} = k \cdot 1 = k$. Hence, $k = v_p\left(p^k\right) \geq i$, so that $i \leq k$ and thus $i \in \{0, 1, \ldots, k\}$ (since $i \in \mathbb{N}$).

We have $u \perp p$. Thus, Exercise 2.10.4 (applied to $a = u$, $b = p$, $n = 1$ and $m = k$) yields $u^1 \perp p^k$. In other words, $u \perp p^k$ (since $u^1 = u$). In other words, $\gcd\left(u, p^k\right) = 1$ (by the definition of coprimality).

But $u \mid up^i \mid p^k$ (as we have shown above). Hence, Proposition 2.9.7 **(i)** (applied to $a = u$ and $b = p^k$) yields $\gcd\left(u, p^k\right) = |u| = u$ (since u is nonnegative). Thus, $u = \gcd\left(u, p^k\right) = 1$. Therefore, from $up^i = d$, we obtain $d = \underbrace{u}_{=1} p^i = p^i \in \left\{p^0, p^1, \ldots, p^k\right\}$ (since $i \in \{0, 1, \ldots, k\}$).

Now, forget that we fixed d. We thus have shown that $d \in \left\{p^0, p^1, \ldots, p^k\right\}$ for each $d \in \left\{\text{the nonnegative divisors of } p^k\right\}$. In other words,

$$\left\{\text{the nonnegative divisors of } p^k\right\} \subseteq \left\{p^0, p^1, \ldots, p^k\right\}.$$

Combining this with (411), we obtain

$$\left\{\text{the nonnegative divisors of } p^k\right\} = \left\{p^0, p^1, \ldots, p^k\right\}.$$

In other words, the nonnegative divisors of p^k are $p^0, p^1, \ldots, p^k$. This solves Exercise 2.13.13. □

10.65. Solution to Exercise 2.14.1

Solution to Exercise 2.14.1. Let M be the set $\left\{1p, 2p, \ldots, p^{k-1}p\right\} = \left\{cp \mid c \in \left\{1, 2, \ldots, p^{k-1}\right\}\right\}$. This set M has p^{k-1} elements (since the p^{k-1} numbers $1p, 2p, \ldots, p^{k-1}p$ are all distinct). In other words, $|M| = p^{k-1}$. Also, $M \subseteq \left\{1, 2, \ldots, p^k\right\}$ [264]. Hence,

$$\left|\left\{1, 2, \ldots, p^k\right\} \setminus M\right| = \underbrace{\left|\left\{1, 2, \ldots, p^k\right\}\right|}_{=p^k} - \underbrace{|M|}_{=p^{k-1}} = p^k - p^{k-1}. \qquad (412)$$

[264] *Proof.* Let $m \in M$. Thus, $m \in M = \left\{1p, 2p, \ldots, p^{k-1}p\right\}$; in other words, $m = cp$ for some $c \in \left\{1, 2, \ldots, p^{k-1}\right\}$. Consider this c. From $c \in \left\{1, 2, \ldots, p^{k-1}\right\}$, we obtain $c \leq p^{k-1}$. We can multiply this inequality by p (since $p > 0$) and thus obtain $cp \leq p^{k-1}p = p^k$. Also, cp is a

Next, we claim that

$$\left\{i \in \left\{1,2,\ldots,p^k\right\} \mid i \perp p^k\right\} \subseteq \left\{1,2,\ldots,p^k\right\} \setminus M. \tag{413}$$

[*Proof of (413):* Let $a \in \{i \in \{1,2,\ldots,p^k\} \mid i \perp p^k\}$. In other words, a is an element of $\{1,2,\ldots,p^k\}$ and satisfies $a \perp p^k$.

Exercise 2.13.3 shows that $a \perp p^k$ holds if and only if $p \nmid a$. Hence, $p \nmid a$ (since $a \perp p^k$), and therefore $a \notin M$ [265]. Combining $a \in \{1,2,\ldots,p^k\}$ with $a \notin M$, we obtain $a \in \{1,2,\ldots,p^k\} \setminus M$.

Now, forget that we fixed a. Thus, we have shown that $a \in \{1,2,\ldots,p^k\} \setminus M$ for each $a \in \{i \in \{1,2,\ldots,p^k\} \mid i \perp p^k\}$. In other words, $\{i \in \{1,2,\ldots,p^k\} \mid i \perp p^k\} \subseteq \{1,2,\ldots,p^k\} \setminus M$. This proves (413).]

Furthermore, we have

$$\left\{1,2,\ldots,p^k\right\} \setminus M \subseteq \left\{i \in \left\{1,2,\ldots,p^k\right\} \mid i \perp p^k\right\}. \tag{414}$$

[*Proof of (414):* Let $a \in \{1,2,\ldots,p^k\} \setminus M$. In other words, $a \in \{1,2,\ldots,p^k\}$ and $a \notin M$.

We have $p \nmid a$ [266]. But Exercise 2.13.3 shows that $a \perp p^k$ holds if and only if $p \nmid a$. Hence, $a \perp p^k$ (since $p \nmid a$). Now, we know that a is an $i \in \{1,2,\ldots,p^k\}$ satisfying $i \perp p^k$ (since $a \in \{1,2,\ldots,p^k\}$ and $a \perp p^k$). In other words, $a \in \{i \in \{1,2,\ldots,p^k\} \mid i \perp p^k\}$.

Now, forget that we fixed a. Thus, we have shown that $a \in \{i \in \{1,2,\ldots,p^k\} \mid i \perp p^k\}$ for each $a \in \{1,2,\ldots,p^k\} \setminus M$. In other words, $\{1,2,\ldots,p^k\} \setminus M \subseteq \{i \in \{1,2,\ldots,p^k\} \mid i \perp p^k\}$. This proves (414).]

Combining (413) with (414), we obtain

$$\left\{i \in \left\{1,2,\ldots,p^k\right\} \mid i \perp p^k\right\} = \left\{1,2,\ldots,p^k\right\} \setminus M.$$

positive integer (since c and p are positive integers). Thus, cp is a positive integer and $\leq p^k$. In other words, $cp \in \left\{1,2,\ldots,p^k\right\}$. Thus, $m = cp \in \left\{1,2,\ldots,p^k\right\}$.

Now, forget that we fixed m. We thus have shown that $m \in \left\{1,2,\ldots,p^k\right\}$ for each $m \in M$. In other words, $M \subseteq \left\{1,2,\ldots,p^k\right\}$.

[265] *Proof.* Assume the contrary. Thus, $a \in M = \left\{1p, 2p, \ldots, p^{k-1}p\right\}$. In other words, $a = cp$ for some $c \in \left\{1,2,\ldots,p^{k-1}\right\}$. Consider this c. Clearly, c is an integer; thus, from $a = cp = pc$, we obtain $p \mid a$. But this contradicts $p \nmid a$. This contradiction shows that our assumption was false, qed.

[266] *Proof.* Assume the contrary. Thus, $p \mid a$. In other words, $a = pc$ for some integer c. Consider this c. We have $a = pc$, thus $c = a/p$ (since p is nonzero). Also, $c = a/p > 0$ (since a and p are positive). Hence, c is a positive integer. Furthermore, from $a \in \left\{1,2,\ldots,p^k\right\}$, we obtain $a \leq p^k$ and thus $a/p \leq p^k/p = p^{k-1}$, so that $c = a/p \leq p^{k-1}$. Thus, $c \in \left\{1,2,\ldots,p^{k-1}\right\}$ (since c is a positive integer) and therefore $cp \in \left\{1p, 2p, \ldots, p^{k-1}p\right\} = M$ (by the definition of M). Now, $a = pc = cp \in M$; but this contradicts $a \notin M$. This contradiction shows that our assumption was false, qed.

Now, (55) (applied to $n = p^k$) yields

$$\begin{aligned}\phi\left(p^k\right) &= \left|\underbrace{\left\{i \in \left\{1,2,\ldots,p^k\right\} \ \mid\ i \perp p^k\right\}}_{=\left\{1,2,\ldots,p^k\right\}\setminus M}\right| = \left|\left\{1,2,\ldots,p^k\right\}\setminus M\right| \\ &= \underbrace{p^k}_{=pp^{k-1}} - p^{k-1} \qquad \text{(by (412))} \\ &= pp^{k-1} - p^{k-1} = (p-1)\,p^{k-1}.\end{aligned}$$

This solves Exercise 2.14.1. □

10.66. Solution to Exercise 2.14.2

Solution to Exercise 2.14.2. **(a)** If I is any set, and if we are given a statement $\mathcal{A}(i)$ for each $i \in I$, then

$$\{i \in I \ \mid\ \text{we don't have } \mathcal{A}(i)\} = I \setminus \{i \in I \ \mid\ \mathcal{A}(i)\}. \tag{415}$$

(This is one of the basic rules of sets and logic.)

Now,

$$\begin{aligned}&\left|\underbrace{\{i \in \{1,2,\ldots,n\} \ \mid\ \text{we don't have } i \perp n\}}_{\substack{=\{1,2,\ldots,n\}\setminus\{i\in\{1,2,\ldots,n\} \ \mid\ i\perp n\} \\ \text{(by (415), applied to } I=\{1,2,\ldots,n\} \text{ and } \mathcal{A}(i)=(i\perp n))}}\right| \\ &= \left|\{1,2,\ldots,n\}\setminus\{i\in\{1,2,\ldots,n\} \ \mid\ i\perp n\}\right| \\ &= \underbrace{\left|\{1,2,\ldots,n\}\right|}_{=n} - \underbrace{\left|\{i\in\{1,2,\ldots,n\} \ \mid\ i\perp n\}\right|}_{\substack{=\phi(n) \\ \text{(by (55))}}} \\ &\qquad \left(\text{since } \{i\in\{1,2,\ldots,n\} \ \mid\ i\perp n\} \subseteq \{1,2,\ldots,n\}\right) \\ &= n - \phi(n).\end{aligned}$$

This solves Exercise 2.14.2 **(a)**.

(b) Exercise 2.14.2 **(a)** yields

$$n - \phi(n) = \left|\{i\in\{1,2,\ldots,n\} \ \mid\ \text{we don't have } i\perp n\}\right| \geq 0$$

(since $|X| \geq 0$ for any finite set X). This solves Exercise 2.14.2 **(b)**.

(c) We have $d \mid n$ and $n \neq 0$ (since n is positive). Thus, Proposition 2.2.3 **(a)** (applied to $a = d$ and $b = n$) yields $|d| \leq |n| = n$ (since n is positive). But $|d| = d$ (since d is positive). Hence, $d = |d| \leq n$.

It is easy to see that

$$\begin{aligned}&\{i\in\{1,2,\ldots,d\} \ \mid\ \text{we don't have } i\perp d\} \\ &\subseteq \{i\in\{1,2,\ldots,n\} \ \mid\ \text{we don't have } i\perp n\}.\end{aligned} \tag{416}$$

[*Proof of (416):* Let $j \in \{i \in \{1,2,\ldots,d\} \mid \text{we don't have } i \perp d\}$. Thus, j is an $i \in \{1,2,\ldots,d\}$ such that we don't have $i \perp d$. In other words, j is an element of $\{1,2,\ldots,d\}$ and has the property that we don't have $j \perp d$.

Now, recall that j is an element of $\{1,2,\ldots,d\}$. Hence, $j \in \{1,2,\ldots,d\} \subseteq \{1,2,\ldots,n\}$ (since $d \leq n$). In other words, j is an element of $\{1,2,\ldots,n\}$.

Also, we don't have $j \perp d$. Hence, we don't have $j \perp n$ [267]. Now, we know that j is an element of $\{1,2,\ldots,n\}$ and has the property that we don't have $j \perp n$. In other words, j is an $i \in \{1,2,\ldots,n\}$ such that we don't have $i \perp n$. In other words, $j \in \{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\}$.

Now, forget that we fixed j. We thus have proven that $j \in \{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\}$ for each $j \in \{i \in \{1,2,\ldots,d\} \mid \text{we don't have } i \perp d\}$. In other words,

$$\{i \in \{1,2,\ldots,d\} \mid \text{we don't have } i \perp d\} \subseteq \{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\}.$$

This proves (416).]

Now, Exercise 2.14.2 **(a)** (applied to d instead of n) yields

$$\begin{aligned} d - \phi(d) &= \left| \underbrace{\{i \in \{1,2,\ldots,d\} \mid \text{we don't have } i \perp d\}}_{\substack{\subseteq \{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\} \\ \text{(by (416))}}} \right| \\ &\leq |\{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\}| = n - \phi(n) \end{aligned}$$

(by Exercise 2.14.2 **(a)**). Thus, Exercise 2.14.2 **(c)** is solved.

(d) In our solution to Exercise 2.14.2 **(c)** above, we have shown that $d \leq n$. Combining this with $d \neq n$, we obtain $d < n$. Thus, $n > d$. Also, $d \geq 1$ (since d is a positive integer). Hence, $n > d \geq 1$.

Define two finite sets

$$\begin{aligned} D &= \{i \in \{1,2,\ldots,d\} \mid \text{we don't have } i \perp d\} \qquad \text{and} \\ N &= \{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\}. \end{aligned}$$

In our solution to Exercise 2.14.2 **(c)** above, we have proven (416). Thus,

$$\begin{aligned} D &= \{i \in \{1,2,\ldots,d\} \mid \text{we don't have } i \perp d\} \\ &\subseteq \{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\} \qquad \text{(by (416))} \\ &= N. \end{aligned}$$

Now, we have $n \in N$.

[267] *Proof:* Assume the contrary. Thus, $j \perp n$. In other words, $\gcd(j,n) = 1$. But $j \mid j$ and $d \mid n$. Hence, Exercise 2.9.4 (applied to j, d, j and n instead of a_1, a_2, b_1 and b_2) yields $\gcd(j,d) \mid \gcd(j,n) = 1$. But $\gcd(j,d)$ is a nonnegative integer (since the gcd of any list of integers is a nonnegative integer). Hence, Exercise 2.2.5 (applied to $g = \gcd(j,d)$) yields $\gcd(j,d) = 1$ (since $\gcd(j,d) \mid 1$). In other words, $j \perp d$. This contradicts the fact that we don't have $j \perp d$. This contradiction shows that our assumption was wrong, qed.

[*Proof:* We have $n \in \{1,2,\ldots,n\}$ (since $n \geq 1$), but we don't have $n \perp n$ [268]. Thus, n is an element of $\{1,2,\ldots,n\}$ such that we don't have $n \perp n$. In other words, n is an $i \in \{1,2,\ldots,n\}$ such that we don't have $i \perp n$. Hence,

$$n \in \{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\}.$$

This rewrites as $n \in N$ (since $N = \{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\}$). Qed.]

Now, we claim that $D \neq N$.

[*Proof:* Assume the contrary. Thus, $D = N$. Hence, $N = D$. Now,

$$n \in N = D = \{i \in \{1,2,\ldots,d\} \mid \text{we don't have } i \perp d\} \subseteq \{1,2,\ldots,d\},$$

so that $n \leq d$. This contradicts $d < n$. This contradiction shows that our assumption was false. Hence, $D \neq N$ is proven.]

Now, D is a subset of N (since $D \subseteq N$), and hence is a proper subset of N (since $D \neq N$). Hence, $|D| < |N|$ (because if X is a proper subset of a finite set Y, then $|X| < |Y|$). But Exercise 2.14.2 **(a)** (applied to d instead of n) yields

$$\begin{aligned} d - \phi(d) &= \left|\underbrace{\{i \in \{1,2,\ldots,d\} \mid \text{we don't have } i \perp d\}}_{=D}\right| = |D| \\ &< \left|\underbrace{N}_{=\{i\in\{1,2,\ldots,n\} \mid \text{we don't have } i\perp n\}}\right| \\ &= |\{i \in \{1,2,\ldots,n\} \mid \text{we don't have } i \perp n\}| = n - \phi(n) \end{aligned}$$

(by Exercise 2.14.2 **(a)**). Thus, Exercise 2.14.2 **(d)** is solved. □

10.67. Solution to Exercise 2.14.4

Solution to Exercise 2.14.4. The following solution is mostly a calque of the proof of Proposition 2.14.7 we gave above, but using subtraction instead of division and using the relation "coprime" instead of "divides".

Clearly, n is a positive integer (since $n > 2$), so that $\phi(n)$ is well-defined.

Let $C = \{i \in \{1,2,\ldots,n\} \mid i \perp n\}$. An element c of C is said to be

- *small* if $c < n - c$;
- *medium* if $c = n - c$;
- *large* if $c > n - c$.

[268] *Proof.* Assume the contrary. Thus, $n \perp n$. In other words, $\gcd(n,n) = 1$. But Proposition 2.9.7 **(i)** (applied to $a = n$ and $b = n$) yields $\gcd(n,n) = |n|$ (since $n \mid n$). Hence, $\gcd(n,n) = |n| = n$ (since $n > 1 > 0$). Therefore, $n = \gcd(n,n) = 1$. This contradicts $n > 1$. This contradiction shows that our assumption was wrong, qed.

Now, it is easy to see that the set C has no medium elements[269]. In other words,

$$|\{\text{medium elements of } C\}| = 0.$$

Furthermore, if $c \in C$, then $n - c \in C$ [270]. This allows us to define a map

$$F : C \to C,$$
$$c \mapsto n - c.$$

This map F has the property that $F \circ F = \text{id}$, because each $c \in C$ satisfies

$$\begin{aligned} (F \circ F)(c) &= F\left(\underbrace{F(c)}_{\substack{=n-c \\ \text{(by the definition of } F)}}\right) = F(n-c) \\ &= n - (n-c) \qquad \text{(by the definition of } F) \\ &= c = \text{id}(c). \end{aligned}$$

Hence, the map F is inverse to itself. Thus, the map F is invertible, i.e., is a bijection.

[269] *Proof.* Let c be a medium element of C. We shall derive a contradiction.

We have $c \in C = \{i \in \{1, 2, \ldots, n\} \mid i \perp n\}$. In other words, c is an element of $\{1, 2, \ldots, n\}$ and satisfies $c \perp n$. Clearly, the integer c is positive (since $c \in \{1, 2, \ldots, n\}$) and we have $\gcd(c, n) = 1$ (since $c \perp n$).

Furthermore, c is medium; in other words, $c = n - c$. Thus, $2c = n$, so that $n = 2c = c \cdot 2$. Hence, $c \mid n$. Thus, Proposition 2.9.7 **(i)** (applied to $a = c$ and $b = n$) yields $\gcd(c, n) = |c| = c$ (since c is positive). But from $2c = n$, we also obtain $c = n/2 > 2/2$ (since $n > 2$). Thus, $\gcd(c, n) = c > 2/2 = 1$. This contradicts $\gcd(c, n) = 1$.

Forget that we fixed c. We thus have obtained a contradiction for each medium element c of C. Thus, there are no such elements. In other words, the set C has no medium elements.

[270] *Proof.* Let $c \in C$.

We have $c \in C = \{i \in \{1, 2, \ldots, n\} \mid i \perp n\}$. In other words, c is an element of $\{1, 2, \ldots, n\}$ and satisfies $c \perp n$. From $c \perp n$, we obtain $n \perp c$ (by Proposition 2.10.4) and thus $\gcd(n, c) = 1$.

But $n \mid n$. Hence, Proposition 2.9.7 **(i)** (applied to $a = n$ and $b = n$) yields $\gcd(n, n) = |n| = n$ (since n is positive). Thus, $\gcd(n, n) = n > 2 > 1$, so that $\gcd(n, n) \neq 1 = \gcd(n, c)$ and therefore $n \neq c$. In other words, $c \neq n$.

Combining $c \in \{1, 2, \ldots, n\}$ with $c \neq n$, we find $c \in \{1, 2, \ldots, n\} \setminus \{n\} = \{1, 2, \ldots, n-1\}$. Hence, $n - c \in \{1, 2, \ldots, n-1\} \subseteq \{1, 2, \ldots, n\}$.

We have $\underbrace{n}_{\equiv 0 \operatorname{mod} n} - c \equiv -c \operatorname{mod} n$. Hence, Proposition 2.9.7 **(d)** (applied to n, $n - c$ and $-c$ instead of a, b and c) yields

$$\begin{aligned} \gcd(n, n-c) &= \gcd(n, -c) \\ &= \gcd(n, c) \qquad \text{(by Proposition 2.9.7 \textbf{(h)} (applied to } a = n \text{ and } b = c)) \\ &= 1. \end{aligned}$$

In other words, $n \perp n - c$. In other words, $n - c \perp n$ (by Proposition 2.10.4).

Combining this with $n - c \in \{1, 2, \ldots, n\}$, we conclude that $n - c$ is an $i \in \{1, 2, \ldots, n\}$ satisfying $i \perp n$. In other words, $n - c \in \{i \in \{1, 2, \ldots, n\} \mid i \perp n\} = C$. Qed.

It is easy to see that if c is a small element of C, then $F(c)$ is a large element of C [271]. Hence, the map

$$F^{+} : \{\text{small elements of } C\} \to \{\text{large elements of } C\}, \\ c \mapsto F(c)$$

is well-defined. Similarly, the map

$$F^{-} : \{\text{large elements of } C\} \to \{\text{small elements of } C\}, \\ c \mapsto F(c)$$

is well-defined. These two maps F^{+} and F^{-} are both restrictions of the map F, and thus are mutually inverse (since the map F is inverse to itself). Hence, the map F^{+} is invertible, i.e., is a bijection. Thus, we have found a bijection from $\{\text{small elements of } C\}$ to $\{\text{large elements of } C\}$ (namely, F^{+}). Therefore,

$$|\{\text{small elements of } C\}| = |\{\text{large elements of } C\}|.$$

Now, (55) yields

$$\begin{aligned}
\phi(n) &= \left| \underbrace{\{i \in \{1,2,\ldots,n\} \ \mid \ i \perp n\}}_{=C} \right| = |C| \\
&= \underbrace{|\{\text{small elements of } C\}|}_{=|\{\text{large elements of } C\}|} + \underbrace{|\{\text{medium elements of } C\}|}_{=0} + |\{\text{large elements of } C\}| \\
&\qquad \left(\begin{array}{c} \text{since each element of } C \text{ is either small or medium or large} \\ \text{(and there is no overlap between these three classes of elements)} \end{array} \right) \\
&= |\{\text{large elements of } C\}| + |\{\text{large elements of } C\}| \\
&= 2 \cdot |\{\text{large elements of } C\}|.
\end{aligned}$$

Thus, $2 \mid \phi(n)$ (since $|\{\text{large elements of } C\}|$ is an integer). In other words, $\phi(n)$ is even. This solves Exercise 2.14.4. □

10.68. Solution to Exercise 2.14.5

Our below solution to Exercise 2.14.5 imitates the proof of Proposition 2.10.12.

Solution to Exercise 2.14.5. We do not have $n \perp n$ [272]. Hence,

$$\{i \in \{1,2,\ldots,n\} \ \mid \ i \perp n\} = \{i \in \{1,2,\ldots,n-1\} \ \mid \ i \perp n\} \tag{417}$$

[271] *Proof.* Let c be a small element of C. Thus, $c < n - c$. Hence, $n - c > c = n - (n - c)$. In view of $F(c) = n - c$, this rewrites as $F(c) > n - F(c)$. In other words, $F(c)$ is a large element of C (by the definition of "large"). Qed.

[272] *Proof.* Assume the contrary. Thus, $n \perp n$. In other words, $\gcd(n,n) = 1$. But Proposition 2.9.7 **(i)** (applied to $a = n$ and $b = n$) yields $\gcd(n,n) = |n|$ (since $n \mid n$). Hence, $\gcd(n,n) = |n| = n$ (since $n > 1 > 0$). Therefore, $n = \gcd(n,n) = 1$. This contradicts $n > 1$. This contradiction shows that our assumption was wrong, qed.

[273]. Now, (55) yields

$$\phi(n) = |\{i \in \{1,2,\ldots,n\} \mid i \perp n\}| \\ = |\{i \in \{1,2,\ldots,n-1\} \mid i \perp n\}| \qquad (418)$$

(by (417)).

On the other hand, for each $k \in \mathbb{Z}$, we have the logical equivalence

$$(n-k \perp n) \iff (k \perp n) \qquad (419)$$

(because Exercise 2.10.7 (applied to $a = k$ and $b = n$) shows that $n-k \perp n$ holds if and

[273] *Proof of (417):* Let $j \in \{i \in \{1,2,\ldots,n\} \mid i \perp n\}$. Thus, j is an element i of $\{1,2,\ldots,n\}$ satisfying $i \perp n$. In other words, j is an element of $\{1,2,\ldots,n\}$ and satisfies $j \perp n$. We have $j \perp n$. If we had $j = n$, then this would rewrite as $n \perp n$, which would contradict the fact that we do not have $n \perp n$. Thus, we cannot have $j = n$. In other words, we have $j \neq n$. Combining $j \in \{1,2,\ldots,n\}$ with $j \neq n$, we obtain $j \in \{1,2,\ldots,n\} \setminus \{n\} = \{1,2,\ldots,n-1\}$. Hence, j is an element of $\{1,2,\ldots,n-1\}$ and satisfies $j \perp n$. In other words, j is an element i of $\{1,2,\ldots,n-1\}$ satisfying $i \perp n$. In other words, $j \in \{i \in \{1,2,\ldots,n-1\} \mid i \perp n\}$.

Now, forget that we fixed j. We thus have proven that $j \in \{i \in \{1,2,\ldots,n-1\} \mid i \perp n\}$ for each $j \in \{i \in \{1,2,\ldots,n\} \mid i \perp n\}$. In other words,

$$\{i \in \{1,2,\ldots,n\} \mid i \perp n\} \subseteq \{i \in \{1,2,\ldots,n-1\} \mid i \perp n\}.$$

Combining this with

$$\left\{i \in \underbrace{\{1,2,\ldots,n-1\}}_{\subseteq\{1,2,\ldots,n\}} \mid i \perp n\right\} \subseteq \{i \in \{1,2,\ldots,n\} \mid i \perp n\},$$

we obtain $\{i \in \{1,2,\ldots,n\} \mid i \perp n\} = \{i \in \{1,2,\ldots,n-1\} \mid i \perp n\}$. This proves (417).

only if $k \perp n$). Now,

$$\begin{aligned}
2 \cdot \sum_{\substack{i \in \{1,2,\ldots,n\};\\ i \perp n}} i &= 2 \cdot \underbrace{\sum_{\substack{k \in \{1,2,\ldots,n\};\\ k \perp n}}}_{\substack{= \sum_{k \in \{i \in \{1,2,\ldots,n\} \ \mid \ i \perp n\}} \\ = \sum_{k \in \{i \in \{1,2,\ldots,n-1\} \ \mid \ i \perp n\}} \\ \text{(by (417))}}} k \qquad \left(\begin{array}{c}\text{here, we have renamed the}\\ \text{summation index } i \text{ as } k\end{array}\right) \\
&= 2 \cdot \underbrace{\sum_{k \in \{i \in \{1,2,\ldots,n-1\} \ \mid \ i \perp n\}}}_{= \sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ k \perp n}}} k = 2 \cdot \sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ k \perp n}} k \\
&= \sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ k \perp n}} k + \sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ k \perp n}} k \\
&= \sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ k \perp n}} k + \underbrace{\sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ n-k \perp n}}}_{\substack{= \sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ k \perp n}} \\ \text{(by the equivalence (419))}}} (n-k) \\
&\qquad \text{(here, we have substituted } n-k \text{ for } k \text{ in the second sum)} \\
&= \sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ k \perp n}} k + \sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ k \perp n}} (n-k) = \sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ k \perp n}} \underbrace{(k + (n-k))}_{=n} \\
&= \sum_{\substack{k \in \{1,2,\ldots,n-1\};\\ k \perp n}} n = \sum_{\substack{i \in \{1,2,\ldots,n-1\};\\ i \perp n}} n \qquad \left(\begin{array}{c}\text{here, we have renamed the}\\ \text{summation index } k \text{ as } i\end{array}\right) \\
&= \underbrace{\left|\{i \in \{1,2,\ldots,n-1\} \ \mid \ i \perp n\}\right|}_{\substack{= \phi(n) \\ \text{(by (418))}}} \cdot n = \phi(n) \cdot n = n\phi(n) .
\end{aligned}$$

Dividing this equality by 2, we obtain

$$\sum_{\substack{i \in \{1,2,\ldots,n\};\\ i \perp n}} i = n\phi(n)/2.$$

This solves Exercise 2.14.5.

[*Remark:* Alternatively, instead of doubling the sum we wanted to compute, we could have paired its addends up with each other: every i gets paired with the respective $n-i$. But this is slightly messy, since $\dfrac{n}{2}$ can happen to be a term of the sum (this happens when $n = 2$), which necessitates a separate argument.] □

10.69. Solution to Exercise 2.15.2

Solution to Exercise 2.15.2. From $u \equiv v \mod p-1$, we obtain $v \equiv u \mod p-1$. Likewise, the congruence $a^u \equiv a^v \mod p$, which we need to prove, is clearly equivalent to $a^v \equiv a^u \mod p$.

Hence, the numbers u and v play symmetric roles in Exercise 2.15.2. Thus, we can WLOG assume that $u \leq v$ (since otherwise, we can simply swap u with v). Assume this.

We have $v \equiv u \mod p-1$. In other words, $p-1 \mid v-u$. Thus, there exists an integer c such that $v-u = (p-1)c$. Consider this c. Thus, $(p-1)c = v - \underbrace{u}_{\leq v} \geq v-v = 0$. But $p > 1$ (since p is a prime), thus $p-1 > 0$. Hence, we can divide the inequality $(p-1)c \geq 0$ by $p-1$, and obtain $c \geq 0$. Hence, $c \in \mathbb{N}$.

Now, Theorem 2.15.1 **(a)** yields $a^{p-1} \equiv 1 \mod p$. We can take this congruence to the c-th power (since $c \in \mathbb{N}$), and obtain $\left(a^{p-1}\right)^c \equiv 1^c = 1 \mod p$. But $\left(a^{p-1}\right)^c = a^{(p-1)c} = a^{v-u}$ (since $(p-1)c = v-u$). Hence, $a^{v-u} = \left(a^{p-1}\right)^c \equiv 1 \mod p$. Multiplying this congruence by the obvious congruence $a^u \equiv a^u \mod p$, we obtain $a^{v-u}a^u \equiv 1a^u = a^u \mod p$. Hence, $a^u \equiv a^{v-u}a^u = a^{(v-u)+u} = a^v \mod p$. This solves Exercise 2.15.2. □

10.70. Solution to Exercise 2.15.4

Solution to Exercise 2.15.4. Theorem 2.15.7 yields

$$(p-1)! \equiv -1 \equiv p-1 \mod p$$

(since $p-1 \equiv -1 \mod p$). In other words, $p \mid (p-1)! - (p-1)$.

On the other hand, $p > 1$ (since p is a prime). Now, the definition of $(p-1)!$ yields

$$(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1) = (1 \cdot 2 \cdot \cdots \cdot (p-2)) \cdot (p-1).$$

Subtracting $p-1$ from both sides of this equality, we obtain

$$\begin{aligned}(p-1)! - (p-1) &= (1 \cdot 2 \cdot \cdots \cdot (p-2)) \cdot (p-1) - (p-1) \\ &= (1 \cdot 2 \cdot \cdots \cdot (p-2) - 1) \cdot (p-1) \\ &= (p-1) \cdot (1 \cdot 2 \cdot \cdots \cdot (p-2) - 1).\end{aligned}$$

Hence, $p-1 \mid (p-1)! - (p-1)$ (since $1 \cdot 2 \cdot \cdots \cdot (p-2) - 1$ is an integer).

Now, it is easy to see that $p-1 \perp p$ [274]. Furthermore, recall that $p-1 \mid (p-1)! - (p-1)$ and $p \mid (p-1)! - (p-1)$. Hence, Theorem 2.10.7 (applied to $a = p-1$, $b = p$ and $c = (p-1)! - (p-1)$) yields

$$(p-1)p \mid (p-1)! - (p-1). \tag{420}$$

[274] *Proof.* Proposition 2.9.7 **(c)** (applied to $a = p-1$, $b = 1$ and $u = 1$) yields $\gcd(p-1, 1(p-1)+1) = \gcd(p-1, 1)$. But Proposition 2.9.7 **(f)** (applied to $a = p-1$ and $b = 1$) yields $\gcd(p-1,1) \mid p-1$ and $\gcd(p-1,1) \mid 1$. Since $\gcd(p-1,1)$ is a nonnegative integer satisfying $\gcd(p-1,1) \mid 1$, we obtain $\gcd(p-1,1) = 1$ (by Exercise 2.2.5, applied to $g = \gcd(p-1,1)$). Hence,

$$\gcd\left(p-1, \underbrace{p}_{=1(p-1)+1}\right) = \gcd(p-1, 1(p-1)+1) = \gcd(p-1,1) = 1.$$

In other words, $p-1 \perp p$.

But Proposition 2.10.12 (applied to $n = p-1$) yields

$$1+2+\cdots+(p-1) = \frac{(p-1)((p-1)+1)}{2} = \frac{(p-1)p}{2}.$$

Hence, $(p-1)p = (1+2+\cdots+(p-1)) \cdot 2$, so that

$$1+2+\cdots+(p-1) \mid (p-1)p \mid (p-1)! - (p-1)$$

(by (420)). In other words, $(p-1)! \equiv p-1 \mod 1+2+\cdots+(p-1)$. This solves Exercise 2.15.4. □

10.71. Solution to Exercise 2.15.5

Solution to Exercise 2.15.5. From $p = 2k+1$, we obtain $p-1 = 2k$. But Theorem 2.15.7 yields $(p-1)! \equiv -1 \mod p$. In view of $p-1 = 2k$, this rewrites as $(2k)! \equiv -1 \mod p$.

But the definition of $(2k)!$ yields

$$(2k)! = 1 \cdot 2 \cdot \cdots \cdot (2k) = \prod_{j=1}^{2k} j = \left(\prod_{j=1}^{k} j\right) \cdot \left(\prod_{j=k+1}^{2k} j\right) \tag{421}$$

(here, we have split the product at $j = k$, because $0 \leq k \leq 2k$). But $\prod_{j=1}^{k} j = 1 \cdot 2 \cdot \cdots \cdot k = k!$ (by the definition of $k!$). Furthermore

$$\begin{aligned}\prod_{j=k+1}^{2k} j &= \prod_{j=p-2k}^{p-(k+1)} (p-j) && \left(\begin{array}{c}\text{here, we have substituted } p-j \\ \text{for } j \text{ in the product}\end{array}\right) \\ &= \prod_{j=1}^{k} \underbrace{(p-j)}_{\equiv -j \mod p} && \left(\begin{array}{c}\text{since } \underbrace{p}_{=2k+1} -2k = (2k+1)-2k = 1 \\ \text{and } \underbrace{p}_{=2k+1} - (k+1) = (2k+1)-(k+1) = k\end{array}\right) \\ &\equiv \prod_{j=1}^{k} (-j) \mod p.\end{aligned}$$

(Here, the last congruence sign is a consequence of (9)[275].) Thus,

$$\prod_{j=k+1}^{2k} j \equiv \prod_{j=1}^{k} (-j) = (-1)^k \underbrace{\prod_{j=1}^{k} j}_{=k!} = (-1)^k \cdot k! \mod p.$$

[275] In more detail: We have $p-s \equiv -s \mod p$ for each $s \in \{1,2,\ldots,k\}$. Hence, (9) (applied to $n = p$, $S = \{1,2,\ldots,k\}$, $a_s = p-s$ and $b_s = -s$) yields $\prod_{s\in\{1,2,\ldots,k\}} (p-s) \equiv \prod_{s\in\{1,2,\ldots,k\}} (-s) \mod p$. If we rename the index s (of the product sign "$\prod_{s\in\{1,2,\ldots,k\}}$") as j on both sides of this congruence, then we obtain $\prod_{j\in\{1,2,\ldots,k\}} (p-j) \equiv \prod_{j\in\{1,2,\ldots,k\}} (-j) \mod p$. This rewrites as $\prod_{j=1}^{k} (p-j) \equiv \prod_{j=1}^{k} (-j) \mod p$ (since the product sign $\prod_{j\in\{1,2,\ldots,k\}}$ is equivalent to the product sign $\prod_{j=1}^{k}$).

Hence, (421) becomes

$$(2k)! = \underbrace{\left(\prod_{j=1}^{k} j\right)}_{=k!} \cdot \underbrace{\left(\prod_{j=k+1}^{2k} j\right)}_{\equiv (-1)^k \cdot k! \bmod p} \equiv k! \cdot (-1)^k \cdot k! = k!^2 \cdot (-1)^k \bmod p.$$

Therefore,

$$k!^2 \cdot (-1)^k \equiv (2k)! \equiv -1 \bmod p.$$

Multiplying this congruence by the obvious congruence $(-1)^k \equiv (-1)^k \bmod p$, we find

$$k!^2 \cdot (-1)^k \cdot (-1)^k \equiv (-1) \cdot (-1)^k = -(-1)^k \bmod p.$$

In view of

$$k!^2 \cdot \underbrace{(-1)^k \cdot (-1)^k}_{\substack{=(-1)^{k+k}=1 \\ \text{(since } k+k=2k \text{ is even)}}} = k!^2,$$

this rewrites as $k!^2 \equiv -(-1)^k \bmod p$. This solves Exercise 2.15.5. □

10.72. Solution to Exercise 2.16.1

Solution to Exercise 2.16.1. We assumed that the integers $n_1, n_2, \ldots, n_k$ are mutually coprime. In other words, we have

$$n_i \perp n_j \text{ for all } i, j \in \{1, 2, \ldots, k\} \text{ satisfying } i \neq j. \tag{422}$$

We claim that

$$\phi(n_1 n_2 \cdots n_i) = \phi(n_1) \cdot \phi(n_2) \cdot \cdots \cdot \phi(n_i) \tag{423}$$

for each $i \in \{0, 1, \ldots, k\}$.

[*Proof of (423):* We shall prove (423) by induction on i:

Induction base: It is easy to see that $\phi(1) = 1$ [276]. But applying the map ϕ to the equality $n_1 n_2 \cdots n_0 = (\text{empty product}) = 1$, we obtain

$$\phi(n_1 n_2 \cdots n_0) = \phi(1) = 1.$$

[276] *Proof.* We have $1 \mid 1$. Hence, Proposition 2.9.7 **(i)** (applied to 1 and 1 instead of a and b) yields $\gcd(1,1) = |1| = 1$. Hence, $1 \perp 1$. Thus, 1 is an $i \in \{1, 2, \ldots, 1\}$ satisfying $i \perp 1$. In other words, 1 is an element of the set $\{i \in \{1, 2, \ldots, 1\} \mid i \perp 1\}$. Since 1 is the **only** element of this set (because every element of $\{i \in \{1, 2, \ldots, 1\} \mid i \perp 1\}$ must belong to the set $\{1, 2, \ldots, 1\} = \{1\}$ and thus must equal to 1), we can thus conclude that $\{i \in \{1, 2, \ldots, 1\} \mid i \perp 1\} = \{1\}$.

But the equality (55) (applied to $n = 1$) yields

$$\phi(1) = \left| \underbrace{\{i \in \{1, 2, \ldots, 1\} \mid i \perp 1\}}_{=\{1\}} \right| = |\{1\}| = 1.$$

Comparing this with $\phi(n_1) \cdot \phi(n_2) \cdot \cdots \cdot \phi(n_0) = (\text{empty product}) = 0$, we obtain $\phi(n_1 n_2 \cdots n_0) = \phi(n_1) \cdot \phi(n_2) \cdot \cdots \cdot \phi(n_0)$. In other words, (423) holds for $i = 0$. This completes the induction base.

Induction step: Let $j \in \{0, 1, \ldots, k\}$ be positive. Assume that (423) holds for $i = j - 1$. We must prove that (423) holds for $i = j$.

For each $i \in \{1, 2, \ldots, j-1\}$, we have $i \leq j - 1 < j$ and thus $i \neq j$ and therefore $n_i \perp n_j$ (by (422)). Hence, Exercise 2.10.2 (applied to $j-1$, n_j and $(n_1, n_2, \ldots, n_{j-1})$ instead of k, c and $(a_1, a_2, \ldots, a_k)$) yields $n_1 n_2 \cdots n_{j-1} \perp n_j$. In other words, the two positive integers $n_1 n_2 \cdots n_{j-1}$ and n_j are coprime. Therefore, Theorem 2.14.4 yields

$$\phi\left(\left(n_1 n_2 \cdots n_{j-1}\right) n_j\right) = \phi\left(n_1 n_2 \cdots n_{j-1}\right) \cdot \phi\left(n_j\right).$$

But we have assumed that (423) holds for $i = j - 1$. In other words, we have

$$\phi\left(n_1 n_2 \cdots n_{j-1}\right) = \phi(n_1) \cdot \phi(n_2) \cdot \cdots \cdot \phi\left(n_{j-1}\right). \tag{424}$$

Now,

$$\begin{aligned}
\phi\left(\underbrace{n_1 n_2 \cdots n_j}_{=\left(n_1 n_2 \cdots n_{j-1}\right) n_j}\right) &= \phi\left(\left(n_1 n_2 \cdots n_{j-1}\right) n_j\right) = \underbrace{\phi\left(n_1 n_2 \cdots n_{j-1}\right)}_{=\phi(n_1)\cdot\phi(n_2)\cdot\cdots\cdot\phi\left(n_{j-1}\right)} \cdot \phi\left(n_j\right) \\
&= \left(\phi(n_1) \cdot \phi(n_2) \cdot \cdots \cdot \phi\left(n_{j-1}\right)\right) \cdot \phi\left(n_j\right) \\
&= \phi(n_1) \cdot \phi(n_2) \cdot \cdots \cdot \phi\left(n_j\right).
\end{aligned}$$

In other words, (423) holds for $i = j$. This completes the induction step. Hence, the induction proof of (423) is complete.]

Now, (423) (applied to $i = k$) yields $\phi(n_1 n_2 \cdots n_k) = \phi(n_1) \cdot \phi(n_2) \cdot \cdots \cdot \phi(n_k)$. This solves Exercise 2.16.1. □

10.73. Solution to Exercise 2.16.2

Solution to Exercise 2.16.2. Exercise 2.16.1 and Exercise 2.16.2 say the same thing: They say that applying the function ϕ to a product of finitely many mutually coprime positive integers yields the same result as applying ϕ to each of these integers separately and then taking the product. The difference between these two exercises is merely how the product is indexed. Thus, deriving Exercise 2.16.2 from Exercise 2.16.1 is merely a matter of bookkeeping (and this is pretty much the same sort of bookkeeping that we used to derive Exercise 2.10.5 from Exercise 2.10.2 above). Let us do this bookkeeping:

The set I is finite; thus, we can define some $k \in \mathbb{N}$ by $k = |I|$. Consider this k. There exists a bijection $f : \{1, 2, \ldots, k\} \to I$ (since $k = |I|$). Pick such an f. Thus, $f(1), f(2), \ldots, f(k)$ are the k elements of I; hence, $n_{f(1)}, n_{f(2)}, \ldots, n_{f(k)}$ are k positive integers. Moreover, these k integers $n_{f(1)}, n_{f(2)}, \ldots, n_{f(k)}$ are mutually coprime[277]. Hence, Exercise 2.16.1 (applied to $n_{f(i)}$ instead of n_i) yields $\phi\left(n_{f(1)} n_{f(2)} \cdots n_{f(k)}\right) = \phi\left(n_{f(1)}\right) \cdot \phi\left(n_{f(2)}\right) \cdot \cdots \cdot \phi\left(n_{f(k)}\right)$.

[277] *Proof.* Let x and y be two distinct elements of $\{1, 2, \ldots, k\}$. We claim that $n_{f(x)} \perp n_{f(y)}$.

Indeed, the map f is a bijection, and thus is injective. But x and y are distinct; thus, $x \neq y$. Therefore, $f(x) \neq f(y)$ (since f is injective). Hence, $f(x)$ and $f(y)$ are two distinct elements of

The map $f : \{1, 2, \ldots, k\} \to I$ is a bijection. Hence, we can substitute $f(j)$ for i in the product $\prod\limits_{i \in I} n_i$. We thus find

$$\prod_{i \in I} n_i = \prod_{j \in \{1,2,\ldots,k\}} n_{f(j)} = \prod_{j=1}^{k} n_{f(j)} = n_{f(1)} n_{f(2)} \cdots n_{f(k)}.$$

Applying the map ϕ to both sides of this equality, we obtain

$$\begin{aligned}\phi\left(\prod_{i \in I} n_i\right) &= \phi\left(n_{f(1)} n_{f(2)} \cdots n_{f(k)}\right) = \phi\left(n_{f(1)}\right) \cdot \phi\left(n_{f(2)}\right) \cdot \cdots \cdot \phi\left(n_{f(k)}\right) \\ &= \prod_{j=1}^{k} \phi\left(n_{f(j)}\right) = \prod_{j \in \{1,2,\ldots,k\}} \phi\left(n_{f(j)}\right) = \prod_{i \in I} \phi(n_i)\end{aligned}$$

(here, we have substituted i for $f(j)$ in the product, since the map $f : \{1, 2, \ldots, k\} \to I$ is a bijection). This solves Exercise 2.16.2. □

10.74. Solution to Exercise 2.16.3

Solution to Exercise 2.16.3. The integer n is positive and thus nonzero. Hence, $v_p(n) \in \mathbb{N}$ for each prime p.

We shall next prove that

$$a^n \equiv a^{n-\phi(n)} \mod p^{v_p(n)} \qquad \text{for every prime } p. \tag{425}$$

Once this congruence is proven, the claim of Exercise 2.16.3 will easily follow using Exercise 2.13.9.

[*Proof of (425):* Let p be a prime. Then, $p > 1$. Hence, $p \neq 1$, and the integer p is positive. Also, Lemma 2.13.27 **(a)** shows that there exists a nonzero integer u such that $u \perp p$ and $n = up^{v_p(n)}$. Consider this u.

We have $v_p(n) \in \mathbb{N}$ (since n is nonzero). Thus, we can define $r \in \mathbb{N}$ by $r = v_p(n)$. Consider this r. Note that p^r is nonzero (since p is positive and thus nonzero).

We have $n = up^{v_p(n)} = up^r$ (since $v_p(n) = r$). Solving this equation for u, we obtain $u = n/p^r$ (since p^r is nonzero). Thus, u is positive (since both n and p are positive).

Now, we claim that

$$up^i - \phi\left(up^i\right) \geq i \qquad \text{for each } i \in \mathbb{N}. \tag{426}$$

Let us give three proofs of this inequality:

- [*First proof of (426):* We shall prove (426) by induction on i:

I. Thus, (76) (applied to $i = f(x)$ and $j = f(y)$) yields $n_{f(x)} \perp n_{f(y)}$.

Now, forget that we fixed x and y. We thus have proven that every two distinct elements x and y of $\{1, 2, \ldots, k\}$ satisfy $n_{f(x)} \perp n_{f(y)}$. In other words, the k integers $n_{f(1)}, n_{f(2)}, \ldots, n_{f(k)}$ are mutually coprime.

Induction base: Exercise 2.14.2 **(b)** (applied to u instead of n) yields $u - \phi(u) \geq 0$. Now, $u \underbrace{p^0}_{=1} - \phi\left(u \underbrace{p^0}_{=1}\right) = u - \phi(u) \geq 0$. In other words, (426) holds for $i = 0$. This completes the induction base.

Induction step: Let j be a positive integer. Assume that (426) holds for $i = j-1$. We must prove that (426) holds for $i = j$.

We have assumed that (426) holds for $i = j-1$. In other words, we have $up^{j-1} - \phi\left(up^{j-1}\right) \geq j-1$.

We have $j - 1 \in \mathbb{N}$ (since j is a positive integer); hence, p^{j-1} is an integer. Thus, up^{j-1} is an integer. Clearly, $up^{j-1} \mid up^j$ (since $up^j = up^{j-1}p$); thus, up^{j-1} is a divisor of up^j. Also, up^{j-1} is positive[278] and satisfies $up^{j-1} \neq up^j$ (since $\dfrac{up^j}{up^{j-1}} = p \neq 1$). Hence, Exercise 2.14.2 **(d)** (applied to up^{j-1} and up^j instead of d and n) yields $up^{j-1} - \phi\left(up^{j-1}\right) < up^j - \phi\left(up^j\right)$. Hence,

$$up^j - \phi\left(up^j\right) > up^{j-1} - \phi\left(up^{j-1}\right) \geq j-1.$$

Since $up^j - \phi\left(up^j\right)$ and $j-1$ are integers, this leads to

$$up^j - \phi\left(up^j\right) \geq (j-1) + 1 = j.$$

In other words, (426) holds for $i = j$. This completes the induction step. Hence, (426) is proven by induction.]

- [*Second proof of (426) (sketched):* Let $j \in \mathbb{N}$. We shall show that $up^j - \phi\left(up^j\right) \geq j$.

  Recall that u is a positive integer. Hence, $u \geq 1$ and thus $\underbrace{u}_{\geq 1} p^j \geq p^j$ (since p^j is a positive integer); in other words, $p^j \leq up^j$. Also, from $p > 1$, we obtain $p^1 < p^2 < \cdots < p^j$. Hence, the j integers $p^1, p^2, \ldots, p^j$ are distinct.

  On the other hand, it is easy to see that

  $$\left\{p^1, p^2, \ldots, p^j\right\} \subseteq \left\{i \in \left\{1, 2, \ldots, up^j\right\} \mid \text{we don't have } i \perp up^j\right\}$$

  [279]. Hence,

  $$\left|\left\{p^1, p^2, \ldots, p^j\right\}\right| \leq \left|\left\{i \in \left\{1, 2, \ldots, up^j\right\} \mid \text{we don't have } i \perp up^j\right\}\right|. \tag{427}$$

[278] since u and p are positive

[279] *Proof.* Let $s \in \{1, 2, \ldots, j\}$. Thus, $s \geq 1$ and $s \leq j$. From $s \geq 1$, we conclude that p^s is a positive integer. Moreover, from $s \geq 1$, we obtain $p^s \geq p^1$ (since $p > 1$), thus $p^s \geq p^1 = p > 1$. From $s \leq j$, we obtain $p^s \leq p^j$ (since $p > 1$) and thus $p^s \leq p^j \leq up^j$. Thus, $p^s \in \left\{1, 2, \ldots, up^j\right\}$ (since p^s is a positive integer). Furthermore, from $s \leq j$, we obtain $p^s \mid p^j$ (by Exercise 2.2.4, applied to p, s and j instead of n, a and b). Thus, $p^s \mid p^j \mid up^j$ (since u is an integer). Hence, Proposition 2.9.7 **(i)** (applied to p^s and up^j instead of a and b) yields $\gcd\left(p^s, up^j\right) = |p^s| = p^s$ (since p^s is positive). But $p > 1$, so that $p^s > 1$ and thus $p^s \neq 1$. Hence, $\gcd\left(p^s, up^j\right) = p^s \neq 1$. In other words, we don't have $p^s \perp up^j$.

So we have shown that p^s is an element of $\left\{1, 2, \ldots, up^j\right\}$ (since $p^s \in \left\{1, 2, \ldots, up^j\right\}$) with the

But Exercise 2.14.2 **(a)** (applied to up^j instead of n) yields

$$\begin{aligned} up^j - \phi\left(up^j\right) &= \left|\left\{i \in \left\{1, 2, \ldots, up^j\right\} \mid \text{we don't have } i \perp up^j\right\}\right| \\ &\geq \left|\left\{p^1, p^2, \ldots, p^j\right\}\right| \qquad \text{(by (427))} \\ &= j \qquad \left(\text{since the } j \text{ integers } p^1, p^2, \ldots, p^j \text{ are distinct}\right). \end{aligned}$$

Now, forget that we fixed j. We thus have proven that $up^j - \phi\left(up^j\right) \geq j$ for each $j \in \mathbb{N}$. Renaming j as i in this statement, we conclude that $up^i - \phi\left(up^i\right) \geq i$ for each $i \in \mathbb{N}$. Thus, (426) is proven.]

- [*Third proof of (426):* The following proof is a typical estimation argument (the kind you see in analysis).

  Fix $i \in \mathbb{N}$. We must prove that $up^i - \phi\left(up^i\right) \geq i$. This is obvious in the case when $i = 0$ (because Exercise 2.14.2 **(b)** (applied to up^0 instead of n) yields $up^0 - \phi\left(up^0\right) \geq 0$). Hence, for the rest of this proof, we WLOG assume that $i \neq 0$. Hence, i is a positive integer (since $i \in \mathbb{N}$). Therefore, Exercise 2.14.1 (applied to $k = i$) yields $\phi\left(p^i\right) = (p-1)\,p^{i-1}$. Hence,

  $$\underbrace{p^i}_{=pp^{i-1}} - \underbrace{\phi\left(p^i\right)}_{=(p-1)p^{i-1}} = pp^{i-1} - (p-1)\,p^{i-1} = p^{i-1}. \tag{428}$$

  Also, $i - 1 \in \mathbb{N}$ (since i is a positive integer). Hence, Exercise 2.13.4 (applied to $k = i - 1$) yields $p^{i-1} > i - 1$. Since p^{i-1} and $i - 1$ are integers (because $i - 1 \in \mathbb{N}$), this leads to $p^{i-1} \geq (i-1) + 1 = i$.

  Note that u is a positive integer. Thus, $u \geq 1$. Exercise 2.14.2 **(b)** (applied to u instead of n) yields $u - \phi(u) \geq 0$. In other words, $\phi(u) \leq u$. Furthermore, p^i is a positive integer; thus, $\phi\left(p^i\right) \geq 0$ (because clearly, $\phi(m) \geq 0$ for every positive integer m).

  But $u \perp p$. Hence, Exercise 2.10.4 (applied to u, p, 1 and i instead of a, b, n and m) yields $u^1 \perp p^i$ (since $i \in \mathbb{N}$). In other words, $u \perp p^i$ (since $u^1 = u$). In other words,

property that we don't have $p^s \perp up^j$. In other words, p^s is an $i \in \left\{1, 2, \ldots, up^j\right\}$ such that we don't have $i \perp up^j$. In other words,

$$p^s \in \left\{i \in \left\{1, 2, \ldots, up^j\right\} \mid \text{we don't have } i \perp up^j\right\}.$$

Now, forget that we fixed s. We thus have proven that

$$p^s \in \left\{i \in \left\{1, 2, \ldots, up^j\right\} \mid \text{we don't have } i \perp up^j\right\}$$

for each $s \in \{1, 2, \ldots, j\}$. In other words,

$$\left\{p^1, p^2, \ldots, p^j\right\} \subseteq \left\{i \in \left\{1, 2, \ldots, up^j\right\} \mid \text{we don't have } i \perp up^j\right\},$$

qed.

the integers u and p^i are coprime. Thus, Theorem 2.14.4 (applied to u and p^i instead of m and n) yields $\phi\left(up^i\right) = \phi\left(u\right) \cdot \phi\left(p^i\right)$ (since u and p^i are positive integers). Thus,

$$\phi\left(up^i\right) = \underbrace{\phi\left(u\right)}_{\leq u} \cdot \phi\left(p^i\right) \leq u \cdot \phi\left(p^i\right) \qquad \left(\text{since } \phi\left(p^i\right) \geq 0\right).$$

Hence,

$$\begin{aligned} up^i - \underbrace{\phi\left(up^i\right)}_{\leq u\cdot\phi\left(p^i\right)} &\geq up^i - u \cdot \phi\left(p^i\right) = u \cdot \underbrace{\left(p^i - \phi\left(p^i\right)\right)}_{\substack{=p^{i-1} \\ \text{(by (428))}}} = \underbrace{u}_{\geq 1} p^{i-1} \\ &\geq 1p^{i-1} \qquad \left(\text{since } p^{i-1} \geq 0\right) \\ &= p^{i-1} \geq i. \end{aligned}$$

Thus, (426) is proven again.]

Now, we can apply (426) to $i = r$ (since $r \in \mathbb{N}$). We thus obtain $up^r - \phi\left(up^r\right) \geq r$. Hence,

$$\underbrace{n}_{=up^r} - \phi\left(\underbrace{n}_{=up^r}\right) = up^r - \phi\left(up^r\right) \geq r. \qquad (429)$$

Now, we are in one of the following two cases:

Case 1: We have $p \mid a$.

Case 2: We don't have $p \mid a$.

Let us first consider Case 1. In this case, $p \mid a$. Now, (429) yields $n - \phi\left(n\right) \geq r \geq 0$ (since $r \in \mathbb{N}$). Hence, $n - \phi\left(n\right) \in \mathbb{N}$ and $r \in \mathbb{N}$. From $n - \phi\left(n\right) \geq r$, we also obtain $r \leq n - \phi\left(n\right)$. Hence, Exercise 2.2.4 (applied to p, r and $n - \phi\left(n\right)$ instead of n, a and b) yields $p^r \mid p^{n-\phi(n)}$. But $p \mid a$. Hence, Exercise 2.2.6 (applied to p, a and $n - \phi\left(n\right)$ instead of a, b and k) yields $p^{n-\phi(n)} \mid a^{n-\phi(n)}$ (since $n - \phi\left(n\right) \in \mathbb{N}$). Hence, $p^r \mid p^{n-\phi(n)} \mid a^{n-\phi(n)}$; in other words, $a^{n-\phi(n)} \equiv 0 \mod p^r$. Now,

$$\begin{aligned} a^n = a^{\phi(n)+(n-\phi(n))} &= a^{\phi(n)} \underbrace{a^{n-\phi(n)}}_{\equiv 0 \mod p^r} \qquad (\text{since } n - \phi\left(n\right) \in \mathbb{N}) \\ &\equiv 0 \equiv a^{n-\phi(n)} \mod p^r \qquad \left(\text{since } a^{n-\phi(n)} \equiv 0 \mod p^r\right). \end{aligned}$$

This rewrites as $a^n \equiv a^{n-\phi(n)} \mod p^{v_p(n)}$ (since $r = v_p\left(n\right)$). Hence, (425) is proven in Case 1.

Let us now consider Case 2. In this case, we don't have $p \mid a$. But Proposition 2.13.5 yields that either $p \mid a$ or $p \perp a$. Hence, $p \perp a$ (since we don't have $p \mid a$). Due to Proposition 2.10.4, this leads to $a \perp p$. Thus, Exercise 2.10.4 (applied to p, 1 and r instead of b, n and m) yields $a^1 \perp p^r$ (since $r \in \mathbb{N}$). In other words, $a \perp p^r$ (since $a^1 = a$). In other words, a is coprime to p^r. Hence, Theorem 2.15.3 (applied to p^r instead of n) yields $a^{\phi(p^r)} \equiv 1 \mod p^r$.

But $u \perp p$. Hence, Exercise 2.10.4 (applied to u, p, 1 and r instead of a, b, n and m) yields $u^1 \perp p^r$ (since $r \in \mathbb{N}$). In other words, $u \perp p^r$ (since $u^1 = u$). In other words, the integers u and p^r are coprime. Thus, Theorem 2.14.4 (applied to u and p^r instead of m and n) yield

$\phi(up^r) = \phi(u) \cdot \phi(p^r)$ (since u and p^r are positive integers). Now, applying the map ϕ to both sides of the equality $n = up^r$, we obtain $\phi(n) = \phi(up^r) = \phi(u) \cdot \phi(p^r) = \phi(p^r) \cdot \phi(u)$. Hence,

$$a^{\phi(n)} = a^{\phi(p^r)\cdot\phi(u)} = \left(\underbrace{a^{\phi(p^r)}}_{\equiv 1 \bmod p^r} \right)^{\phi(u)} \equiv 1^{\phi(u)} = 1 \bmod p^r.$$

Hence,

$$\begin{aligned} a^n = a^{\phi(n)+(n-\phi(n))} &= \underbrace{a^{\phi(n)}}_{\equiv 1 \bmod p^r} a^{n-\phi(n)} \qquad \text{(since } n - \phi(n) \in \mathbb{N}\text{)} \\ &\equiv a^{n-\phi(n)} \bmod p^r. \end{aligned}$$

This rewrites as $a^n \equiv a^{n-\phi(n)} \bmod p^{v_p(n)}$ (since $r = v_p(n)$). Therefore, (425) is proven in Case 2.

We have thus shown (425) in both Cases 1 and 2. These cases cover all possibilities, and so (425) is always proven.]

Hence, Exercise 2.13.9 (applied to a^n and $a^{n-\phi(n)}$ instead of a and b) yields $a^n \equiv a^{n-\phi(n)} \bmod n$. This solves Exercise 2.16.3. □

10.75. Solution to Exercise 2.17.1

Solution to Exercise 2.17.1. A product of k consecutive integers always has the form $(a+1)(a+2)\cdots(a+k)$ for some $a \in \mathbb{Z}$. Thus, we must prove that $(a+1)(a+2)\cdots(a+k)$ is divisible by $k!$ for each $a \in \mathbb{Z}$.

Let $a \in \mathbb{Z}$. We must prove that $(a+1)(a+2)\cdots(a+k)$ is divisible by $k!$.

Proposition 2.17.12 (applied to $n = a + k$) yields that $\dbinom{a+k}{k}$ is an integer. Now, the definition of $\dbinom{a+k}{k}$ yields

$$\binom{a+k}{k} = \frac{(a+k)(a+k-1)(a+k-2)\cdots(a+k-k+1)}{k!}.$$

Multiplying both sides of this equality by $k!$, we find

$$\begin{aligned} k!\binom{a+k}{k} &= (a+k)(a+k-1)(a+k-2)\cdots(a+k-k+1) \\ &= (a+k)(a+k-1)(a+k-2)\cdots(a+1) \\ &= (a+1)(a+2)\cdots(a+k) \end{aligned}$$

(here, we have reversed the order of the factors in the product). Thus, $(a+1)(a+2)\cdots(a+k) = k!\dbinom{a+k}{k}$. Since $\dbinom{a+k}{k}$ is an integer, this equality yields that $(a+1)(a+2)\cdots(a+k)$ is divisible by $k!$. This solves Exercise 2.17.1. □

10.76. Solution to Exercise 2.17.2

Solution to Exercise 2.17.2. **(a)** Let $n \in \mathbb{N}$. Let k be a positive integer. Theorem 2.6.1 (applied to n and k instead of u and n) shows that there exists a unique pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,k-1\}$ such that $n = qk + r$. Consider this pair. Then, $n//k = q$ (by the definition of $n//k$). From $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,k-1\}$, we obtain $q \in \mathbb{Z}$ and $r \in \{0,1,\ldots,k-1\}$. From $r \in \{0,1,\ldots,k-1\}$, we obtain $r \geq 0$ and $r \leq k-1$. From $n = qk + r$, we obtain $qk = \underbrace{n}_{\geq 0} - r \geq - \underbrace{r}_{\leq k-1<k} > -k = (-1)\,k$. If we had $q \leq -1$, then we would have $\underbrace{q}_{\leq -1} k \leq (-1)\,k$ (since k is positive), which would contradict $qk > (-1)\,k$. Thus, we cannot have $q \leq -1$. Hence, $q > -1$. Therefore, $q \geq 0$ (since $q \in \mathbb{Z}$). Also, $n = qk + \underbrace{r}_{\geq 0} \geq qk$ and $n = qk + \underbrace{r}_{\leq k-1<k} < qk + k = (q+1)\,k$.

We have $1 < 2 < \cdots < q$. Since k is positive, we can multiply this chain of inequalities by k, and obtain $1k < 2k < \cdots < qk$. Thus, the q numbers $1k, 2k, \ldots, qk$ are distinct; therefore,

$$|\{1k, 2k, \ldots, qk\}| = q.$$

We now shall show the following:

Claim 1: We have

$$\{i \in \{1,2,\ldots,n\} \text{ satisfying } k \mid i\} = \{1k, 2k, \ldots, qk\}.$$

(We are writing the word "satisfying" out, since the "|" symbol is already being used for divisibility here.)

[*Proof of Claim 1:* Let $j \in \{i \in \{1,2,\ldots,n\} \text{ satisfying } k \mid i\}$. We shall show that $j \in \{1k, 2k, \ldots, qk\}$.

Indeed, we have $j \in \{i \in \{1,2,\ldots,n\} \text{ satisfying } k \mid i\}$. In other words, j is an element of $\{1,2,\ldots,n\}$ satisfying $k \mid j$. From $k \mid j$, we conclude that there exists an integer c such that $j = kc$. Consider this c. From $j \in \{1,2,\ldots,n\}$, we obtain $j \geq 1$ and $j \leq n$. Now, $ck = kc = j \leq n < (q+1)\,k$. We can divide this inequality by k (since k is positive) and thus obtain $c < q+1$. Hence, $c \leq q$ (since c and q are integers).

Also, $ck = kc = j \geq 1 > 0$. We can divide this inequality by k (since k is positive) and thus obtain $c > 0$. Hence, $c \geq 1$ (since c is an integer). Combining this with $c \leq q$, we obtain $c \in \{1,2,\ldots,q\}$ (since c is an integer) and thus $ck \in \{1k, 2k, \ldots, qk\}$. Hence, $j = kc = ck \in \{1k, 2k, \ldots, qk\}$.

Now, forget that we fixed j. We thus have proven that $j \in \{1k, 2k, \ldots, qk\}$ for each $j \in \{i \in \{1,2,\ldots,n\} \text{ satisfying } k \mid i\}$. In other words,

$$\{i \in \{1,2,\ldots,n\} \text{ satisfying } k \mid i\} \subseteq \{1k, 2k, \ldots, qk\}. \tag{430}$$

On the other hand, let $h \in \{1k, 2k, \ldots, qk\}$. We shall show that
$h \in \{i \in \{1,2,\ldots,n\} \text{ satisfying } k \mid i\}$.

Indeed, $h \in \{1k, 2k, \ldots, qk\}$. In other words, $h = dk$ for some $d \in \{1,2,\ldots,q\}$. Consider this d. From $d \in \{1,2,\ldots,q\}$, we obtain $d \geq 1$ and $d \leq q$. We can multiply the inequality

$d \geq 1$ by k (since k is positive) and thus obtain $dk \geq 1k = k \geq 1$ (since k is a positive integer). Also, we can multiply the inequality $d \leq q$ by k (since k is positive) and thus obtain $dk \leq qk \leq n$ (since $n \geq qk$). Combining this with $dk \geq 1$, we obtain $dk \in \{1, 2, \ldots, n\}$ (since dk is an integer). In other words, $h \in \{1, 2, \ldots, n\}$ (since $h = dk$). Moreover, $k \mid h$ (since $h = dk = kd$). Hence, h is an $i \in \{1, 2, \ldots, n\}$ satisfying $k \mid i$ (since $h \in \{1, 2, \ldots, n\}$ and $k \mid h$). In other words, $h \in \{i \in \{1, 2, \ldots, n\} \text{ satisfying } k \mid i\}$.

Now, forget that we fixed h. We thus have proven that $h \in \{i \in \{1, 2, \ldots, n\} \text{ satisfying } k \mid i\}$ for each $h \in \{1k, 2k, \ldots, qk\}$. In other words,

$$\{1k, 2k, \ldots, qk\} \subseteq \{i \in \{1, 2, \ldots, n\} \text{ satisfying } k \mid i\}.$$

Combining this with (430), we obtain $\{i \in \{1, 2, \ldots, n\} \text{ satisfying } k \mid i\} = \{1k, 2k, \ldots, qk\}$. This proves Claim 1.]

Now,

$$\begin{aligned}
\sum_{i=1}^{n} [k \mid i] &= \sum_{i \in \{1,2,\ldots,n\}} [k \mid i] = \sum_{\substack{i \in \{1,2,\ldots,n\};\\ k \mid i}} \underbrace{[k \mid i]}_{\substack{=1\\ (\text{since } k \mid i)}} + \sum_{\substack{i \in \{1,2,\ldots,n\};\\ \text{we don't have } k \mid i}} \underbrace{[k \mid i]}_{\substack{=0\\ (\text{since we don't have } k \mid i)}} \\
&\qquad (\text{since each } i \in \{1, 2, \ldots, n\} \text{ either satisfies } k \mid i \text{ or does not}) \\
&= \sum_{\substack{i \in \{1,2,\ldots,n\};\\ k \mid i}} 1 + \underbrace{\sum_{\substack{i \in \{1,2,\ldots,n\};\\ \text{we don't have } k \mid i}} 0}_{=0} = \sum_{\substack{i \in \{1,2,\ldots,n\};\\ k \mid i}} 1 \\
&= (\text{the number of all } i \in \{1, 2, \ldots, n\} \text{ satisfying } k \mid i) \cdot 1 \\
&= (\text{the number of all } i \in \{1, 2, \ldots, n\} \text{ satisfying } k \mid i) \\
&= |\{i \in \{1, 2, \ldots, n\} \text{ satisfying } k \mid i\}| \\
&= |\{1k, 2k, \ldots, qk\}| \qquad (\text{by Claim 1}) \\
&= q = n // k.
\end{aligned}$$

In other words, $n//k = \sum_{i=1}^{n} [k \mid i]$. This solves Exercise 2.17.2 **(a)**.

(b) Let p be a prime. Let n be a nonzero integer.

Then, $v_p(n)$ is the largest $m \in \mathbb{N}$ such that $p^m \mid n$ (by Definition 2.13.23 **(a)**). Hence, $v_p(n) \in \mathbb{N}$. Thus, $\{1, 2, \ldots, v_p(n)\}$ is a finite set and has size $|\{1, 2, \ldots, v_p(n)\}| = v_p(n)$. Every $i \in \{1, 2, \ldots, v_p(n)\}$ satisfies

$$\left[p^i \mid n\right] = 1 \tag{431}$$

[280]. Moreover, every positive integer i satisfying $i > v_p(n)$ satisfies

$$\left[p^i \mid n\right] = 0 \tag{432}$$

[280] *Proof.* Let $i \in \{1, 2, \ldots, v_p(n)\}$. Thus, i is a positive integer satisfying $i \leq v_p(n)$. Hence, $v_p(n) \geq i$. But Lemma 2.13.25 shows that $p^i \mid n$ if and only if $v_p(n) \geq i$. Thus, we have $p^i \mid n$ (since we have $v_p(n) \geq i$). Therefore, $\left[p^i \mid n\right] = 1$, qed.

[281]. Hence, all but finitely many positive integers i satisfy $\left[p^i \mid n\right] = 0$ (since all but finitely many positive integers i satisfy $i > v_p(n)$). In other words, all but finitely many addends of the sum $\sum\limits_{i\geq 1} \left[p^i \mid n\right]$ are zero. In other words, this sum has only finitely many nonzero addends. Hence, this sum is well-defined.

Now, we can split this sum at $i = v_p(n)$ (since $v_p(n) \geq 0$), and thus obtain

$$\sum_{i\geq 1} \left[p^i \mid n\right] = \sum_{i=1}^{v_p(n)} \underbrace{\left[p^i \mid n\right]}_{\substack{=1 \\ \text{(by (431))}}} + \sum_{i>v_p(n)} \underbrace{\left[p^i \mid n\right]}_{\substack{=0 \\ \text{(by (432))}}} = \sum_{i=1}^{v_p(n)} 1 + \underbrace{\sum_{i>v_p(n)} 0}_{=0} = \sum_{i=1}^{v_p(n)} 1 = v_p(n) \cdot 1 = v_p(n).$$

In other words, $v_p(n) = \sum\limits_{i\geq 1} \left[p^i \mid n\right]$. This solves Exercise 2.17.2 **(b)**.

(c) Let p be a prime. Let $n \in \mathbb{N}$. For every positive integer m, we have

$$\begin{aligned} v_p(m) &= \sum_{i\geq 1} \left[p^i \mid m\right] && \left(\begin{array}{c}\text{by Exercise 2.17.2 (b),} \\ \text{applied to } m \text{ instead of } n\end{array}\right) \\ &= \sum_{j\geq 1} \left[p^j \mid m\right] && (433) \end{aligned}$$

(here, we have renamed the summation index i as j). Note that the sum $\sum\limits_{j\geq 1} \left[p^j \mid m\right]$ on the right hand side of this equality is well-defined, i.e., has only finitely many nonzero addends.

Corollary 2.13.29 (applied to $k = n$ and $a_i = i$) yields

$$v_p(1 \cdot 2 \cdot \cdots \cdot n) = v_p(1) + v_p(2) + \cdots + v_p(n) = \sum_{m=1}^{n} v_p(m).$$

In view of $1 \cdot 2 \cdot \cdots \cdot n = n!$, this rewrites as

$$v_p(n!) = \sum_{m=1}^{n} \underbrace{v_p(m)}_{\substack{= \sum_{j\geq 1} \left[p^j \mid m\right] \\ \text{(by (433))}}} = \sum_{m=1}^{n} \sum_{j\geq 1} \left[p^j \mid m\right] = \sum_{j\geq 1} \sum_{m=1}^{n} \left[p^j \mid m\right]. \qquad (434)$$

(Here, we have interchanged the two summation signs "$\sum\limits_{m=1}^{n}$" and "$\sum\limits_{j\geq 1}$". This is legitimate, since the first summation is finite whereas the second summation has already been proven to be well-defined.) But each positive integer j satisfies

$$\begin{aligned} n//p^j &= \sum_{i=1}^{n} \left[p^j \mid i\right] && \left(\text{by Exercise 2.17.2 (a), applied to } k = p^j\right) \\ &= \sum_{m=1}^{n} \left[p^j \mid m\right] && (435) \end{aligned}$$

[281] *Proof.* Let i be a positive integer satisfying $i > v_p(n)$. We must prove that $\left[p^i \mid n\right] = 0$.

We have $i > v_p(n)$. Thus, we don't have $v_p(n) \geq i$. But Lemma 2.13.25 shows that $p^i \mid n$ if and only if $v_p(n) \geq i$. Hence, we don't have $p^i \mid n$ (since we don't have $v_p(n) \geq i$). Thus, $\left[p^i \mid n\right] = 0$. Qed.

(here, we have renamed the summation index i as m). Thus, (434) becomes

$$v_p(n!) = \sum_{j\geq 1} \underbrace{\sum_{m=1}^{n} \left[p^j \mid m\right]}_{\substack{=n//p^j \\ \text{(by (435))}}} = \sum_{j\geq 1} n//p^j = \sum_{i\geq 1} n//p^i$$

(here, we have renamed the summation index j as i). This solves Exercise 2.17.2 **(c)**.

(d) *Second proof of Corollary 2.17.11.* We must prove that $\binom{n}{k}$ is a nonnegative integer. If $k \notin \mathbb{N}$, then this holds (because if $k \notin \mathbb{N}$, then Definition 2.17.1 **(b)** yields $\binom{n}{k} = 0$). Thus, for the rest of this proof, we WLOG assume that $k \in \mathbb{N}$.

If $k > n$, then we have $\binom{n}{k} = 0$ (by Theorem 2.17.4). Hence, if $k > n$, then $\binom{n}{k}$ is clearly a nonnegative integer. Thus, for the rest of this proof, we WLOG assume that we don't have $k > n$. Hence, $k \leq n$. Therefore, $n \geq k$ and thus $n - k \in \mathbb{N}$. Hence, Theorem 2.17.3 yields

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}. \tag{436}$$

This yields that the number $\binom{n}{k}$ is positive (since the numbers $n!$, $k!$ and $(n-k)!$ are all positive) and therefore nonnegative. It remains to prove that $\binom{n}{k}$ is an integer.

Fix a prime p. We shall show that $v_p(k!\,(n-k)!) \leq v_p(n!)$. (This will then yield $k!\,(n-k)! \mid n!$, and this will in turn yield the integrality of $\binom{n}{k}$ by way of (436).)

Fix a positive integer i. Exercise 2.6.3 **(b)** (applied to k, $n-k$ and p^i instead of u, v and n) yields $(k + (n-k))//p^i - k//p^i - (n-k)//p^i \in \{0,1\} \subseteq \mathbb{N}$. This rewrites as $n//p^i - k//p^i - (n-k)//p^i \in \mathbb{N}$ (since $k + (n-k) = n$). Hence,

$$n//p^i - k//p^i - (n-k)//p^i \geq 0. \tag{437}$$

Now, forget that we fixed i. We thus have proven the inequality (437) for each positive integer i.

Theorem 2.13.28 **(a)** (applied to $a = k!$ and $b = (n-k)!$) yields

$$v_p(k!\,(n-k)!) = v_p(k!) + v_p((n-k)!).$$

Hence,

$$\begin{aligned}
& v_p(n!) - \underbrace{v_p(k!(n-k)!)}_{=v_p(k!)+v_p((n-k)!)} \\
&= v_p(n!) - \left(v_p(k!) + v_p((n-k)!)\right) \\
&= \underbrace{v_p(n!)}_{\substack{=\sum\limits_{i\geq 1} n//p^i \\ \text{(by Exercise 2.17.2 \textbf{(c)})}}} - \underbrace{v_p(k!)}_{\substack{=\sum\limits_{i\geq 1} k//p^i \\ \text{(by Exercise 2.17.2 \textbf{(c)},} \\ \text{applied to } k \text{ instead of } n)}} - \underbrace{v_p((n-k)!)}_{\substack{=\sum\limits_{i\geq 1} (n-k)//p^i \\ \text{(by Exercise 2.17.2 \textbf{(c)},} \\ \text{applied to } n-k \text{ instead of } n)}} \\
&= \sum_{i\geq 1} n//p^i - \sum_{i\geq 1} k//p^i - \sum_{i\geq 1} (n-k)//p^i = \sum_{i\geq 1} \underbrace{\left(n//p^i - k//p^i - (n-k)//p^i\right)}_{\substack{\geq 0 \\ \text{(by (437))}}} \\
&\geq \sum_{i\geq 1} 0 = 0.
\end{aligned}$$

In other words,

$$v_p(k!(n-k)!) \leq v_p(n!).$$

Now, forget that we fixed p. We thus have proven that each prime p satisfies $v_p(k!(n-k)!) \leq v_p(n!)$. But Proposition 2.13.35 (applied to $k!(n-k)!$ and $n!$ instead of n and m), we have $k!(n-k)! \mid n!$ if and only if each prime p satisfies $v_p(k!(n-k)!) \leq v_p(n!)$. Thus, we have $k!(n-k)! \mid n!$ (since each prime p satisfies $v_p(k!(n-k)!) \leq v_p(n!)$). In other words, $\dfrac{n!}{k!(n-k)!}$ is an integer (since $k!(n-k)! \neq 0$). In view of (436), this rewrites as follows: $\dbinom{n}{k}$ is an integer. Hence, $\dbinom{n}{k}$ is a nonnegative integer (since we already know that $\dbinom{n}{k}$ is nonnegative). Hence, Corollary 2.17.11 is proven again.

Thus, Exercise 2.17.2 **(d)** is solved. □

10.77. Solution to Exercise 2.17.3

Solution to Exercise 2.17.3. Let me first informally present the idea of the solution, and afterwards make it into a rigorous proof.

The idea is the following: If we want to choose an m-element subset S of A satisfying $B \subseteq S$, we cannot just arbitrarily pick m elements of A; this would fail to ensure that $B \subseteq S$. Thus, a better method is to start by picking all the b elements of B, and then supplement them with $m - b$ further elements from $A \setminus B$ (which can be picked at random). The only choice we have in this procedure is which $m - b$ elements of $A \setminus B$ we pick in the second step; this can be done in $\dbinom{a-b}{m-b}$ many ways (because it is tantamount to choosing an $(m-b)$-element subset of the $(a-b)$-element set $A \setminus B$; but Theorem 2.17.10 tells us that $\dbinom{a-b}{m-b}$ is the number of such subsets). Hence, the number of m-element subsets S of A satisfying $B \subseteq S$ is $\dbinom{a-b}{m-b}$.

Here is a formal version of this argument: We have $|A| = a$ (since A is an a-element set) and $|B| = b$ (since B is a b-element set). But B is a subset of A; thus, $|A \setminus B| = \underbrace{|A|}_{=a} - \underbrace{|B|}_{=b} = a - b$. In other words, $A \setminus B$ is an $(a-b)$-element set. Thus, Theorem 2.17.10 (applied to $n = a - b$, $k = m - b$ and $N = A \setminus B$) yields that $\dbinom{a-b}{m-b}$ is the number of $(m-b)$-element subsets of $A \setminus B$. In other words,

$$\binom{a-b}{m-b} = (\text{the number of } (m-b)\text{-element subsets of } A \setminus B) . \tag{438}$$

Now, let $\mathbf{L}$ be the set of all m-element subsets S of A satisfying $B \subseteq S$. Hence,

$$|\mathbf{L}| = (\text{the number of } m\text{-element subsets } S \text{ of } A \text{ satisfying } B \subseteq S) . \tag{439}$$

Furthermore, let $\mathbf{K}$ be the set of all $(m-b)$-element subsets of $A \setminus B$. Hence,

$$\begin{aligned} |\mathbf{K}| &= (\text{the number of } (m-b)\text{-element subsets of } A \setminus B) \\ &= \binom{a-b}{m-b} \qquad (\text{by (438)}) . \end{aligned} \tag{440}$$

Now, we shall construct a bijection between $\mathbf{K}$ and $\mathbf{L}$.

For each $P \in \mathbf{L}$, we have $P \setminus B \in \mathbf{K}$ [282]. Thus, we can define a map

$$\begin{aligned} f : \mathbf{L} &\to \mathbf{K}, \\ P &\mapsto P \setminus B. \end{aligned}$$

Consider this map f.

We intend to show that f is a bijection; for that purpose, let us construct its inverse.

For each $Q \in \mathbf{K}$, we have $Q \cup B \in \mathbf{L}$ [283]. Thus, we can define a map

$$\begin{aligned} g : \mathbf{K} &\to \mathbf{L}, \\ Q &\mapsto Q \cup B. \end{aligned}$$

[282] *Proof.* Let $P \in \mathbf{L}$. Thus, P is an m-element subset S of A satisfying $B \subseteq S$ (by the definition of $\mathbf{L}$). In other words, P is an m-element subset of A and satisfies $B \subseteq P$.

Now, P is a subset of A; thus, $P \setminus B$ is a subset of $A \setminus B$. Moreover, $|P| = m$ (since P is an m-element set). From $B \subseteq P$, we obtain $|P \setminus B| = \underbrace{|P|}_{=m} - \underbrace{|B|}_{=b} = m - b$. Hence, $P \setminus B$ is an $(m-b)$-element set. Thus, $P \setminus B$ is an $(m-b)$-element subset of $A \setminus B$. In other words, $P \setminus B \in \mathbf{K}$ (by the definition of $\mathbf{K}$). Qed.

[283] *Proof.* Let $Q \in \mathbf{K}$. Thus, Q is an $(m-b)$-element subset of $A \setminus B$ (by the definition of $\mathbf{K}$). Now, Q is a subset of $A \setminus B$; hence, Q is a subset of A and is disjoint from B. (This follows from basic set theory.)

Now we know that both sets Q and B are subsets of A. Hence, their union $Q \cup B$ is a subset of A as well. Furthermore, $|Q| = m - b$ (since Q is an $(m-b)$-element set). Since Q is disjoint from B, we have $|Q \cup B| = \underbrace{|Q|}_{=m-b} + \underbrace{|B|}_{=b} = (m-b) + b = m$. Thus, $Q \cup B$ is an m-element set. Hence, $Q \cup B$ is an m-element subset of A and satisfies $B \subseteq Q \cup B$ (obviously). In other words, $Q \cup B$ is an m-element subset S of A satisfying $B \subseteq S$. In other words, $Q \cup B \in \mathbf{L}$ (by the definition of $\mathbf{L}$). Qed.

Consider this map g.

We have $f \circ g = \operatorname{id}$ [284] and $g \circ f = \operatorname{id}$ [285]. These two equalities show that the maps f and g are mutually inverse. Hence, the map f is invertible, i.e., bijective. Thus, there exists a bijective map from $\mathbf{L}$ to $\mathbf{K}$ (namely, f). Hence, $|\mathbf{L}| = |\mathbf{K}|$. Comparing this with (439), we obtain

$$(\text{the number of } m\text{-element subsets } S \text{ of } A \text{ satisfying } B \subseteq S) = |\mathbf{K}| = \binom{a-b}{m-b}$$

(by (440)). Thus, Exercise 2.17.3 is rigorously solved. □

10.78. Solution to Exercise 2.17.4

We shall give two solutions to Exercise 2.17.4: one using Lucas's congruence (Theorem 2.17.20), and one using just basic properties of binomial coefficients. We start with the former:

First solution to Exercise 2.17.4. We have $p > 1$ (since p is a prime). Thus, $0 \in \{0, 1, \ldots, p-1\}$.

(a) Theorem 2.17.20 (applied to $a = 2$, $b = 1$, $c = 0$ and $d = 0$) yields

$$\binom{p \cdot 2 + 0}{p \cdot 1 + 0} \equiv \underbrace{\binom{2}{1}}_{=2} \underbrace{\binom{0}{0}}_{=1} = 2 \cdot 1 = 2 \mod p.$$

In view of $p \cdot 2 + 0 = 2p$ and $p \cdot 1 + 0 = p$, this rewrites as $\binom{2p}{p} \equiv 2 \mod p$. This solves Exercise 2.17.4 **(a)**.

(b) Theorem 2.17.20 (applied to $a = 1$, $b = 1$, $c = p-1$ and $d = 0$) yields

$$\binom{p \cdot 1 + (p-1)}{p \cdot 1 + 0} \equiv \underbrace{\binom{1}{1}}_{=1} \underbrace{\binom{p-1}{0}}_{=1} = 1 \cdot 1 = 1 \mod p.$$

[284] *Proof.* Let $Q \in \mathbf{K}$. Then, Q is an $(m-b)$-element subset of $A \setminus B$ (by the definition of $\mathbf{K}$). Now, Q is a subset of $A \setminus B$; hence, Q is a subset of A and is disjoint from B. (This follows from basic set theory.)

The definition of g yields $g(Q) = Q \cup B$. But the definition of f yields $f(g(Q)) = \underbrace{g(Q)}_{=Q \cup B} \setminus B = (Q \cup B) \setminus B = Q \setminus B = Q$ (since Q is disjoint from B). Hence, $(f \circ g)(Q) = f(g(Q)) = Q = \operatorname{id}(Q)$.

Now, forget that we fixed Q. We thus have shown that each $Q \in \mathbf{K}$ satisfies $(f \circ g)(Q) = \operatorname{id}(Q)$. In other words, $f \circ g = \operatorname{id}$.

[285] *Proof.* Let $P \in \mathbf{L}$. Thus, P is an m-element subset S of A satisfying $B \subseteq S$ (by the definition of $\mathbf{L}$). In other words, P is an m-element subset of A and satisfies $B \subseteq P$.

The definition of f yields $f(P) = P \setminus B$. But the definition of g yields $g(f(P)) = \underbrace{f(P)}_{=P \setminus B} \cup B = (P \setminus B) \cup B = P$ (since $B \subseteq P$). Hence, $(g \circ f)(P) = g(f(P)) = P = \operatorname{id}(P)$.

Now, forget that we fixed P. We thus have shown that $(g \circ f)(P) = \operatorname{id}(P)$ for each $P \in \mathbf{L}$. In other words, $g \circ f = \operatorname{id}$.

In view of $p \cdot 1 + (p-1) = 2p-1$ and $p \cdot 1 + 0 = p$, this rewrites as $\dbinom{2p-1}{p} \equiv 1 \bmod p$. This solves Exercise 2.17.4 **(b)**.

(c) Let $k \in \{1, 2, \ldots, p-1\}$. Thus, $k-1 \in \{0, 1, \ldots, p-2\} \subseteq \{0, 1, \ldots, p-1\}$ and $k \in \{1, 2, \ldots, p-1\} \subseteq \{0, 1, \ldots, p-1\}$. Hence, Theorem 2.17.20 (applied to $a = 1$, $b = 0$, $c = k-1$ and $d = k$) yields

$$\binom{p \cdot 1 + (k-1)}{p \cdot 0 + k} \equiv \underbrace{\binom{1}{0}}_{=1} \binom{k-1}{k} = \binom{k-1}{k} \bmod p.$$

In view of $p \cdot 1 + (k-1) = p-1+k$ and $p \cdot 0 + k = k$, this rewrites as

$$\binom{p-1+k}{k} \equiv \binom{k-1}{k} \bmod p. \tag{441}$$

But Theorem 2.17.4 (applied to $n = k-1$) yields $\dbinom{k-1}{k} = 0$ (since $k-1 \in \{0, 1, \ldots, p-1\} \subseteq \mathbb{N}$ and $k > k-1$). Hence, (441) becomes

$$\binom{p-1+k}{k} \equiv \binom{k-1}{k} = 0 \bmod p.$$

This solves Exercise 2.17.4 **(c)**. □

Second solution to Exercise 2.17.4. We have $p > 1$ (since p is a prime). Thus, $0 \in \{0, 1, \ldots, p-1\}$.

Furthermore, we have $(p-1)! \perp p$ [286].

(a) Theorem 2.17.9 (applied to $n = 2p$ and $k = p$) yields

$$p\binom{2p}{p} = 2p\binom{2p-1}{p-1}.$$

We can cancel p from this equality (since p is nonzero); thus, we obtain

$$\binom{2p}{p} = 2\binom{2p-1}{p-1}. \tag{442}$$

Now, $p-1 \in \mathbb{N}$ (since $p > 1$). Thus, the definition of $\dbinom{2p-1}{p-1}$ yields

$$\binom{2p-1}{p-1} = \frac{(2p-1)\left((2p-1)-1\right)\left((2p-1)-2\right)\cdots\left((2p-1)-(p-1)+1\right)}{(p-1)!}.$$

[286] *Proof.* It is easy to derive this from Wilson's theorem (Theorem 2.15.7), but let us give a more elementary proof:

Each $i \in \{1, 2, \ldots, p-1\}$ is coprime to p (by Proposition 2.13.4). In other words, each $i \in \{1, 2, \ldots, p-1\}$ satisfies $i \perp p$. Hence, Exercise 2.10.2 (applied to $c = p$, $k = p-1$ and $a_i = i$) shows that $1 \cdot 2 \cdot \cdots \cdot (p-1) \perp p$. This rewrites as $(p-1)! \perp p$ (since $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$).

Hence,

$$\begin{aligned}(p-1)!\cdot\binom{2p-1}{p-1} &= (2p-1)\left((2p-1)-1\right)\left((2p-1)-2\right)\cdots\left((2p-1)-(p-1)+1\right)\\ &= \prod_{i=0}^{(p-1)-1}\left((2p-1)-i\right) = \prod_{s=1}^{p-1}\underbrace{\left((2p-1)-(p-1-s)\right)}_{=p+s}\\ &\qquad \text{(here, we have substituted } p-1-s \text{ for } i \text{ in the product)}\\ &= \prod_{s=1}^{p-1}\underbrace{(p+s)}_{\equiv s \bmod p} \equiv \prod_{s=1}^{p-1} s \bmod p\end{aligned}$$

[287]. Thus,

$$(p-1)!\cdot\binom{2p-1}{p-1} \equiv \prod_{s=1}^{p-1} s = 1\cdot 2\cdot\cdots\cdot(p-1) = (p-1)! = (p-1)!\cdot 1 \bmod p.$$

Hence, Lemma 2.10.10 (applied to $n=p$, $a=(p-1)!$, $b=\binom{2p-1}{p-1}$ and $c=1$) shows that

$$\binom{2p-1}{p-1} \equiv 1 \bmod p \qquad (443)$$

(since $(p-1)! \perp p$). Thus, (442) becomes

$$\binom{2p}{p} = 2\underbrace{\binom{2p-1}{p-1}}_{\equiv 1 \bmod p} \equiv 2\cdot 1 = 2 \bmod p.$$

This solves Exercise 2.17.4 **(a)**.

(b) We have $2p-1\in\mathbb{N}$ (since $p>1$). Thus, Theorem 2.17.6 (applied to $n=2p-1$ and $k=p$) yields

$$\begin{aligned}\binom{2p-1}{p} &= \binom{2p-1}{(2p-1)-p} = \binom{2p-1}{p-1} \qquad \left(\text{since } (2p-1)-p = p-1\right)\\ &\equiv 1 \bmod p \qquad \text{(by (443))}.\end{aligned}$$

This solves Exercise 2.17.4 **(b)**.

[287] Here is a detailed justification of the last "$\equiv$" sign in this computation: We have $p+s\equiv s \bmod p$ for each $s\in\{1,2,\ldots,p-1\}$. Hence, (9) (applied to $n=p$, $S=\{1,2,\ldots,p-1\}$, $a_s=p+s$ and $b_s=s$) yields

$$\prod_{s\in\{1,2,\ldots,p-1\}}(p+s) \equiv \prod_{s\in\{1,2,\ldots,p-1\}} s \bmod p.$$

This congruence rewrites as $\prod_{s=1}^{p-1}(p+s) \equiv \prod_{s=1}^{p-1} s \bmod p$ (since the "$\prod_{s\in\{1,2,\ldots,p-1\}}$" sign is equivalent to "$\prod_{s=1}^{p-1}$"). Qed.

(c) Let $k \in \{1, 2, \ldots, p-1\}$. Thus, $k - 1 \in \{0, 1, \ldots, p-2\} \subseteq \mathbb{N}$, so that $k - 1 \in \{0, 1, \ldots, k-1\}$.

We have $k \in \{1, 2, \ldots, p-1\}$, so that $k \leq p - 1$. Hence, $k! \perp p$ [288]. Thus, $p \perp k!$ (by Proposition 2.10.4).

The definition of $\dbinom{p-1+k}{k}$ yields

$$\dbinom{p-1+k}{k} = \frac{(p-1+k)\left((p-1+k)-1\right)\left((p-1+k)-2\right)\cdots\left((p-1+k)-k+1\right)}{k!}.$$

Hence,

$$\begin{aligned} & k! \cdot \dbinom{p-1+k}{k} \\ & = (p-1+k)\left((p-1+k)-1\right)\left((p-1+k)-2\right)\cdots\left((p-1+k)-k+1\right) \\ & = \prod_{i=0}^{k-1}\left((p-1+k)-i\right) = \underbrace{\left((p-1+k)-(k-1)\right)}_{=p} \cdot \prod_{i=0}^{k-2}\left((p-1+k)-i\right) \\ & \qquad \left(\begin{array}{c} \text{here, we have split off the factor for } i = k-1 \\ \text{from the product, since } k-1 \in \{0,1,\ldots,k-1\} \end{array}\right) \\ & = p \cdot \prod_{i=0}^{k-2}\left((p-1+k)-i\right). \end{aligned}$$

This shows that $p \mid k! \cdot \dbinom{p-1+k}{k}$ (since $\prod\limits_{i=0}^{k-2}\left((p-1+k)-i\right)$ is an integer). Thus, Theorem 2.10.6 (applied to $a = p$, $b = k!$ and $c = \dbinom{p-1+k}{k}$) yields $p \mid \dbinom{p-1+k}{k}$ (since $p \perp k!$). In other words, $\dbinom{p-1+k}{k} \equiv 0 \mod p$. This solves Exercise 2.17.4 **(c)**. □

10.79. Solution to Exercise 2.18.1

Solution to Exercise 2.18.1. **(a)** For every prime $p > |n|$, we have $v_p(n) = 0$ (by Lemma 2.13.32 **(a)**) and thus

$$p^{0k} + p^{1k} + \cdots + p^{v_p(n) \cdot k} = p^{0k} + p^{1k} + \cdots + p^{0k} = p^{0k} = p^0 = 1.$$

Thus, all but finitely many primes p satisfy $p^{0k} + p^{1k} + \cdots + p^{v_p(n) \cdot k} = 1$ (since all but finitely many primes p satisfy $p > |n|$). Therefore, all but finitely many factors of the product $\prod\limits_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(n) \cdot k}\right)$ are 1. In other words, the product $\prod\limits_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(n) \cdot k}\right)$ has only finitely many factors different from 1. Hence, this product is well-defined. This solves Exercise 2.18.1 **(a)**.

[288] *Proof.* Each $i \in \{1, 2, \ldots, k\}$ satisfies $i \in \{1, 2, \ldots, p-1\}$ (since $k \leq p - 1$) and therefore is coprime to p (by Proposition 2.13.4). In other words, each $i \in \{1, 2, \ldots, k\}$ satisfies $i \perp p$. Hence, Exercise 2.10.2 (applied to $c = p$ and $a_i = i$) shows that $1 \cdot 2 \cdot \cdots \cdot k \perp p$. This rewrites as $k! \perp p$ (since $k! = 1 \cdot 2 \cdot \cdots \cdot k$).

(b) Forget that we fixed k. Instead, fix $w \in \mathbb{Z}$. (The only reason we are doing this is that we will have to use the letter "k" for a different purpose.)

For every prime $p > |n|$, we have $v_p(n) = 0$ (by Lemma 2.13.32 **(a)**). Thus, all but finitely many primes p satisfy $v_p(n) = 0$ (since all but finitely many primes p satisfy $p > |n|$). In other words, the set of all primes p satisfying $v_p(n) \neq 0$ is finite. Let P be this set. Thus, P is finite.

Let $(p_1, p_2, \ldots, p_u)$ be a list of elements of P, with no repetitions.[289] Thus, $\{p_1, p_2, \ldots, p_u\} = P$. Now, the elements $p_1, p_2, \ldots, p_u$ belong to $\{p_1, p_2, \ldots, p_u\} = P$, and thus are primes (since P is a set of primes). Furthermore, the elements $p_1, p_2, \ldots, p_u$ are distinct (since $(p_1, p_2, \ldots, p_u)$ was defined to be a list with no repetitions).

For each $i \in \{1, 2, \ldots, u\}$, define a nonnegative integer a_i by

$$a_i = v_{p_i}(n). \tag{444}$$

This is well-defined, since p_i is a prime (because $p_1, p_2, \ldots, p_u$ are primes) and since n is nonzero.

The following facts have been proven in the proof of Proposition 2.18.1:

- The map $\{1, 2, \ldots, u\} \to \{p_1, p_2, \ldots, p_u\}, \ i \mapsto p_i$ is a bijection.
- If p is a prime such that $p \notin \{p_1, p_2, \ldots, p_u\}$, then
$$v_p(n) = 0. \tag{445}$$
- We have $n = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}$.

If p is a prime such that $p \notin \{p_1, p_2, \ldots, p_u\}$, then

$$\begin{aligned} p^{0w} + p^{1w} + \cdots + p^{v_p(n) \cdot w} &= p^{0w} + p^{1w} + \cdots + p^{0w} && \left(\text{since (445) yields } v_p(n) = 0\right) \\ &= p^{0w} = p^0 = 1. && (446) \end{aligned}$$

Define a set T as in Lemma 2.18.3. Then, Lemma 2.18.3 says that the map

$$\begin{aligned} \Lambda : T &\to \{\text{positive divisors of } n\}, \\ (b_1, b_2, \ldots, b_u) &\mapsto p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u} \end{aligned}$$

is well-defined and bijective. Thus, this map Λ is a bijection.

Now, the summation sign "$\sum\limits_{d|n}$" stands for a sum over all positive divisors of n, and thus

[289] Such a list exists, since P is finite.

is equivalent to the summation sign "$\sum\limits_{d\in\{\text{positive divisors of } n\}}$". Hence,

$$\begin{aligned}
\sum_{d\mid n} d^w &= \sum_{d\in\{\text{positive divisors of } n\}} d^w = \sum_{(b_1,b_2,\ldots,b_u)\in T} \left(\underbrace{\Lambda\left(b_1,b_2,\ldots,b_u\right)}_{\substack{=p_1^{b_1}p_2^{b_2}\cdots p_u^{b_u} \\ \text{(by the definition of } \Lambda)}} \right)^w \\
&\qquad \left(\begin{array}{c} \text{here, we have substituted } \Lambda\left(b_1,b_2,\ldots,b_u\right) \text{ for } d \text{ in the} \\ \text{sum, since the map } \Lambda : T \to \{\text{positive divisors of } n\} \\ \text{is a bijection} \end{array} \right) \\
&= \sum_{(b_1,b_2,\ldots,b_u)\in T} \underbrace{\left(p_1^{b_1}p_2^{b_2}\cdots p_u^{b_u}\right)^w}_{=p_1^{b_1w}p_2^{b_2w}\cdots p_u^{b_uw}=\prod\limits_{i=1}^u p_i^{b_iw}} \\
&= \sum_{(b_1,b_2,\ldots,b_u)\in T} \prod_{i=1}^u p_i^{b_iw}. \qquad (447)
\end{aligned}$$

Now, Lemma 2.18.6 (applied to u, $\{0,1,\ldots,a_i\}$ and p_i^{kw} instead of n, Z_i and $p_{i,k}$) yields

$$\begin{aligned}
\prod_{i=1}^u \sum_{k\in\{0,1,\ldots,a_i\}} p_i^{kw} &= \sum_{(k_1,k_2,\ldots,k_u)\in\{0,1,\ldots,a_1\}\times\{0,1,\ldots,a_2\}\times\cdots\times\{0,1,\ldots,a_u\}} \prod_{i=1}^u p_i^{k_iw} \\
&= \sum_{(b_1,b_2,\ldots,b_u)\in\{0,1,\ldots,a_1\}\times\{0,1,\ldots,a_2\}\times\cdots\times\{0,1,\ldots,a_u\}} \prod_{i=1}^u p_i^{b_iw} \\
&\qquad \left(\begin{array}{c} \text{here, we have renamed the summation} \\ \text{index } \left(k_1,k_2,\ldots,k_u\right) \text{ as } \left(b_1,b_2,\ldots,b_u\right) \end{array} \right) \\
&= \sum_{(b_1,b_2,\ldots,b_u)\in T} \prod_{i=1}^u p_i^{b_iw}
\end{aligned}$$

(since $\{0,1,\ldots,a_1\}\times\{0,1,\ldots,a_2\}\times\cdots\times\{0,1,\ldots,a_u\} = T$). Comparing this with (447), we find

$$\sum_{d\mid n} d^w = \prod_{i=1}^u \underbrace{\sum_{k\in\{0,1,\ldots,a_i\}} p_i^{kw}}_{=p_i^{0w}+p_i^{1w}+\cdots+p_i^{a_iw}} = \prod_{i=1}^u \left(p_i^{0w}+p_i^{1w}+\cdots+p_i^{a_iw}\right).$$

Comparing this with

$$\begin{aligned}
&\prod_{p \text{ prime}} \left(p^{0w} + p^{1w} + \cdots + p^{v_p(n)\cdot w}\right) \\
&= \left(\prod_{\substack{p \text{ prime};\\ p \in \{p_1,p_2,\ldots,p_u\}}} \left(p^{0w} + p^{1w} + \cdots + p^{v_p(n)\cdot w}\right)\right) \left(\prod_{\substack{p \text{ prime};\\ p \notin \{p_1,p_2,\ldots,p_u\}}} \underbrace{\left(p^{0w} + p^{1w} + \cdots + p^{v_p(n)\cdot w}\right)}_{\substack{=1\\ \text{(by (446))}}}\right) \\
&\qquad \left(\begin{array}{c}\text{since each prime } p \text{ satisfies either } p \in \{p_1,p_2,\ldots,p_u\} \\ \text{or } p \notin \{p_1,p_2,\ldots,p_u\} \text{ (but not both simultaneously)}\end{array}\right) \\
&= \left(\prod_{\substack{p \text{ prime};\\ p \in \{p_1,p_2,\ldots,p_u\}}} \left(p^{0w} + p^{1w} + \cdots + p^{v_p(n)\cdot w}\right)\right) \underbrace{\left(\prod_{\substack{p \text{ prime};\\ p \notin \{p_1,p_2,\ldots,p_u\}}} 1 \right)}_{=1} \\
&= \underbrace{\prod_{\substack{p \text{ prime};\\ p \in \{p_1,p_2,\ldots,p_u\}}}}_{\substack{= \prod_{p \in \{p_1,p_2,\ldots,p_u\}} \\ \text{(since each } p \in \{p_1,p_2,\ldots,p_u\} \\ \text{is a prime)}}} \left(p^{0w} + p^{1w} + \cdots + p^{v_p(n)\cdot w}\right) \\
&= \prod_{p \in \{p_1,p_2,\ldots,p_u\}} \left(p^{0w} + p^{1w} + \cdots + p^{v_p(n)\cdot w}\right) = \prod_{i=1}^{u} \underbrace{\left(p_i^{0w} + p_i^{1w} + \cdots + p_i^{v_{p_i}(n)\cdot w}\right)}_{\substack{= p_i^{0w} + p_i^{1w} + \cdots + p_i^{a_i w} \\ \text{(since (444) yields } v_{p_i}(n) = a_i)}} \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } p_i \text{ for } p \text{ in the product,} \\ \text{since the map } \{1,2,\ldots,u\} \to \{p_1,p_2,\ldots,p_u\},\ i \mapsto p_i \text{ is a bijection}\end{array}\right) \\
&= \prod_{i=1}^{u} \left(p_i^{0w} + p_i^{1w} + \cdots + p_i^{a_i w}\right),
\end{aligned}$$

we obtain

$$\sum_{d \mid n} d^w = \prod_{p \text{ prime}} \left(p^{0w} + p^{1w} + \cdots + p^{v_p(n)\cdot w}\right).$$

Now, forget that we fixed w. We thus have proven that every $w \in \mathbb{Z}$ satisfies

$$\sum_{d \mid n} d^w = \prod_{p \text{ prime}} \left(p^{0w} + p^{1w} + \cdots + p^{v_p(n)\cdot w}\right).$$

Renaming the index w as k in this statement, we conclude that every $k \in \mathbb{Z}$ satisfies

$$\sum_{d \mid n} d^k = \prod_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(n)\cdot k}\right).$$

This solves Exercise 2.18.1 **(b)**. □

10.80. Solution to Exercise 2.18.2

We shall prepare for the solution to Exercise 2.18.2 by defining a function L on $\mathbb{Z}$ and proving a bunch of its properties.

Definition 10.80.1. Throughout this section, we shall use the following notation: For each $u \in \mathbb{Z}$, we set

$$L(u) = \begin{cases} 1, & \text{if } u\%4 = 1; \\ -1, & \text{if } u\%4 = 3; \\ 0, & \text{otherwise.} \end{cases}$$

We notice the following properties of this definition:

Lemma 10.80.2. Let $u \in \mathbb{Z}$.

(a) If $\gcd(u, 4) \neq 1$, then $L(u) = 0$.

(b) If $\gcd(u, 4) = 1$, then $L(u) \equiv u \bmod 4$.

Proof of Lemma 10.80.2. Corollary 2.6.9 **(a)** (applied to $n = 4$) yields $u\%4 \in \{0, 1, \ldots, 4-1\}$ and $u\%4 \equiv u \bmod 4$. Hence, $u \equiv u\%4 \bmod 4$ and $u\%4 \in \{0, 1, \ldots, 4-1\} = \{0, 1, 2, 3\}$.

Proposition 2.9.7 **(e)** (applied to $a = 4$ and $b = u$) yields $\gcd(4, u) = \gcd(4, u\%4)$. But Proposition 2.9.7 **(b)** yields

$$\gcd(u, 4) = \gcd(4, u) = \gcd(4, u\%4). \tag{448}$$

We have $u\%4 \in \{0, 1, 2, 3\}$. In other words, we have $u\%4 = 0$ or $u\%4 = 1$ or $u\%4 = 2$ or $u\%4 = 3$. Hence, we are in one of the following four cases:

Case 1: We have $u\%4 = 0$.

Case 2: We have $u\%4 = 1$.

Case 3: We have $u\%4 = 2$.

Case 4: We have $u\%4 = 3$.

Let us first consider Case 1. In this case, we have $u\%4 = 0$. Hence, we have neither $u\%4 = 1$ nor $u\%4 = 3$.

Also, from $u\%4 = 0$, we obtain $\gcd(u, 4) \neq 1$ [290]. Hence, $\gcd(u, 4) = 1$ is false. Thus, the claim of Lemma 10.80.2 **(b)** is vacuously true (in Case 1). Furthermore, the definition of $L(u)$ yields $L(u) = \begin{cases} 1, & \text{if } u\%4 = 1; \\ -1, & \text{if } u\%4 = 3; \\ 0, & \text{otherwise} \end{cases} = 0$ (since we have neither $u\%4 = 1$ nor $u\%4 = 3$). Thus, the claim of Lemma 10.80.2 **(a)** is true (in Case 1). Hence, we have proven that both Lemma 10.80.2 **(a)** and Lemma 10.80.2 **(b)** are true (in Case 1). In other words, Lemma 10.80.2 is proven in Case 1.

Let us next consider Case 2. In this case, we have $u\%4 = 1$.

[290] *Proof.* Proposition 2.9.7 **(a)** (applied to $a = 4$) yields $\gcd(4, 0) = \gcd(4) = |4|$.

Now, (448) becomes $\gcd(u, 4) = \gcd\left(4, \underbrace{u\%4}_{=0}\right) = \gcd(4, 0) = |4| = 4 \neq 1$.

Thus, $\gcd(u,4) = 1$ [291]. Hence, $\gcd(u,4) \neq 1$ is false. Thus, the claim of Lemma 10.80.2 **(a)** is vacuously true (in Case 2). Furthermore, the definition of $L(u)$ yields $L(u) = \begin{cases} 1, & \text{if } u\%4 = 1; \\ -1, & \text{if } u\%4 = 3; \\ 0, & \text{otherwise} \end{cases} = 1$ (since $u\%4 = 1$), so that $L(u) = 1 = u\%4 \equiv u \mod 4$. Thus, the claim of Lemma 10.80.2 **(b)** is true (in Case 2). Hence, we have proven that both Lemma 10.80.2 **(a)** and Lemma 10.80.2 **(b)** are true (in Case 2). In other words, Lemma 10.80.2 is proven in Case 2.

Let us next consider Case 3. In this case, we have $u\%4 = 2$. Hence, we have neither $u\%4 = 1$ nor $u\%4 = 3$.

Also, from $u\%4 = 2$, we obtain $\gcd(u,4) \neq 1$ [292]. Hence, $\gcd(u,4) = 1$ is false. Thus, the claim of Lemma 10.80.2 **(b)** is vacuously true (in Case 3). Furthermore, the definition of $L(u)$ yields $L(u) = \begin{cases} 1, & \text{if } u\%4 = 1; \\ -1, & \text{if } u\%4 = 3; \\ 0, & \text{otherwise} \end{cases} = 0$ (since we have neither $u\%4 = 1$ nor $u\%4 = 3$). Thus, the claim of Lemma 10.80.2 **(a)** is true (in Case 3). Hence, we have proven that both Lemma 10.80.2 **(a)** and Lemma 10.80.2 **(b)** are true (in Case 3). In other words, Lemma 10.80.2 is proven in Case 3.

Finally, let us consider Case 4. In this case, we have $u\%4 = 3$. Thus, $\gcd(u,4) = 1$ [293]. Hence, $\gcd(u,4) \neq 1$ is false. Thus, the claim of Lemma 10.80.2 **(a)** is vacuously true (in Case 4). Furthermore, $-1 \equiv 3 \mod 4$ (since $(-1) - 3 = -4$ is divisible by 4). But the definition of $L(u)$ yields $L(u) = \begin{cases} 1, & \text{if } u\%4 = 1; \\ -1, & \text{if } u\%4 = 3; \\ 0, & \text{otherwise} \end{cases} = -1$ (since $u\%4 = 3$), so that

[291] *Proof.* The equality (448) becomes $\gcd(u,4) = \gcd\left(4, \underbrace{u\%4}_{=1}\right) = \gcd(4,1) = \gcd(1,4)$ (by Proposition 2.9.7 **(b)**). But $1 \mid 4$; hence, Proposition 2.9.7 **(i)** (applied to $a = 1$ and $b = 4$) yields $\gcd(1,4) = |1| = 1$. Hence, $\gcd(u,4) = \gcd(1,4) = 1$.

[292] *Proof.* We have $2 \mid 4$; thus, Proposition 2.9.7 **(i)** (applied to $a = 2$ and $b = 4$) yields $\gcd(2,4) = |2| = 2$. On the other hand, Proposition 2.9.7 **(b)** yields $\gcd(4,2) = \gcd(2,4) = 2$.

Now, (448) becomes $\gcd(u,4) = \gcd\left(4, \underbrace{u\%4}_{=2}\right) = \gcd(4,2) = 2 \neq 1$.

[293] *Proof.* From (448), we obtain

$$\begin{aligned} \gcd(u,4) &= \gcd\left(4, \underbrace{u\%4}_{=3}\right) = \gcd(4,3) = \gcd(3,4) && \text{(by Proposition 2.9.7 (b))} \\ &= \gcd\left(3, \underbrace{4\%3}_{=1}\right) && \text{(by Proposition 2.9.7 (e), applied to } a = 3 \text{ and } b = 4) \\ &= \gcd(3,1) = \gcd(1,3) && \text{(by Proposition 2.9.7 (b))}. \end{aligned}$$

But $1 \mid 3$; thus, Proposition 2.9.7 **(i)** (applied to $a = 1$ and $b = 3$) yields $\gcd(1,3) = |1| = 1$. Hence, $\gcd(u,4) = \gcd(1,3) = 1$.

$L(u) = -1 \equiv 3 = u\%4 \equiv u \mod 4$. Thus, the claim of Lemma 10.80.2 **(b)** is true (in Case 4). Hence, we have proven that both Lemma 10.80.2 **(a)** and Lemma 10.80.2 **(b)** are true (in Case 4). In other words, Lemma 10.80.2 is proven in Case 4.

We have now proven Lemma 10.80.2 in all four Cases 1, 2, 3 and 4. Thus, Lemma 10.80.2 always holds. □

Lemma 10.80.3. *Let x, y, z be three elements of the set $\{-1, 0, 1\}$. If $xy \equiv z \mod 4$, then $xy = z$.*

Proof of Lemma 10.80.3. It is easy to prove this lemma by mechanically verifying that it holds for all 3^3 possible choices of (x, y, z); but here is a "smarter" proof:

We have $x \in \{-1, 0, 1\} = \{-1, 0, \ldots, 1\}$. In other words, $-1 \leq x \leq 1$. In other words, $|x| \leq 1$. Similarly, $|y| \leq 1$. We can multiply the two inequalities $|x| \leq 1$ and $|y| \leq 1$ together (this is legitimate, since all of their sides $|x|$, 1, $|y|$ and 1 are nonnegative reals); thus we obtain $|x| \cdot |y| \leq 1 \cdot 1 = 1$. Now, (3) yields $|xy| = |x| \cdot |y| \leq 1$. In other words, $-1 \leq xy \leq 1$. Furthermore, x and y are two elements of $\{-1, 0, 1\}$ and thus are integers; hence, xy is an integer as well. Thus, from $-1 \leq xy \leq 1$, we obtain $xy \in \{-1, 0, \ldots, 1\} = \{-1, 0, 1\}$. Therefore, $xy + 1 \in \{0, 1, 2\} \subseteq \{0, 1, 2, 3\} = \{0, 1, \ldots, 4 - 1\}$.

Also, from $z \in \{-1, 0, 1\}$, we obtain $z + 1 \in \{0, 1, 2\} \subseteq \{0, 1, 2, 3\} = \{0, 1, \ldots, 4 - 1\}$.

Adding the congruence $xy \equiv z \mod 4$ to the trivial congruence $1 \equiv 1 \mod 4$, we obtain $xy + 1 \equiv z + 1 \mod 4$. Hence, Corollary 2.6.9 **(c)** (applied to $n = 4$, $u = z + 1$ and $c = xy + 1$) shows that

$$xy + 1 = (z + 1) \%4 \tag{449}$$

(since $xy + 1 \in \{0, 1, \ldots, 4 - 1\}$).

On the other hand, $z + 1 \in \{0, 1, \ldots, 4 - 1\}$ and $z + 1 \equiv z + 1 \mod 4$ (obviously). Hence, Corollary 2.6.9 **(c)** (applied to $n = 4$, $u = z + 1$ and $c = z + 1$) shows that $z + 1 = (z + 1) \%4$. Comparing this equality with (449), we find $xy + 1 = z + 1$. Cancelling 1 from this equality, we find $xy = z$. This proves Lemma 10.80.3. □

Lemma 10.80.4. *Let $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$. Then, $L(uv) = L(u) \cdot L(v)$.*

Proof of Lemma 10.80.4. Corollary 2.6.9 **(a)** (applied to $n = 4$) yields $u\%4 \in \{0, 1, \ldots, 4 - 1\}$ and $u\%4 \equiv u \mod 4$. Thus, in particular, $u\%4 \equiv u \mod 4$, so that $u \equiv u\%4 \mod 4$. The same argument (applied to v instead of u) yields $v \equiv v\%4 \mod 4$.

We next observe the following:

Claim 1: If $\gcd(u, 4) \neq 1$, then $L(uv) = L(u) \cdot L(v)$.

[*Proof of Claim 1:* Assume that $\gcd(u, 4) \neq 1$. We must prove that $L(uv) = L(u) \cdot L(v)$.

Note that $\gcd(u, 4)$ is a nonnegative integer (by the definition of a gcd). Hence, if we had $\gcd(u, 4) \mid 1$, then we would have $\gcd(u, 4) = 1$ (by Exercise 2.2.5, applied to $g = \gcd(u, 4)$), which would contradict $\gcd(u, 4) \neq 1$. Thus, we cannot have $\gcd(u, 4) \mid 1$.

Lemma 10.80.2 **(a)** yields $L(u) = 0$ (since $\gcd(u, 4) \neq 1$).

Also, $u \mid uv$ and $4 \mid 4$. Hence, Exercise 2.9.4 (applied to $a_1 = u$, $a_2 = 4$, $b_1 = uv$ and $b_2 = 4$) yields $\gcd(u, 4) \mid \gcd(uv, 4)$. If we had $\gcd(uv, 4) = 1$, then this would entail $\gcd(u, 4) \mid \gcd(uv, 4) = 1$; but this would contradict the fact that we cannot have $\gcd(u, 4) \mid 1$. Hence, we cannot have $\gcd(uv, 4) = 1$. In other words, we must have

$\gcd(uv,4) \neq 1$. Hence, Lemma 10.80.2 **(a)** (applied to uv instead of u) yields $L(uv) = 0$. Comparing this with $\underbrace{L(u)}_{=0} \cdot L(v) = 0$, we obtain $L(uv) = L(u) \cdot L(v)$. This proves Claim 1.]

Claim 2: If $\gcd(v,4) \neq 1$, then $L(uv) = L(u) \cdot L(v)$.

[*Proof of Claim 2:* Claim 2 is obtained from Claim 1 by interchanging u and v (since u and v clearly play symmetric roles in the statement "$L(uv) = L(u) \cdot L(v)$"). Thus, the proof of Claim 2 is analogous to the proof of Claim 1.]

Now, we must prove that $L(uv) = L(u) \cdot L(v)$. If $\gcd(u,4) \neq 1$, then this follows from Claim 1. Hence, for the rest of this proof, we can WLOG assume that $\gcd(u,4) = 1$. Assume this.

Now, we must prove that $L(uv) = L(u) \cdot L(v)$. If $\gcd(v,4) \neq 1$, then this follows from Claim 2. Hence, for the rest of this proof, we can WLOG assume that $\gcd(v,4) = 1$. Assume this.

From $\gcd(u,4) = 1$, we obtain $u \perp 4$ (by the definition of "coprime"). From $\gcd(v,4) = 1$, we obtain $v \perp 4$ (by the definition of "coprime"). Hence, Theorem 2.10.9 (applied to $a = u$, $b = v$ and $c = 4$) yields $uv \perp 4$. In other words, $\gcd(uv,4) = 1$ (by the definition of "coprime"). Hence, Lemma 10.80.2 **(b)** (applied to uv instead of u) yields $L(uv) \equiv uv \mod 4$. Furthermore, recall that $\gcd(u,4) = 1$; hence, Lemma 10.80.2 **(b)** yields $L(u) \equiv u \mod 4$. Moreover, $\gcd(v,4) = 1$; thus, Lemma 10.80.2 **(b)** (applied to v instead of u) yields $L(v) \equiv v \mod 4$. Thus,

$$\underbrace{L(u)}_{\equiv u \mod 4} \cdot \underbrace{L(v)}_{\equiv v \mod 4} \equiv uv \equiv L(uv) \mod 4 \qquad (450)$$

(since $L(uv) \equiv uv \mod 4$).

The definition of $L(u)$ yields $L(u) = \begin{cases} 1, & \text{if } u\%4 = 1; \\ -1, & \text{if } u\%4 = 3; \\ 0, & \text{otherwise} \end{cases} \in \{-1,0,1\}$ (since all three values $1, -1, 0$ belong to the set $\{-1,0,1\}$). The same argument (applied to v instead of u) shows that $L(v) \in \{-1,0,1\}$. Furthermore, the argument that we used to prove $L(u) \in \{-1,0,1\}$ can also be applied to uv instead of u; thus we obtain $L(uv) \in \{-1,0,1\}$. Thus, altogether, we know that $L(u)$, $L(v)$ and $L(uv)$ are three elements of the set $\{-1,0,1\}$. These elements satisfy $L(u) \cdot L(v) \equiv L(uv) \mod 4$ (by (450)). Hence, Lemma 10.80.3 (applied to $x = L(u)$, $y = L(v)$ and $z = L(uv)$) yields $L(u) \cdot L(v) = L(uv)$. In other words, $L(uv) = L(u) \cdot L(v)$. This proves Lemma 10.80.4. □

Lemma 10.80.5. Let $a_1, a_2, \ldots, a_k$ be finitely many integers. Then,

$$L(a_1 a_2 \cdots a_k) = L(a_1) \cdot L(a_2) \cdot \cdots \cdot L(a_k).$$

Proof of Lemma 10.80.5. We claim that

$$L(a_1 a_2 \cdots a_i) = L(a_1) \cdot L(a_2) \cdot \cdots \cdot L(a_i) \qquad (451)$$

for each $i \in \{0, 1, \ldots, k\}$.

[*Proof of (451):* We shall prove (451) by induction on i:

Induction base: We have $a_1a_2\cdots a_0 = (\text{empty product}) = 1$; thus,

$$\begin{aligned} L(a_1a_2\cdots a_0) = L(1) &= \begin{cases} 1, & \text{if } 1\%4 = 1; \\ -1, & \text{if } 1\%4 = 3; \\ 0, & \text{otherwise} \end{cases} \qquad (\text{by the definition of } L(1)) \\ &= 1 \qquad (\text{since } 1\%4 = 1). \end{aligned}$$

Comparing this with $L(a_1)\cdot L(a_2)\cdot\cdots\cdot L(a_0) = (\text{empty product}) = 1$, we obtain

$$L(a_1a_2\cdots a_0) = L(a_1)\cdot L(a_2)\cdot\cdots\cdot L(a_0).$$

In other words, (451) holds for $i=0$. This completes the induction base.

Induction step: Let $j \in \{1,2,\ldots,k\}$. Assume that (451) holds for $i = j-1$. We must prove that (451) holds for $i = j$.

We have assumed that (451) holds for $i = j-1$. In other words, we have

$$L(a_1a_2\cdots a_{j-1}) = L(a_1)\cdot L(a_2)\cdot\cdots\cdot L(a_{j-1}).$$

Now,

$$\begin{aligned} L\left(\underbrace{a_1a_2\cdots a_j}_{=(a_1a_2\cdots a_{j-1})a_j}\right) &= L((a_1a_2\cdots a_{j-1})a_j) = \underbrace{L(a_1a_2\cdots a_{j-1})}_{=L(a_1)\cdot L(a_2)\cdot\cdots\cdot L(a_{j-1})} \cdot L(a_j) \\ &\qquad (\text{by Lemma 10.80.4, applied to } u = a_1a_2\cdots a_{j-1} \text{ and } v = a_j) \\ &= (L(a_1)\cdot L(a_2)\cdot\cdots\cdot L(a_{j-1}))\cdot L(a_j) \\ &= L(a_1)\cdot L(a_2)\cdot\cdots\cdot L(a_j). \end{aligned}$$

In other words, (451) holds for $i = j$. This completes the induction step. Thus, (451) is proven by induction.]

Now, (451) (applied to $i = k$) yields $L(a_1a_2\cdots a_k) = L(a_1)\cdot L(a_2)\cdot\cdots\cdot L(a_k)$. This proves Lemma 10.80.5. □

Lemma 10.80.6. Let $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then, $L(a^k) = (L(a))^k$.

Proof of Lemma 10.80.6. Lemma 10.80.5 (applied to $a_i = a$) yields

$$L\left(\underbrace{aa\cdots a}_{k\text{ times}}\right) = \underbrace{L(a)\cdot L(a)\cdot\cdots\cdot L(a)}_{k\text{ times}} = (L(a))^k.$$

In view of $\underbrace{aa\cdots a}_{k\text{ times}} = a^k$, this rewrites as $L(a^k) = (L(a))^k$. Thus, Lemma 10.80.6 is proven. □

Lemma 10.80.7. Let $u \in \mathbb{N}$. Let $p_1, p_2, \ldots, p_u$ be u integers. Let $b_1, b_2, \ldots, b_u$ be u nonnegative integers. Then,

$$L\left(p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u}\right) = \prod_{i=1}^{u} \left(L\left(p_i\right)\right)^{b_i}.$$

Proof of Lemma 10.80.7. Lemma 10.80.5 (applied to $k = u$ and $a_i = p_i^{b_i}$) yields

$$L\left(p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u}\right) = L\left(p_1^{b_1}\right) \cdot L\left(p_2^{b_2}\right) \cdot \cdots \cdot L\left(p_u^{b_u}\right) = \prod_{i=1}^{u} \underbrace{L\left(p_i^{b_i}\right)}_{\substack{=(L(p_i))^{b_i} \\ \text{(by Lemma 10.80.6,} \\ \text{applied to } a=p_i \\ \text{and } k=b_i\text{)}}} = \prod_{i=1}^{u} \left(L\left(p_i\right)\right)^{b_i}.$$

This proves Lemma 10.80.7. □

Lemma 10.80.8. Let n be a positive integer. Define z as in Exercise 2.18.2. Then,

$$z = \sum_{d \mid n} L\left(d\right).$$

Proof of Lemma 10.80.8. For each integer d, we have the logical equivalence

$$\left(d \equiv 1 \bmod 4\right) \iff \left(d\%4 = 1\right). \tag{452}$$

[*Proof of (452):* Let d be an integer. Exercise 2.6.1 (applied to 4, d and 1 instead of n, u and v) shows that we have $d \equiv 1 \bmod 4$ if and only if $d\%4 = 1\%4$. Thus, we have the following chain of equivalences:

$$\left(d \equiv 1 \bmod 4\right) \iff \left(d\%4 = \underbrace{1\%4}_{=1}\right) \iff \left(d\%4 = 1\right).$$

This proves (452).]

Now, for each positive divisor d of n, the condition "$d \equiv 1 \mod 4$" is equivalent to "$d\%4 = 1$" (by (452)). Hence, the positive divisors d of n such that $d \equiv 1 \mod 4$ are exactly the positive divisors d of n such that $d\%4 = 1$. Thus,

$$\begin{aligned} & \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4\right) \\ & = \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d\%4 = 1\right). \end{aligned} \tag{453}$$

The same argument (but with every appearance of "1" replaced by "3") yields

$$\begin{aligned} & \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4\right) \\ & = \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d\%4 = 3\right). \end{aligned} \tag{454}$$

Furthermore, if d is an integer satisfying $d\%4 = 1$, then

$$\begin{aligned} L(d) &= \begin{cases} 1, & \text{if } d\%4 = 1; \\ -1, & \text{if } d\%4 = 3; \\ 0, & \text{otherwise} \end{cases} \qquad (\text{by the definition of } L(d)) \\ &= 1 \qquad (\text{since } d\%4 = 1). \end{aligned}$$

Summing up this equality over all positive divisors d of n satisfying $d\%4 = 1$, we obtain

$$\begin{aligned} \sum_{\substack{d \mid n; \\ d\%4=1}} L(d) = \sum_{\substack{d \mid n; \\ d\%4=1}} 1 &= (\text{the number of positive divisors } d \text{ of } n \text{ such that } d\%4 = 1) \cdot 1 \\ &= (\text{the number of positive divisors } d \text{ of } n \text{ such that } d\%4 = 1) \\ &= (\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4) \end{aligned}$$

(by (453)).

Also, if d is an integer satisfying $d\%4 = 3$, then

$$\begin{aligned} L(d) &= \begin{cases} 1, & \text{if } d\%4 = 1; \\ -1, & \text{if } d\%4 = 3; \\ 0, & \text{otherwise} \end{cases} \qquad (\text{by the definition of } L(d)) \\ &= -1 \qquad (\text{since } d\%4 = 3). \end{aligned}$$

Summing up this equality over all positive divisors d of n satisfying $d\%4 = 3$, we obtain

$$\begin{aligned} \sum_{\substack{d \mid n; \\ d\%4=3}} L(d) = \sum_{\substack{d \mid n; \\ d\%4=3}} (-1) & \\ &= (\text{the number of positive divisors } d \text{ of } n \text{ such that } d\%4 = 3) \cdot (-1) \\ &= -(\text{the number of positive divisors } d \text{ of } n \text{ such that } d\%4 = 3) \\ &= -(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4) \end{aligned}$$

(by (454)).

Furthermore, if d is an integer satisfying (neither $d\%4 = 1$ nor $d\%4 = 3$), then

$$\begin{aligned} L(d) &= \begin{cases} 1, & \text{if } d\%4 = 1; \\ -1, & \text{if } d\%4 = 3; \\ 0, & \text{otherwise} \end{cases} \qquad (\text{by the definition of } L(d)) \\ &= 0 \qquad (\text{since we have neither } d\%4 = 1 \text{ nor } d\%4 = 3). \end{aligned}$$

Summing up this equality over all positive divisors d of n satisfying (neither $d\%4 = 1$ nor $d\%4 = 3$), we obtain

$$\sum_{\substack{d \mid n; \\ \text{neither } d\%4=1 \text{ nor } d\%4=3}} L(d) = \sum_{\substack{d \mid n; \\ \text{neither } d\%4=1 \text{ nor } d\%4=3}} 0 = 0.$$

Recall that the summation sign "$\sum\limits_{d \mid n}$" stands for a sum over all positive divisors of n. Each positive divisor d of n satisfies either $d\%4 = 1$ or $d\%4 = 3$ or (neither $d\%4 = 1$ nor $d\%4 = 3$)

(and these three options are mutually exclusive). Hence, we can split the sum $\sum\limits_{d\mid n} L\left(d\right)$ as follows:

$$\begin{aligned}
&\sum_{d\mid n} L\left(d\right) \\
&= \underbrace{\sum_{\substack{d\mid n;\\ d\%4=1}} L\left(d\right)}_{=(\text{the number of positive divisors } d \text{ of } n \text{ such that } d\equiv 1 \mod 4)} \\
&\qquad + \underbrace{\sum_{\substack{d\mid n;\\ d\%4=3}} L\left(d\right)}_{=-(\text{the number of positive divisors } d \text{ of } n \text{ such that } d\equiv 3 \mod 4)} \\
&\qquad + \underbrace{\sum_{\substack{d\mid n;\\ \text{neither } d\%4=1 \text{ nor } d\%4=3}} L\left(d\right)}_{=0} \\
&= \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d\equiv 1 \mod 4\right) \\
&\qquad + \left(-\left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d\equiv 3 \mod 4\right)\right) \\
&= \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d\equiv 1 \mod 4\right) \\
&\qquad - \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d\equiv 3 \mod 4\right) \\
&= z
\end{aligned}$$

(by the definition of z). This proves Lemma 10.80.8. □

Next, we define a further notation:

Definition 10.80.9. Throughout this section, we shall use the following notation: For each $p \in \mathbb{Z}$ and $m \in \mathbb{N}$, we set

$$S\left(p, m\right) = \sum_{k=0}^{m} \left(L\left(p\right)\right)^{k}.$$

Lemma 10.80.10. Let p be an integer. Let $m \in \mathbb{N}$.

(a) If $p\%4 = 1$, then $S\left(p, m\right) = m + 1$.

(b) If m is even and $p\%4 = 3$, then $S\left(p, m\right) = 1$.

(c) If m is odd and $p\%4 = 3$, then $S\left(p, m\right) = 0$.

(d) If we have neither $p\%4 = 1$ nor $p\%4 = 3$, then $S\left(p, m\right) = 1$.

Proof of Lemma 10.80.10. **(a)** Assume that $p\%4 = 1$. The definition of $L\left(p\right)$ yields

$$L\left(p\right) = \begin{cases} 1, & \text{if } p\%4 = 1; \\ -1, & \text{if } p\%4 = 3; \\ 0, & \text{otherwise} \end{cases} = 1 \qquad \left(\text{since } p\%4 = 1\right).$$

Hence, the definition of $S\left(p,m\right)$ yields

$$S\left(p,m\right)=\sum_{k=0}^{m}\left(\underbrace{L\left(p\right)}_{=1}\right)^{k}=\sum_{k=0}^{m}\underbrace{1^{k}}_{=1}=\sum_{k=0}^{m}1=\left(m+1\right)\cdot 1=m+1.$$

This proves Lemma 10.80.10 **(a)**.

(b) Assume that m is even and $p\%4=3$. Note that $m+1$ is odd (since m is even). The definition of $L\left(p\right)$ yields

$$L\left(p\right)=\begin{cases}1, & \text{if } p\%4=1;\\ -1, & \text{if } p\%4=3;\\ 0, & \text{otherwise}\end{cases}=-1 \qquad \left(\text{since } p\%4=3\right).$$

Hence, the definition of $S\left(p,m\right)$ yields

$$\begin{aligned}S\left(p,m\right)&=\sum_{k=0}^{m}\left(\underbrace{L\left(p\right)}_{=-1}\right)^{k}=\sum_{k=0}^{m}\left(-1\right)^{k}\\&=\left(-1\right)^{0}+\left(-1\right)^{1}+\cdots+\left(-1\right)^{m}\\&=\underbrace{1+\left(-1\right)+1+\left(-1\right)+\cdots+1+\left(-1\right)+1}_{m+1\text{ many addends, alternating between 1 and }-1}\qquad\left(\text{since } m+1 \text{ is odd}\right)\\&=1\end{aligned}$$

(since $m+1$ is odd). This proves Lemma 10.80.10 **(b)**.

(c) Assume that m is odd and $p\%4=3$. Note that $m+1$ is even (since m is odd). Just as in the proof of Lemma 10.80.10 **(b)** above, we can see that $L\left(p\right)=-1$ and $S\left(p,m\right)=\left(-1\right)^{0}+\left(-1\right)^{1}+\cdots+\left(-1\right)^{m}$. Hence,

$$\begin{aligned}S\left(p,m\right)&=\left(-1\right)^{0}+\left(-1\right)^{1}+\cdots+\left(-1\right)^{m}\\&=\underbrace{1+\left(-1\right)+1+\left(-1\right)+\cdots+1+\left(-1\right)}_{m+1\text{ many addends, alternating between 1 and }-1}\qquad\left(\text{since } m+1 \text{ is even}\right)\\&=0\end{aligned}$$

(since $m+1$ is even). This proves Lemma 10.80.10 **(c)**.

(d) Assume that we have neither $p\%4=1$ nor $p\%4=3$. The definition of $L\left(p\right)$ yields

$$L\left(p\right)=\begin{cases}1, & \text{if } p\%4=1;\\ -1, & \text{if } p\%4=3;\\ 0, & \text{otherwise}\end{cases}=0 \qquad \left(\text{since we have neither } p\%4=1 \text{ nor } p\%4=3\right).$$

Hence, the definition of $S(p,m)$ yields

$$\begin{aligned} S(p,m) &= \sum_{k=0}^{m} \Bigg(\underbrace{L(p)}_{=0}\Bigg)^k = \sum_{k=0}^{m} 0^k = \underbrace{0^0}_{=1} + \sum_{k=1}^{m} \underbrace{0^k}_{\substack{=0 \\ (\text{since } k\geq 1)}} \\ &\qquad \text{(here, we have split off the addend for } k=0 \text{ from the sum)} \\ &= 1 + \underbrace{\sum_{k=1}^{m} 0}_{=0} = 1. \end{aligned}$$

This proves Lemma 10.80.10 **(d)**. □

Solution to Exercise 2.18.2. For every prime $p > |n|$, we have $v_p(n) = 0$ (by Lemma 2.13.32 **(a)**). Thus, all but finitely many primes p satisfy $v_p(n) = 0$ (since all but finitely many primes p satisfy $p > |n|$). In other words, the set of all primes p satisfying $v_p(n) \neq 0$ is finite. Let P be this set. Thus, P is finite.

Let $(p_1, p_2, \ldots, p_u)$ be a list of elements of P, with no repetitions.[294] Thus, $\{p_1, p_2, \ldots, p_u\} = P$. Now, the elements $p_1, p_2, \ldots, p_u$ belong to $\{p_1, p_2, \ldots, p_u\} = P$, and thus are primes (since P is a set of primes). Furthermore, the elements $p_1, p_2, \ldots, p_u$ are distinct (since $(p_1, p_2, \ldots, p_u)$ was defined to be a list with no repetitions).

For each $i \in \{1, 2, \ldots, u\}$, define a nonnegative integer a_i by

$$a_i = v_{p_i}(n). \qquad (455)$$

This is well-defined, since p_i is a prime (because $p_1, p_2, \ldots, p_u$ are primes) and since n is nonzero.

The following facts have been proven in the proof of Proposition 2.18.1:

- The map $\{1, 2, \ldots, u\} \to \{p_1, p_2, \ldots, p_u\}$, $i \mapsto p_i$ is a bijection.
- If p is a prime such that $p \notin \{p_1, p_2, \ldots, p_u\}$, then
$$v_p(n) = 0. \qquad (456)$$
- We have $n = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}$.

Define a set T as in Lemma 2.18.3. Then, Lemma 2.18.3 says that the map

$$\begin{aligned} \Lambda : T &\to \{\text{positive divisors of } n\}, \\ (b_1, b_2, \ldots, b_u) &\mapsto p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u} \end{aligned}$$

is well-defined and bijective. Thus, this map Λ is a bijection.

[294] Such a list exists, since P is finite.

Now, the summation sign "$\sum\limits_{d\mid n}$" stands for a sum over all positive divisors of n, and thus is equivalent to the summation sign "$\sum\limits_{d\in\{\text{positive divisors of } n\}}$". Hence,

$$\begin{aligned}
\sum_{d\mid n} L(d) &= \sum_{d\in\{\text{positive divisors of } n\}} L(d) = \sum_{(b_1,b_2,\ldots,b_u)\in T} L\left(\underbrace{\Lambda(b_1,b_2,\ldots,b_u)}_{\substack{=p_1^{b_1}p_2^{b_2}\cdots p_u^{b_u} \\ \text{(by the definition of } \Lambda)}}\right) \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } \Lambda(b_1,b_2,\ldots,b_u) \text{ for } d \text{ in the} \\ \text{sum, since the map } \Lambda : T \to \{\text{positive divisors of } n\} \\ \text{is a bijection}\end{array}\right) \\
&= \sum_{(b_1,b_2,\ldots,b_u)\in T} \underbrace{L\left(p_1^{b_1}p_2^{b_2}\cdots p_u^{b_u}\right)}_{\substack{=\prod\limits_{i=1}^{u}(L(p_i))^{b_i} \\ \text{(by Lemma 10.80.7)}}} \\
&= \sum_{(b_1,b_2,\ldots,b_u)\in T} \prod_{i=1}^{u} (L(p_i))^{b_i}. \qquad (457)
\end{aligned}$$

Now, Lemma 2.18.6 (applied to u, $\{0,1,\ldots,a_i\}$ and $(L(p_i))^k$ instead of n, Z_i and $p_{i,k}$) yields

$$\begin{aligned}
\prod_{i=1}^{u} \sum_{k\in\{0,1,\ldots,a_i\}} (L(p_i))^k &= \sum_{(k_1,k_2,\ldots,k_u)\in\{0,1,\ldots,a_1\}\times\{0,1,\ldots,a_2\}\times\cdots\times\{0,1,\ldots,a_u\}} \prod_{i=1}^{u} (L(p_i))^{k_i} \\
&= \sum_{(b_1,b_2,\ldots,b_u)\in\{0,1,\ldots,a_1\}\times\{0,1,\ldots,a_2\}\times\cdots\times\{0,1,\ldots,a_u\}} \prod_{i=1}^{u} (L(p_i))^{b_i} \\
&\qquad \left(\begin{array}{c}\text{here, we have renamed the summation} \\ \text{index } (k_1,k_2,\ldots,k_u) \text{ as } (b_1,b_2,\ldots,b_u)\end{array}\right) \\
&= \sum_{(b_1,b_2,\ldots,b_u)\in T} \prod_{i=1}^{u} (L(p_i))^{b_i}
\end{aligned}$$

(since $\{0,1,\ldots,a_1\}\times\{0,1,\ldots,a_2\}\times\cdots\times\{0,1,\ldots,a_u\} = T$). Comparing this with (457), we find

$$\sum_{d\mid n} L(d) = \prod_{i=1}^{u} \underbrace{\sum_{k\in\{0,1,\ldots,a_i\}}}_{=\sum\limits_{k=0}^{a_i}} (L(p_i))^k = \prod_{i=1}^{u}\sum_{k=0}^{a_i} (L(p_i))^k. \qquad (458)$$

But Lemma 10.80.8 yields

$$z = \sum_{d\mid n} L(d) = \prod_{i=1}^{u}\sum_{k=0}^{a_i} (L(p_i))^k \qquad (459)$$

(by (458)).

On the other hand, if p is a prime such that $p \notin \{p_1, p_2, \ldots, p_u\}$, then

$$\begin{aligned} S\left(p, \underbrace{v_p(n)}_{\substack{=0\\ \text{(by (456))}}}\right) &= S(p,0) = \sum_{k=0}^{0} (L(p))^k \qquad \text{(by the definition of } S(p,0)\text{)} \\ &= (L(p))^0 = 1. \qquad (460) \end{aligned}$$

Thus, all but finitely many primes p satisfy $S(p, v_p(n)) = 1$ (since all but finitely many primes p satisfy $p \notin \{p_1, p_2, \ldots, p_u\}$). In other words, all but finitely many factors of the product $\prod_{p \text{ prime}} S(p, v_p(n))$ are 1. Thus, this product is well-defined. Moreover, we can split this product as follows:

$$\begin{aligned} &\prod_{p \text{ prime}} S(p, v_p(n)) \\ &= \left(\prod_{\substack{p \text{ prime};\\ p \in \{p_1,p_2,\ldots,p_u\}}} S(p, v_p(n))\right) \left(\prod_{\substack{p \text{ prime};\\ p \notin \{p_1,p_2,\ldots,p_u\}}} \underbrace{S(p, v_p(n))}_{\substack{=1\\ \text{(by (460))}}}\right) \\ &\qquad \left(\begin{array}{c}\text{since each prime } p \text{ satisfies either } p \in \{p_1,p_2,\ldots,p_u\} \\ \text{or } p \notin \{p_1,p_2,\ldots,p_u\} \text{ (but not both simultaneously)}\end{array}\right) \\ &= \left(\prod_{\substack{p \text{ prime};\\ p \in \{p_1,p_2,\ldots,p_u\}}} S(p, v_p(n))\right) \underbrace{\left(\prod_{\substack{p \text{ prime};\\ p \notin \{p_1,p_2,\ldots,p_u\}}} 1\right)}_{=1} \\ &= \underbrace{\prod_{\substack{p \text{ prime};\\ p \in \{p_1,p_2,\ldots,p_u\}}}}_{\substack{=\prod_{p \in \{p_1,p_2,\ldots,p_u\}}\\ \text{(since each } p \in \{p_1,p_2,\ldots,p_u\}\\ \text{is a prime)}}} S(p, v_p(n)) \\ &= \prod_{p \in \{p_1,p_2,\ldots,p_u\}} S(p, v_p(n)) = \prod_{i=1}^{u} S\left(p_i, \underbrace{v_{p_i}(n)}_{\substack{=a_i\\ \text{(by (455))}}}\right) \\ &\qquad \left(\begin{array}{c}\text{here, we have substituted } p_i \text{ for } p \text{ in the product,} \\ \text{since the map } \{1,2,\ldots,u\} \to \{p_1,p_2,\ldots,p_u\},\ i \mapsto p_i \text{ is a bijection}\end{array}\right) \\ &= \prod_{i=1}^{u} \underbrace{S(p_i, a_i)}_{\substack{=\sum_{k=0}^{a_i} (L(p_i))^k\\ \text{(by the definition of } S(p_i,a_i))}} = \prod_{i=1}^{u} \sum_{k=0}^{a_i} (L(p_i))^k . \end{aligned}$$

Comparing this with (459), we obtain

$$z = \prod_{p \text{ prime}} S\left(p, v_p\left(n\right)\right). \tag{461}$$

(a) Assume that there exists a prime p satisfying $p \equiv 3 \mod 4$ and $v_p\left(n\right) \equiv 1 \mod 2$. Consider this p, and denote it by q. Thus, q is a prime satisfying $q \equiv 3 \mod 4$ and $v_q\left(n\right) \equiv 1 \mod 2$.

Exercise 2.6.1 (applied to 4, q and 3 instead of n, u and v) shows that we have $q \equiv 3 \mod 4$ if and only if $q\%4 = 3\%4$. Hence, from $q \equiv 3 \mod 4$, we conclude that $q\%4 = 3\%4 = 3$. From $v_q\left(n\right) \equiv 1 \mod 2$, we conclude that $v_q\left(n\right)$ is odd. Hence, Lemma 10.80.10 **(c)** (applied to q and $v_q\left(n\right)$ instead of p and m) yields $S\left(q, v_q\left(n\right)\right) = 0$.

But q is a prime. Thus, $S\left(q, v_q\left(n\right)\right)$ is a factor in the product $\prod_{p \text{ prime}} S\left(p, v_p\left(n\right)\right)$. Splitting this factor off, we find

$$\prod_{p \text{ prime}} S\left(p, v_p\left(n\right)\right) = \underbrace{S\left(q, v_q\left(n\right)\right)}_{=0} \cdot \prod_{\substack{p \text{ prime;} \\ p \neq q}} S\left(p, v_p\left(n\right)\right) = 0.$$

Now, (461) becomes $z = \prod_{p \text{ prime}} S\left(p, v_p\left(n\right)\right) = 0$. This solves Exercise 2.18.2 **(a)**.

(b) Assume that there exists no prime p satisfying $p \equiv 3 \mod 4$ and $v_p\left(n\right) \equiv 1 \mod 2$. Renaming p as q in this statement, we obtain the following:

$$\text{There exists no prime } q \text{ satisfying } q \equiv 3 \mod 4 \text{ and } v_q\left(n\right) \equiv 1 \mod 2. \tag{462}$$

We can now easily see the following two auxiliary claims:

Claim 1: Let p be a prime such that $p\%4 \neq 1$. Then, $S\left(p, v_p\left(n\right)\right) = 1$.

[*Proof of Claim 1:* We are in one of the following two cases:

Case 1: We have $p\%4 = 3$.

Case 2: We have $p\%4 \neq 3$.

Let us first consider Case 1. In this case, we have $p\%4 = 3$. Comparing this with $3\%4 = 3$, we obtain $p\%4 = 3\%4$. But Exercise 2.6.1 (applied to 4, p and 3 instead of n, u and v) shows that we have $p \equiv 3 \mod 4$ if and only if $p\%4 = 3\%4$. Hence, from $p\%4 = 3\%4$, we conclude that $p \equiv 3 \mod 4$. If we had $v_p\left(n\right) \equiv 1 \mod 2$, then there would be a prime q satisfying $q \equiv 3 \mod 4$ and $v_q\left(n\right) \equiv 1 \mod 2$ (namely, $q = p$); but this would contradict (462). Hence, we cannot have $v_p\left(n\right) \equiv 1 \mod 2$. In other words, the integer $v_p\left(n\right)$ cannot be odd. Hence, the integer $v_p\left(n\right)$ is even. Thus, Lemma 10.80.10 **(b)** (applied to $m = v_p\left(n\right)$) yields $S\left(p, v_p\left(n\right)\right) = 1$. Hence, Claim 1 is proven in Case 1.

Let us now consider Case 2. In this case, we have $p\%4 \neq 3$. Now, we have neither $p\%4 = 1$ nor $p\%4 = 3$ (since we have $p\%4 \neq 1$ and $p\%4 \neq 3$). Hence, Lemma 10.80.10 **(d)** (applied to $m = v_p\left(n\right)$) yields $S\left(p, v_p\left(n\right)\right) = 1$. Hence, Claim 1 is proven in Case 2.

We have now proven Claim 1 in each of the Cases 1 and 2. Hence, Claim 1 always holds.]

Claim 2: For each integer p, we have the logical equivalence

$$\left(p \equiv 1 \mod 4\right) \iff \left(p\%4 = 1\right).$$

[*Proof of Claim 2:* Claim 2 is precisely the equivalence (452) (with d renamed as p).]

Claim 2 shows that for each prime p, the condition "$p \equiv 1 \mod 4$" is equivalent to the condition "$p\%4 = 1$". Hence, the product sign "$\prod\limits_{\substack{p \text{ prime;} \\ p \equiv 1 \mod 4}}$" is equivalent to "$\prod\limits_{\substack{p \text{ prime;} \\ p\%4=1}}$". Thus,

$$\prod_{\substack{p \text{ prime;} \\ p \equiv 1 \mod 4}} \left(v_p\left(n\right)+1\right) = \prod_{\substack{p \text{ prime;} \\ p\%4=1}} \left(v_p\left(n\right)+1\right). \tag{463}$$

Now, (461) becomes

$$z = \prod_{p \text{ prime}} S\left(p, v_p\left(n\right)\right) = \left(\prod_{\substack{p \text{ prime;} \\ p\%4=1}} \underbrace{S\left(p, v_p\left(n\right)\right)}_{\substack{=v_p(n)+1 \\ \text{(by Lemma 10.80.10 (a)} \\ \text{(applied to } m=v_p(n)))}}\right) \cdot \left(\prod_{\substack{p \text{ prime;} \\ p\%4\neq 1}} \underbrace{S\left(p, v_p\left(n\right)\right)}_{\substack{=1 \\ \text{(by Claim 1)}}}\right)$$

$$\text{(since each prime } p \text{ satisfies either } p\%4 = 1 \text{ or } p\%4 \neq 1 \text{ (but not both))}$$

$$= \left(\prod_{\substack{p \text{ prime;} \\ p\%4=1}} \left(v_p\left(n\right)+1\right)\right) \cdot \underbrace{\left(\prod_{\substack{p \text{ prime;} \\ p\%4\neq 1}} 1\right)}_{=1} = \prod_{\substack{p \text{ prime;} \\ p\%4=1}} \left(v_p\left(n\right)+1\right) = \prod_{\substack{p \text{ prime;} \\ p \equiv 1 \mod 4}} \left(v_p\left(n\right)+1\right)$$

(by (463)). This solves Exercise 2.18.2 **(b)**. □

Remark 10.80.11. Exercise 2.18.2 can be slightly generalized: Let $N \in \{3, 4, 6\}$. Let n be a positive integer. Let

$$z = \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod N\right) \\ - \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv N-1 \mod N\right).$$

Then:

(a) If there exists a prime p satisfying $p \equiv N - 1 \mod N$ and $v_p\left(n\right) \equiv 1 \mod 2$, then $z = 0$.

(b) If there exists no prime p satisfying $p \equiv N - 1 \mod N$ and $v_p\left(n\right) \equiv 1 \mod 2$, then

$$z = \prod_{\substack{p \text{ prime;} \\ p \equiv 1 \mod N}} \left(v_p\left(n\right)+1\right).$$

The solution of Exercise 2.18.2 that we gave above can still be used to prove these two more general claims, once the obvious changes are made (which consist mostly in replacing "3" and "4" by "$N - 1$" and "N", respectively, and adding a few straightforward cases in the proof of Lemma 10.80.2).

Note that the numbers $3, 4, 6$ are precisely the positive integers m satisfying $\phi\left(m\right) = 2$. This is directly connected to the fact that they are the integers N for which these two statements hold. Indeed, Lemma 10.80.2 (modified to use N instead of 4) quickly boils down to the observation that the only elements $i \in \{0, 1, \ldots, N-1\}$ coprime to N are the two elements 1 and $N - 1$ and these two elements are distinct; but this is equivalent to $\phi\left(N\right) = 2$.

10.81. Solution to Exercise 2.19.1

Exercise 2.19.1 demands that we prove Lemma 2.19.3; let us do this:

Proof of Lemma 2.19.3. Lemma 2.18.6 (applied to $Z_i = S$ and $p_{i,k} = a_k$) yields

$$\prod_{i=1}^{n} \sum_{k \in S} a_k = \sum_{(k_1,k_2,\ldots,k_n) \in S \times S \times \cdots \times S} \prod_{i=1}^{n} a_{k_i},$$

where the Cartesian product $S \times S \times \cdots \times S$ has n factors. Since this Cartesian product $S \times S \times \cdots \times S$ is simply S^n, we can rewrite this equality as follows:

$$\prod_{i=1}^{n} \sum_{k \in S} a_k = \sum_{(k_1,k_2,\ldots,k_n) \in S^n} \prod_{i=1}^{n} a_{k_i}.$$

Comparing this with

$$\prod_{i=1}^{n} \underbrace{\sum_{k \in S} a_k}_{=\sum_{s \in S} a_s} = \prod_{i=1}^{n} \sum_{s \in S} a_s = \left(\sum_{s \in S} a_s \right)^n ,$$

we obtain

$$\left(\sum_{s \in S} a_s \right)^n = \sum_{(k_1,k_2,\ldots,k_n) \in S^n} \prod_{i=1}^{n} a_{k_i}.$$

This proves Lemma 2.19.3. □

10.82. Solution to Exercise 2.19.2

Exercise 2.19.2 asks us to prove Lemma 2.19.5 formally. Before we do so, let us restate Lemma 2.19.4 in a more flexible form:

> **Lemma 10.82.1.** Let p be a prime. Let U be a set such that $|U| \geq 2p-1$. For each $s \in U$, let a_s be an integer. Then, there exists a p-element subset T of U such that $p \mid \sum_{s \in T} a_s$.

Proof of Lemma 10.82.1. There exist $2p-1$ distinct elements $u_1, u_2, \ldots, u_{2p-1}$ of U (since $|U| \geq 2p-1$). Choose such $2p-1$ elements. For each $s \in \{1, 2, \ldots, 2p-1\}$, we define an integer b_s by $b_s = a_{u_s}$. Thus, $b_1, b_2, \ldots, b_{2p-1}$ are $2p-1$ integers. Hence, Lemma 2.19.4 (applied to b_i instead of a_i) shows that there exists a p-element subset S of $\{1, 2, \ldots, 2p-1\}$ such that $p \mid \sum_{s \in S} b_s$. Consider this S.

Let Z be the subset $\{u_s \mid s \in S\}$ of U. Thus, $u_s \in Z$ for each $s \in S$. Hence, we can define a map

$$f : S \to Z,$$
$$s \mapsto u_s.$$

This map f is injective[295] and surjective[296]. Hence, the map f is bijective, i.e., is a bijection from S to Z. Thus, we can substitute $f(s)$ for s in the sum $\sum_{s\in Z} a_s$. We thus obtain

$$\sum_{s\in Z} a_s = \sum_{s\in S} \underbrace{a_{f(s)}}_{\substack{=a_{u_s} \\ \text{(since } f(s)=u_s \\ \text{(by the definition of } f))}} = \sum_{s\in S} \underbrace{a_{u_s}}_{\substack{=b_s \\ \text{(by the definition of } b_s)}} = \sum_{s\in S} b_s .$$

Hence, $p \mid \sum_{s\in Z} a_s$ (since $p \mid \sum_{s\in S} b_s$). Moreover, there is a bijection from S to Z (namely, f). Hence, $|Z| = |S| = p$ (since S is a p-element set). Thus, Z is a p-element set.

This p-element set Z is a subset of U and satisfies $p \mid \sum_{s\in Z} a_s$ (as we have seen). Thus, there exists a p-element subset T of U such that $p \mid \sum_{s\in T} a_s$ (namely, $T = Z$). This proves Lemma 10.82.1. □

Now we can prove Lemma 2.19.5:

Proof of Lemma 2.19.5. We shall prove Lemma 2.19.5 by induction on u:

Induction base: Lemma 2.19.5 holds for $u = 1$ [297]. This completes the induction base.

Induction step: Let k be a positive integer. Assume that Lemma 2.19.5 holds for $u = k$. We must prove that Lemma 2.19.5 holds for $u = k+1$.

We have assumed that Lemma 2.19.5 holds for $u = k$. In other words, the following claim holds:

> *Claim 1:* Let p be a prime. Let $a_1, a_2, \ldots, a_{kp-1}$ be any $kp-1$ integers (not necessarily distinct). Then, there exist $k-1$ disjoint p-element subsets $S_1, S_2, \ldots, S_{k-1}$ of $\{1, 2, \ldots, kp-1\}$ such that
>
> $$p \mid \sum_{s\in S_i} a_s \qquad \text{for all } i \in \{1, 2, \ldots, k-1\} .$$

[295] *Proof.* Let i and j be two elements of S such that $f(i) = f(j)$. We shall show that $i = j$.

We have $f(i) = u_i$ (by the definition of f) and $f(j) = u_j$ (likewise). Hence, $u_i = f(i) = f(j) = u_j$. Therefore, $i = j$ (since the elements $u_1, u_2, \ldots, u_{2p-1}$ are distinct).

Now, forget that we fixed i and j. We thus have shown that if i and j are two elements of S such that $f(i) = f(j)$, then $i = j$. In other words, the map f is injective.

[296] *Proof.* Let $z \in Z$. Hence, $z \in Z = \{u_s \mid s \in S\}$. In other words, $z = u_s$ for some $s \in S$. Consider this s. The definition of f yields $f(s) = u_s = z$. Hence, $z = f(s) \in f(S)$ (since $s \in S$).

Now, forget that we fixed z. We thus have shown that $z \in f(S)$ for each $z \in Z$. In other words, $Z \subseteq f(S)$. In other words, the map f is surjective.

[297] *Proof.* Assume that $u = 1$. Thus, $u - 1 = 0$, so that $\{1, 2, \ldots, u-1\} = \varnothing$. But Lemma 2.19.5 claims the existence of $u-1$ disjoint p-element subsets $S_1, S_2, \ldots, S_{u-1}$ of $\{1, 2, \ldots, up-1\}$ such that

$$p \mid \sum_{s\in S_i} a_s \qquad \text{for all } i \in \{1, 2, \ldots, u-1\} . \tag{464}$$

Obviously, we can find $u-1$ disjoint p-element subsets $S_1, S_2, \ldots, S_{u-1}$ of $\{1, 2, \ldots, up-1\}$ (because $u-1 = 0$, so that we don't have to find anything at all), and they will automatically satisfy (464) (indeed, $\{1, 2, \ldots, u-1\} = \varnothing$, so that (464) is vacuously true). Thus, the claim of Lemma 2.19.5 holds.

Thus, we have proven Lemma 2.19.5 for $u = 1$.

We must prove that Lemma 2.19.5 holds for $u = k+1$. In other words, we must prove the following claim:

> *Claim 2:* Let p be a prime. Let $a_1, a_2, \ldots, a_{(k+1)p-1}$ be any $(k+1)p-1$ integers (not necessarily distinct). Then, there exist k disjoint p-element subsets $S_1, S_2, \ldots, S_k$ of $\{1, 2, \ldots, (k+1)p-1\}$ such that
>
> $$p \mid \sum_{s \in S_i} a_s \qquad \text{for all } i \in \{1, 2, \ldots, k\}.$$

[*Proof of Claim 2:* We have $\underbrace{k}_{\leq k+1} p - 1 \leq (k+1)p - 1$ and thus $\{1, 2, \ldots, kp-1\} \subseteq \{1, 2, \ldots, (k+1)p-1\}$.

Consider the first $kp-1$ of our $(k+1)p-1$ integers $a_1, a_2, \ldots, a_{(k+1)p-1}$. Thus, Claim 1 shows that there exist $k-1$ disjoint p-element subsets $S_1, S_2, \ldots, S_{k-1}$ of $\{1, 2, \ldots, kp-1\}$ such that

$$p \mid \sum_{s \in S_i} a_s \qquad \text{for all } i \in \{1, 2, \ldots, k-1\}. \tag{465}$$

Consider these $S_1, S_2, \ldots, S_{k-1}$. These $k-1$ sets $S_1, S_2, \ldots, S_{k-1}$ are subsets of $\{1, 2, \ldots, kp-1\}$ and thus also subsets of $\{1, 2, \ldots, (k+1)p-1\}$ [298]. Moreover, these $k-1$ sets are disjoint; thus, the size of their union is the sum of their sizes. In other words,

$$|S_1 \cup S_2 \cup \cdots \cup S_{k-1}| = |S_1| + |S_2| + \cdots + |S_{k-1}| = \sum_{i=1}^{k-1} \underbrace{|S_i|}_{\substack{=p \\ \text{(since } S_i \text{ is} \\ \text{a } p\text{-element set)}}} = \sum_{i=1}^{k-1} p = (k-1)p.$$

Define a subset U of $\{1, 2, \ldots, (k+1)p-1\}$ by

$$U = \{1, 2, \ldots, (k+1)p-1\} \setminus (S_1 \cup S_2 \cup \cdots \cup S_{k-1}).$$

Then,

$$\begin{aligned}
|U| &= |\{1, 2, \ldots, (k+1)p-1\} \setminus (S_1 \cup S_2 \cup \cdots \cup S_{k-1})| \\
&= \underbrace{|\{1, 2, \ldots, (k+1)p-1\}|}_{=(k+1)p-1} - \underbrace{|S_1 \cup S_2 \cup \cdots \cup S_{k-1}|}_{=(k-1)p} \\
&\qquad \left(\begin{array}{c} \text{since } S_1 \cup S_2 \cup \cdots \cup S_{k-1} \text{ is a subset of } \{1, 2, \ldots, (k+1)p-1\} \\ \text{(because } S_1, S_2, \ldots, S_{k-1} \text{ are subsets of } \{1, 2, \ldots, (k+1)p-1\}\text{)} \end{array} \right) \\
&= (k+1)p - 1 - (k-1)p = 2p - 1.
\end{aligned}$$

Hence, Lemma 10.82.1 shows that there exists a p-element subset T of U such that $p \mid \sum_{s \in T} a_s$. Consider this T.

[298] since $\{1, 2, \ldots, kp-1\} \subseteq \{1, 2, \ldots, (k+1)p-1\}$

Extend our $(k-1)$-tuple $(S_1, S_2, \ldots, S_{k-1})$ of sets to a k-tuple $(S_1, S_2, \ldots, S_k)$ by setting $S_k = T$. Thus, $S_1, S_2, \ldots, S_k$ are p-element subsets of $\{1, 2, \ldots, (k+1)p - 1\}$ [299]. They are furthermore disjoint[300], and satisfy

$$p \mid \sum_{s \in S_i} a_s \qquad \text{for all } i \in \{1, 2, \ldots, k\} \tag{466}$$

[301]. Hence, we have constructed k disjoint p-element subsets $S_1, S_2, \ldots, S_k$ of $\{1, 2, \ldots, (k+1)p - 1\}$ such that

$$p \mid \sum_{s \in S_i} a_s \qquad \text{for all } i \in \{1, 2, \ldots, k\}.$$

Therefore, such k subsets exist. This proves Claim 2.]

We have now proven Claim 2. In other words, we have shown that Lemma 2.19.5 holds for $u = k+1$. This completes the induction step. Thus, Lemma 2.19.5 is proven by induction. □

[299] *Proof.* We only need to prove that S_k is a p-element subset of $\{1, 2, \ldots, (k+1)p - 1\}$ (since we already know that $S_1, S_2, \ldots, S_{k-1}$ are p-element subsets of $\{1, 2, \ldots, (k+1)p - 1\}$). But this is easy: We know that T is a p-element subset of U. In other words, S_k is a p-element subset of U (since $S_k = T$). Hence,

$$S_k \subseteq U = \{1, 2, \ldots, (k+1)p - 1\} \setminus (S_1 \cup S_2 \cup \cdots \cup S_{k-1}) \subseteq \{1, 2, \ldots, (k+1)p - 1\}.$$

Thus, S_k is a subset of $\{1, 2, \ldots, (k+1)p - 1\}$. Hence, S_k is a p-element subset of $\{1, 2, \ldots, (k+1)p - 1\}$, qed.

[300] *Proof.* We must prove that the k sets $S_1, S_2, \ldots, S_k$ are disjoint. Since we already know that the first $k-1$ of them are disjoint (because $S_1, S_2, \ldots, S_{k-1}$ are disjoint), we only need to check that S_k is disjoint from each of the sets $S_1, S_2, \ldots, S_{k-1}$. In other words, we only need to check that S_k is disjoint from S_i for each $i \in \{1, 2, \ldots, k-1\}$.

So let $i \in \{1, 2, \ldots, k-1\}$ be arbitrary. Then,

$$\begin{aligned} S_k &= T \subseteq U \qquad \text{(since } T \text{ is a subset of } U\text{)} \\ &= \{1, 2, \ldots, (k+1)p - 1\} \setminus \underbrace{(S_1 \cup S_2 \cup \cdots \cup S_{k-1})}_{\substack{\supseteq S_i \\ \text{(since } i \in \{1,2,\ldots,k-1\}\text{)}}} \\ &\subseteq \{1, 2, \ldots, (k+1)p - 1\} \setminus S_i. \end{aligned}$$

In other words, S_k is a subset of $\{1, 2, \ldots, (k+1)p - 1\}$ that is disjoint from S_i. In particular, S_k is disjoint from S_i.

Forget that we fixed i. We thus have shown that S_k is disjoint from S_i for each $i \in \{1, 2, \ldots, k-1\}$. As we have explained, this completes our proof.

[301] *Proof of (466):* Let $i \in \{1, 2, \ldots, k\}$. We must prove that $p \mid \sum_{s \in S_i} a_s$. If $i \in \{1, 2, \ldots, k-1\}$, then this follows from (465); thus, for the rest of this proof, we WLOG assume that $i \notin \{1, 2, \ldots, k-1\}$. Hence, $i \in \{1, 2, \ldots, k\}$ but $i \notin \{1, 2, \ldots, k-1\}$. Therefore, $i \in \{1, 2, \ldots, k\} \setminus \{1, 2, \ldots, k-1\} = \{k\}$, so that $i = k$. Thus, $S_i = S_k = T$, so that $\sum_{s \in S_i} a_s = \sum_{s \in T} a_s$. Hence, from $p \mid \sum_{s \in T} a_s$, we obtain $p \mid \sum_{s \in S_i} a_s$. This proves (466).

10.83. Solution to Exercise 3.3.1

Solution to Exercise 3.3.1. Let α and β be two equivalence classes of $\sim$. Thus, $\alpha = [x]_\sim$ and $\beta = [y]_\sim$ for two elements x and y of S (by the definition of "equivalence classes of $\sim$"). Consider these x and y.

If $x \sim y$, then the classes $[x]_\sim$ and $[y]_\sim$ are identical (by Theorem 3.3.5 **(a)**). Otherwise, they are disjoint (by Theorem 3.3.5 **(b)**). Thus, in either case, the classes $[x]_\sim$ and $[y]_\sim$ are either identical or disjoint. In view of $\alpha = [x]_\sim$ and $\beta = [y]_\sim$, this rewrites as follows: The classes α and β are either identical or disjoint.

Now, forget that we fixed α and β. We thus have shown that if α and β are two equivalence classes of $\sim$, then α and β are either identical or disjoint. This solves Exercise 3.3.1. □

10.84. Solution to Exercise 3.3.2

Solution to Exercise 3.3.2. Indeed:

- The relation $\underset{\text{perm}}{\sim}$ is reflexive.

  [*Proof:* Informally, this is obvious, because each k-tuple is a permutation of itself (just permute it by leaving all its entries in place). The formal version of this argument proceeds as follows:

  Let $\mathbf{a} \in A^k$. Write the k-tuple $\mathbf{a}$ in the form $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ for some $a_1, a_2, \ldots, a_k \in A$. Then, $\mathbf{a} = (a_1, a_2, \ldots, a_k) = \left(a_{\operatorname{id}(1)}, a_{\operatorname{id}(2)}, \ldots, a_{\operatorname{id}(k)}\right)$. Hence, the k-tuple $\mathbf{a}$ has the form $\left(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(k)}\right)$ for some permutation σ of the set $\{1, 2, \ldots, k\}$ (namely, for $\sigma = \operatorname{id}$). In other words, $\mathbf{a}$ is a permutation of the k-tuple $(a_1, a_2, \ldots, a_k)$ (by Definition 2.13.16). In other words, $\mathbf{a}$ is a permutation of the k-tuple $\mathbf{a}$ (since $\mathbf{a} = (a_1, a_2, \ldots, a_k)$). In other words, $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{a}$ (by the definition of the relation $\underset{\text{perm}}{\sim}$).

  Now, forget that we fixed $\mathbf{a}$. We thus have proven that every $\mathbf{a} \in A^k$ satisfies $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{a}$. In other words, the relation $\underset{\text{perm}}{\sim}$ is reflexive.]

- The relation $\underset{\text{perm}}{\sim}$ is symmetric.

  [*Proof:* Let $\mathbf{a}, \mathbf{b} \in A^k$ be such that $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{b}$. We shall prove that $\mathbf{b} \underset{\text{perm}}{\sim} \mathbf{a}$.

  Write the k-tuple $\mathbf{a}$ in the form $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ for some $a_1, a_2, \ldots, a_k \in A$. Write the k-tuple $\mathbf{b}$ in the form $\mathbf{b} = (b_1, b_2, \ldots, b_k)$ for some $b_1, b_2, \ldots, b_k \in A$. We have $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{b}$. In other words, $\mathbf{a}$ is a permutation of $\mathbf{b}$ (by the definition of the relation $\underset{\text{perm}}{\sim}$). In other words, $(a_1, a_2, \ldots, a_k)$ is a permutation of $(b_1, b_2, \ldots, b_k)$ (since $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_k)$). Hence, Proposition 2.13.18 (applied to $p_i = b_i$ and $q_i = a_i$) shows that $(b_1, b_2, \ldots, b_k)$ is a permutation of $(a_1, a_2, \ldots, a_k)$. In other words, $\mathbf{b}$ is a permutation of $\mathbf{a}$ (since $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_k)$). In other words, $\mathbf{b} \underset{\text{perm}}{\sim} \mathbf{a}$.

Forget that we fixed $\mathbf{a}$ and $\mathbf{b}$. We thus have shown that every $\mathbf{a}, \mathbf{b} \in A^k$ satisfying $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{b}$ satisfy $\mathbf{b} \underset{\text{perm}}{\sim} \mathbf{a}$. In other words, the relation $\underset{\text{perm}}{\sim}$ is symmetric.]

- The relation $\underset{\text{perm}}{\sim}$ is transitive.

  [*Proof:* Let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in A^k$ be such that $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{b}$ and $\mathbf{b} \underset{\text{perm}}{\sim} \mathbf{c}$. We shall prove that $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{c}$.

  Write the k-tuple $\mathbf{a}$ in the form $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ for some $a_1, a_2, \ldots, a_k \in A$. Write the k-tuple $\mathbf{b}$ in the form $\mathbf{b} = (b_1, b_2, \ldots, b_k)$ for some $b_1, b_2, \ldots, b_k \in A$. Write the k-tuple $\mathbf{c}$ in the form $\mathbf{c} = (c_1, c_2, \ldots, c_k)$ for some $c_1, c_2, \ldots, c_k \in A$.

  We have $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{b}$. In other words, $\mathbf{a}$ is a permutation of $\mathbf{b}$ (by the definition of the relation $\underset{\text{perm}}{\sim}$). In other words, $(a_1, a_2, \ldots, a_k)$ is a permutation of $(b_1, b_2, \ldots, b_k)$ (since $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_k)$). In other words, the k-tuple $(a_1, a_2, \ldots, a_k)$ has the form $\left(b_{\sigma(1)}, b_{\sigma(2)}, \ldots, b_{\sigma(k)}\right)$ for some permutation σ of the set $\{1, 2, \ldots, k\}$ (by Definition 2.13.16). Consider this σ, and denote it by λ. Thus, λ is a permutation of $\{1, 2, \ldots, k\}$ and has the property that $(a_1, a_2, \ldots, a_k) = \left(b_{\lambda(1)}, b_{\lambda(2)}, \ldots, b_{\lambda(k)}\right)$. Likewise, we can find a permutation μ of $\{1, 2, \ldots, k\}$ with the property that $(b_1, b_2, \ldots, b_k) = \left(c_{\mu(1)}, c_{\mu(2)}, \ldots, c_{\mu(k)}\right)$ (because of our assumption that $\mathbf{b} \underset{\text{perm}}{\sim} \mathbf{c}$). Consider this μ as well.

  Now μ and λ are permutations of the set $\{1, 2, \ldots, k\}$, that is, bijective maps $\{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$. Hence, their composition $\mu \circ \lambda$ is a bijective map $\{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$ as well, i.e., is a permutation of the set $\{1, 2, \ldots, k\}$.

  Recall that $(b_1, b_2, \ldots, b_k) = \left(c_{\mu(1)}, c_{\mu(2)}, \ldots, c_{\mu(k)}\right)$. In other words, each $j \in \{1, 2, \ldots, k\}$ satisfies
  $$b_j = c_{\mu(j)}. \tag{467}$$
  Also, $(a_1, a_2, \ldots, a_k) = \left(b_{\lambda(1)}, b_{\lambda(2)}, \ldots, b_{\lambda(k)}\right)$. Hence, each $i \in \{1, 2, \ldots, k\}$ satisfies
  $$\begin{aligned} a_i = b_{\lambda(i)} &= c_{\mu(\lambda(i))} \qquad \text{(by (467), applied to } j = \lambda(i)\text{)} \\ &= c_{(\mu \circ \lambda)(i)}. \end{aligned}$$
  In other words, we have $(a_1, a_2, \ldots, a_k) = \left(c_{(\mu\circ\lambda)(1)}, c_{(\mu\circ\lambda)(2)}, \ldots, c_{(\mu\circ\lambda)(k)}\right)$. Hence, the k-tuple $(a_1, a_2, \ldots, a_k)$ has the form $\left(c_{\sigma(1)}, c_{\sigma(2)}, \ldots, c_{\sigma(k)}\right)$ for some permutation σ of the set $\{1, 2, \ldots, k\}$ (namely, for $\sigma = \mu \circ \lambda$). In other words, the k-tuple $(a_1, a_2, \ldots, a_k)$ is a permutation of $(c_1, c_2, \ldots, c_k)$ (by Definition 2.13.16). In other words, $\mathbf{a}$ is a permutation of $\mathbf{c}$ (since $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{c} = (c_1, c_2, \ldots, c_k)$). In other words, $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{c}$.

  Forget that we fixed $\mathbf{a}, \mathbf{b}, \mathbf{c}$. We thus have shown that every $\mathbf{a}, \mathbf{b}, \mathbf{c} \in A^k$ satisfying $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{b}$ and $\mathbf{b} \underset{\text{perm}}{\sim} \mathbf{c}$ satisfy $\mathbf{a} \underset{\text{perm}}{\sim} \mathbf{c}$. In other words, the relation $\underset{\text{perm}}{\sim}$ is transitive.]

We now know that the relation $\underset{\text{perm}}{\sim}$ is reflexive, symmetric and transitive. In other words, $\underset{\text{perm}}{\sim}$ is an equivalence relation. This solves Exercise 3.3.2. □

10.85. Solution to Exercise 3.3.3

Solution to Exercise 3.3.3. Let T be the quotient set $S/\sim$, and let $f : S \to T$ be the canonical projection $\pi_\sim : S \to S/\sim$. We shall prove that the relation $\sim$ equals the relation $\underset{f}{\equiv}$.

Let $a \in S$ and $b \in S$. Recall that f is the map $\pi_\sim$. Thus, $f = \pi_\sim$, so that $f(a) = \pi_\sim(a) = [a]_\sim$ (by the definition of $\pi_\sim$). The same argument (applied to b instead of a) yields $f(b) = [b]_\sim$.

Theorem 3.3.5 **(e)** (applied to $x = a$ and $y = b$) shows that we have $a \sim b$ if and only if $[a]_\sim = [b]_\sim$. In other words, we have the logical equivalence

$$(a \sim b) \iff ([a]_\sim = [b]_\sim). \tag{468}$$

We have the following chain of logical equivalences:

$$\begin{aligned}\left(a \underset{f}{\equiv} b\right) &\iff \left(\underbrace{f(a)}_{=[a]_\sim} = \underbrace{f(b)}_{=[b]_\sim}\right) \qquad \left(\text{by the definition of the relation } \underset{f}{\equiv}\right)\\ &\iff ([a]_\sim = [b]_\sim) \iff (a \sim b) \qquad (\text{by (468)}).\end{aligned} \tag{469}$$

Now, forget that we fixed a and b. We thus have proven the equivalence (469) for all $a \in S$ and $b \in S$. Now, recall that we have defined a relation on the set S to be a subset of $S \times S$ (namely, the subset of all pairs $(a, b) \in S \times S$ satisfying this relation). Hence, the relation $\sim$ is actually the subset

$$\{(a, b) \in S \times S \mid a \sim b\}$$

of $S \times S$, whereas the relation $\underset{f}{\equiv}$ is actually the subset

$$\left\{(a, b) \in S \times S \mid a \underset{f}{\equiv} b\right\}$$

of $S \times S$. But these two subsets are clearly identical, because we have shown the equivalence (469) for all $a \in S$ and $b \in S$. In other words, the two relations $\sim$ and $\underset{f}{\equiv}$ are identical. In other words, the relation $\sim$ equals the relation $\underset{f}{\equiv}$. This solves Exercise 3.3.3. □

10.86. Solution to Exercise 3.4.1

Solution to Exercise 3.4.1. **(a)** Let r be a nonzero rational number. We must prove that the integer $w_p(r)$ is well-defined. Recall that we have defined $w_p(r)$ by setting $w_p(r) = v_p(a) - v_p(b)$, where we write r in the form $r = a/b$ for two nonzero integers a and b. In order to prove that $w_p(r)$ is well-defined, we must thus verify the following three claims:

> *Claim 1:* It is possible to write r in the form $r = a/b$ for two nonzero integers a and b.

> *Claim 2:* If we write r in the form $r = a/b$ for two nonzero integers a and b, then $v_p(a) - v_p(b)$ is a well-defined integer.[302]

> *Claim 3:* If we write r in the form $r = a/b$ for two nonzero integers a and b, then the integer $v_p(a) - v_p(b)$ depends only on p and r (but not on a and b).

Claim 1 and Claim 2 are easy to verify:

[*Proof of Claim 1:* We know that r is a rational number. Hence, we can write r in the form $r = c/d$ for some integer c and some nonzero integer d. Consider these c and d. If we had $c = 0$, then we would have $r = \underbrace{c}_{=0}/d = 0$; but this would contradict the fact that r is nonzero. Hence, we cannot have $c = 0$. Thus, c is nonzero. Thus, there exist two nonzero integers a and b such that $r = a/b$ (namely, $a = c$ and $b = d$). In other words, it is possible to write r in the form $r = a/b$ for two nonzero integers a and b. This proves Claim 1.]

[*Proof of Claim 2:* Assume that r is written in the form $r = a/b$ for two nonzero integers a and b. Definition 2.13.23 **(a)** shows that $v_p(n) \in \mathbb{N}$ for each nonzero integer n. Thus, $v_p(a) \in \mathbb{N}$ (since a is nonzero) and $v_p(b) \in \mathbb{N}$ (since b is nonzero). Hence, $\underbrace{v_p(a)}_{\in\mathbb{N}} - \underbrace{v_p(b)}_{\in\mathbb{N}} \in \mathbb{Z}$. In other words, $v_p(a) - v_p(b)$ is a well-defined integer. This proves Claim 2.]

It remains to prove Claim 3. Clearly, Claim 3 can be restated as follows:

> *Claim 4:* Let (a_1, b_1) and (a_2, b_2) be two pairs (a, b) of nonzero integers a and b satisfying $r = a/b$. Then, $v_p(a_1) - v_p(b_1) = v_p(a_2) - v_p(b_2)$.

[*Proof of Claim 4:* We have assumed that (a_1, b_1) is a pair (a, b) of nonzero integers a and b satisfying $r = a/b$. In other words, (a_1, b_1) is a pair of nonzero integers satisfying $r = a_1/b_1$. Similarly, (a_2, b_2) is a pair of nonzero integers satisfying $r = a_2/b_2$.

We have $r = a_1/b_1$, thus $a_1/b_1 = r = a_2/b_2$. Multiplying this equality by b_1b_2, we find $a_1b_2 = a_2b_1$. Theorem 2.13.28 **(a)** (applied to $a = a_1$ and $b = b_2$) yields $v_p(a_1b_2) = v_p(a_1) + v_p(b_2)$. Theorem 2.13.28 **(a)** (applied to $a = a_2$ and $b = b_1$) yields $v_p(a_2b_1) = v_p(a_2) + v_p(b_1)$. Now, from $v_p(a_1b_2) = v_p(a_1) + v_p(b_2)$, we obtain

$$v_p(a_1) + v_p(b_2) = v_p\left(\underbrace{a_1b_2}_{=a_2b_1}\right) = v_p(a_2b_1) = v_p(a_2) + v_p(b_1). \tag{470}$$

But b_1 is a nonzero integer (since (a_1, b_1) is a pair of nonzero integers); thus, $v_p(b_1) \in \mathbb{N}$ (since Definition 2.13.23 **(a)** shows that $v_p(n) \in \mathbb{N}$ for each nonzero integer n). Similarly, $v_p(b_2) \in \mathbb{N}$. Hence, $\underbrace{v_p(b_1)}_{\in\mathbb{N}} + \underbrace{v_p(b_2)}_{\in\mathbb{N}} \in \mathbb{N}$. Thus, we can subtract $v_p(b_1) + v_p(b_2)$ from both sides of the equality (470)[303]. We thus obtain $v_p(a_1) - v_p(b_1) = v_p(a_2) - v_p(b_2)$. This proves Claim 4.]

[302] This needs saying, because p-valuations can be ∞ and thus their differences may fail to be well-defined integers (for example, $\infty - \infty$ is not even well-defined).

[303] The reason why we are so circumspect about this is that p-valuations can be ∞, and ∞ cannot be subtracted. So when subtracting a p-valuation, it is important to ensure that this p-valuation is an element of $\mathbb{N}$ (that is, it is not ∞).

As we recall, Claim 4 is just a restatement of Claim 3. Hence, Claim 3 is proven (since Claim 4 is proven). From Claims 1, 2 and 3, we conclude that $w_p(r)$ is well-defined. Thus, Exercise 3.4.1 **(a)** is solved.

Let us state a consequence of the definition of $w_p(r)$: If r is a nonzero rational number, and if a and b are two nonzero integers satisfying $r = a/b$, then

$$w_p(r) = v_p(a) - v_p(b). \tag{471}$$

(b) Let n be a nonzero integer. We must prove that $w_p(n) = v_p(n)$.

We know that n and 1 are two nonzero integers satisfying $n = n/1$. Hence, (471) (applied to $r = n$, $a = n$ and $b = 1$) yields

$$w_p(n) = v_p(n) - \underbrace{v_p(1)}_{\substack{=0 \\ \text{(by Theorem 2.13.28 (c))}}} = v_p(n).$$

This solves Exercise 3.4.1 **(b)**.

(c) Let a and b be two nonzero rational numbers. We must show that $w_p(ab) = w_p(a) + w_p(b)$.

We know that a is a rational number. Thus, we can write a in the form $a = n_1/d_1$ for some integer n_1 and some nonzero integer d_1. Consider these n_1 and d_1. If we had $n_1 = 0$, then we would have $a = \underbrace{n_1}_{=0}/d_1 = 0$, which would contradict the assumption that a is nonzero. Hence, we do not have $n_1 = 0$. In other words, n_1 is nonzero. Thus, (471) (applied to a, n_1 and d_1 instead of r, a and b) yields

$$w_p(a) = v_p(n_1) - v_p(d_1). \tag{472}$$

We know that b is a rational number. Thus, we can write b in the form $b = n_2/d_2$ for some integer n_2 and some nonzero integer d_2. Consider these n_2 and d_2. If we had $n_2 = 0$, then we would have $b = \underbrace{n_2}_{=0}/d_2 = 0$, which would contradict the assumption that b is nonzero. Hence, we do not have $n_2 = 0$. In other words, n_2 is nonzero. Thus, (471) (applied to b, n_2 and d_2 instead of r, a and b) yields

$$w_p(b) = v_p(n_2) - v_p(d_2). \tag{473}$$

From $a = n_1/d_1$ and $b = n_2/d_2$, we obtain

$$ab = (n_1/d_1)(n_2/d_2) = (n_1n_2)/(d_1d_2).$$

Moreover, the integer n_1n_2 is nonzero (since n_1 and n_2 are nonzero), and the integer d_1d_2 is nonzero (since d_1 and d_2 are nonzero). Hence, (471) (applied to ab, n_1n_2 and d_1d_2 instead of r, a and b) yields

$$\begin{aligned} w_p(ab) &= \underbrace{v_p(n_1n_2)}_{\substack{=v_p(n_1)+v_p(n_2) \\ \text{(by Theorem 2.13.28 \textbf{(a)},} \\ \text{applied to } n_1 \text{ and } n_2 \text{ instead of } a \text{ and } b\text{)}}} - \underbrace{v_p(d_1d_2)}_{\substack{=v_p(d_1)+v_p(d_2) \\ \text{(by Theorem 2.13.28 \textbf{(a)},} \\ \text{applied to } d_1 \text{ and } d_2 \text{ instead of } a \text{ and } b\text{)}}} \\ &= \left(v_p(n_1)+v_p(n_2)\right) - \left(v_p(d_1)+v_p(d_2)\right) \\ &= \underbrace{\left(v_p(n_1)-v_p(d_1)\right)}_{\substack{=w_p(a) \\ \text{(by (472))}}} + \underbrace{\left(v_p(n_2)-v_p(d_2)\right)}_{\substack{=w_p(b) \\ \text{(by (473))}}} \\ &= w_p(a)+w_p(b). \end{aligned}$$

This solves Exercise 3.4.1 **(c)**.

(d) Let a and b be two nonzero rational numbers such that $a+b \neq 0$. We must show that $w_p(a+b) \geq \min\{w_p(a), w_p(b)\}$.

Note that $a+b$ is a nonzero rational number (since $a+b \neq 0$); thus, $w_p(a+b)$ is well-defined.

We know that a is a rational number. Thus, we can write a in the form $a = n_1/d_1$ for some integer n_1 and some nonzero integer d_1. Consider these n_1 and d_1. Then, n_1 is nonzero (this is proven in the same way as in our solution to Exercise 3.4.1 **(c)**). Thus, (471) (applied to a, n_1 and d_1 instead of r, a and b) yields

$$w_p(a) = v_p(n_1) - v_p(d_1). \tag{474}$$

We know that b is a rational number. Thus, we can write b in the form $b = n_2/d_2$ for some integer n_2 and some nonzero integer d_2. Consider these n_2 and d_2. Then, n_2 is nonzero (this is proven in the same way as in our solution to Exercise 3.4.1 **(c)**). Thus, (471) (applied to b, n_2 and d_2 instead of r, a and b) yields

$$w_p(b) = v_p(n_2) - v_p(d_2). \tag{475}$$

From $a = n_1/d_1$ and $b = n_2/d_2$, we obtain

$$a+b = (n_1/d_1) + (n_2/d_2) = (n_1d_2 + n_2d_1) / (d_1d_2).$$

Moreover, the integer $n_1d_2+n_2d_1$ is nonzero (because otherwise, we would have $n_1d_2 + n_2d_1 = 0$ and therefore $a+b = \underbrace{(n_1d_2+n_2d_1)}_{=0} / (d_1d_2) = 0$, which would contradict $a+b \neq 0$), and the integer d_1d_2 is nonzero (since d_1 and d_2 are nonzero). Hence, (471) (applied to

$a+b$, $n_1d_2+n_2d_1$ and d_1d_2 instead of r, a and b) yields

$$\begin{aligned} w_p(a+b) &= \underbrace{v_p(n_1d_2+n_2d_1)}_{\substack{\geq \min\left\{v_p(n_1d_2),v_p(n_2d_1)\right\} \\ \text{(by Theorem 2.13.28 \textbf{(b)},} \\ \text{applied to } n_1d_2 \text{ and } n_2d_1 \text{ instead of } a \text{ and } b)}} - \underbrace{v_p(d_1d_2)}_{\substack{=v_p(d_1)+v_p(d_2) \\ \text{(by Theorem 2.13.28 \textbf{(a)},} \\ \text{applied to } d_1 \text{ and } d_2 \text{ instead of } a \text{ and } b)}} \\ &\geq \min\left\{ \underbrace{v_p(n_1d_2)}_{\substack{=v_p(n_1)+v_p(d_2) \\ \text{(by Theorem 2.13.28 \textbf{(a)},} \\ \text{applied to } n_1 \text{ and } d_2 \\ \text{instead of } a \text{ and } b)}}, \underbrace{v_p(n_2d_1)}_{\substack{=v_p(n_2)+v_p(d_1) \\ \text{(by Theorem 2.13.28 \textbf{(a)},} \\ \text{applied to } n_2 \text{ and } d_1 \\ \text{instead of } a \text{ and } b)}} \right\} - \left(v_p(d_1)+v_p(d_2)\right) \\ &= \min\left\{v_p(n_1)+v_p(d_2), v_p(n_2)+v_p(d_1)\right\} - \left(v_p(d_1)+v_p(d_2)\right). \end{aligned} \tag{476}$$

But it is easy to see that any three numbers $i,j,k\in\mathbb{N}$ satisfy

$$\min\{i,j\}-k=\min\{i-k,j-k\} \tag{477}$$

[304]. Also, it is easy to see that the three numbers $v_p(n_1)+v_p(d_2), v_p(n_2)+v_p(d_1), v_p(d_1)+v_p(d_2)$ belong to $\mathbb{N}$ (since n_1,n_2,d_1,d_2 are all nonzero). Hence, (477) (applied to $i=v_p(n_1)+v_p(d_2)$, $j=v_p(n_2)+v_p(d_1)$ and $k=v_p(d_1)+v_p(d_2)$) yields

$$\begin{aligned} &\min\left\{v_p(n_1)+v_p(d_2), v_p(n_2)+v_p(d_1)\right\} - \left(v_p(d_1)+v_p(d_2)\right) \\ &= \min\left\{ \underbrace{v_p(n_1)+v_p(d_2)-\left(v_p(d_1)+v_p(d_2)\right)}_{\substack{=v_p(n_1)-v_p(d_1)=w_p(a) \\ \text{(by (474))}}}, \underbrace{v_p(n_2)+v_p(d_1)-\left(v_p(d_1)+v_p(d_2)\right)}_{\substack{=v_p(n_2)-v_p(d_2)=w_p(b) \\ \text{(by (475))}}} \right\} \\ &= \min\left\{w_p(a), w_p(b)\right\}. \end{aligned}$$

Thus, (476) becomes

$$\begin{aligned} w_p(a+b) &\geq \min\left\{v_p(n_1)+v_p(d_2), v_p(n_2)+v_p(d_1)\right\} - \left(v_p(d_1)+v_p(v_2)\right) \\ &= \min\left\{w_p(a), w_p(b)\right\}. \end{aligned}$$

This solves Exercise 3.4.1 **(d)**. □

[304] *Proof of (477):* Let $i,j,k\in\mathbb{N}$ be three numbers. We must prove the equality (477). We can WLOG assume that $i\leq j$ (since i and j play symmetric roles in our claim, and thus swapping i with j will not change anything). Assume this. Hence, $\underbrace{i}_{\leq j}-k\leq j-k$, thus $\min\{i-k,j-k\}=i-k$. Comparing this with $\underbrace{\min\{i,j\}}_{\substack{=i \\ \text{(since } i\leq j)}}-k=i-k$, we obtain $\min\{i,j\}-k=\min\{i-k,j-k\}$. This proves (477).

10.87. Solution to Exercise 3.4.2

Solution to Exercise 3.4.2. It is possible to write r in the form $r = a/b$ for two nonzero integers a and b. [305] Consider these a and b.

We have $r = a/b$. Thus, for each prime p, we have

$$w_p(r) = v_p(a) - v_p(b) \tag{478}$$

(by (471)). Also, $rb = a$ (since $r = a/b$).

(a) Let p be a prime such that $p > \max\{|a|, |b|\}$. Then, $p > \max\{|a|, |b|\} \geq |a|$. Hence, Lemma 2.13.32 **(a)** (applied to $n = a$) yields $v_p(a) = 0$. The same argument (applied to b instead of a) leads to $v_p(b) = 0$ (since $p > \max\{|a|, |b|\} \geq |b|$). Now, (478) yields $w_p(r) = \underbrace{v_p(a)}_{=0} - \underbrace{v_p(b)}_{=0} = 0 - 0 = 0$.

Now, forget that we fixed p. We thus have proven that every prime p satisfying $p > \max\{|a|, |b|\}$ satisfies $w_p(r) = 0$. Hence, all but finitely many primes p satisfy $w_p(r) = 0$ (since all but finitely many primes p satisfy $p > \max\{|a|, |b|\}$). This solves Exercise 3.4.2 **(a)**.

(b) Exercise 3.4.2 **(a)** shows that all but finitely many primes p satisfy $w_p(r) = 0$. Hence, all but finitely many primes p satisfy $p^{w_p(r)} = p^0 = 1$. In other words, only finitely many primes p satisfy $p^{w_p(r)} \neq 1$. In other words, the product $\prod\limits_{p \text{ prime}} p^{w_p(r)}$ has only finitely many factors different from 1. Hence, this product $\prod\limits_{p \text{ prime}} p^{w_p(r)}$ is well-defined.

It remains to prove that $|r| = \prod\limits_{p \text{ prime}} p^{w_p(r)}$.

Corollary 2.13.34 (applied to $n = a$) yields that

$$|a| = \prod_{p \text{ prime}} p^{v_p(a)} \tag{479}$$

(and, in particular, the infinite product $\prod\limits_{p \text{ prime}} p^{v_p(a)}$ is well-defined). Corollary 2.13.34 (applied to $n = b$) yields that

$$|b| = \prod_{p \text{ prime}} p^{v_p(b)} \tag{480}$$

(and, in particular, the infinite product $\prod\limits_{p \text{ prime}} p^{v_p(b)}$ is well-defined). But $|b|$ is nonzero (since b is nonzero). Hence, we can divide the equality (479) by the equality (480). We thus obtain

$$\frac{|a|}{|b|} = \frac{\prod\limits_{p \text{ prime}} p^{v_p(a)}}{\prod\limits_{p \text{ prime}} p^{v_p(b)}} = \prod_{p \text{ prime}} \underbrace{\frac{p^{v_p(a)}}{p^{v_p(b)}}}_{=p^{v_p(a)-v_p(b)}} = \prod_{p \text{ prime}} p^{v_p(a)-v_p(b)}.$$

But (3) (applied to $x = r$ and $y = b$) yields $|rb| = |r| \cdot |b|$. We can divide this equality by $|b|$ (since $|b|$ is nonzero), and thus obtain $|rb| \,/\, |b| = |r|$. Hence,

$$|r| = \left|\underbrace{rb}_{=a}\right| / |b| = |a| \,/\, |b| = \frac{|a|}{|b|} = \prod_{p \text{ prime}} p^{v_p(a)-v_p(b)}.$$

[305] Indeed, this is precisely Claim 1 in our above solution of Exercise 3.4.1 **(a)**.

Comparing this with

$$\prod_{p \text{ prime}} \underbrace{p^{w_p(r)}}_{\substack{=p^{v_p(a)-v_p(b)} \\ \text{(by (478))}}} = \prod_{p \text{ prime}} p^{v_p(a)-v_p(b)},$$

we obtain $|r| = \prod\limits_{p \text{ prime}} p^{w_p(r)}$. This completes the solution to Exercise 3.4.2 **(b)**.

(c) We have $b \neq 0$ (since b is nonzero). Thus, Proposition 2.2.3 **(c)** (applied to b and a instead of a and b) shows that $b \mid a$ if and only if $\dfrac{a}{b} \in \mathbb{Z}$. In other words, $b \mid a$ if and only if $r \in \mathbb{Z}$ (since $r = a/b = \dfrac{a}{b}$). In other words, we have the following logical equivalence:

$$(b \mid a) \iff (r \in \mathbb{Z}). \qquad (481)$$

But Proposition 2.13.35 (applied to $m = a$ and $n = b$) shows that we have $b \mid a$ if and only if each prime p satisfies $v_p(b) \leq v_p(a)$. In other words, we have the following logical equivalence:

$$(b \mid a) \iff \left(\text{each prime } p \text{ satisfies } v_p(b) \leq v_p(a)\right). \qquad (482)$$

Now, we have the following chain of equivalences:

$$\begin{aligned} (r \in \mathbb{Z}) &\iff (b \mid a) \qquad \text{(by (481))} \\ &\iff \left(\text{each prime } p \text{ satisfies } v_p(b) \leq v_p(a)\right) \qquad \text{(by (482))} \\ &\iff \left(\text{each prime } p \text{ satisfies } \underbrace{v_p(a) - v_p(b)}_{\substack{=w_p(r) \\ \text{(by (478))}}} \geq 0\right) \\ &\qquad \left(\begin{array}{c}\text{because for each prime } p\text{, the inequality } v_p(b) \leq v_p(a) \\ \text{is equivalent to the inequality } v_p(a) - v_p(b) \geq 0\end{array}\right) \\ &\iff \left(\text{each prime } p \text{ satisfies } w_p(r) \geq 0\right). \end{aligned}$$

In other words, $r \in \mathbb{Z}$ if and only if each prime p satisfies $w_p(r) \geq 0$. This solves Exercise 3.4.2 **(c)**.

(d) We must prove the equivalence

$$\begin{aligned} &\left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k r \in \mathbb{Z}\right) \\ &\iff \left(\text{every prime } p \text{ satisfying } w_p(r) < 0 \text{ satisfies } p \mid m\right). \end{aligned}$$

We shall prove its "$\Longrightarrow$" and "$\Longleftarrow$" directions separately:

$\Longrightarrow$: Assume that there exists a $k \in \mathbb{N}$ satisfying $m^k r \in \mathbb{Z}$. We must prove that every prime p satisfying $w_p(r) < 0$ satisfies $p \mid m$.

Let p be a prime satisfying $w_p(r) < 0$. We must then prove that $p \mid m$.

If $m = 0$, then this is obvious[306]. Hence, for the rest of this proof, we WLOG assume that $m \neq 0$. Hence, m is nonzero.

We have assumed that there exists a $k \in \mathbb{N}$ satisfying $m^k r \in \mathbb{Z}$. Consider this k.

[306] because in this case, we have $m = 0 = p \cdot 0$ and thus $p \mid m$

Note that m^k is a nonzero integer (since m is a nonzero integer and $k \in \mathbb{N}$). Hence, Exercise 3.4.1 **(b)** (applied to $n = m^k$) yields $w_p\left(m^k\right) = v_p\left(m^k\right) = kv_p\left(m\right)$ (by Exercise 2.13.6, applied to m instead of a). Also, $m^k r$ is an integer (since $m^k r \in \mathbb{Z}$) and is nonzero (since m^k and r are nonzero). Thus, Exercise 3.4.1 **(b)** (applied to $n = m^k r$) yields $w_p\left(m^k r\right) = v_p\left(m^k r\right) \in \mathbb{N}$ (since the p-valuation of any nonzero integer belongs to $\mathbb{N}$). Hence, $w_p\left(m^k r\right) \geq 0$.

But Exercise 3.4.1 **(c)** (applied to m^k and r instead of a and b) yields

$$w_p\left(m^k r\right) = \underbrace{w_p\left(m^k\right)}_{=kv_p(m)} + \underbrace{w_p\left(r\right)}_{<0} < kv_p\left(m\right),$$

so that $kv_p\left(m\right) > w_p\left(m^k r\right) \geq 0$. Thus, $kv_p\left(m\right) \neq 0$, so that $v_p\left(m\right) \neq 0$. In other words, we don't have $v_p\left(m\right) = 0$.

But Corollary 2.13.26 (applied to $n = m$) shows that $v_p\left(m\right) = 0$ if and only if $p \nmid m$. Hence, we don't have $p \nmid m$ (since we don't have $v_p\left(m\right) = 0$). In other words, we have $p \mid m$.

Now, forget that we fixed p. We thus have proven that every prime p satisfying $w_p\left(r\right) < 0$ satisfies $p \mid m$. This completes the proof of the "$\Longrightarrow$" direction of Exercise 3.4.2 **(d)**.

$\Longleftarrow$: Assume that every prime p satisfying $w_p\left(r\right) < 0$ satisfies $p \mid m$. We must prove that there exists a $k \in \mathbb{N}$ satisfying $m^k r \in \mathbb{Z}$.

If $m = 0$, then this is obvious[307]. Hence, for the rest of this proof, we WLOG assume that $m \neq 0$. Hence, m is nonzero.

We have assumed that

$$\text{every prime } p \text{ satisfying } w_p\left(r\right) < 0 \text{ satisfies } p \mid m. \tag{483}$$

Exercise 3.4.2 **(a)** shows that all but finitely many primes p satisfy $w_p\left(r\right) = 0$. In other words, there is a finite set P of primes such that

$$\text{every prime } p \notin P \text{ must satisfy } w_p\left(r\right) = 0 \tag{484}$$

(where "prime $p \notin P$" means "prime p satisfying $p \notin P$"). Consider this P. Clearly, the set $\left\{w_p\left(r\right) \mid p \in P\right\}$ is finite (since P is finite).

Define a subset W of $\mathbb{Z}$ by

$$W = \left\{w_p\left(r\right) \mid p \in P\right\} \cup \left\{0\right\}$$

[308]. This set W is finite[309]. Moreover, $0 \in \left\{0\right\} \subseteq \left\{w_p\left(r\right) \mid p \in P\right\} \cup \left\{0\right\} = W$. In other words, the set W contains 0, and thus is nonempty.

We have $\left\{w_p\left(r\right) \mid p \in P\right\} \subseteq \left\{w_p\left(r\right) \mid p \in P\right\} \cup \left\{0\right\} = W$. In other words,

$$w_p\left(r\right) \in W \qquad \text{for each } p \in P. \tag{485}$$

[307] because in this case, we can take $k = 1$ and obtain $\underbrace{m^k}_{=m^1=m=0} r = 0 \in \mathbb{Z}$

[308] This is well-defined, since $w_p\left(r\right) \in \mathbb{Z}$ for each $p \in P$.

[309] since it is the union of the two finite sets $\left\{w_p\left(r\right) \mid p \in P\right\}$ and $\left\{0\right\}$

But every nonempty finite subset of $\mathbb{Z}$ has a smallest element. Hence, W has a smallest element (since W is a nonempty finite subset of $\mathbb{Z}$). Let g be this smallest element. Thus, $g \in W \subseteq \mathbb{Z}$ and

$$g \leq i \qquad \text{for each } i \in W \tag{486}$$

(since g is the smallest element of W). Applying (486) to $i = 0$, we obtain $g \leq 0$ (since $0 \in W$). Hence, $-g \geq 0$, so that $-g \in \mathbb{N}$ (since $-g$ is an integer).

Set $h = -g$. Then, $h = -g \in \mathbb{N}$, so that $h \geq 0$.

Now, we shall show that $m^h r \in \mathbb{Z}$. We shall achieve this by applying Exercise 3.4.2 **(c)** to $m^h r$ instead of r.

Indeed, m^h is a nonzero integer (since m is a nonzero integer, and $h \in \mathbb{N}$), thus a nonzero rational number. Hence, $m^h r$ is a nonzero rational number (since m^h and r are nonzero rational numbers). Now, let p be any prime. We shall show that $w_p\left(m^h r\right) \geq 0$.

Indeed, assume the contrary. Thus, $w_p\left(m^h r\right) < 0$. But m^h is a nonzero integer; hence, Exercise 3.4.1 **(b)** (applied to $n = m^h$) yields $w_p\left(m^h\right) = v_p\left(m^h\right) = h v_p(m)$ (by Exercise 2.13.6, applied to m and h instead of a and k). Also, m is a nonzero integer; thus, $v_p(m) \in \mathbb{N}$ (since the p-valuation of any nonzero integer belongs to $\mathbb{N}$). Thus, $\underbrace{h}_{\in\mathbb{N}} \underbrace{v_p(m)}_{\in\mathbb{N}} \in \mathbb{N}$, so that $h v_p(m) \geq 0$.

But Exercise 3.4.1 **(c)** (applied to m^h and r instead of a and b) yields

$$\begin{aligned} w_p\left(m^h r\right) &= \underbrace{w_p\left(m^h\right)}_{=hv_p(m)} + w_p(r) = \underbrace{h v_p(m)}_{\geq 0} + w_p(r) \\ &\geq w_p(r), \end{aligned} \tag{487}$$

and thus $w_p(r) \leq w_p\left(m^h r\right) < 0$. Thus, (483) shows that $p \mid m$. In other words, we don't have $p \nmid m$.

But Corollary 2.13.26 (applied to $n = m$) shows that $v_p(m) = 0$ if and only if $p \nmid m$. Hence, we don't have $v_p(m) = 0$ (since we don't have $p \nmid m$). Thus, $v_p(m) \neq 0$, so that $v_p(m) \geq 1$ (since $v_p(m) \in \mathbb{N}$). Thus, $h \underbrace{v_p(m)}_{\geq 1} \geq h$ (since $h \geq 0$).

If we had $p \notin P$, then we would have $w_p(r) = 0$ (by (484)), which would contradict $w_p(r) < 0$. Thus, we cannot have $p \notin P$. Hence, we have $p \in P$. Thus, (485) yields $w_p(r) \in W$. Hence, (486) (applied to $i = w_p(r)$) yields $g \leq w_p(r)$, so that $w_p(r) \geq g$.

Now, (487) becomes

$$w_p\left(m^h r\right) = \underbrace{h v_p(m)}_{\geq h} + \underbrace{w_p(r)}_{\geq g} \geq h + g = 0 \qquad (\text{since } h = -g).$$

This contradicts $w_p\left(m^h r\right) < 0$. This contradiction shows that our assumption was false. Hence, $w_p\left(m^h r\right) \geq 0$ is proven.

Now, forget that we fixed p. We thus have shown that each prime p satisfies $w_p\left(m^h r\right) \geq 0$.

But Exercise 3.4.2 **(c)** (applied to $m^h r$ instead of r) shows that we have $m^h r \in \mathbb{Z}$ if and only if each prime p satisfies $w_p\left(m^h r\right) \geq 0$. Hence, we have $m^h r \in \mathbb{Z}$ (since each prime p satisfies $w_p\left(m^h r\right) \geq 0$). Thus, there exists a $k \in \mathbb{N}$ satisfying $m^k r \in \mathbb{Z}$ (namely, $k = h$). This proves the "$\Longleftarrow$" direction of Exercise 3.4.2 **(d)**. □

10.88. Solution to Exercise 3.5.1

Solution to Exercise 3.5.1. **(a)** The inverse α^{-1} of α exists (since α has an inverse). We have $\alpha \cdot \alpha^{-1} = [1]_n$ (since α^{-1} is an inverse of α). But Theorem 3.4.23 **(e)** (applied to α^{-1} and α instead of α and β) yields $\alpha^{-1} \cdot \alpha = \alpha \cdot \alpha^{-1} = [1]_n$. In other words, α is an inverse of α^{-1}. Thus, α^{-1} has an inverse (namely, α). Therefore, we can speak of "the inverse of α^{-1}". Moreover, $\left(\alpha^{-1}\right)^{-1} = \left(\text{the inverse of } \alpha^{-1}\right) = \alpha$ (since α is an inverse of α^{-1}). This solves Exercise 3.5.1 **(a)**.

(b) The inverse α^{-1} of α exists (since α has an inverse). We have $\alpha \cdot \alpha^{-1} = [1]_n$ (since α^{-1} is an inverse of α). The inverse β^{-1} of β exists (since β has an inverse). We have $\beta \cdot \beta^{-1} = [1]_n$ (since β^{-1} is an inverse of β). Theorem 3.4.23 **(e)** yields $\alpha \cdot \beta = \beta \cdot \alpha$. In other words, $\alpha\beta = \beta\alpha$.

Theorem 3.4.23 **(f)** (applied to β, α and α^{-1}) yields $\beta \cdot \left(\alpha \cdot \alpha^{-1}\right) = (\beta \cdot \alpha) \cdot \alpha^{-1} = (\beta\alpha) \cdot \alpha^{-1}$, so that

$$(\beta\alpha) \cdot \alpha^{-1} = \beta \cdot \underbrace{\left(\alpha \cdot \alpha^{-1}\right)}_{=[1]_n} = \beta \cdot [1]_n = \beta$$

(by Theorem 3.4.23 **(d)**).

Now, Theorem 3.4.23 **(f)** (applied to $\alpha\beta$, α^{-1} and β^{-1} instead of α, β and γ) yields

$$(\alpha\beta) \cdot \left(\alpha^{-1}\beta^{-1}\right) = \left(\underbrace{(\alpha\beta)}_{=\beta\alpha} \cdot \alpha^{-1}\right) \cdot \beta^{-1} = \underbrace{\left((\beta\alpha) \cdot \alpha^{-1}\right)}_{=\beta} \cdot \beta^{-1} = \beta \cdot \beta^{-1} = [1]_n .$$

In other words, $\alpha^{-1}\beta^{-1}$ is an inverse of $\alpha\beta$. Thus, $\alpha\beta$ has an inverse (namely, $\alpha^{-1}\beta^{-1}$). Therefore, we can speak of "the inverse of $\alpha\beta$". Moreover, $(\alpha\beta)^{-1} = (\text{the inverse of } \alpha\beta) = \alpha^{-1}\beta^{-1}$ (since $\alpha^{-1}\beta^{-1}$ is an inverse of $\alpha\beta$). This solves Exercise 3.5.1 **(b)**.

[*Remark:* In the above solution, we have avoided writing products of the form $\alpha_1\alpha_2\cdots\alpha_k$ with more than 2 factors without explicitly placing parentheses. This was done for the purpose of making each single use of associativity explicit. Had we instead written such products without parenthesization, our solution would have become much simpler; namely, we could simply argue that

$$(\alpha\beta) \cdot \left(\alpha^{-1}\beta^{-1}\right) = \underbrace{\alpha\beta}_{=\beta\alpha} \alpha^{-1}\beta^{-1} = \beta \underbrace{\alpha\alpha^{-1}}_{=[1]_n} \beta^{-1} = \underbrace{\beta\,[1]_n}_{\substack{=\beta \\ \text{(by Theorem 3.4.23 (d))}}} \beta^{-1} = \beta\beta^{-1} = [1]_n .$$

Computations of this kind are perfectly legitimate, because Proposition 3.4.25 shows that products of the form $\alpha_1\alpha_2\cdots\alpha_k$ are well-defined and satisfy the standard rules (which include the one saying that $\alpha_1\alpha_2\cdots\alpha_k = (\alpha_1\alpha_2\cdots\alpha_i)(\alpha_{i+1}\alpha_{i+2}\cdots\alpha_k)$ for each $i \in \{0,1,\ldots,k\}$).]

□

10.89. Solution to Exercise 4.1.1

Proof of Proposition 4.1.20. **(a)** Let $\alpha \in \mathbb{C}$ and $n \in \mathbb{N}$. The definition of α^n yields $\alpha^n = \underbrace{\alpha\alpha\cdots\alpha}_{n\text{ times}}$. The definition of α^{n+1} yields

$$\alpha^{n+1} = \underbrace{\alpha\alpha\cdots\alpha}_{n+1\text{ times}} = \alpha\cdot\underbrace{\alpha\alpha\cdots\alpha}_{n\text{ times}}.$$

Comparing this with

$$\alpha\underbrace{\alpha^n}_{=\underbrace{\alpha\alpha\cdots\alpha}_{n\text{ times}}} = \alpha\cdot\underbrace{\alpha\alpha\cdots\alpha}_{n\text{ times}},$$

we obtain $\alpha^{n+1} = \alpha\alpha^n$. This proves Proposition 4.1.20 **(a)**.

(b) *First proof of Proposition 4.1.20 (b):* Let $\alpha \in \mathbb{C}$ and $n, m \in \mathbb{N}$. Definition 4.1.18 **(a)** yields $\alpha^n = \underbrace{\alpha\alpha\cdots\alpha}_{n\text{ times}}$ and $\alpha^m = \underbrace{\alpha\alpha\cdots\alpha}_{m\text{ times}}$. Multiplying these two equalities, we obtain

$$\alpha^n\alpha^m = \underbrace{\alpha\alpha\cdots\alpha}_{n\text{ times}}\cdot\underbrace{\alpha\alpha\cdots\alpha}_{m\text{ times}} = \underbrace{\alpha\alpha\cdots\alpha}_{n+m\text{ times}}.$$

Comparing this with

$$\alpha^{n+m} = \underbrace{\alpha\alpha\cdots\alpha}_{n+m\text{ times}} \qquad (\text{by Definition 4.1.18 } \textbf{(a)}),$$

we obtain $\alpha^{n+m} = \alpha^n\alpha^m$. This proves Proposition 4.1.20 **(b)**.

Second proof of Proposition 4.1.20 (b): We shall prove Proposition 4.1.20 **(b)** by induction on n:

Induction base: If $\alpha \in \mathbb{C}$ and $m \in \mathbb{N}$, then $\underbrace{\alpha^0}_{=1}\alpha^m = 1\cdot\alpha^m = \alpha^m = \alpha^{0+m}$ (since $m = 0+m$). In other words, we have $\alpha^{0+m} = \alpha^0\alpha^m$ for all $\alpha \in \mathbb{C}$ and $m \in \mathbb{N}$. In other words, Proposition 4.1.20 **(b)** holds for $n = 0$. This completes the induction base.

Induction step: Let $k \in \mathbb{N}$. Assume that Proposition 4.1.20 **(b)** holds for $n = k$. We must prove that Proposition 4.1.20 **(b)** holds for $n = k+1$.

Let $\alpha \in \mathbb{C}$ and $m \in \mathbb{N}$. We have assumed that Proposition 4.1.20 **(b)** holds for $n = k$. Hence, we can apply Proposition 4.1.20 **(b)** to $n = k$. We thus obtain $\alpha^{k+m} = \alpha^k\alpha^m$.

Proposition 4.1.20 **(a)** (applied to $n = k$) yields $\alpha^{k+1} = \alpha\alpha^k$. Also, Proposition 4.1.20 **(a)** (applied to $n = k+m$) yields $\alpha^{(k+m)+1} = \alpha\alpha^{k+m}$.

But $(k+1)+m = (k+m)+1$ and hence

$$\alpha^{(k+1)+m} = \alpha^{(k+m)+1} = \alpha\underbrace{\alpha^{k+m}}_{=\alpha^k\alpha^m} = \alpha\left(\alpha^k\alpha^m\right) = \underbrace{\left(\alpha\alpha^k\right)}_{=\alpha^{k+1}}\alpha^m \qquad (\text{by Theorem 4.1.2 } \textbf{(f)})$$
$$= \alpha^{k+1}\alpha^m.$$

Now, forget that we fixed α and m. We thus have shown that $\alpha^{(k+1)+m} = \alpha^{k+1}\alpha^m$ for all $\alpha \in \mathbb{C}$ and $m \in \mathbb{N}$. In other words, Proposition 4.1.20 **(b)** holds for $n = k+1$. This completes the induction step. Thus, Proposition 4.1.20 **(b)** is proven by induction.

(c) We shall prove Proposition 4.1.20 **(c)** by induction on n:

Induction base: Let $\alpha, \beta \in \mathbb{C}$. Then, $(\alpha\beta)^0 = 1 = \alpha^0\beta^0$ (since $\underbrace{\alpha^0}_{=1} \underbrace{\beta^0}_{=1} = 1 \cdot 1 = 1$).

Forget that we fixed α, β. We thus have shown that $(\alpha\beta)^0 = \alpha^0\beta^0$ for all $\alpha, \beta \in \mathbb{C}$. In other words, Proposition 4.1.20 **(c)** holds for $n = 0$. This completes the induction base.

Induction step: Let $k \in \mathbb{N}$. Assume that Proposition 4.1.20 **(c)** holds for $n = k$. We must prove that Proposition 4.1.20 **(c)** holds for $n = k + 1$.

Let $\alpha, \beta \in \mathbb{C}$. We have assumed that Proposition 4.1.20 **(c)** holds for $n = k$. Hence, $(\alpha\beta)^k = \alpha^k\beta^k$. But Proposition 4.1.20 **(a)** (applied to $n = k$) yields $\alpha^{k+1} = \alpha\alpha^k$. Similarly, $\beta^{k+1} = \beta\beta^k$. Multiplying these two equalities together, we obtain

$$\alpha^{k+1}\beta^{k+1} = \left(\alpha\alpha^k\right)\left(\beta\beta^k\right) = \left(\left(\alpha\alpha^k\right)\beta\right)\beta^k \qquad (488)$$

(by Theorem 4.1.2 **(f)**). But Proposition 4.1.20 **(a)** (applied to $\alpha\beta$ and k instead of α and n) yields[310]

$$\begin{aligned}
(\alpha\beta)^{k+1} &= (\alpha\beta)\underbrace{(\alpha\beta)^k}_{=\alpha^k\beta^k} = (\alpha\beta)\left(\alpha^k\beta^k\right) = \alpha \underbrace{\left(\beta\left(\alpha^k\beta^k\right)\right)}_{\substack{=\left(\beta\alpha^k\right)\beta^k \\ \text{(by Theorem 4.1.2 (f))}}} \\
&\qquad \left(\text{since Theorem 4.1.2 (f) yields } \alpha\left(\beta\left(\alpha^k\beta^k\right)\right) = (\alpha\beta)\left(\alpha^k\beta^k\right)\right) \\
&= \alpha\left(\left(\beta\alpha^k\right)\beta^k\right) = \left(\alpha \underbrace{\left(\beta\alpha^k\right)}_{\substack{=\alpha^k\beta \\ \text{(by Theorem 4.1.2 (e))}}}\right)\beta^k \qquad \text{(by Theorem 4.1.2 (f))} \\
&= \underbrace{\left(\alpha\left(\alpha^k\beta\right)\right)}_{\substack{=\left(\alpha\alpha^k\right)\beta \\ \text{(by Theorem 4.1.2 (f))}}} \beta^k = \left(\left(\alpha\alpha^k\right)\beta\right)\beta^k.
\end{aligned}$$

Comparing this with (488), we obtain $(\alpha\beta)^{k+1} = \alpha^{k+1}\beta^{k+1}$.

Now, forget that we fixed α, β. We thus have shown that $(\alpha\beta)^{k+1} = \alpha^{k+1}\beta^{k+1}$ for all $\alpha, \beta \in \mathbb{C}$. In other words, Proposition 4.1.20 **(c)** holds for $n = k + 1$. Thus, Proposition 4.1.20 **(c)** is proven by induction.

(d) We shall prove Proposition 4.1.20 **(d)** by induction on m:

Induction base: For all $\alpha \in \mathbb{C}$ and $n \in \mathbb{N}$, we have $(\alpha^n)^0 = 1 = \alpha^0 = \alpha^{n \cdot 0}$ (since $0 = n \cdot 0$). In other words, Proposition 4.1.20 **(d)** holds for $m = 0$. This completes the induction base.

Induction step: Let $k \in \mathbb{N}$. Assume that Proposition 4.1.20 **(d)** holds for $m = k$. We must prove that Proposition 4.1.20 **(d)** holds for $m = k + 1$.

[310] The following computation could be much shorter if I used unparenthesized products (i.e., if I wrote "$\alpha\beta\alpha^k\beta^k$" instead of explicitly invoking the associativity of multiplication to move between various ways of parenthesizing this product). I am avoiding unparenthesized products here for the purpose of illustrating how to live without them; in the future I will simply use them wherever they can help.

Let $\alpha \in \mathbb{C}$ and $n \in \mathbb{N}$. Then, $(\alpha^n)^k = \alpha^{nk}$ (since Proposition 4.1.20 **(d)** holds for $m = k$). Now, Proposition 4.1.20 **(a)** (applied to α^n and k instead of α and n) yields

$$(\alpha^n)^{k+1} = \alpha^n \underbrace{(\alpha^n)^k}_{=\alpha^{nk}} = \alpha^n \alpha^{nk}.$$

Comparing this with

$$\begin{aligned} \alpha^{n(k+1)} &= \alpha^{n+nk} && (\text{since } n(k+1) = n + nk) \\ &= \alpha^n \alpha^{nk} && (\text{by Proposition 4.1.20 } \textbf{(b)}, \text{ applied to } m = nk), \end{aligned}$$

we obtain $(\alpha^n)^{k+1} = \alpha^{n(k+1)}$.

Now, forget that we fixed α and n. We thus have shown that $(\alpha^n)^{k+1} = \alpha^{n(k+1)}$ for all $\alpha \in \mathbb{C}$ and $n \in \mathbb{N}$. In other words, Proposition 4.1.20 **(d)** holds for $m = k+1$. Hence, Proposition 4.1.20 **(d)** is proven by induction.

(e) We shall prove Proposition 4.1.20 **(e)** by induction on n:

Induction base: Proposition 4.1.20 **(e)** holds for $n = 0$ (since $1^0 = 1$). This completes the induction base.

Induction step: Let $k \in \mathbb{N}$. Assume that Proposition 4.1.20 **(e)** holds for $n = k$. We must prove that Proposition 4.1.20 **(e)** holds for $n = k+1$.

We have assumed that Proposition 4.1.20 **(e)** holds for $n = k$. In other words, $1^k = 1$. Now, Proposition 4.1.20 **(a)** (applied to $\alpha = 1$ and $n = k$) yields $1^{k+1} = 1 \cdot \underbrace{1^k}_{=1} = 1 \cdot 1 = 1$. In other words, Proposition 4.1.20 **(e)** holds for $n = k+1$. This completes the induction step. Hence, Proposition 4.1.20 **(e)** is proven by induction.

(f) Let $\alpha \in \mathbb{C}$ be nonzero. Let $n \in \mathbb{Z}$. We must prove that $\alpha^{n+1} = \alpha\alpha^n$.

Recall that α^{-1} is the inverse of α; hence, $\alpha\alpha^{-1} = 1$ (by the definition of "inverse").

We are in one of the following three cases:

Case 1: We have $n > -1$.

Case 2: We have $n = -1$.

Case 3: We have $n < -1$.

Let us first consider Case 1. In this case, we have $n > -1$. Thus, $n \geq 0$ (since n is an integer), so that $n \in \mathbb{N}$. Hence, Proposition 4.1.20 **(a)** yields $\alpha^{n+1} = \alpha\alpha^n$. Thus, $\alpha^{n+1} = \alpha\alpha^n$ is proven in Case 1.

Let us next consider Case 2. In this case, we have $n = -1$. Thus, $n + 1 = 0$, so that $\alpha^{n+1} = \alpha^0 = 1$. On the other hand, from $n = -1$, we obtain $\alpha\alpha^n = \alpha\alpha^{-1} = 1$. Comparing this with $\alpha^{n+1} = 1$, we find $\alpha^{n+1} = \alpha\alpha^n$. Hence, $\alpha^{n+1} = \alpha\alpha^n$ is proven in Case 2.

Let us finally consider Case 3. In this case, we have $n < -1$. Hence, $n + 1 < 0$. Therefore, Definition 4.1.19 (applied to $n+1$ instead of n) yields

$$\alpha^{n+1} = \left(\alpha^{-1}\right)^{-(n+1)}. \tag{489}$$

On the other hand, $n + 1 < 0$, hence $-(n+1) > 0$ and thus $-(n+1) \in \mathbb{N}$. Hence, Proposition 4.1.20 **(a)** (applied to α^{-1} and $-(n+1)$ instead of α and n) yields $\left(\alpha^{-1}\right)^{-(n+1)+1} =$

$\alpha^{-1}\left(\alpha^{-1}\right)^{-(n+1)}$. On the other hand, $n<-1<0$. Hence, Definition 4.1.19 yields

$$\alpha^{n}=\left(\alpha^{-1}\right)^{-n}=\left(\alpha^{-1}\right)^{-(n+1)+1} \qquad \left(\text{since } -n=-(n+1)+1\right)$$
$$=\alpha^{-1}\underbrace{\left(\alpha^{-1}\right)^{-(n+1)}}_{\substack{=\alpha^{n+1} \\ \text{(by (489))}}}=\alpha^{-1}\alpha^{n+1}.$$

Thus,

$$\alpha\underbrace{\alpha^{n}}_{=\alpha^{-1}\alpha^{n+1}}=\underbrace{\alpha\alpha^{-1}}_{=1}\alpha^{n+1}=\alpha^{n+1}.$$

In other words, $\alpha^{n+1}=\alpha\alpha^{n}$. Hence, $\alpha^{n+1}=\alpha\alpha^{n}$ is proven in Case 3.

We have now proven $\alpha^{n+1}=\alpha\alpha^{n}$ in all three Cases 1, 2 and 3. Thus, $\alpha^{n+1}=\alpha\alpha^{n}$ always holds. This proves Proposition 4.1.20 **(f)**.

(g) Let $\alpha\in\mathbb{C}$ be nonzero. Let $n\in\mathbb{Z}$. We must prove that $\alpha^{-n}=\left(\alpha^{-1}\right)^{n}$.

We are in one of the following three Cases:

Case 1: We have $n>0$.

Case 2: We have $n=0$.

Case 3: We have $n<0$.

Let us first consider Case 1. In this case, we have $n>0$. Hence, $-n<0$. In other words, $-n$ is negative. Hence, Definition 4.1.19 (applied to $-n$ instead of n) yields $\alpha^{-n}=\left(\alpha^{-1}\right)^{-(-n)}=\left(\alpha^{-1}\right)^{n}$ (since $-(-n)=n$). Hence, $\alpha^{-n}=\left(\alpha^{-1}\right)^{n}$ is proven in Case 1.

Let us next consider Case 2. In this case, we have $n=0$. Hence, $\alpha^{-n}=\alpha^{-0}=\alpha^{0}=1$ and $\left(\alpha^{-1}\right)^{n}=\left(\alpha^{-1}\right)^{0}=1$. Comparing these two equalities, we obtain $\alpha^{-n}=\left(\alpha^{-1}\right)^{n}$. Hence, $\alpha^{-n}=\left(\alpha^{-1}\right)^{n}$ is proven in Case 2.

Let us next consider Case 3. In this case, we have $n<0$. In other words, n is negative.

Recall that α^{-1} is the inverse of α; hence, $\alpha\alpha^{-1}=1$ (by the definition of "inverse"). Hence, $\alpha^{-1}\neq 0$ (since otherwise, we would have $\alpha^{-1}=0$ and thus $1=\alpha\underbrace{\alpha^{-1}}_{=0}=0$, which would be absurd). Hence, Definition 4.1.19 (applied to α^{-1} instead of α) yields $\left(\alpha^{-1}\right)^{n}=\left(\left(\alpha^{-1}\right)^{-1}\right)^{-n}$ (since n is negative).

But Proposition 4.1.16 **(a)** yields $\left(\alpha^{-1}\right)^{-1}=\alpha$. Thus, $\left(\alpha^{-1}\right)^{n}=\left(\underbrace{\left(\alpha^{-1}\right)^{-1}}_{=\alpha}\right)^{-n}=\alpha^{-n}$, so that $\alpha^{-n}=\left(\alpha^{-1}\right)^{n}$. Hence, $\alpha^{-n}=\left(\alpha^{-1}\right)^{n}$ is proven in Case 3.

We have now proven that $\alpha^{-n}=\left(\alpha^{-1}\right)^{n}$ in all three Cases 1, 2 and 3. Thus, $\alpha^{-n}=\left(\alpha^{-1}\right)^{n}$ always holds. This completes the proof of Proposition 4.1.20 **(g)**.

(h) We must prove that $\alpha^{n+m}=\alpha^{n}\alpha^{m}$ for all nonzero $\alpha\in\mathbb{C}$ and all $n,m\in\mathbb{Z}$. We shall first prove the following less general result:

> *Claim 1:* We have $\alpha^{n+m}=\alpha^{n}\alpha^{m}$ for all nonzero $\alpha\in\mathbb{C}$ and all $n\in\mathbb{N}$ and $m\in\mathbb{Z}$.

[*Proof of Claim 1:* The following proof is very similar to our Second proof of Proposition 4.1.20 **(b)** above.

We shall prove Claim 1 by induction on n:

Induction base: If $\alpha \in \mathbb{C}$ is nonzero, and if $m \in \mathbb{Z}$, then $\underbrace{\alpha^0}_{=1} \alpha^m = 1 \cdot \alpha^m = \alpha^m = \alpha^{0+m}$ (since $m = 0 + m$). In other words, we have $\alpha^{0+m} = \alpha^0 \alpha^m$ for all nonzero $\alpha \in \mathbb{C}$ and all $m \in \mathbb{Z}$. In other words, Claim 1 holds for $n = 0$. This completes the induction base.

Induction step: Let $k \in \mathbb{N}$. Assume that Claim 1 holds for $n = k$. We must prove that Claim 1 holds for $n = k + 1$.

Let $\alpha \in \mathbb{C}$ be nonzero, and let $m \in \mathbb{Z}$. We have assumed that Claim 1 holds for $n = k$. Hence, we can apply Claim 1 to $n = k$. We thus obtain $\alpha^{k+m} = \alpha^k \alpha^m$.

Proposition 4.1.20 **(f)** (applied to $n = k$) yields $\alpha^{k+1} = \alpha\alpha^k$. Also, Proposition 4.1.20 **(f)** (applied to $n = k + m$) yields $\alpha^{(k+m)+1} = \alpha\alpha^{k+m}$.

But $(k + 1) + m = (k + m) + 1$ and hence

$$\alpha^{(k+1)+m} = \alpha^{(k+m)+1} = \alpha \underbrace{\alpha^{k+m}}_{=\alpha^k \alpha^m} = \underbrace{\alpha\alpha^k}_{=\alpha^{k+1}} \alpha^m = \alpha^{k+1}\alpha^m.$$

Now, forget that we fixed m. We thus have shown that $\alpha^{(k+1)+m} = \alpha^{k+1}\alpha^m$ for all nonzero $\alpha \in \mathbb{C}$ and all $m \in \mathbb{Z}$. In other words, Claim 1 holds for $n = k + 1$. This completes the induction step. Thus, Claim 1 is proven by induction.]

Now, let us prove Proposition 4.1.20 **(h)** in full generality: Fix a nonzero $\alpha \in \mathbb{C}$. Fix $n, m \in \mathbb{Z}$. We must prove that $\alpha^{n+m} = \alpha^n \alpha^m$. If $n \in \mathbb{N}$, then this follows from Claim 1. Hence, for the rest of this proof, we WLOG assume that we don't have $n \in \mathbb{N}$. Combining this with $n \in \mathbb{Z}$, we obtain $n \in \mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \ldots\}$. In other words, n is negative. Hence, $-n$ is positive. Thus, $-n \in \mathbb{N}$.

Recall that α^{-1} is the inverse of α; hence, $\alpha\alpha^{-1} = 1$ (by the definition of "inverse"). Hence, $\alpha^{-1} \neq 0$ (since otherwise, we would have $\alpha^{-1} = 0$ and thus $1 = \alpha \underbrace{\alpha^{-1}}_{=0} = 0$, which would be absurd). So we have $\alpha^{-1} \neq 0$ and $-n \in \mathbb{N}$. Hence, Claim 1 (applied to α^{-1}, $-n$ and $-m$ instead of α, n and m) yields

$$\left(\alpha^{-1}\right)^{(-n)+(-m)} = \left(\alpha^{-1}\right)^{-n} \left(\alpha^{-1}\right)^{-m}. \tag{490}$$

Definition 4.1.19 yields $\alpha^n = \left(\alpha^{-1}\right)^{-n}$ (since n is negative). Proposition 4.1.20 **(g)** (applied to $-m$ instead of n) yields $\alpha^{-(-m)} = \left(\alpha^{-1}\right)^{-m}$. In view of $-(-m) = m$, this rewrites as $\alpha^m = \left(\alpha^{-1}\right)^{-m}$. The same argument (applied to $n + m$ instead of m) yields $\alpha^{n+m} = \left(\alpha^{-1}\right)^{-(n+m)}$. Hence,

$$\begin{aligned} \alpha^{n+m} &= \left(\alpha^{-1}\right)^{-(n+m)} = \left(\alpha^{-1}\right)^{(-n)+(-m)} && (\text{since } -(n+m) = (-n) + (-m)) \\ &= \left(\alpha^{-1}\right)^{-n} \left(\alpha^{-1}\right)^{-m} && (\text{by (490)}). \end{aligned}$$

Comparing this with

$$\underbrace{\alpha^n}_{=\left(\alpha^{-1}\right)^{-n}} \underbrace{\alpha^m}_{=\left(\alpha^{-1}\right)^{-m}} = \left(\alpha^{-1}\right)^{-n} \left(\alpha^{-1}\right)^{-m},$$

we obtain $\alpha^{n+m} = \alpha^n \alpha^m$. This completes our proof of Proposition 4.1.20 **(h)**.

(i) Let $\alpha, \beta \in \mathbb{C}$ be nonzero. Let $n \in \mathbb{Z}$. We must prove that $(\alpha\beta)^n = \alpha^n \beta^n$.

If $n \in \mathbb{N}$, then this follows from Proposition 4.1.20 **(c)**. Hence, for the rest of this proof, we WLOG assume that we don't have $n \in \mathbb{N}$. Combining this with $n \in \mathbb{Z}$, we obtain $n \in \mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \ldots\}$. In other words, n is negative. Hence, $-n$ is positive. Thus, $-n \in \mathbb{N}$. Hence, Proposition 4.1.20 **(c)** (applied to $-n$, α^{-1} and β^{-1} instead of n, α and β) yields $\left(\alpha^{-1}\beta^{-1}\right)^{-n} = \left(\alpha^{-1}\right)^{-n} \left(\beta^{-1}\right)^{-n}$.

Proposition 4.1.16 **(b)** yields that $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$. Also, Corollary 4.1.17 shows that $\alpha\beta$ is nonzero. Recall also that n is negative. Thus, Definition 4.1.19 (applied to $\alpha\beta$ instead of α) yields

$$(\alpha\beta)^n = \left(\underbrace{(\alpha\beta)^{-1}}_{=\alpha^{-1}\beta^{-1}}\right)^{-n} = \left(\alpha^{-1}\beta^{-1}\right)^{-n} = \left(\alpha^{-1}\right)^{-n} \left(\beta^{-1}\right)^{-n}. \tag{491}$$

On the other hand, Definition 4.1.19 yields $\alpha^n = \left(\alpha^{-1}\right)^{-n}$ (since n is negative). Similarly, $\beta^n = \left(\beta^{-1}\right)^{-n}$. Multiplying these two equalities, we obtain $\alpha^n\beta^n = \left(\alpha^{-1}\right)^{-n} \left(\beta^{-1}\right)^{-n}$. Comparing this with (491), we find $(\alpha\beta)^n = \alpha^n\beta^n$. This completes our proof of Proposition 4.1.20 **(i)**.

(j) Let $n \in \mathbb{Z}$. We must prove that $1^n = 1$. If $n \in \mathbb{N}$, then this follows from Proposition 4.1.20 **(e)**. Hence, for the rest of this proof, we WLOG assume that we don't have $n \in \mathbb{N}$. Combining this with $n \in \mathbb{Z}$, we obtain $n \in \mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \ldots\}$. In other words, n is negative. Hence, $-n$ is positive. Thus, $-n \in \mathbb{N}$. Hence, Proposition 4.1.20 **(e)** (applied to $-n$ instead of n) yields $1^{-n} = 1$.

Also, $1 \cdot 1 = 1$. Hence, 1 is an inverse of 1 (by the definition of "inverse"). Thus, the inverse of 1 is 1. In other words, $1^{-1} = 1$.

But n is negative. Thus, Definition 4.1.19 (applied to $\alpha = 1$) yields $1^n = \left(\underbrace{1^{-1}}_{=1}\right)^{-n} = 1^{-n} = 1$. Hence, Proposition 4.1.20 **(j)** is proven.

(k) Let $\alpha \in \mathbb{C}$ be nonzero. Let $n \in \mathbb{Z}$.

Proposition 4.1.20 **(h)** (applied to $m = -n$) yields $\alpha^{n+(-n)} = \alpha^n\alpha^{-n}$. Hence, $\alpha^n\alpha^{-n} = \alpha^{n+(-n)} = \alpha^0$ (since $n + (-n) = 0$). Thus, $\alpha^n\alpha^{-n} = \alpha^0 = 1$.

Proposition 4.1.20 **(h)** (applied to $-n$ and n instead of n and m) yields $\alpha^{(-n)+n} = \alpha^{-n}\alpha^n$. Hence, $\alpha^{-n}\alpha^n = \alpha^{(-n)+n} = \alpha^0$ (since $(-n) + n = 0$). Thus, $\alpha^{-n}\alpha^n = \alpha^0 = 1$.

If we had $\alpha^n = 0$, then we would have $\underbrace{\alpha^n}_{=0}\alpha^{-n} = 0$, which would contradict $\alpha^n\alpha^{-n} = 1 \neq 0$. Hence, we cannot have $\alpha^n = 0$. In other words, $\alpha^n \neq 0$. Thus, α^n is nonzero. Hence, the inverse $(\alpha^n)^{-1}$ of α^n is well-defined.

We have $\alpha^n\alpha^{-n} = 1$. This equality shows that α^{-n} is an inverse of α^n (by the definition of "inverse"). In other words, the inverse of α^n is α^{-n}. In other words, $(\alpha^n)^{-1} = \alpha^{-n}$. Thus, Proposition 4.1.20 **(k)** is proven.

(l) We must prove that $(\alpha^n)^m = \alpha^{nm}$ for all nonzero $\alpha \in \mathbb{C}$ and all $n, m \in \mathbb{Z}$.

We shall first prove this in lesser generality:

Claim 2: We have $(\alpha^n)^m = \alpha^{nm}$ for all nonzero $\alpha \in \mathbb{C}$ and all $n \in \mathbb{Z}$ and $m \in \mathbb{N}$.

[*Proof of Claim 2:* The following proof is very similar to our proof of Proposition 4.1.20 **(d)** above.

We shall prove Claim 2 by induction on m:

Induction base: For all $\alpha \in \mathbb{C}$ and $n \in \mathbb{Z}$, we have $(\alpha^n)^0 = 1 = \alpha^0 = \alpha^{n \cdot 0}$ (since $0 = n \cdot 0$). In other words, Claim 2 holds for $m = 0$. This completes the induction base.

Induction step: Let $k \in \mathbb{N}$. Assume that Claim 2 holds for $m = k$. We must prove that Claim 2 holds for $m = k + 1$.

Let $\alpha \in \mathbb{C}$ and $n \in \mathbb{Z}$. Then, $(\alpha^n)^k = \alpha^{nk}$ (since Claim 2 holds for $m = k$). Now, Proposition 4.1.20 **(a)** (applied to α^n and k instead of α and n) yields

$$(\alpha^n)^{k+1} = \alpha^n \underbrace{(\alpha^n)^k}_{=\alpha^{nk}} = \alpha^n \alpha^{nk}.$$

Comparing this with

$$\begin{aligned} \alpha^{n(k+1)} &= \alpha^{n+nk} && \left(\text{since } n\,(k+1) = n + nk\right) \\ &= \alpha^n \alpha^{nk} && \left(\text{by Proposition 4.1.20 } \textbf{(h)}\text{, applied to } m = nk\right), \end{aligned}$$

we obtain $(\alpha^n)^{k+1} = \alpha^{n(k+1)}$.

Now, forget that we fixed α and n. We thus have shown that $(\alpha^n)^{k+1} = \alpha^{n(k+1)}$ for all $\alpha \in \mathbb{C}$ and $n \in \mathbb{Z}$. In other words, Claim 2 holds for $m = k + 1$. Hence, Claim 2 is proven by induction.]

Now, let us prove Proposition 4.1.20 **(l)** in full generality: Fix a nonzero $\alpha \in \mathbb{C}$. Fix $n, m \in \mathbb{Z}$. We must prove that $(\alpha^n)^m = \alpha^{nm}$. If $m \in \mathbb{N}$, then this follows from Claim 2. Hence, for the rest of this proof, we WLOG assume that we don't have $m \in \mathbb{N}$. Combining this with $m \in \mathbb{Z}$, we obtain $m \in \mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \ldots\}$. In other words, m is negative. Hence, $-m$ is positive. Thus, $-m \in \mathbb{N}$. Hence, Claim 2 (applied to $-m$ instead of m) yields

$$(\alpha^n)^{-m} = \alpha^{n(-m)} = \alpha^{-nm} \qquad \left(\text{since } n\,(-m) = -nm\right).$$

But Proposition 4.1.20 **(k)** yields that $(\alpha^n)^{-1} = \alpha^{-n}$. In particular, $(\alpha^n)^{-1}$ is well-defined, so that α^n is invertible, and thus α^n is nonzero. Hence, Proposition 4.1.20 **(k)** (applied to α^n and $-m$ instead of α and n) yields

$$\left((\alpha^n)^{-m}\right)^{-1} = (\alpha^n)^{-(-m)} = (\alpha^n)^m \qquad \left(\text{since } -(-m) = m\right).$$

Thus,

$$(\alpha^n)^m = \left(\underbrace{(\alpha^n)^{-m}}_{=\alpha^{-nm}}\right)^{-1} = \left(\alpha^{-nm}\right)^{-1}.$$

But Proposition 4.1.20 **(k)** (applied to $-nm$ instead of n) yields

$$\left(\alpha^{-nm}\right)^{-1} = \alpha^{-(-nm)} = \alpha^{nm} \qquad \left(\text{since } -(-nm) = nm\right).$$

Hence, $(\alpha^n)^m = \left(\alpha^{-nm}\right)^{-1} = \alpha^{nm}$. This completes the proof of Proposition 4.1.20 **(l)**.

(m) This is proven in the same way as the usual binomial formula (i.e., Theorem 2.17.13) is proven. (The only difference is that we are now calling our two numbers α and β rather than x and y, and that we now need to use Theorem 4.1.2 and Proposition 4.1.20 **(a)** instead of the analogous rules for real numbers.) □

10.90. Solution to Exercise 4.2.1

Solution to Exercise 4.2.1. Write the complex number α in the form $\alpha = (x, y)$ for some $x, y \in \mathbb{R}$. Then, $x, y \in \mathbb{Z}$ (since α is a Gaussian integer). Moreover, from $\alpha = (x, y)$, we obtain $\overline{\alpha} = (x, -y)$ (by the definition of $\overline{\alpha}$). Also, $\overline{\alpha}$ is a Gaussian integer (by Proposition 4.2.5).

From $\overline{\alpha} = (x, -y)$, we obtain

$$-\overline{\alpha} = -(x, -y) = \left(-x, \underbrace{-(-y)}_{=y}\right) = (-x, y)$$

and

$$\begin{aligned}\underbrace{i}_{=(0,1)} \underbrace{\overline{\alpha}}_{=(x,-y)} &= (0,1)(x,-y) = \left(\underbrace{0 \cdot x - 1 \cdot (-y)}_{=y}, \underbrace{0 \cdot (-y) + 1 \cdot x}_{=x}\right) \\ &\qquad \text{(by the definition of the operation } \cdot \text{ on } \mathbb{C}) \\ &= (y, x)\end{aligned}$$

and

$$-\underbrace{i\overline{\alpha}}_{=(y,x)} = -(y, x) = (-y, -x).$$

(a) Proposition 4.2.11 (applied to $\beta = \overline{\alpha}$) shows that we have $\alpha \sim \overline{\alpha}$ if and only if

$$(\alpha = \overline{\alpha} \text{ or } \alpha = -\overline{\alpha} \text{ or } \alpha = i\overline{\alpha} \text{ or } \alpha = -i\overline{\alpha}).$$

Hence, we have ($\alpha = \overline{\alpha}$ or $\alpha = -\overline{\alpha}$ or $\alpha = i\overline{\alpha}$ or $\alpha = -i\overline{\alpha}$) (since we have $\alpha \sim \overline{\alpha}$). Thus, we are in one of the following four cases:

Case 1: We have $\alpha = \overline{\alpha}$.

Case 2: We have $\alpha = -\overline{\alpha}$.

Case 3: We have $\alpha = i\overline{\alpha}$.

Case 4: We have $\alpha = -i\overline{\alpha}$.

Let us first consider Case 1. In this case, we have $\alpha = \overline{\alpha}$. Thus, $(x, y) = \alpha = \overline{\alpha} = (x, -y)$. In other words, $x = x$ and $y = -y$. From $y = -y$, we obtain $2y = 0$, thus $y = 0$. Hence, $\alpha = \left(x, \underbrace{y}_{=0}\right) = (x, 0) = x \cdot \underbrace{(1, 0)}_{=1} = x \cdot 1$. Thus, there exist some $g \in \mathbb{Z}$ and $\tau \in \{1, i, 1+i, 1-i\}$ such that $\alpha = g\tau$ (namely, $g = x$ and $\tau = 1$). Thus, Exercise 4.2.1 **(a)** is solved in Case 1.

Let us next consider Case 2. In this case, we have $\alpha = -\overline{\alpha}$. Thus, $(x, y) = \alpha = -\overline{\alpha} = (-x, y)$. In other words, $x = -x$ and $y = y$. From $x = -x$, we obtain $2x = 0$, thus $x = 0$. Hence, $\alpha = \left(\underbrace{x}_{=0}, y\right) = (0, y) = y \cdot \underbrace{(0, 1)}_{=i} = yi$. Thus, there exist some $g \in \mathbb{Z}$ and $\tau \in \{1, i, 1+i, 1-i\}$ such that $\alpha = g\tau$ (namely, $g = y$ and $\tau = i$). Thus, Exercise 4.2.1 **(a)** is solved in Case 2.

Let us now consider Case 3. In this case, we have $\alpha = i\overline{\alpha}$. Thus, $(x, y) = \alpha = i\overline{\alpha} = (y, x)$. In other words, $x = y$ and $y = x$. Hence, $\alpha = \left(x, \underbrace{y}_{=x}\right) = (x, x) = x \cdot \underbrace{(1, 1)}_{=1+i} = x(1+i)$. Thus, there exist some $g \in \mathbb{Z}$ and $\tau \in \{1, i, 1+i, 1-i\}$ such that $\alpha = g\tau$ (namely, $g = x$ and $\tau = 1+i$). Thus, Exercise 4.2.1 **(a)** is solved in Case 3.

Let us finally consider Case 4. In this case, we have $\alpha = -i\overline{\alpha}$. Thus, $(x, y) = \alpha = -i\overline{\alpha} = (-y, -x)$. In other words, $x = -y$ and $y = -x$. Hence, $\alpha = \left(x, \underbrace{y}_{=-x}\right) = (x, -x) = x \cdot \underbrace{(1, -1)}_{=1-i} = x(1-i)$. Thus, there exist some $g \in \mathbb{Z}$ and $\tau \in \{1, i, 1+i, 1-i\}$ such that $\alpha = g\tau$ (namely, $g = x$ and $\tau = 1-i$). Thus, Exercise 4.2.1 **(a)** is solved in Case 4.

We have now solved Exercise 4.2.1 **(a)** in all four Cases 1, 2, 3 and 4. Hence, Exercise 4.2.1 **(a)** is solved (since these four Cases cover all possibilities).

(b) Let $g \in \mathbb{Z}$ and $\tau \in \{1, i, 1+i, 1-i\}$ be such that $\alpha = g\tau$. We must prove that $\operatorname{N}(\alpha) \in \{g^2, 2g^2\}$.

We have $1 + i = (1, 1)$. Thus, the definition of $\operatorname{N}(1+i)$ yields $\operatorname{N}(1+i) = 1^2 + 1^2 = 2$.

We have $1 - i = (1, -1)$. Thus, the definition of $\operatorname{N}(1-i)$ yields $\operatorname{N}(1-i) = 1^2 + (-1)^2 = 2$.

We have $i = (0, 1)$. Thus, the definition of $\operatorname{N}(i)$ yields $\operatorname{N}(i) = 0^2 + 1^2 = 1$.

Proposition 4.1.23 (applied to $a = 1$) yields $\operatorname{N}(1_{\mathbb{C}}) = 1^2 = 1$. In other words, $\operatorname{N}(1) = 1$ (since we identify $1_{\mathbb{C}}$ with 1).

Now, from $\tau \in \{1, i, 1+i, 1-i\}$, we obtain

$$\operatorname{N}(\tau) \in \left\{\underbrace{\operatorname{N}(1)}_{=1}, \underbrace{\operatorname{N}(i)}_{=1}, \underbrace{\operatorname{N}(1+i)}_{=2}, \underbrace{\operatorname{N}(1-i)}_{=2}\right\} = \{1, 1, 2, 2\} = \{1, 2\}.$$

Proposition 4.1.23 (applied to $a = g$) yields $\operatorname{N}(g_{\mathbb{C}}) = g^2$. In other words, $\operatorname{N}(g) = g^2$ (since we identify $g_{\mathbb{C}}$ with g).

Now, Proposition 4.1.27 **(d)** (applied to g and τ instead of α and β) yields

$$\begin{aligned}\operatorname{N}(g\tau) &= \underbrace{\operatorname{N}(g)}_{=g^2} \cdot \operatorname{N}(\tau) = g^2 \cdot \operatorname{N}(\tau) = \operatorname{N}(\tau) \cdot g^2 \in \left\{\underbrace{1g^2}_{=g^2}, 2g^2\right\} \qquad (\text{since } \operatorname{N}(\tau) \in \{1, 2\}) \\ &= \left\{g^2, 2g^2\right\}.\end{aligned}$$

In view of $\alpha = g\tau$, this rewrites as $\operatorname{N}(\alpha) \in \{g^2, 2g^2\}$. This solves Exercise 4.2.1 **(b)**.

(c) Assume the contrary. Thus, $\operatorname{N}(\alpha)$ is an odd prime.

Exercise 4.2.1 **(b)** yields $\operatorname{N}(\alpha) \in \{g^2, 2g^2\}$. In other words, we have $\operatorname{N}(\alpha) = g^2$ or $\operatorname{N}(\alpha) = 2g^2$. But if we had $\operatorname{N}(\alpha) = 2g^2$, then $\operatorname{N}(\alpha)$ would be even (since $g^2 \in \mathbb{Z}$), which would contradict the fact that $\operatorname{N}(\alpha)$ is odd. Hence, we cannot have $\operatorname{N}(\alpha) = 2g^2$. Thus, we must have $\operatorname{N}(\alpha) = g^2$ (because we know that $\operatorname{N}(\alpha) = g^2$ or $\operatorname{N}(\alpha) = 2g^2$). Hence, $\operatorname{N}(\alpha)$ is the square of an integer (since g is an integer), i.e., a perfect square.

But a prime can never be a perfect square[311]. Thus, $\mathrm{N}(\alpha)$ cannot be a perfect square (since $\mathrm{N}(\alpha)$ is prime). This contradicts the fact that $\mathrm{N}(\alpha)$ is a perfect square. This contradiction shows that our assumption was wrong; hence, Exercise 4.2.1 **(c)** is solved. □

10.91. Solution to Exercise 4.2.2

Solution to Exercise 4.2.2. We are in one of the following two cases:

Case 1: We have $\beta \neq 0$.

Case 2: We have $\beta = 0$.

Let us first consider Case 1. In this case, we have $\beta \neq 0$. Thus, the complex number β has an inverse β^{-1} (by Definition 4.1.13). (This β^{-1} may and may not be a Gaussian integer.)

We have $\alpha \mid \beta$. In other words, there exists a Gaussian integer γ such that $\beta = \alpha\gamma$ (by Definition 4.2.17). Consider this γ.

We have $\beta \mid \alpha$. In other words, there exists a Gaussian integer δ such that $\alpha = \beta\delta$ (by Definition 4.2.17). Consider this δ.

Now, $\beta = \underbrace{\alpha}_{=\beta\delta} \gamma = \beta\delta\gamma$. But $\beta^{-1}\beta = 1$. Comparing this with

$$\beta^{-1} \underbrace{\beta}_{=\beta\delta\gamma} = \underbrace{\beta^{-1}\beta}_{=1} \delta\gamma = \delta\gamma,$$

we obtain $\delta\gamma = 1$. In other words, γ is an inverse of δ (by Definition 4.1.11). Thus, the Gaussian integer δ has an inverse in $\mathbb{Z}[i]$ (namely, γ). In other words, the Gaussian integer δ is invertible in $\mathbb{Z}[i]$ (by the definition of "invertible in $\mathbb{Z}[i]$"). In other words, δ is a unit (by the definition of "unit"). Hence, from $\alpha = \beta\delta = \delta\beta$, we conclude that $\alpha \sim \beta$ (by the definition of unit-equivalence). Thus, Exercise 4.2.2 is solved in Case 1.

Let us now consider Case 2. In this case, we have $\beta = 0$. But we have $\beta \mid \alpha$. In other words, there exists a Gaussian integer γ such that $\alpha = \beta\gamma$ (by Definition 4.2.17). Consider this γ. Hence, $\alpha = \underbrace{\beta}_{=0} \gamma = 0\gamma = 0 = \beta$ (since $\beta = 0$). Thus, $\alpha = \beta = 1\beta$, so that $\alpha \sim \beta$ (by the definition of unit-equivalence, since 1 is a unit). Hence, Exercise 4.2.2 is solved in Case 2.

Now, we have solved Exercise 4.2.2 in both Cases 1 and 2. Hence, Exercise 4.2.2 always holds. □

[311] *Proof.* Let p be a prime. We must prove that p cannot be a perfect square.

Indeed, assume the contrary. Thus, p is a perfect square. In other words, $p = m^2$ for some integer m. Consider this m. Let $n = |m|$. Then, n is a nonnegative integer (since m is an integer) and satisfies $n^2 = |m|^2 = m^2 = p$.

But p is a prime. Thus, $p > 1$. Hence, $n^2 = p > 1 = 1^2$. We can take square roots on both sides of this inequality, and obtain $n > 1$ (since n and 1 are nonnegative). Hence, n is positive. Thus, we can multiply the inequality $n > 1$ by n, and obtain $nn > n$. Hence, $n < nn = n^2 = p$, so that $n \neq p$. Also, $n \neq 1$ (since $n > 1$). But n is positive and is a divisor of p (since $n \mid nn = p$). Thus, n is a positive divisor of p. But the only positive divisors of p are 1 and p (since p is prime). Hence, n is either 1 or p (since n is a positive divisor of p). This contradicts the fact that $n \neq 1$ and $n \neq p$. This contradiction shows that our assumption was false.

Hence, we have proven that p cannot be a perfect square. Qed.

10.92. Solution to Exercise 4.2.3

Solution to Exercise 4.2.3. $\Longrightarrow$: Assume that $\alpha \sim \beta$. We must prove that $(\alpha \mid \beta$ and $\beta \mid \alpha)$.

The relation $\sim$ is an equivalence relation (by Proposition 4.2.8), and thus is symmetric (since every equivalence relation is symmetric). Hence, from $\alpha \sim \beta$, we obtain $\beta \sim \alpha$.

We have $\alpha \sim \beta$. In other words, $\alpha = \gamma\beta$ for some unit $\gamma \in \mathbb{Z}[i]$ (by the definition of unit-equivalence). Consider this γ. From $\alpha = \gamma\beta$, we obtain $\beta \mid \alpha$ (since γ is a Gaussian integer). The same argument (with the roles of α and β swapped) yields $\alpha \mid \beta$ (since $\beta \sim \alpha$). Hence, $(\alpha \mid \beta$ and $\beta \mid \alpha)$. This proves the "$\Longrightarrow$" direction of Exercise 4.2.3.

$\Longleftarrow$: We have the logical implication $(\alpha \sim \beta) \Longleftarrow (\alpha \mid \beta$ and $\beta \mid \alpha)$ (due to Exercise 4.2.2). Thus, the "$\Longleftarrow$" direction of Exercise 4.2.3 is proven. □

10.93. Solution to Exercise 4.2.4

Solution to Exercise 4.2.4. The solution to Exercise 4.2.4 is completely analogous to the above solution to Exercise 2.2.3. (As usual, you need to make the obvious changes: Replace all Roman letters $a, b, c, a_1, b_1, a_2, b_2$ by Greek letters $\alpha, \beta, \gamma, \alpha_1, \beta_1, \alpha_2, \beta_2$; replace integers by Gaussian integers; replace the reference to Proposition 2.2.4 by a reference to its analogue for Gaussian integers (which is Proposition 4.2.20). The resulting argument will make use of the fact that we can divide any complex number by any nonzero complex number; but we know this fact from Definition 4.1.14 **(a)**.) □

10.94. Solution to Exercise 4.2.5

Solution to Exercise 4.2.5. The solution to Exercise 4.2.5 is completely analogous to the above solution to Exercise 2.2.4. (Of course, you will have to replace the letter n by ν, and replace integers by Gaussian integers.) □

10.95. Solution to Exercise 4.2.6

Solution to Exercise 4.2.6. The following argument is an analogue of the Second solution to Exercise 2.2.5 we gave above:

We have $\gamma = 1\gamma$. Hence, there exists a Gaussian integer δ such that $\gamma = 1\delta$ (namely, $\delta = \gamma$). In other words, $1 \mid \gamma$ (by the definition of divisibility). But we also have $\gamma \mid 1$ (by assumption). Hence, Exercise 4.2.2 (applied to $\alpha = \gamma$ and $\beta = 1$) yields $\gamma \sim 1$.

But Proposition 4.2.14 (applied to $\alpha = \gamma$) shows that $\gamma \sim 1$ if and only if γ is a unit. Hence, γ is a unit (since $\gamma \sim 1$).

Proposition 4.2.10 shows that the units are $1, -1, i, -i$. Hence, γ is either 1 or -1 or i or $-i$ (since γ is a unit). This solves Exercise 4.2.6. □

10.96. Solution to Exercise 4.2.7

Solution to Exercise 4.2.7. We have $\alpha \mid \beta$. In other words, there exists a Gaussian integer γ such that $\beta = \alpha\gamma$ (by Definition 4.2.17). Consider this γ, and denote it by δ. Thus, δ is a Gaussian integer and satisfies $\beta = \alpha\delta$.

From $\beta = \alpha\delta$, we obtain $\overline{\beta} = \overline{\alpha\delta} = \overline{\alpha} \cdot \overline{\delta}$ (by Proposition 4.1.27 **(c)**, applied to δ instead of β). Also, $\overline{\delta}$ is a Gaussian integer (by Proposition 4.2.5, applied to δ instead of α). Hence, there exists a Gaussian integer γ such that $\overline{\beta} = \overline{\alpha}\gamma$ (namely, $\gamma = \overline{\delta}$). In other words, $\overline{\alpha} \mid \overline{\beta}$ (by Definition 4.2.17). This solves Exercise 4.2.7. □

10.97. Solution to Exercise 4.2.8

Solution to Exercise 4.2.8. The relation $\sim$ on $\mathbb{Z}[i]$ is an equivalence relation (by Proposition 4.2.8), and thus is symmetric.

(a) Assume that $\beta \sim \gamma$. But Exercise 4.2.3 (applied to β and γ instead of α and β) shows that we have the logical equivalence $(\beta \sim \gamma) \iff (\beta \mid \gamma \text{ and } \gamma \mid \beta)$. Hence, we have $(\beta \mid \gamma \text{ and } \gamma \mid \beta)$ (since $\beta \sim \gamma$). Thus, $\beta \mid \gamma$ and $\gamma \mid \beta$.

Thus, in particular, $\beta \mid \gamma$. Hence, if $\alpha \mid \beta$, then $\alpha \mid \gamma$ (by Proposition 4.2.20 **(b)**). In other words, we have proven the implication $(\alpha \mid \beta) \Longrightarrow (\alpha \mid \gamma)$. The same argument (with the roles of β and γ switched) proves the implication $(\alpha \mid \gamma) \Longrightarrow (\alpha \mid \beta)$ (since $\gamma \mid \beta$). Combining these two implications, we obtain the equivalence $(\alpha \mid \beta) \iff (\alpha \mid \gamma)$. This solves Exercise 4.2.8 **(a)**.

(b) Assume that $\alpha \sim \beta$. But Exercise 4.2.3 shows that we have the logical equivalence $(\alpha \sim \beta) \iff (\alpha \mid \beta \text{ and } \beta \mid \alpha)$. Hence, we have $(\alpha \mid \beta \text{ and } \beta \mid \alpha)$ (since $\alpha \sim \beta$). Thus, $\alpha \mid \beta$ and $\beta \mid \alpha$.

Thus, in particular, $\alpha \mid \beta$. Hence, if $\beta \mid \gamma$, then $\alpha \mid \gamma$ (by Proposition 4.2.20 **(b)**). In other words, we have proven the implication $(\beta \mid \gamma) \Longrightarrow (\alpha \mid \gamma)$. The same argument (with the roles of α and β switched) proves the implication $(\alpha \mid \gamma) \Longrightarrow (\beta \mid \gamma)$ (since $\beta \mid \alpha$). Combining these two implications, we obtain the equivalence $(\alpha \mid \gamma) \iff (\beta \mid \gamma)$. This solves Exercise 4.2.8 **(b)**.

(c) Exercise 4.2.8 **(a)** (applied to γ and δ instead of β and γ) yields the logical equivalence $(\alpha \mid \gamma) \iff (\alpha \mid \delta)$ (since $\gamma \sim \delta$). Exercise 4.2.8 **(b)** (applied to δ instead of γ) yields the logical equivalence $(\alpha \mid \delta) \iff (\beta \mid \delta)$ (since $\alpha \sim \beta$). Hence, we obtain the following chain of equivalences:

$$(\alpha \mid \gamma) \iff (\alpha \mid \delta) \iff (\beta \mid \delta).$$

This solves Exercise 4.2.8 **(c)**. □

10.98. Solution to Exercise 4.2.9

Solution to Exercise 4.2.9. Proposition 4.2.8 shows that the relation $\sim$ on $\mathbb{Z}[i]$ is an equivalence relation. Thus, this relation is reflexive and symmetric.

We have $\alpha \mid \beta$. In other words, there exists a Gaussian integer γ such that $\beta = \alpha\gamma$ (by Definition 4.2.17). Consider this γ, and denote it by δ. Thus, δ is a Gaussian integer and satisfies $\beta = \alpha\delta$.

We must prove that $\alpha \sim \beta$. If $\mathrm{N}(\alpha) = 0$, then this is easy to see[312]. Thus, for the rest of this proof, we WLOG assume that we don't have $\mathrm{N}(\alpha) = 0$. Hence, $\mathrm{N}(\alpha) \neq 0$.

[312] *Proof.* Assume that $\mathrm{N}(\alpha) = 0$. Thus, Proposition 4.1.22 **(b)** yields $\alpha = 0$. Hence, $\beta = \underbrace{\alpha}_{=0}\delta = 0\delta = 0 = \alpha$. But the relation $\sim$ on $\mathbb{Z}[i]$ is reflexive. Hence, $\alpha \sim \alpha$. This rewrites as $\alpha \sim \beta$ (since $\beta = \alpha$). Thus, we have proven that $\alpha \sim \beta$ under the assumption that $\mathrm{N}(\alpha) = 0$.

Proposition 4.1.27 **(d)** (applied to δ instead of β) yields $\operatorname{N}(\alpha\delta) = \operatorname{N}(\alpha) \cdot \operatorname{N}(\delta)$. In view of $\beta = \alpha\delta$, this rewrites as $\operatorname{N}(\beta) = \operatorname{N}(\alpha) \cdot \operatorname{N}(\delta)$. Thus, $\operatorname{N}(\alpha) \cdot \operatorname{N}(\delta) = \operatorname{N}(\beta) = \operatorname{N}(\alpha)$. We can divide both sides of this equality by $\operatorname{N}(\alpha)$ (since $\operatorname{N}(\alpha) \neq 0$). Thus, we find $\operatorname{N}(\delta) = 1$.

But Proposition 4.2.9 **(b)** (applied to δ instead of α) shows that we have $\operatorname{N}(\delta) = 1$ if and only if δ is a unit. Hence, δ is a unit (since $\operatorname{N}(\delta) = 1$). This unit δ satisfies $\beta = \alpha\delta = \delta\alpha$. Thus, we have $\beta = \gamma\alpha$ for some unit $\gamma \in \mathbb{Z}[i]$ (namely, for $\gamma = \delta$). In other words, we have $\beta \sim \alpha$ (by the definition of the relation $\sim$ on $\mathbb{Z}[i]$). Hence, $\alpha \sim \beta$ (since the relation $\sim$ on $\mathbb{Z}[i]$ is symmetric). This solves Exercise 4.2.9. □

10.99. Solution to Exercise 4.2.10

Solution to Exercise 4.2.10. We have $a, b \in \mathbb{Z}$ (since (a,b) is a Gaussian integer) and $c, d \in \mathbb{Z}$ (since (c,d) is a Gaussian integer). Thus, all of a, b, c, d are integers. Hence, the statements "$a \equiv c \bmod n$" and "$b \equiv d \bmod n$" make sense. Moreover, $a - c, b - d \in \mathbb{Z}$ (since $a, b, c, d \in \mathbb{Z}$); thus, $(a - c, b - d)$ is a Gaussian integer. Proposition 4.2.18 (applied to n and $(a - c, b - d)$ instead of a and β) yields that we have $n \mid (a - c, b - d)$ if and only if n divides both $a - c$ and $b - d$. In other words, we have the following logical equivalence:

$$(n \mid (a - c, b - d)) \iff (n \text{ divides both } a - c \text{ and } b - d).$$

Now, we have the following chain of logical equivalences:

$$\begin{aligned}
& ((a,b) \equiv (c,d) \bmod n) \\
\iff & \left(n \mid \underbrace{(a,b) - (c,d)}_{=(a-c,b-d)} \right) \qquad \text{(by Definition 4.2.21)} \\
\iff & (n \mid (a - c, b - d)) \iff (n \text{ divides both } a - c \text{ and } b - d) \\
\iff & \left(\underbrace{n \mid a - c}_{\substack{\iff (a \equiv c \bmod n) \\ \text{(by Definition 2.3.1)}}} \quad \text{and} \quad \underbrace{n \mid b - d}_{\substack{\iff (b \equiv d \bmod n) \\ \text{(by Definition 2.3.1)}}} \right) \\
\iff & (a \equiv c \bmod n \text{ and } b \equiv d \bmod n).
\end{aligned}$$

This solves Exercise 4.2.10. □

10.100. Solution to Exercise 4.2.11

Solution to Exercise 4.2.11. **(a)** The solution to Exercise 4.2.11 **(a)** is analogous to the proof of Example 3.2.5 (with the only difference that we have to replace Roman letters by Greek letters, replace integers by Gaussian integers, and use Proposition 4.2.23 instead of Proposition 2.3.4).

(b) We must prove the following two claims:

Claim 1: The equivalence classes of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) are the classes $[a + bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0, 1, \ldots, n-1\}^2$.

Claim 2: The n^2 classes $[a+bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$ are distinct.

Let us start with the proof of Claim 2:

[*Proof of Claim 2:* Let $(a,b), (c,d) \in \{0,1,\ldots,n-1\}^2$ be two pairs such that $[a+bi]_{\underset{n}{\equiv}} = [c+di]_{\underset{n}{\equiv}}$. We shall prove that $(a,b) = (c,d)$.

From $(a,b), (c,d) \in \{0,1,\ldots,n-1\}^2$, we conclude that $a,b,c,d \in \{0,1,\ldots,n-1\} \subseteq \mathbb{Z}$.

Proposition 4.1.8 yields $(a,b) = a+bi$ (since a and b are reals). Thus, $[(a,b)]_{\underset{n}{\equiv}} = [a+bi]_{\underset{n}{\equiv}}$. Similarly, $[(c,d)]_{\underset{n}{\equiv}} = [c+di]_{\underset{n}{\equiv}}$. Hence,

$$[(a,b)]_{\underset{n}{\equiv}} = [a+bi]_{\underset{n}{\equiv}} = [c+di]_{\underset{n}{\equiv}} = [(c,d)]_{\underset{n}{\equiv}}.$$

But Theorem 3.3.5 **(e)** (applied to $\mathbb{Z}[i]$, $\underset{n}{\equiv}$, (a,b) and (c,d) instead of S, $\sim$, x and y) shows that we have $(a,b) \underset{n}{\equiv} (c,d)$ if and only if $[(a,b)]_{\underset{n}{\equiv}} = [(c,d)]_{\underset{n}{\equiv}}$. Hence, $(a,b) \underset{n}{\equiv} (c,d)$ (since we have $[(a,b)]_{\underset{n}{\equiv}} = [(c,d)]_{\underset{n}{\equiv}}$). In other words, $(a,b) \equiv (c,d) \mod n$ (by the definition of the relation $\underset{n}{\equiv}$ on $\mathbb{Z}[i]$).

But (a,b) and (c,d) are two Gaussian integers (since $a,b,c,d \in \mathbb{Z}$). Hence, Exercise 4.2.10 shows that we have the following logical equivalence:

$$((a,b) \equiv (c,d) \mod n) \iff (a \equiv c \mod n \text{ and } b \equiv d \mod n).$$

Thus, we have $(a \equiv c \mod n$ and $b \equiv d \mod n)$ (since we have $(a,b) \equiv (c,d) \mod n$).

Now, $a \in \{0,1,\ldots,n-1\}$ and $a \equiv c \mod n$. Hence, Corollary 2.6.9 **(c)** (applied to c and a instead of u and c) yields $a = c\%n$. On the other hand, $c \in \{0,1,\ldots,n-1\}$ and $c \equiv c \mod n$. Hence, Corollary 2.6.9 **(c)** (applied to c and c instead of u and c) yields $c = c\%n$. Comparing this with $a = c\%n$, we obtain $a = c$. The same argument (but with a and c replaced by b and d) yields $b = d$. Hence, $\left(\underbrace{a}_{=c}, \underbrace{b}_{=d}\right) = (c,d)$.

Now, forget that we fixed $(a,b), (c,d)$. We thus have shown that if $(a,b), (c,d) \in \{0,1,\ldots,n-1\}^2$ are two pairs such that $[a+bi]_{\underset{n}{\equiv}} = [c+di]_{\underset{n}{\equiv}}$, then $(a,b) = (c,d)$. In other words, the n^2 classes $[a+bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$ are distinct. This proves Claim 2.]

[*Proof of Claim 1:* Let ξ be an equivalence class of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$). Thus, $\xi = [\alpha]_{\underset{n}{\equiv}}$ for some $\alpha \in \mathbb{Z}[i]$ (by the definition of an equivalence class). Consider this α. Write the complex number α as $\alpha = (x,y)$ for some $x,y \in \mathbb{R}$. Then, $x,y \in \mathbb{Z}$ (since α is a Gaussian integer).

Corollary 2.6.9 **(a)** (applied to $u = x$) shows that $x\%n \in \{0,1,\ldots,n-1\}$ and $x\%n \equiv x \mod n$. Corollary 2.6.9 **(a)** (applied to $u = y$) shows that $y\%n \in \{0,1,\ldots,n-1\}$ and $y\%n \equiv y \mod n$. From $x\%n \in \{0,1,\ldots,n-1\}$ and $y\%n \in \{0,1,\ldots,n-1\}$, we obtain $(x\%n, y\%n) \in \{0,1,\ldots,n-1\}^2$.

Also, of course, $x\%n, y\%n \in \mathbb{Z}$; thus, the complex number $(x\%n, y\%n)$ is a Gaussian integer. Denote this Gaussian integer by β. Thus, $\beta = (x\%n, y\%n) = x\%n + (y\%n)\,i$ (by Proposition 4.1.8, applied to $(a,b) = (x\%n, y\%n)$). Hence, β is a Gaussian integer of the form $a+bi$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$ (namely, for $(a,b) = (x\%n, y\%n)$). Thus, the equivalence class $[\beta]_{\underset{n}{\equiv}}$ is one of the classes $[a+bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$.

Recall that $(x\%n, y\%n)$ is a Gaussian integer. Hence, Exercise 4.2.10 (applied to $(a,b) = (x\%n, y\%n)$ and $(c,d) = (x,y)$) shows that we have the following logical equivalence:

$$((x\%n, y\%n) \equiv (x,y) \bmod n) \iff (x\%n \equiv x \bmod n \text{ and } y\%n \equiv y \bmod n).$$

Hence, we have $(x\%n, y\%n) \equiv (x,y) \bmod n$ (since we have $x\%n \equiv x \bmod n$ and $y\%n \equiv y \bmod n$). In view of $(x,y) = \alpha$ and $(x\%n, y\%n) = \beta$, this rewrites as $\beta \equiv \alpha \bmod n$. In other words, $\beta \underset{n}{\equiv} \alpha$ (by the definition of the relation $\underset{n}{\equiv}$ on $\mathbb{Z}[i]$).

But Theorem 3.3.5 **(e)** (applied to $\mathbb{Z}[i]$, $\underset{n}{\equiv}$, β and α instead of S, $\sim$, x and y) shows that we have $\beta \underset{n}{\equiv} \alpha$ if and only if $[\beta]_{\underset{n}{\equiv}} = [\alpha]_{\underset{n}{\equiv}}$. Hence, we have $[\beta]_{\underset{n}{\equiv}} = [\alpha]_{\underset{n}{\equiv}}$ (since we have $\beta \underset{n}{\equiv} \alpha$). Comparing this with $\xi = [\alpha]_{\underset{n}{\equiv}}$, we obtain $\xi = [\beta]_{\underset{n}{\equiv}}$.

But recall that $[\beta]_{\underset{n}{\equiv}}$ is one of the classes $[a+bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$. In view of $\xi = [\beta]_{\underset{n}{\equiv}}$, this rewrites as follows: ξ is one of the classes $[a+bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$.

Forget that we fixed ξ. We thus have proven that if ξ is any equivalence class of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$), then ξ is one of the classes $[a+bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$. In other words, each equivalence class of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) is one of the classes $[a+bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$. Conversely, of course, each of the latter classes is an equivalence class of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$). Combining these two statements, we conclude that the equivalence classes of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) are the classes $[a+bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$. This proves Claim 1.]

Having proven both Claim 1 and Claim 2, we now conclude that the equivalence classes of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) are the n^2 classes $[a+bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$, and that these n^2 classes are all distinct. This solves Exercise 4.2.11. □

10.101. Solution to Exercise 5.4.1

In order to solve Exercise 5.4.1, we need to prove Proposition 5.4.9.

Proof of Proposition 5.4.9. The proofs of these rules are analogous to the proofs of the corresponding rules for rationals – at least if you know the right proofs of the latter.

Here are the proofs in detail:

First of all, let us prove (173). Indeed, each $a \in \mathbb{K}$ satisfies

$$\begin{aligned} 0a &= \underbrace{a+a+\cdots+a}_{0\text{ times}} && (\text{by the definition of } 0a\text{, since } 0 \geq 0) \\ &= (\text{empty sum}) = 0_{\mathbb{K}} && (\text{since empty sums of elements of } \mathbb{K} \text{ are defined to be } 0_{\mathbb{K}}). \end{aligned}$$

Thus, (173) is proven.

Next, let us prove (172). Indeed, each $a \in \mathbb{K}$ satisfies

$$\begin{aligned} 1a &= \underbrace{a + a + \cdots + a}_{1 \text{ times}} \qquad \left(\text{by the definition of } 1a \text{, since } 1 \geq 0\right) \\ &= a. \end{aligned}$$

Thus, (172) is proven.

Next, let us prove (174). Indeed, each $a \in \mathbb{K}$ satisfies

$$\begin{aligned} \left(-1\right) a &= -\left(\underbrace{a + a + \cdots + a}_{-(-1) \text{ times}}\right) \qquad \left(\text{by the definition of } \left(-1\right) a \text{, since } -1 < 0\right) \\ &= -\underbrace{\left(\underbrace{a + a + \cdots + a}_{1 \text{ times}}\right)}_{=a} \qquad \left(\text{since } -\left(-1\right) = 1\right) \\ &= -a. \end{aligned}$$

Thus, (174) is proven.

Next, recall that Proposition 5.4.5 **(c)** yields $-0 = 0$; in other words, $-0_{\mathbb{K}} = 0_{\mathbb{K}}$.

We organize the rest of the proof of Proposition 5.4.9 as a sequence of claims, each bringing us one step further to the goals:

Claim 1: We have $na = -\left(\left(-n\right) a\right)$ for all $a \in \mathbb{K}$ and all negative $n \in \mathbb{Z}$.

[*Proof of Claim 1:* Let $a \in \mathbb{K}$. Let $n \in \mathbb{Z}$ be negative. Thus, $n < 0$; hence, the definition of na yields

$$na = -\left(\underbrace{a + a + \cdots + a}_{-n \text{ times}}\right). \tag{492}$$

But $-n > 0$ (since $n < 0$) and thus $-n \in \mathbb{N}$. Hence, the definition of $\left(-n\right) a$ yields

$$\left(-n\right) a = \underbrace{a + a + \cdots + a}_{-n \text{ times}}.$$

Thus,

$$-\left(\left(-n\right) a\right) = -\left(\underbrace{a + a + \cdots + a}_{-n \text{ times}}\right) = na \qquad \left(\text{by (492)}\right).$$

This proves Claim 1.]

Claim 2: We have $\left(-n\right) a = -\left(na\right)$ for all $a \in \mathbb{K}$ and $n \in \mathbb{Z}$.

[*Proof of Claim 2:* Let $a \in \mathbb{K}$ and $n \in \mathbb{Z}$. We are in one of the following three cases:

Case 1: We have $n > 0$.

Case 2: We have $n = 0$.

Case 3: We have $n < 0$.

Let us first consider Case 1. In this case, we have $n > 0$. Hence, $-n < 0$. In other words, $-n$ is negative. Thus, Claim 1 (applied to $-n$ instead of n) yields $(-n) a = -\left(\underbrace{(-(-n))}_{=n} a\right) = -(na)$. Thus, Claim 2 is proven in Case 1.

Let us next consider Case 2. In this case, we have $n = 0$. Thus, $na = 0a = 0_{\mathbb{K}}$ (by (173)). Hence, $-(na) = -0_{\mathbb{K}} = 0_{\mathbb{K}}$. Comparing this with $\left(-\underbrace{n}_{=0}\right) a = \underbrace{(-0)}_{=0} a = 0a = 0_{\mathbb{K}}$, we obtain $(-n) a = -(na)$. Thus, Claim 2 is proven in Case 2.

Let us finally consider Case 3. In this case, we have $n < 0$. Thus, n is negative. Hence, Claim 1 yields $na = -((-n) a)$. Thus, $-(na) = -(-((-n) a)) = (-n) a$ (by Proposition 5.4.5 **(e)**, applied to $(-n) a$, 0 and 0 instead of a, b and c). Thus, $(-n) a = -(na)$. Hence, Claim 2 is proven in Case 3.

Thus, we have proven Claim 2 in all three Cases 1, 2 and 3. Hence, Claim 2 is proven.]

Claim 3: We have $(n+m) a = na + ma$ for all $a \in \mathbb{K}$ and $n, m \in \mathbb{N}$.

[*Proof of Claim 3:* Let $a \in \mathbb{K}$ and $n, m \in \mathbb{N}$. We have $n \in \mathbb{N}$ and thus $n \geq 0$; thus, the definition of na yields

$$na = \underbrace{a + a + \cdots + a}_{n \text{ times}}.$$

The same argument (applied to m instead of n) yields

$$ma = \underbrace{a + a + \cdots + a}_{m \text{ times}}.$$

Adding these two equalities together, we find

$$na + ma = \underbrace{a + a + \cdots + a}_{n \text{ times}} + \underbrace{a + a + \cdots + a}_{m \text{ times}} = \underbrace{a + a + \cdots + a}_{n+m \text{ times}}. \tag{493}$$

On the other hand, $n + m \in \mathbb{N}$ (since $n \in \mathbb{N}$ and $m \in \mathbb{N}$); thus, the definition of $(n+m) a$ yields

$$(n+m) a = \underbrace{a + a + \cdots + a}_{n+m \text{ times}}.$$

Comparing this with (493), we obtain $(n+m) a = na + ma$. This proves Claim 3.]

Claim 4: We have $(n-m) a = na - ma$ for all $a \in \mathbb{K}$ and $n, m \in \mathbb{N}$.

[*Proof of Claim 4:* Let $a \in \mathbb{K}$ and $n, m \in \mathbb{N}$. We are in one of the following two cases:

Case 1: We have $n \geq m$.

Case 2: We have $n < m$.

Let us first consider Case 1. In this case, we have $n \geq m$. Thus, $n - m \geq 0$. Hence, $n - m \in \mathbb{N}$. Thus, Claim 3 (applied to m and $n - m$ instead of n and m) yields

$$(m + (n-m)) a = ma + (n-m) a.$$

In view of $m + (n - m) = n$, this rewrites as $na = ma + (n - m)\,a$. But Proposition 5.4.5 **(a)** (applied to na, ma and $(n - m)\,a$ instead of a, b and c) yields that we have $na - ma = (n - m)\,a$ if and only if $na = ma + (n - m)\,a$. Hence, we have $na - ma = (n - m)\,a$ (since $na = ma + (n - m)\,a$). In other words, $(n - m)\,a = na - ma$. Thus, Claim 4 is proven in Case 1.

Let us now consider Case 2. In this case, we have $n < m$. Thus, $m - n > 0$. Hence, $m - n \in \mathbb{N}$. Thus, Claim 3 (applied to $m - n$ instead of m) yields $(n + (m - n))\,a = na + (m - n)\,a$. In view of $n + (m - n) = m$, this rewrites as $ma = na + (m - n)\,a$. But Proposition 5.4.5 **(a)** (applied to ma, na and $(m - n)\,a$ instead of a, b and c) yields that we have $ma - na = (m - n)\,a$ if and only if $ma = na + (m - n)\,a$. Hence, we have

$$ma - na = (m - n)\,a \qquad (494)$$

(since $ma = na + (m - n)\,a$).

But Claim 2 (applied to $m - n$ instead of n) yields

$$(-(m - n))\,a = -\underbrace{((m - n)\,a)}_{\substack{=ma-na \\ \text{(by (494))}}} = -(ma - na) = na - ma$$

(by Proposition 5.4.5 **(i)**, applied to ma, na and 0 instead of a, b and c). In view of $-(m - n) = n - m$, this rewrites as $(n - m)\,a = na - ma$. Hence, Claim 4 is proven in Case 2.

We have now proven Claim 4 in both Cases 1 and 2. Hence, Claim 4 is proven.]

Next let us generalize Claim 3 by allowing m to be negative:

> *Claim 5:* We have $(n + m)\,a = na + ma$ for all $a \in \mathbb{K}$ and $n \in \mathbb{N}$ and $m \in \mathbb{Z}$.

[*Proof of Claim 5:* Let $a \in \mathbb{K}$ and $n \in \mathbb{N}$ and $m \in \mathbb{Z}$. We must prove that $(n + m)\,a = na + ma$. If $m \in \mathbb{N}$, then this follows from Claim 3. Hence, for the rest of this proof, we WLOG assume that we don't have $m \in \mathbb{N}$. Thus, we have $m \in \mathbb{Z}$ but not $m \in \mathbb{N}$. Hence, $m \in \mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \ldots\}$. In other words, $m < 0$. Hence, $-m > 0$, so that $-m \in \mathbb{N}$. Hence, Claim 4 (applied to $-m$ instead of m) yields $(n - (-m))\,a = na - (-m)\,a$. In view of $n - (-m) = n + m$, this rewrites as $(n + m)\,a = na - (-m)\,a$. But Claim 2 (applied to m instead of n) yields $(-m)\,a = -(ma)$. Hence,

$$(n + m)\,a = na - \underbrace{(-m)\,a}_{=-(-ma)} = na - (-(ma)) = na + ma$$

(by Proposition 5.4.5 **(j)**, applied to na, ma and 0 instead of a, b and c). This proves Claim 5.]

Finally, we can generalize this further by allowing n to be negative as well:

> *Claim 6:* We have $(n + m)\,a = na + ma$ for all $a \in \mathbb{K}$ and $n, m \in \mathbb{Z}$.

[*Proof of Claim 6:* Let $a \in \mathbb{K}$ and $n, m \in \mathbb{Z}$. We must prove that $(n + m)\,a = na + ma$. If $n \in \mathbb{N}$, then this follows from Claim 5. Hence, for the rest of this proof, we WLOG assume that we don't have $n \in \mathbb{N}$. Thus, we have $n \in \mathbb{Z}$ but not $n \in \mathbb{N}$. Hence, $n \in \mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \ldots\}$. In other words, $n < 0$. Hence, $-n > 0$, so that $-n \in \mathbb{N}$. Hence, Claim 5 (applied to $-n$ and $-m$ instead of n and m) yields $((-n)+(-m))\,a = (-n)\,a + (-m)\,a$. In view of $(-n)+(-m) = -(n+m)$, this rewrites as

$$(-(n+m))\,a = (-n)\,a + (-m)\,a. \tag{495}$$

But Claim 2 yields $(-n)\,a = -(na)$. Also, Claim 2 (applied to m instead of n) yields $(-m)\,a = -(ma)$. Hence, (495) becomes

$$(-(n+m))\,a = \underbrace{(-n)\,a}_{=-(na)} + \underbrace{(-m)\,a}_{=-(ma)} = (-(na)) + (-(ma)). \tag{496}$$

Also, Claim 2 (applied to $n+m$ instead of n) yields $(-(n+m))\,a = -((n+m)\,a)$. Comparing this with (496), we obtain

$$-((n+m)\,a) = (-(na)) + (-(ma)). \tag{497}$$

But Proposition 5.4.5 **(b)** (applied to na, ma and 0 instead of a, b and c) yields

$$-(na+ma) = (-(na)) + (-(ma)).$$

Comparing this with (497), we find $-((n+m)\,a) = -(na+ma)$. Hence, Proposition 5.4.5 **(l)** (applied to $(n+m)\,a$, $na+ma$ and 0 instead of a, b and c) yields $(n+m)\,a = na+ma$. This proves Claim 6.]

Claim 6 is precisely the statement of (166). Thus, (166) is now proven.

Claim 7: We have $(nm)\,a = n\,(ma)$ for all $a \in \mathbb{K}$ and $n \in \mathbb{N}$ and $m \in \mathbb{Z}$.

[*Proof of Claim 7:* We shall prove Claim 7 by induction on n:

Induction base: We have $(0m)\,a = 0\,(ma)$ for all $a \in \mathbb{K}$ and $m \in \mathbb{Z}$ (because if $a \in \mathbb{K}$ and $m \in \mathbb{Z}$, then

$$\underbrace{(0m)}_{=0}\,a = 0a = 0_{\mathbb{K}} \qquad \text{(by (173))}$$

and

$$0\,(ma) = 0_{\mathbb{K}} \qquad \text{(by (173), applied to } ma \text{ instead of } a\text{)}$$

and thus $(0m)\,a = 0_{\mathbb{K}} = 0\,(ma)$). In other words, Claim 7 holds for $n = 0$. This completes the induction base.

Induction step: Let $k \in \mathbb{N}$. Assume that Claim 7 holds for $n = k$. We must prove that Claim 7 holds for $n = k+1$.

We have assumed that Claim 7 holds for $n = k$. In other words, we have

$$(km)\,a = k\,(ma) \qquad \text{for all } a \in \mathbb{K} \text{ and } m \in \mathbb{Z}. \tag{498}$$

Now, let $a \in \mathbb{K}$ and $m \in \mathbb{Z}$. Then,

$$\begin{aligned}\underbrace{((k+1)\,m)}_{=km+m}\,a = (km+m)\,a &= \underbrace{(km)\,a}_{\substack{=k(ma)\\ \text{(by (498))}}} + ma \qquad \text{(by Claim 6, applied to } n = km\text{)}\\ &= k\,(ma) + ma.\end{aligned}$$

Comparing this with

$$(k+1)(ma) = k(ma) + \underbrace{1(ma)}_{\substack{=ma \\ \text{(by (172), applied} \\ \text{to } ma \text{ instead of } a)}}$$
$$\text{(by Claim 6, applied to } k\text{, 1 and } ma \text{ instead of } n\text{, } m \text{ and } a\text{)}$$
$$= k(ma) + ma,$$

we find $((k+1)m)a = (k+1)(ma)$.

Now, forget that we fixed a and m. We thus have shown that $((k+1)m)a = (k+1)(ma)$ for all $a \in \mathbb{K}$ and $m \in \mathbb{Z}$. In other words, Claim 7 holds for $n = k+1$. This completes the induction step. Thus, Claim 7 is proven.]

Claim 8: We have $(nm)a = n(ma)$ for all $a \in \mathbb{K}$ and $n, m \in \mathbb{Z}$.

[*Proof of Claim 8:* Let $a \in \mathbb{K}$ and $n, m \in \mathbb{Z}$. We must prove that $(nm)a = n(ma)$. If $n \in \mathbb{N}$, then this follows from Claim 7. Hence, for the rest of this proof, we WLOG assume that we don't have $n \in \mathbb{N}$. Thus, we have $n \in \mathbb{Z}$ but not $n \in \mathbb{N}$. Hence, $n \in \mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \ldots\}$. In other words, $n < 0$. Hence, $-n > 0$, so that $-n \in \mathbb{N}$. Hence, Claim 7 (applied to $-n$ instead of n) yields $((-n)m)a = (-n)(ma)$. Thus,

$$\underbrace{(-nm)}_{=(-n)m} a = ((-n)m)a = (-n)(ma) = -(n(ma)) \tag{499}$$

(by Claim 2, applied to ma instead of a). On the other hand, Claim 2 (applied to nm instead of n) yields $(-nm)a = -((nm)a)$. Comparing this with (499), we obtain $-((nm)a) = -(n(ma))$. Thus, Proposition 5.4.5 **(l)** (applied to $(nm)a$, $n(ma)$ and 0 instead of a, b and c) yields $(nm)a = n(ma)$. Thus, Claim 8 is proven.]

Claim 8 is precisely (169). Thus, we have now proven (169).

Claim 9: We have $n(a+b) = na + nb$ for all $a, b \in \mathbb{K}$ and $n \in \mathbb{N}$.

[*Proof of Claim 9:* We shall prove Claim 9 by induction on n:

Induction base: If $a, b \in \mathbb{K}$, then

$$\underbrace{0a}_{\substack{=0_{\mathbb{K}} \\ \text{(by (173))}}} + \underbrace{0b}_{\substack{=0_{\mathbb{K}} \\ \text{(by (173), applied} \\ \text{to } b \text{ instead of } a)}} = 0_{\mathbb{K}} + 0_{\mathbb{K}} = 0_{\mathbb{K}} = 0(a+b)$$

(since (173) (applied to $a+b$ instead of a) yields $0(a+b) = 0_{\mathbb{K}}$). Hence, we have $0(a+b) = 0a + 0b$ for all $a, b \in \mathbb{K}$. In other words, Claim 9 holds for $n = 0$. This completes the induction base.

Induction step: Let $k \in \mathbb{N}$. Assume that Claim 9 holds for $n = k$. We must prove that Claim 9 holds for $n = k+1$.

We have assumed that Claim 9 holds for $n = k$. In other words, we have

$$k(a+b) = ka + kb \qquad \text{for all } a, b \in \mathbb{K}. \tag{500}$$

Now, let $a, b \in \mathbb{K}$. Then,

$$\begin{aligned}(k+1)(a+b) &= \underbrace{k(a+b)}_{\substack{=ka+kb \\ \text{(by (500))}}} + \underbrace{1(a+b)}_{\substack{=a+b \\ \text{(by (172)} \\ \text{(applied to } a+b \text{ instead of } a))}} \\ &\qquad \text{(by Claim 3, applied to } k\text{, } 1 \text{ and } a+b \text{ instead of } n\text{, } m \text{ and } a) \\ &= ka+kb+a+b = ka+a+kb+b. \end{aligned} \tag{501}$$

On the other hand, Claim 3 (applied to $n = k$ and $m = 1$) yields $(k+1)a = ka + \underbrace{1a}_{\substack{=a \\ \text{(by (172))}}} = ka + a$. The same argument (applied to b instead of a) yields $(k+1)b = kb + b$. Adding these two equalities together, we obtain

$$(k+1)a + (k+1)b = (ka+a) + (kb+b) = ka+a+kb+b.$$

Comparing this with (501), we find $(k+1)(a+b) = (k+1)a + (k+1)b$.

Now, forget that we fixed a, b. We thus have proven that

$$(k+1)(a+b) = (k+1)a + (k+1)b \qquad \text{for all } a, b \in \mathbb{K}.$$

In other words, Claim 9 holds for $n = k+1$. This completes the induction step. Thus, Claim 9 is proven.]

Claim 10: We have $n(a+b) = na + nb$ for all $a, b \in \mathbb{K}$ and $n \in \mathbb{Z}$.

[*Proof of Claim 10:* Let $a, b \in \mathbb{K}$ and $n \in \mathbb{Z}$. We must prove that $n(a+b) = na + nb$. If $n \in \mathbb{N}$, then this follows from Claim 9. Hence, for the rest of this proof, we WLOG assume that we don't have $n \in \mathbb{N}$. Thus, we have $n \in \mathbb{Z}$ but not $n \in \mathbb{N}$. Hence, $n \in \mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \ldots\}$. In other words, $n < 0$. Hence, $-n > 0$, so that $-n \in \mathbb{N}$. Hence, Claim 9 (applied to $-n$ instead of n) yields

$$(-n)(a+b) = \underbrace{(-n)a}_{\substack{=-(na) \\ \text{(by Claim 2)}}} + \underbrace{(-n)b}_{\substack{=-(nb) \\ \text{(by Claim 2,} \\ \text{applied to } b \text{ instead of } a)}} = (-(na)) + (-(nb)).$$

Comparing this with

$$(-n)(a+b) = -(n(a+b)) \qquad \text{(by Claim 2, applied to } a+b \text{ instead of } a),$$

we find

$$-(n(a+b)) = (-(na)) + (-(nb)).$$

On the other hand, Proposition 5.4.5 **(b)** (applied to na and nb instead of a and b) yields

$$-(na+nb) = (-(na)) + (-(nb)).$$

Comparing these two equalities, we obtain $-(n(a+b)) = -(na+nb)$. Thus, Proposition 5.4.5 **(l)** (applied to $n(a+b)$, $na+nb$ and 0 instead of a, b and c) yields $n(a+b) = na+nb$. Thus, Claim 10 is proven.]

Claim 10 is precisely (167). Thus, we have proven (167).

Claim 11: We have $n0_{\mathbb{K}} = 0_{\mathbb{K}}$ for all $n \in \mathbb{N}$.

[*Proof of Claim 11:* We shall prove Claim 11 by induction on n:

Induction base: The equality (173) (applied to $a = 0_{\mathbb{K}}$) yields $0 \cdot 0_{\mathbb{K}} = 0_{\mathbb{K}}$. In other words, Claim 11 holds for $n = 0$. This completes the induction base.

Induction step: Let $k \in \mathbb{N}$. Assume that Claim 11 holds for $n = k$. We must prove that Claim 11 holds for $n = k + 1$.

We have assumed that Claim 11 holds for $n = k$. In other words, we have $k0_{\mathbb{K}} = 0_{\mathbb{K}}$. Now, Claim 3 (applied to $n = k$, $m = 1$ and $a = 0_{\mathbb{K}}$) yields $(k+1)\, 0_{\mathbb{K}} = k0_{\mathbb{K}} + \underbrace{1 \cdot 0_{\mathbb{K}}}_{\substack{=0_{\mathbb{K}} \\ \text{(by (172))}}} = k0_{\mathbb{K}} = 0_{\mathbb{K}}$. In other words, Claim 11 holds for $n = k + 1$. This completes the induction step. Thus, Claim 11 is proven.]

Claim 12: We have $n0_{\mathbb{K}} = 0_{\mathbb{K}}$ for all $n \in \mathbb{Z}$.

[*Proof of Claim 12:* Let $n \in \mathbb{Z}$. We must prove that $n0_{\mathbb{K}} = 0_{\mathbb{K}}$. If $n \in \mathbb{N}$, then this follows from Claim 12. Hence, for the rest of this proof, we WLOG assume that we don't have $n \in \mathbb{N}$. Thus, we have $n \in \mathbb{Z}$ but not $n \in \mathbb{N}$. Hence, $n \in \mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \ldots\}$. In other words, $n < 0$. Hence, $-n > 0$, so that $-n \in \mathbb{N}$. Hence, Claim 12 (applied to $-n$ instead of n) yields $(-n)\, 0_{\mathbb{K}} = 0_{\mathbb{K}}$. But Claim 2 (applied to $a = 0_{\mathbb{K}}$) yields $(-n)\, 0_{\mathbb{K}} = -\,(n0_{\mathbb{K}})$. Hence, $-\,(n0_{\mathbb{K}}) = (-n)\, 0_{\mathbb{K}} = 0_{\mathbb{K}} = -0_{\mathbb{K}}$ (since $-0_{\mathbb{K}} = 0_{\mathbb{K}}$). Thus, Proposition 5.4.5 **(l)** (applied to $n0_{\mathbb{K}}$, $0_{\mathbb{K}}$ and $0_{\mathbb{K}}$ instead of a, b and c) yields $n0_{\mathbb{K}} = 0_{\mathbb{K}}$. This proves Claim 12.]

Claim 12 is precisely (171). Thus, (171) is now proven.

Claim 13: We have $(-n)\, a = n\,(-a)$ for all $a \in \mathbb{K}$ and $n \in \mathbb{Z}$.

[*Proof of Claim 13:* Let $a \in \mathbb{K}$ and $n \in \mathbb{Z}$. Then, Claim 10 (applied to $b = -a$) yields $n\,(a + (-a)) = na + n\,(-a)$. Comparing this with

$$n \underbrace{(a + (-a))}_{=0_{\mathbb{K}}} = n0_{\mathbb{K}} = 0_{\mathbb{K}} \qquad \text{(by Claim 12)},$$

we obtain $na + n\,(-a) = 0_{\mathbb{K}}$. Subtracting na from both sides of this equality, we find $n\,(-a) = 0_{\mathbb{K}} - na = 0 - na = -\,(na)$ (by Proposition 5.4.5 **(d)**, applied to na instead of a). But Claim 2 yields $(-n)\, a = -\,(na) = n\,(-a)$ (since $n\,(-a) = -\,(na)$). This proves Claim 13.]

Now, any $a \in \mathbb{K}$ and $n \in \mathbb{Z}$ satisfy

$$\begin{aligned} -\,(na) &= (-n)\, a && \text{(by Claim 2)} \\ &= n\,(-a) && \text{(by Claim 13)}. \end{aligned}$$

This proves (168).

Claim 14: We have $n\,(ab) = (na)\, b = a\,(nb)$ for all $a, b \in \mathbb{K}$ and $n \in \mathbb{N}$.

[*Proof of Claim 14:* We shall prove Claim 14 by induction on n:

Induction base: It is easy to see that $0(ab) = (0a)b = a(0b)$ for all $a, b \in \mathbb{K}$ [313]. In other words, Claim 14 holds for $n = 0$.

Induction step: Let $k \in \mathbb{N}$. Assume that Claim 14 holds for $n = k$. We must prove that Claim 14 holds for $n = k + 1$.

We have assumed that Claim 14 holds for $n = k$. In other words, we have

$$k(ab) = (ka)b = a(kb) \qquad \text{for all } a, b \in \mathbb{K}. \tag{502}$$

Now, let $a, b \in \mathbb{K}$. Then, (502) yields $k(ab) = (ka)b = a(kb)$.

Claim 3 (applied to $n = k$ and $m = 1$) yields $(k+1)a = ka + \underbrace{1a}_{\substack{=a \\ \text{(by (172))}}} = ka + a$. The same argument (applied to b instead of a) yields $(k+1)b = kb + b$. Also, the same argument that we used to prove $(k+1)a = ka + a$ can be applied to ab instead of a; it then shows that $(k+1)(ab) = k(ab) + ab$.

Now,

$$\underbrace{((k+1)a)}_{=ka+a} b = (ka + a)b = (ka)b + ab \qquad \text{(by the distributivity axiom)}.$$

Comparing this with

$$(k+1)(ab) = \underbrace{k(ab)}_{=(ka)b} + ab = (ka)b + ab,$$

we obtain

$$(k+1)(ab) = ((k+1)a)b. \tag{503}$$

Furthermore,

$$a\underbrace{((k+1)b)}_{=kb+b} = a(kb + b) = a(kb) + ab \qquad \text{(by the distributivity axiom)}.$$

Comparing this with

$$(k+1)(ab) = \underbrace{k(ab)}_{=a(kb)} + ab = a(kb) + ab,$$

we obtain

$$(k+1)(ab) = a((k+1)b).$$

Combining this equality with (503), we obtain

$$(k+1)(ab) = ((k+1)a)b = a((k+1)b).$$

Now, forget that we fixed a, b. We thus have proven that $(k+1)(ab) = ((k+1)a)b = a((k+1)b)$ for all $a, b \in \mathbb{K}$. In other words, Claim 14 holds for $n = k + 1$. This completes the induction step. Thus, Claim 14 is proven.]

[313] *Proof.* Let $a, b \in \mathbb{K}$. Then, $0a = 0_{\mathbb{K}}$ (by (173)). Thus, $(0a)b = 0_{\mathbb{K}}b = 0_{\mathbb{K}}$ (by the "Annihilation" axiom for the ring $\mathbb{K}$). Furthermore, $0b = 0_{\mathbb{K}}$ (by (173), applied to b instead of a). Thus, $a(0b) = a0_{\mathbb{K}} = 0_{\mathbb{K}}$ (by the "Annihilation" axiom for the ring $\mathbb{K}$). Finally, $0(a+b) = 0_{\mathbb{K}}$ (by (173), applied to $a + b$ instead of a). Thus, $0(ab) = 0_{\mathbb{K}}$ (by the "Annihilation" axiom for the ring $\mathbb{K}$). Comparing this equality with the equalities $(0a)b = 0_{\mathbb{K}}$ and $a(0b) = 0_{\mathbb{K}}$, we obtain $0(ab) = (0a)b = a(0b)$. Qed.

Claim 15: We have $n(ab) = (na)b = a(nb)$ for all $a, b \in \mathbb{K}$ and $n \in \mathbb{Z}$.

[*Proof of Claim 15:* Let $a, b \in \mathbb{K}$ and $n \in \mathbb{Z}$. We must prove that $n(ab) = (na)b = a(nb)$. If $n \in \mathbb{N}$, then this follows from Claim 14. Hence, for the rest of this proof, we WLOG assume that we don't have $n \in \mathbb{N}$. Thus, we have $n \in \mathbb{Z}$ but not $n \in \mathbb{N}$. Hence, $n \in \mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \ldots\}$. In other words, $n < 0$. Hence, $-n > 0$, so that $-n \in \mathbb{N}$. Hence, Claim 14 (applied to $-n$ instead of n) yields $(-n)(ab) = ((-n)a)b = a((-n)b)$.

Proposition 5.4.5 **(f)** (applied to na and 0 instead of a and c) yields $-((na)b) = (-(na))b = (na)(-b)$. Proposition 5.4.5 **(f)** (applied to nb and 0 instead of b and c) yields $-(a(nb)) = (-a)(nb) = a(-(nb))$.

But Claim 2 (applied to ab instead of a) yields $(-n)(ab) = -(n(ab))$. Thus,

$$-(n(ab)) = (-n)(ab) = \underbrace{((-n)a)}_{\substack{=-(na) \\ \text{(by Claim 2)}}} b = (-(na))b = -((na)b)$$

(since $-((na)b) = (-(na))b$). Hence, Proposition 5.4.5 **(l)** (applied to $n(ab)$, $(na)b$ and 0 instead of a, b and c) yields $n(ab) = (na)b$.

Also,

$$-(n(ab)) = (-n)(ab) = a \underbrace{((-n)b)}_{\substack{=-(nb) \\ \text{(by Claim 2, applied} \\ \text{to } b \text{ instead of } a)}} = a(-(nb)) = -(a(nb))$$

(since $-(a(nb)) = a(-(nb))$). Hence, Proposition 5.4.5 **(l)** (applied to $n(ab)$, $a(nb)$ and 0 instead of a, b and c) yields $n(ab) = a(nb)$.

Combining the equalities $n(ab) = (na)b$ and $n(ab) = a(nb)$, we obtain $n(ab) = (na)b = a(nb)$. This proves Claim 15.]

But Claim 15 is precisely (170). Hence, (170) is proven. Thus, our proof of Proposition 5.4.9 is complete. □

References

[AigZie18] Martin Aigner, Günter M. Ziegler, *Proofs from the Book*, 6th edition, Springer 2018.

[AloDub93] Noga Alon and Moshe Dubiner, *Zero-sum sets of prescribed size*, in: "Combinatorics, Paul Erdős is Eighty", Bolyai Society, Mathematical Studies, Keszthely, Hungary, 1993, pp. 33–50. `https://m.tau.ac.il/~nogaa/PDFS/egz1.pdf`

[AmaEsc05] Herbert Amann, Joachim Escher, *Analysis I*, translated from the German by Gary Brookfield, Birkhäuser 2005.

[AndAnd14] Titu Andreescu, Dorin Andrica, *Complex Numbers from A to... Z*, 2nd edition, Springer 2014.

[Armstr18] Drew Armstrong, *Abstract Algebra I & Abstract Algebra II*, 2019.
I: `https://www.math.miami.edu/~armstrong/561fa18.php` ;
II: `https://www.math.miami.edu/~armstrong/562sp19.php`

[Artin10] Michael Artin, *Algebra*, 2nd edition, Pearson 2010.

[Boreic08] Iurie Boreico, *Linear Independence of Radicals*, The Harvard College Mathematics Review 2.1 (2008).
`https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.630.1024&rep=rep1&type=pdf`

[Bosch18] Siegfried Bosch, *Algebra – From the Viewpoint of Galois Theory*, Springer 2018.
`https://www.springer.com/la/book/9783319951768`

[Bump02] Daniel Bump, *Mathematics of the Rubik's Cube*, lecture notes (in 2 versions).
`http://sporadic.stanford.edu/bump/match/rubik.html`

[Burton10] David M. Burton, *Elementary Number Theory*, 7th edition, McGraw-Hill 2010.

[Carrel05] James B. Carrell, *Fundamentals of Linear Algebra*, 31 October 2005.
`https://www.math.ubc.ca/~carrell/NB.pdf`

[Carrel17] James B. Carrell, *Groups, Matrices, and Vector Spaces: A Group Theoretic Approach*, Springer 2017.
`https://dx.doi.org/10.1007/978-0-387-79428-0`

[Childs00] Lindsay N. Childs, *A Concrete Introduction to Higher Algebra*, 3rd edition, Springer 2009.

[CoLiOs15] David A. Cox, John Little, Donal O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, 4th edition, Springer 2015.
`https://dx.doi.org/10.1007/978-3-319-16721-3`

[Conrad*] Keith Conrad, *Expository notes ("blurbs").*
`https://kconrad.math.uconn.edu/blurbs/`

[ConradD] Keith Conrad, *The dimension of a vector space.*
`https://kconrad.math.uconn.edu/blurbs/linmultialg/dimension.pdf`

[ConradE] Keith Conrad, *Euler's theorem.*
`https://kconrad.math.uconn.edu/blurbs/ugradnumthy/eulerthm.pdf`

[ConradF] Keith Conrad, *Finite fields*, 4 February 2018.
`https://kconrad.math.uconn.edu/blurbs/galoistheory/finitefields.pdf`

[ConradG] Keith Conrad, *The Gaussian integers*.
`https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf`

[ConradI] Keith Conrad, *Examples of proofs by induction*.
`https://kconrad.math.uconn.edu/blurbs/proofs/induction.pdf`

[ConradS] Keith Conrad, *Modules over a PID*.
`https://kconrad.math.uconn.edu/blurbs/linmultialg/modulesoverPID.pdf`

[ConradW] Keith Conrad, *Well-defined functions*.
`https://kconrad.math.uconn.edu/blurbs/proofs/welldefined.pdf`

[Cox13] David A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley, 2nd edition 2013.

[daSilv12] Patrick Da Silva, *Polynomial in $\mathbb{Q}[x]$ sending integers to integers?, math.stackexchange answer #108318*.

[Day16] Martin V. Day, *An Introduction to Proofs and the Mathematical Vernacular*, 7 December 2016.
`https://www.math.vt.edu/people/day/ProofsBook/IPaMV.pdf` .

[DumFoo04] David S. Dummit, Richard M. Foote, *Abstract Algebra*, 3rd edition, Wiley 2004.
See `http://www.cems.uvm.edu/~rfoote/errata_3rd_edition.pdf` for errata.

[Dummit16] Evan Dummit, *Mathematical Cryptography, Spring 2016*, handouts.
`https://math.la.asu.edu/~dummit/handouts.html`

[Elman18] Richard Elman, *Lectures on Abstract Algebra*, 17 September 2018.
`https://www.math.ucla.edu/~rse/algebra_book.pdf`

[ErGiZi61] P. Erdős, A. Ginzburg, A. Ziv, *Theorem in the additive number theory*, Bull. Research Council Israel 10F (1961), pp. 41–43.
`https://pdfs.semanticscholar.org/2860/2b7734c115bbab7141a1942a2c974057ddc0.pdf`

[Escofi01] Jean-Pierre Escofier, *Galois Theory*, translated by Leila Schneps, Springer 2001.

[Galvin17] David Galvin, *Basic discrete mathematics*, 13 December 2017.
`http://www-users.math.umn.edu/~dgrinber/comb/60610lectures2017-Galvin.pdf`
(The URL might change, and the text may get updated. In order to reliably obtain the version of 13 December 2017, you can use the archive.org Wayback Machine: `https://web.archive.org/web/20180205122609/http://www-users.math.umn.edu/~dgrinber/comb/60610lectures2017-Galvin.pdf` .)

[GalQua17] Jean Gallier, Jocelyn Quaintance, *Notes on Primality Testing And Public Key Cryptography, Part 1*, 27 February 2019.
`https://www.cis.upenn.edu/~jean/RSA-primality-testing.pdf`

[GalQua18] Jean Gallier and Jocelyn Quaintance, *Algebra, Topology, Differential Calculus, and Optimization Theory For Computer Science and Engineering*, 2 August 2019.
`https://www.cis.upenn.edu/~jean/gbooks/geomath.html`

[Garret03] Paul Garrett, *Crypto and Number Theory*, slides, 2003.
`http://www-users.math.umn.edu/~garrett/crypto/`

[Garret07] Paul Garrett, *The Mathematics of Coding: Information, Compression, Error Correction, and Finite Fields*, 2007.
`http://www-users.math.umn.edu/~garrett/coding/CodingNotes.pdf`

[Goodma16] Frederick M. Goodman, *Algebra: Abstract and Concrete*, edition 2.6, 12 October 2016.
`https://homepage.divms.uiowa.edu/~goodman/algebrabook.dir/algebrabook.html`

[Granvi05] Andrew Granville, *Binomial coefficients modulo prime powers*, preprint.
`https://web.archive.org/web/20181024055320/http://ebooks.bharathuniv.ac.in/gdlc1/gdlc1/EngineeringMergedLibraryv3.0/AndrewGranville/BinomialCoefficientsModuloPrimePowers(5579)/BinomialCoefficientsModuloPrimePowers-AndrewGranville.pdf`

[Grinbe15] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
`https://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf`
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see `https://github.com/darijgr/detnotes/releases/tag/2019-01-10` .

[Grinbe16] Darij Grinberg, *18.781 (Spring 2016): Floor and arithmetic functions*, 13 April 2019.
`https://www.cip.ifi.lmu.de/~grinberg/floor.pdf`

[Grinbe17] Darij Grinberg, *The Lucas and Babbage congruences*, 10 January 2019.
`https://www.cip.ifi.lmu.de/~grinberg/lucascong.pdf`

[Grinbe18] Darij Grinberg, *Notes on linear algebra*, version of 13 December 2016.
`https://github.com/darijgr/lina`

[Grinbe19a] Darij Grinberg, *Regular elements of a ring, monic polynomials and "lcm-coprimality"*, 2019.
`https://www.cip.ifi.lmu.de/~grinberg/algebra/regpol.pdf`

[Grinbe19b] Darij Grinberg, *The existence of finite fields, again*, 31 May 2019.
`https://www.cip.ifi.lmu.de/~grinberg/t/19s/fpnexists.pdf`

[GrKnPa94] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Concrete Mathematics, Second Edition*, Addison-Wesley 1994.
See `https://www-cs-faculty.stanford.edu/~knuth/gkp.html` for errata.

[Hammac18] Richard Hammack, *Book of Proof*, 3rd edition 2018.
`https://www.people.vcu.edu/~rhammack/BookOfProof/`

[Heffer17] Jim Hefferon, *Linear Algebra*, 3rd edition 2017.
`http://joshua.smcvt.edu/linearalgebra/`

[Hunger03] Thomas W. Hungerford, *Algebra*, 12th printing, Springer 2003.

[Hunger14] Thomas W. Hungerford, *Abstract Algebra: An Introduction*, 3rd edition, Brooks/Cole 2014.

[Jia13] Yan-Bin Jia, *Quaternions and Rotations (Com S 477/577 Notes)*, 10 September 2013.
`https://graphics.stanford.edu/courses/cs348a-17-winter/Papers/quaternion.pdf`

[Joyner08] W. D. Joyner, *Mathematics of the Rubik's cube*, 19 August 2008.
`https://web.archive.org/web/20160304122348/http://www.permutationpuzzles.org/rubik/webnotes/` (link to the PDF at the bottom).

[Knapp16a] Anthony W. Knapp, *Basic Algebra*, digital 2nd edition 2016.
`https://www.math.stonybrook.edu/~aknapp/download.html`

[Knapp16b] Anthony W. Knapp, *Advanced Algebra*, digital 2nd edition 2016.
`https://www.math.stonybrook.edu/~aknapp/download.html`

[Knuth98] Donald Ervin Knuth, *The art of computer programming, volume 2*, Addison–Wesley 1998.

[LaNaSc16] Isaiah Lankham, Bruno Nachtergaele, Anne Schilling, *Linear Algebra As an Introduction to Abstract Mathematics*, 2016.
`https://www.math.ucdavis.edu/~anne/linear_algebra/mat67_course_notes.pdf`

[LeLeMe18] Eric Lehman, F. Thomson Leighton, Albert R. Meyer, *Mathematics for Computer Science*, revised Tuesday 6th June 2018.
`https://courses.csail.mit.edu/6.042/spring18/mcs.pdf` .

[LidNie97] Rudolf Lidl, Harald Niederreiter, *Finite fields*, 2nd edition, Cambridge University Press 1997.

[Loehr11] Nicholas A. Loehr, *Bijective Combinatorics*, Chapman & Hall/CRC 2011.

[Mate14] Attila Maté, *Determinants*, version 1 October 2017.
`http://www.sci.brooklyn.cuny.edu/~mate/misc/determinants.pdf`

[Muir30] Thomas Muir, *The theory of determinants in the historical order of development*, 5 volumes (1906–1930), later reprinted by Dover.

[MuiMet60] Thomas Muir, *A Treatise on the Theory of Determinants*, revised and enlarged by William H. Metzler, Dover 1960.

[Mestro14] Romeo Meštrović, *Lucas' theorem: its generalizations, extensions and applications (1878–2014)*, arXiv:1409.3820v1.

[Milne17] James S. Milne, *Group theory*, version v3.14, March 17, 2017.
`https://www.jmilne.org/math/CourseNotes/gt.html`

[Mulhol16] Jamie Mulholland, *Permutation Puzzles: A Mathematical Perspective*,
`https://www.sfu.ca/~jtmulhol/math302/`

[NiZuMo91] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition 1991.

[Payne09] S. E. Payne, *A Second Semester of Linear Algebra*, 19 January 2009.
`https://web.archive.org/web/20161207060453/http://math.ucdenver.edu/~spayne/classnotes/09LinAlg.pdf`

[Pinkha15] Henry C. Pinkham, *Linear Algebra*, draft of a textbook, version 10 July 2015.
`https://www.math.columbia.edu/~pinkham/HCP_LinearAlgebra.pdf`

[Pinter10] Charles C. Pinter, *A book of abstract algebra*, 2nd edition, Dover 2010.
`https://www.amazon.com/Book-Abstract-Algebra-Second-Mathematics/dp/0486474178`

[Polya19] Georg Pólya, *Über ganzwertige Polynome in algebraischen Zahlkörpern*, Journal für die Reine und Angewandte Mathematik (Crelle's Journal), **149** (1919), pp. 97–116.

[Rothma15] Tony Rothman, *Cardano v Tartaglia: The Great Feud Goes Supernatural*, arXiv:1308.2181v5, published in: The Mathematical Intelligencer, 36(4), pp. 53–66.

[Siksek15] Samir Siksek, *Introduction to Abstract Algebra*, 2015.
`https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/aa/aanotes.pdf`

[Stewar15] Ian Stewart, *Galois theory*, 4th edition, CRC Press 2015.
`http://matematicaeducativa.com/foro/download/file.php?id=1647`

[Strick13] Neil Strickland, *Linear mathematics for applications*, 2013.
`https://neil-strickland.staff.shef.ac.uk/courses/MAS201/MAS201.pdf`

[Swanso18] Irena Swanson, *Introduction to Analysis*, with construction of the number systems, 19 June 2019.
`https://people.reed.edu/~iswanson/analysisconstructR.pdf`

[Tignol01] Jean-Pierre Tignol, *Galois' Theory of Algebraic Equations*, World Scientific 2001.

[Trefet11] Lloyd N. Trefethen, *Six Myths of Polynomial Interpolation and Quadrature*, Maths. Today **47** (2011), pp. 184–188.
`https://people.maths.ox.ac.uk/trefethen/publication/PDF/2011_139.pdf`

[UspHea39] J. V. Uspensky, M. A. Heaslet, *Elementary Number Theory*, McGraw-Hill 1939.

[Vogan07] David Vogan, *The Character Table for E_8*, Notices of the American Mathematical Society 2007/09.

[Waerde91a] B.L. van der Waerden, *Algebra, Volume I*, translated 7th edition, Springer 1991.

[Waerde91b] B.L. van der Waerden, *Algebra, Volume II*, translated 5th edition, Springer 1991.

[Walker87] Elbert A. Walker, *Introduction to Abstract Algebra*, Random House/Birkhauser, New York, 1987.

[Wan11] Zhe-Xian Wan, *Finite fields and Galois rings*, World Scientific 2011.

[Ward91] James Ward, *100 years of Dixon's identity*, Irish Mathematical Society Bulletin **27** (1991), pp. 46–54.
`https://www.maths.tcd.ie/pub/ims/bull27/bull27_46-54.pdf`

[Warner71] Seth Warner, *Classical Modern Algebra*, Prentice-Hall 1971.

[Wilf94] Herbert S. Wilf, *generatingfunctionology*, 1999.
`https://www.math.upenn.edu/~wilf/DownldGF.html`