# Axiomatic Set Theory

Tom Leinster, University of Edinburgh

Version of 25 November 2024

# Note to the reader

This is the text for Axiomatic Set Theory, University of Edinburgh, 2024–25.

**Structure** Each chapter corresponds to one week of the semester. You are expected to read Chapter $n$ before the lectures in Week $n$, except for Chapter 1. I am writing these notes as we go along, so new chapters will appear progressively.

References to theorem numbers, page numbers, etc., are clickable links.

**Exercises** looking like this are sprinkled through the notes. The idea is that you try them immediately, before you continue reading.

Most of them are meant to be quick and easy, much easier than assignment or workshop questions. If you can do them, you can take it as a sign that you're following successfully. For those that defeat you, chat with others in the class, ask on Piazza, or ask me.

I promise you that if you make it a habit to try every exercise, you'll enjoy the course more and understand it better than if you don't.

**Digressions** like this are optional and not examinable, but might interest you. They're usually on points that *I* find interesting, and often describe connections between set theory and other parts of mathematics.

**Prerequisites** This course has very few formal prerequisites: just Proofs and Problem Solving or similar. (See Path for details.)

You should know the following basic set-theoretic concepts: function, domain, codomain, element, subset, equivalence relation, cartesian product, injection, surjection, bijection, image, and preimage (inverse image). If you are unsure what any of those terms mean, you should look them up and do some exercises on them straight away.

It would also be ideal if you have some of the following qualities:

- **Experience with proof-based courses.** You should have some previous experience with courses centred on definitions, theorems and proofs. Otherwise, you will probably find this course hard going.
- **Patience.** Building everything up from a small collection of axioms is slow going at first. We will spend some time proving statements that might seem obvious, before picking up speed and striking out into the unknown.
- **A spirit of adventure.** As far as I know, this is the first time anywhere in the world that a course like this has been taught (taking the particular approach that we'll take). I'm excited to have this opportunity, and I hope you'll find it exciting too to be part of something genuinely new. But do be aware that unlike most courses you've taken, the material *hasn't* had years of polishing. I'll do my best to make it as smooth as possible, but there may be occasional rough edges. That's life! And although I'll try to split the material into 20 similar-sized chunks (one per class), there may be some variation in length.

**Further reading** These notes are self-contained. You do not need to read anything else. In fact, because the approach taken in this course is new, no existing texts cover it. Almost all books on set theory take an entirely different approach. (You could read them for context, but they would not help you follow this course, and might be actively unhelpful.) The closest approximation is Lawvere and Rosebrugh's book *Sets for Mathematics*, but that puts categories at the heart of its exposition, whereas I will neither assume nor teach anything about categories.

**Mistakes** I'll be grateful to hear of mistakes in these notes (Tom.Leinster@ed.ac.uk), even if it's something tiny and even if you're not sure.

# A note on logic

An important role in this course is played by 'universal properties', which have this form:

> for all *something*, there exists a unique *something* such that *something*.

This is slightly complicated logically, but no worse than the definition of continuity. However, learners often trip up on the word *unique*, so I want to address that point directly before we get started.

The heart of the problem is that *unique* has a different meaning in mathematics than in everyday English. For example, the English statement 'Anna has a unique sense of humour' means that no one else has the same sense of humour as Anna. So if we take the function

$$f\colon \{\text{people}\} \to \{\text{senses of humour}\}$$

that assigns to each person their sense of humour, what's being said is that

$$f(x) = f(\text{Anna}) \implies x = \text{Anna}$$

for all people $x$.

On the other hand, the mathematical statement 'every real number has a unique square' means that for all real numbers $x$, there is one and only one number $y$ that is the square of $x$. If we take the function

$$s\colon \mathbb{R} \to \mathbb{R}$$

that assigns to each number $x$ its square $x^2$, what's being said is that for every $x \in \mathbb{R}$, there is a unique $y \in \mathbb{R}$ such that $s(x) = y$. (That's what it means for $s$ to be a function.) In contrast with the everyday English example, we're *not* saying that

$$s(x) = s(x') \implies x = x'$$

for all real $x$ and $x'$. In fact, that's false, since $s(10) = s(-10)$, for instance.

More to the point, consider the statement 'for all real numbers $x$, there exists a unique integer $n$ such that $x - 1 < n \leq x$'. This means that given any real $x$, there is

*one and only one* integer $n$ such that $x - 1 < n \leq x$. (There *is* one, and there's *only* one.) For example, if $x = 4.8$ then the unique integer $n$ such that $3.8 < n \leq 4.8$ is 4, and generally, this $n$ is the so-called integer part or floor of $x$, denoted by $\lfloor x \rfloor$. The word 'unique' here does *not* mean that different values of $x$ give different values of $n$. And they don't: $\lfloor 4.8 \rfloor = \lfloor 4.9 \rfloor$, for instance.

Here's my top tip:

> *Whenever you see the words 'a unique', replace them mentally by 'exactly one'.*

For instance, the two mathematical statements above become 'every real number has exactly one square' and 'for all real numbers $x$, there exists exactly one integer $n$ such that $x - 1 < n \leq x$'.

To prove the statement 'there exists a unique *something* such that *whatever*', you therefore have to do two things.

- First, show there *exists* a something such that whatever—in other words, there is *at least one* something such that whatever. This often involves actually constructing the thing, then proving that the thing you constructed satisfies the condition I'm calling 'whatever'.

- Then, prove *uniqueness*: there is *only one* something such that whatever. Typically, you do this by saying 'let $m$ and $n$ be somethings such that whatever' then proving that $m = n$.

A common error that people make in uniqueness proofs is writing sentences like '$n$ is unique.' This rarely makes sense. Almost always, what you should be writing is something like '$n$ is the unique integer such that whatever'.

If all this sounds rather general, don't worry: in a week or two, you'll start working with specific cases. And if you keep it firmly in mind that 'a unique' means 'exactly one', you should never go wrong.

# Chapter 1

# Introduction

*To read by Friday 20 September: Sections 1.1–1.8.*
*Optional: Section 1.9.*

This course is in some respects unlike any course you're likely to have taken before. Especially in the early parts, it requires thinking in a different way. In this introduction, I'll explain what axiomatic set theory is all about, then tell you about the particular approach to it that we're going to take.

Also, this chapter is different from all the others: there are no theorems, proofs, or even definitions here. However, the *ideas* I'll explain here are crucial. If you take the time to understand them, you should find it helps you enormously for the whole of the course.

## 1.1 What are axioms and why do we need them?

I once began a talk to a large roomful of mathematicians by asking everyone to raise their hand if they were sure they knew the definition of group. Everyone's hand went up. While the hands stayed up, we agreed that the definition began: 'a group is a set equipped with . . . '. So, I said, if you're confident you know what a group is, and the definition of group depends on the definition of set, then you must be at least as confident that you know what a set is. Nervous laughter. Then I asked the audience to keep their hands up if they were sure they knew what a set was—if they could state a rigorous definition or axioms. More nervous chuckles, and almost every hand went down.

This is, as I said to the audience, a very peculiar situation. Sets appear implicitly or explicitly on almost every page of every mathematical publication, yet very few mathematicians can say precisely what a set actually is. We pride ourselves on our

rigour—some would say that rigour is even what *defines* mathematics—but when it comes to this very basic concept, we seem to give ourselves a free pass.

You've probably never read a sentence beginning 'Definition: a *set* is . . . '—at least, not a rigorous one. Why not?

For a start, because the concept of set is usually seen as very fundamental and basic, so it would be unusual to define it in terms of some other concept, which would have to be *even more* fundamental and basic. But more importantly, because we have to stop somewhere. If sets were defined in terms of some other concept, then how would that other concept be defined? We can't keep retreating forever.

On the other hand, mathematics is supposed to be absolutely rigorous and watertight. We're not supposed to rely on intuition, which can easily lead us astray. (For example, we might fall into the trap of thinking that infinite sets behave like finite sets.) What if my intuition about sets was different from yours? How would we decide who was right?

The solution is that we don't attempt to *define* sets, but we do *axiomatize* them. In other words, we write down a list of properties (**axioms**) and assume that sets satisfy them.

This list of axioms acts like a contract or agreement. For instance, if you claim that some construction with sets can be done, but I'm sceptical, then you can point to the list of axioms and say 'look, it follows from Axioms 2, 4 and 6, by this argument.' Or if I claim that some theorem holds for sets, but you disagree, you can say 'look, I can construct a counterexample using Axioms 3, 6 and 9.'

So an axiomatization functions as an agreed set of rules, just like for football or chess. The axioms are *not* statements about what's 'true' for sets, because what would that even mean? It's not as if there's a physical world of sets against which we can test the truth of statements. An axiomatization is just an agreement about how we're going to use the word 'set'.

**Digression 1.1.1** It may be that some questions can't be settled from the axioms. For example, the **continuum hypothesis** states that every infinite subset of $\mathbb{R}$ is in bijection with either $\mathbb{N}$ or $\mathbb{R}$. The most common axiomatizations of sets, including the one we'll use, do not determine whether the continuum hypothesis is true or false. In other words, they imply neither the continuum hypothesis nor its negation.

In fact, Gödel's first incompleteness theorem implies (roughly) that however long our list of axioms is, there will always be some statement that can neither be proved nor disproved from the axioms.

All this is well beyond the scope of this course. We'll focus on the things that *can* be proved from our axioms, which will already fill up our time.

There's another reason to axiomatize sets: it's good for you! What I mean

is that many other parts of mathematics depend on sets, so being confident in manipulating sets will help you across the board. And building up the theory of sets from a short list of axioms—as we'll do—will really improve your skills.

For example, many students find quotient groups (or rings) and the first isomorphism theorem quite difficult. One reason is that when quotient groups are defined, two things are being done at once: something purely set-theoretic (quotienting a set by an equivalence relation) and something specifically group-theoretic. Similarly, there's a first isomorphism theorem for sets (which we'll do in Chapter 6), and it's helpful to get to know that first before meeting its more sophisticated group-theoretic cousin. Swallowing two things simultaneously is harder than swallowing them one at a time.

What is a set anyway? Well, it's whatever our axioms say it is. You know how mathematical definitions work: if a natural number $n$ is defined to be *enormous* if $n < 10$, then that's simply what 'enormous' means, regardless of the conflict with ordinary English usage. If the rules of chess say that bishops can move in this way but not that way, then that's just how it is.

But of course, we want to choose our axioms so that they reflect as closely as possible how sets are actually used in mathematical practice, by the 99% or so of mathematicians who are not set theorists.

So how *are* sets used in practice? The first point is that the sets arising in mathematics almost always come with some extra structure: they're not merely sets. For example, $\mathbb{R}$ has *lots* of structure: it's a group (you can add and subtract real numbers), it's a ring (you can also multiply them), it's a metric space (there's a notion of the distance between two reals), it's an ordered set (we know what it means for one real number to be less than another), and so on.

You might think that a random-looking set like $\{7, 10, 12\}$ has no extra structure, but it does. Since the elements have been called 7, 10 and 12, we're supposed to think of it as a subset of the natural numbers, which means that it comes with an inclusion function

$$i\colon \{7, 10, 12\} \to \mathbb{N}$$

(the function defined by $i(7) = 7$, $i(10) = 10$ and $i(12) = 12$). That's extra structure already. But it also means, for instance, that $\{7, 10, 12\}$ inherits the structure of an ordered set and a metric space from $\mathbb{N}$ (e.g. $7 < 10$, and the distance between 7 and 10 is 3) .

Similarly, if someone says 'the set $P$ of prime numbers', they obviously don't just mean a countably infinite set: they have in mind the inclusion of $P$ into $\mathbb{N}$. Otherwise, it would be impossible to make sense of questions like 'which prime numbers can be expressed as the sum of two squares?'

The upshot is that almost everyone is much more used to handling sets with extra structure than sets with *no* structure. So if we want our set theory to fit well

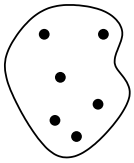


Figure 1.1: A set is a bag of featureless dots (perhaps infinitely many).

with how the rest of mathematics is done, we should take our inspiration from the way sets are handled when they're structured.

It's therefore helpful to think of sets as like groups with no group structure, or metric spaces with no metric, etc. Our theory of sets will be like the theory of groups, or rings, or topological spaces, or vector spaces, or any other kind of set-with-structure—but in the extreme case that there happens to be *no* structure.

For example, treating $\mathbb{R}$ as a mere set means ignoring all the structure on it (its addition, multiplication, metric, order, ...), and viewing it as no more than a bunch of featureless dots (Figure 1.1).

Figuring out a good axiomatization of sets is in a kind of mathematical modelling. A mathematical biologist might create a model of how wildebeest populations move about the landscape. What we're modelling is not wildebeest but mathematicians, and specifically, how mathematicians use sets in their day-to-day work. We should choose axioms that embody ordinary mathematical practice.

**Warning 1.1.2** Mathematicians are human beings! And although mathematical language is much more precise than most natural languages, there are still some inconsistencies.

For example, most mathematicians would say that $\mathbb{R}$ is a subset of $\mathbb{C}$, and the set $\mathbb{C}$ is often defined as $\mathbb{R}^2$. But 6 is an element of $\mathbb{R}$, so if $\mathbb{R} \subseteq \mathbb{C} = \mathbb{R}^2$ then 6 is an element of $\mathbb{R}^2$—which we would *not* say.

Small inconsistencies like this are all over mathematics. (Another example: we blur the distinction between a $1 \times 1$ matrix and a scalar.) They are often called *abuses of language* or *abuses of notation*, and they're essential in real-life human mathematics to prevent us from being buried in an avalanche of symbols.

Where these abuses of language concern sets, it's the business of axiomatic set theory to justify them. In other words, we have to figure out exactly what is going on, in rigorous terms. Once we've done that, we can join in with the same abuses of language as everyone else. But if we want mathematics to be 100% watertight, then sooner or later we have to justify the liberties that we habitually take.

## 1.2 Selecting the primitive concepts

Given elements $v, w, x, y, z$ of a vector space $V$, we can form the new element

$$3v - w - 2x + 4y + z$$

of $V$. However, if you look in the definition of vector space for the operation that takes $(v, w, x, y, z)$ as input and produces $3v - w - 2x + 4y + z$ as output, it's nowhere to be seen. The standard definition only involves adding up *two* elements, and multiplying one element by a scalar. To get $3v - w - 2x + 4y + z$, you have to repeatedly apply the 'primitive' operations—the ones actually appearing in the definition. Way back in time, someone figured out that the most efficient way to present the definition of vector space was to take certain operations (like adding up two elements) as primitive, and derive all the other operations (like $(v, w, x, y, z) \mapsto 3v - w - 2x + 4y + z$) from them.

Similarly, when we axiomatize sets, we're going to have to choose some set-theoretic concepts as the 'primitive' ones, and derive the others. Your everyday set-theoretic vocabulary involves concepts like set, subset, element, function, equivalence relation, and so on. Eventually, we want to derive all of them. But which ones should we take as primitive?

Your first thought might be that *element* should be a primitive concept. After all, almost everyone is first introduced to sets with examples like $\{\text{apple}, \text{banana}, \text{cherry}\}$ or $\{\text{Akil}, \text{Ben}, \text{Charlotte}\}$. This suggests a universe of 'things', and that every set we meet contains some of those things as elements but not others.

But mathematics doesn't really work like that. In actual mathematical practice, it doesn't matter what the elements of a set 'are' or are called. For example, what are the elements of the group $C_2$ of order 2? You could write them as $\{e, x\}$, or $\{1, \sigma\}$, or $\{-1, +1\}$, and clearly it makes no difference. No meaningful group-theoretic statement depends on the names of the elements. Similarly, the numerals $1, 2, 3, 4, \ldots$ are just arbitrary symbols invented at some point in history, and, for instance, no theorem about the integers would suddenly become false if instead we wrote *1*, *2*, *3*, *4*, ... or I, II, III, IV, ... instead.

Modern mathematics takes this point in its stride with the notion of *isomorphism*. This has many incarnations. You've probably met isomorphism for groups and rings, and maybe vector spaces too; perhaps you've also met it for metric spaces (where it's called isometry), topological spaces (where it's called homeomorphism), or even manifolds (where it's called diffeomorphism). In all cases, an isomorphism is an invertible map $f$ such that both $f$ and $f^{-1}$ preserve whatever structure we're considering. An isomorphism can often be understood as a renaming or relabelling of the elements. For example, the three versions of $C_2$ in

the previous paragraph are all isomorphic, because you can get between them by simply renaming the elements.

So if someone asks 'is $x$ an element of $C_2$?', there is no meaningful answer. If you call the elements $e$ and $x$, yes. If you call them $e$ and $y$, no. The group $C_2$ is only defined up to isomorphism.

In fact, modern mathematics makes crucial use of not just *isomorphisms* but arbitrary *functions*. I've already mentioned quite a few functions implicitly. For example, addition and multiplication of real numbers are functions

$$+\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \qquad \cdot\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}.$$

I've also mentioned inclusion functions, such as the inclusion

$$\{\text{prime numbers}\} \to \mathbb{N}.$$

The order relation $\leq$ on $\mathbb{R}$ can be viewed as a function too, namely, the inclusion

$$\{(x, y) \in \mathbb{R}^2 : x \leq y\} \to \mathbb{R}^2.$$

We'll soon see that *even the concept of element is a special case of the concept of function!*

So: our approach will be to take sets and functions as the primitive concepts. We will take composition of functions and identity functions as primitive too. Every other set-theoretic concept will be derived from these four primitive concepts.

This approach to axiomatizing sets was introduced in the 1960s by F. William Lawvere. So it's not new! However, for various historical reasons, it hasn't received the full development that it might have. In this course, we'll develop it fully.

Lawvere's axiomatization is called **ETCS**, which stands for the Elementary Theory of the Category of Sets. It has been studied quite intensively within category theory, or more specifically in a sub-branch of category theory called topos theory. But in this course, I'll present it in a completely elementary way. I won't assume you know about categories, and I won't teach you about categories. Building up set theory from the ETCS axioms in an elementary, category-free way is what's new about this course.

## 1.3 Elements as functions

We will state our axioms on sets and functions in Chapters 2 and 3. However, I want to prepare you now for one of the big ideas behind those axioms, which is that elements can be understood as special functions.

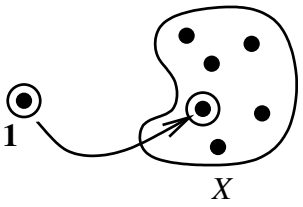



Figure 1.2: An element of a set $X$ is a function from the one-element set $\mathbf{1}$ to $X$.

Suppose that we have somehow managed to lay our hands on a one-element set without having a prior notion of element. (You'll see how to do that next week.) Fix a one-element set $\mathbf{1} = \{\bullet\}$.

For any set $X$, a function $\mathbf{1} \to X$ is essentially just an element of $X$ (Figure 1.2). In more detail: given a function $\mathbf{1} \to X$, we get the element $x = f(\bullet)$ of $X$, and given an element $x \in X$, there is a function $\bar{x} \colon \mathbf{1} \to X$ defined by $\bar{x}(\bullet) = x$. This defines a one-to-one correspondence between functions $\mathbf{1} \to X$ and elements of $X$.

In the next chapter, we're going to *define* an element of $X$ to be a function $\mathbf{1} \to X$. That's how we'll derive the concept of element from the concept of function. In a slogan:

*Elements are a special case of functions.*

In other words, we're going to erase the distinction between the element $x$ and the function that we just called $\bar{x}$. For us, they're the same thing; $x$ *is* $\bar{x}$, so there's no need for the bar.

This may make you uncomfortable. You'll agree, I hope, that there is a one-to-one correspondence between elements of $X$ and functions $\mathbf{1} \to X$, but you might feel it's a step too far to say they're literally the same thing.

If so, I'd first of all mention the point made earlier: in mathematics generally, there's no meaningful distinction between objects that are isomorphic.

Second, you're already very used to a similar definition. Every calculus book defines a *sequence* as a function with domain $\mathbb{N}$. Now, we don't usually *think* of sequences as functions, and that's reflected in the notation. No one says 'let $f$ be a sequence'; we say 'let $(x_n)_{n=0}^{\infty}$ be a sequence', and write $x_n$ instead of $f(n)$. But that's how sequences are formally defined, and it's hard to think of any other possible definition.

If someone said to you 'I agree that there's a one-to-one correspondence between real sequences and functions $\mathbb{N} \to \mathbb{R}$, but *defining* them that way is a step too far', it would be quite hard to answer them, because there's not really a mathematical point there. The same goes for elements and functions out of $\mathbf{1}$.

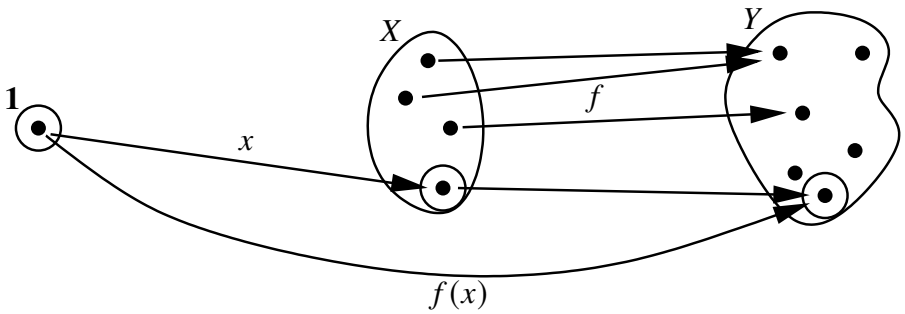



Figure 1.3: Evaluating a function $f\colon X \to Y$ at an element $x \in X$ gives an element $f(x) \in Y$.

**Digression 1.3.1** If you still resist defining elements as special functions, it's not a deal-breaker. We could adapt the axiomatization in Chapters 2 and 3 by adding elements as a fifth primitive concept. Then we would need to add a bunch of further axioms involving elements. And those axioms would in any case imply that there is a one-to-one correspondence between elements of $X$ and functions $\mathbf{1} \to X$, for any set $X$. It can be done, but it adds complication for no real gain.

We have seen that elements are a special case of functions. There is another fundamental way in which elements and functions interact: given a function $f\colon X \to Y$ and an element $x \in X$, we can evaluate $f$ at $x$ to obtain a new element, $f(x) \in Y$. Viewing elements as functions out of $\mathbf{1}$, this element $f(x)$ is nothing but the composite of $f$ with $x$ (Figure 1.3):

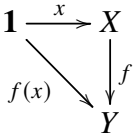
$$f(x) = f \circ x.$$

If you want to go back to the bar notation, where $\bar{x}\colon \mathbf{1} \to X$ denotes the function corresponding to an element $x \in X$, then the equation is

$$\overline{f(x)} = f \circ \bar{x}.$$

But we drop the bars. In fact, we sometimes also drop the brackets around $x$ (like writing $\log x$ instead of $\log(x)$), and we often write a composite $f \circ g$ as just $fg$, so both sides of the equation can reasonably be written as just $fx$.

Another way to say this is that the diagram



'commutes'. I'll often use this terminology: for a diagram to **commute** (or to be **commutative**) means that whenever you have two different paths from one object to another (here, $\mathbf{1}$ and $Y$), composing along one path gives the same result as composing along the other. Here, it means $f \circ x = f(x)$.

In summary:

*Evaluation is a special case of composition.*

So far in this section, I've outlined how the concepts of element and of evaluation of a function at an element can be derived from our four primitive concepts: set, function, composition and identities. What about subsets?

We'll get into this in more detail in a couple of weeks, but here's a brief explanation. Suppose that we've somehow managed to lay our hands on a two-element set. Call it $\mathbf{2} = \{\mathsf{T}, \mathsf{F}\}$, for 'true' and 'false'. To specify a subset $A$ of a set $X$, we have to answer the question 'is $x \in A$?' for each element $x \in X$. The answer can either be 'true' or 'false'. So, to specify a subset of $X$ is exactly to give a function $X \to \mathbf{2}$. We will *define* a subset of $X$ to be a function $X \to \mathbf{2}$.

There is an alternative way of getting the subset concept from our primitive concepts. We already glimpsed it when we discussed inclusion functions. A subset of $X$ is essentially just an injection $A \to X$. The idea is that given any 'actual' subset, we have the inclusion $A \to X$, which is injective. On the other hand, given any injection $i\colon A \to X$, we can take its image, which is a subset of $X$. These back-and-forth processes between subsets of $X$ and injections into $X$ are more or less inverse to each other, but not quite, because two different injections into $X$ can have the same image. We'll look at this more carefully in Week 3.

## 1.4 Everyday operating principles

Let's go back to that talk I gave, in which it became apparent that only a very small proportion of mathematicians could give a rigorous definition or axiomatization of sets if their lives depended on it.

The fact remains that mathematicians manipulate sets with confidence every day. Whenever you work with sets of real or complex numbers, or the set of solutions of a differential equation, or groups or topological spaces or manifolds, you're working with sets. The underlying set-theoretic manipulations are usually only the most trivial part of what we do, so we barely even give them a thought, but they're there under the surface all the time.

What this suggests is that even though few of us know any 'official' system of axioms, we all carry around with us a reliable body of operating principles that we use when manipulating sets. The idea of this course is to write down some of these principles and adopt them as our axioms.

| | |
|---|---|
| 1 | Composition of functions obeys associativity and identity laws. |
| 2 | There is a set with exactly one element. |
| 3 | A function is determined by its effect on elements. |
| 4 | There is a set with no elements. |
| 5 | Given sets $X$ and $Y$, one can form their cartesian product $X \times Y$. |
| 6 | Given sets $X$ and $Y$, one can form the set of functions from $X$ to $Y$. |
| 7 | Given $f : X \to Y$ and $y \in Y$, one can form the preimage $f^{-1}(y)$. |
| 8 | The subsets of a set $X$ correspond to the functions from $X$ to $\{\mathsf{T}, \mathsf{F}\}$. |
| 9 | The natural numbers form a set. |
| 10 | Every surjection has a right inverse. |

Figure 1.4: Informal summary of the axioms.

The list of axioms we'll arrive at is stated informally in Figure 1.4. Over the next two weeks, we'll make them formal and precise. For now, here's a quick overview.

Recall that we're taking the following as our primitive concepts:

- sets;
- functions between sets;
- composition of functions;
- identity functions.

Every other concept has to be defined in terms of these. So, for instance, when 'elements' are mentioned in this list, we define elements in terms of functions, as in Section 1.3. And as hinted above, for Axiom 2, we'll find a way of saying 'set with exactly one element' without knowing what 'element' means.

In Axioms 5–7, we'll need to find ways to say 'cartesian product', 'set of functions' and 'preimage' in terms of sets and functions only. And Axiom 9 is vague as it stands: what are the natural numbers anyway?

Axiom 8 expresses the correspondence described at the end of Section 1.3. In other words, it says (loosely) that injections into $X$ correspond to functions $X \to \{\mathsf{T}, \mathsf{F}\}$. In fact, the formal axiom will be weaker: it will only say that *there is some set* $\Omega$ such that for all sets $X$, injections into $X$ correspond to functions $X \to \Omega$. But the other axioms imply that $\Omega$ has exactly two elements, as we'll prove.

An important feature of the approach we take is that *we never ask whether two sets are equal*, just as a group theorist would never ask whether two groups are equal—only whether they're isomorphic. (Is *this* trivial group equal to *that* trivial

group? Who cares! It's barely even a meaningful question.) As we'll see, it's fine to ask whether two *subsets* of a given set are equal, just as a group theorist might ask whether two subgroups of a given group are equal. Again, we're imitating how everyday mathematics works.

**Digression 1.4.1** Another feature of our approach is that each of the axioms has a life outside set theory. I mentioned that it's useful to think of sets as being like any other kind of sets-with-structure (groups, rings, fields, vector spaces, metric spaces, topological spaces, ...), just in the extreme case where there happens to be no structure at all. If you pick any other type of set-with-structure, you'll find that some of the set axioms hold and others don't, and where they fail is usually a point of interest.

For example, consider Axiom 10, which is called the axiom of choice. The squaring map $\mathbb{C} \to \mathbb{C}$ is continuous and surjective but has no continuous right inverse. That is, there is no continuous function $\sqrt{}: \mathbb{C} \to \mathbb{C}$ such that $\sqrt{z}^2 = z$ for all $z \in \mathbb{C}$. (If you believe there is, think about what would happen to $\sqrt{z}$ as you gradually moved $z$ one revolution around the unit circle.) The absence of a continuous square root function is highly significant in complex analysis, and is an instance of the fact that the axiom of choice fails for topological spaces and continuous maps.

At the end of Section 1.2, I mentioned that the axioms originally arose in the context of category theory (which isn't a part of this course). Axiom 1 says that sets and functions form a category, and the job of the other axioms is to distinguish it from other categories. Some collections of the axioms are particularly significant; for example, Axioms 1–2 and 5–8 are the axioms for a topos (ignoring one technicality), and toposes are an especially important type of category at the heart of an incredible story unifying geometry and logic. Sadly, there's no time to tell that story here.

## 1.5 The importance of codomains

As you (hopefully) learned in Proofs and Problem Solving, a function consists of not one but three things:

- a set $X$, called the *domain*;
- a set $Y$, called the *codomain*;
- a 'rule' $f$ assigning to each element of $X$ exactly one element of $Y$.

We then write the function as $f: X \to Y$, as I've been doing so far.

'Rule' is not a precise word, and our axioms will address that. But the point I want to make now is that a function isn't just an '$f$'; it comes along with a domain and a codomain. If you change the domain or codomain, you change the function. If you don't specify a domain or codomain, you haven't specified a function. And if $f$ and $g$ have different domains or different codomains, then it's inconceivable that $f$ and $g$ could be equal, just as it's inconceivable for a $3 \times 4$ matrix to be equal to a $5 \times 2$ matrix.

For example, the functions

$$\begin{array}{rccc} f\colon & \mathbb{R} & \to & \mathbb{R}, \\ & x & \mapsto & x^2 \end{array} \qquad \begin{array}{rccc} g\colon & \mathbb{R} & \to & \mathbb{C}, \\ & y & \mapsto & y^2 \end{array} \qquad \begin{array}{rccc} h\colon & \mathbb{C} & \to & \mathbb{C} \\ & z & \mapsto & z^2 \end{array}$$

are all different, even though they're all defined by the same 'rule'. That's just how the definition of function works. They're *related*; for example, you can get from $f$ to $g$ by composing with the inclusion $\mathbb{R} \to \mathbb{C}$. But they're not the same.

The idea that a function should have a specified codomain can take some getting used to, but it's crucial for everything we do, so I'm going to use this section to explain.

First, we need to distinguish between codomains and images. The codomain of a function $f\colon X \to Y$ is $Y$, by definition. But the image is

$$\operatorname{im} f = \{y \in Y : y = f(x) \text{ for some } x \in X\}.$$

This is a *subset* of the codomain $Y$, and not always equal to it. For example, the squaring map $f\colon \mathbb{R} \to \mathbb{R}$ has codomain $\mathbb{R}$ and image $\mathbb{R}^+$. The image is only equal to the codomain when the function is surjective.

**Warning 1.5.1** The word *range* is often used instead of image. However, *range* is also used by some authors to mean codomain. To avoid ambiguity, I will avoid the word entirely.

But why do we need the concept of codomain at all? Why don't we stick with images? Mathematicians only came to realize the importance of codomains quite recently—about the 1940s, which counts as recent in the history of mathematics. So it's not obvious. Here are several answers.

- *Images can be hard to describe.* What is the image of the function $f\colon \mathbb{R} \to \mathbb{R}$ defined by
$$f(x) = x^6 + 3x^4 - 2x + 5?$$
I have no idea. But the codomain is easy: by definition, it's just $\mathbb{R}$.

- *We want to combine functions of the same type.* For example, given any set $X$ and functions $f, g\colon X \to \mathbb{R}$, we can form the sum function $f+g\colon X \to \mathbb{R}$ and the product function $f \cdot g\colon X \to \mathbb{R}$. This makes the set of functions from $X$ to $\mathbb{R}$ into a ring, which turns out to be a very important insight in subjects such as functional analysis. But the images of $f+g$ and $f \cdot g$ are different from those of $f$ and $g$, so it would be hard to express this insight without the concept of codomain.

- *We want to consider collections of functions.* In dynamical systems, for instance, we may have a space $X$ of some kind and a function $f\colon X \to X$, and the goal is to consider the sequence of iterated composites

$$f^1 = f,\ f^2 = f \circ f,\ f^3 = f \circ f \circ f,\ \ldots$$

  as the number of iterates tends to infinity. The image of $f^n$ may vary wildly and unpredictably as $n$ grows, but by definition, the codomain is always just $X$.

- *It allows you to talk about surjectivity.* A function is surjective if its image is the whole codomain. So the concept of surjectivity is impossible to express without the concept of codomain. (Of course, you can then ask what the point of surjectivity is. . . )

- *It fits with other parts of mathematics.* For example, you learned in Introduction to Linear Algebra about the one-to-one correspondence between $m \times n$ real matrices and linear transformations $\mathbb{R}^n \to \mathbb{R}^m$. Here the codomain is $\mathbb{R}^m$, but once again, the image is a more complicated and sensitive object. In this case, it has to do with the column space of the corresponding matrix.

- *Some subjects are unthinkable without it.* For example, homology theory (which you may meet if you take Algebraic Topology) is full of diagrams like this:

$$\cdots \xrightarrow{f_{n+1}} A_n \xrightarrow{f_n} A_{n-1} \xrightarrow{f_{n-1}} \cdots,$$

  where each $A_n$ is a group and each $f_n$ is a homomorphism. We then do things like comparing the image of $f_{n+1}$ with the kernel of $f_n$ (both being subgroups of $A_n$). The whole subject is simply unthinkable without systematic use of codomains.

- *What exactly would the alternative be?* Mathematics uses functions that take values not just in the real numbers, but in arbitrary groups, rings, vector spaces, manifolds, etc., so it's not so clear how else we could set things up. There's no 'universal set' containing all the objects we might ever think of.

> Defining functions without codomains *can* be done (I won't explain how), but only at the cost of a distorted interpretation of mathematics as it's usually practised.

The domain of a function is its 'input type': the type of thing that the function takes as its input. The codomain, similarly, is the 'output type'. Keeping track of the type of everything is very useful in mathematics. But what do I mean by 'type'? Read on...

## 1.6 Types

Suppose someone asks you 'is $\sqrt{2} = \pi$?' Your answer, of course, is 'no'. Now suppose someone asks you 'is $\sqrt{2} = \log$?' You might frown and wonder if you had heard right, and perhaps your answer would again be 'no'; but it would be a different kind of 'no'. After all, $\sqrt{2}$ is a number, whereas log is a function, so it is inconceivable that they could be equal. A better answer would be 'your question makes no sense'.

This illustrates the idea of **types**. The square root of 2 is a real number, $\mathbb{Q}$ is a field, $S_3$ is a group, log is a function from $(0, \infty)$ to $\mathbb{R}$, and $\frac{d}{dx}$ is an operation that takes as input one function from $\mathbb{R}$ to $\mathbb{R}$ and produces as output another such function. We say that the type of $\sqrt{2}$ is 'real number', the type of $\mathbb{Q}$ is 'field', and so on. We all have an inbuilt sense of type, and it would not usually occur to us to ask whether two things of different types were equal.

School-level mathematics doesn't involve many different types, maybe not much more than integers, real numbers, and maybe vectors and matrices. They're managed informally, with types distinguished by conventions like using $n$ for integers and underlining vectors. But at university level and beyond, the diversity of types grows fast and we need to be systematic.

For example, in Proofs and Problem Solving, you met the set $S_n$ of permutations of $n$ letters. The elements of $S_n$ are certain functions from the set $\{1, \ldots, n\}$ to itself. You also met the composition operation

$$\circ \colon S_n \times S_n \to S_n.$$

What is its type? It's

> a function from a product of two sets of functions between sets to a set of functions between sets.

And that's just the first year.

Human beings make all sorts of intuitive leaps. If you meet something called $\varepsilon$, you assume it's a small positive real number. If you're told to take the gcd of

$x$ and $y$, you probably assume they're integers. Mathematical language as used by humans contains many hidden assumptions. But an axiom system has to bring the hidden assumptions out into the open. To get into the right frame of mind, it's useful to think about communicating with computers, which don't know anything unless they're told.

In fact, you may have already met the idea of type if you've done some programming. Many programming languages require you to declare the type of a variable before you first use it. For example, you might declare that $x$ is to be a variable of type 'real number', $n$ a variable of type 'integer', $M$ a variable of type '$3 \times 3$ matrix of lists of binary digits', and so on.

Now suppose you have a programming language or computer algebra package that has a built-in function for taking the square root of a nonnegative real number. You define a new variable $n$ of type 'natural number', you set $n$ to 2, then you ask the computer to take the square root of $n$. The result may be an error message, because you didn't give the square root function an input of the right type. To make it work, you first have to convert $n$ into a nonnegative real, and only then take its square root. In set-theoretic terms, you're forming the composite function

$$\mathbb{N} \xrightarrow{i} \mathbb{R}^+ \xrightarrow{\sqrt{}} \mathbb{R},$$

where $i$ is the inclusion. Alternatively, if your language does 'type inference', it may silently convert $n$ into a nonnegative real, guessing that's what you meant, as a human would. But it's the same composite process. In both cases, the first step is to pass from the natural number $n$ to the real number $i(n)$.

However, passing to a bigger type isn't always the right thing to do. For example, suppose our language also has a built-in function for taking the prime factorization of a natural number. If we apply this function to our variable $n$, then we definitely *don't* want to convert $n$ into a real number first, as prime factorization isn't defined for the reals.

And in any case, there's no 'biggest type' containing all others. Beyond number systems like $\mathbb{N}$, $\mathbb{R}$ and $\mathbb{C}$, mathematics contains polynomial rings $\mathbb{C}[x_1, \ldots, x_n]$, vector spaces like $\mathbb{C}^n$, rings of matrices, arbitrary rings, groups, sets of functions of various kinds (remember the composition operation on $S_n$), and so on.

So far I've described a world of different types related by inclusions between them, like $\mathbb{N}$ being included in $\mathbb{R}$. But some types are related in other ways. For instance, $\mathbb{Z}/3\mathbb{Z}$, the system of integers mod 3, is obtained from $\mathbb{Z}$ by regarding $m, n \in \mathbb{Z}$ as equal whenever $m - n$ is divisible by 3. In set-theoretic terms, there's a surjection $p\colon \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ that sends an integer $n$ to its congruence class $p(n)$. So $\mathbb{Z}/3\mathbb{Z}$ is most naturally seen as a *quotient* of $\mathbb{Z}$, not a subset.

## 1.7 An element is an element of only one set

I've said that we're going to define an element $x$ of a set $X$ to be a function $x\colon \mathbf{1} \to X$, where $\mathbf{1}$ is a fixed one-element set. I've also emphasized that every function comes with a specified codomain, and that changing the codomain changes the function. Putting those two points together, the result is that

*every element is an element of only one set.*

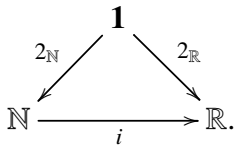
After all, if $x$ is an element of both $X$ and $Y$, that means the codomain of $x$ (as a function) is both $X$ and $Y$. And since a function has only one codomain, that can only happen if $X = Y$.

Is this right? We're trying to set things up to align with everyday mathematical practice, but surely 2 is an element of both $\mathbb{N}$ and $\mathbb{R}$, for example?

I want to convince you that it *is* right, and it *does* align with everyday practice.

First, let's turn the question around: given two different sets $X$ and $Y$, does it make sense to ask whether an element of $X$ is equal to an element of $Y$? For instance, does it make sense to ask whether an element of the cyclic group $C_5$ is equal to an element of $\mathbb{Z}$? No. We've already seen this: for example, if you write $C_5$ as $\{0, 1, 2, 3, 4\}$ (the integers modulo 5) then it looks as if all its elements are in $\mathbb{Z}$, but if you write them as $\{e, x, x^2, x^3, x^4\}$, it looks as if none of them are. And no meaningful mathematical statement should depend on how you happen to name the elements of your sets. Everything should be isomorphism-invariant.

But although the general answer is no, there are cases where you might argue that the answer should be yes. For instance, you might feel it makes sense to ask whether an element of $\mathbb{N}$ is equal to an element of $\mathbb{R}$. What's going on here is that *in this particular case*, we intuitively link up the two sets by the inclusion function $i : \mathbb{N} \to \mathbb{R}$. So, for example, if we write $2_{\mathbb{N}}$ for the natural number 2 and $2_{\mathbb{R}}$ for the real number 2, then $i(2_{\mathbb{N}}) = 2_{\mathbb{R}}$. In a commutative diagram:




Remember the example in the previous section about asking a computer to take the square root of a natural number $n$, and how we first had to take the step of converting $n$ into a (nonnegative) real. The situation here is just the same. Everything has just one type, just as every element is an element of just one set.

Of course, in everyday mathematics we don't write $2_{\mathbb{N}}$ or $2_{\mathbb{R}}$; we just write 2. As fallible human beings who cope badly with too many symbols, we minimize notation as much as we can get away with. But sometimes we have to be careful.

For example, the ring $\mathbb{Z}/3\mathbb{Z}$ has an element usually called 2. Is this equal to the integer 2? If you think it is, then you presumably also think that the integer 2 is equal to the element 2 of $\mathbb{Z}/5\mathbb{Z}$. So by transitivity, you're forced to conclude that the elements $2 \in \mathbb{Z}/3\mathbb{Z}$ and $2 \in \mathbb{Z}/5\mathbb{Z}$ are equal. But what does it mean for an element of $\mathbb{Z}/3\mathbb{Z}$ to be 'equal' to an element of $\mathbb{Z}/5\mathbb{Z}$? I know of no reasonable definition, and I don't believe there is one. So the moral is that it's better *not* to start talking about elements of $\mathbb{Z}$ being 'equal' (or not) to elements of $\mathbb{Z}/n\mathbb{Z}$.

There's another practical reason why it's essential to keep track of your ambient set. Consider the following questions:

- Does 2 have a square root? No if you're working in $\mathbb{Z}$ or $\mathbb{Q}$; yes if you're working in $\mathbb{R}$ or $\mathbb{C}$. That is, the element of $2_{\mathbb{Z}}$ of $\mathbb{Z}$ has no square root, but the element $2_{\mathbb{R}}$ of $\mathbb{R}$ does, etc. The question as stated has no clear yes/no answer.

- Does the sequence $3, 3.1, 3.14, 3.141, \ldots$ of approximations to $\pi$ converge? No in $\mathbb{Q}$, yes in $\mathbb{R}$. It depends on which set our numbers are taken to live in.

- Is the number 13 prime? Yes in $\mathbb{Z}$, but no in the ring

$$\{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\},$$

  since $13 = (3 - 2i)(3 + 2i)$. (This thought leads to a very nice proof that any prime congruent to 1 mod 4 is the sum of two integer squares, Dedekind's second proof.)

In all these cases, the set $X$ in which our elements live is not just a set but a set *with structure*, and the question can only be answered once we know what $X$ is.

I'm trying to persuade you that if we want our approach to set theory to both be rigorous and fit well with how mathematics is actually done, it's best to adopt the view that any element of a set is an element of *only* that set. 'But hold on,' I hear you say. 'If we have an element $n$ of $\mathbb{N}$, don't I have the right to ask whether $n \in \{8, 9, 10\}$?'

This is a good question. In brief, the answer is that there are actually *two* kinds of set membership in play. When we say 'let $n \in \mathbb{N}$' to introduce a thing called $n$ for the first time, that's a type declaration. We're declaring that $n$ will denote a variable of type 'natural number'. It's not something that's true or false. But when we ask 'is $n \in \{8, 9, 10\}$?', that is a true/false question. Again, the distinction between the two kinds of membership is made in some programming languages. We will come back to this point in Chapter 4 (Subsets).

The attitude of the vast majority of mathematicians to questions like 'is the natural number 2 literally *equal* to the real number 2?' or 'is $\mathbb{R}$ *literally* a subset of $\mathbb{C}$, or is there just a canonical embedding of $\mathbb{R}$ into $\mathbb{C}$?' is that they very profoundly

do not care. They just want to get on with solving their differential equation, or proving a new central limit theorem, etc. They would typically regard these questions as having no bearing whatsoever on real mathematics. So it's our job to find a way of handling such issues that's rigorous, but as frictionless and fuss-free as possible. That's the mission.

There's an old book called *Mathematics Made Difficult*, by Carl E. Linderholm, that makes fun of all this. For example, he writes on page 48:

> is it 48 the natural number, or 48 the integer that is being used to number this page?

We don't want to get hung up on questions like this any more than anyone else. What we want to do is:

- figure out a rigorous way of handling this kind of issue; then
- understand what details are routinely swept under the carpet and why that's harmless; then
- take the same liberties as everyone else.

We will come away with two prizes: first, a rigorous underpinning for how sets are manipulated, and second, a better understanding of what mathematicians are actually doing in their everyday use of sets.

## 1.8 The plan

The rest of this course is in three phases.

First, we formulate the axioms (Chapters 2 and 3). This means writing down in precise terms ten standard principles for manipulating sets. We saw informal versions of these principles in Figure 1.4.

The second phase is catching up. There are hundreds of obvious-sounding statements about sets that we could write down, and only a few of them are axioms. The others have to be *deduced* from the axioms. Some such deductions happen in Chapters 4–7, although these chapters also contain new concepts and results that are not so obvious.

In the third and final phase (Chapters 8–10), we prove theorems that are very likely new to you. For example, we'll show that for any two sets $X$ and $Y$, either there's an injection $X \to Y$ or there's an injection $Y \to X$. We'll also show that $X \times X \cong X$ for any infinite set $X$, and a lot more besides.

## 1.9 What's wrong with ZFC? (Optional)

*This section is non-examinable.*

The traditional axiomatization of sets is called Zermelo–Fraenkel with Choice (ZFC). It was formulated in the early part of the twentieth century, and it has held the unquestioned position as the standard axiomatization of sets ever since. Indeed, it is the only one that most mathematicians have heard of.

But the axiom system we'll use, ETCS, is radically different from ZFC. So why aren't we doing ZFC? What's wrong with it?

In a nutshell, it's that how ZFC handles sets conflicts with how almost all mathematicians handle them.

Before I explain, I need to tell you what ZFC actually looks like. In outline, it says:

- there are some things called sets;
- there is a binary relation $\in$ on sets;
- some axioms hold.

Let's unpack that.

First, in the world of ZFC, the *only* things are sets.

Second, saying that there is a binary relation $\in$ on sets means that for any two sets $X$ and $Y$, the statement '$X \in Y$' is either true or false. It is always assigned one of those two truth values.

Third, that second bullet point also implicitly means that every element of a set is again a set. (Remember, in ZFC, sets are the only things.)

The conflict between ZFC sets and ordinary mathematical sets is not so much in the ZFC *axioms*, but in the very *setup* (Figure 1.5). For example, we just saw that in the ZFC setup, every element of a set is a set. In ordinary mathematics, $\mathbb{R}$ is a set and $\pi$ is an element of $\mathbb{R}$, but $\pi$ is not a set: there is no natural concept of an 'element of $\pi$'. Perhaps you'd say that real numbers have *no* elements. But that doesn't fix it: the first axiom of ZFC is that sets with the same elements are equal, so if all real numbers have no elements, then all real numbers are equal.

This aspect of ZFC, that an element of a set is again a set, is not an accident but an integral part of how it works. For example, another of the axioms (called 'foundation') states that every nonempty set $X$ has an element $x$ such that $x \cap X = \varnothing$. This makes sense in the ZFC setup, because $x$ is an element of a set and is therefore a set itself. But again, let's try it out on an ordinary mathematical set such as $\mathbb{R}$. Is there some real number $x$ such that $x \cap \mathbb{R} = \varnothing$? In other words, is there a real number $x$ such that none of the elements of $x$ are real numbers? Again, from the

| | Ordinary mathematics | ETCS | ZFC |
|---|---|---|---|
| Every element of a set is a set | No | No | Yes |
| For all sets $X$ and $Y$, it is meaningful to ask whether $X \in Y$ | No | No | Yes |

Figure 1.5: The mismatch between ZFC's usage of 'set' and ordinary mathematical usage.

viewpoint of ordinary mathematics, the question doesn't even make sense. Real numbers just don't have elements; they're not sets.

The idea of taking elements of elements of elements ... occurs throughout ZFC-based set theory. For example, one of the basic definitions is that a set $X$ is *transitive* if every element of an element of $X$ is an element of $X$. Once more, let's try it out on $X = \mathbb{R}$. For $\mathbb{R}$ to be transitive would mean that every element of a real number is a real number, and we run into the same problem that the condition doesn't even make sense, because real numbers aren't a type of thing that can *have* elements. Now, we could have taken a more favourable example where $X$ is a set of sets. For instance, take $X$ to be the set of all subsets of $\mathbb{R}$. Then for $X$ to be transitive would mean that every real number was a subset of $\mathbb{R}$. But once more, this isn't just false but nonsensical: there's no possibility of a real number being a subset of $\mathbb{R}$, because it's not even a set.

**Digression 1.9.1** In ZFC-based set theory, ingenious ways have been devised to encode all kinds of mathematical objects as sets, from real numbers to random variables to differential operators. This is like the way in which computers encode files of all kinds (text, graphics, video, ...) as sequences of bits. But in both cases, even the designers would freely admit that the encoding is quite arbitrary.

So far, I've explained the mismatches with ordinary mathematics caused by stipulating that every element of a set is also a set. But there are further problems still. In the ZFC setup, for any sets $X$ and $Y$, there is a meaningful answer to the question 'is $X \in Y$?' For example, one can legitimately ask weird questions like whether the vector space $\mathbb{R}^3$ is a point on the unit sphere, and there is a definite answer of 'yes' or 'no'. But also, since in ZFC every element of a set is a set, there is a definite answer to questions like 'is the integer 2 an element of the cyclic group $C_5$?' And as we have already seen, questions like that make no sense in modern, isomorphism-invariant, mathematics.

As an undergraduate, I took an axiomatic set theory course based on ZFC and very much enjoyed it. (And the last hundred years of research in ZFC-type set

theory have produced some amazing results.) But as the years passed, I came to understand how disconnected it was from the mathematics that I and everyone I knew was doing. Later still, I realized how much the ZFC setup actually *conflicts* with how ordinary mathematicians use sets. The big advantage of ETCS, the set theory developed in this course, over ZFC is that there is no such conflict. ETCS only uses concepts that everyone agrees make sense.

If you want to read a slightly longer critique of ZFC, and a comparison with ETCS, you can try my short paper Rethinking set theory. But this is not a course on ZFC (which is why this section is optional), and I will barely mention ZFC again.

# Chapter 2

# The axioms, part one

*To read by Monday 23 September: Sections 2.1–2.5.*
*To read by Friday 27 September: Sections 2.6 and 2.7.*

Now we get started in earnest. In this chapter and the next, we will formulate precise versions of the axioms stated roughly in Figure 1.4. We'll do the first six in this chapter, and the last four in the next.

As explained in Chapter 1, the idea is to take ten standard principles that mathematicians use every day (perhaps subconsciously), and adopt them as formal axioms.

Each section covers one axiom, and has the following format.

- We will discuss one aspect of how sets and functions are used in day-to-day mathematics.
- Before we can state the axiom, we will usually need to give one or two preliminary definitions.
- We then state the axiom. To distinguish the formal axiomatization from the informal discussion, I will put it in coloured boxes.
- Having stated the axiom, we will assume it from then on. (For instance, after Axioms 1–3 have been stated, we will assume our sets and functions satisfy Axioms 1–3.) Then we will spend some time working out the consequences of our new axiom.

I want to make clear what's going on here logically. There are two sides to what we're doing: the preliminary discussion (first bullet point) and the formal development (the other three bullet points). Logically speaking, the preliminary discussion is not necessary; it's purely to explain and motivate. In it, I will refer

to your experience of using sets, and I'll say things along the lines of 'if we want the sets in our axiomatization to behave like sets as used in most of mathematics, we'd better adopt *this* principle.'

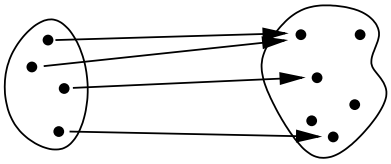
So on the one hand, we have the world of our previous mathematical experience, and on the other hand, we have the world of our axiomatization. The goal is to choose the axioms to make the two worlds match up—so that everything we're accustomed to doing with sets can actually be done on the basis of the axioms alone.

But before we can state any of the axioms, we need to specify the data to which the axioms apply. That's the content of the first section.

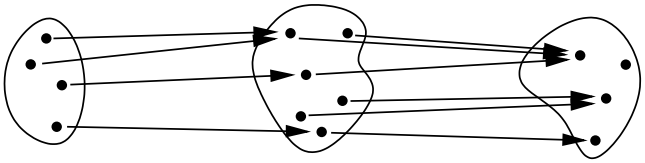
## 2.1 The data

As explained in Chapter 1, we will build our world on the concepts of set, function, composition of functions and identity functions.

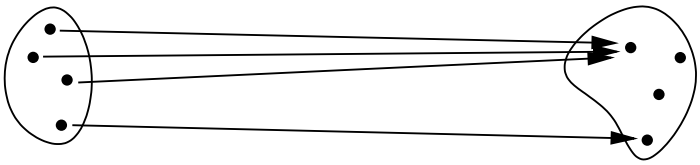
Intuitively, a set is a bag of featureless dots or points (Figure 1.1). A function $X \to Y$ is an assignment of a point in bag $Y$ to each point in bag $X$:



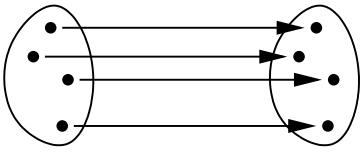
We can do one function after another: given functions



we obtain a composite function



Identity functions look like this:



Formally, the data to which our axioms will apply is as follows.

**Data**

- *Some things called* **sets**;
- *for each set $X$ and set $Y$, some things called* **functions from $X$ to $Y$**, *with functions $f$ from $X$ to $Y$ written as $f : X \to Y$;*
- *for each set $X$, set $Y$ and set $Z$, an operation called* **composition** *assigning to each $f : X \to Y$ and $g : Y \to Z$ a function $g \circ f : X \to Z$;*
- *for each set $X$, a function $\mathrm{id}_X : X \to X$, called an* **identity function**.

You might think the word 'thing' isn't very formal. If you read an introductory book on logic then you'll learn more official-sounding terms, but ultimately they're just substitutes for the word 'thing'. We have to start somewhere.

We often write $f : X \to Y$ as $X \xrightarrow{f} Y$. We often omit the composition sign $\circ$, writing $g \circ f$ as just $gf$, and we often write $\mathrm{id}_X$ as just $\mathrm{id}$.

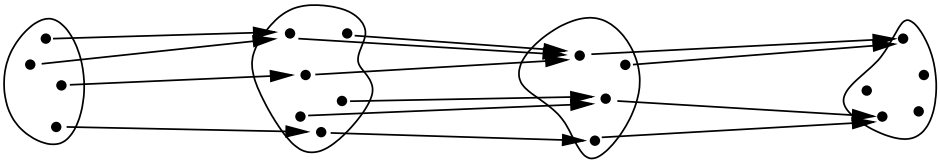
**Warning 2.1.1** I've used the words 'set', 'function', 'composition' and 'identity', but it's important to realize that they're *just words*. I could equally well have used 'splodge', 'floop', etc., and it would have had exactly the same mathematical content. Nothing in the formal statement so far tells us that they behave anything like the sets and functions we're familiar with. The purpose of the axioms that follow is to ensure that they do.

**Remark 2.1.2** We can, if we like, omit the last piece of data—the identity functions—if we change the axioms slightly. A question in Workshop 1 will show you how.

**Warning 2.1.3** A small point of English: *composition* is the operation of composing, and a *composite* is the result. Compare *integration* versus *integral*, or *multiplication* versus *product*. Often people say 'the composition $g \circ f$', but it should really be 'the composite $g \circ f$'.

## 2.2 Associativity and identities

Three functions in a chain like this—



—should have a single unambiguous composite: $(h \circ g) \circ f$ and $h \circ (g \circ f)$ should be equal. Also, composing a function with an identity, either beforehand or afterwards, should not change it. Our first axiom states that these properties hold.

**Axiom 1 (Associativity and identity)** *Composition of functions is* **associative**: *for all sets $W, X, Y, Z$ and functions*

$$W \xrightarrow{f} X \xrightarrow{g} Y \xrightarrow{h} Z,$$

*we have $(h \circ g) \circ f = h \circ (g \circ f)$. It also satisfies* **identity laws**: *for all sets $X$ and $Y$ and functions $f : X \to Y$, we have $f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f$.*

From now on, we will assume that Axiom 1 holds.

**Digression 2.2.1** If you know about categories, you will recognize that Axiom 1 states that sets and functions form a category. The remaining axioms are there to distinguish the category of sets from other categories.

Axiom 1 alone is enough to let us define and discuss isomorphism, which as we saw in the Introduction, is a very important concept.

**Definition 2.2.2** Let $f : X \to Y$ be a function. An **inverse** of $f$ is a function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$.

Both conditions here are necessary: neither implies the other.

**Exercise 2.2.3** Find an example of sets and functions $f : X \to Y$ and $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ but $f \circ g \neq \mathrm{id}_Y$. (In exercises like this, you are allowed to use your general mathematical knowledge; the example doesn't have to be based on the axioms alone.)

From Axiom 1 and Definition 2.2.2, it is conceivable at first glance that a function could have *many* inverses. However:

**Lemma 2.2.4** *A function has at most one inverse.*

**Proof** Let $f\colon X \to Y$ be a function, and let $g, g'\colon Y \to X$ be inverses of $f$. Then

$$g = g \circ \mathrm{id}_Y = g \circ (f \circ g') = (g \circ f) \circ g' = \mathrm{id}_X \circ g' = g',$$

using Axiom 1 three times. Hence $g = g'$. □

Lemma 2.2.4 gives us the right to speak of *the* inverse of a function, if it has one at all. As you would expect, we write it as $f^{-1}$.

**Definition 2.2.5** A function is an **isomorphism** or **invertible** if it has an inverse.

You may never have heard anyone talking about isomorphisms between *sets*. More often, this terminology is used for groups, rings, etc. We will see that they're the same as bijections, but that will be a theorem, not a definition.

**Lemma 2.2.6** *i. For all sets $X$, the identity function $\mathrm{id}_X$ is an isomorphism, and $\mathrm{id}_X^{-1} = \mathrm{id}_X$.*

*ii. For all sets and functions $X \xrightarrow{f} Y \xrightarrow{g} Z$, if $f$ and $g$ are isomorphisms then so is $g \circ f$, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

*iii. For all functions $f\colon X \to Y$, if $f$ is an isomorphism then so is $f^{-1}$, and $(f^{-1})^{-1} = f$.*

**Proof** For (i), let $X$ be a set. Then $\mathrm{id}_X \circ \mathrm{id}_X = \mathrm{id}_X$ by either of the identity laws, so $\mathrm{id}_X$ is an inverse to $\mathrm{id}_X$.

For (ii), take isomorphisms $X \xrightarrow{f} Y \xrightarrow{g} Z$. Then

$$\begin{aligned}(f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ (g \circ f)) \\ &= f^{-1} \circ ((g^{-1} \circ g) \circ f) \\ &= f^{-1} \circ (\mathrm{id}_Y \circ f) \\ &= f^{-1} \circ f \\ &= \mathrm{id}_X,\end{aligned}$$

repeatedly using Axiom 1 and the definition of inverse. A similar argument shows that

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_Z.$$

Hence $f^{-1} \circ g^{-1}$ is an inverse of $g \circ f$.

Part (iii) is similar and left as an exercise. □

**Exercise 2.2.7** Prove Lemma 2.2.6(iii).

The reversal of order in part (ii), $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, is often explained like this: in the morning, you put on your socks and then put on your shoes, but in the evening, you take off your shoes and then take off your socks.

Up to now, I have been very careful to insert all the proper brackets and to say where I'm using Axiom 1. But I'll be looser from now on, writing things like $h \circ g \circ f$ (or just $hgf$) and taking the associativity and identity laws for granted. You are probably already well used to this kind of thing from other courses.

**Definition 2.2.8** Sets $X$ and $Y$ are **isomorphic**, written as $X \cong Y$, if there exists an isomorphism from $X$ to $Y$.

**Lemma 2.2.9** *i.* $X \cong X$ *for all sets* $X$.

*ii.* *If* $X \cong Y \cong Z$ *then* $X \cong Z$, *for all sets* $X$, $Y$ *and* $Z$.

*iii.* *If* $X \cong Y$ *then* $Y \cong X$, *for all sets* $X$ *and* $Y$.

**Proof** These three statements follow from the the corresponding three parts of Lemma 2.2.6. For instance, for (ii), if $X \cong Y \cong Z$ then there exist isomorphisms $X \xrightarrow{f} Y \xrightarrow{g} Z$, and then Lemma 2.2.6(ii) implies that $gf\colon X \to Z$ is an isomorphism. □

**Digression 2.2.10** The word 'isomorphism' and the symbol $\cong$ are deliberately overloaded in mathematics. That is, we intentionally use them with several related but conflicting meanings. Which meaning is intended has to be inferred from the context. For example, is $\mathbb{C} \cong \mathbb{R}^2$? As sets, groups, or metric spaces, yes. As rings, no. So we sometimes have to clarify by saying 'they are isomorphic *as groups*', etc. But since this is a set theory course, the term 'isomorphism' and the symbol $\cong$ will always mean isomorphism *of sets*, unless stated otherwise.

As discussed in Section 1.1, almost every set we meet in mathematical practice has some extra structure. The way language is used is that 'isomorphisms' are intended to preserve that structure. For example, isomorphisms of groups preserve the group structure, by definition. But in the world of set theory, there is no structure to be preserved.

Most other texts do not use the word 'isomorphic' for sets. Instead, they use words like **equinumerous** or **equipotent**, or, most often these days, they say that the sets **have the same cardinality**. And instead of writing $X \cong Y$, they

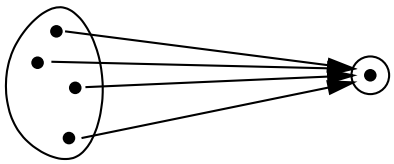


Figure 2.1: The definition of terminal set.

write $|X| = |Y|$, often without giving a meaning to '$|X|$' in isolation. (The term **cardinality** can loosely be understood as meaning 'isomorphism class of sets'.)

For example, later we will construct the sets $\mathbb{N}$ and $\mathbb{Q}$ and prove that there is an isomorphism between them: $\mathbb{N} \cong \mathbb{Q}$. Most texts would express this as '$\mathbb{N}$ and $\mathbb{Q}$ have the same cardinality' or '$|\mathbb{N}| = |\mathbb{Q}|$'.

## 2.3 The one-element set

Our next task is to derive the concept of element from our primitive concepts of set, function and composition. As described in Section 1.3, we use a two-step strategy. First, we find a way to say what it means for a set to have exactly one element, without yet having a notion of element. Then, we define an element of a set $X$ to be a function from the one-element set to $X$.

We begin by describing one-element sets without knowing what 'element' means. The key insight is that when $T$ is a one-element set, and $X$ is any set, there should be exactly one function from $X$ to $T$. ('Should be' refers to what happens in the everyday mathematics that we're all familiar with, which is what we're trying to capture with our axiomatization.) Why? Because a function from $X$ to $T$ should be something that assigns to each element of $X$ an element of $T$, and there's only one possible choice (Figure 2.1).

**Definition 2.3.1** A set $T$ is **terminal** if for all sets $X$, there is a unique function from $X$ to $T$.

The definition of terminal set is the simplest example of a so-called **universal property**. It situates $T$ within the universe of all sets and functions. The term 'universal property' doesn't have a precise definition, but you will see several examples soon.

**Warning 2.3.2** A very common error is to slip up on the meaning of the word 'unique'. I strongly encourage you to read the *Note on logic* (p. 5) if you haven't done so already.

In this case, an alternative phrasing is that $T$ is terminal if for every set $X$, there is exactly one function from $X$ to $T$: a function from $X$ to $T$ exists, and any two functions from $X$ to $T$ are equal.

**Axiom 2 (Terminal set)** *There exists a terminal set.*

From now on, we will assume that Axiom 2 holds.

The concept of terminality is isomorphism-invariant:

**Lemma 2.3.3** *Any set isomorphic to a terminal set is terminal.*

**Proof** Let $T$ be a terminal set, let $T'$ be any set, and suppose there is an isomorphism $j : T \to T'$. We prove that $T'$ is terminal.

Our task is to show that for every set $X$, there exists a unique function from $X$ to $T'$. Let $X$ be a set.

*Existence:* Since $T$ is terminal, there exists a function $f : X \to T$. Then $j \circ f$ is a function $X \to T'$.

*Uniqueness:* Let $f'$ and $g'$ be functions from $X$ to $T'$. Then $j^{-1} \circ f'$ and $j^{-1} \circ g'$ are functions from $X$ to $T$. Since $T$ is terminal, it follows that $j^{-1} \circ f' = j^{-1} \circ g'$. Composing each side with $j$ gives $f' = g'$. □

*Everything we ever do* will be isomorphism-invariant. In fact, it would be near-impossible in our framework to write down a definition that wasn't isomorphism-invariant. This should become increasingly clear as we go along.

We now prove a second lemma about terminality and isomorphism, which is also of absolutely fundamental importance.

**Lemma 2.3.4** *Any two terminal sets are isomorphic.*

Pay close attention to the pattern of the proof, because we'll see proofs like it again and again. This is the simplest version.

**Proof** Let $T$ and $T'$ be terminal sets. We must prove that $T \cong T'$.

Since $T'$ is terminal, there is a unique function $T \to T'$; call it $f$.

Since $T$ is terminal, there is a unique function $T' \to T$; call it $f'$.

We now have functions $T \underset{f'}{\overset{f}{\rightleftarrows}} T'$, and we prove that they are mutually inverse (each is the inverse of the other).

First, both $f' \circ f$ and $\mathrm{id}_T$ are functions $T \to T$. Since $T$ is terminal, the uniqueness part of the definition of terminality implies that $f' \circ f = \mathrm{id}_T$.

Similarly, both $f \circ f'$ and $\mathrm{id}_{T'}$ are functions $T' \to T'$. Since $T'$ is terminal, the uniqueness part of the definition of terminality implies that $f \circ f' = \mathrm{id}_{T'}$.

Hence $f'$ is inverse to $f : T \to T'$. So $f$ is an isomorphism and $T \cong T'$. □

Axiom 2 tells us that there is at least one terminal set, and Lemma 2.3.4 tells us that up to isomorphism, there is only one. So we have the right to speak of *the* terminal set, and to give it a name, **1**. In other words, we fix a terminal set and call it **1**.

**Remark 2.3.5** If you're worried about fixing a particular terminal set, hold on until Section 2.6, where I'll explain why it's harmless.

Given a set $X$, there is exactly one function from $X$ to the terminal set **1**. When we need a name for it, we call it $!_X \colon X \to \mathbf{1}$, or just $! \colon X \to \mathbf{1}$. Or we can simply use an unlabelled arrow $X \to \mathbf{1}$, as there's only one function it could possibly be.

We have now completed the first step of the two-step strategy mentioned at the start of this section. Here is the second.

**Definition 2.3.6** An **element** of a set $X$ is a function $\mathbf{1} \to X$. We write $x \in X$ to mean $x \colon \mathbf{1} \to X$.

We saw in Section 1.3 why this is a reasonable definition. We also saw that whenever we have a function $f \colon X \to Y$ and an element $x \in X$, it's reasonable to write the composite function $f \circ x$ as $f(x)$:

$$f(x) = \left(\mathbf{1} \xrightarrow{x} X \xrightarrow{f} Y\right) \in Y.$$

This is the *definition* of $f(x)$.

**Lemma 2.3.7** *i. For all sets $X$ and elements $x \in X$, we have $\mathrm{id}_X(x) = x$.*

*ii. For all sets and functions $X \xrightarrow{f} Y \xrightarrow{g} Z$ and elements $x \in X$, we have $(g \circ f)(x) = g(f(x))$.*

In our approach, these statements are theorems, not definitions.

**Proof** Part (i) is left as an exercise. For (ii),

$$(g \circ f)(x) = (g \circ f) \circ x = g \circ (f \circ x) = g(f \circ x) = g(f(x)),$$

where the second equality follows from Axiom 1 and all the others are by definition of the '$f(x)$' notation (for various functions $f$ and elements $x$). □

**Exercise 2.3.8** Prove part (i).

## 2.4 A function is determined by its effect on elements

When are two functions equal?

For a start, as explained in Section 1.5, it's only conceivable that they could be equal if their domains and codomains both match, just as it's only conceivable for two matrices to be equal if they have the same numbers of rows and columns.

So, given sets $X$ and $Y$, when are two functions $f, g\colon X \to Y$ equal? In normal mathematical practice, they're equal precisely when

$$f(x) = g(x) \text{ for all } x \in X.$$

Nothing in our axioms so far guarantees that this is the case. So, we adopt it as an axiom.

**Axiom 3 (A function is determined by its effect on elements)** *For all sets $X$ and $Y$ and functions $f, g\colon X \to Y$, if $f(x) = g(x)$ for all $x \in X$ then $f = g$.*

From now on, we will assume that Axiom 3 holds. Using it, we can prove a result that justifies the narrative in Section 2.3:

**Lemma 2.4.1** *A set is terminal if and only if it has exactly one element.*

Since we have no concept yet of one, two, three, ..., I should be clear what I mean by 'has exactly one element'. I mean that there exists an element of the set, and if $x$ and $y$ are elements then $x = y$.

**Proof** First let $T$ be a terminal set. Then by definition of terminality, there is exactly one function $\mathbf{1} \to T$, or in other words, $T$ has exactly one element.

Conversely, let $T$ be a set with exactly one element. Call it $t$. Then we have functions $T \underset{t}{\overset{!_T}{\rightleftarrows}} \mathbf{1}$, which we will show are mutually inverse.

First, $!_T \circ t$ and $\mathrm{id}_{\mathbf{1}}$ are both functions $\mathbf{1} \to \mathbf{1}$, and $\mathbf{1}$ is terminal, so by the uniqueness part of the definition of terminality, $!_T \circ t = \mathrm{id}_{\mathbf{1}}$. To prove that the functions

$$t \circ !_T, \mathrm{id}_T\colon T \to T$$

are also equal, it is enough (by Axiom 3) to show that they take the same values on all elements of $T$. But the only element of $T$ is $t$, so it is enough to show that

$$t \circ !_T \circ t = \mathrm{id}_T \circ t,$$

and this is true since $!_T \circ t = \mathrm{id}_{\mathbf{1}}$. Hence $!_T$ and $t$ are indeed mutually inverse. It follows that $T \cong \mathbf{1}$, so by Lemma 2.3.3, $T$ is terminal. □

## 2.5 The empty set

**Definition 2.5.1** A set is **empty** if it has no elements.

**Axiom 4 (Empty set)** *There exists an empty set.*

From now on, we will assume that Axiom 4 holds.

**Example 2.5.2** The terminal set $\mathbf{1}$ is not empty, since it has an element—in fact, exactly one element, by Lemma 2.4.1.

**Warning 2.5.3** At this point in the axiomatization, nothing guarantees that all empty sets are isomorphic. So we don't yet have the right to speak of 'the' empty set (as in the title of this section) or give 'it' a name (such as $\varnothing$). But our later axioms will in fact imply that all empty sets are isomorphic, as we'll see.

**Digression 2.5.4** The prospect of multiple non-isomorphic empty sets isn't as exotic as it may seem. Suppose we interpret the 'sets' of our axiomatization as what would be ordinarily be called an ordered pair $(X, X')$ of sets, and a 'function' from $(X, X')$ to $(Y, Y')$ as a pair of ordinary functions

$$(f\colon X \to Y, f'\colon X' \to Y').$$

(I leave you to work out what the composition and identities must be. There is only one sensible possibility.) Then there is exactly one 'function' from any 'set' $(X, X')$ to the 'set' $(\mathbf{1}, \mathbf{1})$, which means that $(\mathbf{1}, \mathbf{1})$ is the terminal 'set'. It follows that an element of a 'set' $(X, X')$ consists of an ordinary element of $X$ together with an ordinary element of $X'$. So a 'set' $(X, X')$ is empty if *either* of the sets $X$ and $X'$ is empty in the usual sense. For example, the 'set' $(X, \varnothing)$ is empty for any ordinary set $X$ whatsoever, giving multiple non-isomorphic empty 'sets'.

## 2.6 Products

What is $\mathbb{R}^2$? What does the coordinate notation $(x, y)$ mean? What makes it possible to define a function $h\colon [0, 2\pi] \to \mathbb{R}^2$ by

$$h(\theta) = (\cos\theta, \sin\theta) \tag{2.1}$$

($\theta \in [0, 2\pi]$), assuming that we already have the functions $\cos, \sin\colon [0, 2\pi] \to \mathbb{R}$?

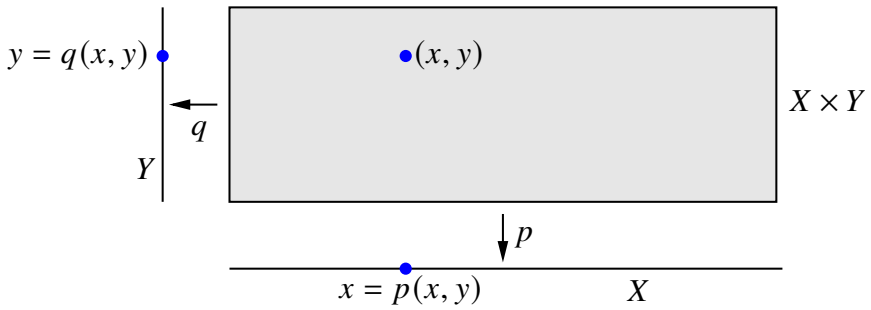



Figure 2.2: The product of two sets $X$ and $Y$, showing the projection functions $p\colon X \times Y \to X$ and $q\colon X \times Y \to Y$ and their effects on an element $(x, y) \in X \times Y$.

These questions are answered by the concept of cartesian product, or product for short, which hopefully you met in Proofs and Problem Solving and which you have certainly met implicitly in coordinate geometry. Any two sets $X$ and $Y$ should have a product $X \times Y$, whose elements are ordered pairs $(x, y)$ with $x \in X$ and $y \in Y$. (Again, I use 'should' to refer to the familiar world of mathematics, which we're aiming to axiomatize.) See Figure 2.2. The notation is chosen because when $X$ and $Y$ are finite sets with $m$ and $n$ elements respectively, $X \times Y$ has $m \times n$ elements.

It doesn't matter what an ordered pair 'is'. All that matters is that they have the property

$$(x, y) = (x', y') \iff x = x' \text{ and } y = y'$$

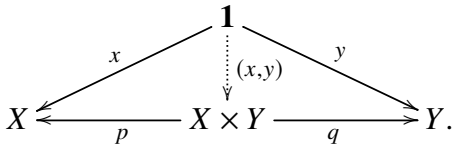
for $x, x' \in X$ and $y, y' \in Y$. In fact, you can recover $x$ and $y$ from $(x, y)$ by applying the functions

$$\begin{array}{ccccc} X & \overset{p}{\leftarrow} & X \times Y & \overset{q}{\rightarrow} & Y \\ x & \mapsto & (x, y) & \mapsto & y. \end{array}$$

The way ordered pairs work can be summarized like this:

> for all $x \in X$ and $y \in Y$, there is a unique element $z \in X \times Y$ such that $p(z) = x$ and $q(z) = y$, and we write this element $z$ as $(x, y)$.

The equation $p(z) = x$ says that the first coordinate of $z$ is $x$, and the equation $q(z) = y$ says that the second is $y$. In a commutative diagram:




(2.2)

(Recall the definition of commutative diagram from p. 15. In this case, for the diagram to commute means $p(x, y) = x$ and $q(x, y) = y$. We sometimes use dotted

arrows in situations where the corresponding function is determined uniquely by other data. Here, $(x, y)$ is determined uniquely by $x$ and $y$.)

**Example 2.6.1** Taking $X = Y = \mathbb{R}$, there is a unique element $z$ of $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ with first coordinate 8 and second coordinate 5, namely, $z = (8, 5)$.

What about that function $h\colon [0, 2\pi] \to \mathbb{R}^2$ from equation (2.1)? Why should such a function exist?

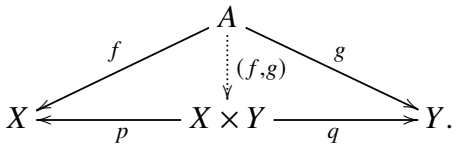
The principle we're implicitly using is this:

> for all sets $A$ and functions $f\colon A \to X$ and $g\colon A \to Y$, there is a unique function $h\colon A \to X \times Y$ with first coordinate $f$ and second coordinate $g$.

(In our example, $A = [0, 2\pi]$, $X = Y = \mathbb{R}$, $f = \cos$ and $g = \sin$.) More formally, the principle is:

> for all sets $A$ and functions $f\colon A \to X$ and $g\colon A \to Y$, there is a unique function $h\colon A \to X \times Y$ such that $p \circ h = f$ and $q \circ h = g$.

This function $h$ could reasonably be written as $(f, g)$, since the equations $p \circ h = f$ and $q \circ h = g$ say that $h(a) = (f(a), g(a))$ for all $a \in A$. In a commutative diagram:




The commutative diagram (2.2) that we drew before when we were thinking about *elements* of products is the special case $A = \mathbf{1}$.

So far in this section, we've examined how products behave in the familiar mathematical world. Let's now build that into our axiomatization.

**Definition 2.6.2** Let $X$ and $Y$ be sets. A **product** of $X$ and $Y$ consists of sets and functions

$$X \xleftarrow{p} P \xrightarrow{q} Y$$

with the following property:

> for all sets $A$ and functions $f\colon A \to X$ and $g\colon A \to Y$, there is a unique function $h\colon A \to P$ such that $p \circ h = f$ and $q \circ h = g$.

This is another example of a universal property. It situates products of $X$ and $Y$ in the universe of all diagrams $X \xleftarrow{?} ? \xrightarrow{?} Y$.

**Warning 2.6.3** Understanding the definition of product requires being crystal clear on how the word 'unique' is used in mathematics (a very common source of trouble). This is explained in the *Note on logic* (p. 5). The take-home message: wherever you see the words 'a unique', you can mentally replace them by 'exactly one'.

**Exercise 2.6.4** Let $X$ and $Y$ be sets and $X \xleftarrow{p} P \xrightarrow{q} Y$ a product of $X$ and $Y$. Prove that if $X$ is empty then so is $P$.

**Axiom 5 (Products)** *Let $X$ and $Y$ be sets. Then $X$ and $Y$ have a product.*

From now on, we will assume that Axiom 5 holds.

**Remark 2.6.5** Strictly speaking, a product of $X$ and $Y$ consists of not only the set $P$ but also the functions $p$ and $q$. But more casually, it's common to refer to $P$ alone as the product of $X$ and $Y$, and to call

$$X \xleftarrow{p} P \xrightarrow{q} Y$$

a **product diagram**. The functions $p$ and $q$ are called the **projections**. For example, if $X$ and $Y$ are both $\mathbb{R}$ (which we haven't constructed in our axiom system yet), then $p$ and $q$ are what are ordinarily called the orthogonal projections of $\mathbb{R}^2$ onto the $x$-axis and the $y$-axis, as Figure 2.2 suggests.

We now prove a pair of lemmas about products and isomorphisms, analogous to Lemmas 2.3.3 and 2.3.4 for terminal sets. First, the concept of product is isomorphism-invariant:

**Lemma 2.6.6** *Let*

$$X \xleftarrow{p} P \xrightarrow{q} Y \quad \text{and} \quad X \xleftarrow{p'} P' \xrightarrow{q'} Y \tag{2.3}$$

*be sets and functions, and suppose there exists an isomorphism $j : P \to P'$ such that the diagram*

$$\begin{array}{ccccc} & & P & & \\ & \overset{p}{\swarrow} & \cong\downarrow j & \overset{q}{\searrow} & \\ X & & & & Y \\ & \underset{p'}{\nwarrow} & & \underset{q'}{\nearrow} & \\ & & P' & & \end{array}$$

*commutes. If one of the diagrams (2.3) is a product then so is the other.*

**Proof** Suppose $X \xleftarrow{p} P \xrightarrow{q} Y$ is a product diagram. To show that $X \xleftarrow{p'} P' \xrightarrow{q'} Y$ is also a product diagram, take sets and functions

$$X \xleftarrow{f} A \xrightarrow{g} Y.$$

We must prove that there exists a unique function $h' \colon A \to P'$ such that $p'h' = f$ and $q'h' = g$.

*Existence:* Since $X \xleftarrow{p} P \xrightarrow{q} Y$ is a product diagram, there is a unique function $h \colon A \to P$ such that $ph = f$ and $qh = g$. If we define $h' = jh \colon A \to P'$ then

$$p'h' = p'jh = ph = f,$$

and similarly $q'h' = g$, as required.

*Uniqueness:* Now take two functions $h'_1, h'_2 \colon A \to P'$ such that $p'h'_i = f$ and $q'h'_i = g$ for $i = 1, 2$. Define

$$h_i = j^{-1}h'_i \colon A \to P$$

($i = 1, 2$). Then for both $i = 1$ and $i = 2$,

$$ph_i = pj^{-1}h'_i = p'h'_i = f,$$

and similarly $qh_i = g$. Since $X \xleftarrow{f} P \xrightarrow{g} Y$ is a product diagram, the uniqueness part of the definition of product implies that $h_1 = h_2$. But $h'_1 = jh_1$ and $h'_2 = jh_2$, so $h'_1 = h'_2$, as required. □

Although that proof may look somewhat complicated, the result is really a foregone conclusion. As remarked after Lemma 2.3.3, everything in our axiomatic world is destined to be isomorphism-invariant.

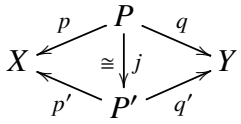
**Exercise 2.6.7** As a kind of companion to Lemma 2.6.6, show that whenever we have a product diagram $X \xleftarrow{p} P \xrightarrow{q} Y$ and isomorphisms $X \xrightarrow{j} X'$ and $Y \xrightarrow{k} Y'$, then $X' \xleftarrow{jp} P \xrightarrow{kq} Y'$ is also a product diagram.

We now show that products are essentially unique.

**Lemma 2.6.8** *Let $X$ and $Y$ be sets, and let*

$$X \xleftarrow{p} P \xrightarrow{q} Y \quad \text{and} \quad X \xleftarrow{p'} P' \xrightarrow{q'} Y$$

*be product diagrams. Then there is a unique isomorphism $j \colon P \to P'$ such that the diagram*

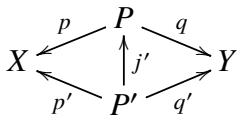



*commutes. In particular, $P \cong P'$.*

This is an analogue of Lemma 2.3.4, and the proof is analogous too.

**Proof** Since $X \xleftarrow{p'} P' \xrightarrow{q'} Y$ is a product diagram, there is a unique function $j\colon P \to P'$ such that the diagram above commutes. We have to show that $j$ is an isomorphism.

Since $X \xleftarrow{p} P \xrightarrow{q} Y$ is a product diagram, there is also a unique function $j'\colon P' \to P$ such that the diagram




commutes.

We now have functions $P \underset{j'}{\overset{j}{\rightleftarrows}} P'$, and we prove that they are mutually inverse.

First, the function $j'j\colon P \to P$ satisfies

$$p(j'j) = (pj')j = p'j = p,$$

and similarly $q(j'j) = q$. So

$$p \circ (j'j) = p, \quad q \circ (j'j) = q.$$

But also, the identity function $\mathrm{id}_P\colon P \to P$ satisfies

$$p \circ \mathrm{id}_P = p, \quad q \circ \mathrm{id}_P = q.$$

Since $X \xleftarrow{p} P \xrightarrow{q} Y$ is a product diagram, the uniqueness part of the definition of product implies that $j'j = \mathrm{id}_P$.

A similar argument using the product property of $X \xleftarrow{p'} P' \xrightarrow{q'} Y$ proves that $jj' = \mathrm{id}_{P'}$.

Hence $j'$ is inverse to $j$, so $j$ is an isomorphism, as required. □

Since products are unique up to isomorphism, we have the right to talk about *the* product of $X$ and $Y$ and to give it a name. We write it like this:

$$X \xleftarrow{\mathrm{pr}_1^{X,Y}} X \times Y \xrightarrow{\mathrm{pr}_2^{X,Y}} Y.$$

Often we abbreviate the projections $\mathrm{pr}_1^{X,Y}$ and $\mathrm{pr}_2^{X,Y}$ as just $\mathrm{pr}_1$ and $\mathrm{pr}_2$.

**Digression 2.6.9** We have chosen once and for all a particular terminal set **1** and a particular product for each pair of sets. Is this reasonable?

In fact, this kind of thing is extremely common in everyday mathematics. In group theory, we speak of *the* trivial group and give it a name like 1 or $\{e\}$, even though there are conceivably many trivial groups, all isomorphic. In linear algebra, we speak of *the* direct sum of two vector spaces and use the notation $V \oplus W$, even though again, it's only really defined up to isomorphism.

If you prefer not to fix a particular terminal set and particular products, you can do it by adopting some circumlocutions. For example, instead of saying 'for all elements $x \in X$' (which implicitly refers to the chosen terminal set **1**), you can say 'for all terminal sets $T$ and functions $x\colon T \to X$'.

An alternative strategy is to extend the list of primitive concepts. To the existing list (sets, functions, composition and identities), we add:

- a distinguished set, **1**;
- an operation assigning to each pair of sets $X, Y$ a set $X \times Y$ and functions $X \xleftarrow{\mathrm{pr}_1^{X,Y}} X \times Y \xrightarrow{\mathrm{pr}_2^{X,Y}} Y$.

Axiom 2 is then replaced by the statement that **1** is terminal, and Axiom 5 by the statement that the data in the second bullet point is a product diagram.

Ultimately, the difference between these various approaches is cosmetic. The one we have chosen seems closest to normal mathematical practice.

Given sets and functions

$$X \xleftarrow{f} A \xrightarrow{g} Y,$$

we write

$$(f, g)\colon A \to X \times Y$$

for the unique function $A \to X \times Y$ satisfying

$$\mathrm{pr}_1 \circ (f, g) = f, \quad \mathrm{pr}_2 \circ (f, g) = g.$$

Note that every function $h\colon A \to X \times Y$ is equal to $(f, g)$ for some $f$ and $g$, namely, $f = \mathrm{pr}_1 \circ h$ and $g = \mathrm{pr}_2 \circ h$.

In the case $A = \mathbf{1}$, this means that given elements $x \in X$ and $y \in Y$, we write $(x, y)$ for the unique element of $X \times Y$ satisfying $\mathrm{pr}_1(x, y) = x$ and $\mathrm{pr}_2(x, y) = y$ (as you would expect). And every element $z$ of $X \times Y$ is equal to $(x, y)$ for some $x \in X$ and $y \in Y$, namely, $x = \mathrm{pr}_1(z)$ and $y = \mathrm{pr}_2(z)$.

**Lemma 2.6.10** *Take sets and functions $X \xleftarrow{f} A \xrightarrow{g} Y$. Then*

$$(f, g)(a) = (f(a), g(a)) \tag{2.4}$$

*for all $a \in A$.*

**Proof** Let $a \in A$. First, both sides of (2.4) are elements of $X \times Y$, so the equation makes sense. Now $\mathrm{pr}_1 \circ (f, g) = f$, so $\mathrm{pr}_1((f, g)(a)) = f(a)$, and similarly $\mathrm{pr}_2((f, g)(a)) = g(a)$. Since $(f(a), g(a))$ is the *unique* element $z$ of $X \times Y$ such that $\mathrm{pr}_1(z) = f(a)$ and $\mathrm{pr}_2(z) = g(a)$, the result follows. □

**Examples 2.6.11**

i. For every set $X$, the functions $X \xleftarrow{\mathrm{id}_X} X \xrightarrow{\mathrm{id}_X} X$ give rise to a function $\Delta_X = (\mathrm{id}_X, \mathrm{id}_X) \colon X \to X \times X$. By Lemma 2.6.10, $\Delta_X(x) = (x, x)$ for all $x \in X$. We call $\Delta_X$ the **diagonal function** of $X$.

ii. Consider the functions $\cos, \sin \colon [0, 2\pi] \to \mathbb{R}$. (We have not constructed any of these sets or functions from our axioms yet.) Then $(\cos, \sin)$ is the unique function $[0, 2\pi] \to \mathbb{R} \times \mathbb{R}$ such that

$$(\cos, \sin)(a) = (\cos(a), \sin(a))$$

for all $a \in [0, 2\pi]$.

iii. Suppose that we have also constructed the addition function $+ \colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, and adopted the usual convention that $+(x, y)$ is written as $x + y$. Then we can make definitions like 'define $\varphi \colon [0, 2\pi] \to \mathbb{R}$ by $\varphi(a) = \cos a + \sin a$', which means that $\varphi$ is defined to be the composite function

$$[0, 2\pi] \xrightarrow{(\cos,\sin)} \mathbb{R} \times \mathbb{R} \xrightarrow{+} \mathbb{R}.$$

**Exercise 2.6.12** Let $f, f' \colon A \to X$ and $g, g' \colon A \to Y$. Prove that $(f, g) = (f', g')$ if and only if $f = f'$ and $g = g'$.

Given functions $X \xrightarrow{f} X'$ and $Y \xrightarrow{g} Y'$, we would like to be able to define a function $X \times Y \to X' \times Y'$ by $(x, y) \mapsto (f(x), g(y))$. The next lemma says that our axioms are powerful enough to make this possible.

**Lemma 2.6.13** *Let $X \xrightarrow{f} X'$ and $Y \xrightarrow{g} Y'$ be functions. Then there is a unique function $f \times g \colon X \times Y \to X' \times Y'$ such that*

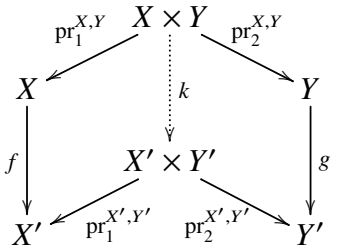
$$(f \times g)(x, y) = (f(x), g(y))$$

*for all $x \in X$ and $y \in Y$.*

In other words, there is a unique function $k \colon X \times Y \to X' \times Y'$ with this property, and we are defining $f \times g$ to be this $k$.

**Proof** *Uniqueness:* Since every element of $X \times Y$ is equal to $(x, y)$ for some $x \in X$ and $y \in Y$, uniqueness follows from Axiom 3.

*Existence:* By the product property of $X' \times Y'$, there is a function $k$ such that the diagram




commutes. For each $(x, y) \in X \times Y$, we therefore have

$$\mathrm{pr}_1(k(x, y)) = f(\mathrm{pr}_1(x, y)) = f(x),$$

and similarly $\mathrm{pr}_2(k(x, y)) = g(y)$. Hence $k(x, y) = (f(x), g(y))$. □

**Warning 2.6.14** Don't mix up $(f, g)$ and $f \times g$. Here are the differences:

- Given $A \xrightarrow{f} X$ and $A \xrightarrow{g} Y$, we get $A \xrightarrow{(f,g)} X \times Y$. So $(f, g)$ is only defined when $f$ and $g$ have the same domain. It satisfies $(f, g)(a) = (f(a), g(a))$ for all $a \in A$. The notation generalizes the familiar $(x, y)$ coordinate notation, which is the case $A = \mathbf{1}$.
- Given $X \xrightarrow{f} X'$ and $Y \xrightarrow{g} Y'$, we get $X \times Y \xrightarrow{f \times g} X' \times Y'$. So $f \times g$ is defined even if $f$ and $g$ have different domains. It satisfies $(f \times g)(x, y) = (f(x), g(y))$ for all $x \in X$ and $y \in Y$.

As we'll gradually discover, there is an algebra of sets somewhat like the familiar algebra of numbers. The final result of this section gives a taste of it.

**Proposition 2.6.15** *i.* $X \times Y \cong Y \times X$ *for all sets* $X$ *and* $Y$.

*ii.* $X \times \mathbf{1} \cong X$ *for all sets* $X$.

*iii.* $(X \times Y) \times Z \cong X \times (Y \times Z)$ *for all sets* $X, Y, Z$.

**Proof** Part (i) is left as an exercise. For (ii), let $X$ be a set. We will prove that the functions

$$X \times \mathbf{1} \underset{(\mathrm{id}_X, !_X)}{\overset{\mathrm{pr}_1}{\rightleftarrows}} X$$

are mutually inverse. First, $\mathrm{pr}_1 \circ (\mathrm{id}_X, !_X) = \mathrm{id}_X$, by definition of the bracket notation. Second, write $\star$ for the unique element of $\mathbf{1}$; then for all $x \in X$,

$$(\mathrm{id}_X, !_X)\mathrm{pr}_1(x, \star) = (\mathrm{id}_X, !_X)(x) = (\mathrm{id}_X(x), !_X(x)) = (x, \star),$$

using Lemma 2.6.10 in the middle equality. Hence $(\mathrm{id}_X, !_X) \circ \mathrm{pr}_1 = \mathrm{id}_{X \times \mathbf{1}}$, as required.

Now we prove (iii). Let $X$, $Y$ and $Z$ be sets. Define functions

$$p = \left((X \times Y) \times Z \xrightarrow{\mathrm{pr}_1^{X\times Y, Z}} X \times Y \xrightarrow{\mathrm{pr}_1^{X,Y}} X\right)$$

and

$$q = \left((X \times Y) \times Z \xrightarrow{\mathrm{pr}_2^{X,Y} \times \mathrm{id}_Z} Y \times Z\right).$$

Then define

$$f = (p, q) \colon (X \times Y) \times Z \to X \times (Y \times Z).$$

For all $x \in X$, $y \in Y$ and $z \in Z$, we have

$$p((x, y), z) = x, \quad \text{and} \quad q((x, y), z) = (y, z),$$

and so $f((x, y), z) = (x, (y, z))$. Similarly, there is a function

$$f' \colon X \times (Y \times Z) \to (X \times Y) \times Z$$

such that $f'(x, (y, z)) = ((x, y), z)$ for all $x, y, z$. It follows that $f$ and $f'$ are mutually inverse, and so $(X \times Y) \times Z \cong X \times (Y \times Z)$. □

**Exercise 2.6.16** Prove part (i) of Proposition 2.6.15. (Take your inspiration from the proofs of parts (ii) and (iii).)

**Remark 2.6.17** The unique element of $\mathbf{1}$ is the unique function $\mathbf{1} \to \mathbf{1}$, which is $\mathrm{id}_{\mathbf{1}}$. However, it's traditional to write it as $\star$, as I did in the proof above.

## 2.7 Sets of functions

In everyday mathematics, we can form the set of functions from one set $X$ to another set $Y$, often denoted by $Y^X$. We will need to add an axiom to guarantee that such sets exist.

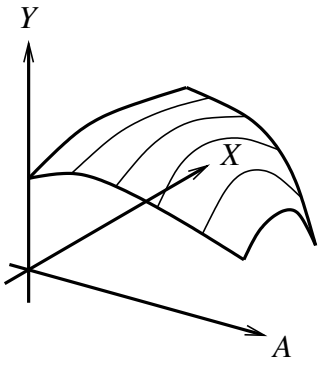



Figure 2.3: A function $A \times X \to Y$ can be seen as a way of assigning to each element of $A$ a function $X \to Y$.

**Exercise 2.7.1** Convince yourself that if $X$ and $Y$ are finite sets with $m$ and $n$ elements respectively, then $Y^X$ has $n^m$ elements.

Here is the key observation. For any set $A$, the functions $q\colon A \times X \to Y$ should correspond one-to-one with the functions $\bar{q}\colon A \to Y^X$, simply by changing the punctuation:

$$q(a,x) = (\bar{q}(a))(x) \tag{2.5}$$

$(a \in A, x \in X)$.

**Examples 2.7.2** i. Figure 2.3 shows an example with $A = X = Y = \mathbb{R}$. A function from $A \times X = \mathbb{R}^2$ to $Y = \mathbb{R}$ is drawn as a surface. A function from $A = \mathbb{R}$ to $Y^X = \{\text{functions } \mathbb{R} \to \mathbb{R}\}$ is a way of assigning to each $a \in \mathbb{R}$ a function $\bar{q}(a)\colon \mathbb{R} \to \mathbb{R}$, and each of these functions $\mathbb{R} \to \mathbb{R}$ is drawn as a curve. These curves together make up the surface. (If we were talking about *continuous* curves and surfaces then there would be further analytic questions, but these are completely arbitrary functions we're considering.)

ii. Take $A = \mathbb{N}$. Then a function $A \to Y^X$ is a sequence $(q_n)$ of functions from $X$ to $Y$. If we write the element $q_n(x)$ of $Y$ as $q(n,x)$, then $q$ is a function $\mathbb{N} \times X \to Y$, and it should be clear that the function $q$ contains exactly the same information as the sequence of functions $(q_n)$. In the notation above, $q_n$ would be written as $\bar{q}(n)$.

In the case $A = \mathbf{1}$, what is the correspondence between functions $A \times X \to Y$ and $A \to Y^X$? By Proposition 2.6.15, $\mathbf{1} \times X \cong X$, so it's a one-to-one correspondence between functions $X \to Y$ and elements of $Y^X$. In other words, elements of $Y^X$ are the same thing as functions $X \to Y$. That's exactly what we want.

On the right-hand side of (2.5), $\bar{q}(a)$ is an element of $Y^X$ and $x$ is an element of $X$; then $(\bar{q}(a))(x)$ denotes the function $\bar{q}(a)$ evaluated at $x$. So, we are implicitly using the evaluation function

$$\begin{array}{rccc} e\colon & Y^X \times X & \to & Y \\ & (f,x) & \mapsto & f(x). \end{array}$$

Then (2.5) becomes the equation

$$q(a,x) = e(\bar{q}(a),x),$$

as in the following definition.

**Definition 2.7.3** Let $X$ and $Y$ be sets. A **function set** from $X$ to $Y$ is a set $F$ together with a function $e\colon F \times X \to Y$, with the following property:

> for all sets $A$ and functions $q\colon A \times X \to Y$, there is a unique function $\bar{q}\colon A \to F$ such that $q(a,x) = e(\bar{q}(a),x)$ for all $a \in A$ and $x \in X$.

The condition that $q(a,x) = e(\bar{q}(a),x)$ for all $a$ and $x$ can be expressed as a commutative diagram:

$$\begin{array}{ccc} A \times X & & \\ {\scriptstyle \bar{q}\times \mathrm{id}_X}\downarrow & \searrow^{q} & \\ F \times X & \xrightarrow[e]{} & Y. \end{array}$$

**Axiom 6 (Function sets)** *Let $X$ and $Y$ be sets. Then there exists a function set from $X$ to $Y$.*

From now on, we will assume that Axiom 6 holds.

**Remark 2.7.4** As in Remark 2.6.5 for products, a function set is strictly speaking a set $F$ *together with* a function $e$ with the required properties, but we often casually use 'function set' to mean just the set $F$. The function $e$ is called **evaluation**.

Definition 2.7.3 is another universal property, and I hope by now you won't be surprised that we're about to state a pair of lemmas: functions sets are isomorphism-invariant and unique up to isomorphism.

**Lemma 2.7.5** *Let $X$ and $Y$ be sets. Take sets $F$ and $F'$ and functions*

$$F \times X \xrightarrow{e} Y, \quad F' \times X \xrightarrow{e'} Y,$$

*and suppose there exists an isomorphism $j\colon F \to F'$ such that the diagram*

$$\begin{array}{ccc} F \times X & & \\ {\scriptstyle j\times \mathrm{id}_X}\downarrow{\scriptstyle \cong} & \searrow^{e} & \\ F' \times X & \nearrow_{e'} & Y \end{array}$$

*commutes. Then $F$ together with $e$ is a function set from $X$ to $Y$ if and only if $F'$ together with $e'$ is.*

**Proof** This is similar to the proofs of Lemmas 2.3.3 for terminal sets and 2.6.6 for products, and is set as a question on Workshop 2. □

I hope it will soon become intuitively obvious to you that everything we do—every property, every theorem and every construction—is isomorphism-invariant, that it would be inconceivable for anything not to be.

**Lemma 2.7.6** *Let $X$ and $Y$ be sets. Let $F$ together with $e\colon F \times X \to Y$ be a function set from $X$ to $Y$, and let $F'$ together with $e'\colon F' \times X \to Y$ be another function set from $X$ to $Y$. Then there is a unique isomorphism $j\colon F \to F'$ such that the diagram*

$$\begin{array}{ccc} F \times X & & \\ {\scriptstyle j\times \mathrm{id}_X}\downarrow{\scriptstyle \cong} & \searrow^{e} & \\ F' \times X & \nearrow_{e'} & Y \end{array}$$

*commutes. In particular, $F \cong F'$.*

**Proof** Again, this is analogous to the proofs of Lemmas 2.3.4 for terminal sets and 2.6.8 for products, and is set as a question on Workshop 2. □

Let $X$ and $Y$ be sets. Lemma 2.7.6 gives us the right to speak of *the* function set from $X$ to $Y$ (do you see a pattern here?), and to give it a name. We write $Y^X$ for the function set from $X$ to $Y$, and

$$\mathrm{ev}_{X,Y}\colon Y^X \times X \to Y$$

(or sometimes just ev) for the evaluation function.

Given a function $q\colon A \times X \to Y$, we write $\bar{q}$ for the corresponding function $A \to Y^X$, as in Definition 2.7.3.

**Remark 2.7.7** In the case $A = \mathbf{1}$, we have $\mathbf{1} \times X \cong X$ (by Proposition 2.6.15), so functions $X \to Y$ correspond one-to-one with functions $\mathbf{1} \times X \to Y$, which in turn correspond one-to-one with functions $\mathbf{1} \to Y^X$, that is, to elements of $Y^X$. So, functions $X \to Y$ correspond to elements of $Y^X$. For a function $f\colon X \to Y$, we write $\bar{f}$ for the corresponding element of $Y^X$.

We are taking a slight liberty here, since according to the general '$\bar{q}$' notation introduced above, we should really write $\bar{f}$ as $\overline{f \circ \mathrm{pr}_2}$, where $\mathrm{pr}_2 \colon \mathbf{1} \times X \to X$ is the isomorphism from Proposition 2.6.15. But we reduce notation by taking this isomorphism for granted.

Sometimes we even write $\bar{f}$ as just $f$, relying on the context to make it clear. Then $f$ denotes both the function $X \to Y$ and the corresponding element of $Y^X$. Using this notation,

$$\mathrm{ev}(f, x) = f(x)$$

for all $x \in X$.

The elements of $Y^X$ correspond to the functions $X \to Y$, but sometimes it is helpful to think of them a bit differently.

**Definition 2.7.8** Let $X$ and $Y$ be sets. An **$X$-indexed family of elements of $Y$** is a function from $X$ to $Y$.

This is nothing more than language, but sometimes the shift in perspective is natural. There are occasions when we think of a function from $X$ to $Y$ as a family $(y_x)_{x \in X}$, with one element $y_x$ of $Y$ for each element $x$ of $X$. The corresponding function $f \colon X \to Y$ is given by $f(x) = y_x$.

**Example 2.7.9** Let $X$ be $\mathbb{N}$ (which we have not yet constructed from our axioms). Then $Y^X = Y^{\mathbb{N}}$ can be thought of as the set of sequences $(y_n)_{n \in \mathbb{N}}$ of elements of $Y$, as discussed in Section 1.3.

We will return to families in Chapter 6. Now, we establish some fundamental properties of function sets.

**Lemma 2.7.10** *i. Let $X$ be a set and $v \colon Y \to Y'$ a function. Then there is a unique function $v^X \colon Y^X \to Y'^X$ such that $v^X(f) = v \circ f$ for all $f \in Y^X$.*

*ii. Let $Y$ be a set and $u \colon X \to X'$ a function. Then there is a unique function $Y^u \colon Y^{X'} \to Y^X$ such that $Y^u(f') = f' \circ u$ for all $f' \in Y^{X'}$.*

In the statement of this lemma, we are taking the notational liberty described in the last paragraph of Remark 2.7.7.

**Warning 2.7.11** Note the reversal of direction in Lemma 2.7.10(ii)! A function $u \colon X \to X'$ induces a function $Y^{X'} \to Y^X$, not the other way round. That's just a fact of life: there is simply no way to compose $u$ with a function $X \to Y$ to get a function $X' \to Y$.

**Proof of Lemma 2.7.10** For (i), uniqueness is immediate from Axiom 3. For existence, let $q$ be the composite

$$Y^X \times X \xrightarrow{\mathrm{ev}_{X,Y}} Y \xrightarrow{v} Y'.$$

Then $q(f,x) = v(f(x))$ for all $f \in Y^X$ and $x \in X$. Using the definition of function set, we obtain a function $\bar{q}\colon Y^X \to Y'^X$ such that $(\bar{q}(f))(x) = (v \circ f)(x)$ for all $f \in Y^X$ and $x \in X$, or equivalently, $\bar{q}(f) = v \circ f$ for all $f \in Y^X$. Hence $\bar{q}$ has the property required of $v^X$.

The proof of (ii) is similar, so I will just sketch it. For the existence part, we take $q$ to be the composite

$$Y^{X'} \times X \xrightarrow{\mathrm{id}\times u} Y^{X'} \times X' \xrightarrow{\mathrm{ev}_{X',Y}} Y,$$

then prove that $\bar{q}\colon Y^{X'} \to Y^X$ has the property required of $Y^u$. □

We finish with another taste of the algebra of sets, reminiscent of familiar algebraic laws.

**Proposition 2.7.12** *i.* $(Y \times Z)^X \cong Y^X \times Z^X$ *for all sets* $X, Y, Z$, *and* $\mathbf{1}^X \cong \mathbf{1}$ *for all sets* $X$.

*ii.* $Z^{X\times Y} \cong (Z^Y)^X$ *for all sets* $X, Y, Z$, *and* $Y^{\mathbf{1}} \cong Y$ *for all sets* $Y$.

Let me say a little about the proof before we launch in. Consider the first isomorphism, $(Y \times Z)^X \cong Y^X \times Z^X$. Intuitively, it's true because every function $X \to Y \times Z$ is uniquely of the form $(f,g)$ where $f\colon X \to Y$ and $g\colon X \to Z$. Hence the functions $X \to Y \times Z$ are in one-to-one correspondence with pairs of functions $(f\colon X \to Y, g\colon X \to Z)$. But what makes the proof more challenging is that we have to construct this one-to-one correspondence *from the axioms*. Remember, the axioms are all we're allowed to use.

**Proof** For the first part of (i), take sets $X, Y, Z$. The function $\mathrm{pr}_1^{Y,Z}\colon Y \times Z \to Y$ induces a function

$$\begin{array}{rccc} \left(\mathrm{pr}_1^{Y,Z}\right)^X\colon & (Y\times Z)^X & \to & Y^X \\ & h & \mapsto & \mathrm{pr}_1 \circ h, \end{array}$$

as in Lemma 2.7.10(i). The same goes for the second projection. Putting the two together gives a function

$$\begin{array}{rccc} j = \left(\left(\mathrm{pr}_1^{Y,Z}\right)^X, \left(\mathrm{pr}_2^{Y,Z}\right)^X\right)\colon & (Y\times Z)^X & \to & Y^X \times Z^X \\ & h & \mapsto & (\mathrm{pr}_1 \circ h, \mathrm{pr}_2 \circ h). \end{array} \tag{2.6}$$

Now we construct an inverse to $j$. First let $q$ be the composite function

$$Y^X \times Z^X \times X \xrightarrow{\mathrm{id}\times\mathrm{id}\times\Delta_X} Y^X \times Z^X \times X \times X \xrightarrow{\mathrm{id}\times\sigma\times\mathrm{id}} Y^X \times X \times Z^X \times X \xrightarrow{\mathrm{ev}_{X,Y}\times\mathrm{ev}_{X,Z}} Y \times Z,$$

where $\Delta_X$ is the diagonal function defined in Example 2.6.11(i), $\sigma$ is the isomorphism $Z^X \times X \to X \times Z^X$ from Proposition 2.6.15(i), and I have used the associativity of products (Proposition 2.6.15(iii)) as an excuse to omit brackets. The effect of this composite on elements is

$$(f, g, x) \mapsto (f, g, x, x) \mapsto (f, x, g, x) \mapsto (f(x), g(x))$$

($f \in Y^X$, $g \in Z^X$, $x \in X$). So, $q(f, g, x) = (f(x), g(x))$. Now $q$ induces a function

$$\bar{q} \colon Y^X \times Z^X \to (Y \times Z)^X$$

(by the universal property of the function set $(Y \times Z)^X$), which therefore satisfies

$$(\bar{q}(f, g))(x) = (f(x), g(x)) \tag{2.7}$$

($f \in Y^X$, $g \in Z^X$, $x \in X$). We will show that $\bar{q}$ is inverse to $j$.

In one direction, let $h \in (Y \times Z)^X$. For each $x \in X$,

$$\big(\bar{q}(j(h))\big)(x) = \big(\bar{q}(\mathrm{pr}_1 \circ h, \mathrm{pr}_2 \circ h)\big)(x) = (\mathrm{pr}_1 h(x), \mathrm{pr}_2 h(x)) = h(x),$$

using equations (2.6) and (2.7). So $\bar{q}(j(h)) = h$. In the other direction, let $(f, g) \in Y^X \times Z^X$. Write $j(\bar{q}(f, g)) \in Y^X \times Z^X$ as $(f', g')$ .Then $f' = \mathrm{pr}_1 \circ \bar{q}(f, g)$ by equation (2.6), which by equation (2.7) implies that $f' = f$. Similarly, $g' = g$. Hence $j(\bar{q}(f, g)) = (f, g)$. This completes the proof that $j$ and $\bar{q}$ are mutually inverse, and it follows that $(Y \times Z)^X \cong Y^X \times Z^X$.

The remaining parts of the proposition appear as a guided exercise in Workshop 2. □

# Chapter 3

# The axioms, part two

*To read by Monday 30 September: Sections 3.1 and 3.2.*
*To read by Friday 4 October: Sections 3.3–3.5.*

I hope you're getting the idea. We've stated some axioms (six so far), which assert the existence of certain sets and functions and impose rules on how they behave. By using the axioms repeatedly, we can construct more sets and functions and prove more results about their behaviour.

For example, at the end of the last chapter, we used the product and function set axioms to construct sets $(Y \times Z)^X$ and $Y^X \times Z^X$ for any given sets $X$, $Y$ and $Z$. Then we used the axioms to construct certain functions $(Y \times Z)^X \rightleftarrows Y^X \times Z^X$. Then we used the axioms again to prove that these functions are mutually inverse, thus establishing that $(Y \times Z)^X \cong Y^X \times Z^X$.

In this chapter, we state the last four of the ten axioms. Once we've got all ten, we'll spend the rest of the course constructing more things from them and proving new results from them—both familiar and unfamiliar.

## 3.1 Fibres

Given a function $f : X \to Y$ and an element $y \in Y$, we ought to be able to construct the subset

$$\{x \in X : f(x) = y\} \tag{3.1}$$

of $X$. You've already met (3.1): it's the preimage or inverse image $f^{-1}\{y\}$ of the subset $\{y\} \subseteq Y$. We can talk about the preimage of *any* subset of $Y$, not just one-element subsets. But preimages of one-element subsets are especially interesting and have a special name: $f^{-1}\{y\}$ is called the 'fibre' of $f$ over $y$, and often written as $f^{-1}(y)$, with round rather than curly brackets. Figure 3.1 is meant to suggest the reason for the name.

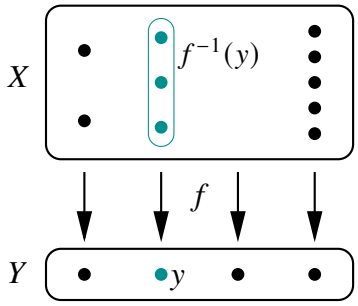



Figure 3.1: The fibre $f^{-1}(y)$ of a function $f$ over an element $y$.

**Warning 3.1.1** A classic mistake is to think that preimages are defined in terms of inverse functions. They're not! For *any* function $f\colon X \to Y$ whatsoever—invertible or not—and any subset $B \subseteq Y$, we can define the preimage or inverse image

$$f^{-1}B = \{x \in X : f(x) \in B\}.$$

As you can see, this definition makes perfect sense whether or not $f$ has an inverse. And there's no function '$f^{-1}$' appearing in the definition.

Here I'm talking about the ordinary mathematics that you're used to. We haven't defined preimages in our axiomatic development yet, but when we do, it will also be the case that they're defined whether or not the function is invertible.

**Warning 3.1.2** Make sure you've digested Warning 3.1.1! This is an extremely common misunderstanding. If you're unsure, please ask.

**Exercise 3.1.3** For which functions $f$ are all the fibres of $f$ nonempty?

Let $f\colon X \to Y$ and $y \in Y$. Axiom 7 will state that the fibre $f^{-1}(y)$ exists. But how can we say this formally?

To begin with, $f^{-1}(y)$ is not just a set but a *subset* of $X$: it comes equipped with an inclusion function

$$i\colon f^{-1}(y) \to X.$$

So the question is, what are the crucial properties of the set $f^{-1}(y)$ and the inclusion function $i\colon f^{-1}(y) \to X$?

First, $f(i(u)) = y$ for all $u \in f^{-1}(y)$.

Second, and conversely, if $x \in X$ with $f(x) = y$ then $x = i(u)$ for a unique element $u \in f^{-1}(y)$.

The previous paragraph was about *elements* of $X$ and $f^{-1}(y)$, and elements are functions out of $\mathbf{1}$. More generally, we can consider functions out of an arbitrary set instead (as we did when formulating the definitions of product and function set). Let $A$ be any set, not necessarily $\mathbf{1}$. What's a function $A \to f^{-1}(y)$? It's essentially a function $A \to X$ which when followed by $f$ has constant value $y$. More formally, given a function $q\colon A \to X$ such that $f(q(a)) = y$ for all $a \in A$, there should be a unique function $\bar{q}\colon A \to f^{-1}(y)$ such that $q = i \circ \bar{q}$. The previous paragraph is the case $A = \mathbf{1}$ (writing $q = x$ and $\bar{q} = u$).

In diagrams, the fact that $f(i(u)) = y$ for all $u \in f^{-1}(y)$ means that the square

$$\begin{array}{ccc} f^{-1}(y) & \longrightarrow & \mathbf{1} \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle y} \\ X & \xrightarrow[f]{} & Y \end{array}$$

commutes. Here the clockwise composite $f^{-1}(y) \to \mathbf{1} \xrightarrow{y} Y$ is the function $f^{-1}(y) \to Y$ with constant value $y$. And the property of the fibre just described can be illustrated like this:

$$\begin{array}{ccccc} A & & \overset{\bar{q}}{\cdots\!\to} & & \\ & \searrow & & f^{-1}(y) & \longrightarrow \mathbf{1} \\ & {\scriptstyle q}\searrow & & {\scriptstyle i}\downarrow & \downarrow{\scriptstyle y} \\ & & & X & \xrightarrow[f]{} Y \end{array} \tag{3.2}$$

This suggests the following definition, in which I'll write $U$ instead of $f^{-1}(y)$.

**Definition 3.1.4** Let $f\colon X \to Y$ be a function and $y \in Y$. A **fibre** of $f$ over $y$ is a set $U$ together with a function $i\colon U \to X$, such that $f(i(u)) = y$ for all $u \in U$ and the following property holds:

> for all sets $A$ and functions $q\colon A \to X$ such that $f(q(a)) = y$ for all $a \in A$, there is a unique function $\bar{q}\colon A \to U$ such that $q = i \circ \bar{q}$.

**Remark 3.1.5** Again, the special case $A = \mathbf{1}$ is particularly important. It tells us that for all $x \in X$ satisfying $f(x) = y$, there is a unique $u \in U$ such that $x = i(u)$.

**Axiom 7 (Fibres)** *For every function $f : X \to Y$ and element $y \in Y$, there exists a fibre of $f$ over $y$.*

From now on, we will assume that Axiom 7 holds.

It won't surprise you by now that although a fibre is officially a set $U$ *together with* a function $i : U \to X$ with the property above, we often casually use 'fibre' to mean just the set $U$, and refer to $i$ as the **inclusion** of the fibre.

As you'll also expect by now, fibres are both isomorphism-invariant and unique up to isomorphism:

**Lemma 3.1.6** *Let $f : X \to Y$ be a function and $y \in Y$. Take sets and functions $U \xrightarrow{i} X$ and $U' \xrightarrow{i'} X$, and suppose there exists an isomorphism $j : U \to U'$ such that the diagram*

$$\begin{array}{ccc} U & & \\ {\scriptstyle j}\downarrow{\scriptstyle \cong} & \searrow^{i} & \\ U' & \nearrow_{i'} & X \end{array}$$

*commutes. Then $U \xrightarrow{i} X$ is a fibre of $f$ over $y$ if and only if $U' \xrightarrow{i'} X$ is.*

**Proof** Similar to the proofs of Lemmas 2.3.3, 2.6.6 and 2.7.5, and omitted. □

**Lemma 3.1.7** *Let $f : X \to Y$ be a function and $y \in Y$. Let $U \xrightarrow{i} X$ and $U' \xrightarrow{i'} X$ be fibres of $f$ over $y$. Then there is a unique isomorphism $j : U \to U'$ such that the diagram*

$$\begin{array}{ccc} U & & \\ {\scriptstyle j}\downarrow{\scriptstyle \cong} & \searrow^{i} & \\ U' & \nearrow_{i'} & X \end{array}$$

*commutes.*

**Proof** Similar to the proofs of Lemmas 2.3.4, 2.6.8 and 2.7.6, and omitted. □

Lemma 3.1.7 allows us to speak of *the* fibre of $f$ over $y$ and to give it a name, $f^{-1}(y)$. The inclusion $f^{-1}(y) \to X$ usually goes nameless, although I will sometimes use the symbol $\hookrightarrow$ (a combination of an arrow and a subset symbol), as in $f^{-1}(y) \hookrightarrow X$.

Next we'll show that the inclusion of a fibre is always injective—a term we haven't defined yet.

**Definition 3.1.8** Let $S$ and $T$ be sets. A function $g : S \to T$ is:

i. **injective** if for all $s, s' \in S$,

$$g(s) = g(s') \implies s = s';$$

ii. **surjective** if for all $t \in T$, there exists $s \in S$ such that $g(s) = t$;

iii. **bijective** if it is injective and surjective.

In the next section, we will prove that being bijective is equivalent to being invertible.

**Examples 3.1.9** i. Any function with domain $\mathbf{1}$ is injective, since $\mathbf{1}$ has only one element. So too is any function with empty domain.

ii. Let $g\colon S \to T$ and $h\colon T \to S$ be functions such that $hg = \mathrm{id}_S$. Then $g$ is injective and $h$ is surjective. You can show this directly or deduce it from question 8 on Workshop 1.

**Exercise 3.1.10** Forgetting the axioms for a moment, do you expect it to be the case that if $g\colon S \to T$ is injective, there exists a function $h\colon T \to S$ such that $hg = \mathrm{id}_S$?

**Lemma 3.1.11** *Let $f\colon X \to Y$ be a function and $y \in Y$. Then the inclusion $f^{-1}(y) \hookrightarrow X$ is injective.*

**Proof** Write $i\colon f^{-1}(y) \to X$ for the inclusion. Let $u, u' \in f^{-1}(y)$ with $i(u) = i(u')$. Write $x = i(u) = i(u') \in X$. Then $f(x) = f(i(u)) = y$, so by definition of fibre (and Remark 3.1.5), there is a *unique* $v \in U$ such that $i(v) = x$. But $v = u$ and $v = u'$ both have this property, so $u = u'$. □

## 3.2 Subsets

Sometimes we want to define a function on a case-by-case basis. For example, we might want to define $h\colon \mathbb{R} \to \mathbb{R}$ by

$$h(x) = \begin{cases} x \sin(1/x) & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

A simple instance is the definition of characteristic function. Fix a two-element set $\mathbf{2} = \{\mathsf{T}, \mathsf{F}\}$ (for 'true' and 'false'). Given a subset $A$ of a set $X$, its characteristic function $\chi_A\colon X \to \mathbf{2}$ is defined by

$$\chi_A(x) = \begin{cases} \mathsf{T} & \text{if } x \in A, \\ \mathsf{F} & \text{if } x \notin A. \end{cases}$$

It is the unique function $\chi\colon X \to \mathbf{2}$ such that $\chi^{-1}(\mathsf{T}) = A$.

This is how characteristic functions work ordinarily. To ensure that they work the same way in our set theory, we now demand that there exist a set $\mathbf{2}$ and an element $\top \in \mathbf{2}$ with the property just stated. But we don't have a definition of 'subset' yet! So instead, we phrase the axiom in terms of injections. Here we have in mind that subset inclusions are injective.

In the following definition, we write $\Omega$ and $t$ instead of $\mathbf{2}$ and $\top$.

**Definition 3.2.1** A **subset classifier** is a set $\Omega$ together with an element $t \in \Omega$, with the following property:

> for all sets $A$ and $X$ and injections $i\colon A \to X$, there is a unique function $\chi\colon X \to \Omega$ such that $i\colon A \to X$ is a fibre of $\chi$ over $t$.

In a diagram:

$$\begin{array}{ccc} A & \longrightarrow & \mathbf{1} \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle t} \\ X & \xrightarrow[\chi]{} & \Omega. \end{array}$$

**Axiom 8 (Subsets)** *There exists a subset classifier.*

From now on, we will assume that Axiom 8 holds.

At the end of Section 1.3, we saw that there are two different ways of accessing the notion of subset via functions. One is that a subset of $X$ is essentially an injection into $X$: think about inclusion functions. The other is that a subset of $X$ is a function from $X$ to a two-element set: each element of $X$ is switched on or off. Axiom 8 essentially says that the two approaches are equivalent.

As you'd guess, subset classifiers are isomorphism-invariant and unique up to isomorphism:

**Lemma 3.2.2** *Let $\Omega$ and $\Omega'$ be sets, and let $t \in \Omega$ and $t' \in \Omega'$. Suppose there exists an isomorphism $j\colon \Omega \to \Omega'$ such that $j(t) = t'$. Then $\Omega$ together with $t$ is a subset classifier if and only if $\Omega'$ together with $t'$ is.*

**Proof** Similar to the proofs of Lemmas 2.3.3, 2.6.6, 2.7.5 and 3.1.6, and omitted. □

**Lemma 3.2.3** *Let $\Omega$ together with $t \in \Omega$ be a subset classifier, and let $\Omega'$ together with $t' \in \Omega'$ be another subset classifier. Then there is a unique isomorphism $j\colon \Omega \to \Omega'$ such that $j(t) = t'$.*

**Proof** Similar to the proofs of Lemmas 2.3.4, 2.6.8, 2.7.6 and 3.1.7, and omitted. Here we use the fact that $t\colon \mathbf{1} \to \Omega$ and $t'\colon \mathbf{1} \to \Omega'$ are injective (Example 3.1.9(i)). □

As usual, Lemma 3.2.3 gives us the right to speak of *the* subset classifier, and to give it a name. We denote the set by **2** and its distinguished element by $\mathsf{T}$.

**Warning 3.2.4** For now, **2** is just suggestive notation. We haven't explicitly specified that **2** has exactly two elements. In fact, it does, as we'll prove in the next chapter—but it's a theorem, not an axiom.

Also, we haven't defined an element of **2** called $\mathsf{F}$ yet. This will be done in the next chapter too.

Given an injection $A \xrightarrow{i} X$, we write $\chi_i$ for the unique function $X \to \mathbf{2}$ whose fibre over $\mathsf{T}$ is $A \xrightarrow{i} X$. It is called the **characteristic function** of $i$. In a diagram:

$$\begin{array}{ccc} A & \longrightarrow & \mathbf{1} \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle \mathsf{T}} \\ X & \xrightarrow[\chi_i]{} & \mathbf{2}. \end{array} \tag{3.3}$$

The next lemma says that characteristic functions do what we intend.

**Lemma 3.2.5** *Let $i\colon A \to X$ be an injection and $x \in X$. Then*

$$\chi_i(x) = \mathsf{T} \iff \textit{there exists } a \in A \textit{ such that } i(a) = x.$$

Since $i$ is injective, the $a$ here is necessarily unique.

**Proof** $\Longleftarrow$ : by definition of characteristic function, $A \xrightarrow{i} X$ is the fibre of $\chi_i\colon X \to \mathbf{2}$ over $\mathsf{T} \in \mathbf{2}$. Then by definition of fibre (Definition 3.1.4), $\chi_i(i(a)) = \mathsf{T}$ for all $a \in A$.

$\Longrightarrow$ : suppose that $\chi_i(x) = \mathsf{T}$. Then again by definition of fibre (and Remark 3.1.5), there is a unique $a \in A$ such that $x = i(a)$. □

For an injection $A \xrightarrow{i} X$, we sometimes write $\chi_i$ as $\chi_A$ and call it the characteristic function of $A$. This is risky, since $\chi_i$ genuinely depends on $i$, not just $A$ (as Example 3.2.6(ii) shows). We do it when the choice of $i$ is somehow 'obvious' given $A$ and $X$ (as in Example 3.2.6(i)).

**Examples 3.2.6** In these examples, I will use the natural numbers and curly bracket notation, even though they haven't been defined yet.

i. Let $A = \{8, 9\}$ and $X = \mathbb{N}$. The inclusion $i\colon \{8, 9\} \to \mathbb{N}$ has characteristic function $\chi_i\colon \mathbb{N} \to \mathbf{2}$ satisfying

$$\chi_i(n) = \mathsf{T} \iff n = 8 \text{ or } n = 9$$

($n \in \mathbb{N}$). In this case, there's an obvious injection $\{8, 9\} \to \mathbb{N}$ (namely, $i$), so it's reasonable to write $\chi_i$ as $\chi_{\{8,9\}}$.

ii. Let $A = \mathbf{1}$ and $X = \mathbb{N}$. A function $\mathbf{1} \to \mathbb{N}$ is a natural number $i$, and all functions $\mathbf{1} \to \mathbb{N}$ are injective (Example 3.1.9(i)). The characteristic function of $i\colon \mathbf{1} \to \mathbb{N}$ satisfies

$$\chi_i(n) = \mathsf{T} \iff n = i$$

($n \in \mathbb{N}$). In particular, different numbers $i$ have different characteristic functions $\chi_i$, so we need the fussier notation: we can't call them all $\chi_{\mathbf{1}}$.

**Digression 3.2.7** In probability and measure theory, subsets are often handled using their characteristic functions. For example, given an integration operator $\int$ on a space $X$, we obtain a measure $\mu$ on $X$ by defining $\mu(A) = \int_X \chi_A$ for each measurable subset $A$ of $X$. Here $\chi_A(x)$ is 1 if $x \in A$ and 0 otherwise; that is, we use 1 and 0 instead of $\mathsf{T}$ and $\mathsf{F}$. (Also, measure theorists usually write $\chi_A$ as $I_A$ and call it an indicator function.) Similarly, the probability of an event is the expectation of its characteristic function.

The influential probability theorist Bruno de Finetti advocated using the *same symbol* for a subset and its characteristic function. He would have written $\chi_A$ as just $A$. For him, a subset of $X$ was literally the same thing as a function from $X$ to the two-element set. And in fact, that is how we will *define* subsets.

**Definition 3.2.8** Let $X$ be a set. A **subset** of $X$ is a function $X \to \mathbf{2}$.

Think of a function $X \to \mathbf{2}$ as saying 'yes' or 'no' to each element of $X$. That's what a subset is.

**Definition 3.2.9** Let $X$ be a set. The **power set** of $X$ is $\mathbf{2}^X$, also written as $\mathscr{P}(X)$.

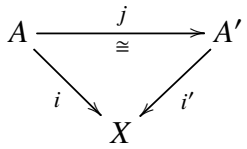
The elements of the power set are the functions $X \to \mathbf{2}$, that is, the subsets of $X$.

**Exercise 3.2.10** Take a finite set with $n$ elements. How many elements should its power set have? (We haven't defined 'finite' or 'number of elements' in our axiomatic development yet, but use what you know.)

**Exercise 3.2.11** If you had to write down all the subsets of a ten-element set, how would you do it?

We now look more closely at the correspondence between injections into $X$ and functions $X \to \mathbf{2}$. Different injections into $X$ can have the same characteristic function. When does this happen?

**Definition 3.2.12** Let $X$ be a set. Two functions $A \xrightarrow{i} X$ and $A' \xrightarrow{i'} X$ are **isomorphic over** $X$ if there exists an isomorphism $j\colon A \to A'$ such that the diagram




commutes. We then write $(A \xrightarrow{i} X) \cong_X (A' \xrightarrow{i'} X)$ or, less formally, $A \cong_X A'$.

**Examples 3.2.13** In these examples, I will again use the natural numbers and curly bracket notation, even though we haven't defined them yet.

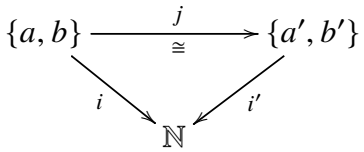
i. Let $\{a, b\}$ and $\{a', b'\}$ be two-element sets. Define $i\colon \{a, b\} \to \mathbb{N}$ and $i'\colon \{a', b'\} \to \mathbb{N}$ by

$$i(a) = i'(a') = 10, \quad i(b) = i'(b') = 12.$$

Then $\{a, b\} \xrightarrow{i} \mathbb{N}$ and $\{a', b'\} \xrightarrow{i'} \mathbb{N}$ are isomorphic over $\mathbb{N}$, since there is an isomorphism $j\colon \{a, b\} \to \{a', b'\}$ defined by

$$j(a) = a', \ j(b) = b', \tag{3.4}$$

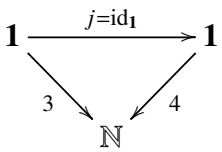
and it makes the diagram




(3.5)

commute. (We'll show later that the 'definition' of $j$ is valid, i.e. there really does exist an isomorphism $j\colon \{a, b\} \to \{a', b'\}$ satisfying (3.4).)

ii. Consider the elements $3\colon \mathbf{1} \to \mathbb{N}$ and $4\colon \mathbf{1} \to \mathbb{N}$ of $\mathbb{N}$. As functions into $\mathbb{N}$, they are *not* isomorphic over $\mathbb{N}$. Indeed, there is only one isomorphism $j\colon \mathbf{1} \to \mathbf{1}$, namely, the identity; but the diagram




does not commute, since $3 \neq 4$.

**Exercise 3.2.14** Why does the triangle (3.5) commute?

Informally put, two injections into $X$ are isomorphic over $X$ if and only if they have the same image. (But we haven't defined images yet!)

**Warning 3.2.15** If $(A \xrightarrow{i} X)$ and $(A' \xrightarrow{i'} X)$ are isomorphic over $X$ then $A \cong A'$, by definition. But the converse is false, as Example 3.2.13(ii) shows. So being isomorphic over $X$ is a stronger property than merely being isomorphic.

**Lemma 3.2.16** *Let $X$ be a set, and let $A \xrightarrow{i} X$ and $A' \xrightarrow{i'} X$ be injections. Then*

$$(A \xrightarrow{i} X) \cong_X (A' \xrightarrow{i'} X) \iff \chi_i = \chi_{i'}.$$

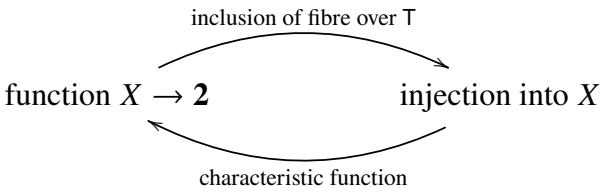
Or in more casual notation, $A \cong_X A' \iff \chi_A = \chi_{A'}$.

**Proof** For $\Longrightarrow$, suppose that $(A \xrightarrow{i} X) \cong_X (A' \xrightarrow{i'} X)$. By definition, $A \xrightarrow{i} X$ is a fibre of $\chi_A$ over $\mathsf{T}$. Lemma 3.1.6 tells us that fibres are invariant under isomorphism over $X$, so $A' \xrightarrow{i'} X$ is also a fibre of $\chi_A$ over $\mathsf{T}$. On the other hand, by definition of characteristic function, $\chi_{A'}$ is the *unique* function $\chi\colon X \to \mathbf{2}$ such that $A' \xrightarrow{i'} X$ is a fibre of $\chi$ over $\mathsf{T}$. Hence $\chi_A = \chi_{A'}$.

For $\Longleftarrow$, suppose that $\chi_i = \chi_{i'}$. Then $A \xrightarrow{i} X$ and $A' \xrightarrow{i'} X$ are both fibres of $\chi_i$ over $\mathsf{T}$. Lemma 3.1.7 tells us that fibres are unique up to isomorphism over $X$, so $(A \xrightarrow{i} X) \cong_X (A' \xrightarrow{i'} X)$. □

**Remark 3.2.17** Let's think again about the two ways of viewing subsets as functions.

Given a function $\chi\colon X \to \mathbf{2}$, we get the inclusion function $\chi^{-1}(\mathsf{T}) \hookrightarrow X$, which is an injection into $X$ (by Lemma 3.1.11). In the other direction, given an injection $A \xrightarrow{i} X$, we get its characteristic function $\chi_i\colon X \to \mathbf{2}$:




If we start on the left with a function $\chi\colon X \to \mathbf{2}$, then take the inclusion $\chi^{-1}(\mathsf{T}) \hookrightarrow X$, then take *its* characteristic function, we get back to $\chi$ again, by definition of characteristic function.

On the other hand, suppose we start on the right with an injection $A \overset{i}{\to} X$, take its characteristic function $\chi_i \colon X \to \mathbf{2}$, then form the fibre $\chi_i^{-1}(\mathsf{T}) \hookrightarrow X$. Since $A \overset{i}{\to} X$ is also a fibre of $\chi_i$ over $\mathsf{T}$ (by definition of characteristic function), and fibres are unique up to isomorphism over $X$ (Lemma 3.1.7), the injection $\chi_i^{-1}(\mathsf{T}) \hookrightarrow X$ that we end up with is isomorphic over $X$ to our original injection $A \overset{i}{\to} X$. (Whether they are literally equal is not really a meaningful question. To be equal, we'd need their domains to be equal; but we never ask whether two sets are equal, only whether they're isomorphic.)

Putting this all together:

> *There is a one-to-one correspondence between functions $X \to \mathbf{2}$ and isomorphism classes of injections into $X$,*

where 'isomorphism' means isomorphism over $X$.

We will use this correspondence all the time, usually without mentioning it. In particular, although a subset of $X$ is officially defined as a function $X \to \mathbf{2}$, we will often view subsets as injections into $X$, with the understanding that we never distinguish between injections into $X$ that are isomorphic over $X$.

Axiom 8 is very powerful. We now prove two results that we couldn't prove before: bijections are invertible, and all empty sets are isomorphic.

**Proposition 3.2.18** *Let $i \colon A \to X$ be a function. The following are equivalent:*

*i. $i$ is an isomorphism;*

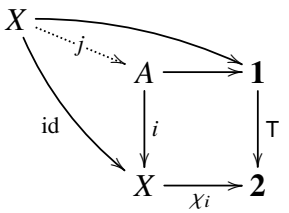
*ii. $i$ is a bijection;*

*iii. $i$ is an injection and $\chi_i(x) = \mathsf{T}$ for all $x \in X$.*

**Proof** (i) $\Longrightarrow$ (ii) is Workshop 1, question 9.

(ii) $\Longrightarrow$ (iii): assuming (ii), certainly $i$ is injective. Let $x \in X$. Since $i$ is surjective, we can choose $a \in A$ such that $i(a) = x$. Then $\chi_i(x) = \chi_i(i(a)) = \mathsf{T}$, since $A \overset{i}{\to} X$ is the fibre of $\chi_i$ over $\mathsf{T}$ (diagram (3.3)).

(iii) $\Longrightarrow$ (i): assuming (iii), the outer square of the diagram



commutes. (Compare diagram (3.2).) So by definition of fibre, there is a unique function $j\colon X \to A$ such that $i \circ j = \mathrm{id}_X$. Now for all $a \in A$, we have $iji(a) = \mathrm{id}_X i(a) = i(a)$, and $i$ is injective, so $ji(a) = a$. Hence $j \circ i = \mathrm{id}_A$, completing the proof that $i$ is an isomorphism. □

The most important part of Proposition 3.2.18 is that every bijection is an isomorphism.

**Example 3.2.19** How is the square root function $\sqrt{\ }\colon \mathbb{R}^+ \to \mathbb{R}^+$ defined? One route often taken in analysis is as follows. First you define the squaring function $f\colon \mathbb{R}^+ \to \mathbb{R}^+$. Then you show that $f$ is injective (by basic algebra) and surjective (using the intermediate value theorem). Hence $f$ is bijective. We now want to define $\sqrt{\ }\colon \mathbb{R}^+ \to \mathbb{R}^+$ as the inverse function of $f$. But how do we know that a bijection *has* an inverse? That's exactly what Proposition 3.2.18 does for us.

(Again, this example uses concepts such as the real numbers that haven't officially been defined yet.)

**Digression 3.2.20** The equivalence between bijectivity and invertibility is typical of algebraic rather than geometric structures. (Sets are a degenerate case of both.) For example, it's a very useful lemma that a bijective group or ring homomorphism is an isomorphism—meaning that its inverse is a homomorphism too. Similarly, given a bijective linear map between vector spaces, its inverse is also linear. But for a bijective continuous map between topological spaces, the inverse is not always continuous. An example is the bijection from $[0, 1)$ to the unit circle in $\mathbb{C}$ given by $t \mapsto e^{2\pi i t}$.

Next we show that all empty sets are isomorphic.

**Definition 3.2.21** A set $I$ is **initial** if for all sets $X$, there is a unique function from $I$ to $X$.

Initiality is the dual concept of terminality, in the sense that the two definitions are the same but with the directions of the functions reversed.

Any two initial sets are isomorphic, just as for terminality (Lemma 2.3.4); this is Workshop 1, question 11(i).

**Proposition 3.2.22** *A set is empty if and only if it is initial.*

**Proof** First let $E$ be an empty set. To show that $E$ is initial, let $X$ be any set. We must prove that there exists a unique function $E \to X$.

*Existence:* Consider the product diagram

$$E \xleftarrow{\mathrm{pr}_1} E \times X \xrightarrow{\mathrm{pr}_2} X.$$

Any function into an empty set is bijective (Workshop 1, question 10), so $\mathrm{pr}_1$ is bijective. Proposition 3.2.18 then implies that $\mathrm{pr}_1$ is invertible, giving us the function $\mathrm{pr}_2 \circ \mathrm{pr}_1^{-1} : E \to X$.

*Uniqueness:* Since a function is determined by its effect on elements, and $E$ has no elements, all functions $E \to X$ are equal.

Conversely, every initial set is empty (Workshop 1, question 11(ii)). □

**Corollary 3.2.23** *Any two empty sets are isomorphic.*

**Proof** This follows from Proposition 3.2.22 and the fact that any two initial sets are isomorphic. □

Corollary 3.2.23 gives us the right to speak of *the* empty set and to give it a name, $\varnothing$. Since we're writing $\mathbf{1}$ and $\mathbf{2}$ for the one- and two-element sets, it would be more consistent to write the empty set as $\mathbf{0}$. But $\varnothing$ is traditional.

For a set $X$, we write the unique function $\varnothing \to X$ as $!_X$ or $!$, or just leave it nameless.

**Warning 3.2.24** We also use $!_X$ or $!$ to mean the unique function $X \to \mathbf{1}$. But if we're conscientious about specifying our domains and codomains, no confusion should arise.

## 3.3 The natural numbers

**Warning 3.3.1** In this course, 0 is a natural number.

On the basis of the axioms so far, all sets could be finite. Nothing in them prevents that. Our next axiom will.

Loosely, the axiom says 'the natural numbers form a set'. We're going to formalize this by thinking about sequences. In ordinary mathematics, a sequence in a set $X$ is nothing but a function $\mathbb{N} \to X$, as we recalled in Section 1.3. And we expect to be able to define sequences recursively as follows: given an element $a \in X$ and a function $r : X \to X$, we should get a sequence

$$a,\ r(a),\ r(r(a)),\ \ldots.$$

More formally, there should be a unique sequence $(x_n)_{n=0}^{\infty}$ in $X$ such that

$$x_0 = a, \qquad x_{n+1} = r(x_n) \text{ for all } n \in \mathbb{N}. \tag{3.6}$$

Here we're using two pieces of structure on $\mathbb{N}$: the element 0, and the function $s\colon \mathbb{N} \to \mathbb{N}$ given by $s(n) = n + 1$. Equations (3.6) can be expressed as a commutative diagram, writing $x\colon \mathbb{N} \to X$ for the sequence $(x_n)_{n=0}^{\infty}$:

$$\begin{array}{ccccc} \mathbf{1} & \xrightarrow{0} & \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ {\scriptstyle \mathrm{id}}\downarrow & & \vdots x & & \vdots x \\ \mathbf{1} & \xrightarrow[a]{} & X & \xrightarrow[r]{} & X. \end{array}$$

The commutativity of the left-hand square says $x_0 = a$, and that of the right-hand square says $x_{n+1} = r(x_n)$ for all $n \in \mathbb{N}$.

We're now going to use this principle—that it's possible to define sequences recursively like this—to *characterize* the natural numbers. In the following definition, we write $N$, $z$ and $\sigma$ instead of $\mathbb{N}$, 0 and $s$.

**Definition 3.3.2** A **natural number system** is a set $N$ together with an element $z \in N$ and a function $\sigma\colon N \to N$, with the following property:

> for all sets $X$, elements $a \in X$ and functions $r\colon X \to X$, there is a unique function $x\colon N \to X$ such that $x(z) = a$ and $x(\sigma(n)) = r(x(n))$ for all $n \in N$.

In a diagram:

$$\begin{array}{ccccc} \mathbf{1} & \xrightarrow{z} & N & \xrightarrow{\sigma} & N \\ {\scriptstyle \mathrm{id}}\downarrow & & \vdots x & & \vdots x \\ \mathbf{1} & \xrightarrow[a]{} & X & \xrightarrow[r]{} & X. \end{array}$$

**Axiom 9 (Natural numbers)** *There exists a natural number system.*

From now on, we will assume that Axiom 9 holds.

Definition 3.3.2 is another universal property (our sixth!). One last time, we have the usual pair of lemmas: isomorphism-invariance and uniqueness up to isomorphism.

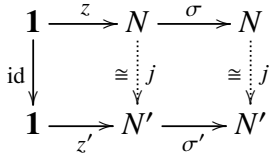
**Lemma 3.3.3** *Let $N$ and $N'$ be sets, let $z \in N$ and $z' \in N'$, and let $\sigma\colon N \to N$ and $\sigma'\colon N' \to N'$. Suppose there exists an isomorphism $j\colon N \to N'$ such that the diagram*

$$\begin{array}{ccccc} \mathbf{1} & \xrightarrow{z} & N & \xrightarrow{\sigma} & N \\ {\scriptstyle \mathrm{id}}\downarrow & & \cong \vdots j & & \cong \vdots j \\ \mathbf{1} & \xrightarrow[z']{} & N' & \xrightarrow[\sigma']{} & N' \end{array}$$

*commutes. Then $N$ together with $z$ and $\sigma$ is a natural number system if and only if $N'$ together with $z'$ and $\sigma'$ is.*

**Proof** Similar to the proofs of Lemmas 2.3.3, 2.6.6, 2.7.5, 3.1.6 and 3.2.2, and omitted. □

**Lemma 3.3.4** *Let $N$ together with $z \in N$ and $\sigma\colon N \to N$ be a natural number system, and let $N'$ together with $z' \in N'$ and $\sigma'\colon N' \to N'$ be another natural number system. Then there is a unique isomorphism $j\colon N \to N'$ such that the diagram*




*commutes.*

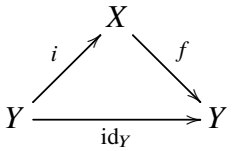
**Proof** Similar to the proofs of Lemmas 2.3.4, 2.6.8, 2.7.6, 3.1.7 and 3.2.3, and omitted. □

Lemma 3.3.4 gives us the right to speak of *the* natural number system. We write it as $\mathbb{N}$ together with $0 \in \mathbb{N}$ and $s\colon \mathbb{N} \to \mathbb{N}$. The function $s$ is called the **successor** function.

These are the *definitions* of $\mathbb{N}$, 0 and $s$. We don't have definitions of $1 \in \mathbb{N}$ or addition in $\mathbb{N}$ yet, so it doesn't make sense yet to say '$s(n) = n + 1$', even though that's the intention. In Chapter 7, we'll make these definitions and prove that, indeed, $s(n) = n + 1$ for all $n \in \mathbb{N}$.

## 3.4 The axiom of choice

Consider a pair of functions $X \underset{i}{\overset{f}{\rightleftarrows}} Y$ such that $f \circ i = \mathrm{id}_Y$: the diagram




commutes. As we saw in Example 3.1.9(ii), $f$ must then be surjective, and $i$ injective.

**Definition 3.4.1** A **section** of a function $f\colon X \to Y$ is a function $i\colon Y \to X$ such that $f \circ i = \mathrm{id}_Y$.

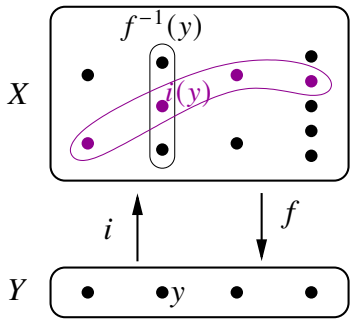



Figure 3.2: A surjection $f$ with a section $i$.

'Section' is just another word for 'right inverse'. I believe it is derived from 'cross section' (Figure 3.2). A section of $f$ picks out one element $i(y)$ of the fibre $f^{-1}(y)$ for each $y \in Y$. Figure 3.2 shows a particular element $y \in Y$, its fibre $f^{-1}(y)$ (the vertical oval), and the chosen element $i(y)$ of the fibre. The banana shape shows all the elements picked out by $i$.

As mentioned above, every function with a section is surjective. Figure 3.2 should also make this intuitively clear: in order to be able to pick out an element $i(y)$ of each fibre $f^{-1}(y)$, we need all these fibres to be nonempty, which means exactly that $f$ is surjective.

What about the converse? Does every surjective function have a section? Our final axiom says 'yes'.

**Axiom 10 (Axiom of choice)** *Every surjection has a section.*

It is called the axiom of choice because a section of a surjection $f\colon X \to Y$ is a choice, for each $y \in Y$, of an element of the nonempty set $f^{-1}(y)$. If $Y$ is infinite then finding a section means making infinitely many choices, and it's maybe less intuitively obvious that this should be possible. (We'll define 'finite' and 'infinite' later.)

An informal example: if you have an infinite number of pairs of shoes and want to choose one from each pair, you don't need the axiom of choice: just choose the left shoe every time. But for the same problem with socks, you have infinitely many arbitrary choices to make, and you do need the axiom of choice.

**Warning 3.4.2** Most of our axioms involve some kind of uniqueness. But the axiom of choice does not. A surjection $f$ typically has *many* sections, as Figure 3.2 suggests.

**Exercise 3.4.3** How many sections does the surjection $f$ of Figure 3.2 have?

You'll be expecting me to say that from now on, we will assume Axiom 10. And we will, but with a difference. Mathematicians often consider it in poor taste to use the axiom of choice unnecessarily. We, too, will take care not to use it unless we absolutely have to. And in fact, we will not need it until Chapter 9.

**Digression 3.4.4** Attitudes to the axiom of choice differ. Reading textbooks, you can be made to feel like some kind of pedant for using it:

> wise-guys who like using the axiom of choice will have to worry about [continuity], along with wolves under the bed, etc

(Strichartz, *A Guide to Distribution Theory and Fourier Transforms*, p. 2), but you can also find yourself mocked for *not* wanting to use it:

> It even avoids using the axiom of choice, as if that mattered

(Weaver, *Lipschitz Algebras*, p. 4). Where subjects contain results that are felt by its practitioners to be counterintuitive or 'pathological', it's a sign that the formalization doesn't match the intuition, and suggests that the foundations of the subject aren't right. But it is sometimes blamed on the axiom of choice.

There are practical reasons to avoid using choice unnecessarily. It *isn't* just because of philosophical concerns over whether the axiom of choice is 'true' (whatever that means). For example, if we use the axiom of choice in some argument about sets then there's little chance of being able to translate it into an analogous argument about topological spaces, since the topological analogue of the axiom of choice is false (Digression 1.4.1). Or if we are interested in computer science then we may want all our functions to be computable—executable by an algorithm—in which case we also need to avoid using the axiom of choice, because everything has to be constructive.

## 3.5 Summary of the axioms

Here I will simply restate the axiomatization concisely.

The data to which the axioms apply:

- Some things called sets;
- for each set $X$ and set $Y$, some things called functions from $X$ to $Y$, with functions $f$ from $X$ to $Y$ written as $f\colon X \to Y$;

- for each set $X$, set $Y$ and set $Z$, an operation called composition assigning to each $f\colon X \to Y$ and $g\colon Y \to Z$ a function $g \circ f\colon X \to Z$;
- for each set $X$, a function $\mathrm{id}_X\colon X \to X$, called an identity function.

The axioms:

1. Composition of functions is associative, and the identity functions act as identities.
2. There exists a terminal set.
3. If $f, g\colon X \to Y$ with $f(x) = g(x)$ for all $x \in X$, then $f = g$.
4. There exists an empty set.
5. Let $X$ and $Y$ be sets. Then there exists a product of $X$ and $Y$.
6. Let $X$ and $Y$ be sets. Then there exists a function set from $X$ to $Y$.
7. Let $f\colon X \to Y$ and $y \in Y$. Then there exists a fibre of $f$ over $y$.
8. There exists a subset classifier.
9. There exists a natural number system.
10. Every surjection has a section.

Axioms 2 and 5–9 all involve universal properties, and all characterize the set concerned uniquely up to isomorphism.

Axioms 3, 4 and 7 all refer to elements, defined as functions whose domain is the terminal set $\mathbf{1}$.

Axiom 8 is weaker than the informal version in Figure 1.4 suggests. The informal version says that for all sets $X$, subsets of $X$ correspond to functions from $X$ to the *two-element* set. But Axiom 8 doesn't actually mention the two-element set. It only says that there is *some* set $\mathbf{2}$ such that for all sets $X$, subsets of $X$ (or really, injections into $X$) correspond to functions from $X$ to $\mathbf{2}$. Showing that $\mathbf{2}$ has two elements is one of our tasks for the next chapter.

Now that we've formulated our axioms, the rest of the course is about building the familiar apparatus of mathematics on top of them. Every time we succeed in constructing something important from the axioms (like the real numbers or the principle of mathematical induction), it should give us a little bit more confidence that our axioms were well-chosen—that they're powerful enough to enable us to do everything we ever want.

# Chapter 4

# Subsets

*To read by Monday 7 October: Sections 4.1 and 4.2.*
*To read by Friday 11 October: Sections 4.3 and 4.4.*

The axioms are powerful enough to provide just about everything a mathematician might ever need to do with sets. But at this early stage, many questions remain unanswered—some of which you've already asked me during class. Several of these questions involve subsets. For instance:

- Given that an element is an element of only one set, how can we make sense of statements like '$4 \in \mathbb{N}$ belongs to the subset $\{1, 2, 3, 4, 5\}$ of $\mathbb{N}$'?
- What should it mean for one subset of a set to be contained in another?
- Is the subset classifier $\mathbf{2}$ a two-element set?
- Can we define the intersection and union of two subsets?
- We took it as an axiom that fibres exist, and fibres are preimages of singletons, but what about preimages of arbitrary subsets? And what about images?

In this chapter, we'll answer all these questions.

To help your intuition, I will sometimes use examples involving objects that have not been constructed from the axioms yet, but which you know from elsewhere in your mathematical life. For instance, the real numbers will not be defined until Chapter 7, but will nonetheless appear in examples before then.

Such examples are purely for explanatory purposes and are not part of the formal development, so there is no logical circularity. When I use them, I will put an hourglass in the margin as a reminder that something in the example hasn't been defined yet.

## 4.1 Elements and subsets

Let $X$ be a set. In Section 3.2, we showed that

> *There is a one-to-one correspondence between functions $X \to \mathbf{2}$ and isomorphism classes of injections into $X$,*

where 'isomorphism' means isomorphism over $X$. The correspondence is given in one direction by taking the fibre over $\mathsf{T}$, and in the other by taking the characteristic function (Remark 3.2.17).

Although the official definition of subset of $X$ is a function $X \to \mathbf{2}$, we use this correspondence as justification for sometimes taking 'subset of $X$' to mean injection into $X$, with the understanding that two injections into $X$ are regarded as the same if they are isomorphic over $X$.

**Definition 4.1.1** For an injection $i\colon A \to X$, we write $A \subseteq X$ **with inclusion** $i$.

We often write the inclusion using a hooked arrow, $i\colon A \hookrightarrow X$. (We first introduced this symbol for inclusions of fibres, in Section 3.1.) 'Inclusion' is just another word for 'injection', but it signals a particular viewpoint.

**Remark 4.1.2** If the choice of $i$ is understood, we sometimes more casually say '$A$ is a subset of $X$'. But it's important to understand that a subset of $X$ isn't a set $A$ *such that* something or other; it's a set $A$ *equipped with* some extra data, namely, an injection into $X$. Example 3.2.6(ii) gives an example of different subsets that have the same '$A$'.

Everyday mathematical language is fuzzy on the difference between sets and subsets. For example, people often talk about 'open sets' in $\mathbb{R}^n$, or more generally in a topological space $X$. 'Open set in $X$' really means 'open *subset* of $X$', and the choice of $X$ genuinely matters. For example, it doesn't make sense to ask 'is the set $[0, 1)$ open?' It's not an open subset of $\mathbb{R}$, but it is an open subset of $[0, 2]$.

Similarly, in linear algebra, when people talk about a 'spanning set' in a vector space $X$, this really means 'subset of $X$ that spans $X$', and again the choice of $X$ matters. For example, $\{(1, 0, 0), (0, 1, 0)\}$ is not a spanning subset of $\mathbb{R}^3$, but it is a spanning subset of $\{(x, y, z) \in \mathbb{R}^3 : z = 0\}$.

In short, to regard $A$ as a subset of $X$ (and not just as an abstract set) is to take into account the relationship between $A$ and $X$.

**Warning 4.1.3** Some people use the symbol $\subset$ to mean subset, which we write as $\subseteq$. Others use $\subset$ to mean *proper* subset (by analogy with $<$ and $\leq$). To avoid ambiguity, I will not use $\subset$ at all.

**Examples 4.1.4** Let $X$ be a set.

i. The unique function $!_X \colon \varnothing \to X$ is injective (Example 3.1.9(i)), so $\varnothing \subseteq X$ with inclusion $!_X$.

ii. The identity $\mathrm{id}_X$ is injective, and $X \subseteq X$ with inclusion $\mathrm{id}_X$.

iii. Let $x \in X$. Then the function $x \colon \mathbf{1} \to X$ is injective (Example 3.1.9(i)) and therefore defines a subset of $X$. We write $\{x\} \hookrightarrow X$ for this subset, and call it a **singleton** subset of $X$. In other words, $\{x\} \hookrightarrow X$ is just $\mathbf{1} \xrightarrow{x} X$ (at least, up to isomorphism over $X$, which is all we care about). So $\{x\}$ means a one-element set equipped with the injection $\{x\} \to X$ that is isomorphic over $X$ to $x \colon \mathbf{1} \to X$.

   This is the first time we have rigorously defined anything involving curly brackets. For now, all we have defined is $\{x\}$ for a single element $x$. Subsets like $\{x, y\}$ will come later.

iv. In Example 2.6.11(i), we met the diagonal function $\Delta_X \colon X \to X \times X$. It is injective, so we can regard $X$ as a subset of $X \times X$ with inclusion $\Delta_X$.

**Exercise 4.1.5** Prove that for every set $X$, the diagonal function $\Delta_X \colon X \to X \times X$ is injective. Why do you think the word 'diagonal' is used? (Try drawing a diagram with $X = \mathbb{R}$.)

**Digression 4.1.6** As pointed out in both Warning 1.1.2 and Remark 4.1.2, the everyday mathematical language of subsets can be hazy, inexact, and even contradictory. But any rigorous axiomatic development has to be clear, precise and free from contradiction. So, there is inevitably some friction between the two. In other words, in any axiomatic system whatsoever, the formal language is never going to exactly mirror the language that mathematicians normally use; it will feel somewhat unfamiliar. You may already have had that feeling from Examples 4.1.4.

Given a subset $A \subseteq X$ and an element $x \in X$, we would like to be able to ask 'is $x \in A$?' For example, given $n \in \mathbb{N}$, the question 'is $n \in \{\text{primes}\}$?' should make sense.

However, with our current setup, this question barely makes sense (unless $A$ is $X$). By definition, $x$ is a function $\mathbf{1} \to X$, whereas '$x \in A$' means that $x$ is a function $\mathbf{1} \to A$. Since $X$ and $A$ are different, and every function comes with a specified codomain, it's inconceivable that both could be true.

The following definition provides the language we need.

**Definition 4.1.7** Let $X$ be a set, let $A \subseteq X$ with inclusion $i$, and let $x \in X$. If there exists $a \in A$ such that $i(a) = x$ then we write $x \in_X A$ and call $x$ an **$X$-element** of $A$.

Since $i$ is injective, the element $a$ in the definition is uniquely determined by $x$.

Strictly speaking, we should write $x \in_X (A \xrightarrow{i} X)$, because whether or not $x \in_X A$ depends on $i$ as well as $A$. But in practice, we almost always use the shorter notation.

**Example 4.1.8** This example is to explain the difference between the two kinds of membership, $\in$ and $\in_X$. In everyday mathematics, someone might write:

> Let $z \in \mathbb{C}$. If $z = \bar{z}$ then $z \in \mathbb{R}$.

Here '$z \in \mathbb{C}$' is a type declaration. In other words, the author is telling us that they're going to use $z$ to denote a complex number. It's not something that could be true or false. But once that declaration is made, '$z \in \mathbb{R}$' *is* a statement that's either true or false, for any given complex number $z$. In our notation, we would write:

> Let $z \in \mathbb{C}$. If $z = \bar{z}$ then $z \in_{\mathbb{C}} \mathbb{R}$.

Writing $i \colon \mathbb{R} \hookrightarrow \mathbb{C}$ for the inclusion of $\mathbb{R}$ into $\mathbb{C}$, the statement '$z \in_{\mathbb{C}} \mathbb{R}$' means there is some $x \in \mathbb{R}$ such that $z = i(x)$.

You might feel that this $i$ business is overly fussy. In that case, I'd remind you of the kind of inconsistency mentioned in Warning 1.1.2, and how the rigorous approach taken here is similar to that of some programming languages (Section 1.6). We use named inclusions such as $i$ when we want to be completely rigorous, even though most of the time we don't mention them because we humans 'know what we mean'.

**Examples 4.1.9** Here we follow Examples 4.1.4. Let $X$ be a set.

i. Consider $\varnothing \subseteq X$. There is no $x \in X$ such that $x \in_X \varnothing$, since this would mean that there is some $a \in \varnothing$ such that. . . , but there is no $a \in \varnothing$ at all.

ii. Consider $X \subseteq X$, or more formally, the injection $\mathrm{id}_X \colon X \to X$. Then $x \in_X X$ for all $x \in X$, since $x = \mathrm{id}_X(x)$.

iii. Let $x \in X$ and consider $\{x\} \hookrightarrow X$, recalling from Example 4.1.4(iii) that this just means $\mathbf{1} \xrightarrow{x} X$. Let $y \in X$. Working directly from the definition of $\in_X$, we have $y \in_X \{x\}$ if and only if $y = x$. This is exactly what the notation leads us to expect.

iv. Consider the diagonal $\Delta_X \colon X \to X \times X$. For which $(x, y) \in X \times X$ is it the case that $(x, y) \in_{X \times X} (X \xrightarrow{\Delta_X} X \times X)$? (Here we are using the fussier notation introduced after Definition 4.1.7.) By definition, it means that there is some $z \in X$ such that $(x, y) = \Delta_X(z)$, that is, $(x, y) = (z, z)$. So

$$(x, y) \in_{X \times X} \left(X \xrightarrow{\Delta_X} X \times X\right) \iff x = y.$$

**Exercise 4.1.10** In Example 4.1.9(iii), why is it true that $x \in_X \{y\}$ if and only if $x = y$?

Generally, for $A \subseteq X$, the elements of $A$ correspond one-to-one with the elements $x$ of $X$ such that $x \in_X A$. The correspondence works as follows. Given an element $a \in A$, we get an element $x = i(a)$ of $X$ (where $i$ is the inclusion), and then $x \in_X A$ by definition of $\in_X$. In the other direction, given an element $x \in X$ such that $x \in_X A$, there is a unique element $a \in A$ such that $x = i(a)$.

Because of this one-to-one correspondence, it is generally safe to drop the subscript and just write $\in$ instead of $\in_X$. This is one of those small notational liberties that is standard in everyday mathematical language, but which can't be taken in a careful axiomatic development (or some programming languages). For clarity, I will keep making the distinction between $\in$ and $\in_X$ for the rest of this chapter at least.

The next lemma describes the elements of fibres. They're what you think!

**Lemma 4.1.11** *Let $f\colon X \to Y$ be a function and $y \in Y$. Then for all $x \in X$,*

$$x \in_X f^{-1}(y) \iff f(x) = y.$$

**Proof** Write $i\colon f^{-1}(y) \hookrightarrow X$ for the inclusion. Let $x \in X$.

$\Longrightarrow$ : suppose that $x \in_X f^{-1}(y)$. Then $x = i(u)$ for some $u \in f^{-1}(y)$, and then $f(x) = f(i(u)) = y$ by definition of fibre (Definition 3.1.4).

$\Longleftarrow$ follows from Remark 3.1.5. □

An important special case expresses $\in_X$ in terms of characteristic functions:

**Lemma 4.1.12** *Let $X$ be a set and $A \subseteq X$. For $x \in X$,*

$$x \in_X A \iff \chi_A(x) = \mathsf{T}.$$

**Proof** This is Lemma 4.1.11 in the case where $f\colon X \to Y$ is $\chi_A\colon X \to \mathbf{2}$ and $y = \mathsf{T}$. Alternatively, it is just a restatement of Lemma 3.2.5. □

Just as there are two slightly different notions of element, $\in$ and $\in_X$, there are two slightly different notions of subset:

**Example 4.1.13** Consider the following piece of ordinary mathematical language:

Let $A \subseteq \mathbb{C}$. If $z = \bar{z}$ for all $z \in A$ then $A \subseteq \mathbb{R}$.

Here '$A \subseteq \mathbb{C}$' is a type declaration. The author is saying that they're going to use $A$ to denote a subset of $\mathbb{C}$. It's not something that could be true or false. But once that declaration is made, '$A \subseteq \mathbb{R}$' *is* a statement that's either true or false, for any given $A$. Both $A$ and $\mathbb{R}$ are subsets of $\mathbb{C}$ (with inclusion functions left nameless), and it either is or isn't the case that $A \subseteq \mathbb{R}$.

Generally, given subsets $A$ and $B$ of a set $X$ (or more formally, injections $A \xrightarrow{i} X$ and $B \xrightarrow{j} X$), we want to define what it means for $A$ to be contained in $B$. Here's our definition:

**Definition 4.1.14** Let $X$ be a set and $A, B \subseteq X$. We write $A \subseteq_X B$ if for all $x \in X$,

$$x \in_X A \implies x \in_X B.$$

**Example 4.1.15** In this notation, the text of Example 4.1.13 becomes:

Let $A \subseteq \mathbb{C}$. If $z = \bar{z}$ for all $z \in A$ then $A \subseteq_{\mathbb{C}} \mathbb{R}$.

It will be easier to give more examples once we have proved some basic results.

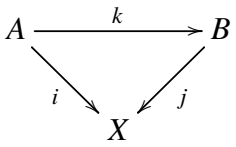
**Exercise 4.1.16** Show that if $A \subseteq_X B \subseteq_X C$ then $A \subseteq_X C$, and that if $A \cong_X B$ then $A \subseteq_X B$.

**Lemma 4.1.17** *Let $X$ be a set. Let $A \overset{i}{\hookrightarrow} X$ and $B \overset{j}{\hookrightarrow} X$ be subsets of $X$. The following are equivalent:*

*i.* $A \subseteq_X B$;

*ii.* $\chi_A(x) = \mathsf{T} \implies \chi_B(x) = \mathsf{T}$, *for* $x \in X$;

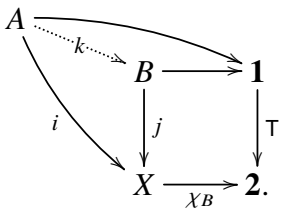
*iii. there exists a function* $k \colon A \to B$ *such that the triangle*




*commutes.*

**Proof** (i) $\iff$ (ii) follows from Lemma 4.1.12.

(ii) $\implies$ (iii): assume (ii), and consider the diagram




For each $a \in A$, we have $\chi_A(i(a)) = \mathsf{T}$, so $\chi_B(i(a)) = \mathsf{T}$ by (ii). Hence $\chi_B \circ i$ has constant value $\mathsf{T}$. Since $B \xrightarrow{j} X$ is the fibre of $\chi_B$ over $\mathsf{T}$, there is a unique function $k \colon A \to B$ such that $j \circ k = i$.

(iii) $\implies$ (i): take a function $k$ as in (iii). Let $x \in X$ such that $x \in_X A$. Then $x = i(a)$ for some $a \in A$; but $i = j \circ k$, so $x = j(k(a))$ with $k(a) \in B$. Hence $x \in_X B$. □

Think of the function $k$ of (iii) as the inclusion of $A$ into $B$. It is uniquely determined by $i$ and $j$; we showed this in the proof, and it also follows from this useful lemma:

**Lemma 4.1.18** *Let $j\colon B \to X$ be an injection, and let $k, k'\colon A \to B$ be functions such that $j \circ k = j \circ k'$. Then $k = k'$.*

**Proof** For all $a \in A$, we have $jk(a) = jk'(a)$, and $j$ is injective, so $k(a) = k'(a)$. Hence $k = k'$. □

**Exercise 4.1.19** When the equivalent conditions of Lemma 4.1.17 hold, prove that the function $k$ of (iii) is injective.

Two subsets should be the same if and only if each is contained in the other. The important next result says that this is true in our system.

**Proposition 4.1.20** *Let $X$ be a set and $A, B \subseteq X$. The following are equivalent:*

*i.* $A \cong_X B$;

*ii.* $\chi_A = \chi_B$;

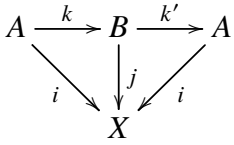
*iii.* $A \subseteq_X B$ *and* $B \subseteq_X A$;

*iv.* $x \in_X A \iff x \in_X B$, *for* $x \in X$.

**Proof** (i) $\iff$ (ii) is Lemma 3.2.16, and (iii) $\iff$ (iv) is by definition of $\subseteq_X$.

(ii) $\implies$ (iii) follows from Lemma 4.1.17.

(iii) $\implies$ (i): assuming (iii), Lemma 4.1.17 gives functions $A \underset{k'}{\overset{k}{\rightleftarrows}} B$ such that the diagram




commutes, where $i$ and $j$ are the inclusions of $A$ and $B$ into $X$. Now $i(k'k) = jk = i = i\mathrm{id}_A$, so by Lemma 4.1.18, $k'k = \mathrm{id}_A$. Similarly, $kk' = \mathrm{id}_B$. Hence $A \cong_X B$. □

**Examples 4.1.21** i. Let $X$ be a set, consider the subset $\varnothing$ of $X$ (Example 4.1.4(i)), and let $A \subseteq X$ be another subset.

First, $\varnothing \subseteq_X A$. By definition, this means that every $X$-element of $\varnothing$ is an $X$-element of $A$; but $\varnothing$ *has* no $X$-elements (Example 4.1.9(i)), so this is vacuously true.

When is $A \subseteq_X \varnothing$? If $A$ is empty then no element of $X$ is an $X$-element of $A$, so $A \subseteq_X \varnothing$ vacuously. Conversely, suppose that $A \subseteq_X \varnothing$. Since $\varnothing$ has no $X$-elements, $A$ cannot have any either, which implies that $A$ is empty. So $A \subseteq_X \varnothing$ if and only if $A$ is empty. And in that case, condition (iii) of Proposition 4.1.20 holds and $A \cong_X \varnothing$.

ii. Let $X$ be a set, consider the subset $X$ of $X$ (Example 4.1.4(ii)), and let $A \subseteq X$ be another subset.

First, $A \subseteq_X X$. By definition, this means that every element of $X$ that is an $X$-element of $A$ is an $X$-element of $X$. But *every* element of $X$ is an $X$-element of $X$ (Example 4.1.9(ii)), so this is trivially true.

When is $X \subseteq_X A$? Certainly this is true if $A \cong_X X$ (by Exercise 4.1.16). Conversely, suppose that $X \subseteq_X A$. Since also $A \subseteq_X X$, Proposition 4.1.20 implies that $A \cong_X X$. So $X \subseteq_X A$ if and only if $A \cong_X X$.

iii. Let $X$ be a set and $x \in X$. Consider the subset $\{x\}$ of $X$ (Example 4.1.4(iii)), and let $A \subseteq X$ be another subset.

When is $\{x\} \subseteq_X A$? In Example 4.1.9(iii), we showed that the one and only $X$-element of $\{x\}$ is $x$ itself. Hence $\{x\} \subseteq_X A$ if and only if $x \in_X A$.

When is $A \subseteq_X \{x\}$? By Example 4.1.9(iii) again, $A \subseteq_X \{x\}$ if and only if every $X$-element of $A$ is equal to $x$. In that case, there are two possibilities. The first is that $A$ has no $X$-elements, in which case $A$ is empty and $A \cong_X \varnothing$. The second is that the one and only $X$-element of $A$ is $x$. Then $A$ and $\{x\}$ have the same $X$-elements, so $A \cong_X \{x\}$ by Proposition 4.1.20. In conclusion, $A \subseteq_X \{x\}$ if and only if $A \cong_X \varnothing$ or $A \cong_X \{x\}$.

Of course, in everyday practice we don't write $\subseteq_X$: we just write $\subseteq$, erasing the distinction between the two notions of subset, as in Example 4.1.13.

**Warning 4.1.22** More riskily, we sometimes write $A = B$ to mean $A \cong_X B$.

When we do this, we're taking two liberties. First, we're not mentioning the names of the inclusions: really we should write $(A \xrightarrow{i} X) \cong_X (B \xrightarrow{j} X)$. (Example 3.2.13(ii) shows why.) Second, $A$ and $B$ aren't *equal as sets*. As I've emphasized, we never ask whether two sets are equal, only whether they're isomorphic.

So the risk is that someone might interpret '$A = B$' as meaning that the two sets are literally equal. In this course, you can be sure it won't mean that: it must be that $A$ and $B$ come equipped with inclusions

into some set $X$, and the meaning of '$A = B$' is that $A$ and $B$ represent the same subset of $X$. In other words, they satisfy the equivalent conditions of Proposition 4.1.20: $A \cong_X B$, or $\chi_A = \chi_B$, or $A$ and $B$ have the same $X$-elements.

## 4.2 Truth values

Back at the start of Section 3.2, we recalled that in ordinary mathematics, every subset $A$ of a set $X$ has a characteristic function $\chi_A \colon X \to \mathbf{2} = \{\mathsf{T}, \mathsf{F}\}$, given by

$$\chi_A(x) = \begin{cases} \mathsf{T} & \text{if } x \in A, \\ \mathsf{F} & \text{otherwise.} \end{cases} \tag{4.1}$$

We now know that '$x \in A$' should be interpreted as '$x \in_X A$'. Axiom 8 provides a set $\mathbf{2}$ with a specified element $\mathsf{T}$, and we showed in Lemma 4.1.12 that $\chi_A(x) = \mathsf{T} \iff x \in_X A$.

However, we have not proved equation (4.1) yet, or even defined an element of $\mathbf{2}$ called $\mathsf{F}$. And for all we know so far, $\mathbf{2}$ could have 17 elements, or infinitely many; or perhaps $\mathsf{T}$ is its only element. Our job now is to fill these gaps.

To show that $\mathbf{2}$ has exactly two elements, our strategy is as follows. The elements of $\mathbf{2}$ are the functions $\mathbf{1} \to \mathbf{2}$, which are the subsets of $\mathbf{1}$, which can be viewed as isomorphism classes of injections into $\mathbf{1}$. We'll prove that there are exactly two of these, namely, the isomorphism classes of $\mathbf{1} \xrightarrow{\mathrm{id}} \mathbf{1}$ and of $\varnothing \xrightarrow{!} \mathbf{1}$. The first has characteristic function $\mathsf{T} \colon \mathbf{1} \to \mathbf{2}$, by Proposition 3.2.18. As for the second:

**Definition 4.2.1** The element $\mathsf{F}$ of $\mathbf{2}$ (pronounced 'false') is $\chi_{\varnothing \to \mathbf{1}}$.

To see that this makes sense, note that the unique function $\varnothing \to \mathbf{1}$ is injective, and therefore has a characteristic function $\chi_{\varnothing \to \mathbf{1}} \colon \mathbf{1} \to \mathbf{2}$. This is then an element of $\mathbf{2}$, which we are calling $\mathsf{F}$.

**Theorem 4.2.2** *The subset classifier* $\mathbf{2}$ *has exactly two elements,* $\mathsf{T}$ *and* $\mathsf{F}$*. That is,* $\mathsf{T} \neq \mathsf{F}$*, and every element of* $\mathbf{2}$ *is equal to* $\mathsf{T}$ *or* $\mathsf{F}$*.*

**Proof** First, $\mathsf{T} \neq \mathsf{F}$. Indeed, if $\mathsf{T} = \mathsf{F}$ then the injections $\mathbf{1} \to \mathbf{1}$ and $\varnothing \to \mathbf{1}$ have the same characteristic function, so by Lemma 3.2.16, they are isomorphic over $\mathbf{1}$. Hence there is a function $\mathbf{1} \to \varnothing$, contradicting $\varnothing$ being empty.

Now let $\chi \in \mathbf{2}$. We show that $\chi = \mathsf{T}$ or $\chi = \mathsf{F}$. Viewing $\chi$ as a function $\mathbf{1} \to \mathbf{2}$, take the fibre $A = \chi^{-1}(\mathsf{T}) \overset{i}{\hookrightarrow} \mathbf{1}$. Then $\chi_A = \chi$.

If $A$ is empty then $A \cong_X \varnothing$ (Example 4.1.21(i)), so $\chi_A = \chi_\varnothing$ by Proposition 4.1.20. But $\chi_A = \chi$ and $\chi_\varnothing = \mathsf{F}$, so $\chi = \mathsf{F}$.

Now suppose that $A$ is nonempty, and take an element $a \in A$. Then $a$ must be the only element of $A$: for if $b \in A$ then $i(b) = i(a)$ (since $\mathbf{1}$ has only element), hence $b = a$ (since $i$ is injective). It follows that $i\colon A \to \mathbf{1}$ is bijective. Hence by Proposition 3.2.18, $\chi_A = \mathsf{T}$; that is, $\chi = \mathsf{T}$, completing the proof. □

The elements of $\mathbf{2}$ are called **truth values**.

**Corollary 4.2.3** *Let $X$ be a set, and let $A \subseteq X$. Then for $x \in X$,*

$$\chi_A(x) = \begin{cases} \mathsf{T} & \text{if } x \in_X A, \\ \mathsf{F} & \text{otherwise.} \end{cases}$$

**Proof** Follows from Lemma 4.1.12 and Theorem 4.2.2. □

**Examples 4.2.4** Let $X$ be a set.

i. $\chi_\varnothing(x) = \mathsf{F}$ for all $x \in X$, by Example 4.1.9(i).

ii. $\chi_X(x) = \mathsf{T}$ for all $x \in X$, by Example 4.1.9(ii).

iii. Let $x \in X$. Then for $y \in X$,

$$\chi_{\{x\}}(y) = \begin{cases} \mathsf{T} & \text{if } y = x, \\ \mathsf{F} & \text{otherwise,} \end{cases}$$

by Example 4.1.9(iii).

iv. Consider the diagonal function $\Delta_X\colon X \to X \times X$ (Example 4.1.9(iv)). Its characteristic function is denoted by $\delta_X\colon X \times X \to \mathbf{2}$, and satisfies

$$\delta_X(x, y) = \begin{cases} \mathsf{T} & \text{if } x = y, \\ \mathsf{F} & \text{otherwise} \end{cases}$$

$(x, y \in X)$. You could reasonably call $\delta_X$ the 'equality function' on $X$.

**Remark 4.2.5** Let $X$ be a set. The function $\delta_X\colon X \times X \to \mathbf{2}$ corresponds to a function $\overline{\delta_X}\colon X \to \mathbf{2}^X$, by definition of function set. Explicitly,

$$\big(\overline{\delta_X}(x)\big)(y) = \delta_X(x, y) = \chi_{\{x\}}(y)$$

for all $x, y \in X$, by Examples 4.2.4(iii) and (iv). Hence $\overline{\delta_X}(x) = \chi_{\{x\}}$ for each $x \in X$. Put another way, $\overline{\delta_X}$ is the function

$$\begin{array}{ccc} X & \to & \mathbf{2}^X = \mathscr{P}(X) \\ x & \mapsto & \{x\}. \end{array}$$

We therefore write $\overline{\delta_X}$ as $\{-\}$. Here the symbol '$-$' is a blank into which arguments can be inserted: applying the function $\{-\} = \overline{\delta_X}$ to $x$ gives $\{x\}$.

The point here is that although we'd previously constructed the subset $\{x\}$ of $X$ for each *individual* $x \in X$ (Example 4.1.4(iii)), we've now constructed the *function* $X \to \mathscr{P}(X)$ that takes $x$ as input and returns $\{x\}$ as output.

**Digression 4.2.6** When we showed that $\mathbf{2}$ had exactly two elements, $\mathsf{T}$ and $\mathsf{F}$, you might have wondered how it could possibly have been otherwise. What truth values could there ever be, apart from true or false? What kind of exotic logical system could that happen in?

In fact, there's a very commonplace situation where the truth values aren't just true and false: yes/no questions where the answer varies through space or time. Was it raining at noon on 1 October 2024? The answer depends on location. An answer of yes or no is meaningless without location, and a full answer to the question is not a yes or a no but a subset of the sphere, namely, the set of points on Earth where it was raining at that time. For such questions, the set of truth values is something like the power set of the sphere.

Systems of truth values like this appear in topos theory, a subject I've mentioned a couple of times previously, and which is well beyond this course. But we won't need to think about them here.

For the rest of this section, we will look at 'logical operators': ways of combining and modifying truth values, like *and* and *not*.

**Definition 4.2.7** The **negation operator** $\neg\colon \mathbf{2} \to \mathbf{2}$ is $\chi_{\{\mathsf{F}\}}$, the characteristic function of $\{\mathsf{F}\} \subseteq \mathbf{2}$.

We pronounce $\neg\alpha$ as 'not $\alpha$', for $\alpha \in \mathbf{2}$.

**Lemma 4.2.8** $\neg\mathsf{T} = \mathsf{F}$ *and* $\neg\mathsf{F} = \mathsf{T}$.

**Proof** Follows from Example 4.2.4(iii). □

**Lemma 4.2.9** $\neg \circ \neg = \mathrm{id}_{\mathbf{2}}$.

**Proof** By Lemma 4.2.8 and Theorem 4.2.2, $\neg\neg\alpha = \alpha$ for all $\alpha \in \mathbf{2}$. □

**Digression 4.2.10** Lemma 4.2.9 is called the **law of the excluded middle**. It corresponds to the idea that being not not true is the same as being true, which is the principle behind proof by contradiction. There are some logical systems where the law of the excluded middle does not hold. I won't give you any examples (try a web search if you're interested), but you can get an informal sense of it by contemplating the difference between 'I'm not unhappy' and 'I'm happy'.

Now we move on to logical operators with two arguments, beginning with *and*.

**Definition 4.2.11** The **conjunction operator** $\wedge\colon \mathbf{2}\times\mathbf{2}\to\mathbf{2}$ is $\chi_{\{(\mathsf{T},\mathsf{T})\}}$, the characteristic function of $\{(\mathsf{T},\mathsf{T})\}\subseteq\mathbf{2}\times\mathbf{2}$.

For $\alpha,\beta\in\mathbf{2}$, we write $\wedge(\alpha,\beta)$ as $\alpha\wedge\beta$ and pronounce it as '$\alpha$ and $\beta$'.

**Warning 4.2.12** Sometimes, people write $\wedge$ as an abbreviation for the word 'and', as in '$\{x\in\mathbb{R}: x\geq 0\wedge x\leq 1\}$'. To avoid confusion, don't do that in this course. Just write 'and'. For us, $\wedge$ is a certain function $\mathbf{2}\times\mathbf{2}\to\mathbf{2}$, and that's all. So $\alpha\wedge\beta$ is defined when $\alpha$ and $\beta$ are elements of $\mathbf{2}$, *not* when they're statements like '$x\geq 0$'.

**Lemma 4.2.13** *The conjunction operator has truth table*

| $\alpha$ | $\beta$ | $\alpha\wedge\beta$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | F |

*That is,* $\mathsf{T}\wedge\mathsf{T}=\mathsf{T}$, $\mathsf{T}\wedge\mathsf{F}=\mathsf{F}$, *etc.*

**Proof** Follows from Example 4.2.4(iii). □

**Remark 4.2.14** Suppose I make up a random truth table, say with two inputs (like the one above). Since a function is determined by its effect on elements, there's at most one function $\mathbf{2}\times\mathbf{2}\to\mathbf{2}$ with that as its truth table. But it's not obvious that there are any functions $\mathbf{2}\times\mathbf{2}\to\mathbf{2}$ *at all* with this truth table. It has to be deduced from the axioms.

There are $2^{2^2}=16$ truth tables with two inputs, and by the time you've got to the end of this section, you'll be able to prove that each one of them does arise from some function $\mathbf{2}\times\mathbf{2}\to\mathbf{2}$ (a long but fulfilling exercise). When we study the natural numbers in Chapter 7, we'll find a more systematic approach.

**Definition 4.2.15** The **disjunction operator** $\vee\colon \mathbf{2}\times\mathbf{2}\to\mathbf{2}$ is the composite function

$$\mathbf{2}\times\mathbf{2}\xrightarrow{\neg\times\neg}\mathbf{2}\times\mathbf{2}\xrightarrow{\wedge}\mathbf{2}\xrightarrow{\neg}\mathbf{2}.$$

We write $\vee(\alpha,\beta)$ as $\alpha\vee\beta$ and pronounce it as '$\alpha$ or $\beta$', for $\alpha,\beta\in\mathbf{2}$.

To understand Definition 4.2.15, first recall the '$f\times g$' notation from Lemma 2.6.13. Then the definition says that

$$\alpha\vee\beta=\neg((\neg\alpha)\wedge(\neg\beta))$$

$(\alpha,\beta\in\mathbf{2})$. Informally, for one thing or another to be true means they're not both false.

**Lemma 4.2.16** *The disjunction operator has truth table*

| $\alpha$ | $\beta$ | $\alpha\vee\beta$ |
|---|---|---|
| T | T | T |
| T | F | T |
| F | T | T |
| F | F | F |

**Proof** This follows from Lemmas 4.2.8 and 4.2.13. For example,

$$\mathsf{T}\vee\mathsf{F}=\neg((\neg\mathsf{T})\wedge(\neg\mathsf{F}))=\neg(\mathsf{F}\wedge\mathsf{T})=\neg\mathsf{F}=\mathsf{T}.$$ □

We could go on to define implication, double implication, etc., in terms of $\wedge$ and $\neg$, in a way that may be familiar to you from Proofs and Problem Solving. But instead, we look at something perhaps less familiar: conjunction and disjunction of potentially infinitely many truth values.

Let $I$ be any set (perhaps infinite, whatever that means). The set $\mathbf{2}^I$ can be understood in three slightly different ways: as the power set of $I$, as the set of functions $I\to\mathbf{2}$, or as the set of $I$-indexed families of truth values (Definition 2.7.8).

We will adopt the third perspective. So, we will write an element of $\mathbf{2}^I$ as a family $(\alpha_i)_{i\in I}$, with $\alpha_i\in\mathbf{2}$ for each $i\in I$. For instance, $(\mathsf{T})_{i\in I}\in\mathbf{2}^I$ is the family $(\alpha_i)_{i\in I}$ where $\alpha_i=\mathsf{T}$ for all $i$. It corresponds to the function $I\to\mathbf{2}$ with constant value T.

**Definition 4.2.17** For a set $I$, the **$I$-fold conjunction operator** $\bigwedge_I\colon\mathbf{2}^I\to\mathbf{2}$ is $\chi_{\{(\mathsf{T})_{i\in I}\}}$, the characteristic function of $\{(\mathsf{T})_{i\in I}\}\subseteq\mathbf{2}^I$.

For a family $(\alpha_i)_{i\in I}\in\mathbf{2}^I$, we write $\bigwedge_I\big((\alpha_i)_{i\in I}\big)$ as $\bigwedge_{i\in I}\alpha_i$.

**Lemma 4.2.18** *Let $I$ be a set and $(\alpha_i)_{i\in I}\in\mathbf{2}^I$. Then $\bigwedge_{i\in I}\alpha_i=\mathsf{T}$ if and only if $\alpha_i=\mathsf{T}$ for all $i\in I$.*

**Proof** By Example 4.2.4(iii), $\bigwedge_{i\in I} \alpha_i = \mathsf{T}$ if and only if $(\alpha_i)_{i\in I} = (\mathsf{T})_{i\in I}$. Since a function is determined by its effect on elements, and a family is just a function in different notation, this in turn is equivalent to $\alpha_i = \mathsf{T}$ for all $i \in I$. □

We derive $I$-fold disjunction from $I$-fold conjunction by the same procedure as when there were only two arguments (Definition 4.2.15): negate each input, take the conjunction, then negate the result.

**Definition 4.2.19** Let $I$ be a set. The ***I*-fold disjunction operator** $\bigvee_I \colon \mathbf{2}^I \to \mathbf{2}$ is the composite

$$\mathbf{2}^I \xrightarrow{\neg^I} \mathbf{2}^I \xrightarrow{\bigwedge_I} \mathbf{2} \xrightarrow{\neg} \mathbf{2}.$$

For the definition of $\neg^I$, see Lemma 2.7.10(i). The effect of this composite on a family $(\alpha_i)_{i\in I}$ of truth values is

$$(\alpha_i)_{i\in I} \mapsto (\neg\alpha_i)_{i\in I} \mapsto \bigwedge_{i\in I} \neg\alpha_i \mapsto \neg \bigwedge_{i\in I} \neg\alpha_i.$$

We write $\bigvee_I\big((\alpha_i)_{i\in I}\big)$ as $\bigvee_{i\in I} \alpha_i$. So,

$$\bigvee_{i\in I} \alpha_i = \neg \bigwedge_{i\in I} \neg\alpha_i. \tag{4.2}$$

**Lemma 4.2.20** *Let $I$ be a set and $(\alpha_i)_{i\in I} \in \mathbf{2}^I$. Then $\bigvee_{i\in I} \alpha_i = \mathsf{T}$ if and only if $\alpha_i = \mathsf{T}$ for some $i \in I$.*

**Proof** By equation (4.2), $\bigvee_{i\in I} \alpha_i = \mathsf{T}$ if and only if $\bigwedge_{i\in I} \neg\alpha_i = \mathsf{F}$. By Lemma 4.2.18, this is equivalent to $\neg\alpha_i = \mathsf{F}$ for some $i \in I$, which in turn is equivalent to $\alpha_i = \mathsf{T}$ for some $i \in I$. □

## 4.3 Operations on subsets

Let $X$ be a set. In ordinary mathematics, we can perform operations such as intersection, union and complement on subsets of $X$. But what does it actually mean to be able to take the union of $A$ and $B$, for example? It means there is a subset $C$ of $X$ such that for all $x \in X$,

$$x \in_X C \iff (x \in_X A \text{ or } x \in_X B).$$

By Proposition 4.1.20, there is at most one subset of $X$ with this property. The question now is whether any subset with this property exists at all.

In this section, we show that our axioms are indeed powerful enough to define intersections, unions and complements, and to prove that they all behave as you'd expect. The key idea is to use our results on logical operators from Section 4.2.

**Digression 4.3.1** We only ever take intersections and unions of *subsets* of some set $X$, and never intersections and unions of plain *sets*. It doesn't really make sense to ask what the intersection or union of two sets is, at least if you take an isomorphism-approach to mathematics.

As is often the case with these questions, it's clarifying to think about sets with structure. For instance, what happens if we ask for the intersection of the cyclic groups $C_2$ and $C_3$? If you write $C_2 = \{1, x\}$ and $C_3 = \{1, x, x^2\}$ then their intersection has two elements, but if you write $C_2 = \{1, x\}$ and $C_3 = \{1, y, y^2\}$ then it has one element. No reasonable question about groups depends on what the elements happen to be called, so this isn't a reasonable question. A similar argument can be made for unions.

The moral: we shouldn't (and won't) try to define the intersection or union of sets, only of subsets of the same set.

**Definition 4.3.2** Let $X$ be a set and $A, B \subseteq X$. Their **intersection** $A \cap B$ is the subset of $X$ whose characteristic function is the composite

$$X \xrightarrow{(\chi_A, \chi_B)} \mathbf{2} \times \mathbf{2} \xrightarrow{\wedge} \mathbf{2}.$$

I am now using subset language quite loosely. According to Definition 3.2.8, a subset of $X$ *is* a function $X \to \mathbf{2}$. But here I am viewing subsets of $X$ as injections into $X$ (taken up to isomorphism over $X$), as per the correspondence described in Remark 3.2.17. And I am not mentioning the names of the inclusion functions.

A more formal statement would go as follows. Take injections $A \overset{i}{\hookrightarrow} X$ and $B \overset{j}{\hookrightarrow} X$. Then $A \cap B \overset{k}{\hookrightarrow} X$ is the fibre over $\mathsf{T}$ of the composite $X \xrightarrow{(\chi_i, \chi_j)} \mathbf{2} \times \mathbf{2} \xrightarrow{\wedge} \mathbf{2}$. Equivalently, $\chi_k(x) = \chi_i(x) \wedge \chi_j(x)$ for all $x \in X$.

**Lemma 4.3.3** *Let $X$ be a set and $A, B \subseteq X$. Then for $x \in X$,*

$$x \in_X A \cap B \iff (x \in_X A \text{ and } x \in_X B).$$

**Proof** Let $x \in X$. Then

$$\begin{aligned} x \in_X A \cap B &\iff \chi_A(x) \wedge \chi_B(x) = \mathsf{T} && (4.3)\\ &\iff \chi_A(x) = \mathsf{T} \text{ and } \chi_B(x) = \mathsf{T} && (4.4)\\ &\iff x \in_X A \text{ and } x \in_X B, && (4.5) \end{aligned}$$

using the definition of $A \cap B$ and Lemma 4.1.12 in (4.3), Lemma 4.2.13 in (4.4), then Lemma 4.1.12 again in (4.5). □

The definition of union is very similar.

**Definition 4.3.4** Let $X$ be a set and $A, B \subseteq X$. Their **union** $A \cup B$ is the subset of $X$ whose characteristic function is the composite

$$X \xrightarrow{(\chi_A, \chi_B)} \mathbf{2} \times \mathbf{2} \xrightarrow{\vee} \mathbf{2}.$$

**Lemma 4.3.5** *Let $X$ be a set and $A, B \subseteq X$. Then for $x \in X$,*

$$x \in_X A \cup B \iff (x \in_X A \text{ or } x \in_X B).$$

**Proof** The same as the proof of Lemma 4.3.3, but using Lemma 4.2.16 instead of Lemma 4.2.13. □

For complements, we first consider only complements in $X$ itself.

**Definition 4.3.6** Let $X$ be a set and $A \subseteq X$. Its **complement** $X \setminus A$ is the subset of $X$ whose characteristic function is the composite

$$X \xrightarrow{\chi_A} \mathbf{2} \xrightarrow{\neg} \mathbf{2}.$$

**Lemma 4.3.7** *Let $X$ be a set and $A \subseteq X$. Then for $x \in X$,*

$$x \in_X X \setminus A \iff x \notin_X A.$$

**Proof** Again, this is similar and left as an exercise. □

**Exercise 4.3.8** Prove Lemma 4.3.7, imitating the proof of Lemma 4.3.3 if you like.

Next we record the basic algebraic properties of these subset operations. From here on, I will often take the notational liberty described in Warning 4.1.22, writing $A = B$ to mean $A \cong_X B$.

**Lemma 4.3.9** *Let $X$ be a set and $A, B, C \subseteq X$. Then the following laws hold.*

*i. Intersection laws:*

*(a)* $A \cap B = B \cap A$;

*(b)* $(A \cap B) \cap C = A \cap (B \cap C)$;

*(c)* $A \cap X = A$;

*(d)* $A \cap A = A$.

*ii. Union laws:*

(a) $A \cup B = B \cup A$;

(b) $(A \cup B) \cup C = A \cup (B \cup C)$;

(c) $A \cup \varnothing = A$;

(d) $A \cup A = A$.

iii. *Distributivity laws:*

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;

(b) $A \cap \varnothing = \varnothing$;

(c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

(d) $A \cup X = X$.

iv. *De Morgan laws:*

(a) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$;

(b) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

v. *Complement laws:*

(a) $A \cup (X \setminus A) = X$;

(b) $A \cap (X \setminus A) = \varnothing$;

(c) $X \setminus (X \setminus A) = A$.

**Proof** These all follow from Lemmas 4.3.3, 4.3.5 and 4.3.7, using the fact that two subsets are equal if and only if they have the same $X$-elements (Proposition 4.1.20).

For instance, let's prove (iiia). By Proposition 4.1.20, it is enough to prove that for all $x \in X$,

$$x \in_X A \cap (B \cup C) \iff x \in_X (A \cap B) \cup (A \cap C).$$

Suppose that $x \in_X A \cap (B \cup C)$. By Lemma 4.3.3, $x \in_X A$ and $x \in_X B \cup C$. Then by Lemma 4.3.5, $x \in_X B$ or $x \in_X C$. If $x \in_X B$ then, since also $x \in_X A$, we have $x \in_X A \cap B$ by Lemma 4.3.3 again. If $x \in_X C$ then, similarly, $x \in_X A \cap C$. Since one of the two holds, $x \in_X (A \cap B) \cup (A \cap C)$ by Lemma 4.3.5. This proves one implication, and the converse is similar. □

In short, all these identities are proved by exactly the kind of argument you've been familiar with for years.

**Exercise 4.3.10** Choose one or two other parts of Lemma 4.3.9 and prove them.

For completeness, we also define relative complements.

**Definition 4.3.11** Let $X$ be a set and $A, B \subseteq X$. The **relative complement** $B \setminus A$ is $B \cap (X \setminus A)$.

**Lemma 4.3.12** *Let $X$ be a set and $A, B \subseteq X$. Then for $x \in X$,*

$$x \in_X B \setminus A \iff x \in_X B \text{ and } x \notin_X A.$$

**Proof** Follows from Lemmas 4.3.3 and 4.3.7. □

Finally, what about intersections and unions of more than two subsets? Take a set $I$. Then an element of $\mathscr{P}(X)^I$ can be seen as an $I$-indexed family of subsets of $X$, say $(A_i)_{i\in I}$, and we want to define $\bigcap_{i\in I} A_i$ and $\bigcup_{i\in I} A_i$. Now,

$$\mathscr{P}(X)^I = (\mathbf{2}^X)^I \cong \mathbf{2}^{I\times X} \cong \mathbf{2}^{X\times I} \cong (\mathbf{2}^I)^X,$$

using Propositions 2.7.12 and 2.6.15. Under the composite isomorphism $\mathscr{P}(X)^I \cong (\mathbf{2}^I)^X$, the family $(A_i)_{i\in I} \in \mathscr{P}(X)^I$ corresponds to the function

$$\begin{array}{ccc} X & \to & \mathbf{2}^I \\ x & \mapsto & (\chi_{A_i}(x))_{i\in I}. \end{array}$$

In the following definition, I will write this function as $(\chi_{A_i})_{i\in I}$.

**Definition 4.3.13** Let $X$ and $I$ be sets, and let $(A_i)_{i\in I} \in \mathscr{P}(X)^I$ be an $I$-indexed family of subsets of $X$.

i. The **intersection** $\bigcap_{i\in I} A_i$ is the subset of $X$ whose characteristic function is the composite
$$X \xrightarrow{(\chi_{A_i})_{i\in I}} \mathbf{2}^I \xrightarrow{\bigwedge_I} \mathbf{2}.$$

ii. The **union** $\bigcup_{i\in I} A_i$ is the subset of $X$ whose characteristic function is the composite
$$X \xrightarrow{(\chi_{A_i})_{i\in I}} \mathbf{2}^I \xrightarrow{\bigvee_I} \mathbf{2}.$$

These definitions do what they're supposed to:

**Lemma 4.3.14** *Let $X$ and $I$ be sets, and let $(A_i)_{i\in I} \in \mathscr{P}(X)^I$ be an $I$-indexed family of subsets of $X$. Then for $x \in X$,*

*i.* $x \in_X \bigcap_{i\in I} A_i \iff x \in_X A_i$ *for all* $i \in I$*;*

*ii.* $x \in_X \bigcup_{i\in I} A_i \iff x \in_X A_i$ *for some* $i \in I$*.*

**Proof** For (i),

$$x \in_X \bigcap_{i\in I} A_i \iff \bigwedge_{i\in I} \chi_{A_i}(x) = \mathsf{T} \tag{4.6}$$

$$\iff \chi_{A_i}(x) = \mathsf{T} \text{ for all } i \in I \tag{4.7}$$

$$\iff x \in_X A_i \text{ for all } i \in I, \tag{4.8}$$

using the definition of $\bigcap_{i\in I} A_i$ and Lemma 4.1.12 in (4.6), Lemma 4.2.18 in (4.7), then Lemma 4.1.12 again in (4.8). Part (ii) is similar. □

## 4.4 Images and preimages

In our axiomatization, we didn't explicitly assume the existence of images or preimages, except in the special case of fibres (preimages of singletons). We now show that the axioms do in fact imply the existence of all images and preimages, and that they have all the properties we'd expect. We also prove some properties that you might not be so familiar with.

**Warning 4.4.1** Given a function $f\colon X \to Y$, the image of $A \subseteq X$ under $f$ is usually written as $fA$, and the preimage of $B \subseteq Y$ under $f$ is usually written as $f^{-1}B$. However, this can lead to confusion, as per Warning 3.1.1. So in this section, while we are carefully laying the groundwork, I will use the alternative notation $f_*A$ for $fA$ and $f^*B$ for $f^{-1}B$.

We begin with images. Let $f\colon X \to Y$ be a function and $A \subseteq X$ with inclusion $i$. How are we going to construct the image $f_*A$? The idea is to use unions. An element of $Y$ should belong to $f_*A$ if there is some $a \in A$ such that $y = fi(a)$. So, we should be able to construct the image as $\bigcup_{a\in A}\{fi(a)\}$.

To make this precise, consider the composite function

$$A \overset{i}{\hookrightarrow} X \overset{f}{\to} Y \overset{\{-\}}{\longrightarrow} \mathscr{P}(Y).$$

The last function here is $y \mapsto \{y\}$, constructed in Remark 4.2.5. The effect on an element $a \in A$ of this string of functions is

$$a \mapsto i(a) \mapsto fi(a) \mapsto \{fi(a)\}.$$

Seen as an $A$-indexed family, our composite function $A \to \mathscr{P}(Y)$ is $\big(\{fi(a)\}\big)_{a\in A}$, and the **image of $A$ under $f$** is defined to be

$$f_*A = \bigcup_{a\in A}\{fi(a)\} \subseteq Y.$$

We now check that this definition does what it's supposed to.

**Lemma 4.4.2** *Let $f\colon X \to Y$ be a function and $A \subseteq X$. Then for $y \in Y$,*

$$y \in_Y f_*A \iff y = f(x) \text{ for some } x \in X \text{ such that } x \in_X A.$$

**Proof** By Lemma 4.3.14(ii) and the definition of image, $y \in_Y f_*A$ if and only if $y \in_Y \{fi(a)\}$ for some $a \in A$. By Example 4.1.9(iii), this holds if and only if $y = fi(a)$ for some $a \in A$. And by definition of $\in_X$, this holds if and only if $y = f(x)$ for some $x \in X$ such that $x \in_X A$. □

**Examples 4.4.3** Let $f\colon X \to Y$ be a function.

i. The image under $f$ of the empty set is empty: $f_*\varnothing = \varnothing$. Indeed, there is no $x \in X$ such that $x \in_X \varnothing$, so by Lemma 4.4.2, there is no $y \in Y$ such that $y \in_Y f_*\varnothing$. Hence $f_*\varnothing$ is empty.

ii. Consider the subset $X$ of $X$. Its image $f_*X \subseteq Y$ has the property that for $y \in Y$,
$$y \in_Y f_*X \iff y = f(x) \text{ for some } x \in X.$$
We call $f_*X$ the **image of $f$** and write it as $\operatorname{im} f$.

What is the image of a union or an intersection?

**Lemma 4.4.4** *Let $f\colon X \to Y$ be a function, let $I$ be a set, and let $(A_i)_{i\in I}$ be a family of subsets of $X$. Then*

$$f_*\Big(\bigcup_{i\in I} A_i\Big) = \bigcup_{i\in I} f_*A_i, \qquad f_*\Big(\bigcap_{i\in I} A_i\Big) \subseteq \bigcap_{i\in I} f_*A_i.$$

**Proof** For the first equation, let $y \in Y$. Then

$$\begin{aligned}
y \in_Y f_*\Big(\bigcup_{i\in I} A_i\Big) &\iff y = f(x) \text{ for some } x \in X \text{ such that } x \in_X \bigcup_{i\in I} A_i && (4.9)\\
&\iff y = f(x) \text{ for some } x \in X \text{ and } j \in I \text{ such that } x \in_X A_j && (4.10)\\
&\iff y \in f_*A_j \text{ for some } j \in I && (4.11)\\
&\iff y \in \bigcup_{i\in I} f_*A_i, && (4.12)
\end{aligned}$$

where (4.9) and (4.11) follow from Lemma 4.4.2, and (4.10) and (4.12) from Lemma 4.3.14(ii).

The second statement is similar and left as an exercise. □

**Warning 4.4.5** The second statement is an inclusion only! It is not an equality in general. You can find a counterexample where all the sets involved have two or fewer elements, or you can peek at the solution to Workshop 1, question 5.

Now we turn to preimages. Take a function $f\colon X \to Y$ and a subset $B \subseteq Y$. The key to constructing the preimage $f^{-1}B$ (or $f^*B$, as we'll call it) is the result of the following exercise.

**Exercise 4.4.6** Forgetting the axioms for the moment and using what you know about sets, show that $\chi_{f^{-1}B} = \chi_B \circ f$.

Inspired by this, we define the **preimage of $B$ under $f$** to be the subset $f^*B$ of $X$ whose characteristic function is the composite

$$X \xrightarrow{f} Y \xrightarrow{\chi_B} \mathbf{2}.$$

This definition does what it should:

**Lemma 4.4.7** *Let $f\colon X \to Y$ be a function and $B \subseteq Y$. Then for $x \in X$,*

$$x \in_X f^*B \iff f(x) \in_Y B.$$

**Proof** We have

$$x \in_X f^*B \iff \chi_{f^*B}(x) = \mathsf{T} \iff \chi_B(f(x)) = \mathsf{T} \iff f(x) \in_Y B,$$

where the middle equivalence is by definition of $f^*B$ and the others are by Lemma 4.1.12. □

**Examples 4.4.8** Let $f\colon X \to Y$ be a function.

i. Consider $\varnothing \subseteq Y$. There is no $x \in X$ such that $f(x) \in_Y \varnothing$, so by Lemma 4.4.7, there is no $x \in X$ such that $x \in_X f^*\varnothing$. Hence $f^*\varnothing = \varnothing$.

ii. Consider $Y \subseteq Y$. All $x \in X$ satisfy $f(x) \in_Y Y$, so by Lemma 4.4.7, all $x \in X$ satisfy $x \in_X f^*Y$. Hence $f^*Y = X$.

iii. Take an element $y \in Y$ and consider $\{y\} \subseteq Y$. For $x \in X$, we have $f(x) \in_Y \{y\}$ if and only if $f(x) = y$, by Example 4.1.9(iii). Hence by Lemma 4.4.7, $x \in_X f^*\{y\}$ if and only if $f(x) = y$.

On the other hand, Lemma 4.1.11 on fibres states that $x \in_X f^{-1}(y)$ if and only if $f(x) = y$. Subsets of $X$ with the same $X$-elements are the same (Proposition 4.1.20), so $f^*\{y\} = f^{-1}(y)$. This confirms that fibres really are preimages of singletons.

Preimages are sometimes easier to work with than images, because they preserve both unions *and* intersections. (Recall Warning 4.4.5.)

**Lemma 4.4.9** *Let $f\colon X \to Y$ be a function, let $I$ be a set, and let $(B_i)_{i\in I}$ be a family of subsets of $Y$. Then*

$$f^*\Big(\bigcup_{i\in I} B_i\Big) = \bigcup_{i\in I} f^* B_i, \qquad f^*\Big(\bigcap_{i\in I} B_i\Big) = \bigcap_{i\in I} f^* B_i.$$

**Proof** As for Lemma 4.4.4, we can use the same kind of elementwise reasoning that you know well. I will prove the second equation and leave the first as an exercise. Let $x \in X$. Then

$$\begin{aligned}
x \in_X f^*\Big(\bigcap_{i\in I} B_i\Big) &\iff f(x) \in_Y \bigcap_{i\in I} B_i && (4.13)\\
&\iff f(x) \in_Y B_i \text{ for all } i \in I && (4.14)\\
&\iff x \in_X f^* B_i \text{ for all } i \in I && (4.15)\\
&\iff x \in_X \bigcap_{i\in I} f^* B_i, && (4.16)
\end{aligned}$$

where (4.13) and (4.15) follow from Lemma 4.4.7, and (4.14) and (4.16) from Lemma 4.3.14(i). The result follows. □

Finally, we look at the interaction between images and preimages.

**Lemma 4.4.10** *Let $f\colon X \to Y$ be an* invertible *function and $B \subseteq Y$. Then $(f^{-1})_* B = f^* B$.*

**Proof** For $x \in X$,

$$\begin{aligned}
x \in (f^{-1})_* B &\iff x = f^{-1}(y) \text{ for some } y \in Y \text{ such that } y \in_Y B && (4.17)\\
&\iff f(x) \in_Y B && (4.18)\\
&\iff x \in_X f^* B, && (4.19)
\end{aligned}$$

where (4.17) is by Lemma 4.4.2, (4.18) follows by applying $f$ to each side of the equation $x = f^{-1}(y)$, and (4.19) is by Lemma 4.4.7. □

**Remark 4.4.11** The point of Lemma 4.4.10 is that if we use the standard notation of $fA$ and $f^{-1}B$ for image and preimage, then when $f$ is invertible, the expression '$f^{-1}B$' appears to be ambiguous: does it mean $(f^{-1})_*B$ or $f^*B$? But the lemma shows that there's no ambiguity after all.

The next result is the fundamental relation between images and preimages.

**Lemma 4.4.12** *Let $f\colon X \to Y$ be a function, let $A \subseteq X$, and let $B \subseteq Y$. Then*

$$f_*A \subseteq_Y B \iff A \subseteq_X f^*B.$$

**Proof** Both sides are equivalent to the statement that $f(x) \in_Y B$ for all $x \in X$ such that $x \in_X A$, by Lemmas 4.4.2 and 4.4.7. □

**Lemma 4.4.13** *Let $f\colon X \to Y$. Then $A \subseteq_X f^*f_*A$ for all $A \subseteq X$, and $f_*f^*B \subseteq_Y B$ for all $B \subseteq Y$.*

**Proof** Both statements follow from Lemma 4.4.12, the first by taking $B = f_*A$ and the second by taking $A = f^*B$. □

Workshop 1, question 4 invites you to find examples showing that these inclusions are not in general equalities.

Now that we have carefully established the properties of images $f_*A$ and preimages $f^*B$, we will relax and switch to the standard notation, $fA$ and $f^{-1}B$.

**Warning 4.4.14** In the standard notation, Lemma 4.4.13 says that $A \subseteq_X f^{-1}fA$ and $ff^{-1}B \subseteq_Y B$. But as just noted, equality does not always hold—another way in which the standard notation is treacherous.

# Chapter 5

# Relations

*To read by Monday 14 October: Sections 5.1–5.3.*
*To read by Friday 18 October: Sections 5.4 and 5.5.*

Every mathematician wants to be able to define a subset of a set $X$ by just writing down an expression like $\{x \in X : \text{some property of } x \text{ holds}\}$, and to define a function $f : Y \to Z$ by just writing down a formula for $f(y)$ $(y \in Y)$. So far, we haven't shown that these are valid methods: that there really *is* a subset consisting of the elements satisfying a given property, or a function that satisfies a given formula.

This week, our major feat will be to show that it's possible. The key to achieving it is the concept of relation.

## 5.1 Definitions and examples of relations

The concept of relation is best explained by an example.

**Example 5.1.1** For any real number $x$ and natural number $n$, we can ask whether $x$ has a real $n$th root.

The statement '$x$ has a real $n$th root' is true for some pairs $(x, n) \in \mathbb{R} \times \mathbb{N}$ and false for others. So it gives us a function $\rho : \mathbb{R} \times \mathbb{N} \to \mathbf{2}$, where $\rho(x, n)$ is $\mathsf{T}$ if $x$ has a real $n$th root and $\mathsf{F}$ otherwise. The function $\rho$ encapsulates all the information on which pairs the condition holds for and which it doesn't.

Alternatively, the information on which roots exist is encapsulated by the set $R$ of pairs $(x, n)$ such that $x$ has a real $n$th root, together with its inclusion function $R \hookrightarrow \mathbb{R} \times \mathbb{N}$.

So we have two different ways of looking at our condition: as a function $\rho : \mathbb{R} \times \mathbb{N} \to \mathbf{2}$, or as a set $R$ together with an injection $R \hookrightarrow \mathbb{R} \times \mathbb{N}$. These two

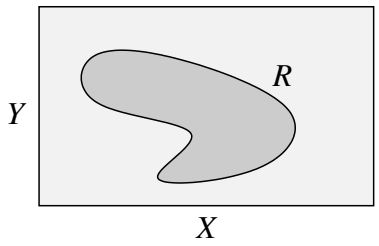



Figure 5.1: A relation $R$ between sets $X$ and $Y$.

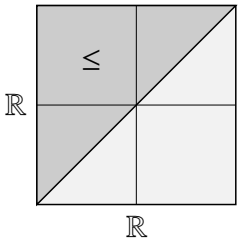



Figure 5.2: The relation $\leq$ on $\mathbb{R}$.

perspectives are equivalent, and they both say that we have a subset of $\mathbb{R} \times \mathbb{N}$. They're the two equivalent perspectives on subsets introduced in Section 3.2.

Inspired by this example, we make the following definition (Figure 5.1).

**Definition 5.1.2** Let $X$ and $Y$ be sets. A **relation between $X$ and $Y$** is a subset of $X \times Y$. When $X = Y$, we call it a **relation on $X$**.

Let $R$ be a relation between $X$ and $Y$. Given $x \in X$ and $y \in Y$, we often write $xRy$ to mean $(x, y) \in_{X \times Y} R$.

**Examples 5.1.3**

i. The usual relation $\leq$ on $\mathbb{R}$ is, formally, the subset of $\mathbb{R} \times \mathbb{R}$ consisting of all pairs $(x, y)$ such that $x \leq y$ (Figure 5.2). In other words, $\leq$ *is* the subset $\{(x, y) : x \leq y\}$ of $\mathbb{R} \times \mathbb{R}$ (using curly bracket notation that we haven't defined yet). Of course, no one writes '$(x, y) \in_{\mathbb{R} \times \mathbb{R}} \leq$' or even '$(x, y) \in \leq$'; we write '$x \leq y$'. This is a familiar example of the $xRy$ notation.

ii. Let $X$ be a set. The diagonal subset $\Delta_X \colon X \hookrightarrow X \times X$ can be seen as a relation on $X$, which we call $\Delta_X$. (Relations are normally named after the *domain* of the inclusion, but in this case we name it after the inclusion itself.) As we saw in Example 4.1.9(iv), for $x, y \in X$,

$$(x, y) \in_{X \times X} \left(X \overset{\Delta_X}{\hookrightarrow} X \times X\right) \iff x = y.$$

That is, $x\Delta_X y \iff x = y$. We call $\Delta_X$ the **equality relation** or **identity relation** on $X$.

iii. Let $X$ and $Y$ be sets. Then the subset $X \times Y$ of itself is a trivial example of a relation $R$ between $X$ and $Y$. It satisfies $xRy$ for *all* $x \in X$ and $y \in Y$.

iv. More generally, let $X$ and $Y$ be sets, let $A \subseteq X$, and let $B \subseteq Y$. Then we obtain a subset $A \times B$ of $X \times Y$, by Exercise 5.1.4 below. Viewing this subset as a relation $R$ between $X$ and $Y$, we have $xRy$ if and only if $x \in_X A$ and $y \in_Y B$.

v. Let $X$ be a set, and consider the evaluation function

$$\begin{array}{rccc} \mathrm{ev} = \mathrm{ev}_{X,\mathbf{2}}\colon & \mathbf{2}^X \times X & \to & \mathbf{2} \\ & (\chi, x) & \mapsto & \chi(x). \end{array}$$

Then ev is (the characteristic function of) a subset of $\mathbf{2}^X \times X$; that is, it is a relation between $\mathbf{2}^X$ and $X$.

What *is* this relation? By definition, $\mathbf{2}^X$ is the power set $\mathscr{P}(X)$ of $X$, whose elements can be viewed as injections into $X$ taken up to isomorphism over $X$. Given an injection $A \hookrightarrow X$, we have $\chi_A(x) = \mathsf{T} \iff x \in_X A$, by Lemma 4.1.12. Thus, the subset $R$ of $\mathscr{P}(X) \times X$ with characteristic function ev satisfies

$$ARx \iff x \in_X A$$

$(A \in \mathscr{P}(X), x \in X)$. We write $R$ as $\ni_X$, so that $A \ni_X x \iff x \in_X A$.

vi. Define the **implication** operator $\rightarrowtriangle\colon \mathbf{2} \times \mathbf{2} \to \mathbf{2}$ to be the composite

$$\mathbf{2} \times \mathbf{2} \xrightarrow{\neg \times \mathrm{id}} \mathbf{2} \times \mathbf{2} \xrightarrow{\vee} \mathbf{2},$$

and for $\alpha, \beta \in \mathbf{2}$, write $\rightarrowtriangle(\alpha, \beta)$ as $\alpha \rightarrowtriangle \beta$. Then $\alpha \rightarrowtriangle \beta = \neg\alpha \vee \beta$ for all $\alpha, \beta \in \mathbf{2}$, and $\rightarrowtriangle$ has truth table

| $\alpha$ | $\beta$ | $\alpha \rightarrowtriangle \beta$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

(I use the arrow style $\rightarrowtriangle$ to distinguish it from the arrow $\to$ for functions and the ordinary implication symbol $\Rightarrow$. Compare Warning 4.2.12.)

Since $\twoheadrightarrow$ is a function $\mathbf{2}\times\mathbf{2}\to\mathbf{2}$, it can be regarded as a subset of $\mathbf{2}\times\mathbf{2}$. The corresponding injection into $\mathbf{2}\times\mathbf{2}$ will be denoted by $\leq \hookrightarrow \mathbf{2}\times\mathbf{2}$. Thus, $\leq$ is a relation on $\mathbf{2}$, and for $\alpha,\beta\in\mathbf{2}$,

$$\begin{aligned}\alpha\leq\beta &\iff (\alpha\twoheadrightarrow\beta)=\mathsf{T}\\ &\iff \alpha=\beta \text{ or } (\alpha,\beta)=(\mathsf{F},\mathsf{T})\\ &\iff (\alpha,\beta)\neq(\mathsf{T},\mathsf{F}).\end{aligned}$$

Sometimes people write 0 instead of $\mathsf{F}$ and 1 instead of $\mathsf{T}$, in which case the relation $\leq$ on $\mathbf{2}$ does what you would guess.

vii. Let $X$ be a set. We show that there exists a relation $R$ on $\mathscr{P}(X)=\mathbf{2}^X$ such that

$$ARB \iff A\subseteq_X B$$

for all $A,B\subseteq X$. Naturally, we write $R$ as $\subseteq_X$.

To construct $R$, first note that by Lemma 4.1.17, $A\subseteq_X B$ if and only if $(\chi_A(x)\twoheadrightarrow\chi_B(x))=\mathsf{T}$ for all $x\in X$. Now consider the composite function

$$\rho=\Big(\mathbf{2}^X\times\mathbf{2}^X\cong(\mathbf{2}\times\mathbf{2})^X\xrightarrow{\twoheadrightarrow^X}\mathbf{2}^X\xrightarrow{\bigwedge_X}\mathbf{2}\Big),$$

where the isomorphism is from Proposition 2.7.12(i), the function $\twoheadrightarrow^X$ is constructed from $\twoheadrightarrow$ as in Lemma 2.7.10(i), and $\bigwedge_X$ is the $X$-fold conjunction operator (Definition 4.2.17). For $A,B\subseteq X$, the element $(\chi_A,\chi_B)$ of $\mathbf{2}^X\times\mathbf{2}^X$ corresponds to the family $\big((\chi_A(x),\chi_B(x))\big)_{x\in X}\in(\mathbf{2}\times\mathbf{2})^X$, and so

$$\rho(\chi_A,\chi_B)=\bigwedge_{x\in X}\big(\chi_A(x)\twoheadrightarrow\chi_B(x)\big).$$

It follows that $\rho(\chi_A,\chi_B)=\mathsf{T}$ if and only if $A\subseteq_X B$ (using Lemma 4.2.18). Hence the subset $R$ of $\mathscr{P}(X)\times\mathscr{P}(X)$ with characteristic function $\rho$ has the property we seek: $ARB$ if and only if $A\subseteq_X B$.

viii. Given sets and functions

$$X\xrightarrow{f}Z\xleftarrow{g}Y,$$

there is a relation $R$ between $X$ and $Y$ satisfying

$$xRy \iff f(x)=g(y)$$

$(x\in X, y\in Y)$. Indeed, take $R\hookrightarrow X\times Y$ to be the preimage of $Z\xhookrightarrow{\Delta_Z}Z\times Z$ under $X\times Y\xrightarrow{f\times g}Z\times Z$. Then for $(x,y)\in X\times Y$,

$$\begin{aligned}xRy &\iff (x,y)\in_{X\times Y}R\\ &\iff (f\times g)(x,y)\in_{Z\times Z}\big(Z\xhookrightarrow{\Delta_Z}Z\times Z\big)\\ &\iff f(x)=g(y),\end{aligned}$$

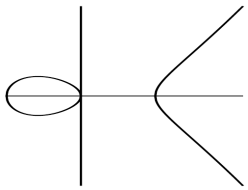


Figure 5.3: The curve $x(x^2 - 1) = y^2$. (Figure from Milne, *Elliptic Curves*, p. 1.)

where the first step is by definition of $xRy$, the second is by the fundamental property of preimages (Lemma 4.4.7), and the last is by definition of $f \times g$ and Example 4.1.9(iv).

The set $R$ is called the **pullback** of $f$ and $g$, and we will meet it again later. There are many familiar examples of pullbacks. For instance, let $X = Y = Z = \mathbb{R}$, and let $f$ and $g$ be the functions given by $f(x) = x(x^2 - 1)$ and $g(y) = y^2$. Then $R$ is the set of pairs $(x, y)$ such that $x(x^2 - 1) = y^2$ (a so-called 'elliptic curve'; Figure 5.3). This is not the graph of a function $\mathbb{R} \to \mathbb{R}$, because some $x$-values are related to more than one $y$-value and some are related to none.

**Exercise 5.1.4** Let $A \xrightarrow{i} X$ and $B \xrightarrow{j} Y$ be injective functions. Prove that $A \times B \xrightarrow{i \times j} X \times Y$ is injective.

**Warning 5.1.5** Relations between $X$ and $Y$ are subsets of $X \times Y$, and can therefore be seen as injections into $X \times Y$, with two such injections regarded as the same if they are isomorphic over $X \times Y$. The official notation for this is $\cong_{X \times Y}$, but instead, I will just write $=$. As noted in Warning 4.1.22, this is slightly risky; go back and read that warning if you're in any doubt.

Relations can be turned around. Given a relation $R$ between sets $X$ and $Y$, we can reverse the order of the arguments using the isomorphism

$$\begin{array}{rccc} \sigma\colon & X \times Y & \to & Y \times X \\ & (x, y) & \mapsto & (y, x) \end{array}$$

that you found in Assignment 1. The composite

$$R \hookrightarrow X \times Y \xrightarrow{\sigma} Y \times X$$

is also an injection, so it gives a subset of $Y \times X$. We write this subset of $Y \times X$ as $R^{\mathrm{op}}$ and call it the **opposite** of $R$. (Other names are **converse** and **inverse**.) So $R^{\mathrm{op}}$ is a relation from $Y$ to $X$, and

$$yR^{\mathrm{op}}x \iff xRy$$

$(y \in Y, x \in X)$.

**Remark 5.1.6** As a mere *set*, $R^{\mathrm{op}}$ is the same as $R$. But these are *subsets* (of $Y \times X$ and $X \times Y$ respectively), and we are abusing language by not mentioning the inclusions. If the inclusion of $R$ into $X \times Y$ is called $i$ then the inclusion of $R^{\mathrm{op}}$ into $Y \times X$ is $\sigma \circ i$.

**Examples 5.1.7** i. The opposite of the relation $\leq$ on $\mathbb{R}$ (Example 5.1.3(i)) is $\geq$.That is, $\leq^{\mathrm{op}} = \geq$.

ii. The opposite of the equality relation $\Delta_X$ on a set $X$ (Example 5.1.3(ii)) is itself, since $y = x \iff x = y$.

iii. Let $X$ be a set. The opposite of the relation $\ni_X$ between $\mathscr{P}(X)$ and $X$ (Example 5.1.3(v)) is the relation $\in_X$ between $X$ and $\mathscr{P}(X)$.

iv. For a set $X$, the opposite of the relation $\subseteq_X$ on $\mathscr{P}(X)$ (Example 5.1.3(vii)) is denoted by $\supseteq_X$.

**Warning 5.1.8** Don't confuse $R^{\mathrm{op}}$ with the complement or negation of $R$, which is the relation $R' = (X \times Y) \setminus R$ between $X$ and $Y$ satisfying $xR'y \iff \text{not } xRy$.

When $X = Y$, both $R^{\mathrm{op}}$ and $R$ are relations on $X$, so we can ask whether they are equal.

**Definition 5.1.9** A relation $R$ on a set $X$ is **symmetric** if $R^{\mathrm{op}} = R$.

That is, $R$ is symmetric if $xRy \iff yRx$, for all $x, y \in X$.

**Examples 5.1.10** i. The relation $\leq$ on $\mathbb{R}$ is not symmetric, since $0 \leq 1$ but $1 \not\leq 0$ (for instance!)

ii. The equality relation $\Delta_X$ on any set $X$ is symmetric.

iii. The trivial relation $X \times X$ on a set $X$ (Example 5.1.3(iii)) is symmetric.

For a relation $R$ between sets $X$ and $Y$, we can ask which elements of $Y$ each element of $X$ is related to (Figure 5.4).

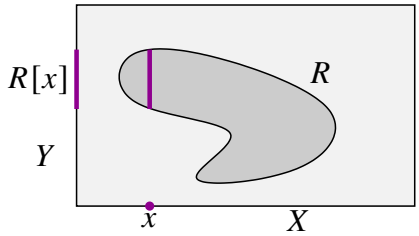



Figure 5.4: A relation $R$ between sets $X$ and $Y$, an element $x \in X$, and the subset $R[x]$ of $Y$.

**Lemma 5.1.11** *Let $R$ be a relation between sets $X$ and $Y$. Then for each $x \in X$, there is a unique subset $R[x]$ of $Y$ such that for $y \in Y$,*

$$y \in_Y R[x] \iff xRy.$$

**Proof** Uniqueness holds because a subset of $Y$ is determined by its $Y$-elements (Proposition 4.1.20).

To prove that such a subset exists, let $\rho\colon X \times Y \to \mathbf{2}$ be the characteristic function of $R$. By definition of function set, $\rho$ corresponds to a function $\bar{\rho}\colon X \to \mathbf{2}^Y$, where $(\bar{\rho}(x))(y) = \rho(x, y)$ $(x \in X, y \in Y)$. Given $x \in X$, let $R[x]$ be the subset of $Y$ with characteristic function $\bar{\rho}(x)$. Then for $y \in Y$,

$$y \in_Y R[x] \iff (\bar{\rho}(x))(y) = \mathsf{T} \iff \rho(x, y) = \mathsf{T} \iff xRy,$$

as required. □

**Remark 5.1.12** What about the other way round? If we start with an element $y \in Y$, then $R^{\mathrm{op}}[y]$ is the subset of $X$ such that for all $x \in X$,

$$x \in_X R^{\mathrm{op}}[y] \iff xRy.$$

**Examples 5.1.13**

i. Take the relation $\leq$ on $\mathbb{R}$ and a real number $x$. Then $y \in \leq[x] \iff x \leq y$, so $\leq[x] = [x, \infty)$. Similarly, $\leq^{\mathrm{op}}[y] = \geq[y] = (-\infty, y]$.

ii. Take the equality relation $\Delta_X$ on a set $X$. Then $\Delta_X[x] = \{x\}$ for all $x \in X$.

iii. Consider the relation $\ni_X$ between $\mathscr{P}X$ and $X$ (Example 5.1.3(v)). Let $A \in \mathscr{P}X$. Then $\ni_X[A]$ is the subset of $X$ such that for $x \in X$,

$$x \in_X \ni_X[A] \iff A \ni_X x \iff x \in_X A.$$

(That's not a typo! The left-hand side means $x \in_X R[A]$ where $R$ is the relation $\ni_X$.) Hence $\ni_X[A] = A$.

In the next section, we'll see how relations can be seen as generalized functions. One aspect of this is that relations, like functions, can be composed.

**Lemma 5.1.14** *Let $X$, $Y$ and $Z$ be sets, let $R$ be a relation between $X$ and $Y$, and let $S$ be a relation between $Y$ and $Z$. Then there is a unique relation $S \circ R$ between $X$ and $Z$ such that for all $x \in X$ and $z \in Z$,*

$$x(S \circ R)z \iff (xRy \text{ and } ySz \text{ for some } y \in Y).$$

The relation $S \circ R$ is called the **composite** of $R$ and $S$.

**Proof** Uniqueness is immediate from Proposition 4.1.20, so we only need to prove existence.

For each $y \in Y$, we have subsets $R^{\mathrm{op}}[y] \subseteq X$ and $S[y] \subseteq Z$, giving another subset $R^{\mathrm{op}}[y] \times S[y] \subseteq X \times Z$. Put

$$S \circ R = \bigcup_{y \in Y} R^{\mathrm{op}}[y] \times S[y] \subseteq X \times Z.$$

The result follows by the fundamental property of unions (Lemma 4.3.14(ii)). □

**Exercise 5.1.15** There is a lapse in rigour in the proof of Lemma 5.1.14. What is it, and how would you fix it?

**Example 5.1.16** There is a relation $R$ between {polynomials over $\mathbb{R}$} and $\mathbb{R}$ given by $fRx \iff f(x) = 0$. We also have the relation $\in_{\mathbb{R}}$ between $\mathbb{R}$ and $\mathscr{P}(\mathbb{R})$. Then the composite $\in_{\mathbb{R}} \circ R$ is given by

$$f(\in_{\mathbb{R}} \circ R)A \iff f(x) = 0 \text{ for some } x \in A,$$

for polynomials $f$ and subsets $A \subseteq \mathbb{R}$. In other words, $\in_{\mathbb{R}} \circ R$ is the relation between {polynomials over $\mathbb{R}$} and $\mathscr{P}(\mathbb{R})$ that, given a polynomial and a subset of $\mathbb{R}$, tells us whether our polynomial has a root in our subset.

Composition of relations is associative, identity relations are identities for composition, and taking the opposite reverses the order of composition:

**Lemma 5.1.17**

*i. Let $Q$ be a relation between $W$ and $X$, let $R$ be a relation between $X$ and $Y$, and let $S$ be a relation between $Y$ and $Z$. Then $(S \circ R) \circ Q = S \circ (R \circ Q)$.*

*ii. Let $R$ be a relation between $X$ and $Y$. Then $R \circ \Delta_X = R = \Delta_Y \circ R$.*

*iii. Let $R$ be a relation between $X$ and $Y$ and $S$ a relation between $Y$ and $Z$. Then $(S \circ R)^{\mathrm{op}} = R^{\mathrm{op}} \circ S^{\mathrm{op}}$.*

**Proof** I will prove (i) and leave the rest to you. Let $w \in W$ and $z \in Z$. Then

$$\begin{aligned} w((S \circ R) \circ Q)z &\iff wQx \text{ and } x(S \circ R)z \text{ for some } x \in X \\ &\iff wQx \text{ and } xRy \text{ and } ySz \text{ for some } x \in X, y \in Y. \end{aligned}$$

A similar argument applies to $S \circ (R \circ Q)$, and the result follows. □

We focus now on relations between a set and itself. Some types of relation are especially important.

**Definition 5.1.18** A relation $R$ on a set $X$ is:

i. **reflexive** if $xRx$ for all $x \in X$;

ii. **transitive** if ($xRy$ and $yRz$) $\implies xRz$, for $x, y, z \in X$;

iii. **antisymmetric** if ($xRy$ and $yRx$) $\implies x = y$, for $x, y \in X$.

**Exercise 5.1.19** Prove that $R$ is reflexive if and only if $\Delta_X \subseteq_{X\times X} R$, transitive if and only if $R \circ R \subseteq_{X\times X} R$, and antisymmetric if and only if $R \cap R^{\mathrm{op}} \subseteq_{X\times X} \Delta_X$.

**Examples 5.1.20** i. The relation $\leq$ on $\mathbb{R}$ has all three properties.

ii. The equality relation $\Delta_X$ on a set $X$ has all three properties.

iii. The trivial relation $R = X \times X$ on a set $X$ is reflexive and transitive, but not in general antisymmetric. For instance, taking $X = \mathbf{2}$, we have $\mathsf{T}R\mathsf{F}$ and $\mathsf{F}R\mathsf{T}$ but $\mathsf{T} \neq \mathsf{F}$.

iv. For any set $X$, the relation $\subseteq_X$ on $\mathscr{P}(X)$ has all three properties.

**Definition 5.1.21** An **order** (or **order relation** or **ordering**) on a set $X$ is a relation on $X$ that is reflexive, transitive and antisymmetric. A set together with an order on it is called an **ordered set**.

**Examples 5.1.22** By Examples 5.1.20, $\leq$ is an order on $\mathbb{R}$, equality on any set is an order, and $\subseteq_X$ is an order on $\mathscr{P}(X)$ for every set $X$.

Orders are typically denoted by $\leq$. People often say **partial order** instead of order, and **partially ordered set** or **poset** instead of ordered set. The word 'partial' refers to the possibility that there are elements $x$ and $y$ of our set such that neither $x \leq y$ nor $y \leq x$.

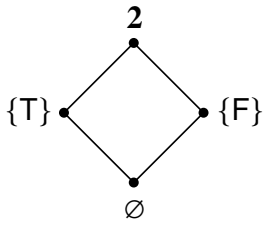



Figure 5.5: The power set of **2**. Lines indicate inclusions, e.g. $\{\mathsf{T}\} \subseteq_{\mathbf{2}} \mathbf{2}$.

**Definition 5.1.23** An order $\leq$ on a set $X$ is **total** if for all $x, y \in X$, we have $x \leq y$ or $y \leq x$. Then $X$ together with $\leq$ is called a **totally ordered set**.

**Examples 5.1.24** i. The order $\leq$ on $\mathbb{R}$ is total.

ii. The identity relation on a set $X$ is not total if $X$ has two or more elements, since if $x, y \in X$ are distinct then $x \neq y$ and $y \neq x$!

iii. The order $\subseteq_X$ on $\mathscr{P}(X)$ is also not total if $X$ has two or more elements. Indeed, let $x$ and $y$ be distinct elements of $X$. Then by Example 4.1.21(ii), $\{x\} \not\subseteq_X \{y\}$ and $\{y\} \not\subseteq_X \{x\}$. Figure 5.5 shows an example with $X = \mathbf{2}$.

## 5.2 Graphs

Graphs appear in nearly every scientific publication. At least when $X$ and $Y$ are subsets of $\mathbb{R}$, a function $f\colon X \to Y$ is depicted as a subset of $X \times Y$, consisting of those points $(x, y)$ such that $f(x) = y$. Since $X \times Y$ is a subset of $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, it's drawable on a two-dimensional page.

But aside from their importance as a visualization tool, graphs are also important mathematically, as we will see.

**Definition 5.2.1** Let $f\colon X \to Y$ be a function. The **graph** of $f$ is the function $\Gamma_f = (\mathrm{id}_X, f)\colon X \to X \times Y$.

Thus, $\Gamma_f(x) = (x, f(x))$ for all $x \in X$ (Figure 5.6).

**Exercise 5.2.2** Prove that $\Gamma_f$ is injective for all functions $f$.

Since $\Gamma_f$ is injective, we can view $X \xrightarrow{\Gamma_f} X \times Y$ as a subset of $X \times Y$. In other words, $\Gamma_f$ can be understood as a relation between $X$ and $Y$. (As in the case of

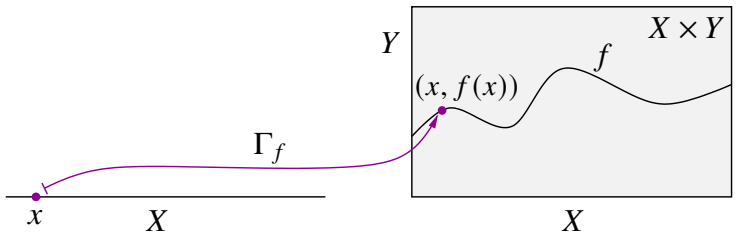



Figure 5.6: The graph $\Gamma_f$ of a function $f\colon X \to Y$.

$\Delta_X$—Example 5.1.3(ii)—we name this relation after the injection itself rather than its codomain.) Explicitly,

$$x\Gamma_f y \iff f(x) = y$$

$(x \in X,\, y \in Y)$ .

The idea now is that relations are more general than functions. A function from a set $X$ to a set $Y$ assigns to each element of $X$ exactly one element of $Y$: not none, not many, but exactly one. But a relation between $X$ and $Y$ relates each element of $X$ to any number of elements of $Y$: none, one, or many.

So, we should be able to understand functions as special relations. The next definition pins down the meaning of 'special'.

**Definition 5.2.3** Let $X$ and $Y$ be sets. A relation $R$ between $X$ and $Y$ is **functional** if for all $x \in X$, there exists a unique $y \in Y$ such that $(x, y) \in_{X\times Y} R$.

We now prove that the functions from $X$ to $Y$ are in one-to-one correspondence with the functional relations between $X$ and $Y$.

**Theorem 5.2.4** *Let $X$ and $Y$ be sets.*

*i. For every function $f\colon X \to Y$, the graph $\Gamma_f$ is a functional relation between $X$ and $Y$.*

*ii. For every functional relation $R$ between $X$ and $Y$, there is a unique function $f\colon X \to Y$ such that the relations $\Gamma_f$ and $R$ are equal.*

**Proof** Part (i) simply says that given a function $f\colon X \to Y$ and an element $x \in X$, there is exactly one element $y \in Y$ such that $y = f(x)$. This is trivially true.

For (ii), let $R$ be a functional relation between $X$ and $Y$. We must show that there exists a unique function $f\colon X \to Y$ such that $\Gamma_f = R$, or equivalently, such that

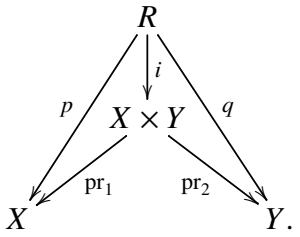
$$xRy \iff f(x) = y$$

($x \in X$, $y \in Y$).

*Uniqueness:* A function is determined by its effect on elements, so this is immediate.

*Existence:* This is the substantial part of the theorem. The idea is that given a functional relation $R$, there is for each $x \in X$ a unique $y \in Y$ such that $(x, y) \in_{X \times Y} R$, and we take $f(x)$ to be that $y$. The challenge is to show that such a function $f$ exists.

Write $i \colon R \hookrightarrow X \times Y$ for the inclusion, and put $p = \mathrm{pr}_1^{X,Y} \circ i$ and $q = \mathrm{pr}_2^{X,Y} \circ i$, as in the commutative diagram




Since $R$ is a functional relation, $p$ is bijective: it is surjective by the existence part of Definition 5.2.3, and injective by the uniqueness part. Since bijections are invertible (Proposition 3.2.18), we can define $f = q \circ p^{-1} \colon X \to Y$.

(The idea here is that given $x \in X$, the element $p^{-1}(x)$ of $R$ is $(x, y)$ for some $y \in Y$, and then $qp^{-1}(x) = y$.)

It remains to show that $X \xrightarrow{\Gamma_f} X \times Y$ and $R \xrightarrow{i} X \times Y$ are equal as subsets of $X \times Y$, or more properly, isomorphic over $X \times Y$. By Proposition 4.1.20, an equivalent condition is that for all $x \in X$ and $y \in Y$,

$$(x, y) \in_{X \times Y} \left(X \xrightarrow{\Gamma_f} X \times Y\right) \iff (x, y) \in_{X \times Y} \left(R \xrightarrow{i} X \times Y\right).$$

In other words, we have to show that for $x \in X$ and $y \in Y$,

$$y = f(x) \iff xRy.$$

The remaining details are covered in a question on Workshop 3. □

Theorem 5.2.4 is extraordinarily useful. It lets us view functions from $X$ to $Y$ as certain subsets of $X \times Y$, so any techniques we have for constructing subsets can be used to construct functions. We do already have some subset construction techniques (union, intersection, complement, . . . ), but the full power of Theorem 5.2.4 won't be clear until we have the further techniques described in Section 5.4. I will therefore delay examples until later in this chapter.

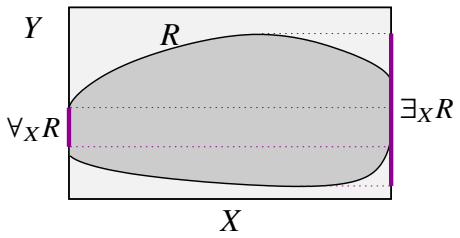



Figure 5.7: The subsets $\forall_X R$ and $\exists_X R$ of $Y$, for a relation $R$ between $X$ and $Y$.

## 5.3 Quantifiers

In Section 4.2, we introduced logical operators such as *and* and *not*. But so far, we haven't said anything about quantifiers: 'for all' and 'there exists'.

Let $R$ be a relation between sets $X$ and $Y$. We'd like to be able to define two subsets of $Y$:

$$\{y \in Y : (\forall x \in X) xRy\}, \qquad \{y \in Y : (\exists x \in X) xRy\},$$

or more wordily,

$$\{y \in Y : xRy \text{ for all } x \in X\}, \qquad \{y \in Y : xRy \text{ for some } x \in X\}.$$

We haven't defined the curly bracket notation yet (coming soon!), but in this short section, we show that these subsets of $Y$ do indeed exist. For now, we will call these sets $\forall_X R$ and $\exists_X R$ (Figure 5.7).

To define them, recall from the proof of Lemma 5.1.11 that, writing $\rho\colon X \times Y \to \mathbf{2}$ for the characteristic function of $R \subseteq X \times Y$, the corresponding function $\bar{\rho}\colon X \to \mathbf{2}^Y$ is $x \mapsto R[x]$. So $\bar{\rho}$, viewed as an $X$-indexed family of subsets of $Y$, is $(R[x])_{x \in X}$. Define

$$\forall_X R = \bigcap_{x \in X} R[x], \qquad \exists_X R = \bigcup_{x \in X} R[x],$$

which are both subsets of $Y$.

**Lemma 5.3.1** *Let $R$ be a relation between sets $X$ and $Y$. Then for $y \in Y$,*

*i. $y \in_Y \forall_X R$ if and only if ($xRy$ for all $x \in X$);*

*ii. $y \in_Y \exists_X R$ if and only if ($xRy$ for some $x \in X$).*

**Proof** Let $y \in Y$. For (i), $y \in_Y \forall_X R$ if and only if $y \in_Y R[x]$ for all $x \in X$ (by the fundamental property of intersections, Lemma 4.3.14(i)). But this just means that $xRy$ for all $x \in X$. Part (ii) is similar. □

**Examples 5.3.2** i. Let $X = [-1, 1]$, let $Y = \mathbb{R}$, and let

$$R = \{(x, y) \in [-1, 1] \times \mathbb{R} : x^2 + y^2 \leq 1\}.$$

Then $\forall_X R = \{0\}$ and $\exists_X R = [-1, 1]$. (Draw a picture!)

ii. Let $f : X \to Y$ be any function. Then $\exists_X \Gamma_f$ consists of the elements $y \in Y$ such that $x \Gamma_f y$ for some $x \in X$, or equivalently, such that $f(x) = y$ for some $x \in X$. So $\exists_X \Gamma_f = \operatorname{im} f$.

**Exercise 5.3.3** Let $Y$ be a set and let $R$ be the one and only relation between $\varnothing$ and $Y$. What are $\forall_\varnothing R$ and $\exists_\varnothing R$?

## 5.4 Specifying subsets

We would like to be able to define the set of prime numbers using the 'set-builder' or curly bracket notation that you're used to:

$$\{p \in \mathbb{N} : p \neq 1 \text{ and } (\forall m, n \in \mathbb{N})(p = mn \implies m = 1 \text{ or } n = 1)\} \subseteq \mathbb{N}. \quad (5.1)$$

Similarly, given a function $f : \mathbb{R} \to \mathbb{R}$, we would like to be able to define the subset of $\mathbb{R}$ consisting of the points at which $f$ is continuous:

$$\{x \in \mathbb{R} : (\forall \varepsilon > 0)(\exists \delta > 0)(\forall x' \in \mathbb{R})(|x - x'| < \delta \implies |f(x) - f(x')| < \varepsilon)\}. \quad (5.2)$$

Of course, we haven't defined multiplication on $\mathbb{N}$, or the set $\mathbb{R}$, etc. But even assuming we have, how do we know that such subsets exist?

In general, given a set $X$ and a true/false property $P(x)$ of elements $x \in X$, we would like to be able to define a subset

$$\{x \in X : P(x)\}$$

of $X$. That is, we want to prove that there exists a unique subset $A$ of $X$ such that for all $x \in X$,

$$x \in_X A \iff P(x).$$

Uniqueness is immediate, since a subset of $X$ is determined by its $X$-elements (Proposition 4.1.20). It is existence that we have to prove. And then we will define $\{x \in X : P(x)\}$ to be that subset $A$.

I will not define 'property' precisely. (If you're interested, try an introductory text on logic.) Instead, I will give you practical tools that will enable you to show that expressions like (5.1) and (5.2) really do define subsets.

**Remark 5.4.1** Although I won't give a rigorous definition of property, I do need to explain something about the meaning of the $x$ in '$P(x)$'.

Consider, for instance, the following property $P(x)$ of a real number $x$:

$$(\forall y \in \mathbb{R})(x < y^2 - 3y + 1).$$

You can see that $x$ and $y$ play different roles here. The variable $y$ is **bound**, which means it's had a quantifier applied to it. (That's 'bound', not 'bounded', the idea being that the quantifier 'binds' the variable.) Because $y$ is quantified, if you changed every $y$ to a $z$, it wouldn't change the property. That is, $P(x)$ could equivalently be defined as

$$(\forall z \in \mathbb{R})(x < z^2 - 3z + 1).$$

Variables that aren't bound are said to be **free**. So in this example, $x$ is free. The notation for the property only mentions the free variables, which is why we call it $P(x)$ and not $P(x, y)$.

Another way to look at it: when a variable is free, you can substitute particular values for it and the expression still has a meaning. For instance, substituting $x = 4$, the expression $P(4)$ is

$$(\forall y \in \mathbb{R})(4 < y^2 - 3y + 1),$$

which is a meaningful statement. But when a variable is bound, you can't. For instance, substituting $y = 4$ in $P(x)$ gives us the nonsensical expression

$$(\forall 4 \in \mathbb{R})(x < 4^2 - 3 \times 4 + 1)$$

('$\forall 4$'?!)

For another example, here is a property $P(x, n)$ of $x \in \mathbb{R}$ and $n \in \mathbb{N}$:

$$(\exists y \in \mathbb{R})(\forall q \in \mathbb{Q})(x^n + y \neq \cos q).$$

In this expression, $x$ and $n$ are free and $y$ and $q$ are bound, which is why we call the property $P(x, n)$. It's a statement that is either true or false for any particular pair $(x, n) \in \mathbb{R} \times \mathbb{N}$.

We now return to our mission.

**Definition 5.4.2** Let $X$ be a set and let $P(x)$ be a property of elements $x \in X$. We say that $P(x)$ **specifies a subset of** $X$ if there exists $A \subseteq X$ such that for $x \in X$,

$$x \in_X A \iff P(x). \tag{5.3}$$

In that case, we define $\{x \in X : P(x)\}$ to be this subset $A$ of $X$.

By Proposition 4.1.20, there can be only *one* subset $A \subseteq X$ satisfying (5.3), so this definition of $\{x \in X : P(x)\}$ is valid.

Slightly informally, I will sometimes say that $\{x \in X : P(x)\}$ **exists** to mean that $P(x)$ specifies a subset of $X$.

Our goal now is to build up a large class of properties that specify subsets. This will enable us to make definitions like (5.1) and (5.2).

**Examples 5.4.3** i. Let $X$ be a set and $a \in X$. Let $P(x)$ be the property $x = a$ of elements $x \in X$. Then $P(x)$ specifies a subset of $X$ (that is, '$\{x \in X : P(x)\}$ exists'), since the subset $\{a\}$ of $X$ (defined in Example 4.1.4(iii)) has the property that

$$x \in_X \{a\} \iff x = a$$

$(x \in X)$. Hence

$$\{x \in X : x = a\} = \{a\}.$$

ii. Let $X$ be a set and $A \subseteq X$. Let $P(x)$ be the property $x \in_X A$ of elements $x \in X$. Then $P(x)$ specifies a subset of $X$, since tautologously,

$$x \in_X A \iff x \in_X A \quad (!)$$

Hence

$$\{x \in X : x \in_X A\} = A.$$

Our next lemma is a plentiful source of subsets.

**Lemma 5.4.4** *For sets and functions* $X \overset{f}{\underset{g}{\rightrightarrows}} Y$*, the subset* $\{x \in X : f(x) = g(x)\}$ *of* $X$ *exists.*

This means there is a subset $A \subseteq X$ such that $x \in_X A \iff f(x) = g(x)$, for $x \in X$. Definition 5.4.2 then defines $\{x \in X : f(x) = g(x)\}$ to be that subset $A$. It is called the **equalizer** of $f$ and $g$, because it consists of the elements of $X$ on which $f$ and $g$ are equal.

**Proof** Let $A$ be the preimage of $Y \overset{\Delta_Y}{\hookrightarrow} Y \times Y$ under the function $(f, g) : X \to Y \times Y$. Then for $x \in X$,

$$\begin{aligned} x \in_X A &\iff (f, g)(x) \in_{Y \times Y} (Y \overset{\Delta_Y}{\hookrightarrow} Y \times Y) \\ &\iff (f(x), g(x)) \in_{Y \times Y} (Y \overset{\Delta_Y}{\hookrightarrow} Y \times Y) \\ &\iff f(x) = g(x), \end{aligned}$$

using the fundamental property of preimages and Example 4.1.9(iv). □

**Examples 5.4.5** In these examples, I will assume we have already constructed the real numbers and all the functions concerned.

i. The subset $\{x \in \mathbb{R} : x = 1 + x^2\}$ of $\mathbb{R}$ exists. This follows from Lemma 5.4.4 by taking $X = Y = \mathbb{R}$, $f = \mathrm{id}_{\mathbb{R}}$, and $g : \mathbb{R} \to \mathbb{R}$ to be the function $x \mapsto 1 + x^2$.

ii. The subset $\{(x, y) \in \mathbb{R} \times \mathbb{R} : xy = 1\}$ of $\mathbb{R} \times \mathbb{R}$ (a hyperbola) exists, by Lemma 5.4.4 applied to the functions $f, g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ with $f(x, y) = xy$ and $g(x, y) = 1$. In this example, the set '$X$' of Definition 5.4.2 is presented as a product of two sets ($\mathbb{R} \times \mathbb{R}$), so its elements are ordered pairs.

iii. Given sets and functions

$$X \xrightarrow{f} Z \xleftarrow{g} Y,$$

the property $f(x) = g(y)$ of elements $(x, y) \in X \times Y$ specifies a subset of $X \times Y$. This subset,

$$\{(x, y) \in X \times Y : f(x) = g(y)\} \subseteq X \times Y,$$

is exactly the pullback of $f$ and $g$ (Example 5.1.3(viii)). We already constructed it in that example, but another way to obtain it is as the equalizer of the functions

$$\begin{array}{ccccc} X \times Y & \xrightarrow{\mathrm{pr}_1} & X & \xrightarrow{f} & Z \\ (x, y) & \mapsto & x & \mapsto & f(x), \end{array} \qquad \begin{array}{ccccc} X \times Y & \xrightarrow{\mathrm{pr}_2} & Y & \xrightarrow{g} & Z \\ (x, y) & \mapsto & y & \mapsto & g(y). \end{array}$$

**Exercise 5.4.6** Let $X$ be a set. How would you show that the property $x = y$ of elements $(x, y) \in X \times X$ specifies a subset of $X \times X$? What is this subset called?

Now we think about combining properties. For example, given properties $P(x)$ and $Q(x)$ of elements $x \in X$, we get a new property ($P(x)$ or $Q(x)$) of elements $x \in X$. If $P(x)$ and $Q(x)$ both specify subsets of $X$, does ($P(x)$ or $Q(x)$)? Yes, and much else besides:

**Lemma 5.4.7** *Let $X$ be a set, and let $P(x)$ and $Q(x)$ be properties of elements $x \in X$. If $P(x)$ and $Q(x)$ specify subsets of $X$, then so do the following properties of elements $x \in X$:*

*i. not $P(x)$;*

*ii. $P(x)$ and $Q(x)$;*

*iii. $P(x)$ or $Q(x)$;*

*iv.* $P(x) \implies Q(x)$;

*v.* $P(x) \iff Q(x)$.

**Proof** By hypothesis, the subsets $A = \{x \in X : P(x)\}$ and $B = \{x \in X : Q(x)\}$ of $X$ exist.

For (i), consider $X \setminus A \subseteq X$. For $x \in X$,

$$x \in_X X \setminus A \iff x \notin_X A \iff (\text{not } P(x)),$$

where the first equivalence is by Lemma 4.3.7 and the second is by definition of $A$. Hence (not $P(x)$) specifies a subset of $X$, with

$$\{x \in X : \text{not } P(x)\} = X \setminus \{x \in X : P(x)\}.$$

Similarly, for (ii), consider $A \cap B \subseteq X$. For $x \in X$,

$$x \in_X A \cap B \iff (x \in_X A \text{ and } x \in_X B) \iff (P(x) \text{ and } Q(x)),$$

by Lemma 4.3.3 and definition of $A$ and $B$. Part (iii) is similar. Part (iv) follows, since $(P(x) \implies Q(x))$ is equivalent to ((not $P(x)$) or $Q(x)$). And (v) follows in turn, since $(P(x) \iff Q(x))$ is equivalent to

$$(P(x) \implies Q(x)) \text{ and } (Q(x) \implies P(x)).$$ □

**Warning 5.4.8** Recall Warning 4.2.12. I'm *not* writing things like '$P(x) \wedge Q(x)$' because the symbol $\wedge$ is reserved for a certain function $\mathbf{2} \times \mathbf{2} \to \mathbf{2}$. To make the distinction, I'm writing '$P(x)$ and $Q(x)$' instead. Similar points apply to the other logical operators.

**Example 5.4.9** The subset

$$\{x \in \mathbb{R} : x^2 + x = 12 \text{ and } x \neq 3\}$$

of $\mathbb{R}$ exists. That is, the property ($x^2+x = 12$ and $x \neq 3$) of elements $x \in \mathbb{R}$ specifies a subset of $\mathbb{R}$ (assuming we've already constructed $\mathbb{R}$ and these functions).

To see this, first note that $x^2 + x = 12$ specifies a subset of $\mathbb{R}$ (as in Example 5.4.5(i)), as does $x = 3$ (for the same reason, or because of Example 5.4.3(i)). By Lemma 5.4.7(i), $x \neq 3$ does too. Hence by Lemma 5.4.7(ii),

$$x^2 + x = 12 \text{ and } x \neq 3$$

also specifies a subset of $\mathbb{R}$.

Perhaps you noticed that our property is equivalent to '$x = -4$', which certainly specifies a subset of $\mathbb{R}$ (namely, $\{-4\}$). But there's no need to solve any equations! The argument above is completely mechanical, and I hope you can see that it can be applied in arbitrarily complicated situations.

We now think about transferring properties between different sets.

**Lemma 5.4.10** *Let $f\colon X \to Y$ be a function. Let $Q(y)$ be a property of elements $y \in Y$, and define a property $P(x)$ of elements $x \in X$ by $P(x) = Q(f(x))$. If $Q(y)$ specifies a subset of $Y$ then $P(x)$ specifies a subset of $X$.*

**Proof** Let $A \subseteq X$ be the preimage $f^{-1}\{y \in Y : Q(y)\}$. Then for $x \in X$,

$$x \in_X A \iff f(x) \in_Y \{y \in Y : Q(y)\} \iff Q(f(x)) \iff P(x),$$

by the fundamental property of preimages and then the definitions of $\{y \in Y : Q(y)\}$ and $P(x)$. Hence $P(x)$ specifies a subset of $X$ (namely, $A$). □

**Examples 5.4.11** i. Suppose we have already constructed the function

$$\begin{array}{rccc} f\colon & \mathbb{R}^3 & \to & \mathbb{R} \\ & (x,y,z) & \mapsto & x^2+y^2+z^2 \end{array}$$

and shown that the subset $\{v \in \mathbb{R} : 10 \leq v \leq 11\}$ of $\mathbb{R}$ exists. Then the subset

$$\{(x,y,z) \in \mathbb{R}^3 : 10 \leq x^2+y^2+z^2 \leq 11\}$$

of $\mathbb{R}^3$ exists. It is the preimage $v^{-1}[10,11]$.

ii. Let $X$ and $Y$ be sets, and let $Q(y)$ be a property of elements $y \in Y$. Then there is a property $P(x,y)$ of elements $(x,y) \in X \times Y$ defined by $P(x,y) = Q(y)$.

For instance, if $Q(y)$ is the property '$y$ is a square' of elements $y \in \mathbb{Z}$, then $P(x,y)$ is the property '$y$ is a square' of elements $(x,y) \in \mathbb{R} \times \mathbb{Z}$; it's just one in which $x$ happens not to be mentioned.

Applying Lemma 5.4.10 to $\mathrm{pr}_2\colon X \times Y \to Y$ tells us that if the subset $\{y \in Y : Q(y)\}$ exists then so does the subset $\{(x,y) \in X \times Y : Q(y)\}$ of $X \times Y$. It is simply $X \times \{y \in Y : Q(y)\}$.

iii. We can permute variables. Let $X$ and $Y$ be sets, and let $Q(x,y)$ be a property of elements $(x,y) \in X \times Y$. Then there is a property $P(y,x)$ of elements $(y,x) \in Y \times X$ defined by $P(y,x) = Q(x,y)$. Applying Lemma 5.4.10 to the usual isomorphism $Y \times X \to X \times Y$ tells us that if $\{(x,y) \in X \times Y : Q(x,y)\}$ exists then so does $\{(y,x) \in Y \times X : Q(x,y)\}$. As relations, one is the opposite of the other.

We can consider properties of elements of a product set, as in Example 5.4.5(ii).

**Lemma 5.4.12** *Let $P(x,y)$ be a property of elements $(x,y) \in X \times Y$ that specifies a subset of $X \times Y$. Then $(\forall x \in X)P(x,y)$ and $(\exists x \in X)P(x,y)$ are properties of elements $y \in Y$ that specify subsets of $Y$.*

To see that this statement even makes sense, look back at Remark 5.4.1, which should persuade you that both $(\forall x \in X)P(x, y)$ and $(\exists x \in X)P(x, y)$ have $y$ as their one and only free variable.

**Proof** By hypothesis, $P(x, y)$ specifies a subset

$$R = \{(x, y) \in X \times Y : P(x, y)\}$$

of $X \times Y$. Then $R$ is a relation between $X$ and $Y$, and for $x \in X$ and $y \in Y$, we have $xRy \iff P(x, y)$.

In Section 5.3, we constructed subsets $\forall_X R$ and $\exists_X R$ of $Y$, and we showed in Lemma 5.3.1 that for $y \in Y$,

$$y \in_Y \forall_X R \iff xRy \text{ for all } x \in X.$$

But the right-hand side here is equivalent to $(\forall x \in X)P(x, y)$, so $(\forall x \in X)P(x, y)$ specifies a subset of $Y$, namely, $\forall_X R$. The same argument holds for $\exists$. □

We have now finished assembling the logical apparatus, and we can deduce the existence of a very large variety of subsets. I'll demonstrate this by returning to the example where we began.

**Example 5.4.13** We now show that the subset

$$\{p \in \mathbb{N} : p \neq 1 \text{ and } (\forall m, n \in \mathbb{N})(p = mn \implies m = 1 \text{ or } n = 1)\}$$

of $\mathbb{N}$ (the prime numbers) exists—at least, assuming that we have already defined the multiplication function $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and the element $1 \in \mathbb{N}$.

We begin with two ingredients.

- The property $x = 1$ of $x \in \mathbb{N}$ specifies a subset of $\mathbb{N}$ (namely, $\{1\}$), by Example 5.4.3(i).
- The property $p = mn$ of $(p, m, n) \in \mathbb{N}\times\mathbb{N}\times\mathbb{N}$ specifies a subset of $\mathbb{N}\times\mathbb{N}\times\mathbb{N}$, by Lemma 5.4.4 on equalizers applied to these functions $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \rightrightarrows \mathbb{N}$:

$$\begin{array}{ccccc} \mathbb{N}\times\mathbb{N}\times\mathbb{N} & \xrightarrow{\mathrm{pr}_1} & \mathbb{N} & \qquad & \mathbb{N}\times(\mathbb{N}\times\mathbb{N}) & \xrightarrow{\mathrm{pr}_2} & \mathbb{N}\times\mathbb{N} & \xrightarrow{\cdot} & \mathbb{N} \\ (p,m,n) & \mapsto & p, & & (p,(m,n)) & \mapsto & (m,n) & \mapsto & mn. \end{array}$$

Now we repeatedly apply Lemmas 5.4.7, 5.4.10 and 5.4.12.

- The property $p = 1$ of elements $p \in \mathbb{N}$ specifies a subset of $\mathbb{N}$, so by Lemma 5.4.7(i), the property $p \neq 1$ does too.

- The property $m = 1$ of elements $m \in \mathbb{N}$ specifies a subset of $\mathbb{N}$, so by Examples 5.4.11(ii) and (iii), the property $m = 1$ of elements $(p, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ specifies a subset of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$.
- Similarly, the property $n = 1$ of elements $(p, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ specifies a subset of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$.
- Hence by Lemma 5.4.7(iii), the property $(m = 1 \text{ or } n = 1)$ of elements $(p, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ specifies a subset of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$.
- Now using the second 'ingredient' and Lemma 5.4.7(iv), the property

  $$p = mn \implies m = 1 \text{ or } n = 1$$

  of elements $(p, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ specifies a subset of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$.
- Hence by Lemma 5.4.12, the property

  $$(\forall n \in \mathbb{N})(p = mn \implies m = 1 \text{ or } n = 1)$$

  of elements $(p, m) \in \mathbb{N} \times \mathbb{N}$ specifies a subset of $\mathbb{N} \times \mathbb{N}$.
- And then by Lemma 5.4.12, the property

  $$(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})(p = mn \implies m = 1 \text{ or } n = 1)$$

  of elements $p \in \mathbb{N}$ specifies a subset of $\mathbb{N}$. (We normally abbreviate $(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})$ to $(\forall m, n \in \mathbb{N})$.)
- Finally, combining the previous bullet point with the first bullet point and using Lemma 5.4.7(ii), the property

  $$p \neq 1 \text{ and } (\forall m, n \in \mathbb{N})(p = mn \implies m = 1 \text{ or } n = 1)$$

  of elements $p \in \mathbb{N}$ specifies a subset of $\mathbb{N}$.

I've written out this example in full detail to show you the method in a nontrivial case. Try the method yourself on the continuity example, equation (5.2). But after you've done a couple, you should never need to do it again: you'll be able to just glance at expressions like (5.1) or (5.2) and know that they do define subsets.

Our final example gives a fundamental construction in set theory.

**Example 5.4.14** Let $X$ be a set. We have already defined the intersection and union of an $I$-indexed family $(A_i)_{i\in I} \in \mathscr{P}(X)^I$ of subsets of $X$, for any set $I$ (Definition 4.3.13). Here we do something related but different, defining the intersection and union of a *set* of subsets. (I will explain the difference between sets and families in the next chapter.)

So, given $\mathscr{U} \in \mathscr{P}(\mathscr{P}(X))$, we will define $\bigcap \mathscr{U}, \bigcup \mathscr{U} \in \mathscr{P}(X)$. Alternative notation for $\bigcap \mathscr{U}$ is $\bigcap_{A\in\mathscr{U}} A$; it should be a subset of $X$ with the property that for $x \in X$,

$$x \in_X \bigcap \mathscr{U} \iff (x \in_X A \text{ for all } A \in \mathscr{U}).$$

Does such a subset of $X$ exist? Formally, we are asking whether the property

$$(\forall A \in \mathscr{P}(X))(A \in_{\mathscr{P}(X)} \mathscr{U} \implies x \in_X A)$$

of elements $x \in X$ specifies a subset of $X$. And it does, using a similar argument to Example 5.4.13. The same goes for $\bigcup \mathscr{U}$.

**Exercise 5.4.15** Adapt Example 5.4.14 from intersections to unions. In particular, how does the sentence beginning 'Formally' change?

## 5.5 Specifying functions

We would like to be able to specify functions by formulas. For example, given elements $a$ and $b$ of a set $X$, we would like to be able to define the function $f\colon X \to X$ that swaps $a$ and $b$ and fixes everything else, via the formula

$$f(x) = \begin{cases} b & \text{if } x = a, \\ a & \text{if } x = b, \\ x & \text{otherwise} \end{cases} \tag{5.4}$$

(Figure 5.8). But can we just write down a function like this? That is, does there exist a unique function $f\colon X \to X$ satisfying (5.4)? Uniqueness is immediate, since a function is determined by its effect on elements (Axiom 3). The challenge is to prove existence.

We now have a powerful and very versatile method for doing this. It's the combination of two things: Theorem 5.2.4 on graphs, which describes functions $X \to Y$ as certain subsets of $X \times Y$, and the results of the previous section on specifying subsets. Together, they will give us an easy way of constructing functions by formulas like (5.4).

But before we do this, let's go back to a point first mentioned in Example 2.6.11(iii), on how composition and products alone allow us to combine simple

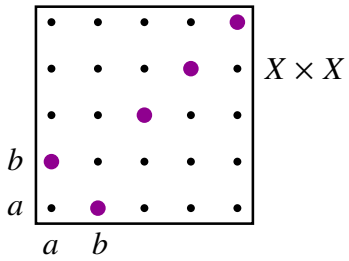



Figure 5.8: The function that swaps two elements $a$ and $b$ of a five-element set $X$. The graph of the function is the subset of $X \times X$ consisting of the large purple dots.

operations to build complex ones. I will elaborate on it here with a more substantial example.

**Example 5.5.1** Suppose we have defined $\mathbb{R}$, the addition and multiplication functions $+, \cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, and the element $5 \in \mathbb{R}$. How do we know that there exists a function $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ satisfying

$$f(x, y) = x^3 y + 5x$$

for all $x, y \in \mathbb{R}$?

We build $f$ up in stages. First, we have the threefold multiplication function $m : \mathbb{R} \times \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, defined as the composite

$$\begin{array}{ccccc} \mathbb{R} \times \mathbb{R} \times \mathbb{R} & \xrightarrow{\cdot \times \mathrm{id}} & \mathbb{R} \times \mathbb{R} & \xrightarrow{\cdot} & \mathbb{R} \\ (x, y, z) & \mapsto & (xy, z) & \mapsto & xyz. \end{array}$$

Hence we have the cubing function $c : \mathbb{R} \to \mathbb{R}$, the composite

$$\begin{array}{ccccc} \mathbb{R} & \xrightarrow{(\mathrm{id},\mathrm{id},\mathrm{id})} & \mathbb{R} \times \mathbb{R} \times \mathbb{R} & \xrightarrow{m} & \mathbb{R} \\ x & \mapsto & (x, x, x) & \mapsto & x^3. \end{array}$$

From this we get the function $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined as the composite

$$\begin{array}{ccccc} \mathbb{R} \times \mathbb{R} & \xrightarrow{c \times \mathrm{id}} & \mathbb{R} \times \mathbb{R} & \xrightarrow{\cdot} & \mathbb{R} \\ (x, y) & \mapsto & (x^3, y) & \mapsto & x^3 y. \end{array}$$

We also have the function $\Delta 5 : \mathbb{R} \to \mathbb{R}$ with constant value 5, constructed as the composite $\mathbb{R} \xrightarrow{!} \mathbf{1} \xrightarrow{5} \mathbb{R}$. Hence we have the composite function

$$\begin{array}{ccccc} \mathbb{R} & \xrightarrow{(\Delta 5,\mathrm{id})} & \mathbb{R} \times \mathbb{R} & \xrightarrow{\cdot} & \mathbb{R} \\ x & \mapsto & (5, x) & \mapsto & 5x, \end{array}$$

which I will write as $5 \cdot - : \mathbb{R} \to \mathbb{R}$. And this gives us the function $g' : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined as the composite

$$\begin{array}{ccccc} \mathbb{R} \times \mathbb{R} & \xrightarrow{\mathrm{pr}_1} & \mathbb{R} & \xrightarrow{5\cdot -} & \mathbb{R} \\ (x, y) & \mapsto & x & \mapsto & 5x. \end{array}$$

Finally, let $f$ be the composite

$$\begin{array}{ccccc} \mathbb{R} \times \mathbb{R} & \xrightarrow{(g,g')} & \mathbb{R} \times \mathbb{R} & \xrightarrow{+} & \mathbb{R} \\ (x, y) & \mapsto & (x^3 y, 5x) & \mapsto & x^3 y + 5x. \end{array}$$

This proves the existence of a function $f : \mathbb{R} \to \mathbb{R}$ such that $f(x, y) = x^3 y + 5x$ for all $x, y$. But I hope it's clear that this is just a random example, and that the same method applies much more generally.

Now let's return to the swapping function (equation (5.4)).

**Example 5.5.2** Let $X$ be a set and $a, b \in X$. By the results of Section 5.4, the subset

$$R = \big\{(x, y) \in X : (x = a \text{ and } y = b) \text{ or } (x = b \text{ and } y = a) \text{ or } (x \neq a \text{ and } x \neq b \text{ and } y = x)\big\}$$

of $X \times X$ exists. It is a functional relation on $X$, that is, for each $x \in X$, there exists a unique $y \in Y$ such that $(x, y) \in_{X \times X} R$. (Consider the three cases $x = a$, $x = b$, and $x \neq a, b$.) Hence by Theorem 5.2.4, $R$ is the graph of a function $f : X \to X$, which by construction satisfies equation (5.4).

For our next illustration of the power of the method, we revisit Exercise 3.1.10. A **retraction** of a function $i : Y \to X$ is a function $f : X \to Y$ such that $f \circ i = \mathrm{id}_Y$. Any function with a retraction must be injective (Example 3.1.9(ii)). Here we prove that except in one trivial case, the converse also holds.

**Lemma 5.5.3** *Every injection with nonempty domain has a retraction.*

**Exercise 5.5.4** Why do we need the nonemptiness hypothesis?

The proof strategy is shown in Figure 5.9.

**Proof** Let $i : Y \to X$ be an injection. Assuming $Y$ is nonempty, we can fix an element $b \in Y$. By the results of Section 5.4, the subset

$$R = \big\{(x, y) \in X \times Y : x = i(y) \text{ or } (x \notin_X \operatorname{im} i \text{ and } y = b)\big\}$$

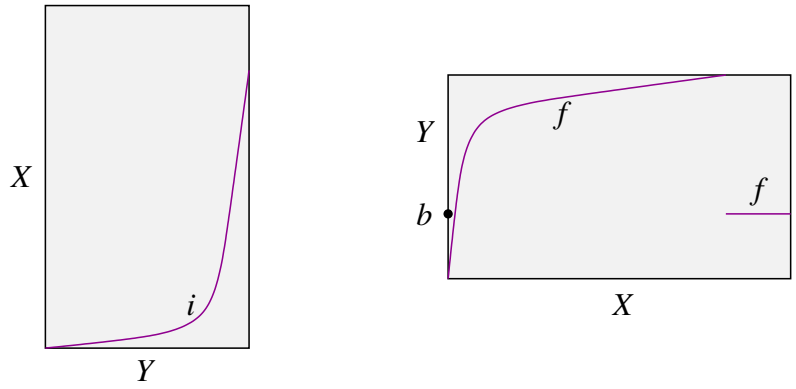



Figure 5.9: The graphs of an injection $i\colon Y \to X$ and a retraction $f$ of $i$ (Lemma 5.5.3).

of $X \times Y$ exists, where $\operatorname{im} i \subseteq X$ is the image of the function $i$ (defined in Example 4.4.3(ii)).

I claim that the relation $R$ between $X$ and $Y$ is functional. Let $x \in X$. If $x \notin_X \operatorname{im} i$ then there is a unique $y \in Y$ such that $xRy$, namely, $b$. If $x \in_X \operatorname{im} i$ then there is some $y \in Y$ such that $x = i(y)$, and since $i$ is injective, there is exactly one such $y$. In either case, there is a unique $y \in Y$ such that $xRy$, proving the claim.

Now by Theorem 5.2.4, $R$ is the graph of a function $f\colon X \to Y$. For each $y \in Y$, we have $(i(y), y) \in R$, so $f(i(y)) = y$. Hence $f \circ i = \mathrm{id}_Y$. □

Next we show that the complement, intersection and union constructions are actually *functions*, in the following sense.

**Lemma 5.5.5** *Let $X$ be a set. Then there is a function $X \setminus -\colon \mathscr{P}(X) \to \mathscr{P}(X)$ such that $(X \setminus -)(A) = X \setminus A$ for all $A \in \mathscr{P}(X)$.*

**Proof** By the results of Section 5.4, the subset

$$R = \big\{(A, B) \in \mathscr{P}(X) \times \mathscr{P}(X) : (\forall x \in X)(x \in_X A \iff x \notin_X B)\big\}$$

of $\mathscr{P}(X) \times \mathscr{P}(X)$ exists. Then $ARB$ if and only if $B = X \setminus A$. Hence $R$ is a functional relation, and it is the graph of a function $f\colon \mathscr{P}(X) \to \mathscr{P}(X)$ satisfying $f(A) = X \setminus A$ for all $A \in \mathscr{P}(X)$. □

**Lemma 5.5.6** *Let $X$ be a set. Then there exist functions $\bigcap, \bigcup\colon \mathscr{P}(\mathscr{P}(X)) \to \mathscr{P}(X)$ such that $\bigcap \mathscr{U}$ and $\bigcup \mathscr{U}$ are the subsets of $X$ constructed in Example 5.4.14, for all $\mathscr{U} \in \mathscr{P}(\mathscr{P}(X))$.*

**Proof** We prove it for $\bigcap$ only; $\bigcup$ is similar. If we can prove that the subset

$$R = \left\{(\mathscr{U}, B) \in \mathscr{P}(\mathscr{P}(X)) \times \mathscr{P}(X) : \bigcap \mathscr{U} = B\right\}$$

of $\mathscr{P}(\mathscr{P}(X)) \times \mathscr{P}(X)$ exists then the result follows by the usual argument: $R$ is then functional, so it is the graph of a function, which has the desired property of mapping $\mathscr{U}$ to $\bigcap \mathscr{U}$.

Recall from Example 5.4.14 that for $\mathscr{U} \in \mathscr{P}(\mathscr{P}(X))$ and $x \in X$,

$$x \in_X \bigcap \mathscr{U} \iff (\forall A \in \mathscr{P}(X))(A \in_{\mathscr{P}(X)} \mathscr{U} \implies x \in_X A).$$

Hence the property $\bigcap \mathscr{U} = B$ of elements $(\mathscr{U}, B)$ of $\mathscr{P}(\mathscr{P}(X)) \times \mathscr{P}(X)$ is equivalent to

$$(\forall x \in X)\big(x \in_X B \iff (\forall A \in \mathscr{P}(X))(A \in_{\mathscr{P}(X)} \mathscr{U} \implies x \in_X A)\big).$$

By the results of Section 5.4, this property specifies a subset of $\mathscr{P}(\mathscr{P}(X)) \times \mathscr{P}(X)$, or equivalently, $\bigcap \mathscr{U} = B$ does too. □

For our final illustration of specifying functions via their graphs, we consider corestriction, the lesser-known cousin of restriction.

Let $f : X \to Y$ be a function. For a subset $A \overset{i}{\hookrightarrow} X$, the **restriction** of $f$ to $A$ is $f \circ i : A \to Y$. So, restriction just replaces the domain of a function by a subset, without affecting what the function does to elements.

**Example 5.7.7** The restriction of the squaring function $\mathbb{C} \to \mathbb{C}$ (given by $z \mapsto z^2$) to $\mathbb{R} \subseteq \mathbb{C}$ is the squaring function $\mathbb{R} \to \mathbb{C}$.

But what about changing the *co*domain? For example, the squaring function $s : \mathbb{R} \to \mathbb{C}$ satisfies $s(x) \in_{\mathbb{C}} \mathbb{R}$ for all $x \in \mathbb{R}$, so shouldn't we be able to shrink the codomain from $\mathbb{C}$ to $\mathbb{R}$? Of course, changing the codomain changes the function, but with that understood, the answer is yes:

**Lemma 5.5.8** *Let $f : X \to Y$ be a function. Let $B \overset{j}{\hookrightarrow} Y$ be a subset such that* $\operatorname{im} f \subseteq_Y B$. *Then there is a unique function $f' : X \to B$ such that $j(f'(x)) = f(x)$ for all $x \in X$.*

The function $f'$ is called the **corestriction** of $f$ to $B$. In less fussy notation, not writing the inclusion function, the equation says $f'(x) = f(x)$ for all $x \in X$.

**Proof** As usual, uniqueness is immediate since a function is determined by its effect on elements. For existence, the subset

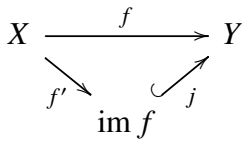
$$R = \{(x, b) \in X \times B : f(x) = j(b)\}$$

of $X \times B$ exists, since it is the pullback of $f$ and $j$, which we have already constructed (Example 5.4.5(iii)). Since $\operatorname{im} f \subseteq_Y B$, the relation $R$ is functional, so it is the graph of a function $f' : X \to B$, which then has the property required. □

**Example 5.5.9** Let $s : \mathbb{R} \to \mathbb{C}$ be the squaring function. Since $x^2 \in_{\mathbb{C}} \mathbb{R}$ for all $x \in \mathbb{R}$, there is a unique function $s' : \mathbb{R} \to \mathbb{R}$ such that $j(s'(x)) = x^2$ for all $x \in \mathbb{R}$ (where $j : \mathbb{R} \hookrightarrow \mathbb{C}$ is the inclusion)—or more casually, $s'(x) = x^2$ for all $x \in \mathbb{R}$. This function $s'$ is the corestriction of $s$ to $\mathbb{R}$.

A special case is important:

**Proposition 5.5.10** *Let $f : X \to Y$ be a function. Write $j$ for the inclusion $\operatorname{im} f \hookrightarrow Y$. Then there is a unique function $f' : X \to \operatorname{im} f$ such that the triangle*




*commutes, and $f'$ is surjective.*

**Proof** This is the case of Lemma 5.5.8 where $B = \operatorname{im} f$. That $f'$ is surjective follows from the definition of $\operatorname{im} f$. □

**Corollary 5.5.11** *Every function can be expressed as the composite of a surjection followed by an injection.* □

**Exercise 5.5.12** How can the squaring function $\mathbb{R} \to \mathbb{R}$ be expressed as a surjection followed by an injection?

# Chapter 6

# Gluing

*To read by Monday 21 October: Sections 6.1 and 6.2.*
*To read by Friday 25 October: Sections 6.3–6.5.*

Sets can be 'glued' in several ways. Elements of a single set can be glued to each other, which means taking the quotient by an equivalence relation. Two sets can be glued together, without overlap, to form a new set called their disjoint union or coproduct. We can also think about assembling any family of sets (finitely or infinitely many) into one big set.

A gluing argument is used to prove the first theorem of the course that I think qualifies as surprising, or at least not obvious. The Cantor–Bernstein theorem says that given two sets $X$ and $Y$, if there exist injections $X \to Y$ and $Y \to X$, then there exists a bijection between $X$ and $Y$. This is clear enough for finite sets, but not in general. If you think it's obvious, and your argument involves the concept of 'same number of elements' or 'same cardinality', ask yourself how exactly you'd define that concept!

We will also prove the first isomorphism theorem for sets—a grandparent of the famous result for groups and rings.

From this chapter onwards, I will usually drop the subscripts on $\in$ and $\subseteq$ introduced in Section 4.1. That is, I will write $\in$ for both types of membership, previously written as $\in$ and $\in_X$, and $\subseteq$ for both types of subset relation, previously written as $\subseteq$ and $\subseteq_X$. And I will often omit names of subset inclusions. For example, if $A \subseteq X$ and $a \in A$, I will often write $a \in X$ rather than the strictly correct $i(a) \in X$ (where $i$ is the inclusion $A \hookrightarrow X$).

I will also make free use of the methods for specifying subsets and functions that we developed in Chapter 5, usually without mentioning it.

## 6.1 Equivalence relations

You already know about equivalence relations, but in this section and the next, we will revisit them in our rigorous, axiomatic way. We will also prove some fundamental results that are probably new to you.

**Definition 6.1.1** An **equivalence relation** on a set $X$ is a reflexive, transitive, symmetric relation on $X$.

**Examples 6.1.2**

i. The identity relation $\Delta_X$ on a set $X$ is an equivalence relation. It can also be written as $=$, since $xRy \iff x = y$.

ii. The trivial relation $X \times X$ on a set $X$ is an equivalence relation. Writing it as $\sim$, we have $x \sim y$ for all $x, y \in X$.

iii. Let $n \in \mathbb{N}$. There is an equivalence relation $\equiv_n$ on $\mathbb{Z}$ defined by $x \equiv_n y$ if and only if $x \equiv y \pmod{n}$, that is, $x - y$ is an integer multiple of $n$.

iv. A very important example: any function $f : X \to Y$ gives rise to an equivalence relation $\sim_f$ on $X$, where $x \sim_f x'$ if and only if $f(x) = f(x')$. We call $\sim_f$ the equivalence relation **induced** by $f$. As we will see, *every* equivalence relation on every set arises in this way.

Let's check that $\sim_f$ really is an equivalence relation on $X$. First, it's a *relation* on $X$, that is, the subset

$$\{(x, x') \in X \times X : f(x) = f(x')\}$$

of $X \times X$ exists. This follows from the results of Section 5.4. (Specifically, it's the pullback of $f$ and $f$: Example 5.4.5(iii).) That it's an *equivalence* relation on $X$ follows from the fact that equality is an equivalence relation on $Y$; for instance, it is symmetric because if $f(x) = f(x')$ then $f(x') = f(x)$!

v. A random example: let $X$ be a set and $a, b \in X$. Then

$$\{(x, y) \in X \times X : x = y \text{ or } (x, y) = (a, b) \text{ or } (x, y) = (b, a)\}$$

is an equivalence relation on $X$ (Figure 6.1). It's a relation on $X$ by the results of Section 5.4, and you can check it's reflexive, transitive and symmetric by going through the various cases.

vi. A non-examinable example: let $G$ be a group and $N$ a normal subgroup. There is an equivalence relation $\sim$ on $G$ defined by $g \sim h \iff g^{-1}h \in N$ $(g, h \in G)$. Similarly, given a ring $R$ and an ideal $I$, there is an equivalence relation $\sim$ on $R$ defined by $r \sim s \iff s - r \in I$ $(r, s \in R)$.

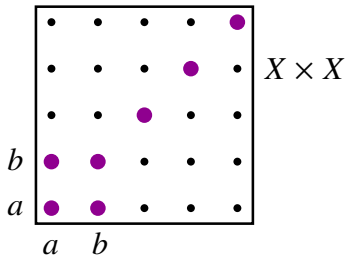



Figure 6.1: The equivalence relation $\sim$ of Example 6.1.2(v), for a five-element set $X$. Pairs $(x, y)$ such that $x \sim y$ are shown as large purple dots.

**Exercise 6.1.3** Looking at Example 6.1.2(iii), where have you met $\equiv_1$ and $\equiv_0$ before?

Sometimes we have a relation $R$ that is not an equivalence relation, but we want to turn it into one—that is, form the smallest equivalence relation $\sim$ that contains $R$. By 'contains' I mean that $xRy \implies x \sim y$, or equivalently, $R \subseteq \sim$. By 'smallest', I mean that any other equivalence relation containing $R$ must also contain $\sim$. You can think of this as similar to taking the span of a subset of $\mathbb{R}^n$, which is the smallest linear subspace containing that subset.

How do we know that there *is* a smallest equivalence relation containing a given relation? The following little result is the key.

**Lemma 6.1.4** *The intersection of any set of equivalence relations is an equivalence relation. That is, let $X$ be a set, let $\mathscr{E} \subseteq \mathscr{P}(X \times X)$, and suppose that each element $E \in \mathscr{E}$ is an equivalence relation on $X$. Then $\bigcap \mathscr{E}$ is an equivalence relation on $X$.*

When you read this sort of statement, the first thing you should do is check it makes sense. By 'makes sense' I don't mean *true*, but that it's a meaningful statement capable of being true or false. In particular, I highly recommend checking through the types of all the objects involved.

Here, $\mathscr{E}$ is a subset of $\mathscr{P}(X \times X)$, which means it is a subset of the set of all relations on $X$. So each element $E$ of $\mathscr{E}$ is a relation on $X$. Hence it is legitimate to suppose that each such $E$ is an *equivalence* relation on $X$. (It wouldn't be, for instance, if $E$ was an element of $X$.) Then $\bigcap \mathscr{E}$, defined in Example 5.4.14, is also a subset of $X \times X$, that is, a relation on $X$. So again, it makes sense to say that it is an equivalence relation.

**Proof** Write $S = \bigcap \mathscr{E} \subseteq X \times X$. I will prove that $S$ is transitive, and leave reflexivity and symmetry to you. Let $x, y, z \in X$ with $(x, y), (y, z) \in \bigcap \mathscr{E}$. We must show that $(x, z) \in \bigcap \mathscr{E}$, or equivalently that $(x, z) \in E$ for all $E \in \mathscr{E}$.

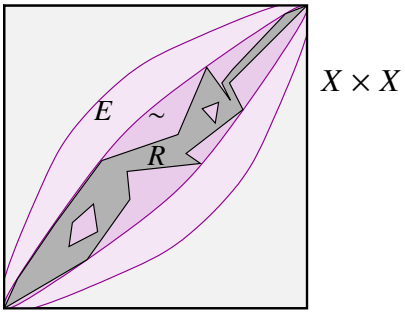



Figure 6.2: The equivalence relation $\sim$ generated by a relation $R$, and another equivalence relation $E$ containing $R$.

So, let $E \in \mathscr{E}$. Since $(x, y) \in \bigcap \mathscr{E}$, we have $(x, y) \in E$. Similarly, $(y, z) \in E$. Since $E$ is an equivalence relation, it is transitive, so $(x, z) \in E$, as required. □

**Definition 6.1.5** Let $R$ be a relation on a set $X$. The **equivalence relation generated by** $R$ is the intersection of all equivalence relations on $X$ containing $R$.

That is, the equivalence relation generated by $R$ is

$$\bigcap \{E \in \mathscr{P}(X \times X) : E \text{ is an equivalence relation on } X \text{ and } R \subseteq E\}. \tag{6.1}$$

This description might seem hard to work with, because it involves considering *all* the equivalence relations containing our original relation $R$. In Workshop 4, we'll derive a more concrete description of the equivalence relation generated by a relation. But for now, let's just check that the definition does what we hope and work through an example.

**Lemma 6.1.6** *Let $R$ be a relation on a set $X$, and let $\sim$ be the equivalence relation on $X$ generated by $R$. Then:*

*i. $\sim$ is an equivalence relation containing $R$;*

*ii. any equivalence relation containing $R$ also contains $\sim$.*

In a nutshell, $\sim$ is the smallest equivalence relation containing $R$ (Figure 6.2).

**Proof** For (i), $\sim$ is an equivalence relation by Lemma 6.1.4, and it contains $R$ because it is the intersection (6.1) of subsets of $X \times X$ that each contain $R$.

For (ii), let $E$ be an equivalence relation on $X$ containing $R$. Then $E$ is one of the subsets of $X \times X$ that we took the intersection of to define $\sim$ (see (6.1)), so $\sim$ is a subset of $E$. □

There can only be *one* smallest equivalence relation containing $R$, since if we have two smallest equivalence relations containing $R$ then each contains the other, which implies that they're equal. So Lemma 6.1.6 uniquely characterizes the equivalence relation generated by $R$.

**Example 6.1.7** Consider the relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : b = a + 7\}$$

on $\mathbb{Z}$. I claim that the equivalence relation on $\mathbb{Z}$ generated by $\mathbb{R}$ is $\equiv_7$, congruence mod 7 (Example 6.1.2(iii)).

By the comments above, it's enough to show that $\equiv_7$ is the smallest equivalence relation containing $R$. It's certainly an equivalence relation, and it contains $R$ since if $b = a + 7$ then $a \equiv_7 b$.

Now let $E$ be any equivalence relation on $\mathbb{Z}$ containing $R$, that is, satisfying $aEb$ whenever $b = a + 7$. We have to prove that $E$ contains $\equiv_7$, that is, $aEb$ whenever $a \equiv b \pmod 7$. So, let $a, b \in \mathbb{Z}$ with $a \equiv b \pmod 7$. There are three cases.

- If $a = b$ then $aEb$, since $E$ is reflexive.
- Suppose that $a < b$. Since $xEy$ whenever $y = x + 7$, we can prove by induction that $xEy$ whenever $y = x + 7k$ for some integer $k > 0$, using the transitivity of $E$. (We will establish the principle of proof by induction in Chapter 7.) Since $a < b$, we have $b = a + 7k$ for some integer $k > 0$, and so $aEb$.
- Suppose that $a > b$. We have $b \equiv a \pmod 7$ with $b < a$, so by the previous bullet point, $bEa$. But $E$ is symmetric, so $aEb$.

In all cases, $aEb$, as required.

**Exercise 6.1.8** Let $X$ be a set and $a, b \in X$. Prove that the equivalence relation generated by $\{(a, b)\} \subseteq X \times X$ is the equivalence relation $\sim$ of Example 6.1.2(v).

## 6.2 Quotients

When you take a piece of string and glue the ends together to form a loop, or (more mathematically) when you take the real interval $[0, 1]$ and declare 0 to be equivalent to 1, you're forming a quotient. When you take $\mathbb{Z}$ and declare that integers differing by a multiple of 5 are to be seen as equal, you're forming a

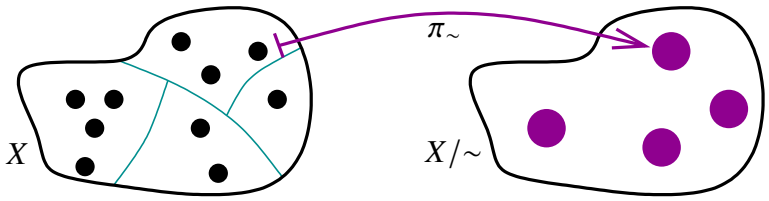



Figure 6.3: An equivalence relation $\sim$ on a set $X$, with four equivalence classes; the four-element quotient set $X/\sim$; and the effect of the natural surjection $\pi_\sim : X \to X/\sim$ on an element of $X$.

quotient. Generally, forming a quotient of a set means gluing some of its elements to each other.

The theories of quotient groups, rings and topological spaces involve algebraic and topological considerations. But underneath it all is a fundamental process: forming a quotient of a set. The idea is that given an equivalence relation $\sim$ on a set $X$, we glue all the elements of $X$ that are equivalent into a single blob, resulting in a new set $X/\sim$ (Figure 6.3). This quotient set $X/\sim$ can be seen as a kind of coarsening of $X$.

Let $E$ be an equivalence relation on a set $X$. The **equivalence class** of an element $x \in X$ is the subset $E[x]$ of $X$, as defined in Lemma 5.1.11. By that lemma, the $X$-elements of $E[x]$ are the elements $y \in X$ equivalent to $x$.

When we are writing our equivalence relation as $\sim$, we denote the equivalence class of $x$ by $[x]_\sim$ or just $[x]$.

**Examples 6.2.1**

i. When $\sim$ is equality on a set $X$ (Example 6.1.2(i)), $[x] = \{x\}$ for all $x \in X$.

ii. When $\sim$ is the trivial relation on a set $X$ (Example 6.1.2(ii)), $[x] = X$ for all $x \in X$.

iii. Let $n \in \mathbb{N}$ and consider congruence mod $n$ as an equivalence relation $\equiv_n$ on $\mathbb{Z}$ (Example 6.1.2(iii)). Then $[x] = \{y \in \mathbb{Z} : x \equiv y \pmod{n}\}$ for all $x \in \mathbb{Z}$. For example, if $n = 5$ then $[7] = \{\ldots, -3, 2, 7, 12, \ldots\}$.

iv. A function $f : X \to Y$ induces an equivalence relation $\sim_f$ on $X$ (Example 6.1.2(iv)). The equivalence class of $x \in X$ is $\{x' \in X : f(x) = f(x')\} = f^{-1}f\{x\}$. As in Warning 4.4.14, this is typically larger than $\{x\}$.

v. A non-examinable example: let $G$ be a group and take the equivalence relation on $G$ associated with a normal subgroup $N$ of $G$ (Example 6.1.2(vi)). Then the equivalence classes are the cosets of $N$. The same goes for rings and ideals.

**Exercise 6.2.2** What are the equivalence classes of the equivalence relation of Example 6.1.2(v)?

**Lemma 6.2.3** *Let $\sim$ be an equivalence relation on a set $X$. Then for $x, y \in X$,*

$$x \sim y \iff [x] = [y].$$

**Proof** Suppose that $x \sim y$. We have to prove that for $z \in X$,

$$z \in [x] \iff z \in [y].$$

If $z \in [x]$ then $x \sim z$ (by definition of $[x]$). Also, $y \sim x$ (since $x \sim y$ and $\sim$ is symmetric). We now have $y \sim x$ and $x \sim z$, and $\sim$ is transitive, so $y \sim z$. That is, $z \in [y]$. The converse is similar.

Now suppose that $[x] = [y]$. Since $\sim$ is reflexive, $y \in [y]$. Hence $y \in [x]$, that is, $x \sim y$. □

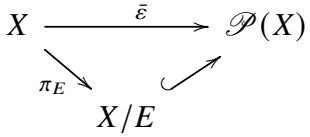
**Exercise 6.2.4** Supply the missing part of that proof, where I wrote 'The converse is similar'.

Let $E$ be an equivalence relation on a set $X$. As we saw in the proof of Lemma 5.1.11, $E$ corresponds to a function

$$\begin{array}{rccc} \bar{\varepsilon}\colon & X & \to & \mathscr{P}(X) \\ & x & \mapsto & E[x]. \end{array}$$

Define $X/E$, the **quotient of $X$ by $E$**, to be the image of $\bar{\varepsilon}$. That is, $X/E$ is the subset of $\mathscr{P}(X)$ whose elements are the equivalence classes. Or more simply still, $X/E$ is the set of equivalence classes!

By Proposition 5.5.10, there is a unique function $\pi_E\colon X \to X/E$ such that $\pi_E(x) = E[x]$ for all $x \in X$; that is, the diagram




commutes. This function $\pi_E\colon X \to X/E$ is surjective by Proposition 5.5.10 (or concretely, because every equivalence class is the equivalence class of something). We call $\pi_E$ the **natural surjection**; it is also known as the **canonical surjection** or **quotient map**.

So: an equivalence relation $\sim$ on a set $X$ gives rise to a set $X/\sim$ and a surjection

$$\begin{array}{rccc} \pi_\sim\colon & X & \to & X/\sim \\ & x & \mapsto & [x]_\sim. \end{array}$$

Here's the crucial property of the natural surjection (Figure 6.4).

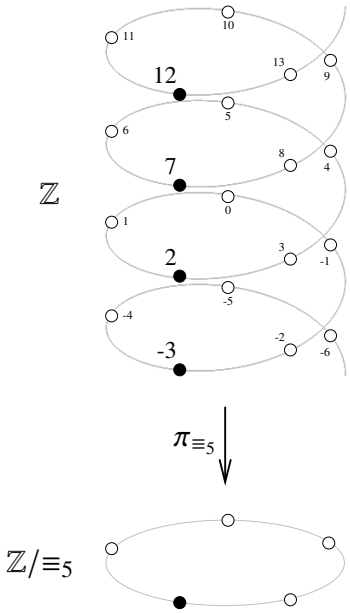



Figure 6.4: Congruence mod 5 as an equivalence relation $\equiv_5$ on $\mathbb{Z}$. The figure shows the quotient $\mathbb{Z}/\equiv_5$ and the natural surjection $\pi_{\equiv_5}$ with one fibre highlighted. The fibres of the natural surjection are the equivalence classes.

**Lemma 6.2.5** *Let $\sim$ be an equivalence relation on a set $X$. Then for $x, y \in X$,*

$$\pi_\sim(x) = \pi_\sim(y) \iff x \sim y.$$

**Proof** This is immediate from Lemma 6.2.3. □

Lemma 6.2.5 states that the equivalence relation $\sim_{\pi_\sim}$ induced by $\pi_\sim$ (Example 6.1.2(iv)) is $\sim$ itself. So we have now proved the claim made in that example: every equivalence relation on $X$ is the equivalence relation $\sim_f$ induced by some function $f$ out of $X$.

Now that we have Lemma 6.2.5, *we can completely forget the construction of $X/\sim$ as a set of equivalence classes*. Everything we need to know is contained in the statement that $\pi_\sim : X \to X/\sim$ is a surjection whose induced equivalence relation is $\sim$. The theorems and proofs that follow will demonstrate that.

**Digression 6.2.6** If you *want* to think of the elements of a quotient group as being cosets, you can, but you don't *need* to. All that matters about the group $G/N$ is that it comes with a surjection $\pi : G \to G/N$ whose kernel is $N$ (or equivalently, such that $\pi(g) = \pi(h) \iff g^{-1}h \in N$, for $g, h \in G$). The same goes for quotient rings, vector spaces and modules.

**Examples 6.2.7** i. Let $\sim$ be equality on a set $X$. Then $\pi_\sim : X \to X/\sim$ is an isomorphism.

ii. Let $\sim$ be the trivial relation $X \times X$ on a set $X$. Then $X/\sim$ is a one-element set and $\pi_\sim$ is the unique function $X \to X/\sim$.

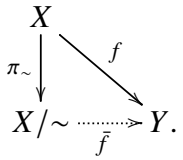
iii. Let $n \in \mathbb{N}$. Then $\mathbb{Z}/\equiv_n$ is the set $\mathbb{Z}/n\mathbb{Z}$ of integers mod $n$, and $\pi_{\equiv_n}(x)$ is the congruence class of $x$ mod $n$.

**Proposition 6.2.8 (Universal property of quotients)** *Let $\sim$ be an equivalence relation on a set $X$. Let $Y$ be a set and $f : X \to Y$ a function such that for $x, x' \in X$,*

$$x \sim x' \implies f(x) = f(x').$$

*Then there is a unique function $\bar{f} : X/\sim \to Y$ such that $\bar{f}(\pi_\sim(x)) = f(x)$ for all $x \in X$.*

The conclusion can be expressed in a commutative diagram:




**Proof** *Uniqueness:* This follows from $\pi_\sim$ being surjective.

*Existence:* Let

$$R = \big\{(\xi, y) \in (X/\sim) \times Y : (\exists x \in X)(\xi = \pi_\sim(x) \text{ and } y = f(x))\big\}.$$

That is, $R \subseteq (X/\sim) \times Y$ consists of all pairs $(\pi_\sim(x), f(x))$ with $x \in X$. I claim that $R$ is a functional relation between $X/\sim$ and $Y$.

To prove this, let $\xi \in X/\sim$. We have to show that there exists a unique element $y \in Y$ such that $(\xi, y) \in R$.

- *Existence:* Since $\pi_\sim$ is surjective, $\xi = \pi_\sim(x)$ for some $x \in X$, and then $(\xi, f(x)) \in R$.
- *Uniqueness:* Let $y, y' \in Y$ with $(\xi, y), (\xi, y') \in R$. Then there exist $x, x' \in X$ such that

  $$(\xi, y) = (\pi_\sim(x), f(x)), \qquad (\xi, y') = (\pi_\sim(x'), f(x')).$$

  Now $\pi_\sim(x) = \xi = \pi_\sim(x')$, so $x \sim x'$ by Lemma 6.2.5, so $f(x) = f(x')$ by hypothesis. Hence $y = y'$, as required.

This proves the claim that $R$ is a functional relation. Hence $R = \Gamma_{\bar{f}}$ for some function $\bar{f} : X/\sim \to Y$. And by construction, $\bar{f}(\pi_\sim(x)) = f(x)$ for all $x \in X$. □

**Exercise 6.2.9** At the start of the proof, how exactly does uniqueness follow from $\pi_\sim$ being surjective?

When you see the strange term 'well defined' in a mathematics text, it's usually a signal that Proposition 6.2.8 is needed. The pattern is this: someone makes a definition, then they say 'Oops! Maybe that's not a valid definition, because it looks like it depends on a choice of representative of some equivalence class. So we'd better check it doesn't, i.e. it's well defined.' This is not mathematical rigour's finest hour. Proposition 6.2.8 puts everything on a firm footing, as the following example shows.

**Example 6.2.10** Consider squaring of integers mod $n$, where $n \in \mathbb{N}$ is fixed. We want to define it by $[x]^2 = [x^2]$ $(x \in \mathbb{Z})$, but is this a valid definition? Rigorously: does there exist a function $s\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ such that $s([x]) = [x^2]$ for all $x \in \mathbb{Z}$?

Let us apply Proposition 6.2.8, taking $X = \mathbb{Z}$ and $f$ to be the composite

$$\mathbb{Z} \xrightarrow{x \mapsto x^2} \mathbb{Z} \xrightarrow{\pi_{\equiv_n}} \mathbb{Z}/n\mathbb{Z}.$$

A short piece of algebra shows that

$$x \equiv_n x' \implies f(x) = f(x')$$

for all $x, x' \in \mathbb{Z}$, or concretely,

$$x \equiv x' \pmod{n} \implies x^2 \equiv x'^2 \pmod{n}.$$

(This is the step where an author usually says they're checking their definition is 'well-defined'.) Hence Proposition 6.2.8 can be applied. It implies that there exists a unique function $\bar{f}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ such that $\bar{f}(\pi_{\equiv_n}(x)) = f(x)$ for all $x \in \mathbb{Z}$, that is, $\bar{f}([x]) = [x^2]$ for all $x \in \mathbb{Z}$. So $\bar{f}$ is exactly the squaring function $s$ that we wanted to construct.

A similar example can be given for multiplication mod $n$.

**Theorem 6.2.11 (First isomorphism theorem)** *Let $X$ and $Y$ be sets, and let $f\colon X \to Y$ be a surjection. Then there is a unique isomorphism $\bar{f}\colon X/{\sim_f} \to Y$ such that $\bar{f}(\pi_{\sim_f}(x)) = f(x)$ for all $x \in X$. In particular, $X/{\sim_f} \cong Y$.*

So, every surjection is the natural surjection of some equivalence relation. Recall that $\sim_f$ denotes the equivalence relation on $X$ induced by $f$ (Example 6.1.2(iv)). Diagram:

$$\begin{array}{ccc} X & & \\ {\scriptstyle \pi_{\sim_f}}\downarrow & \searrow^{f} & \\ X/{\sim_f} & \overset{\bar{f}}{\dashrightarrow}_{\cong} & Y. \end{array}$$

**Proof** By definition of $\sim_f$, we have

$$x \sim_f x' \iff f(x) = f(x') \tag{6.2}$$

for all $x, x' \in X$. Hence by Proposition 6.2.8, there is a unique *function* $\bar{f}\colon X/\!\sim_f \to Y$ such that $\bar{f}(\pi_{\sim_f}(x)) = f(x)$ for all $x \in X$. It remains to prove that $\bar{f}$ is an isomorphism, or equivalently, bijective. Write $\pi$ for $\pi_{\sim_f}$.

Surjectivity holds because $\bar{f} \circ \pi = f$ and $f$ is surjective. (See Workshop 1, question 8(ii).) For injectivity, let $\xi, \xi' \in X/\!\sim_f$ with $\bar{f}(\xi) = \bar{f}(\xi')$. We have $\xi = \pi(x)$ and $\xi' = \pi(x')$ for some $x, x' \in X$, and then $\bar{f}(\pi(x)) = \bar{f}(\pi(x'))$, so $f(x) = f(x')$. Hence by (6.2), $x \sim_f x'$, giving $\xi = \xi'$. □

A question on Workshop 3 invites you to use the first isomorphism theorem for sets as a step in proving the first isomorphism theorem for groups or rings.

**Example 6.2.12** Let $f\colon \mathbb{N} \to \{0,1,2,3,4,5,6,7,8,9\}$ be the function assigning to a natural number the last digit of its decimal expansion. (Among the various things here that we haven't defined yet is the list notation in the codomain.) Certainly $f$ is surjective. One can show that $f(x) = f(x') \iff x \equiv x' \pmod{10}$, for $x, x' \in \mathbb{N}$. So the first isomorphism theorem implies that $\mathbb{N}/\!\equiv_{10} \cong \{0, 1, \ldots, 9\}$.

**Digression 6.2.13** We've seen that subsets of a set $X$ correspond to injections into $X$, taken up to isomorphism over $X$. Dually, equivalence relations on a set $X$ correspond to surjections out of $X$, taken up to isomorphism 'under $X$'. (Functions $f\colon X \to Y$ and $f'\colon X \to Y'$ are **isomorphic under** $X$ if there exists an isomorphism $j\colon Y \to Y'$ such that $jf = f'$.)

This correspondence works as follows.

- An equivalence relation $\sim$ on $X$ gives a surjection $\pi_\sim\colon X \to X/\!\sim$.
- A surjection $f\colon X \to Y$ induces an equivalence relation $\sim_f$ on $X$.
- Starting with an equivalence relation $\sim$ on $X$, then taking its natural surjection $\pi_\sim$, then taking *its* induced equivalence relation $\sim_{\pi_\sim}$ gets us back to our original equivalence relation $\sim$, by Lemma 6.2.5.
- Finally, starting with a surjection $f\colon X \to Y$, then taking its induced equivalence relation $\sim_f$, then taking *its* natural surjection $\pi_{\sim_f}\colon X \to X/\!\sim_f$ gets us back to something isomorphic under $X$ to our original surjection $f$, by the first isomorphism theorem.

## 6.3 Disjoint unions and coproducts

You already know that sets can be multiplied. Here we will see that they can also be added (Figure 6.5).

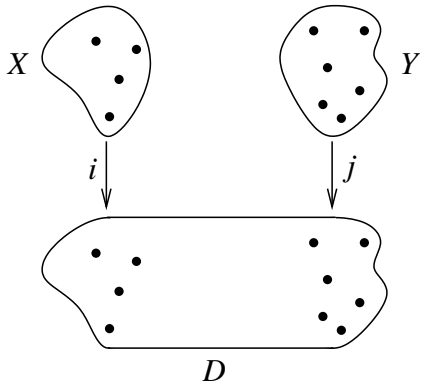



Figure 6.5: Disjoint union $D$ of sets $X$ and $Y$.

**Definition 6.3.1** A **disjoint union diagram** consists of sets and functions

$$X \xrightarrow{i} D \xleftarrow{j} Y \tag{6.3}$$

with the following properties:

i. $i$ and $j$ are injective;

ii. the union of $X \xrightarrow{i} D$ and $Y \xrightarrow{j} D$ (seen as subsets of $D$) is $D$;

iii. the intersection of $X \xrightarrow{i} D$ and $Y \xrightarrow{j} D$ is empty (they are **disjoint**).

Put another way, given injections $X \xhookrightarrow{i} D$ and $Y \xhookrightarrow{j} D$ into a set $D$, the diagram (6.3) is a disjoint union diagram if and only if every element of $D$ belongs to exactly one of $X$ and $Y$. That is, for all $d \in D$, we have $d \in X$ or $d \in Y$, but not both. A further equivalent condition is that $Y = D \setminus X$ (by Lemma 4.3.7), or equivalently again, that $X = D \setminus Y$.

**Exercise 6.3.2** Persuade yourself that if $X$ and $Y$ are finite sets with $m$ and $n$ elements respectively, then a disjoint union of $X$ and $Y$ should have $m + n$ elements.

For a disjoint union diagram (6.3), we say that $D$ (together with $i$ and $j$) is a **disjoint union** of $X$ and $Y$.

Examples of disjoint unions are easy to come by: take any set $D$ and any subset $X \subseteq D$, then put $Y = D \setminus X$. But here's a harder question: if I give you two sets $X$ and $Y$, can you find a set $D$ that is a disjoint union of $X$ and $Y$?

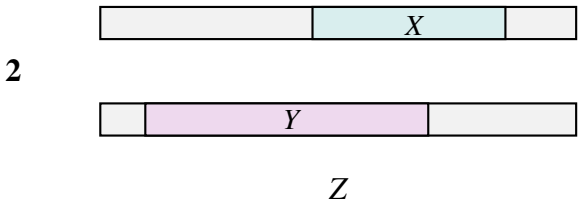



Figure 6.6: Proof strategy for Proposition 6.3.4. We find a set $Z$ into which both $X$ and $Y$ embed, then show that the union of the shaded subsets of $\mathbf{2} \times Z$ is a disjoint union of $X$ and $Y$.

**Warning 6.3.3** 'Let $D = X \cup Y$' is not a valid answer, for two reasons.

First, we haven't defined the union of two sets. We've only defined the union of two *subsets* of a set (Definition 4.3.4). In our current situation, it's not even clear that there's any set containing both $X$ and $Y$ as subsets.

Second, the concept of the union of two sets makes no sense in an isomorphism-invariant world. For instance, if $X$ has two elements and $Y$ has three, how many elements should their union have? Certainly at most five, but it will be fewer than five if one of the elements of $X$ happens to be 'equal' to one of the elements of $Y$. And whether elements of one set are 'equal' to elements of another depends on their names, so it's not invariant under isomorphism. (I put 'equal' in inverted commas because we never ask whether an element of one set is equal to an element of another, for the same reason; see Section 1.7.) A similar point was made for intersections in Digression 4.3.1.

We'll show now that every pair of sets *does* have a disjoint union. The idea is that it's easy to find a disjoint union of a set $Z$ with *itself*, namely, $\mathbf{2} \times Z$. After all, $\mathbf{2} \times Z$ is the union of disjoint subsets $\{\mathsf{T}\} \times Z$ and $\{\mathsf{F}\} \times Z$, each isomorphic to $Z$. And for arbitrary sets $X$ and $Y$, if we can find any common set $Z$ into which $X$ and $Y$ both embed (not necessarily disjointly) then we should be able to find a disjoint union of them in the way suggested by Figure 6.6.

**Proposition 6.3.4** *Every pair of sets has a disjoint union.*

**Proof** Let $X$ and $Y$ be sets. The proof proceeds in three steps.

First we show that there exist a set $Z$ and injections $X \xrightarrow{k} Z \xleftarrow{\ell} Y$. If $X$ is empty, take $Z = Y$ and $\ell = \mathrm{id}_Y$ (and $k$ to be the one and only function $X \to Z$). Similarly, if $Y$ is empty, take $Z = X$ and $k = \mathrm{id}_X$. If both are nonempty, choose

elements $a \in X$ and $b \in Y$, put $Z = X \times Y$, and take

$$\begin{array}{rccc} k\colon & X & \to & X \times Y \\ & x & \mapsto & (x, b), \end{array} \qquad \begin{array}{rccc} \ell\colon & Y & \to & X \times Y \\ & y & \mapsto & (a, y). \end{array}$$

This completes the first step.

Second, we show that $X$ and $Y$ embed *disjointly* into some set. Define

$$\begin{array}{rccc} m\colon & X & \to & \mathbf{2} \times Z \\ & x & \mapsto & (\mathsf{T}, k(x)), \end{array} \qquad \begin{array}{rccc} n\colon & Y & \to & \mathbf{2} \times Z \\ & x & \mapsto & (\mathsf{F}, \ell(x)). \end{array}$$

Then $m$ and $n$ are injective since $k$ and $\ell$ are, and the subsets $X \overset{m}{\hookrightarrow} \mathbf{2} \times Z$ and $Y \overset{n}{\hookrightarrow} \mathbf{2} \times Z$ of $\mathbf{2} \times Z$ are disjoint since $\mathsf{T} \neq \mathsf{F}$.

Third, let $D \subseteq \mathbf{2} \times Z$ be the union of the subsets $X \overset{m}{\hookrightarrow} \mathbf{2} \times Z$ and $Y \overset{n}{\hookrightarrow} \mathbf{2} \times Z$. Let $i\colon X \to D$ be the corestriction of $m$ to $D$. (Corestriction was defined in Lemma 5.5.8. Concretely, if we leave the inclusion $D \hookrightarrow \mathbf{2} \times Z$ nameless then $i(x) = m(x)$ for all $x \in X$.) Similarly, let $j\colon Y \to D$ be the corestriction of $n$ to $D$. Then $i$ and $j$ are injective since $m$ and $n$ are. Also, the union of the subsets $X \overset{i}{\hookrightarrow} D$ and $Y \overset{j}{\hookrightarrow} D$ is $D$ (by construction), and their intersection is empty by the previous paragraph. Hence $X \overset{i}{\to} D \overset{j}{\leftarrow} Y$ is a disjoint union diagram. □

We would like to be able to define functions in a case-by-case way, as in the following example.

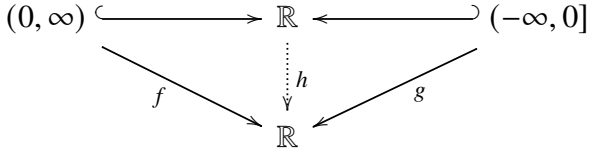
**Example 6.3.5** We want to be able to define a function $h\colon \mathbb{R} \to \mathbb{R}$ by

$$h(t) = \begin{cases} t \sin(1/t) & \text{if } t > 0, \\ 0 & \text{if } t \leq 0 \end{cases} \tag{6.4}$$

($t \in \mathbb{R}$). Assume here that we have already defined the set $\mathbb{R}$, the subsets $(0, \infty)$ and $(-\infty, 0]$, and the functions

$$\begin{array}{rccc} f\colon & (0,\infty) & \to & \mathbb{R} \\ & x & \mapsto & x \sin(1/x), \end{array} \qquad \begin{array}{rccc} g\colon & (-\infty, 0] & \to & \mathbb{R} \\ & y & \mapsto & 0. \end{array}$$

Since $\mathbb{R}$ is the disjoint union of $(0, \infty)$ and $(-\infty, 0]$, we would like there to be a unique function $h\colon \mathbb{R} \to \mathbb{R}$ such that the diagram




commutes (which is equivalent to equation (6.4)).

This should remind you of something! It looks exactly like the definition of product, but with all the arrows reversed.

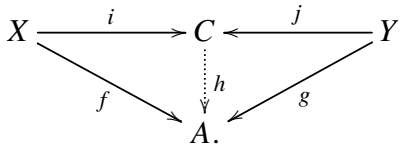
**Definition 6.3.6** Let $X$ and $Y$ be sets. A **coproduct** (or **sum**) of $X$ and $Y$ consists of sets and functions

$$X \xrightarrow{i} C \xleftarrow{j} Y$$

with the following property:

> for all sets $A$ and functions $f\colon X \to A$ and $g\colon Y \to A$, there is a unique function $h\colon C \to A$ such that $h \circ i = f$ and $h \circ j = g$.

In a commutative diagram:




Coproducts are unique up to isomorphism, in the same sense as Lemma 2.6.8 for products and with the same proof, but with all the arrows turned around. And the same conventions are used for coproducts as products: we sometimes refer to $C$ alone as a coproduct of $X$ and $Y$ (even though a coproduct officially consists of $C$ together with $i$ and $j$), and we sometimes call $X \xrightarrow{i} C \xleftarrow{j} Y$ a **coproduct diagram**.

But does every pair of sets *have* a coproduct? We will prove that it does.

**Proposition 6.3.7** *A diagram $X \xrightarrow{i} C \xleftarrow{j} Y$ is a disjoint union diagram if and only if it is a coproduct diagram.*

**Proof** First suppose that $X \xrightarrow{i} C \xleftarrow{j} Y$ is a disjoint union diagram. Take sets and functions $X \xrightarrow{f} A \xleftarrow{g} Y$. We must prove that there exists a unique function $h\colon C \to A$ such that $h \circ i = f$ and $h \circ j = g$.

*Uniqueness:* Let $h, h'\colon C \to A$ be functions that both have these properties. To prove that $h = h'$, let $c \in C$. Since $C$ is the union of $X \xrightarrow{i} C$ and $Y \xrightarrow{j} C$, we can assume without loss of generality that $c = i(x)$ for some $x \in X$. Then $h(c) = h(i(x)) = f(x) = h'(i(x)) = h'(c)$, so $h(c) = h'(c)$. This holds for all $c \in C$, so $h = h'$.

*Existence:* We will construct $h$ via its graph. Let

$$\begin{aligned} R_1 &= \big\{(c,a) \in C \times A : (\exists x \in X)\big((c,a) = (i(x), f(x))\big)\big\}, \\ R_2 &= \big\{(c,a) \in C \times A : (\exists y \in Y)\big((c,a) = (j(y), g(y))\big)\big\}, \\ R &= R_1 \cup R_2. \end{aligned}$$

(Loosely put, $R$ is the union of the graphs of $f$ and $g$. Suggestion: draw a diagram!) I claim that $R$ is a functional relation between $C$ and $A$. To prove this, let $c \in C$; we must show that there exists a unique $a \in A$ such that $(c, a) \in R$. Since $C$ is the union of $X \xrightarrow{i} C$ and $Y \xrightarrow{j} C$, we can assume without loss of generality that $c = i(x)$ for some $x \in X$, and since $i$ is injective, there is a unique such $x$.

- *Existence:* We have $(i(x), f(x)) \in R_1 \subseteq R$, hence $(c, f(x)) \in R$.
- *Uniqueness:* Let $a \in A$ with $(c, a) \in R$; we will show that $a = f(x)$.

  If $(c, a) \in R_2$ then $(c, a) = (j(y), g(y))$ for some $y \in Y$; but then $i(x) = j(y)$, contradicting the assumption that $X \xrightarrow{i} C$ and $Y \xrightarrow{j} C$ are disjoint. Hence $(c, a) \in R_1$. This means $(c, a) = (i(x'), f(x'))$ for some $x' \in X$. But then $i(x') = i(x)$, and $i$ is injective, so $x' = x$. Hence $a = f(x') = f(x)$, as claimed.

This completes the proof that $R$ is a functional relation between $C$ and $A$. Hence by Theorem 5.2.4, $R$ is the graph of a function $h\colon C \to A$. For all $x \in X$, we have $(i(x), f(x)) \in \Gamma_h$, so $h(i(x)) = f(x)$. Hence $h \circ i = f$. Similarly, $h \circ j = g$. This completes the proof that $X \xrightarrow{i} C \xleftarrow{j} Y$ is a coproduct diagram.

Conversely, suppose that $X \xrightarrow{i} C \xleftarrow{j} Y$ is a coproduct diagram. By Proposition 6.3.4, there exists a disjoint union diagram $X \xrightarrow{i'} C' \xleftarrow{j'} Y$. By the implication just proved, this is also a coproduct diagram. Since coproducts are unique up to isomorphism, the two diagrams are isomorphic. But $X \xrightarrow{i'} C' \xleftarrow{j'} Y$ is a disjoint union diagram, so it follows that $X \xrightarrow{i} C \xleftarrow{j} Y$ is a disjoint union diagram too. □

**Theorem 6.3.8** *Every pair of sets has a coproduct.*

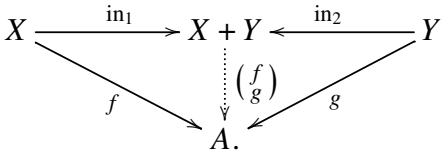
**Proof** Follows from Propositions 6.3.4 and 6.3.7. □

We now know that for all sets $X$ and $Y$, there is exactly one coproduct of $X$ and $Y$, up to isomorphism. So we can speak of *the* coproduct, or equivalently *the* disjoint union. We denote it by

$$X \xrightarrow{\text{in}_1} X + Y \xleftarrow{\text{in}_2} Y,$$

and call $\text{in}_1$ and $\text{in}_2$ the **inclusions** of the coproduct. (They are injective, by Proposition 6.3.7.) Sometimes we write $X \amalg Y$ instead of $X + Y$. Given a set $A$

and functions $X \xrightarrow{f} A \xleftarrow{g} Y$, we write $\binom{f}{g}$ for the unique function $X+Y \to A$ such that the diagram




commutes. (This is the function previously called $h$.)

By now you won't be surprised to learn that we sometimes use more casual notation. Officially, the elements of $X+Y$ are either of the form $\mathrm{in}_1(x)$ for some $x \in X$ or $\mathrm{in}_2(y)$ for some $y \in Y$. But we often leave the inclusions nameless, so that elements of $X+Y$ are called just $x$ or $y$. With this more relaxed notation, $\binom{f}{g}$ is given on elements $z \in X+Y$ by

$$\binom{f}{g}(z) = \begin{cases} f(z) & \text{if } z \in X, \\ g(z) & \text{if } z \in Y. \end{cases}$$

**Warning 6.3.9** This relaxed convention can cause confusion when $X = Y$: given $x \in X$, what would the element '$x$' of $X + X$ mean? You'd have to specify whether you meant the $x$ in the first copy of $X$ or the $x$ in the second.

**Examples 6.3.10** i. Since $\mathbb{R} = (0,\infty) \amalg (-\infty, 0]$, we can define a function $h$ as in Example 6.3.5. In the notation of that example, $h = \binom{f}{g}$.

ii. Sometimes it is useful to adjoin a new element called $\infty$ to the natural numbers. Formally, take the coproduct $\mathbb{N} + \mathbf{1}$ and denote the inclusion $\mathbf{1} \to \mathbb{N} + \mathbf{1}$ by the symbol $\infty$. Then, for instance, it follows from the definition of coproduct that there is a unique function $h\colon \mathbb{N} + \mathbf{1} \to \mathbb{R}$ such that

$$h(n) = \begin{cases} 2^{-n} & \text{if } n \in \mathbb{N}, \\ 0 & \text{if } n = \infty \end{cases}$$

($n \in \mathbb{N}+\mathbf{1}$). Here I have assumed that the function $\mathbb{N} \to \mathbb{R}$ given by $n \mapsto 2^{-n}$ has already been defined.

**Remark 6.3.11** Suppose we start with a set $D$, together with subsets $X$ and $Y$. It either is or isn't the case that $X \cup Y = D$ and $X \cap Y = \varnothing$. If it is, we tend to use the term 'disjoint union' rather than coproduct, and the notation $X \amalg Y$ rather than $X + Y$ for $D$. Example 6.3.10(i) is of this type.

On the other hand, suppose we start with just sets $X$ and $Y$. We can then build their coproduct $X + Y$. Although this *is* a disjoint union of its subsets $X$ and

$Y$, in this situation we tend to use the term 'coproduct' and the notation $X + Y$. Example 6.3.10(ii) is of this type.

So although the terms 'disjoint union' and 'coproduct' are equivalent, as are the symbols $\amalg$ and $+$, we typically use them in different situations.

**Digression 6.3.12** You can usefully compare this situation with direct sums of vector spaces. Although we only have one term, 'direct sum', and one symbol, $\oplus$, there are really two different scenarios.

First, suppose we are given a vector space $D$ with linear subspaces $X$ and $Y$. It either is or isn't the case that $X + Y = D$ and $X \cap Y = \{0\}$. If it is, we call $D$ the direct sum of $X$ and $Y$ and write $D = X \oplus Y$.

On the other hand, suppose we start with just vector spaces $X$ and $Y$. We can then form what is *also* called the direct sum $X \oplus Y$ of $X$ and $Y$; its underlying set is $X \times Y$, and we make it into a vector space by defining $(x, y)+(x', y') = (x+x', y+y')$, etc. It comes with inclusions $X \xrightarrow{i} X \oplus Y \xleftarrow{j} Y$, where $i(x) = (x, 0)$ and $j(y) = (0, y)$.

The two concepts of direct sum are equivalent, in much the same sense that disjoint unions and coproducts of sets are equivalent. This is why it's safe to use the same notation and terminology for both.

In Propositions 2.6.15 and 2.7.12, we started to show that there is an algebra of sets similar to the algebra of numbers, with laws like $(Y \times Z)^X \cong Y^X \times Z^X$. Here are some more such laws, these ones involving $+$.

**Proposition 6.3.13** *Let $X$, $Y$ and $Z$ be sets. Then we have the following isomorphisms.*

*i. Coproduct isomorphisms:*

*(a)* $X + Y \cong Y + X$;

*(b)* $X + \varnothing \cong X$;

*(c)* $(X + Y) + Z \cong X + (Y + Z)$.

*ii. Distributivity isomorphisms:*

*(a)* $X \times (Y + Z) \cong (X \times Y) + (X \times Z)$;

*(b)* $X \times \varnothing \cong \varnothing$.

*iii. Coproduct and function set isomorphisms:*

*(a)* $Z^{X+Y} \cong Z^X \times Z^Y$;

*(b)* $Z^{\emptyset} \cong \mathbf{1}$.

**Proof** The proof is omitted and not for examination. It is long but not difficult. I will sketch a typical argument. To prove

$$X \times (Y + Z) \cong (X \times Y) + (X \times Z),$$

first note that the inclusions $Y \to Y + Z \leftarrow Z$ induce functions

$$X \times Y \to X \times (Y + Z) \leftarrow X \times Z,$$

which in turn give us a function

$$(X \times Y) + (X \times Z) \to X \times (Y + Z).$$

One shows directly that this is bijective, which implies that it is an isomorphism.□

## 6.4 Comparing sizes of sets

What should it mean for one set to be 'bigger' than another? Or to contain 'more' elements? For finite sets it is clear enough, but things become slippery when the sets may be infinite. In this section, we make the fundamental definitions and prove two fundamental results.

**Definition 6.4.1** For sets $X$ and $Y$, write $X \leq Y$ if there exists an injection $X \to Y$.

**Lemma 6.4.2** *i. Let $X$, $Y$ and $Z$ be sets. If $X \leq Y$ and $Y \leq Z$ then $X \leq Z$.*

*ii. Let $X$ and $Y$ be sets. If $X \cong Y$ then $X \leq Y$.*

**Proof** (i) holds because a composite of injections is injective, and (ii) because an isomorphism is injective. □

Here is an equivalent way to define $\leq$.

**Lemma 6.4.3** *Let $X$ and $Y$ be sets. Then $X \leq Y$ if and only if there exists a set $A$ such that $X + A \cong Y$.*

**Proof** First assume that $X \leq Y$, and take an injection $X \hookrightarrow Y$. Let $A \hookrightarrow Y$ be the complement of $X$ in $Y$. Then $Y$ is the disjoint union of $X$ and $A$, so $Y \cong X + A$.

Conversely, if there exists $A$ such that $X + A \cong Y$ then $X \leq Y$, because the inclusion $X \hookrightarrow X + A$ is injective. □

We write $X < Y$ if $X \leq Y$ but $X \not\cong Y$, and we define $\geq$ and $>$ as you would imagine.

Here is the first fundamental result on inequalities between sets.

**Theorem 6.4.4 (Cantor)** *$X < \mathscr{P}(X)$ for all sets $X$.*

**Proof** Let $X$ be a set. The function $\{-\}\colon X \to \mathscr{P}(X)$ (defined in Remark 4.2.5) is injective, so $X \leq \mathscr{P}(X)$.

Now suppose for a contradiction that $X \cong \mathscr{P}(X)$. In particular, there is a surjection $F\colon X \to \mathscr{P}(X)$. Define

$$A = \{x \in X : x \notin F(x)\} \subseteq X.$$

Since $F$ is surjective, $A = F(x)$ for some $x \in X$. Now the definition of $A$ and the equation $A = F(x)$ give

$$x \in A \iff x \notin F(x) \iff x \notin A,$$

a contradiction. Hence $X \ncong \mathscr{P}(X)$, giving $X < \mathscr{P}(X)$. □

Cantor's theorem implies that there is no largest set.

We know from Lemma 6.4.2(ii) that $X \cong Y \implies X \leq Y \leq X$. But what about the converse? If $X$ and $Y$ each admit injections into the other, is there necessarily a bijection between them?

**Warning 6.4.5** Don't let finite sets lead you astray. If $X$ and $Y$ are finite (a term we'll define in Chapter 9) and $X \leq Y$ then the number of elements of $X$ is less than or equal to the number in $Y$. Hence if $X \leq Y \leq X$ then $X$ and $Y$ have the same number of elements, which implies that there is indeed a bijection between them.

But for infinite sets, it's far from obvious. For example, take the injections between real intervals $[0, 1) \underset{j}{\overset{i}{\rightleftarrows}} [0, 1]$ given by $i(x) = x$ and $j(y) = y/2$. From the existence of these injections, is it obvious that there is a bijection between $[0, 1)$ and $[0, 1]$? Can you think of one?

We now show that $X \leq Y \leq X$ does indeed imply $X \cong Y$.

Here's the idea. We have injections $X \underset{j}{\overset{i}{\rightleftarrows}} Y$. Probably neither $i$ nor $j$ is bijective. (Consider the example in Warning 6.4.5.) However, we do know that $iA \cong A$ for all $A \subseteq X$ and $jB \cong B$ for all $B \subseteq Y$, since $i$ and $j$ are injective. If we can find $A \subseteq X$ and $B \subseteq Y$ such that

$$A = X \setminus jB, \qquad B = Y \setminus iA \tag{6.5}$$

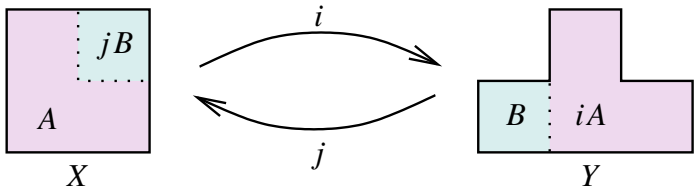



Figure 6.7: The strategy of the proof of the Cantor–Bernstein theorem.

then it will follow that $X \cong Y$ (Figure 6.7). We can simplify (6.5), eliminating $B$ to obtain the single equation

$$A = X \setminus j(Y \setminus iA). \tag{6.6}$$

If we can find a subset $A \subseteq X$ satisfying (6.6) then we can put $B = Y \setminus iA$ to make (6.5) hold, and then $X \cong Y$. So, our strategy is to find an $A$ satisfying (6.6).

We do so using some order theory. Recall the notion of order relation (Definition 5.1.21).

**Definition 6.4.6** Let $P$ be a set with an order $\leq$, and let $Q$ be a set with an order $\trianglelefteq$. A function $\varphi\colon P \to Q$ is **order-preserving** if

$$p \leq p' \implies \varphi(p) \trianglelefteq \varphi(p')$$

for all $p, p' \in P$.

**Examples 6.4.7** i. Any function $f\colon X \to Y$ induces a function

$$\begin{array}{rccc} f_*\colon & \mathscr{P}(X) & \to & \mathscr{P}(Y) \\ & A & \mapsto & fA \end{array}$$

(as a Workshop 3 question asks you to show). Regard $\mathscr{P}(X)$ as an ordered set with order $\subseteq_X$ (Examples 5.1.22), and similarly $\mathscr{P}(Y)$ with order $\subseteq_Y$. Then $f_*$ is order-preserving, since if $A, A' \subseteq X$ with $A \subseteq_X A'$ then $fA \subseteq_Y fA'$.

ii. Take sets and functions $X \underset{g}{\overset{f}{\rightleftarrows}} Y$. Define $\varphi\colon \mathscr{P}(X) \to \mathscr{P}(X)$ by

$$\varphi(A) = X \setminus g(Y \setminus fA)$$

($A \subseteq X$). (There *is* such a function, as you can show using (i) and Lemma 5.5.5.) It is order-preserving with respect to $\subseteq_X$, since for $A, A' \subseteq X$,

$$\begin{aligned} A \subseteq_X A' &\implies fA \subseteq_Y fA' \\ &\implies Y \setminus fA \supseteq_Y Y \setminus fA' \\ &\implies g(Y \setminus fA) \supseteq_X g(Y \setminus fA') \\ &\implies X \setminus g(Y \setminus fA) \subseteq_X X \setminus g(Y \setminus fA'). \end{aligned}$$

**Proposition 6.4.8 (Knaster–Tarski fixed point theorem)** *Let $X$ be a set, and let $\varphi\colon \mathscr{P}(X) \to \mathscr{P}(X)$ be a function that is order-preserving with respect to $\subseteq_X$. Then there exists $A \subseteq X$ such that $\varphi(A) = A$.*

**Proof** Put

$$\mathscr{U} = \{B \in \mathscr{P}(X) : B \subseteq \varphi(B)\} \in \mathscr{P}(\mathscr{P}(X)),$$

then put $A = \bigcup \mathscr{U} \in \mathscr{P}(X)$. We will prove that $\varphi(A) = A$.

First we show that $A \subseteq \varphi(A)$. For all $B \in \mathscr{U}$, we have $B \subseteq A$ by definition of union, so $\varphi(B) \subseteq \varphi(A)$ since $\varphi$ is order-preserving; but also $B \subseteq \varphi(B)$, so $B \subseteq \varphi(A)$. This holds for all $B \in \mathscr{U}$, and $A = \bigcup \mathscr{U}$, so $A \subseteq \varphi(A)$.

Now $A \subseteq \varphi(A)$ and $\varphi$ is order-preserving, so $\varphi(A) \subseteq \varphi(\varphi(A))$. That is, $\varphi(A) \in \mathscr{U}$. But by definition of union, $B \subseteq A$ for all $B \in \mathscr{U}$, so $\varphi(A) \subseteq A$. Hence $\varphi(A) = A$. □

**Exercise 6.4.9** Show that the subset $A$ constructed in Proposition 6.4.8 is the *largest* fixed point of $\varphi$, that is, contains all other subsets $A'$ of $X$ satisfying $\varphi(A') = A'$. Can you also construct a *smallest* fixed point?

**Theorem 6.4.10 (Cantor–Bernstein)** *Let $X$ and $Y$ be sets. If $X \leq Y$ and $Y \leq X$ then $X \cong Y$.*

**Proof** Take injections $X \underset{j}{\overset{i}{\rightleftarrows}} Y$. Let $\varphi\colon \mathscr{P}(X) \to \mathscr{P}(X)$ be the function defined by

$$\varphi(A) = X \setminus j(Y \setminus iA)$$

($A \subseteq X$). By Example 6.4.7(ii), $\varphi$ is order-preserving with respect to $\subseteq_X$. Then by Proposition 6.4.8, there exists $A \subseteq X$ such that $\varphi(A) = A$.

Put $B = Y \setminus iA$. Then $A = X \setminus jB$. Since disjoint unions are coproducts, $X \cong A + jB$ and $Y \cong iA + B$. But $i$ and $j$ are injective, so $iA \cong A$ and $jB \cong B$. Hence $X$ and $Y$ are both isomorphic to $A + B$, giving $X \cong Y$. □

**Warning 6.4.11** Finite sets $X$ have the further feature that any injection $X \to X$ must be bijective. (This is a version of the pigeonhole principle, and again we'll prove it in Chapter 10.) It follows that if we have injections $X \underset{j}{\overset{i}{\rightleftarrows}} Y$ where $X$ and $Y$ are both finite then not only are $X$ and $Y$ isomorphic, but $i$ and $j$ are isomorphisms.

This is false for infinite sets. The Cantor–Bernstein theorem does *not* say that $i$ or $j$ is an isomorphism, only that there *exists* an isomorphism between $X$ and $Y$. For example, consider $X = Y = \mathbb{N}$ with $i(n) = j(n) = n + 1$ for all $n \in \mathbb{N}$.

The Cantor–Bernstein theorem is an extremely useful labour-saving device:

**Example 6.4.12** Here we show that $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$, assuming some standard facts about $\mathbb{N}$ that we haven't proved. Define $\mathbb{N} \times \mathbb{N} \underset{j}{\overset{i}{\rightleftarrows}} \mathbb{N}$ by $i(a, b) = 2^a 3^b$ and $j(c) = (c, c)$. Then $i$ is injective by uniqueness of prime factorization, and $j$ is clearly injective. Hence by the Cantor–Bernstein theorem, $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$.

In this particular case, it's not enormously hard to write down an actual bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$. But what we've just done is easier. And in general, if we want to show that two sets are isomorphic, finding an injection in each direction is never going to be harder than finding a bijection.

**Digression 6.4.13** Cantor–Bernstein-type theorems do not hold for many types of structure other than sets. For example, its topological analogue is false: the intervals $(0, 1)$ and $[0, 1]$ embed as subspaces of one another, but are not homeomorphic. The group-theoretic analogue also fails: the groups $\mathbb{R} \times \mathbb{R} \times \cdots$ and $\mathbb{Z} \times \mathbb{R} \times \mathbb{R} \times \cdots$ embed as subgroups of one another, but are not isomorphic. So the Cantor–Bernstein property is really special to sets.

**Digression 6.4.14** In English-language texts, the Cantor–Bernstein theorem is often called the Schröder–Bernstein theorem, but Schröder's only contribution was an attempted proof that he himself conceded was wrong. Texts in French usually give it the more accurate name of Cantor–Bernstein.

## 6.5 Families

This section is about two related but different concepts: families of *elements* of a set, and families of *sets*. We consider the first one first.

Let $X$ be a set. For a set $I$, an $I$-indexed family of elements of $X$ is nothing but a function $I \to X$. This is Definition 2.7.8, and as briefly discussed after that definition, it's simply a notational shift. Sometimes, it feels more natural to write $(x_i)_{i \in I}$ than $f : I \to X$. Here, $x_i$ is alternative notation for $f(i)$.

As you saw in Example 2.7.9, you're very familiar with the family notation when $I = \mathbb{N}$. You rarely hear someone say 'let $f$ be a function from $\mathbb{N}$ to $X$'; one almost always says 'let $(x_n)$ be a sequence in $X$'.

Now we come to the crucial point, the banana skin on which many slip.

**Warning 6.5.1** A family of elements of $X$ is different from a subset of $X$! In particular, $(x_i)_{i \in I}$ is different from $\{x_i : i \in I\}$.

To see how, let's look at the case $I = \mathbb{N}$ of sequences, with $X = \mathbb{R}$. An $\mathbb{N}$-indexed family in $\mathbb{R}$ is a real sequence $x_0, x_1, \ldots$. There is one real number $x_n$ assigned to each natural number $n$. So if you change the order, you change the sequence. If you repeat some elements, you change the sequence. For example, $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ is different from $\frac{1}{2}, 1, \frac{1}{3}, \frac{1}{4}, \ldots$, and also different from $1, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$. Formally, $(x_n)_{n\in\mathbb{N}} = (y_n)_{n\in\mathbb{N}}$ if and only if $x_n = y_n$ for all $n \in \mathbb{N}$, so all three sequences are different.

Every sequence $(x_n)$ in $\mathbb{R}$ *gives rise to* a subset of $\mathbb{R}$, namely, $\{x_0, x_1, \ldots\}$. But in passing from the sequence to the subset, we lose information. For example, all three sequences above give rise to the same subset. If you're only told the subset, you can't reconstruct the sequence. For instance, if you're given that $\{x_0, x_1, \ldots\} = \{0, 1\}$, you can't tell whether or not the sequence is increasing, or converges. (Consider the sequences $0, 1, 1, 1, \ldots$ and $0, 1, 0, 1, \ldots$.)

In terms of functions, the sequence $(x_n)_{n\in\mathbb{N}}$ is a function $\mathbb{N} \to X$, and the set $\{x_n : n \in \mathbb{N}\}$ is common notation for $\{y \in \mathbb{R} : x_n = y \text{ for some } n \in \mathbb{N}\}$, which is the *image* of the function $f$.

In general, an $I$-indexed family $(x_i)_{i\in I}$ in a set $X$ is a function $f : I \to X$, and the subset $\{x_i : i \in I\}$ is alternative notation for $\{x \in X : f(i) = x \text{ for some } i \in I\}$, which is the subset $\operatorname{im} f$ of $X$. And you can't reconstruct a function from its image alone.

We keep things clear by always using *round brackets for families and curly brackets for subsets*.

**Warning 6.5.2** Confusion is sown by texts that use the unfortunate notation $\{x_n\}$ for sequences. I encourage you not to do that!

**Exercise 6.5.3** Definition 5.3 of the set text for Introduction to Linear Algebra, Nicholson's *Linear Algebra with Applications*, says this:

> we call a set $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\}$ of vectors **linearly independent** [. . . ] if it satisfies the following condition:
>
> If $t_1\mathbf{x}_1 + t_2\mathbf{x}_2 + \cdots + t_k\mathbf{x}_k = \mathbf{0}$ then $t_1 = t_2 = \cdots = t_k = 0$.

Strictly speaking, this doesn't make sense. What's the problem?

Now that we're clear on families of *elements* of a given set $X$, let's start to think about families of *sets*.

We've already used families of *subsets* of a given set. For example, we did this when we were defining the intersection $\bigcap_{i\in I} A_i$ and union $\bigcup_{i\in I} A_i$, since in this

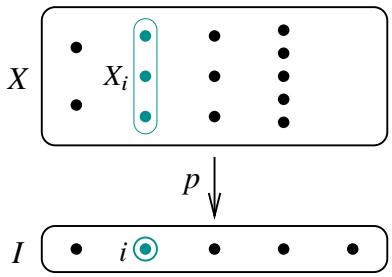



Figure 6.8: An $I$-indexed family of sets, showing an element $i \in I$ and the corresponding member $X_i$ of the family.

case, $(A_i)_{i\in I}$ is a family of subsets of a fixed set $Y$. In other words, $(A_i)_{i\in I} \in \mathscr{P}(Y)^I$. So the set called '$X$' in the discussion above is now a power set $\mathscr{P}(Y)$.

But what if we want to consider any old family $(X_i)_{i\in I}$ of sets, where the $X_i$ don't all come embedded into a single large set? For example, what if we want to consider the sequence of sets $(\mathbb{R}^n)_{n\in\mathbb{N}}$? What does the notation $(X_i)_{i\in I}$ even *mean* in this case?

We haven't given it a meaning yet, but we will. The idea is shown in Figure 6.8. Informally, we put all the sets $X_i$ in the family side by side to form one big set $X$, then we take the function $p\colon X \to I$ that sends every element of $X_i$ to $i \in I$. Formally:

**Definition 6.5.4** Let $I$ be a set. An **$I$-indexed family of sets** is a set $X$ together with a function $p\colon X \to I$.

So a family of sets is simply a function, but from yet another viewpoint. A function $A \to B$ can be viewed as a function, or as an $A$-indexed family of elements of $B$, or as a $B$-indexed family of sets!

In the situation of Definition 6.5.4, we call $I$ the **indexing set**, write the fibre $p^{-1}(i)$ as $X_i$, and call $X_i$ the $i$th **member** of the family.

**Examples 6.5.5**

i. Take a family $p\colon X \to I$. Then $p$ is surjective if and only if each member $X_i$ of the family has at least one element (is nonempty), injective if and only if each $X_i$ has at most one element (is $\varnothing$ or $\mathbf{1}$), and bijective if and only if each $X_i$ has exactly one element (is $\mathbf{1}$).

ii. Let $I$ and $Y$ be sets, and let $p = \mathrm{pr}_1\colon I \times Y \to I$. Then

$$p^{-1}(i) = \{i\} \times Y \cong Y$$

for each $i \in I$, so every member of the family is isomorphic to $Y$. A family is **constant** if all its members are isomorphic.

iii. Let $X$ and $Y$ be sets. Define a function $p\colon X + Y \to \mathbf{2}$ by

$$p(z) = \begin{cases} \mathsf{T} & \text{if } z \in X, \\ \mathsf{F} & \text{if } z \in Y \end{cases}$$

($z \in X + Y$). (See the passage before Warning 6.3.9 for explanation of the notation.) We can view $X + Y \xrightarrow{p} \mathbf{2}$ as a $\mathbf{2}$-indexed family of sets, that is, a two-member family; the two members are $p^{-1}(\mathsf{T}) \cong X$ and $p^{-1}(\mathsf{F}) \cong Y$.

Just after Exercise 6.5.3, I recalled that we've already met families of subsets of a given set $Y$. If we have a family of subsets of $Y$, then by forgetting about the inclusion functions, we should get a family of sets, right? That's what the next result says.

**Lemma 6.5.6** *Let $Y$ and $I$ be sets, and let $(A_i \hookrightarrow Y)_{i \in I}$ be an $I$-indexed family of subsets of $Y$. Then there exists an $I$-indexed family of sets $X \to I$ such that $X_i \cong A_i$ for all $i \in I$.*

**Proof** Let

$$X = \{(i, y) \in I \times Y : y \in A_i\} \subseteq I \times Y,$$

and let $p\colon X \to I$ be the composite

$$X \hookrightarrow I \times Y \xrightarrow{\mathrm{pr}_1} I.$$

Then for each $i \in I$,

$$p^{-1}(i) = \{i\} \times A_i \cong A_i,$$

as required. □

**Example 6.5.7** Let $Y$ be a set. The identity function $\mathrm{id}\colon \mathscr{P}(Y) \to \mathscr{P}(Y)$, seen as a $\mathscr{P}(Y)$-indexed family of elements of $\mathscr{P}(Y)$, is $(A)_{A \in \mathscr{P}(Y)}$. Applying Lemma 6.5.6 to this example, the set $X$ in the proof is

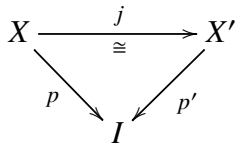
$$\{(A, y) \in \mathscr{P}(Y) \times Y : y \in A\} \subseteq \mathscr{P}(Y) \times Y.$$

That is, $X$ is the relation $\ni_Y$ between $\mathscr{P}(Y)$ and $Y$ (Example 5.1.3(v)), and $p\colon X \to \mathscr{P}(Y)$ is $(A, y) \mapsto A$. The fibre of $p$ over $A$ is $A$ itself.

When are two families essentially the same?

**Definition 6.5.8** Let $I$ be a set. Two $I$-indexed families $X \xrightarrow{p} I$ and $X' \xrightarrow{p'} I$ are said to be **isomorphic** if they are isomorphic over $I$ (Definition 3.2.12).

If the $I$-indexed families $X \xrightarrow{p} I$ and $X' \xrightarrow{p'} I$ are isomorphic then by definition, there exists a bijection $j : X \to X'$ such that the diagram




commutes. In that case, $X_i \cong X'_i$ for all $i \in I$.

**Exercise 6.5.9** Why is $X_i \cong X'_i$ for all $i \in I$? Prove it. (Hint: you can derive an isomorphism $X_i \to X'_i$ from $j$.)

The converse also holds:

**Lemma 6.5.10** *Let $I$ be a set, and let $X \to I$ and $X' \to I$ be $I$-indexed families. If $X_i \cong X'_i$ for all $i \in I$ then the families $X \to I$ and $X' \to I$ are isomorphic.*

**Proof** Deferred to Chapter 9. □

The proof is deferred because it uses the axiom of choice, which we are not discussing yet. We will not *need* Lemma 6.5.10 before then. However...

We often write a family of sets $X \xrightarrow{p} I$ as $(X_i)_{i \in I}$, and call $p$ the **projection** of the family. (Recall that $X_i$ means the fibre $p^{-1}(i)$.) Now, denoting the family by $(X_i)_{i \in I}$ is potentially dangerous. Everything we do is supposed to be isomorphism-invariant, so in order for this notation to be safe, we need it to be the case that if $X_i \cong Y_i$ for all $i \in I$ then the families $(X_i)_{i \in I}$ and $(Y_i)_{i \in I}$ are isomorphic. Otherwise, we could take a family $(X_i)_{i \in I}$, replace the sets $X_i$ by isomorphic copies, and end up with a genuinely different family—not isomorphic to the original.

Lemma 6.5.10 guarantees that there is no such danger. I will use it between now and Chapter 9, even though it hasn't been proved. But I will only use it to make the notation nicer, not for any essential purpose, so there is no logical circularity.

**Example 6.5.11** In this notation, the constant family $I \times Y \xrightarrow{\mathrm{pr}_1} I$ (Example 6.5.5(ii)) is $(Y)_{i \in I}$.

So far in this section, we have mostly just set up the language of families of sets. But now we come to an important result.

**Proposition 6.5.12** *Let $(X_i)_{i \in I}$ be a family of sets. Then there exists a set not isomorphic to any of the sets $X_i$ ($i \in I$).*

**Proof** By definition, there is a function $X \xrightarrow{p} I$ such that $p^{-1}(i) = X_i$ for all $i \in I$. Let $i \in I$. We have $X_i \subseteq X$, so $X_i \leq X$. Also, $X < \mathscr{P}(X)$ by Cantor's theorem (Theorem 6.4.4). Since $X_i \leq X < \mathscr{P}(X)$, it follows that $X_i < \mathscr{P}(X)$. In particular, $X_i \not\cong \mathscr{P}(X)$. □

**Exercise 6.5.13** Where I wrote 'it follows that', I was implicitly using the principle that if $W \leq X < Y$ then $W < Y$, for sets $W$, $X$ and $Y$. Prove this. (You'll need the Cantor–Bernstein theorem.)

Proposition 6.5.12 is a version of the idea that 'there is no set of all sets'. In fact, it is the stronger statement that if you have a set-indexed family of sets then not only is there some set not *equal* to any of them, but there is some set not *isomorphic* to any of them. Since equality of sets is unimportant, this stronger result is much more interesting and significant.

# Chapter 7

# Number systems

*To read by Monday 28 October: Sections 7.1 and 7.2.*
*Part of Section 7.2 is labelled as non-examinable.*
*To read by Friday 1 November: Sections 7.3–7.5.*

The main point of set theory is to be useful for the rest of mathematics. Most of mathematics involves numbers of some kind, so if we want our axiomatization of sets to be useful, we'd better develop the usual number systems within it.

This chapter is relatively concrete and algebraic. There are no big new concepts. But we *will* use the natural numbers axiom (Axiom 9) for the first time in this course, so before you go on, I suggest you refresh your memory by rereading Section 3.3.

We'll begin with $\mathbb{N}$, then use $\mathbb{N}$ to define $\mathbb{Z}$, then use $\mathbb{Z}$ to define $\mathbb{Q}$, and finally use $\mathbb{Q}$ to define $\mathbb{R}$. Along the way, we'll establish the inestimably important principle of mathematical induction.

Occasionally I will mention rings, fields, etc. Since these concepts are not in the official prerequisites for the course, anything I say about them is non-examinable. But they will help us to organize our thoughts.

## 7.1 The natural numbers

Recall from Section 3.3 that Axiom 9 provides us with a set $\mathbb{N}$, called the set of natural numbers, an element of $\mathbb{N}$ called 0, and a function $s\colon \mathbb{N} \to \mathbb{N}$ called the successor function. The idea is that $s(n) = n + 1$ ($n \in \mathbb{N}$), although we have not defined either + or 1 yet. The set $\mathbb{N}$, element 0 and function $s$ together satisfy the universal property of Definition 3.3.2.

**Theorem 7.1.1 (Principle of induction)** *Let $A \subseteq \mathbb{N}$. Suppose that $0 \in_{\mathbb{N}} A$ and that for all $n \in \mathbb{N}$, we have $n \in_{\mathbb{N}} A \implies s(n) \in_{\mathbb{N}} A$. Then $A = \mathbb{N}$.*

**Proof** Here I will be more careful than usual about writing inclusion functions and distinguishing between $\in$ and $\in_{\mathbb{N}}$.

Write $i\colon A \hookrightarrow \mathbb{N}$ for the inclusion. The main hypothesis is equivalent to $\mathrm{im}(si) \subseteq A$, so by Lemma 5.5.8, there is a unique function $s'\colon A \to A$ such that $is'(a) = si(a)$ for all $a \in A$. (If we don't write the inclusion functions, this just says $s'(a) = s(a)$ for all $a \in A$.) Also, $0 \in_{\mathbb{N}} A$, which means there is an element $0' \in A$ such that $i(0') = 0$.

So by the universal property of the natural numbers (Definition 3.3.2), there is a function $f\colon \mathbb{N} \to A$ such that $f(0) = 0'$ and $fs = s'f$. Now also, $i\colon A \to \mathbb{N}$ satisfies $i(0') = 0$ and $is' = si$. It follows that the function $if\colon \mathbb{N} \to \mathbb{N}$ satisfies $if(0) = 0$ and $(if)s = s(if)$. But $\mathrm{id}_{\mathbb{N}}\colon \mathbb{N} \to \mathbb{N}$ also satisfies $\mathrm{id}_{\mathbb{N}}(0) = 0$ and $\mathrm{id}_{\mathbb{N}}s = s\mathrm{id}_{\mathbb{N}}$, so by the uniqueness part of the universal property, $if = \mathrm{id}_{\mathbb{N}}$. Hence the inclusion $i$ is surjective, that is, $A = \mathbb{N}$. □

**Example 7.1.2** The subset $A = \{0\} \cup \mathrm{im}(s)$ of $\mathbb{N}$ satisfies the hypotheses of Theorem 7.1.1. Hence $\{0\} \cup \mathrm{im}(s) = \mathbb{N}$: every natural number is 0 or a **successor** (equal to $s(n)$ for some $n \in \mathbb{N}$).

In a typical proof by induction, you have some property $P(n)$ of natural numbers $n$, you prove the base case $P(0)$, then you prove the inductive step: $P(n) \implies P(n+1)$ whenever $n \in \mathbb{N}$. You want to conclude that $P(n)$ holds for all $n \in \mathbb{N}$. Theorem 7.1.1 lets us do this, by taking $A = \{n \in \mathbb{N} : P(n)\}$. At least, this is true as long as $P(n)$ specifies a subset of $\mathbb{N}$—but as we saw in Chapter 5, pretty much any property we can think of does.

We still don't know some basic things about $\mathbb{N}$. For instance, is 0 a successor? We'd guess not, but can we prove it? The next lemma is the key.

**Lemma 7.1.3** *The function $\binom{0}{s}\colon \mathbf{1} + \mathbb{N} \to \mathbb{N}$ is an isomorphism.*

Here I am using the notation $\binom{f}{g}$ defined after Theorem 6.3.8. The picture for the lemma is this:

$$\begin{array}{ccccccc} \star & 0 & 1 & 2 & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0 & 1 & 2 & 3 & \cdots \end{array}$$

The top-to-bottom function is $\binom{0}{s}$, and its inverse has to be constructed.

**Proof** Write $\star$ for the unique element of $\mathbf{1}$. Define $t\colon \mathbf{1} + \mathbb{N} \to \mathbf{1} + \mathbb{N}$ by $t(\star) = 0$ and $t(n) = s(n)$ for $n \in \mathbb{N}$. (In the diagram, $t$ is the function that shifts each element of the top row one place to the right.) By the universal property of the

natural numbers, there is a unique function $f\colon \mathbb{N} \to \mathbf{1} + \mathbb{N}$ such that $f(0) = \star$ and $f \circ s = t \circ f$. (Think of $f$ as the bottom-to-top function.) We will show that $f$ is inverse to $\binom{0}{s}$.

By definition, $\binom{0}{s}(\star) = 0$. Also, $\binom{0}{s} \circ t = s \circ \binom{0}{s}$ (exercise). From this and the defining properties of $f$, it follows that $\binom{0}{s} \circ f\colon \mathbb{N} \to \mathbb{N}$ satisfies

$$\left(\binom{0}{s} \circ f\right)(0) = 0, \qquad \left(\binom{0}{s} \circ f\right) \circ s = s \circ \left(\binom{0}{s} \circ f\right).$$

But $\mathrm{id}_{\mathbb{N}}\colon \mathbb{N} \to \mathbb{N}$ also satisfies these equations, so by the uniqueness part of the universal property, $\binom{0}{s} \circ f = \mathrm{id}_{\mathbb{N}}$. Hence for all $n \in \mathbb{N}$,

$$n = \binom{0}{s}(f(n)) = \begin{cases} 0 & \text{if } f(n) = \star, \\ s(f(n)) & \text{if } f(n) \in \mathbb{N}. \end{cases} \tag{7.1}$$

It remains to show that $f \circ \binom{0}{s} = \mathrm{id}_{\mathbf{1}+\mathbb{N}}$. First,

$$\left(f \circ \binom{0}{s}\right)(\star) = f(0) = \star.$$

Second, for all $n \in \mathbb{N}$,

$$\left(f \circ \binom{0}{s}\right)(n) = f(s(n)) = t(f(n)) = \begin{cases} 0 & \text{if } f(n) = \star, \\ s(f(n)) & \text{if } f(n) \in \mathbb{N}. \end{cases}$$

By equation (7.1), this is equal to $n$ in either case, completing the proof. □

**Proposition 7.1.4** *i. Every natural number is* 0 *or a successor.*

*ii.* 0 *is not a successor.*

*iii. If* $s(n) = s(m)$ *then* $n = m$*, for* $n, m \in \mathbb{N}$.

**Proof** Lemma 7.1.3 implies that $\mathbf{1} \xrightarrow{0} \mathbb{N} \xleftarrow{s} \mathbb{N}$ is a coproduct diagram. So by Proposition 6.3.7, it is a disjoint union diagram. Hence $s$ is injective, $\{0\} \cup \mathrm{im}(s) = \mathbb{N}$, and $\{0\} \cap \mathrm{im}(s) = \varnothing$, which are the three statements to be proved. □

Now we define the algebraic structure on $\mathbb{N}$. Here is the idea. We want, among other things, to define an addition function $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. The only tool we have is the universal property of $\mathbb{N}$, which gives a supply of functions with domain $\mathbb{N}$. Our hoped-for addition function has domain $\mathbb{N} \times \mathbb{N}$, so we seem to be stuck. However, the function set axiom gives a correspondence between functions $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and functions $\mathbb{N} \to \mathbb{N}^{\mathbb{N}}$, and the latter *do* have domain $\mathbb{N}$. So, we

define addition by first constructing the function $\mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ that corresponds to it. Concretely, this is the sequence $(\alpha_m)_{m\in\mathbb{N}}$, where $\alpha_m \in \mathbb{N}^{\mathbb{N}}$ is $n \mapsto m + n$. Each entry $\alpha_m$ should be characterized by $\alpha_m(0) = m$ and $\alpha_m(s(n)) = s(\alpha_m(n))$, as in the following proof (where $\alpha_m$ is called $\alpha(m)$).

**Lemma 7.1.5** *There exists a unique function* $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *such that, writing* $+(m, n)$ *as* $m + n$*,*

$$m + 0 = m \text{ for all } m \in \mathbb{N},$$
$$m + s(n) = s(m + n) \text{ for all } m, n \in \mathbb{N}.$$

**Proof** *Uniqueness:* Let $+$ and $\oplus$ be two functions with the stated properties. Let $m \in \mathbb{N}$. A simple proof by induction on $n$ shows that $m + n = m \oplus n$ for all $n \in \mathbb{N}$. Hence $+ = \oplus$.

*Existence:* By the results on specifying subsets in Chapter 5, there is a subset

$$R = \left\{(m, f) \in \mathbb{N} \times \mathbb{N}^{\mathbb{N}} : f(0) = m \text{ and } (\forall n \in \mathbb{N})(fs(n) = sf(n))\right\} \tag{7.2}$$

of $\mathbb{N} \times \mathbb{N}^{\mathbb{N}}$. For each $m \in \mathbb{N}$, the natural numbers axiom implies that there is a unique element $f \in \mathbb{N}^{\mathbb{N}}$ such that $(m, f) \in R$. So $R$ is a functional relation, which by Theorem 5.2.4 means that $R$ is the graph of a function $\alpha\colon \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$. By construction, for each $m \in \mathbb{N}$, we have $(m, \alpha(m)) \in R$; that is,

$$\alpha(m)(0) = m, \qquad \alpha(m)(s(n)) = s(\alpha(m)(n)) \text{ for all } n \in \mathbb{N}.$$

Let $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the function corresponding to $\alpha$ via the function set axiom. Then

$$+(m, 0) = m, \qquad +(m, s(n)) = s(+(m, n)) \text{ for all } n \in \mathbb{N},$$

as required. □

**Lemma 7.1.6** *There exists a unique function* $\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *such that, writing* $\cdot(m, n)$ *as* $m \cdot n$*,*

$$m \cdot 0 = 0 \text{ for all } m \in \mathbb{N},$$
$$m \cdot s(n) = m \cdot n + m \text{ for all } m, n \in \mathbb{N}.$$

**Proof** This is very similar to the proof of Lemma 7.1.5, so I will just mention the parts that change. Put

$$R = \left\{(m, f) \in \mathbb{N} \times \mathbb{N}^{\mathbb{N}} : f(0) = 0 \text{ and } (\forall n \in \mathbb{N})(fs(n) = f(n) + m)\right\}.$$

We get a function $\mu\colon \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ with graph $R$, and then for all $m \in \mathbb{N}$,

$$\mu(m)(0) = 0, \qquad \mu(m)(s(n)) = \mu(m)(n) + m \text{ for all } n \in \mathbb{N}.$$

Then define $\cdot$ to be the function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ corresponding to $\mu$. □

Of course, we call + and · **addition** and **multiplication** on $\mathbb{N}$, and we usually write $m \cdot n$ as $mn$. We also define the natural number 1 (or $1_{\mathbb{N}}$ if we're being fussy) as $s(0)$.

**Lemma 7.1.7** *There exists a unique function* $E : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *such that, writing* $E(m, n)$ *as* $m^n$,

$$m^0 = 1 \text{ for all } m \in \mathbb{N},$$
$$m^{s(n)} = m^n \cdot m \text{ for all } m, n \in \mathbb{N}.$$

**Proof** This is very similar to the last two proofs, taking

$$R = \left\{(m, f) \in \mathbb{N} \times \mathbb{N}^{\mathbb{N}} : f(0) = 1 \text{ and } (\forall n \in \mathbb{N})(fs(n) = f(n) \cdot m)\right\}. \qquad \square$$

Let's just check that the successor function $s$ does what we think:

**Lemma 7.1.8** $s(n) = n + 1$ *for all* $n \in \mathbb{N}$.

**Proof** By Lemma 7.1.5, $s(n) = s(n + 0) = n + s(0) = n + 1$. $\square$

Now we define inequality of natural numbers.

**Definition 7.1.9** The relation $\leq$ on $\mathbb{N}$ is defined by

$$m \leq n \iff k + m = n \text{ for some } k \in \mathbb{N}$$

$(m, n \in \mathbb{N})$. We define $m < n$ to mean $m \leq n$ and $m \neq n$, and $m \geq n$ to mean $n \leq m$, and, finally, $m > n$ to mean $n < m$.

We will show soon that $\leq$ is an order relation. But first, we work out how $\leq$ interacts with the successor function.

**Lemma 7.1.10**

*i.* $m \leq n \iff s(m) \leq s(n)$, *for* $m, n \in \mathbb{N}$.

*ii.* $m < n \iff s(m) < s(n)$, *for* $m, n \in \mathbb{N}$.

*iii.* $n \geq 0$ *for all* $n \in \mathbb{N}$.

*iv.* $n \leq 0 \implies n = 0$, *for* $n \in \mathbb{N}$.

*v.* $m < s(n) \iff m \leq n$, *for* $m, n \in \mathbb{N}$.

**Proof** For (i), using the injectivity of $s$ and Lemma 7.1.5,

$$\begin{aligned} m \leq n &\iff k + m = n \text{ for some } k \in \mathbb{N} \\ &\iff s(k + m) = s(n) \text{ for some } k \in \mathbb{N} \\ &\iff k + s(m) = s(n) \text{ for some } k \in \mathbb{N} \\ &\iff s(m) \leq s(n). \end{aligned}$$

Part (ii) follows from (i) and the injectivity of $s$.

For (iii), we have $n + 0 = n$ by Lemma 7.1.5, giving $0 \leq n$ by definition of $\leq$.

For (iv), suppose that $n \leq 0$. Then $k + n = 0$ for some $k \in \mathbb{N}$. If $n \neq 0$ then by Proposition 7.1.4(i), $n = s(m)$ for some $m \in \mathbb{N}$, giving $k + s(m) = 0$, which by Lemma 7.1.5 means $s(k + m) = 0$—contradicting the fact that 0 is not a successor (Proposition 7.1.4(ii)). So $n = 0$.

We prove (v) by induction on $m$ for all $n$ simultaneously. For the base case $m = 0$, we have $0 < s(n)$ for all $n$ (by (iii) and because 0 is not a successor) and $0 \leq n$ for all $n$ (by (iii)), so both sides of the double implication hold.

For the inductive step, suppose that $m < s(n) \iff m \leq n$ for all $n \in \mathbb{N}$; we have to show that

$$s(m) < s(n) \iff s(m) \leq n$$

for all $n \in \mathbb{N}$. So, let $n \in \mathbb{N}$. If $n = 0$, both sides are false: if $s(m) < s(0)$ then $m < 0$ by (ii), contradicting (iv), and if $s(m) \leq 0$ then $s(m) = 0$ by (iv), contradicting the fact that 0 is not a successor. If $n \neq 0$ then $n = s(n')$ for some $n' \in \mathbb{N}$, and then

$$s(m) < s(n) \iff m < n \iff m < s(n') \iff m \leq n' \iff s(m) \leq n,$$

where the first and last equivalences follow from parts (ii) and (i), the second is because $n = s(n')$, and the third is by inductive hypothesis. This completes the induction. □

**Remark 7.1.11** In Section 5.5, we gave a precise meaning to the notation $\{x \in X : P(x)\}$. There's another everyday piece of curly bracket notation that I should have defined but didn't: for a function $f : X \to Y$, we write $\{f(x) : x \in X\}$ for the image $\operatorname{im} f = \{y \in Y : (\exists x \in X) f(x) = y\}$.

For elements $x$ of a set $X$, we have already defined the singleton $\{x\} \subseteq X$ (Example 4.1.4(iii)). For elements $x$ and $y$ of $X$, we define $\{x, y\} = \{x\} \cup \{y\}$. For elements $x$, $y$ and $z$ of $X$, we (of course!) define $\{x, y, z\} = \{x\} \cup \{y\} \cup \{z\}$. 'And so on'.

What exactly does 'and so on' mean? Suppose we have natural numbers $m \leq n$ and, for each $i$ between $m$ and $n$, an element $x_i$ of $X$. Formally, this means we have a function

$$f : \{i \in \mathbb{N} : m \leq i \leq n\} \to X,$$

and we're writing $f(i)$ as $x_i$. Then $\{x_m, x_{m+1}, \ldots, x_n\}$ is notation for $\mathrm{im}\, f$. Thus, an element $x \in X$ belongs to this subset if and only if it is equal to $x_i$ for some $i \in \mathbb{N}$ between $m$ and $n$.

The notation $\{x_m, x_{m+1}, \ldots, x_n\}$ is informal, as it makes the reader guess what '…' stands for—that is, guess the function $f$. For instance, $\{-1, -2, \ldots, -n\}$ *probably* means the image of the function $f\colon \{i \in \mathbb{N} : 1 \leq i \leq 10\} \to \mathbb{Z}$ with $f(i) = -i$, but perhaps the writer had a different sequence in mind. Despite the ambiguity, this notation is in extremely wide usage.

**Definition 7.1.12** For $n \in \mathbb{N}$, we write $B(n) = \{i \in \mathbb{N} : i < n\}$.

Informally, that means $B(n) = \{0, 1, \ldots, n-1\}$: it's an $n$-element set, whatever that means (and we'll be precise about this kind of thing in Chapter 10). The notation $B(n)$ is not standard and we'll only use it temporarily, for reasons you'll discover soon.

Remember how we keep seeing glimpses of an algebra of sets that looks like the familiar algebra of natural numbers? We're now going to make that connection precise, using the idea that $B(n)$ is the set companion of the number $n$. At the same time, we're going to prove that the addition, multiplication and power operations on $\mathbb{N}$ satisfy all the usual algebraic laws, as does the inequality relation on $\mathbb{N}$—and all with surprisingly little effort.

**Lemma 7.1.13** $B(s(n)) \cong B(n) + \mathbf{1}$ *for all* $n \in \mathbb{N}$.

**Proof** Let $n \in \mathbb{N}$. By Lemma 7.1.10(v), $B(s(n)) = \{i \in \mathbb{N} : i \leq n\}$. But the right-hand side is the disjoint union $\{i \in \mathbb{N} : i < n\} \amalg \{n\}$, so $B(s(n)) \cong B(n) + \mathbf{1}$.□

**Proposition 7.1.14** *For all* $m, n \in \mathbb{N}$,

*i.* $B(m+n) \cong B(m) + B(n)$, *and* $B(0) \cong \varnothing$;

*ii.* $B(m \cdot n) \cong B(m) \times B(n)$, *and* $B(1) \cong \mathbf{1}$;

*iii.* $B(m^n) \cong B(m)^{B(n)}$.

In (i), the + on the left-hand side of the first isomorphism is addition of natural numbers, whereas the + on the right is coproduct of sets. Similar comments apply to (ii) and (iii).

**Proof** For (i), $B(0)$ is empty by Lemma 7.1.10(iv). To prove the main statement, fix $m \in \mathbb{N}$; we show by induction on $n$ that $B(m+n) \cong B(m) + B(n)$. The base case $n = 0$ holds because $m + 0 = m$ (by Lemma 7.1.5) and $B(m) \cong B(m) + \varnothing$ (by

Proposition 6.3.13(ib)). For the inductive step, suppose the result holds for $n$. We have

$$\begin{aligned} B(m + s(n)) &= B(s(m + n)) && \text{by Lemma 7.1.5} \\ &\cong B(m + n) + \mathbf{1} && \text{by Lemma 7.1.13} \\ &\cong (B(m) + B(n)) + \mathbf{1} && \text{by inductive hypothesis} \\ &\cong B(m) + (B(n) + \mathbf{1}) && \text{by Proposition 6.3.13(ic)} \\ &\cong B(m) + B(s(n)) && \text{by Lemma 7.1.13,} \end{aligned}$$

completing the induction.

Parts (ii) and (iii) are very similar and left as exercises. (They wouldn't make bad exam questions.) □

We've now seen that the algebraic operations on $\mathbb{N}$ are compatible with the algebraic operations on sets. Next we do the same thing for inequality. For this, we use a general lemma that has nothing intrinsically to do with natural numbers.

**Lemma 7.1.15** *Let $X$ and $Y$ be sets. Then:*

*i.* $X \cong Y \iff X + \mathbf{1} \cong Y + \mathbf{1}$;

*ii.* $X \leq Y \iff X + \mathbf{1} \leq Y + \mathbf{1}$.

**Proof** For (i), '$\Rightarrow$' holds simply because the coproduct construction (like everything else) is isomorphism-invariant. Now suppose we have an isomorphism $f : X + \mathbf{1} \to Y + \mathbf{1}$. Write the unique element of $\mathbf{1}$ as $\star$.

We have elements $f(\star)$ and $\star$ of $Y + \mathbf{1}$. By Example 5.5.2, there is a function $g : Y + \mathbf{1} \to Y + \mathbf{1}$ that swaps $f(\star)$ with $\star$ and fixes all other elements. In fact, $g$ is an isomorphism, as it is self-inverse. Then $g \circ f$ is an isomorphism $X + \mathbf{1} \to Y + \mathbf{1}$ satisfying $(g \circ f)(\star) = \star$. Hence $(g \circ f)X = Y$ with $g \circ f$ injective, giving $X \cong Y$.

To deduce (ii), we use Lemma 6.4.3: $X \leq Y$ if and only if $A + X \cong Y$ for some set $A$, which by (i) is equivalent to $A + X + \mathbf{1} \cong Y + \mathbf{1}$ for some set $A$, which by Lemma 6.4.3 again is equivalent to $X + \mathbf{1} \leq Y + \mathbf{1}$. □

**Lemma 7.1.16** $m \leq n \iff B(m) \leq B(n)$, *for* $m, n \in \mathbb{N}$.

Here, the $\leq$ on the left-hand side is inequality of natural numbers (Definition 7.1.9) and the $\leq$ on the right-hand side is inequality of sets (Definition 6.4.1).

**Proof** First note that $B(m)$ is empty if and only if $m = 0$, by Lemma 7.1.10(iii), (iv). Now we prove the result by induction on $n$ for all $m$ simultaneously.

Base case: $m \leq 0$ if and only if $m = 0$, and $B(m) \leq B(0)$ if and only if $B(m)$ is empty (since $B(0)$ is empty), if and only if $m = 0$.

Inductive step: assume the result for $n$. Let $m \in \mathbb{N}$. If $m = 0$ then $m = 0 \leq n$ and $B(m) \cong \varnothing \leq B(n)$, so both sides of the double implication hold. Otherwise, $m = s(m')$ for some $m' \in \mathbb{N}$, and

$$\begin{aligned}
m \leq s(n) &\iff s(m') \leq s(n) && \text{since } m = s(m') \\
&\iff m' \leq n && \text{by Lemma 7.1.10(i)} \\
&\iff B(m') \leq B(n) && \text{by inductive hypothesis} \\
&\iff B(m') + \mathbf{1} \leq B(n) + \mathbf{1} && \text{by Lemma 7.1.15(ii)} \\
&\iff B(s(m')) \leq B(s(n)) && \text{by Lemma 7.1.13} \\
&\iff B(m) \leq B(s(n)) && \text{since } m = s(m'),
\end{aligned}$$

completing the induction. □

One last lemma of this kind tells us that different numbers $n$ always have different set counterparts $B(n)$.

**Lemma 7.1.17** *$m = n \iff B(m) \cong B(n)$, for $m, n \in \mathbb{N}$.*

**Proof** This is very similar to the proof of Lemma 7.1.16, using part (i) rather than part (ii) of Lemma 7.1.15. □

Now comes the best bit! We can show that addition, multiplication and powers in $\mathbb{N}$ satisfy the laws we expect, by simply *deducing* them from what we already know about sets. The alternative would be to prove them directly by lots of tedious inductions—but we avoid that work entirely.

**Proposition 7.1.18** *The following laws hold for all $m, n, p \in \mathbb{N}$.*

*i. Addition laws: $m + n = n + m$, $n + 0 = n$, and $(m + n) + p = m + (n + p)$.*

*ii. Multiplication laws: $mn = nm$, $n1 = n$, and $(mn)p = m(np)$.*

*iii. Distributivity laws: $m(n + p) = mn + mp$ and $n0 = 0$.*

*iv. Addition/power laws: $p^{m+n} = p^m p^n$ and $p^0 = 1$.*

*v. Multiplication/power laws: $(np)^m = n^m p^m$, $1^n = 1$, $p^{mn} = (p^n)^m$, and $p^1 = p$.*

**Proof** All of these follow from the corresponding results for sets. For instance, take the distributivity law $m(n + p) = mn + mp$ of (iii). We have

$$B(m(n + p)) \cong B(m) \times B(n + p) \cong B(m) \times (B(n) + B(p))$$

by Proposition 7.1.14. But $X \times (Y + Z) \cong (X \times Y) + (X \times Z)$ for all sets $X, Y$ and $Z$ (Proposition 6.3.13), so this is isomorphic to

$$(B(m) \times B(n)) + (B(m) \times B(p)) \cong B(mn) + B(mp) \cong B(mn + mp),$$

using Proposition 7.1.14 again. So

$$B(m(n + p)) \cong B(mn + mp),$$

which by Lemma 7.1.17 gives $m(n + p) = mn + mp$.

All the other parts are similar, using Proposition 6.3.13 for (i), (iii) and (iv), Proposition 2.6.15 for (ii), and Proposition 2.7.12 for (v). □

We can do something similar for inequalities in $\mathbb{N}$.

**Proposition 7.1.19** *i. The relation $\leq$ on $\mathbb{N}$ is an order.*

*ii. Let $m, n \in \mathbb{N}$ with $m \leq n$. Then for all $p \in \mathbb{N}$, we have $m + p \leq n + p$, $mp \leq np$, and $m^p \leq n^p$; if also $p > 0$ then $p^m \leq p^n$.*

**Exercise 7.1.20** What can go wrong with that last part if $p = 0$?

**Proof** For (i), reflexivity and transitivity of the relation $\leq$ on $\mathbb{N}$ follow from Lemma 6.4.2 on inequality of sets, using Lemma 7.1.16. For instance, if $m \leq n$ and $n \leq p$ then $B(m) \leq B(n)$ and $B(n) \leq B(p)$ by Lemma 7.1.16, so $B(m) \leq B(p)$ by Lemma 6.4.2, so $m \leq p$ by Lemma 7.1.16 again. For antisymmetry, if $m \leq n \leq m$ then $B(m) \leq B(n) \leq B(m)$, which by the Cantor–Bernstein theorem implies that $B(m) \cong B(n)$; hence $m = n$ by Lemma 7.1.17.

The argument for (ii) is similar, but using a Workshop 4 question in which you're asked to prove that for sets $X, Y$ and $Z$, if $X \leq Y$ then $X + Z \leq Y + Z$, etc.□

Although this method for proving results about $\mathbb{N}$ is very powerful, there are a few further basic facts about $\mathbb{N}$ that it doesn't work for. Principally these are about cancellation.

**Lemma 7.1.21** *Let $m, n \in \mathbb{N}$. If $m + n = 0$ then $m = n = 0$, and if $mn = 0$ then $m = 0$ or $n = 0$.*

**Proof** This one *does* follow by the same method. Suppose that $m + n = 0$. Then $B(m + n) \cong B(0)$, or equivalently, $B(m) + B(n) \cong B(0) \cong \varnothing$. It is easily shown that if the coproduct of two sets is empty then so are both sets. Hence $B(m) \cong B(0) \cong B(n)$, giving $m = 0 = n$. A similar argument applies to $mn = 0$.□

**Lemma 7.1.22** *Let $m, n, p \in \mathbb{N}$. If $m + p = n + p$ then $m = n$.*

**Proof** By induction on $p$. The base case is trivial. Supposing inductively that the result holds for $p$, if $m + p + 1 = n + p + 1$ then $m + p = n + p$ since $s$ is injective, and the inductive hypothesis then gives $m = n$. □

**Exercise 7.1.23** Prove that $n < n + 1$ for all natural numbers $n$. There are several ways to do this.

**Lemma 7.1.24** *Let $m, n, p \in \mathbb{N}$ with $p \neq 0$. If $mp = np$ then $m = n$.*

**Proof** We fix $0 \neq p \in \mathbb{N}$ and prove the result by induction on $m$ for all $n$ simultaneously.

Base case: when $m = 0$, we have to prove that if $n \in \mathbb{N}$ with $0 = np$ then $0 = n$. This is the second part of Lemma 7.1.21.

Inductive step: assume the result for $m$, and let $n \in \mathbb{N}$ with $(m + 1)p = np$. The successor $m + 1$ is not equal to 0, and nor is $p$, so $np \neq 0$ by Lemma 7.1.21. Hence $n \neq 0$, and so $n$ is a successor; say $n = n' + 1$. Now $(m+1)p = (n'+1)p$, so $mp + p = n'p + p$, which by Lemma 7.1.22 gives $mp = n'p$. Hence by inductive hypothesis, $m = n'$, giving $m + 1 = n' + 1 = n$. □

**Exercise 7.1.25** Let $X$, $Y$ and $Z$ be sets. If $X + Z \cong Y + Z$, does it follow that $X \cong Y$? If $X \times Z \cong Y \times Z$ with $Z$ nonempty, does it follow that $X \cong Y$?

We've shown that the relation $\leq$ on $\mathbb{N}$ is an order (Proposition 7.1.19), which means a *partial* order. Our last result improves on this:

**Lemma 7.1.26** *The relation $\leq$ on $\mathbb{N}$ is a total order.*

**Proof** It remains to show that for all $m, n \in \mathbb{N}$, either $m \leq n$ or $n \leq m$. We prove this by induction on $m$ for all $n$ simultaneously.

Base case: if $m = 0$ then $m \leq n$ for all $n \in \mathbb{N}$.

Inductive step: assume the result for $m$, and let $n \in \mathbb{N}$. We must show that $m + 1 \leq n$ or $n \leq m + 1$. If $n = 0$ then $n \leq m + 1$. Otherwise, $n = n' + 1$ for some $n' \in \mathbb{N}$. By inductive hypothesis, $m \leq n'$ or $n' \leq m$, and then Lemma 7.1.10(i) gives either $m + 1 \leq n' + 1 = n$ or $n = n' + 1 \leq m + 1$. □

**Remark 7.1.27** From now on, I will write $B(n)$ as $\mathbf{n}$. Thus, $\mathbf{n} = \{i \in \mathbb{N} : i < n\}$. This *is* fairly standard notation.

The reason for not calling it $\mathbf{n}$ from the start is that it would have created ambiguity. Does $\mathbf{m^n}$ mean $B(m)^{B(n)}$ or $B(m^n)$, for instance? Proposition 7.1.14

tells us that it doesn't matter. The same goes for $\mathbf{m} + \mathbf{n}$. Proposition 7.1.14 also ensures that the notation '$\mathbf{1}$' is unambiguous: you can interpret it as either $B(1)$ or the terminal set that we've been calling $\mathbf{1}$ all along, and again, it doesn't matter since they're the same.

One more thing along these lines: define the natural number 2 to be $s(1)$. By Lemma 7.1.13 and Proposition 7.1.14, $B(2) \cong B(1) + \mathbf{1} \cong \mathbf{1} + \mathbf{1}$. But the subset classifier $\mathbf{2}$ is the disjoint union of its two one-element subsets $\{\mathsf{T}\}$ and $\{\mathsf{F}\}$, so it too is the coproduct $\mathbf{1} + \mathbf{1}$. Since coproducts are unique up to isomorphism, $B(2)$ and the subset classifier $\mathbf{2}$ are isomorphic. Hence the notation '$\mathbf{2}$' is unambiguous.

## 7.2 Induction and recursion

Theorem 7.1.1 is the principle of mathematical induction, but you know that we sometimes need a more powerful principle: *strong* induction. This states that any property $P(n)$ of natural numbers $n$ satisfying

$$(P(i) \text{ for all } i < n) \implies P(n)$$

$(n \in \mathbb{N})$ must hold for all $n \in \mathbb{N}$.

**Exercise 7.2.1** In the principle of strong induction, why is no base case needed?

To prove the principle of strong induction, the following notation will be useful.

**Definition 7.2.2** Let $\leq$ be an order relation on a set $X$. For $x \in X$, we write $\downarrow x$ for the subset $\{y \in X : y < x\}$ of $X$.

**Remark 7.2.3** In the case of the usual order $\leq$ on $\mathbb{N}$, when $x = n \in \mathbb{N}$, we have met $\downarrow n$ before: it is the set $\mathbf{n}$ (previously called $B(n)$). We tend to use the notation $\downarrow n$ when we are considering it as a *subset* of $\mathbb{N}$, and $\mathbf{n}$ when we are considering it as a mere *set* (that is, ignoring its inclusion function into $\mathbb{N}$).

**Theorem 7.2.4 (Principle of strong induction)** *Let $A$ be a subset of $\mathbb{N}$ such that for all $n \in \mathbb{N}$,*

$$(i \in A \text{ for all natural numbers } i < n) \implies n \in A.$$

*Then $A = \mathbb{N}$.*

**Proof** First we prove by ordinary induction (Theorem 7.1.1) that $\downarrow n \subseteq A$ for all $n \in \mathbb{N}$. The base case $n = 0$ is immediate, since $\downarrow 0$ is empty. For the inductive step, assume that $\downarrow n \subseteq A$. Then $n \in A$ by hypothesis, so $\downarrow n \cup \{n\} \subseteq A$. That is, $\{m \in \mathbb{N} : m \leq n\} \subseteq A$. By Lemma 7.1.10(v), an equivalent statement is $\downarrow s(n) \subseteq A$, completing the induction.

Now let $n \in \mathbb{N}$. We have $n < s(n)$ (Exercise 7.1.23), so $n \in \downarrow s(n) \subseteq A$, so $n \in A$. Hence $A = \mathbb{N}$. □

**Example 7.2.5** Here we use strong induction to show that every nonempty subset of $\mathbb{N}$ has a least element. Terminology: for a set $X$ with order $\leq$, a **least** element of a subset $A \subseteq X$ is an element $a \in A$ such that $a \leq b$ for all $b \in A$. By antisymmetry, a subset can have at most one least element. But not every subset has one; for example, the set of strictly positive reals as a subset of $\mathbb{R}$ with its usual order has no least element. (A least element of $A$ must be an element of $A$!)

In fact, we will prove the contrapositive: a subset $A \subseteq \mathbb{N}$ with no least element is empty. Take such an $A$. Our inductive hypothesis on $n \in \mathbb{N}$ is that $n \notin A$.

Let $n \in \mathbb{N}$, and suppose that $i \notin A$ for all $i < n$. Since $\leq$ is a *total* order, $i \geq n$ for all $i \in A$. So if $n \in A$ then $n$ is least in $A$, contradicting our assumption on $A$. Hence $n \notin A$. Thus, by Theorem 7.2.4, $n \notin A$ for all $n \in \mathbb{N}$, and so $A$ is empty.

*The rest of Section 7.2 is optional and non-examinable.*

People often talk about constructing or defining a sequence 'inductively'. Strictly speaking, it's only proofs that are inductive; the proper word for an 'inductive' construction is *recursive*. For example, when we say that the factorial function is defined by $0! = 1$ and $(n+1)! = (n+1) \cdot n!$, that's a recursive definition (and we'll see why it's valid soon).

The definition of natural number system involves recursion of a simple kind: given an element $a$ of a set $X$ and a function $r : X \to X$, there is a unique sequence $(x_n)_{n \in \mathbb{N}}$ in $X$ such that

$$x_0 = a, \qquad x_{n+1} = r(x_n) \text{ for all } n \in \mathbb{N},$$

as we saw in Section 3.3.

This simple kind of recursion certainly has its uses. For example, it can be used to derive a description of the equivalence relation generated by a relation that's more explicit than the one in Definition 6.1.5. A question on Workshop 4 shows you how.

However, this is still recursion of a very limited kind. For example, it doesn't capture the definition of factorial, because we'd want to take $r$ to be the function $x \mapsto (n+1)x$, which depends on $n$, and that's not allowed. So we need a more powerful recursion principle.

More generally, we want to capture recursive definitions of sequences $(x_n)$ where $x_n$ may depend not just on $x_{n-1}$ and $n$, but on all previous members $x_0, \ldots, x_{n-1}$. Random example: we should be able to define a sequence $(x_n)_{n\in\mathbb{N}}$ of natural numbers by

$$x_n = nx_0 + (n-1)x_1 + \cdots + 2x_{n-2} + x_{n-1} + 1.$$

What I mean by 'capture' is that we want to know that there *exists* a sequence with this property. (And we want uniqueness, but it's existence that's the main challenge.) It's a situation now familiar to you: conceivably our axioms aren't powerful enough to guarantee that such a sequence exists, and it will be another piece of evidence that our axioms are well chosen if they *do* guarantee this.

Informally, the theorem we're about to meet says the following. Take a set $X$ and, for each $n \in \mathbb{N}$, a function $r_n \colon X^n \to X$. Then there exists a unique sequence $(x_n)$ in $X$ such that

$$x_n = r_n(x_0, x_1, \ldots, x_{n-1}) \tag{7.3}$$

for all $n \in \mathbb{N}$.

Before I say more, let's get a couple of details out of the way. The notation '$X^n$' is best interpreted as the function set $X^{\mathbf{n}}$, so we want $r_n$ to be a function $X^{\mathbf{n}} \to X$. A sequence $(x_n)$ in $X$ is a function $f \colon \mathbb{N} \to X$, and equation (7.3) then states that $f(n) = r_n(f|_{\downarrow n})$, where $f|_{\downarrow n}$ means the restriction of $f$ to $\downarrow n$.

To state the result formally, we need to say exactly what type of thing the sequence of functions $(r_n)_{n\in\mathbb{N}}$ is. Since $r_n \in X^{(X^{\mathbf{n}})}$ for each $n$, the whole sequence $(r_n)_{n\in\mathbb{N}}$ should be an element of the product $\prod_{n\in\mathbb{N}} X^{(X^{\mathbf{n}})}$. But there's an implicit assumption here: that there *exists* a family of sets $(S_n)_{n\in\mathbb{N}}$ with $S_n \cong X^{(X^{\mathbf{n}})}$ for each $n \in \mathbb{N}$. (Uniqueness is guaranteed by Lemma 6.5.10.)

This is true, but we haven't proved it. The general fact is that given families of sets $(X_i)_{i\in I}$ and $(Y_i)_{i\in I}$, there is a family of sets $(Z_i)_{i\in I}$ such that $Z_i \cong Y_i^{X_i}$ for each $i \in I$. Applying this principle to the constant family $(X)_{n\in\mathbb{N}}$ and the family $(\mathbf{n})_{n\in\mathbb{N}}$ gives the family $(X^{\mathbf{n}})_{n\in\mathbb{N}}$, then applying it again gives the family $(X^{(X^{\mathbf{n}})})_{n\in\mathbb{N}}$, whose product we can then form.

(Similarly, given $(X_i)_{i\in I}$ and $(Y_i)_{i\in I}$, we can construct families $(X_i + Y_i)_{i\in I}$ and $(X_i \times Y_i)_{i\in I}$. These are relatively easy, but the one with function sets is harder.)

Here is our general recursion principle.

**Proposition 7.2.6** *Let $X$ be a set and $(r_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} X^{(X^{\mathbf{n}})}$. Then there exists a unique function $f \colon \mathbb{N} \to X$ such that $f(n) = r_n(f|_{\downarrow n})$ for all $n \in \mathbb{N}$.*

**Proof** Uniqueness follows by strong induction. The proof of existence is omitted but not too hard; ultimately it relies on the universal property of $\mathbb{N}$. □

**Digression 7.2.7** Even Proposition 7.2.6 is not the most general recursion principle for sequences. For example, consider the following 'definition' of a sequence $(x_n)$ in $\mathbb{Q}$:

$$x_0 = 2, \quad x_{n+1} = \frac{1}{1 - x_n} \ (n \in \mathbb{N}),$$

or the following 'definition' of a sequence $(y_n)$ in $\mathbb{R}$:

$$y_n = (n+1)\left(3 + \sqrt{1 - \frac{y_0 + \cdots + y_{n-1}}{2n(n+1)}}\right).$$

In the first case, the definition only makes sense if $x_n$ never takes the value 1, otherwise we're dividing by 0. In the second, we need to make sure we're never trying to take the square root of a negative number. In both cases, we want to simultaneously define the sequence and prove by induction that the definition makes sense. Proposition 7.2.6 doesn't cover this scenario.

So, we can dream of a more general recursion principle able to handle this kind of example. There is one, but I won't explain it here.

## 7.3 The integers

To construct $\mathbb{Z}$ from $\mathbb{N}$, we need to create room for subtraction. The rough idea is to define $\mathbb{Z}$ as the set of 'expressions' $m - n$ with $m, n \in \mathbb{N}$, much as you might define $\mathbb{C}$ as the set of 'expressions' $x + yi$ with $x, y \in \mathbb{R}$. However, we want $3 - 5$ to mean the same thing as $8 - 10$ (for instance), so we need to quotient out by a suitable equivalence relation.

These 'expressions' are essentially just pairs $(m, n) \in \mathbb{N} \times \mathbb{N}$. We want to declare $(m, n)$ to be equivalent to $(m', n')$ if $m - n = m' - n'$. This doesn't make sense yet, as $m - n$ and $m' - n'$ aren't necessarily natural numbers, and anyway we haven't defined subtraction. But fortunately, this condition can be rearranged to banish negativity: it's equivalent to $m + n' = m' + n$.

So, in this section we write $\sim$ for the relation on $\mathbb{N} \times \mathbb{N}$ defined by

$$(m, n) \sim (m', n') \iff m + n' = m' + n$$

$(m, m', n, n' \in \mathbb{N})$.

**Lemma 7.3.1** *The relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ is an equivalence relation.*

**Proof** Reflexivity and symmetry are immediate. For transitivity, suppose that $(m, n) \sim (m', n') \sim (m'', n'')$. Then

$$m + n' = m' + n, \qquad m' + n'' = m'' + n',$$

and we want to show that $m + n'' = m'' + n$. Using the two equations above,

$$m + n' + n'' = m' + n + n'' = n + m' + n'' = n + m'' + n'.$$

Hence $m + n' + n'' = n + m'' + n'$. By Lemma 7.1.22, we can cancel $n'$, giving the result. □

**Definition 7.3.2** The set $\mathbb{Z}$ of **integers** is $(\mathbb{N} \times \mathbb{N})/\sim$.

Thus, an integer is an equivalence class $[(m, n)]_\sim$ with $m, n \in \mathbb{N}$. To reduce clutter, we write this as $[m, n]$ (and think of it as '$m - n$', although we haven't defined subtraction yet). In this section, we write $i : \mathbb{N} \to \mathbb{Z}$ for the function given by $i(n) = [n, 0]$, and we call $i$ the **inclusion** of $\mathbb{N}$ into $\mathbb{Z}$.

**Exercise 7.3.3** Prove that $i$ is injective.

**Digression 7.3.4** You might be thinking there's an easier way. We should have $\mathbb{Z} = \{0, 1, 2, \ldots\} \cup \{-1, -2, \ldots\}$, which looks like the disjoint union of two copies of $\mathbb{N}$. Can't we construct $\mathbb{Z}$ that way?

We can, but we'd probably regret it. The problem is that everything would split into cases. Think about how you'd define the sum $a + b$ of two integers: you'd have to consider different cases according to the signs of $a$ and $b$, and maybe of $a + b$ too. The same goes for multiplication. And life would get even worse when you came to prove laws like associativity and distributivity involving *three* numbers. Case-by-case arguments are a last resort, and mathematicians usually try to avoid them, for good reason.

To define the addition and multiplication functions $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, we will need to deal with $\mathbb{Z} \times \mathbb{Z}$, which is the product of two quotient sets. We'll need this lemma:

**Lemma 7.3.5** *Let $\sim_1$ be an equivalence relation on a set $X$ and $\sim_2$ an equivalence relation on a set $Y$. Then the relation $\sim$ on $X \times Y$ defined by*

$$(x, y) \sim (x', y') \iff x \sim_1 x' \text{ and } y \sim_2 y'$$

*$(x, x' \in X,\ y, y' \in Y)$ is an equivalence relation. Moreover,*

$$(X \times Y)/\sim \cong X/\sim_1 \times Y/\sim_2.$$

**Proof** You did this as an exercise at the start of a recent class. The second part is done by applying the first isomorphism theorem to

$$\pi_{\sim_1} \times \pi_{\sim_2} : X \times Y \to X/\sim_1 \times Y/\sim_2.$$

□

Define $0_{\mathbb{Z}}, 1_{\mathbb{Z}} \in \mathbb{Z}$ by $0_{\mathbb{Z}} = i(0) = [0,0]$ and $1_{\mathbb{Z}} = i(1) = [1,0]$. Here the unsubscripted 0 and 1 are elements of $\mathbb{N}$. Very soon, I will drop the subscripts on $0_{\mathbb{Z}}$ and $1_{\mathbb{Z}}$ too. And similarly, $+$ with no subscript will for now denote addition on $\mathbb{N}$, whereas addition on $\mathbb{Z}$ will temporarily be denoted by $+_{\mathbb{Z}}$, until we relax and call it $+$ too.

To define addition, the idea is that $(k-\ell)+(m-n)$ should be $(k+m)-(\ell+n)$.

**Lemma 7.3.6** *There exists a unique function $+_{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ such that*

$$[k,\ell] +_{\mathbb{Z}} [m,n] = [k+m, \ell+n]$$

*for all $k, \ell, m, n \in \mathbb{N}$ (where $a +_{\mathbb{Z}} b$ means $+_{\mathbb{Z}}(a,b)$).*

**Proof** By Lemma 7.3.5 and the universal property of quotients (Proposition 6.2.8), it is enough to show that the function

$$\begin{array}{rccc} f: & (\mathbb{N}\times\mathbb{N}) \times (\mathbb{N}\times\mathbb{N}) & \to & \mathbb{Z} \\ & ((k,\ell),(m,n)) & \mapsto & [k+m, \ell+n] \end{array}$$

has the property that

$$\big((k,\ell) \sim (k',\ell') \text{ and } (m,n) \sim (m',n')\big) \implies [k+m,\ell+n] = [k'+m',\ell'+n'].$$

(Or in the usual loose language discussed in Example 6.2.10, our task is to show that $+_{\mathbb{Z}}$ is 'well defined'.) Explicitly, this means showing that

$$\big(k+\ell' = k'+\ell \text{ and } m+n' = m'+n\big) \implies k+m+\ell'+n' = k'+m'+\ell+n$$

for all $k, k', \ell, \ell', m, m', n, n' \in \mathbb{N}$. This follows by adding together the first two equations and using the laws for addition of natural numbers. □

While we're thinking about addition, we should also think about negatives. The idea now is that $-(m-n)$ should be equal to $n-m$.

**Lemma 7.3.7** *There exists a unique function $\mathbb{Z} \to \mathbb{Z}$, written as $a \mapsto -a$, such that $-[m,n] = [n,m]$ for all $m, n \in \mathbb{N}$.*

**Proof** Just as in the proof of the last lemma, we have to show that

$$(m,n) \sim (m',n') \implies (n,m) \sim (n',m'),$$

or equivalently that

$$m+n' = m'+n \implies n+m' = n'+m.$$

This follows from commutativity of addition on $\mathbb{N}$. □

Naturally, we write $a - b$ to mean $a + (-b)$, for $a, b \in \mathbb{Z}$. Then for $m, n \in \mathbb{N}$,

$$i(m) - i(n) = [m, 0] + (-[n, 0]) = [m, 0] + [0, n] = [m, n],$$

so $[m, n] = i(m) - i(n)$. If we don't write the inclusions $i$, this says $[m, n] = m - n$, which was the idea all along.

For multiplication, the motivating thought is that we should have

$$(k - \ell)(m - n) = (km + \ell n) - (kn + \ell m).$$

**Lemma 7.3.8** *There exists a unique function $\cdot_{\mathbb{Z}} \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ such that*

$$[k, \ell] \cdot_{\mathbb{Z}} [m, n] = [km + \ell n, kn + \ell m]$$

*for all $k, \ell, m, n \in \mathbb{N}$ (where $a \cdot_{\mathbb{Z}} b$ means $\cdot_{\mathbb{Z}}(a, b)$).*

**Proof** This is similar to the proof of Lemma 7.3.6 but a little more complicated. You can try it for yourself now, or wait for the guided question on Workshop 4. □

**Proposition 7.3.9** *$\mathbb{Z}$ is a commutative ring under the operations defined above. That is, the following laws hold for all $a, b, c \in \mathbb{Z}$ (dropping the $\mathbb{Z}$ subscripts and writing $a \cdot b$ as $ab$).*

*i. Addition and subtraction laws: $a+b = b+a$, $a+0 = a$, $(a+b)+c = a+(b+c)$, and $a - a = 0$.*

*ii. Multiplication laws: $ab = ba$, $a1 = a$, and $(ab)c = a(bc)$.*

*iii. Distributivity laws: $a(b + c) = ab + ac$ and $a0 = 0$.*

**Proof** Straightforward, if tedious. For example, let us prove the distributivity law $a(b + c) = ab + ac$. Write

$$a = [a_+, a_-], \quad b = [b_+, b_-], \quad c = [c_+, c_-].$$

On the one hand,

$$\begin{aligned} a(b + c) &= [a_+, a_-]([b_+, b_-] + [c_+, c_-]) \\ &= [a_+, a_-][b_+ + c_+, b_- + c_-] \\ &= [a_+(b_+ + c_+) + a_-(b_- + c_-), a_+(b_- + c_-) + a_-(b_+ + c_+)] \\ &= [a_+b_+ + a_+c_+ + a_-b_- + a_-c_-, a_+b_- + a_+c_- + a_-b_+ + a_-c_+]. \end{aligned}$$

On the other,

$$\begin{aligned} ab + ac &= [a_+, a_-][b_+, b_-] + [a_+, a_-][c_+, c_-] \\ &= [a_+b_+ + a_-b_-, a_+b_- + a_-b_+] + [a_+c_+ + a_-c_-, a_+c_- + a_-c_+] \\ &= [a_+b_+ + a_-b_- + a_+c_+ + a_-c_-, a_+b_- + a_-b_+ + a_+c_- + a_-c_+]. \end{aligned}$$

Comparing the two expressions and using the commutativity of addition in $\mathbb{N}$, we see that $a(b + c) = ab + ac$. □

The algebraic structure on $\mathbb{Z}$ is compatible with that on $\mathbb{N}$, via the inclusion $i\colon \mathbb{N} \to \mathbb{Z}$:

**Lemma 7.3.10** *$i(0) = 0_{\mathbb{Z}}$ and $i(1) = 1_{\mathbb{Z}}$; also $i(m+n) = i(m) +_{\mathbb{Z}} i(n)$ and $i(mn) = i(m) \cdot_{\mathbb{Z}} i(n)$ for all $m, n \in \mathbb{N}$.*

**Proof** The first two equations are simply the definitions of $0_{\mathbb{Z}}$ and $1_{\mathbb{Z}}$, and the last two follow easily from the definitions of $+_{\mathbb{Z}}$ and $\cdot_{\mathbb{Z}}$. □

This lemma makes it safe to write $n$ to mean $i(n)$ (for $n \in \mathbb{N}$) and to write $+$ for both $+_{\mathbb{N}}$ and $+_{\mathbb{Z}}$, and similarly for 0, 1 and $\cdot$. It ensures there is no ambiguity.

Next, we give the integers an order.

**Definition 7.3.11** The relation $\leq$ on $\mathbb{Z}$ is defined by

$$a \leq b \iff b = n + a \text{ for some } n \in \mathbb{N}$$

$(a, b \in \mathbb{Z})$.

Strictly speaking, this expression '$b = n + a$' should be '$b = i(n) + a$', but I am dropping the inclusion function $i$. Note that $b \geq 0$ if and only if $b \in \mathbb{N}$.

**Lemma 7.3.12** *$\leq$ is a total order on $\mathbb{Z}$.*

**Proof** Reflexivity holds since $a = 0 + a$ for all $a \in \mathbb{Z}$.

Transitivity: let $a, b, c \in \mathbb{Z}$ with $a \leq b \leq c$. Then $b = n + a$ and $c = m + b$ for some $n, m \in \mathbb{N}$, so $c = (m + n) + a$ with $m + n \in \mathbb{N}$, giving $a \leq c$.

Antisymmetry: let $a, b \in \mathbb{Z}$ with $a \leq b \leq a$. Then $b = n + a$ and $a = m + b$ for some $n, m \in \mathbb{N}$, giving $a = m + n + a$. Subtracting $a$ from each side gives $m + n = 0$, so $m = n = 0$ by Lemma 7.1.21. Hence $a = b$.

Totality: let $a, b \in \mathbb{Z}$. Write $a = [m_+, m_-]$ and $b = [n_+, n_-]$. Since the order $\leq_{\mathbb{N}}$ on $\mathbb{N}$ is total (Lemma 7.1.26), we may assume without loss of generality that $m_+ + n_- \leq_{\mathbb{N}} n_+ + m_-$ (otherwise swap the roles of $a$ and $b$). By definition of $\leq_{\mathbb{N}}$, this means $m_+ + n_- + k = n_+ + m_-$ for some $k \in \mathbb{N}$. It follows that $[m_+, m_-] + [k, 0] = [n_+, n_-]$, or equivalently, $a + k = b$. Hence $a \leq b$. □

It is immediate from the definitions that the order on $\mathbb{Z}$ is compatible with the order on $\mathbb{N}$: for $m, n \in \mathbb{N}$, we have $m \leq_{\mathbb{N}} n$ if and only if $i(m) \leq_{\mathbb{Z}} i(n)$. It is also compatible with the algebraic structure on $\mathbb{Z}$:

**Lemma 7.3.13** *i. $a \leq b \implies a + c \leq b + c$, for $a, b, c \in \mathbb{Z}$;*

*ii. $a, b \geq 0 \implies ab \geq 0$, for $a, b \in \mathbb{Z}$.*

The jargon for this is that $\mathbb{Z}$ is an **ordered ring**.

**Proof** For (i), suppose that $a \leq b$. Then $n + a = b$ for some $n \in \mathbb{N}$, and then also $n + a + c = b + c$, giving $a + c \leq b + c$.

For (ii), suppose that $a, b \geq 0$. Then $a = i(m)$ and $b = i(n)$ for some $m, n \in \mathbb{N}$, giving $ab = i(mn)$ with $mn \in \mathbb{N}$, and so $ab \geq 0$. □

**Lemma 7.3.14** *$a \leq 0 \iff -a \geq 0$, for all $a \in \mathbb{Z}$.*

**Proof** Both implications follow from Lemma 7.3.13(i), taking $c = \pm a$. □

We now use the order on $\mathbb{Z}$ to deduce non-order-theoretic properties.

**Lemma 7.3.15** *i. $ab = 0 \implies a = 0$ or $b = 0$, for $a, b \in \mathbb{Z}$.*

*ii. $ac = bc \implies a = b$, for $a, b, c \in \mathbb{Z}$ with $c \neq 0$.*

*iii. $a \leq b \iff ac \leq bc$, for $a, b, c \in \mathbb{Z}$ with $c > 0$.*

**Proof** For (i), let $a, b \in \mathbb{Z}$ with $ab = 0$. By Lemma 7.3.12, either $a \geq 0$ or $a \leq 0$, and either $b \geq 0$ or $b \leq 0$. (Yes, we're going to do a proof by cases!)

If $a \geq 0$ and $b \geq 0$ then $a \in \mathbb{N}$ and $b \in \mathbb{N}$, so $a = 0$ or $b = 0$ by Lemma 7.1.21.

Suppose that $a \geq 0$ and $b \leq 0$. By Lemma 7.3.14, $-b \geq 0$. Now $a(-b) = -(ab) = 0$, so by the first case, $a = 0$ or $-b = 0$. Hence $a = 0$ or $b = 0$.

The other two cases are similar.

For (ii), if $ac = bc$ then $(a - b)c = 0$, and (i) then gives $a - b = 0$ or $c = 0$.

For (iii), if $a \leq b$ then $b - a \geq 0$, so $(b - a)c \geq 0$ by Lemma 7.3.13(ii), so $ac \leq bc$. To prove the converse, we show that $a > b \implies ac > bc$. Indeed, if $a > b$ then $a - b, c > 0$, which by Lemma 7.3.13(ii) and part (i) of this lemma implies $(a - b)c > 0$, that is, $ac > bc$. □

## 7.4 The rational numbers

Building $\mathbb{Q}$ from $\mathbb{Z}$ is very much like building $\mathbb{Z}$ from $\mathbb{N}$. Instead of creating room to subtract, we now have to create room to divide. We use the same idea: a rational number should be an 'expression' $a/b$ where $a, b \in \mathbb{Z}$ with $b \neq 0$, and two 'expressions' $a/b$ and $a'/b'$ should be regarded as the same if $ab' = a'b$.

Write $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. In this section, I will write $\sim$ for the relation on $\mathbb{Z} \times \mathbb{Z}^*$ defined by

$$(a, b) \sim (a', b') \iff ab' = a'b$$

$(a, a' \in \mathbb{Z}, b, b' \in \mathbb{Z}^*)$.

**Lemma 7.4.1** *$\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^*$.*

**Proof** The proof is very much like the proof of Lemma 7.3.1, but with multiplication instead of addition. In the final step, we use the fact that it is possible to cancel nonzero factors in $\mathbb{Z}$ (Lemma 7.3.15(ii)). □

**Exercise 7.4.2** Give a detailed proof of Lemma 7.4.1.

**Definition 7.4.3** The set $\mathbb{Q}$ of **rational numbers** is $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$.

We write the equivalence class $[(a, b)]_\sim$ of $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ as $[a, b]$. In this section, I will write $i : \mathbb{Z} \to \mathbb{Q}$ for the function $a \mapsto [a, 1]$. You can check that $i$ is injective; we call it the **inclusion** of $\mathbb{Z}$ into $\mathbb{Q}$.

Define $0_\mathbb{Q} = i(0)$ and $1_\mathbb{Q} = i(1)$, where $0, 1 \in \mathbb{Z}$. We now define addition and multiplication on $\mathbb{Q}$. As in the last section, we sometimes use subscripts like $+_\mathbb{Q}$ to clarify where the operations are taking place, but usually we drop them.

**Remark 7.4.4** Explicitly, $0_\mathbb{Q} = [0, 1]$. So for $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, we have $[a, b] = 0_\mathbb{Q}$ if and only if $(a, b) \sim (0, 1)$, if and only if $a = 0$.

To define addition, the idea is that we should have $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.

**Lemma 7.4.5** *There exists a unique function $+_\mathbb{Q} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ such that*

$$[a, b] +_\mathbb{Q} [c, d] = [ad + bc, bd]$$

*for all $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{Z}^*$.*

**Proof** As in the proof of Lemma 7.4.5, we have to show that if $(a, b), (a', b') \in \mathbb{Z} \times \mathbb{Z}^*$ with $(a, b) \sim (a', b')$, and $(c, d), (c', d') \in \mathbb{Z} \times \mathbb{Z}^*$ with $(c, d) \sim (c', d')$, then

$$(ad + bc, bd) \sim (a'd' + b'c', b'd').$$

Explicitly, this means

$$(ab' = a'b \text{ and } cd' = c'd) \implies (ad + bc)b'd' = (a'd' + b'c')bd,$$

which is easily shown using distributivity in $\mathbb{Z}$. □

**Lemma 7.4.6** *There exists a unique function $\mathbb{Q} \to \mathbb{Q}$, written as $q \mapsto -q$, such that $-[a, b] = [-a, b]$ for all $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^*$.*

**Proof** We have to show that

$$(a, b) \sim (a', b') \implies (-a, b) \sim (-a', b'),$$

which follows from the definition of $\sim$ and algebraic properties of $\mathbb{Z}$. □

**Lemma 7.4.7** *There exists a unique function* $\cdot_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ *such that*

$$[a, b] \cdot_{\mathbb{Q}} [c, d] = [ac, bd]$$

*for all* $a, c \in \mathbb{Z}$ *and* $b, d \in \mathbb{Z}^*$.

**Proof** This is similar to the last two proofs. □

What distinguishes $\mathbb{Q}$ from $\mathbb{N}$ and $\mathbb{Z}$ is that we can take reciprocals:

**Lemma 7.4.8** *There is a unique function* $\mathbb{Q} \setminus \{0\} \to \mathbb{Q}$, *written as* $q \mapsto q^{-1}$, *such that* $1/[a, b] = [b, a]$ *for all* $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$.

Recall from Remark 7.4.4 that $[a, b] \neq 0_{\mathbb{Q}}$ if and only if $a \neq 0$. For '$[b, a]$' to even make sense, we need $a \neq 0$, which is why I have written $\mathbb{Z}^* \times \mathbb{Z}^*$ rather than $\mathbb{Z} \times \mathbb{Z}^*$.

**Proof** We have to show that if $(a, b) \sim (a', b')$ then $(b, a) \sim (b', a')$, for all $a, b, a', b' \in \mathbb{Z}^*$. This just says $ab' = a'b \implies ba' = b'a$. □

As you'd expect, given $q, r \in \mathbb{Q}$ with $r \neq 0$, we write $q/r$ for $q \cdot r^{-1}$. For $a, b \in \mathbb{Z}$ with $b \neq 0$,

$$i(a)/i(b) = [a, 1] \cdot [b, 1]^{-1} = [a, 1][1, b] = [a, b],$$

so $[a, b] = i(a)/i(b)$. If we don't write the inclusions $i$, this says $[a, b] = a/b$, which was the idea all along.

**Proposition 7.4.9** $\mathbb{Q}$ *is a field under the operations defined above. That is, the same laws hold as listed for* $\mathbb{Z}$ *in Proposition 7.3.9, and every nonzero element* $q \in \mathbb{Q}$ *has a multiplicative inverse.*

**Proof** Verifying the ring laws is another series of explicit checks, using the ring laws that we already know to hold for $\mathbb{Z}$. One also checks that for each nonzero $q \in \mathbb{Q}$, the element $q^{-1}$ constructed in Lemma 7.4.8 satisfies $q \cdot q^{-1} = 1$. □

It is easy to check that the inclusion $i\colon \mathbb{Z} \to \mathbb{Q}$ is a ring homomorphism:

$$\begin{aligned} i(a+b) &= i(a) + i(b), & i(0) &= 0, & i(-a) &= -i(a), \\ i(ab) &= i(a)i(b), & i(1) &= 1 \end{aligned}$$

for all $a, b \in \mathbb{Z}$. This allows us to drop the $i$ and the subscripts on $+$, $0$, etc.

Next, we define the order on $\mathbb{Q}$. To do it, we need a small observation, which basically says that a fraction can always be written with a *positive* denominator.

**Lemma 7.4.10** *For all $q \in \mathbb{Q}$, there exist $a, b \in \mathbb{Z}$ such that $q = [a, b]$ and $b > 0$.*

**Proof** By definition, $q = [c, d]$ for some $c, d \in \mathbb{Z}$ with $d \neq 0$. If $d > 0$, we are done. Otherwise, $d < 0$ since the order on $\mathbb{Z}$ is total, and Lemma 7.3.14 then implies that $-d > 0$. Now $q = [-c, -d]$ with $-d > 0$. □

To define $\leq_{\mathbb{Q}}$, the idea is that we should have $a/b \leq c/d$ if and only if $ad \leq bc$, *assuming* that $b, d > 0$.

**Lemma 7.4.11** *There is a unique relation $\leq_{\mathbb{Q}}$ on $\mathbb{Q}$ such that*

$$[a, b] \leq_{\mathbb{Q}} [c, d] \iff ad \leq bc$$

*for all $a, b, c, d \in \mathbb{Z}$ with $b, d > 0$.*

**Proof** Uniqueness follows from Lemma 7.4.10. For existence, we have to check that if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$ then $ad \leq bc \iff a'd' \leq b'c'$, for all integers $a, a', c, c'$ and positive integers $b, b', d, d'$.

So, assume that $ab' = a'b$, $cd' = c'd$. Using Lemma 7.3.15(iii),

$$ad \leq bc \iff ab'dd' \leq bb'cd' \iff a'bdd' \leq bb'c'd \iff a'd' \leq b'c',$$

as required. □

**Lemma 7.4.12** *$\leq_{\mathbb{Q}}$ is a total order on $\mathbb{Q}$.*

**Proof** I will prove that $\leq_{\mathbb{Q}}$ is total and leave the proof that it is an order to you. Let $q, r \in \mathbb{Q}$. By Lemma 7.4.10, $q = [a, b]$ and $r = [c, d]$ for some $a, b, c, d \in \mathbb{Z}$ with $b, d > 0$. Since the order on $\mathbb{Z}$ is total, $ad \leq bc$ or $bc \leq ad$. Hence $[a, b] \leq [c, d]$ or $[c, d] \leq [a, b]$, as required. □

The inclusion $i\colon \mathbb{Z} \to \mathbb{Q}$ is compatible with the orders on $\mathbb{Z}$ and $\mathbb{Q}$, since

$$i(a) \leq_{\mathbb{Q}} i(b) \iff [a, 1] \leq_{\mathbb{Q}} [b, 1] \iff a \cdot 1 \leq_{\mathbb{Z}} b \cdot 1 \iff a \leq_{\mathbb{Z}} b.$$

Hence we can drop the subscripts and just write $\leq$.

Finally, $\mathbb{Q}$ is an **ordered field**, which means the following.

**Lemma 7.4.13** *i.* $q \leq r \implies q + s \leq r + s$, *for* $q, r, s \in \mathbb{Q}$;

*ii.* $q, r \geq 0 \implies qr \geq 0$, *for* $q, r \in \mathbb{Q}$.

**Proof** To prove (i), it is enough to show that $q \leq r \iff 0 \leq r - q$ for all $q, r \in \mathbb{Q}$, since $(r + s) - (q + s) = r - q$.

So, let $q, r \in \mathbb{Q}$. Writing $q = [a, b]$ and $r = [c, d]$ with $a, b, c, d \in \mathbb{Z}$ and $b, d > 0$, we have $r - q = [bc - ad, bd]$. Note that $bd > 0$, by Lemmas 7.3.13(ii) and 7.3.15(i). Hence

$$q \leq r \iff ad \leq bc \iff bc - ad \geq 0 \iff r - q \geq 0,$$

as required.

Part (ii) follows from the definition of multiplication and the analogous result for $\mathbb{Z}$, Lemma 7.3.13(ii). □

## 7.5 The real numbers

This week's climax is the construction of the real numbers. To do it, the key insight is that between any two real numbers, there should lie at least one rational number (in fact, infinitely many, but never mind). You probably saw this proved in Proofs and Problem Solving, and it's also clear if you think about decimal expansions: for example, between the real numbers 2.498357 . . . and 2.498362 . . ., there lies the rational number 2.49836.

It follows that for distinct real numbers $x$ and $y$, the subsets $L_x = \{q \in \mathbb{Q} : q \leq x\}$ and $L_y = \{q \in \mathbb{Q} : q \leq y\}$ should be different. And, similarly, the subsets $U_x = \{q \in \mathbb{Q} : q \geq x\}$ and $U_y = \{q \in \mathbb{Q} : q \geq y\}$ should be different. We'll use this idea to define the real numbers.

First, we need some general definitions.

**Definition 7.5.1** Let $X$ be a set with an order $\leq$, and let $A \subseteq X$. A **lower bound** of $A$ in $X$ is an element $\ell \in X$ such that $\ell \leq a$ for all $a \in A$. We write

$$\mathrm{lb}(A) = \{\ell \in X : \ell \text{ is a lower bound of } A\}.$$

The set $\mathrm{ub}(A)$ of **upper bounds** is defined similarly.

**Warning 7.5.2** Lower bounds of $A$ do not have to belong to $A$. For example, taking $X$ to be $\mathbb{N}$ with its usual ordering, 38 is a lower bound of $\{90, 95\}$. In fact, $\mathrm{lb}(\{90, 95\}) = \{0, 1, \ldots, 90\}$.

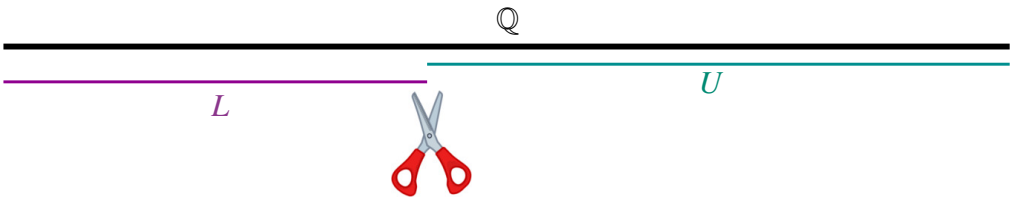



Figure 7.1: A Dedekind cut $(L, U)$.

Each real number $x$ should give rise to a pair $(L_x, U_x)$ of subsets of $\mathbb{Q}$ (as above), in which $L_x$ should be the set of lower bounds of $U_x$ in $\mathbb{Q}$, and similarly $U_x$ should be the set of upper bounds of $L_x$ in $\mathbb{Q}$. Of course, we don't know what a real number is yet. But we will make this the *definition*.

**Definition 7.5.3** A **Dedekind cut** is a pair $(L, U) \in \mathscr{P}(\mathbb{Q}) \times \mathscr{P}(\mathbb{Q})$ such that $L = \mathrm{lb}(U)$ and $U = \mathrm{ub}(L)$ (Figure 7.1). It is **proper** if $L$ and $U$ are nonempty.

**Examples 7.5.4** i. The pairs $(\varnothing, \mathbb{Q})$ and $(\mathbb{Q}, \varnothing)$ are both Dedekind cuts, but not proper. They are the *only* improper Dedekind cuts.

ii. For $q \in \mathbb{Q}$, define

$$\downarrow q = \{r \in \mathbb{Q} : r \leq q\}, \qquad \uparrow q = \{r \in \mathbb{Q} : r \geq q\}.$$

Then $(\downarrow q, \uparrow q)$ is a Dedekind cut. It has the property that $\downarrow q$ has a greatest element (namely, $q$) and $\uparrow q$ has a least element (also $q$).

iii. Let

$$L = \{q \in \mathbb{Q} : q \leq 0 \text{ or } (q \geq 0 \text{ and } q^2 \leq 2)\},$$
$$U = \{q \in \mathbb{Q} : q \geq 0 \text{ and } q^2 \geq 2\}.$$

You can check that $(L, R)$ is a Dedekind cut. The idea is that $L = \{q \in \mathbb{Q} : q \leq \sqrt{2}\}$ and $U = \{q \in \mathbb{Q} : q \geq \sqrt{2}\}$; so in the notation above, $L = L_{\sqrt{2}}$ and $U = U_{\sqrt{2}}$. But of course, we don't have anything called '$\sqrt{2}$' yet, because there is no rational square root of 2. For the same reason, this Dedekind cut has the property that $L$ has no greatest element and $U$ has no least element.

**Exercise 7.5.5** Check that all these examples really are Dedekind cuts.

**Digression 7.5.6** There are several small variations on the notion of Dedekind cut. Some authors use only one of $L$ and $U$, which is fine as each determines the other. Where I have used non-strict inequalities, most authors use strict inequalities; the version here is sometimes called a 'closed Dedekind cut'.

**Definition 7.5.7** The set $\mathbb{R}$ of **real numbers** is

$$\{(L, U) \in \mathscr{P}(\mathbb{Q}) \times \mathscr{P}(\mathbb{Q}) : (L, U) \text{ is a proper Dedekind cut}\}.$$

The **inclusion** $i\colon \mathbb{Q} \to \mathbb{R}$ is defined by $i(q) = (\downarrow q, \uparrow q)$. It is injective, by antisymmetry of $\leq_{\mathbb{Q}}$.

**Lemma 7.5.8** *Let $(L, U)$ be a Dedekind cut. Then the subset $L$ of $\mathbb{Q}$ is* **downwards closed***; that is, if $q, r \in \mathbb{Q}$ with $q \leq r$ and $r \in L$, then $q \in L$. Similarly, $U$ is upwards closed.*

**Proof** Let $q, r \in \mathbb{Q}$ with $q \leq r$ and $r \in L$. Then $r$ is a lower bound of $U$, since $L = \mathrm{lb}(U)$. But $q \leq r$, so $q$ is also a lower bound of $U$. Hence $q \in L$. A similar proof shows that $U$ is upwards closed. □

We now define inequality on $\mathbb{R}$.

**Definition 7.5.9** The relation $\leq_{\mathbb{R}}$ (or just $\leq$) on $\mathbb{R}$ is defined by

$$(L, U) \leq_{\mathbb{R}} (L', U') \iff L \subseteq L'$$

for $(L, U), (L', U') \in \mathbb{R}$.

**Example 7.5.10** Let $q, r \in \mathbb{Q}$. Then $i(q) \leq_{\mathbb{R}} i(r)$ if and only if $\downarrow q \subseteq \downarrow r$. If $\downarrow q \subseteq \downarrow r$ then, since $q \in \downarrow q$, we must have $q \in \downarrow r$; thus, $q \leq r$. Conversely, if $q \leq r$ then any rational number less than or equal to $q$ is less than or equal to $r$, so $\downarrow q \subseteq \downarrow r$. Hence

$$q \leq r \iff i(q) \leq_{\mathbb{R}} i(r).$$

This equivalence makes it safe to not write the subscripts on the $\leq$ signs, or write the inclusion symbol $i$.

**Lemma 7.5.11** *The relation $\leq_{\mathbb{R}}$ on $\mathbb{R}$ is a total order.*

**Proof** That $\leq_{\mathbb{R}}$ is an order follows from $\subseteq$ being an order on $\mathscr{P}(\mathbb{Q})$ (Examples 5.1.22). To see that it is total, let $(L, U), (L', U') \in \mathbb{R}$. If $U = U'$ then $L = \mathrm{lb}(U) = \mathrm{lb}(U') = L'$, so $(L, U) = (L', U')$. Otherwise, we can assume without loss of generality that there is some element $u \in U \setminus U'$. We will show that $(L, U) \leq_{\mathbb{R}} (L', U')$, that is, $L \subseteq L'$.

Let $\ell \in L$. Since $u \in U = \mathrm{ub}(L)$, we have $\ell \leq u$. Also, $u \notin U' = \mathrm{ub}(L')$, so there is some $\ell' \in L'$ such that $u < \ell'$. We now have $\ell \leq u < \ell'$, giving $\ell < \ell'$. But $L'$ is downwards closed (Lemma 7.5.8), so $\ell \in L'$. Hence $L \subseteq L'$. □

As every introduction to analysis tells you, the most important feature of $\mathbb{R}$ is that it's complete. This means every nonempty subset of $\mathbb{R}$ that has an upper bound has a *least* upper bound. (There are other, equivalent, formulations.)

Let's go through the definitions. Let $A \subseteq \mathbb{R}$. A **least upper bound** of $A$ in $\mathbb{R}$ is a least element of the set of upper bounds of $A$ in $\mathbb{R}$. (See Example 7.2.5 for the definition of 'least element'.) That is, a real number $\ell$ is a least upper bound of $A$ if it is an upper bound of $A$ in $\mathbb{R}$, and if $\ell \leq \ell'$ for every upper bound $\ell'$ of $A$ in $\mathbb{R}$.

**Example 7.5.12** Every introduction to analysis also makes the point that a least upper bound of a subset $A \subseteq \mathbb{R}$ need not lie in $A$. For example, the least upper bound of $\{x \in \mathbb{R} : x < 0\}$ is 0.

**Theorem 7.5.13** *Every nonempty subset of $\mathbb{R}$ that has an upper bound has a least upper bound.*

**Proof** *(Non-examinable.)* Let $A$ be a nonempty subset of $\mathbb{R}$ with an upper bound. Put

$$U^+ = \bigcap_{(L,U)\in A} U, \qquad L^+ = \mathrm{lb}(U^+).$$

We will show that $(L^+, U^+)$ is a least upper bound of $A$ in $\mathbb{R}$.

(If you were expecting to take $L^+ = \bigcup_{(L,U)\in A} L$, think about the case $A = \{i(q) : q < 0\}$ to see why this won't work.)

First we have to show that $(L^+, U^+)$ is a real number, that is, a proper Dedekind cut. Properness means that $L^+$ and $U^+$ are nonempty:

- For $L^+$, we are given that $A$ is nonempty, so we can choose some $(L, U) \in A$. Since $(L, U)$ is itself a proper Dedekind cut, $L$ contains some element $\ell$. Then $\ell$ is a lower bound of $U$, which contains $U^+$, so $\ell \in \mathrm{lb}(U^+) = L^+$.

- For $U^+$, we are given that $A$ has an upper bound $(L', U')$. Since this is itself a proper Dedekind cut, $U'$ is nonempty. For all $(L, U) \in A$, we have $L \subseteq L'$ (by definition of upper bound). It follows that $U' \subseteq U$: for if $u' \in U'$ then $u'$ is an upper bound of $L'$, which contains $L$, so $u' \in \mathrm{ub}(L) = U$. So $U' \subseteq U$ for all $(L, U) \in A$, giving $U' \subseteq U^+$. And since $U'$ is nonempty, so is $U^+$.

Now we show that $(L^+, U^+)$ is a Dedekind cut: $L^+ = \mathrm{lb}(U^+)$ and $U^+ = \mathrm{ub}(L^+)$. The first is immediate, so we just have to prove the second.

In one direction, let $u \in U^+$. We must show that $\ell \leq u$ for all $\ell \in L^+$. But this is true by definition of $L^+$ as $\mathrm{lb}(U^+)$.

In the other direction, let $q \in \mathrm{ub}(L^+)$. To prove that $q \in U^+$, let $(L, U) \in A$; we must show that $q \in U$. Now $U = \mathrm{ub}(L)$, so let $\ell \in L$; we must show that

$\ell \leq q$. Since $\ell \in L = \mathrm{lb}(U)$, and $U$ contains $U^+$, we have $\ell \in \mathrm{lb}(U^+) = L^+$. But $q \in \mathrm{ub}(L^+)$, so $\ell \leq q$, as required.

This completes the proof that $(L^+, U^+)$ is a proper Dedekind cut, that is, a real number. Now we have to prove that $(L^+, U^+)$ is a least upper bound of $A$.

First, it is an upper bound. For let $(L, U) \in A$. We have to show that $L \subseteq L^+$, so let $\ell \in L$. Then $\ell$ is a lower bound of $U$, which contains $U^+$, so $\ell \in \mathrm{lb}(U^+) = L^+$.

Second, it is the *least* upper bound. Indeed, let $(L', U') \in \mathbb{R}$ be any upper bound of $A$. For each $u' \in U'$ and $(L, U) \in A$, we have $L \subseteq L'$; but $u'$ is an upper bound of $L'$, so it is an upper bound of $L$, giving $u' \in U$. This proves that $U' \subseteq U^+$. Hence every lower bound of $U^+$ is a lower bound of $U'$; that is, $L^+ \subseteq L'$, as required. □

What's left? We should now define addition and multiplication on $\mathbb{R}$, and prove that they have all the right properties to make $\mathbb{R}$ into an ordered field. However, we're not going to do this. Defining addition and (especially) multiplication of Dedekind cuts is fiddly and not much fun. *Working* with the definitions is even less fun. To get an idea of the obstacles, ask yourself how you'd define $(L, U) \cdot (L', U')$, bearing in mind that the product of two negative numbers is positive. It's not tremendously *difficult* to do all this, just long, but let's spend our time on more rewarding things.

Once the field structure on $\mathbb{R}$ has been established, Theorem 7.5.13 tells us that $\mathbb{R}$ is a *complete* ordered field. It can be shown that up to isomorphism (in the appropriate sense), there is only one complete ordered field. So, all we ever need to know about $\mathbb{R}$ is that it's a complete ordered field. We can now forget about Dedekind cuts entirely. They were only a means to proving that a complete ordered field exists.

Most analysis books begin by taking as given the existence of a complete ordered field, which they call $\mathbb{R}$. That's their starting point, so it can be our finishing point. We hand over the baton, and our work here is done.

# Chapter 8

# Well ordered sets

*To read by Monday 4 November: Sections 8.1 and 8.2.*
*To read by Friday 8 November: Sections 8.3 and 8.4.*
*Optional: Section 8.5.*

Just as there are theories of groups, rings, etc., there is a theory of ordered sets. Just as a group is nothing more than a set equipped with an operation satisfying the group axioms, an ordered set is nothing more than a set equipped with a relation satisfying the order axioms (reflexivity, transitivity and antisymmetry: Definition 5.1.21). Just as the group operation usually denoted by $\cdot$ needn't be anything like ordinary multiplication (and could in fact be addition), the order relation usually denoted by $\leq$ needn't be anything like ordinary 'less than or equal to' (and could in fact be 'greater than or equal to'). And just as different kinds of group are of particular interest (finite, abelian, simple, solvable, ...), so too are different kinds of ordered set (totally ordered sets, lattices, Boolean algebras, ...).

Here, we study the so-called 'well ordered' sets. The theory of well ordered sets is very neat, but the reason we study them is that they turn out to be extremely useful for proving results about *ordinary* sets. For example, we will use well ordered sets, plus other parts of order theory, to prove that $X \times X \cong X$ for every infinite set $X$.

You might wonder how order theory could possibly help to prove a result that seems to have nothing whatsoever to do with order. As a hint of how this comes to be, think about combinatorial arguments with finite sets that you might have done in the past. If you ever found yourself saying 'take the first element of the set...' then you were implicitly choosing an order on your set. Something similar can be done for infinite sets. In fact, well ordered sets are designed as a way to 'count' all the way through even sets that are uncountable—as we'll see.

## 8.1 Definitions and examples

We will be talking a lot about ordered sets. Recall from Definition 5.1.21 that an order $\leq$ on a set $X$ is a relation on $X$ that is reflexive, transitive and antisymmetric, and that an ordered set is a set $X$ together with an order relation $\leq$. Rather than writing 'a set $X$ with an order relation $\leq$' every time, I will just say 'an ordered set $(X, \leq)$', or often simply 'an ordered set $X$', leaving it implicit that the order relation is called $\leq$.

**Warning 8.1.1** There are three standard abuses of notation going on here.

First, the notation $(X, \leq)$ looks like an ordered pair but isn't really: when $a \in A$ and $b \in B$, we write $(a, b)$ for the resulting element of the product $A \times B$, but there is no set containing all possible sets $X$ as elements, nor one containing all possible order relations.

Second, we tend to use the same symbol $\leq$ for the order relation in all ordered sets, just as we typically call the group operation $(g, h) \mapsto gh$ in all groups. We could be more careful, using $\leq$ and $\leq'$ etc., just as the first few pages of an introduction to group theory might use something like $\cdot$ and $*$ for group operations in different groups. But we usually rely on the context to make things clear.

Finally, writing $X$ to mean $(X, \leq)$ is certainly ambiguous. The same set can have multiple orders on it. For example, a two-element set $\{a, b\}$ carries three orders: one where $a \leq b$, one where $b \leq a$, and one where neither holds. But again, it's a standard abuse, just like 'let $G$ be a group' or 'let $X$ be a metric space'.

If we're going to talk about ordered sets, we need to know what it means for them to be isomorphic. Let $X = (X, \leq)$ and $Y = (Y, \leq)$ be ordered sets. An **isomorphism of ordered sets** or **order isomorphism** $X \to Y$ is an order-preserving bijection whose inverse is also order-preserving.

**Exercise 8.1.2** Let $f : X \to Y$ be an order-preserving bijection. Prove that if $X$ is totally ordered then $f$ is an order isomorphism. (A question on Workshop 4 shows that this result fails for general ordered sets.)

If there exists an order isomorphism $X \to Y$, we say that $X$ and $Y$ are **order isomorphic**, or just **isomorphic**, and write $X \cong Y$.

Care is needed, as two ordered sets may be isomorphic *as sets* but not isomorphic *as ordered sets*. (We'll see an example soon.) If it's unclear from the context which is meant, we have to say.

Recall from Example 7.2.5 that for an ordered set $(X, \leq)$ and a subset $A$ of $X$, a least element of $A$ is an element $a \in A$ such that $a \leq b$ for all $b \in A$.

**Definition 8.1.3** An order $\leq$ on a set $W$ is a **well order** if every nonempty subset of $W$ has a least element. A set together with a well order is called a **well ordered set**.

Before I give examples, here's an immediate consequence:

**Lemma 8.1.4** *Every well ordered set is totally ordered.*

**Proof** Let $(W, \leq)$ be a well ordered set. Let $w, w' \in W$. Then $\{w, w'\}$ has a least element. If it's $w$ then $w \leq w'$, and if it's $w'$ then $w' \leq w$. □

**Examples 8.1.5**

i. We proved in Example 7.2.5 that the usual order on $\mathbb{N}$ is a well order: every nonempty set of natural numbers has a least element. Thus, $(\mathbb{N}, \leq)$ is a well ordered set.

When we are viewing $\mathbb{N}$ as a well ordered set, it is traditional to call it $\omega$ rather than $\mathbb{N}$. (That's an omega, not a w.)

ii. For any ordered set $(X, \leq)$ and subset $A \overset{i}{\hookrightarrow} X$, there is an order $\leq'$ on $A$ defined by $a \leq' b \iff i(a) \leq i(b)$. It is called the **induced** order on $A$ (and usually written with the same symbol $\leq$). You can easily check that if $\leq$ is a *well* order on $X$ then the induced order on any subset of $X$ is also a well order.

iii. In particular, let $n \in \mathbb{N}$, and recall the notation $\mathbf{n} = \{i \in \mathbb{N} : i < n\}$ from Remark 7.1.27. Since $\mathbf{n}$ is a subset of $\mathbb{N}$, the induced order on $\mathbf{n}$ is a well order. This is also clear intuitively: every nonempty subset of $\{0, 1, \ldots, n-1\}$ has a least element.

iv. The usual order on $\mathbb{Z}$ is *not* a well order. For example, the subset $\mathbb{Z}$ of $\mathbb{Z}$ has no least element.

v. The usual order on the set $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\}$ is *not* a well order. For example, the subset $(0, \infty) = \{x \in \mathbb{R} : x > 0\}$ of $\mathbb{R}^+$ has no least element. It has a greatest lower bound (infimum) in $\mathbb{R}^+$, namely, 0; but this is not an element of $(0, \infty)$, so it's certainly not a *least* element.

**Warning 8.1.6** For a subset $A$ of an ordered set $X$, a least element of $A$ must, in particular, be an element of $A$. Don't confuse the concepts of least element and greatest lower bound. If $A$ has a least element then, yes, it's a greatest lower bound of $A$ in $X$. But as that last example shows, a greatest lower bound of $A$ in $X$ needn't be a least element of $A$, because it needn't be an element of $A$ at all.

To generate more interesting examples of well ordered sets, two constructions are invaluable.

**Definition 8.1.7** Let $X = (X, \leq_1)$ and $Y = (Y, \leq_2)$ be ordered sets.

i. The **ordinal sum** of $X$ and $Y$ is the coproduct $X + Y$ with the following order relation $\leq$: for $z, z' \in X + Y$, we define $z \leq z'$ if and only if

$$(z, z' \in X \text{ and } z \leq_1 z') \text{ or } (z, z' \in Y \text{ and } z \leq_2 z') \text{ or } (z \in X \text{ and } z' \in Y).$$

ii. The **ordinal product** of $X$ and $Y$ is the product $X \times Y$ with the following order relation $\leq$: for $(x, y), (x', y') \in X \times Y$, we define $(x, y) \leq (x', y')$ if and only if

$$(y <_2 y') \text{ or } (y = y' \text{ and } x \leq_1 x').$$

The idea of the order on the ordinal sum is that $X$ and $Y$ each individually carry the same order as before, and we declare everything in $X$ to be less than everything in $Y$. So it's 'first $X$, then $Y$'.

In the definition of ordinal product, I used the symbol $<_2$. Generally, in any ordered set, $y < y'$ means $y \leq y'$ and $y \neq y'$. You can guess how $\geq$ and $>$ are defined.

The order on the ordinal product is called the **reverse lexicographic order**. It's the order a dictionary is in, in a language like Arabic or Hebrew where words are written from right to left. Here you should imagine a dictionary consisting of only two-letter words.

A question on Workshop 4 asks you to show that the two relations defined in Definition 8.1.7 are indeed orders, for arbitrary ordered sets $X$ and $Y$. But here, we'll only be interested in the case where $X$ and $Y$ are well ordered.

**Lemma 8.1.8** *The ordinal sum and ordinal product of two well ordered sets are well ordered.*

**Proof** Let $(V, \leq_1)$ and $(W, \leq_2)$ be well ordered sets.

To show that their ordinal sum $(V + W, \leq)$ is well ordered, let $\varnothing \neq A \subseteq V + W$. If $A$ contains at least one element of $V$ then the subset $A \cap V$ of $V$ has an element

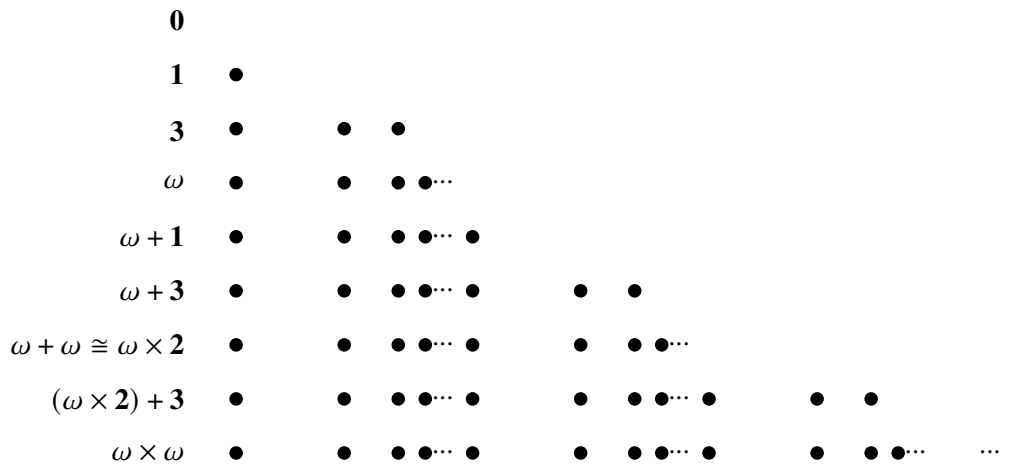



Figure 8.1: Some examples of well ordered sets.

that's least with respect to $\leq_1$, which is then also least in $A$ with respect to $\leq$. Otherwise, $A$ is a nonempty subset of $W$, so it has an element that's least with respect to $\leq_2$, which is then also least in $A$ with respect to $\leq$.

Now take a nonempty subset $A$ of the ordinal product $(V \times W, \leq)$. The subset

$$\{w \in W : (v, w) \in A \text{ for some } v \in V\}$$

of $W$ is nonempty and therefore has a least element $w$. The subset

$$\{v \in V : (v, w) \in A\}$$

is then also nonempty, and so has a least element $v$. Then $(v, w)$ is least in $A$. □

**Warning 8.1.9** Another warning! These addition and multiplication operations do not satisfy many of the algebraic laws that you'd expect given their names, even if you only consider *well* ordered sets.

It *is* true that they're associative. They also have identities: $\varnothing + W \cong W \cong W + \varnothing$ and $\mathbf{1} \times W \cong W \cong W \times \mathbf{1}$ for all $W$.

However, neither $+$ nor $\times$ is commutative. (It's rare in mathematics that something called addition is noncommutative, but here we are.) For instance, if you look at Examples 8.1.10, you should be able to see that $\mathbf{1} + \omega \cong \omega \ncong \omega + \mathbf{1}$ and $\mathbf{2} \times \omega \cong \omega \ncong \omega \times \mathbf{2}$. And distributivity works on one side only: $V \times (W + X) \cong (V \times W) + (V \times X)$, but in general $(V + W) \times X \ncong (V \times X) + (W \times X)$. So assume nothing!

Using these constructions, we can manufacture many more well ordered sets (Figure 8.1).

**Examples 8.1.10** i. The well ordered set $\omega + \mathbf{1}$ consists of the natural numbers $0, 1, \ldots$ together with one new element $0'$ greater than all the natural numbers (Figure 8.1). Note that the *sets* $\omega + \mathbf{1}$ and $\omega$ are isomorphic, by Lemma 7.1.3. But the *ordered sets* $\omega + \mathbf{1}$ and $\omega$ are not, since one has a greatest element and the other does not.

ii. Similarly, $\omega + \mathbf{3}$ (where of course $3 \in \mathbb{N}$ is defined to be $s(2)$) has elements

$$0, 1, 2, \ldots, 0', 1', 2'$$

in that order. (As ever, it doesn't matter what names we give elements; $0'$, $1'$ and $2'$ are just the names I'm calling the elements of the second copy of $\mathbb{N}$. See also Warning 6.3.9.)

iii. The well ordered set $\omega + \omega$ consists of elements

$$0, 1, 2, \ldots, 0', 1', 2', \ldots,$$

in that order. In fact, $\omega + \omega \cong \omega \times \mathbf{2}$, as you can check.

iv. Similarly, the well ordered set $\omega + \omega + \mathbf{3} \cong (\omega \times \mathbf{2}) + \mathbf{3}$ consists of elements

$$0, 1, 2, \ldots, 0', 1', 2', \ldots, 0'', 1'', 2'',$$

in that order.

v. A final example: $\omega \times \omega$ consists of elements

$$\begin{gathered}(0,0), (1,0), (2,0), \ldots, \\ (0,1), (1,1), (2,1), \ldots, \\ (0,2), (1,2), (2,2), \ldots, \\ \ldots,\end{gathered}$$

in that order (with infinitely many rows).

**Exercise 8.1.11** In Warning 8.1.9, I gave counterexamples to addition and multiplication of well ordered sets being commutative. Check them.

A well ordered set can be thought of as a set in which there is a notion of 'next'. Imagine you've used up some but not all elements of your set. Then having a well order means you always know which element to use next. It's the least element of the set of elements you haven't used so far.

However, there's no notion of 'previous'. For instance, in $\omega + \mathbf{1}$, there's no element that could be said to come immediately before the greatest element.

**Remark 8.1.12** All of the well ordered sets in Examples 8.1.10 are isomorphic *as sets*. (They're all countably infinite, a concept we'll study in Chapter 10.) However, no two of them are isomorphic *as ordered sets*, as we'll see in Section 8.2. Moral: the same set can support multiple non-isomorphic order structures. This is like the fact that there can be multiple non-isomorphic groups of the same order.

Finite sets could lead you astray here. There's only *one* well ordered set of each finite cardinality. Put another way, if a well ordered set is isomorphic *as a set* to $\mathbf{n}$ for some $n \in \mathbb{N}$, then in fact it's *order isomorphic* to $\mathbf{n}$. Again, there's a question on this in the next workshop.

A well ordered set is called a **successor** if it is isomorphic to $V + \mathbf{1}$ for some well ordered set $V$, and a **limit** otherwise.

**Lemma 8.1.13** *A well ordered set is a successor if and only if it is has a greatest element.*

**Proof** Any successor certainly has a greatest element. Conversely, suppose that $W$ has a greatest element, $\mathsf{T}$. Define $V = W \setminus \{\mathsf{T}\}$ with the induced order, which is a well order (Example 8.1.5(ii)). You can check that $W \cong V + \mathbf{1}$. □

**Exercise 8.1.14** Which of the well ordered sets in Figure 8.1 are successors, and which are limits?

**Definition 8.1.15** A subset $A$ of an ordered set $X$ is **downwards closed**, or a **downset**, if for all $x, y \in X$,

$$(x \leq y \text{ and } y \in A) \implies x \in A.$$

(We met this terminology in the case $X = \mathbb{Q}$ in Lemma 7.5.8.)

**Examples 8.1.16**

i. Recall from Definition 7.2.2 that $\downarrow x$ means $\{y \in X : y < x\}$, for an element $x$ of an ordered set $X$. Such a subset $\downarrow x$ is always a downset. For example, in $\omega$, the subset $\downarrow 4 = \{0, 1, 2, 3\}$ is a downset (but $\{1, 2, 3\}$ is not).

ii. Trivially, $X$ is downwards closed in $X$, for any ordered set $X$.

In a well ordered set, all the downsets are of one of the two types just mentioned:

**Lemma 8.1.17** *Let $W$ be a well ordered set and let $A$ be a downset in $W$. Then $A = W$ or there exists a unique $w \in W$ such that $A = \downarrow w$.*

The two cases are mutually exclusive: $\downarrow w \neq W$, since $w \notin \downarrow w$.

**Proof** Let $A$ be a downset in $W$, and assume that $A \neq W$. Then $W \setminus A$ is a nonempty subset of $W$, and therefore has a least element $w$. We will show that $A = {\downarrow}w$.

In one direction, let $a \in A$. If $w \leq a$ then, since $A$ is downwards closed, $w \in A$, a contradiction since $w \in W \setminus A$. Since $W$ is totally ordered, it follows that $a < w$, that is, $a \in {\downarrow}w$.

In the other, let $x \in {\downarrow}w$. Since $w$ is the *least* element of $W$ not in $A$, we must have $x \in A$.

Hence $A = {\downarrow}w$, as claimed. It only remains to prove uniqueness: that if also $A = {\downarrow}v$ then $v = w$. Indeed, if ${\downarrow}v = {\downarrow}w$ with $v \neq w$ then since $W$ is totally ordered, we can assume without loss of generality that $v < w$. But then $v \in {\downarrow}w = {\downarrow}v$, giving $v < v$, a contradiction. □

There is an induction principle for an arbitrary well ordered set that generalizes the strong induction principle for the natural numbers (Theorem 7.2.4). Although it's trivial to prove, I'll call it a theorem since it's important.

**Theorem 8.1.18 (Transfinite induction)** *Let $W$ be a well ordered set. Let $A$ be a subset of $W$ such that for all $w \in W$,*

$$ {\downarrow}w \subseteq A \implies w \in A. $$

*Then $A = W$.*

Theorem 7.2.4 is the case $W = \omega$.

**Proof** Suppose for a contradiction that $A \neq W$. Then $W \setminus A$ is a nonempty subset of $W$ and therefore has a least element $w$. It follows that every element of $W$ less than $w$ is in $A$, that is, ${\downarrow}w \subseteq A$. So by hypothesis, $w \in A$, a contradiction. □

The collection of well ordered sets, taken up to isomorphism, is often seen as an extension of the natural numbers. You count like this:

$$ 0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, $$

(dropping the customary bold face), and then

$$ \omega + \omega = \omega \cdot 2, \omega \cdot 2 + 1, \omega \cdot 2 + 2, \ldots, \omega \cdot 3, \omega \cdot 3 + 1, \omega \cdot 3 + 2, \ldots, $$

(writing $\cdot$ instead of $\times$), and then

$$ \omega \cdot \omega, \omega \cdot \omega + 1, \omega \cdot \omega + 2, \ldots, \omega \cdot \omega + \omega = \omega \cdot (\omega + 1), \ldots, $$

'and so on' (whatever that means). The theory we develop in the next section should clarify the picture.

When well ordered sets are thought of as a counting system like this, the word **ordinal** is often used. It can be taken to mean either an isomorphism class of well ordered sets or simply a well ordered set, with the understanding that they're always considered up to isomorphism. So, $0, 1, 2, \ldots, \omega, \omega + 1, \ldots$ (or their isomorphism classes if you prefer) are all ordinals.

## 8.2 Comparing well ordered sets

The examples in Figure 8.1 suggest that the well ordered sets can themselves be put in order. For example, $\mathbf{1}$ is isomorphic to a downset of $\mathbf{3}$, which in turn is isomorphic to a downset of $\omega$, which is isomorphic to a downset of $\omega + \mathbf{1}$, and so on. Here, we develop this idea.

**Definition 8.2.1** Let $V$ and $W$ be well ordered sets. A **map of well ordered sets** (or just a **map**) from $V$ to $W$ is an order-preserving injection whose image is downwards closed.

Note that an order-preserving injection $f : V \to W$ is *strictly* order-preserving: if $v < v'$ then $f(v) < f(v')$. This follows directly from the definitions.

**Examples 8.2.2**

i. Let $n$ be a natural number. The inclusion $i : \mathbf{n} \to \omega$ (that is, $\{0, \ldots, n-1\} \hookrightarrow \mathbb{N}$) is a map of well ordered sets.

ii. In Figure 8.1, the inclusion of each well ordered set into the one in the next row is a map of well ordered sets.

**Exercise 8.2.3** Prove that for maps of well ordered sets $f : V \to W$ and $g : W \to X$, the composite $g \circ f : V \to X$ is also a map.

Can there be two different maps from one well ordered set to another? No!

**Lemma 8.2.4** *Let $f, g : V \to W$ be maps of well ordered sets. Then $f = g$.*

**Proof** We prove by transfinite induction (Theorem 8.1.18) on $v \in V$ that $f(v) = g(v)$. So, let $v \in V$ and assume that $f(v') = g(v')$ for all $v' < v$. We must prove that $f(v) = g(v)$.

Without loss of generality, $f(v) \leq g(v)$. Since $\operatorname{im} g$ is downwards closed, $f(v) = g(u)$ for some $u \in V$.

If $u > v$ then since $g$ is an order-preserving injection, $g(v) < g(u)$, giving $f(v) \leq g(v) < g(u) = f(v)$, a contradiction.

If $u < v$ then $f(u) = g(u)$ by inductive hypothesis. But $f(v) = g(u)$ too, so $f(u) = f(v)$, which since $f$ is injective implies $u = v$—again, a contradiction.

Hence $u = v$. But $f(v) = g(u)$, so $f(v) = g(v)$, completing the induction. □

**Definition 8.2.5** For well ordered sets $V$ and $W$, we write $V \preceq W$ if there exists a map of well ordered sets $V \to W$.

**Example 8.2.6** Denoting the well ordered sets of Figure 8.1 by $W_1, W_2, \ldots, W_9$, we have $W_1 \preceq W_2 \preceq \cdots \preceq W_9$ by Examples 8.2.2(ii).

Now we show that $\preceq$ is the relation described in the first paragraph of this section. We also characterize the relation $\prec$, defined by

$$V \prec W \iff (V \preceq W \text{ and } V \not\cong W).$$

You can guess how $\succeq$ and $\succ$ are defined.

**Lemma 8.2.7** *Let $V$ and $W$ be well ordered sets. Then $V \preceq W$ if and only if $V$ is isomorphic to a downset of $W$. Moreover, $V \prec W$ if and only if $V$ is isomorphic to a proper downset of $W$.*

In this statement, we take a couple of things for granted: that 'isomorphic' means 'order isomorphic' (because we're talking about ordered sets), and that when subsets of $W$ are treated as ordered sets, it's with the induced order (because what else would it be?). Also, I've somehow got this far without saying that a **proper** subset of a set $X$ is one not equal to $X$.

**Proof** Suppose that $V \preceq W$. Write $f$ for the unique map $V \to W$. Then $f$ corestricts to a function $f' \colon V \to \operatorname{im} f$ (Lemma 5.5.8), which satisfies $f'(v) = f(v)$ for all $v \in V$. Since $f$ is injective and order-preserving, so is $f'$. Also, $f'$ is surjective by definition. So $f'$ is an order-preserving bijection from $V$ to the downset $\operatorname{im} f$ of $W$, and then by Exercise 8.1.2, $f'$ is an order isomorphism. For 'moreover', if $V \prec W$ then $V \not\cong W$, so $V$ can only be isomorphic to a proper downset of $W$.

Conversely, suppose there is an order isomorphism $f'$ from $V$ to a downset $B$ of $W$. Let $f$ be the composite $V \xrightarrow{f'} B \hookrightarrow W$. Then $f$ is injective and order-preserving since both $f'$ and the inclusion are. Moreover, its image is $B$, which is downwards closed in $W$. Hence $f \colon V \to W$ is a map of well ordered sets, giving $V \preceq W$. For 'moreover', if $B$ is a proper subset of $W$ then the map $f \colon V \to W$ is not an isomorphism, which by Lemma 8.2.4 implies that there is *no* isomorphism $V \to W$. Hence $V \not\cong W$, giving $V \prec W$. □

**Corollary 8.2.8** *Let $V$ and $W$ be well ordered sets. If $V$ is isomorphic to a proper downset of $W$ then $V \not\cong W$.* □

**Examples 8.2.9** i. As in Example 8.2.6, write the well ordered sets of Figure 8.1 as $W_1, \ldots, W_9$. Then by Lemma 8.2.7, $W_1 \prec \cdots \prec W_9$. In particular, no two of these nine well ordered sets are isomorphic.

ii. $W \prec W + \mathbf{1}$ for every well ordered set $W$, since the inclusion $W \hookrightarrow W + \mathbf{1}$ makes $W$ isomorphic to a proper downset of $W + \mathbf{1}$.

**Warning 8.2.10** It's easy to confuse the various notions of inequality in play.

- We're considering individual ordered sets, whose order relation we usually denote by $\leq$. So, for $w, w' \in W$, it may or may not be that $w \leq w'$.
- We're also considering a relationship *between* well ordered sets, denoted by $\preceq$. So, for well ordered sets $V$ and $W$, it may or may not be that $V \preceq W$.
- There's also the notion of inequality between *sets* (not ordered), as in Definition 6.4.1. So, for sets $X$ and $Y$, it may or may not be that $X \leq Y$ (meaning that there exists an injection $X \to Y$).

For well ordered sets $V$ and $W$, if $V \preceq W$ (inequality between well ordered sets) then $V \leq W$ (inequality between sets), since maps of well ordered sets are by definition injective. But the converse is false. For example, $\omega + \mathbf{1} \leq \omega$ *as sets*; in fact, they're isomorphic, by Lemma 7.1.3. However, $\omega + \mathbf{1} \not\preceq \omega$, by Example 8.2.9(ii).

It would be misleading to use the symbol $\preceq$ if it didn't have the following properties.

**Lemma 8.2.11** *Let $V$, $W$ and $X$ be well ordered sets. Then:*

*i.* $V \cong W \implies V \preceq W$;

*ii.* $(V \preceq W$ *and* $W \preceq X) \implies V \preceq X$;

*iii.* $(V \preceq W$ *and* $W \preceq V) \implies V \cong W$.

**Proof** Part (i) is immediate from the definition, and (ii) follows from Exercise 8.2.3. For (iii), take maps $f\colon V \to W$ and $g\colon W \to V$. Then $gf$ is a map $V \to V$ (by that same exercise), so $gf = \mathrm{id}_V$ by Lemma 8.2.4. Similarly, $fg = \mathrm{id}_W$. Hence $f$ is an isomorphism and $V \cong W$. □

We now build up to showing that *roughly speaking*, $\preceq$ is a well order on well ordered sets!

This doesn't entirely make sense, for a couple of reasons. First, one usually only speaks of orders on a *set*, and there are too many well ordered sets to form

a set (a theme we'll revisit in the next section). Second, we've just seen that $V \preceq W \preceq V \iff V \cong W$, so $\preceq$ only satisfies an up-to-isomorphism kind of antisymmetry—which is as it should be, since we never care about *equality* of sets (or ordered sets).

These quibbles aside, what we'll show is that every nonempty family of well ordered sets has a least element with respect to $\preceq$. The first and hardest step is to prove this for two-member families:

**Lemma 8.2.12** *For well ordered sets $V$ and $W$, either $V \preceq W$ or $W \preceq V$.*

**Proof** For the purposes of this proof, say that a downset $A$ of $V$ is *good* if $A \preceq W$. Let $V'$ be the union of the good downsets in $V$. Like any union of downsets, $V'$ is a downset. We show that $V'$ is good.

For each good downset $A$ of $V$, there is a unique map $f_A \colon A \to W$ (by Lemma 8.2.4). When $A$ and $A'$ are both good downsets, the composites

$$A \cap A' \hookrightarrow A \xrightarrow{f_A} W, \qquad A \cap A' \hookrightarrow A' \xrightarrow{f_{A'}} W$$

must be equal, by Lemma 8.2.4 again; that is, $f_A|_{A \cap A'} = f_{A'}|_{A \cap A'}$. We now want to 'define' $f \colon V' \to W$ by $f(v) = f_A(v)$ whenever $A$ is good and $v \in A$. To show that a function with this property exists, put

$$R = \bigcup_{\text{good } A} \{(v, w) \in V' \times W : v \in A \text{ and } f_A(v) = w\} \subseteq V' \times W.$$

The observations above imply that the relation $R$ is functional, so it is the graph of a function $f \colon V' \to W$ such that $f(v) = f_A(v)$ whenever $A$ is good and $v \in A$.

To finish the proof that $V'$ is good, it is enough to show that $f$ is a map of well ordered sets. To see that $f$ is injective and order-preserving, take $v_1 < v_2$ in $V'$. There is some good downset $A$ containing $v_2$, which then also contains $v_1$. Since $f_A$ is injective and order-preserving, $f_A(v_1) < f_A(v_2)$. But $f|_A = f_A$, so $f(v_1) < f(v_2)$. Finally, $\operatorname{im} f = \bigcup_{\text{good } A} \operatorname{im} f_A$, which is a union of downsets and therefore a downset. So $f \colon V' \to W$ is a map of well ordered sets.

We have now proved that the downset $V'$ of $V$ satisfies $V' \preceq W$. If $V' = V$ then $V \preceq W$. If $f \colon V' \to W$ is surjective then $V' \cong W$, so $W$ is isomorphic to a downset of $V$, giving $W \preceq V$ by Lemma 8.2.7. If neither are true then we can choose the least element $v \in V \setminus V'$ and the least element $w \in W \setminus \operatorname{im} f$. Then $V' \cup \{v\}$ is a downset of $V$. The union $V' \cup \{v\}$ is disjoint, that is, a coproduct, so we can define $g \colon V' \cup \{v\} \to W$ by

$$g(u) = \begin{cases} f(u) & \text{if } u \in V', \\ w & \text{if } u = v. \end{cases}$$

One easily checks that $g$ is a map of well ordered sets. Hence $V' \cup \{v\}$ is a good downset of $V$. But $V'$ is the union of the good downsets of $V$, so $v \in V'$, contradicting the definition of $v$. So $V \preceq W$ or $W \preceq V$. □

Now we can show that the well ordered sets are well ordered.

**Theorem 8.2.13** *Let $I$ be a nonempty set and $(W_i)_{i \in I}$ a family of well ordered sets. Then there is some $i \in I$ such that for all $j \in I$, we have $W_i \preceq W_j$.*

**Proof** Since $I$ is nonempty, we can choose $k \in I$. Let $J = \{j \in I : W_j \prec W_k\}$. If $J$ is empty then by Lemma 8.2.12, we can take $i = k$. Assume otherwise.

For each $j \in J$, by Lemma 8.2.7, $W_j$ is isomorphic to a proper downset of $W_k$, which by Lemma 8.1.17 is $\downarrow w_j$ for a unique $w_j \in W_k$. Since the subset $\{w_j : j \in J\}$ of $W_k$ is nonempty, it has a least element, say $w_i$. For each $j \in J$, then, $w_i \leq w_j$, and the inclusion $\downarrow w_i \hookrightarrow \downarrow w_j$ is a map of well ordered sets. But $W_i \cong \downarrow w_i$ and $W_j \cong \downarrow w_j$, so $W_i \preceq W_j$.

We have now found an element $i \in J$ such that for all $j \in J$, we have $W_i \preceq W_j$. On the other hand, for $\ell \in I \setminus J$, we have $W_\ell \succeq W_k$ (by Lemma 8.2.12), so $W_i \prec W_k \preceq W_\ell$, giving $W_i \preceq W_\ell$. Hence for all $j \in I$, whether or not $j \in J$, we have $W_i \preceq W_j$. □

**Digression 8.2.14** There is a little gap in rigour here. I defined 'family of sets' (Section 6.5), but not 'family of well ordered sets'. Giving the formal definition requires a bit more work than you might imagine, and we're skipping it.

**Digression 8.2.15** In Section 9.3, we'll use Theorem 8.2.13 to prove that any nonempty family of *ordinary* sets has a member that's least with respect to $\leq$, that is, injects into all the others. The proof uses both Theorem 8.2.13 and the axiom of choice.

The fact that every nonempty family of sets has a least member is why well orders are inevitable in set theory.

The final result of this section starts from an observation. Take a subset $A$ of $\omega$; say, $\{8, 12, 14\}$ or the set of prime numbers. Giving $A$ the induced order makes it into a well ordered set. The inclusion $A \hookrightarrow \omega$ is *not* a map of well ordered sets, since the image is not necessarily downwards closed. Nevertheless, these examples (where $A$ is isomorphic to $\mathbf{3}$ or $\omega$) suggest that $A \preceq \omega$ anyway. In fact, this is always true, by the following result.

**Proposition 8.2.16** *Let $W$ be a well ordered set. Let $A$ be a subset of $W$ with the induced order. Then $A \preceq W$.*

Recall from Example 8.1.5(ii) that the induced order on $A$ is a *well* order.

**Proof** Suppose for a contradiction that $A \not\preceq W$. By Lemma 8.2.12, $W \prec A$. The unique map of ordered sets $f\colon W \to A$ then satisfies $\operatorname{im} f = \{a \in A : a < b\}$ for some $b \in A$, by Lemma 8.1.17. Clearly $f(b) \in \operatorname{im} f$, so $f(b) < b$. Hence the set $S = \{w \in W : f(w) < w\}$ is nonempty, and therefore has a least element $x$. Now $f(x) < x$, and $f$ is an order-preserving injection, so $f(f(x)) < f(x)$. This means that $f(x) \in S$ with $f(x) < x$, contradicting the minimality of $x$. □

Another way to state this result is that for well ordered sets $V$ and $W$, if there are any order-preserving injections $V \to W$ at all, then there is one whose image is downwards closed.

## 8.3 The Hartogs theorem

The examples of well ordered sets that we've seen so far are not very big. For a start, they're all countable, which means that *as sets* (ignoring the order), you can embed each of them into $\mathbb{N}$. (We'll define countability in Chapter 10 and prove results about it there.) But the Hartogs theorem says that there are arbitrarily large well ordered sets. More exactly, it says that no matter what set $X$ you pick, there's some well ordered set that *doesn't* embed (as a set) into $X$.

To understand what this means, it's important to get straight the difference between $\preceq$ for well ordered sets and $\leq$ for ordinary sets. See Warning 8.2.10. The Hartogs theorem doesn't involve $\preceq$, just $\leq$.

**Theorem 8.3.1 (Hartogs)** *For every set $X$, there exists a well ordered set $(H, \leq)$ such that $H \not\leq X$.*

Recall that $H \not\leq X$ means there is no injection $H \to X$.

**Warning 8.3.2** Once we deploy the axiom of choice in the next chapter, we'll be able to prove 'cardinal comparability': for any two sets $X$ and $Y$, either $X \leq Y$ or $Y \leq X$. So in the Hartogs theorem, we'll be able to conclude that $H > X$. But without choice, $H \not\leq X$ is the best we can do.

Here is the rough idea of the proof. We're given a set $X$, and we want to cook up a well ordered set that's 'large' relative to it. If we just wanted a *set* that was larger than $X$, we could take the set $\mathscr{P}(X)$ of subsets of $X$ (Theorem 6.4.4). Because we're after a *well ordered* set, we're going to take the set of subsets of $X$ equipped with well orders, with the idea in mind that the collection of all well ordered sets is itself well ordered by $\preceq$ (loosely speaking: Theorem 8.2.13). And to make everything work properly, we quotient out by isomorphism.

**Proof of Theorem 8.3.1** Let $X$ be a set. The plan is to take $H$ to be the set of isomorphism classes of well ordered sets $(W, \leq)$ such that $W \leq X$, with $\preceq$ as the order on $H$, and then prove that $H \not\leq X$.

To define $H$ rigorously, we proceed as follows. First let $G$ be the set of pairs $(W, \leq) \in \mathscr{P}(X) \times \mathscr{P}(X \times X)$ such that $\leq \subseteq_{X \times X} W \times W$ and the subset $\leq \hookrightarrow W \times W$ is a well order on $W$. Thus, an element $(W, \leq)$ of $G$ amounts to a subset $W \subseteq X$ together with a well order $\leq$ on $W$.

Next, define an equivalence relation $\sim$ on $G$ by $(W, \leq) \sim (W', \leq')$ if and only if the well ordered sets $(W, \leq)$ and $(W', \leq')$ are isomorphic. Put $H = G/\sim$ and write $[(W, \leq)]$ for the equivalence class of $(W, \leq)$. Thus, an element of $H$ is an isomorphism class of well ordered sets $(W, \leq)$ such that $W \leq X$.

(Example: let $X = \{0, 1\}$. Then $G$ has five elements: the empty well ordered set, $\{0\}$ with its unique well order, $\{1\}$ with its unique well order, and $\{0, 1\}$ with its two well orders. *Finite* well ordered sets with the same number of elements are isomorphic, so $H$ has three elements: the isomorphism class of empty well ordered sets, the isomorphism class of one-element well ordered sets, and the isomorphism class of two-element well ordered sets. Note that $H$ has one more element than $X$, so there can be no injection $H \to X$.)

There is a relation $\trianglelefteq$ on $H$ defined by $[(W, \leq)] \trianglelefteq [(W', \leq')]$ if and only if $(W, \leq) \preceq (W', \leq')$. (You can check that this is well defined.) By Theorem 8.2.13, $\trianglelefteq$ is a well order on $H$.

Claim: $(W, \leq) \prec (H, \trianglelefteq)$ for all well ordered sets $(W, \leq)$ such that $W \leq X$.

Proof: define $f \colon W \to H$ by $f(w) = [{\downarrow}w]$ for all $w \in W$. Here ${\downarrow}w$ is given the induced order from $W$. Then $f$ is injective and order-preserving: for if $w' < w$ then ${\downarrow}w'$ is a proper downset of ${\downarrow}w$, which by Lemma 8.2.7 implies that ${\downarrow}w' \prec {\downarrow}w$, that is, $f(w') \triangleleft f(w)$. The image of $f$ is downwards closed, since every downset of ${\downarrow}w$ is equal to ${\downarrow}w'$ for some $w' \leq w$ (by Lemma 8.1.17). Hence $f$ is a map of well ordered sets.

However, $f$ is not surjective, since $[W] \notin \operatorname{im} f$. Indeed, for each $w \in W$ we have ${\downarrow}w \not\cong W$ (by Corollary 8.2.8), and so $f(w) = [{\downarrow}w] \neq [W]$.

Hence there is a non-surjective map of well ordered sets $(W, \leq) \to (H, \trianglelefteq)$, and the claim follows.

To prove the theorem itself, suppose that $H \leq X$. Then $(H, \trianglelefteq)$ is a well ordered set such that $H \leq X$, so by the claim, $(H, \trianglelefteq) \prec (H, \trianglelefteq)$, a contradiction. □

## 8.4 Chains and their upper bounds

Here we use the theory of *well* ordered sets to prove a result about *arbitrary* ordered sets. It is very closely related to the important Zorn's lemma, which we will meet

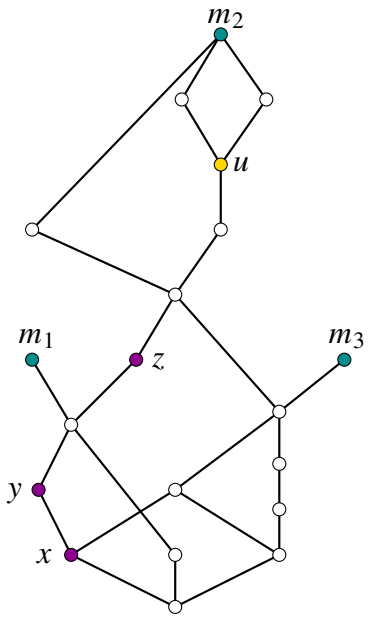



Figure 8.2: A finite ordered set $X$, showing a chain $\{x, y, z\}$, an upper bound $u$ of that chain, and the three maximal elements $m_1, m_2, m_3$ of $X$, none of which is a greatest element of $X$. (Maximal elements will be introduced in Chapter 9.)

in the next chapter and which needs the axiom of choice. But the theorem we will prove here does not need the axiom of choice.

**Definition 8.4.1** Let $(X, \leq)$ be an ordered set. A **chain** in $X$ is a subset $C \subseteq X$ such that for all $x, y \in C$, either $x \leq y$ or $y \leq x$.

Equivalently, a subset $C$ of $X$ is a chain if it is totally ordered with respect to the induced ordering. It would be reasonable to call $C$ a 'totally ordered subset', but 'chain' is traditional. Figure 8.2 shows a random finite ordered set and a chain in it.

**Examples 8.4.2** i. If $(X, \leq)$ is totally ordered then every subset is a chain.

ii. Let $X$ be the power set $\mathscr{P}(\{0, 1, 2, 3\})$, ordered by inclusion. Then $\{\{2\}, \{0, 2\}\}$ is a chain in $X$, but $\{\{1\}, \{0, 2\}\}$ is not.

iii. Take $\mathbb{N}$ with the divisibility ordering: $x \leq y$ if and only if $x$ divides $y$. Then $\{6^n : n \in \mathbb{N}\}$ is a chain.

Recall that we can speak of the 'upper bounds' of a subset $A$ of an ordered set $X$ (Definition 7.5.1). And recall from Warning 7.5.2 that an upper bound of a

subset $A$ of $X$ does not have to belong to $A$. For example, in Figure 8.2, $u$ is an upper bound of the chain $\{x, y, z\}$ but does not belong to $\{x, y, z\}$.

Many of the ordered sets that arise in mathematics have the special property that every chain has an upper bound. We'll see some examples in Chapter 9. This means that the following result is quite widely applicable.

**Proposition 8.4.3** *Let $X = (X, \leq)$ be an ordered set, and let*

$$\varphi\colon \{\textit{chains in } X\} \to X$$

*be a function assigning to each chain $C$ an upper bound $\varphi(C)$ in $X$. Then $\varphi(C) \in C$ for some chain $C$.*

It might seem intuitively clear that Proposition 8.4.3 holds in the finite case. Maybe you can stare at Figure 8.2 and see why the proposition holds there. But the general case is harder. Here's the idea of the proof.

We start with the empty subset of $X$. This is a chain, so we can apply $\varphi$ to it, giving an element $x_0 = \varphi(\varnothing) \in X$.

Now $\{x_0\}$ is also a chain in $X$, so we can apply $\varphi$ to it, giving an new element $x_1 = \varphi(\{x_0\}) \in X$. Since $\varphi(\{x_0\})$ is an upper bound of $\{x_0\}$, we have $x_0 \leq x_1$.

So $\{x_0, x_1\}$ is a chain in $X$. This means we can apply $\varphi$ to it, giving a new element $x_2 = \varphi(\{x_0, x_1\})$, and then $x_0 \leq x_1 \leq x_2$.

If we can keep going until the chain grows so long that there is no room for it to grow any further, then the 'new element' constructed at the next stage must already be in the chain we've grown so far, proving the result. We do this by iterating not just through the natural numbers, but beyond, through a large well ordered set. By 'large' I mean one provided by the Hartogs theorem: larger than $X$.

**Proof of Proposition 8.4.3** The proof is quite similar to that of Lemma 8.2.12.

By the Hartogs theorem, there is a well ordered set $(W, \leq)$ such that $W \not\leq X$. For the purposes of this proof, say that a downset $A$ of $W$ is *good* if there exists an order-preserving function $g\colon A \to X$ such that

$$g(w) = \varphi(g(\downarrow w)) \tag{8.1}$$

for all $w \in A$. Here $\downarrow w$ is a *subset* of $A$, so $g(\downarrow w)$ means the image of $\downarrow w \subseteq A$ under $g\colon A \to X$. (It's not an *element* of $A$ at which we're evaluating $g$.) Moreover, since $g$ is order-preserving and $\downarrow w$ is totally ordered, it follows that $g(\downarrow w)$ is a chain; hence the right-hand side of (8.1) is defined.

For good downsets $A$, there is only one function $g\colon A \to X$ with the properties above. Indeed, if $g$ and $g'$ both have the property then we can prove by transfinite induction (Theorem 8.1.18) that $g(w) = g'(w)$ for all $w \in A$. Write $g_A\colon A \to X$ for the unique function with the properties above.

Now arguing just as in the proof of Lemma 8.2.12, let $W'$ be the union of the good downsets in $W$ (which is a downset), and put

$$R = \bigcup_{\text{good } A} \{(w, x) \in W' \times X : w \in A \text{ and } g_A(w) = x\} \subseteq W' \times X.$$

As in Lemma 8.2.12, the relation $R$ is functional, so it is the graph of a function $g : W' \to X$ such that $g(w) = g_A(w)$ whenever $A$ is good and $w \in A$. Each of the functions $g_A$ is order-preserving and satisfies (8.1) for every $w \in A$, and it follows that $g$ is order-preserving and satisfies (8.1) for every $w \in W'$. Thus, $W'$ is good.

We now show that $W' = W$. Suppose not. Then $W \setminus W'$ has a least element $v$, and then $W' \cup \{v\}$ is a downset of $W$. Since $W'$ is totally ordered and $g_{W'} : W' \to X$ is order-preserving, $\operatorname{im} g_{W'}$ is a chain, so $\varphi(\operatorname{im} g_{W'})$ is defined. The union $W' \cup \{v\}$ is disjoint, that is, a coproduct, so we can define $g : W' \cup \{v\} \to X$ by

$$g(u) = \begin{cases} g_{W'}(u) & \text{if } u \in W', \\ \varphi(\operatorname{im} g_{W'}) & \text{if } u = v. \end{cases}$$

Then $g$ is order-preserving, because $g_{W'}$ is and $\varphi(\operatorname{im} g_{W'})$ is an upper bound of $\operatorname{im} g_{W'}$. It also satisfies (8.1) for all $w \in W' \cup \{v\}$, since $g_{W'}$ satisfies it for all $w \in W'$. Hence $W' \cup \{v\}$ is a good downset. But $W'$ is the union of all good downsets in $W$, so $v \in W'$, contradicting the definition of $v$. So $W' = W$, as claimed.

We have now shown that $W'$ is good and $W' = W$. Hence $W$ is good. That is, there is an order-preserving function $g : W \to X$ satisfying (8.1) for all $w \in W$. By definition of $W$ at the start of the proof, $g$ is not injective. Hence $g(v) = g(w)$ for some distinct $v, w \in W$, say with $v < w$. Then $v \in {\downarrow} w$, so

$$\varphi(g({\downarrow} w)) = g(w) = g(v) \in g({\downarrow} w).$$

Taking $C$ to be the chain $g({\downarrow} w)$ in $X$, we then have $\varphi(C) \in C$, as required. □

**Exercise 8.4.4** Do the proof by transfinite induction mentioned in the third paragraph of the proof.

The proofs of both Lemma 8.2.12 and Proposition 8.4.3 are disguised versions of transfinite recursion, which we're not covering explicitly. At least, we're not covering it for exam, but you can read about it in the next section if you're interested.

## 8.5 Transfinite recursion (optional)

*This section is non-examinable.*

Instead of giving you another theorem, I'm going to talk you through a single example of transfinite recursion. In fact, this example is where set theory began.

Georg Cantor (1845–1918) is widely viewed as the founder of set theory. What led him to it was questions about the convergence of Fourier series. Fourier series can fail to converge at certain points of $\mathbb{R}$, and the set of points where convergence fails can have intricate structure. Studying them led Cantor down the path I'll describe now.

Let $X$ be a subset of $\mathbb{R}$. A point $x$ of $X$ is **isolated** if for some $\delta > 0$, the interval $(x - \delta, x + \delta)$ contains no other point of $X$.

*Question:* can we remove all isolated points from $X$ to obtain a subset with no isolated points?

At first glance, the answer might seem obvious. Surely we can do it by just defining $X' \subseteq X$ to be the set of non-isolated points of $X$. Then $X'$ contains no isolated points, right?

Wrong! For example, consider

$$X = \{0\} \cup \{2^{-n} : n \geq 1\}.$$

Then the isolated points in $X$ are $1/2, 1/4, \ldots$, but not 0, so $X' = \{0\}$. And $X'$ *does* have an isolated point, namely, 0. The point is that although 0 wasn't isolated in $X$, it is isolated in $X'$. The meaning of 'isolated' depends on the ambient set.

Since removing the isolated points once didn't work, what about doing it twice? Let $X''$ be the set of non-isolated points of $X'$. Is $X''$ a set with no isolated points? In the example just given, yes, because $X'' = \varnothing$. But in general, no.

For instance, let $Y$ be the subset of $[0, 1)$ consisting of the numbers with a binary expansion containing at most two copies of 1. Thus, $Y$ consists of 0, numbers like 0.00001, and numbers like 0.0010000001. Then $Y'$ is the set $X$ of the previous example, so $Y''$ is $\{0\}$, which still has an isolated point.

The set $X' = X \setminus \{\text{isolated points of } X\}$ is called the **Cantor–Bendixson derivative** or **derived set** of $X$. We use the familiar notation $X^{(n)}$ for higher derivatives, putting $X^{(0)} = X$ and $X^{(n+1)} = (X^{(n)})'$ for all $n \in \mathbb{N}$.

We've seen so far that both the first and second Cantor–Bendixson derivatives of a subset of $\mathbb{R}$ can have isolated points. So it probably won't surprise you that however many derivatives you take, you still might not have succeeded in removing all the isolated points.

The set I called $Y$ suggests an example to prove this. Let $B_n$ be the set of all real numbers in $[0, 1)$ with a binary expansion containing at most $n$ copies of 1. (So $Y = B_2$.) Then $B_n' = B_{n-1}$, and it follows that $B_n^{(n)} = \{0\}$. In particular, the $n$th derivative of $B_n$ has an isolated point.

So, taking derivatives $n$ times isn't enough to eliminate the isolated points of all subsets of $\mathbb{R}$, no matter how large $n$ is. What about taking derivatives *infinitely*

many times? Let $X^{(\omega)}$ be the intersection of the subsets

$$X \supseteq X' \supseteq \cdots \supseteq X^{(n)} \supseteq \cdots$$

of $\mathbb{R}$ (or more formally, $X^{(\omega)} = \bigcap_{n\in\mathbb{N}} X^{(n)}$). Surely we've removed all the isolated points *now*?

In the case of our examples $B_n$, yes. But there are more devious examples showing that in general, no: $X^{(\omega)}$ can still have isolated points. This pushes us to go one step further, defining

$$X^{(\omega+1)} = (X^{(\omega)})'.$$

And so on! You can see that there's a pattern emerging.

(With the notation introduced in earlier sections, I should really write $\omega + \mathbf{1}$ rather than $\omega + 1$, but I will drop the bold face.)

In general, we can define the higher Cantor–Bendixson derivative $X^{(W)}$ of $X$ for any well ordered set $W$, as follows. There are three cases.

- The empty set: $X^{(0)} = X$.
- Successors: if $W \cong V + 1$ for some well ordered set $V$, then $X^{(W)} = (X^{(V)})'$.
- Limits: if $W$ is not empty or a successor then $X^{(W)} = \bigcap_{V\prec W} X^{(V)}$.

This is a definition of $X^{(W)}$ by transfinite recursion. Showing that it is a valid method of definition requires some work, which we will not do. But I hope this example gives the idea.

Let's go back to the question: if we take a high enough derivative of $X$, do we eventually end up with a set with no isolated points?

The answer is yes, and the reason is the Hartogs theorem.

Indeed, the Hartogs theorem lets us choose a well ordered set $W$ such that there is no injection $W \to \mathscr{P}(\mathbb{R})$. For each $w \in W$, we have a well ordered set $\downarrow w$ and therefore a subset $X^{(\downarrow w)}$ of $\mathbb{R}$. This process defines a function

$$\begin{array}{rcl} W & \to & \mathscr{P}(\mathbb{R}) \\ w & \mapsto & X^{(\downarrow w)}. \end{array}$$

By the choice of $W$, this function is not injective. So, $X^{(\downarrow u)} = X^{(\downarrow v)}$ for some $u, v \in W$ with $u < v$. If we write $U = \downarrow u$ and $V = \downarrow v$, then $X^{(U)} = X^{(V)}$ with $U \prec V$. Now $U \prec U + 1 \preceq V$, and it follows that

$$X^{(U)} \supseteq X^{(U+1)} \supseteq X^{(V)}$$

(since the derivative of a set is contained in it). But $X^{(U)} = X^{(V)}$, so $X^{(U+1)} = X^{(U)}$. That is, $(X^{(U)})' = X^{(U)}$. Or in other words, the iterated derivative $X^{(U)}$ has no isolated points! Mission accomplished.

Thus, we've used well ordered sets, transfinite induction and the Hartogs theorem to find a way of removing all the isolated points from a subset of $\mathbb{R}$. A set with no isolated points is called **perfect**: so we've found a way to attain perfection.

**Digression 8.5.1** A note for those taking General Topology. I told this story for subsets of $\mathbb{R}$, but you can tell it in any topological space. A point $x$ of a topological space $X$ is **isolated** if $\{x\}$ is an open subset of $X$. The argument above shows that there is always some well ordered set $V$ such that $X^{(V)}$ is perfect (has no isolated points).

# Chapter 9

# The axiom of choice

*To read by Monday 11 November: Sections 9.1 and 9.2.*
*To read by Friday 15 November: Sections 9.3 and 9.4.*

So far, we've got by without Axiom 10, the axiom of choice. We've seen that a lot can be done without it. However, the axiom of choice *is* needed for many standard results in analysis, algebra, topology, applied mathematics, etc.

Typically, you need the axiom of choice when you have to make infinitely many arbitrary choices, where 'arbitrary' means something like 'it's not possible to write down a rule telling someone how to choose'. The example in Section 3.4 with infinitely many pairs of shoes and socks illustrates this point: 'always choose the left one' is a rule that works for shoes, but there's no such rule for socks.

We'll prove lots of big theorems in this chapter. There will also be some examples. As usual, the examples are intended to help your understanding, and I hope you'll also *enjoy* them: they demonstrate how you can apply what you've learned here to other parts of mathematics. But at the administrative level, as this course has very few official prerequisites, the examples involving concepts such as vector spaces, groups or rings are non-examinable.

## 9.1 Easy equivalents of the axiom of choice

To use the axiom of choice, it helps to have it available in several different but equivalent forms. In any given application, one form of it is often easier to apply than others.

**Definition 9.1.1** A statement $S$ is **equivalent to the axiom of choice** if (i) Axioms 1–9 together with the axiom of choice imply $S$, and (ii) Axioms 1–9 together with $S$ imply the axiom of choice.

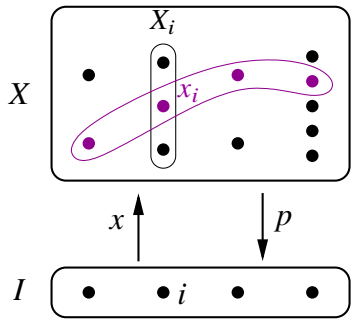



Figure 9.1: An element $x$ of the product $\prod X_i$ is a section of $p\colon X \to I$.

In this section, we meet four statements that can be shown relatively easily to be equivalent to the axiom of choice. Each of them requires some terminology, which I will introduce now.

Recall from Section 6.5 that a family of sets, indexed by a set $I$, is simply a set $X$ together with a function $X \xrightarrow{p} I$. We write $X_i = p^{-1}(i)$ and think of it as the $i$th member of the family.

We can then form a set that deserves to be called $\prod_{i\in I} X_i$, the product of the sets $X_i$. Informally, an element of $\prod_{i\in I} X_i$ should be a family $(x_i)_{i\in I}$ with $x_i \in X_i$ for each $i \in I$. Since $X_i \subseteq X$ is the fibre of $p$ over $i$, that means $x_i \in X$ with $p(x_i) = i$ for each $i \in I$. Writing $x_i$ as $x(i)$, we see that the family $(x_i)_{i\in I}$ amounts to a function $x\colon I \to X$ such that $p(x(i)) = i$ for all $i \in I$. That is, it's just a section of $p$! See Figure 9.1.

Formally, for a family $X \xrightarrow{p} I$, we define its **product** to be

$$\prod_{i\in I} X_i = \{\text{sections of } p\} = \{x \in X^I : p \circ x = \mathrm{id}_I\}.$$

And as above, we usually write elements $x \in \prod_{i\in I} X_i$ as $(x_i)_{i\in I}$, where $x_i = x(i)$.

**Examples 9.1.2** i. Let $X$ and $Y$ be sets, and form the two-member family $(X_i)_{i\in \mathbf{2}}$ with $X_\mathsf{T} = X$ and $X_\mathsf{F} = Y$, as in Example 6.5.5(iii). Then the product $\prod_{i\in\mathbf{2}} X_i$ is $X \times Y$, as a Workshop 5 question asks you to show.

ii. Let $I$ and $Y$ be sets, and take the constant family $I \times Y \xrightarrow{\mathrm{pr}_1} I$ (Example 6.5.5(ii)), also written as $(Y)_{i\in I}$ (Example 6.5.11). What is its product?

A section of $\mathrm{pr}_1$ is a function $(e, f)\colon I \to I \times Y$ such that $\mathrm{pr}_1 \circ (e, f) = \mathrm{id}_I$. Here $e\colon I \to I$ and $f\colon I \to Y$. But $\mathrm{pr}_1 \circ (e, f) = e$, so this just means $e = \mathrm{id}_I$. Hence the sections of $\mathrm{pr}_1$ are in bijection with the functions $f\colon I \to Y$, giving

$$\prod_{i\in I} Y \cong Y^I.$$

This is what the notation leads us to expect.

iii. Let $(X_i)_{i\in I}$ be a family such that $X_j$ is empty for some $j \in I$. Then for the corresponding function $X \xrightarrow{p} I$, the fibre $p^{-1}(j)$ is empty. Since a section $x$ of $p$ must satisfy $x_j \in p^{-1}(j)$, there are no sections. So $\prod_{i\in I} X_i$ is empty. Again, the notation leads us to expect this: multiplying by zero should give zero!

Now here's a question.

*Is a product of nonempty sets necessarily nonempty?*

An answer of 'yes' means we always have a way of choosing a family $(x_i)_{i\in I} \in \prod_{i\in I} X_i$, as long as each individual set $X_i$ has at least one element. We will see that it is equivalent to the axiom of choice.

Next: a relation $R$ between sets $X$ and $Y$ is **total** if for all $x \in X$, there exists $y \in Y$ such that $xRy$. We can think of $R$ as a 'multi-valued function' from $X$ to $Y$, where we assign to each $x \in X$ not just one element of $Y$, but potentially many of them—and always at least one, if $R$ is total.

Let us say that a function $f\colon X \to Y$ **refines** $R$ if $xRf(x)$ for all $x \in X$. Question:

*Can every total relation be refined to a function?*

That is, for every total relation, is there a function that refines it? A 'yes' to this question is equivalent to the axiom of choice.

**Warning 9.1.3** The meaning of 'total' here is different from its meaning in 'total order'. To avoid confusion, sometimes total relations are called entire relations instead. But total relation seems to be the most common name.

Next, write $\mathscr{P}'(X) = \{A \in \mathscr{P}(X) : A \text{ is nonempty}\}$ for the set of nonempty subsets of a set $X$. A **choice function** on $X$ is a function $f\colon \mathscr{P}'(X) \to X$ such that $f(A) \in A$ for all $A \in \mathscr{P}'(X)$. Question:

*Does every set have a choice function?*

It's clear that *some* sets do. For example, if $X = \mathbb{N}$ then we can define $f(A)$ to be the least element of $A$. The same argument works for any set that has at least one well ordering on it. But it's not so clear in general. A 'yes' answer means that no matter what $X$ is, we have a way of choosing an element of each nonempty subset. We will see that it is equivalent to the axiom of choice.

Finally, let $\sim$ be an equivalence relation on a set $X$. A **system of representatives** for $\sim$ is a subset $A$ of $X$ with the following property: for all $x \in X$, there exists a unique $a \in A$ such that $x \sim a$. For example, if $X = \mathbb{Z}$ and $\sim$ is congruence mod 5, then $\{0, 1, 2, 3, 4\}$ is a system of representatives for $\sim$, as is $\{-10, 12, 6, 24, -97\}$. Question:

*Does every equivalence relation have a system of representatives?*

A 'yes' answer means that we always have a way of choosing one element from each equivalence class. And this, too, is equivalent to the axiom of choice.

Now let's prove all these equivalences.

**Proposition 9.1.4** *Each of the following statements is equivalent to the axiom of choice.*

*i. The product of any family of nonempty sets is nonempty.*

*ii. Every total relation can be refined to a function.*

*iii. Every set has a choice function.*

*iv. Every equivalence relation has a system of representatives.*

**Proof** Assume Axioms 1–9.

Axiom of choice $\Leftrightarrow$ (i): a function $X \xrightarrow{p} I$ is surjective if and only if each of its fibres is nonempty. Both the axiom of choice and (i) state that such a function has a section.

Now we prove that (axiom of choice) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (axiom of choice).

Axiom of choice $\Rightarrow$ (ii): let $R$ be a total relation between sets $X$ and $Y$. The function

$$\begin{array}{rccc} p\colon & R & \to & X \\ & (x, y) & \mapsto & x \end{array}$$

is surjective since $R$ is total. So by the axiom of choice, $p$ has a section, which can be written as $x \mapsto (x, f(x))$ for some function $f\colon X \to Y$. Then $(x, f(x)) \in R$ for all $x \in X$, so $f$ refines $R$.

(More formally: if $h\colon X \to R$ is a section of $p$ and we define $f$ as the composite $X \xrightarrow{h} R \hookrightarrow X \times Y \xrightarrow{\mathrm{pr}_2} Y$, then $h(x) = (x, f(x))$ for all $x \in X$.)

(ii) $\Rightarrow$ (iii): let $X$ be a set. There is a relation $\ni'_X$ between $\mathscr{P}'(X)$ and $X$ defined by $A \ni'_X x \iff x \in_X A$, for $A \in \mathscr{P}'(X)$ and $x \in X$. Then $\ni'_X$ is total, because $\mathscr{P}'(X)$ consists of only *nonempty* sets. Hence by (ii), it can be refined to a function $\mathscr{P}'(X) \to X$, which by definition is a choice function.

(iii) $\Rightarrow$ (iv): let $\sim$ be an equivalence relation on a set $X$. By (iii), there is a choice function $f$ on $X$. Put $A = \{f([x]) : x \in X\}$, where $[x]$ is the equivalence class of $X$ (which is nonempty as it contains $x$). We show that $A$ is a system of representatives of $\sim$.

Let $x \in X$; we must prove there exists a unique element of $A$ equivalent to $x$. For existence, $f([x]) \in [x]$, so $f([x]) \sim x$ with $f([x]) \in A$. For uniqueness, let $y \in X$ with $f([y]) \sim x$. Since $f([y]) \in [y]$, we also have $f([y]) \sim y$. Hence $x \sim y$, giving $[x] = [y]$ and so $f([y]) = f([x])$.

(iv) $\Rightarrow$ axiom of choice: let $X \xrightarrow{p} I$ be a surjection. By (iv), the induced equivalence relation $\sim_p$ on $X$ has a system of representatives $A$. Let

$$R = \{(i, x) \in I \times X : i = p(x) \text{ and } x \in_X A\} \subseteq I \times X.$$

For each $i \in I$, the fibre $p^{-1}(i)$ is an equivalence class of $\sim_p$ and therefore contains a unique element of $A$. It follows that the relation $R$ between $I$ and $X$ is functional. Hence there is a unique function $h\colon I \to X$ with graph $R$. For each $i \in I$, the pair $(i, h(i))$ is an element of the graph of $h$, which is equal to $R$, so $i = p(h(i))$ by definition of $R$. Hence $h$ is a section of $p$. □

**Examples 9.1.5** We can use the axiom of choice and Proposition 9.1.4 to prove some results outside set theory.

i. Let $f\colon \mathbb{R} \to \mathbb{R}$ be a function that is 'sequentially continuous' at 0, that is, for every real sequence $(x_n)$,

$$x_n \to 0 \text{ as } n \to \infty \quad \Longrightarrow \quad f(x_n) \to f(0) \text{ as } n \to \infty.$$

Then $f$ is continuous at 0.

You've probably seen a proof that goes like this. We prove the contrapositive. Suppose $f$ is not continuous at 0. Then there exists $\varepsilon > 0$ such that for all $\delta > 0$, there is some $x \in (-\delta, \delta)$ with $|f(x) - f(0)| \geq \varepsilon$. So for each integer $n \geq 1$, we can choose some $x_n \in (-1/n, 1/n)$ such that $|f(x_n) - f(0)| \geq \varepsilon$. Then $(x_n)$ is a sequence with $x_n \to 0$ but $f(x_n) \not\to f(0)$.

There is an implicit use of the axiom of choice here. First we said that for each $n$, there exists a real number $x_n$ with a certain property, and then we jumped to saying that there exists a *sequence* $(x_n)$ such that $x_n$ has that property for each $n$. We're implicitly using part (i) of Proposition 9.1.4: a product of nonempty sets is nonempty. Formally, if we put

$$X_n = \{x \in \mathbb{R} : x \in (-1/n, 1/n) \text{ and } |f(x) - f(0)| \geq \varepsilon\}$$

then each $X_n$ is nonempty. Hence by the axiom of choice, $\prod_{n \geq 1} X_n$ is nonempty, which means there is a sequence $(x_n)$ with the property required.

ii. Here's a theorem you may have met in a course on analysis or topology.

Let $X_0 \supseteq X_1 \supseteq \cdots$ be a sequence of nonempty closed subsets of $\mathbb{R}^N$ (or more generally, any complete metric space), and suppose that $\mathrm{diam}(X_n) \to 0$ as $n \to \infty$. Here $\mathrm{diam}(X)$ is the **diameter** of $X$, defined as $\sup\{d(x, y) : x, y \in X\}$. Theorem: $\bigcap_{n\in\mathbb{N}} X_n$ has exactly one element.

That it has at most one element follows immediately from the assumption that $\mathrm{diam}(X_n) \to 0$ as $n \to \infty$. Where the axiom of choice comes in is in showing that it has any elements at all.

The argument goes like this. Since each $X_n$ is nonempty, the axiom of choice lets us choose a sequence $(x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} X_n$. The diameter hypothesis implies that the sequence is Cauchy, which implies that it converges, and one can show that the point of convergence must lie in $\bigcap_{n\in\mathbb{N}} X_n$.

iii. We could dream of assigning a length to every subset of $\mathbb{R}$, an area to every subset of $\mathbb{R}^2$, and so on. This is, however, impossible, at least if the concepts of length, area, etc., are to behave in a sensible way. In the jargon, **unmeasurable** sets exist. (This is a precise term which I will not define.)

Here's how to construct one. Define an equivalence relation $\sim$ on $[0, 1]$ by $x \sim y \iff x - y \in \mathbb{Q}$. By the axiom of choice and Proposition 9.1.4(iv), we can choose a system $A$ of representatives of $\sim$. A short argument shows that $A$ is unmeasurable. Details are omitted here, but if you're interested, look up Vitali sets.

Proposition 9.1.4 also enables us to pay off a debt. Back in Lemma 6.5.10, I claimed that if we have two $I$-indexed families of sets $X \to I$ and $X' \to I$ such that $X_i \cong X'_i$ for all $i \in I$, then the families are in fact isomorphic (in the sense of Definition 6.5.8). This result is needed in order for the notation $(X_i)_{i\in I}$ to be reasonable, as explained after the statement of the lemma. We couldn't prove it then, but we can prove it now.

**Proof of Lemma 6.5.10** Let $X \xrightarrow{p} I$ and $X' \xrightarrow{p'} I$ be families of sets, and suppose that $X_i \cong X'_i$ for all $i \in I$ (where as usual $X_i$ means $p^{-1}(i)$, and $X'_i$ similarly). We have to prove there is a bijection $k : X \to X'$ such that $p' \circ k = p$.

For sets $A$ and $B$, write $\mathrm{Iso}(A, B)$ for the set of isomorphisms $A \to B$. For each $i \in I$, the set $\mathrm{Iso}(X_i, Y_i)$ is nonempty. So, using the axiom of choice and Proposition 9.1.4(i), the product $\prod_{i\in I} \mathrm{Iso}(X_i, Y_i)$ is nonempty. Choose an element $(k_i)_{i\in I}$. Then $k_i$ is an isomorphism $X_i \to Y_i$ for each $i \in I$.

Now put

$$R = \{(x, x') \in X \times X' : \text{there exists } i \in I \text{ such that } x \in_X X_i \text{ and } k_i(x) = x'\}.$$

Since each element of $X$ lies in exactly one of the sets $X_i$, the relation $R$ between $X$ and $X'$ is functional. It is therefore the graph of a function $k\colon X \to X'$. By construction, $k(x) = k_i(x)$ whenever $x \in X_i$.

It remains to show that $k\colon X \to X'$ is an isomorphism over $I$, that is, $p' \circ k = p$ and $k$ is an isomorphism of sets. For each $i \in I$ and $x \in X_i$, we have $k(x) = k_i(x) \in X'_i$, so $p'(k(x)) = i = p(x)$. Hence $p' \circ k = p$. I leave the proof that $k$ is an isomorphism of sets to you. □

**Exercise 9.1.6** As in the last paragraph of the proof, show that the function $k\colon X \to X'$ is an isomorphism of sets. (You can either show it's a bijection or find an inverse.)

**Digression 9.1.7** There is another small gap in the proof above. I formed the product $\prod \mathrm{Iso}(X_i, X'_i)$, thus taking for granted that there exists a family $Y \xrightarrow{q} I$ such that $q^{-1}(i) \cong \mathrm{Iso}(X_i, X'_i)$ for each $i \in I$. It's easy enough to show this *if* we know there's a family $Z \xrightarrow{r} I$ such that $r^{-1}(i) \cong {X'_i}^{X_i}$ for all $i \in I$, since we can define $Y$ as a suitable subset of $Z$. But how do we know that such a family $Z \to I$ exists?

In fact, given families $X \to I$ and $X' \to I$, it's always possible to form three new families indexed by $I$: one whose $i$th member is $X_i + X'_i$, one whose $i$th member is $X_i \times X'_i$, and one whose $i$th member is ${X'_i}^{X_i}$. The first two are relatively easy to construct, but the last (which is the one we need here) is harder. For the sake of time, I've skipped all three. But if you're feeling adventurous, see if you can figure out how you'd construct them.

## 9.2 Zorn's lemma

Sometimes in mathematics, we want to find an object that is 'maximal' in an appropriate sense. For example, a basis of a vector space is a linearly independent set that is maximal in the sense that no more elements can be added to it while keeping it linearly independent. Or in a commutative ring, a maximal ideal is a proper ideal that cannot be enlarged any further—the only other ideal containing it is the whole ring. (The maximal ideals are important because they are exactly the ideals $I$ such that $R/I$ is a field.)

Generally, an element $m$ of an ordered set $X$ is **maximal** if there is no element $x \in X$ such that $m < x$.

**Warning 9.2.1** A **greatest** element of an ordered set $X$ is an element $g$ such that $x \leq g$ for all $x \in X$. A greatest element is certainly maximal, but a maximal element need not be greatest. And an ordered set can have at most one greatest element, but multiple maximal elements.

For *totally* ordered sets, maximal is equivalent to greatest, but for ordered sets in general, being greatest is a stronger condition.

**Examples 9.2.2** i. The ordered set of Figure 8.2 has three maximal elements, but no greatest element.

ii. None of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$ (with their standard orderings) has a maximal element.

iii. Let $V$ be a vector space. Let $X$ be the set of linearly independent subsets of $V$, ordered by $\subseteq$. Then the maximal elements of $X$ are precisely the bases of $V$.

(Reminder: anything involving groups, rings, vector spaces, etc. is non-examinable. But I suggest you read all the examples that you have the background for, as they'll help you to understand the general concepts.)

iv. Let $R$ be a commutative ring. Let $X$ be the set of proper ideals of $R$, ordered by $\subseteq$. Then a maximal ideal of $R$ is, by definition, a maximal element of the ordered set $X$.

**Exercise 9.2.3** Prove the statement about bases made in Example 9.2.2(iii).

If we had an ordered set and wanted to prove it had a maximal element, how could we go about it?

We could start by choosing an element $x_0$ at random. If $x_0$ is maximal, we're done. If not, that means there's some element $x_1$ with $x_0 < x_1$. If $x_1$ is maximal, we're done. If not, there's some $x_2$ with $x_0 < x_1 < x_2$. And we can imagine continuing like this, building up a longer and longer chain, and hoping it eventually reaches a maximal element.

If this reminds you of the preamble to the proof of Proposition 8.4.3, good! In fact, Proposition 8.4.3 will make it easy to prove the following major result.

**Theorem 9.2.4 (Zorn's lemma)** *Let $X$ be an ordered set in which every chain has an upper bound. Then $X$ contains a maximal element.*

**Proof** Suppose for a contradiction that $X$ has no maximal element. For each chain $C$ in $X$, there is an upper bound $u$ of $C$ in $X$, and since $u$ is not maximal, there is some element $v > u$ of $X$. Then $v$ is an upper bound of $C$ in $X$ that is not in $C$.

So, every chain $C$ has an upper bound in $X$ that does not belong to $C$. Now by the axiom of choice, there is a function $\varphi\colon \{\text{chains in } X\} \to X$ assigning to each chain $C$ an upper bound $\varphi(C)$ not in $C$. This contradicts Proposition 8.4.3 and completes the proof.

(Formally, at the point where we used the axiom of choice, we were applying Proposition 9.1.4(ii) to the total relation $R$ between $\{\text{chains in } C\}$ and $X$ defined by $CRx$ if and only if $x$ is an upper bound of $C$ not in $C$.) □

**Exercise 9.2.5** The empty ordered set obviously has no maximal element, so in Zorn's lemma, why don't we need to add the hypothesis that $X$ is nonempty?

**Exercise 9.2.6** If we already know Zorn's lemma then Proposition 8.4.3 follows very quickly. How?

We will need Zorn's lemma in Chapter 10 to prove our main results in cardinal arithmetic. But here are two of its uses in algebra, plus a cautionary non-example.

**Examples 9.2.7** i. Every vector space has a basis. You already know this for *finite-dimensional* vector spaces, but beyond finite dimensions, it's much less obvious. For example, the continuous functions $[0, 1] \to \mathbb{R}$ form a real vector space, but finding an explicit basis for it is probably impossible (try!).

Here is the proof that every vector space $V$ has a basis, using Zorn's lemma. As in Example 9.2.2(iii), let $X$ be the set of linearly independent subsets of $V$, ordered by $\subseteq$. We saw there that its maximal elements are exactly the bases. So by Zorn's lemma, a basis exists as long as every chain in $X$ has an upper bound.

So, let $C$ be a chain in $X$. This means that $C$ is a set of linearly independent subsets of $V$ such that for all $S, S' \in C$, either $S \subseteq S'$ or $S' \subseteq S$. We will prove that $C$ has an upper bound. Let $T = \bigcup_{S \in C} S$. If we can show that $T$ is linearly independent then $T$ is an upper bound of $C$ in $X$, and we are done.

To show that $T$ is linearly independent, let $v_1, \ldots, v_n$ be distinct elements of $T$ and let $\alpha_1, \ldots, \alpha_n$ be scalars such that $\sum \alpha_i v_i = 0$. By definition of $T$, there are $S_1, \ldots, S_n \in C$ such that $v_1 \in S_1, \ldots, v_n \in S_n$. Since $C$ is a chain, there is some $k \in \{1, \ldots, n\}$ such that $S_k$ contains all of $S_1, \ldots, S_n$. (See Workshop 4, question 9(i).) Then $v_1, \ldots, v_n$ are distinct elements of the linearly independent set $S_k$ with $\sum \alpha_i v_i = 0$, so $\alpha_1 = \cdots = \alpha_n = 0$, as required.

ii. Here we show that for every commutative ring $R$ with multiplicative identity, there exists a surjective homomorphism from $R$ to some field. (It's not even obvious that there's *any* homomorphism from $R$ to a field.)

As in Example 9.2.2(iv), let $X$ be the set of proper ideals of $R$, ordered by $\subseteq$. To show that every chain $C$ in $X$ has an upper bound, we can take its union $J = \bigcup_{I \in C} I$. You can verify that $J$ is an ideal, but there is a subtlety here: the elements of $X$ are the *proper* ideals, and how do you know that $J$ is proper? The key is that in a ring with 1, an ideal is proper if and only if it does not contain 1. Since no ideal in $C$ contains 1, neither does $J$.

So we can apply Zorn's lemma to conclude that $R$ contains a maximal ideal $I$. Then the canonical homomorphism $R \to R/I$ is a surjection to a field.

iii. A non-example to show you the limitations of Zorn's lemma: not every group (even abelian) has a maximal proper subgroup. For instance, the additive group $\mathbb{Q}$ doesn't. (The proof is too much of a digression, and omitted.)

Why can't we prove that every group $G$ has a maximal proper subgroup by applying Zorn's lemma to the set of proper subgroups of $G$, ordered by inclusion? Doesn't every chain have an upper bound, namely, its union?

It's true that the union of a chain of subgroups is a subgroup. However, the union of a chain of *proper* subgroups need not be proper. For example, let $H_n$ be the set of rational numbers that can be expressed as a fraction with denominator $n!$. You can check that $H_n$ is a proper subgroup of $\mathbb{Q}$ for each $n \in \mathbb{N}$. And $H_0 \subseteq H_1 \subseteq \cdots$, so in the ordered set of proper subgroups, $\{H_n : n \in \mathbb{N}\}$ is a chain. However, $\bigcup_{n \in \mathbb{N}} H_n = \mathbb{Q}$, since every rational number can be expressed as a fraction whose denominator is a factorial. So this chain has no upper bound, and Zorn's lemma can't be applied.

**Digression 9.2.8** Theorem 9.2.4 is referred to as Zorn's lemma by almost everyone, a notable exception being Max Zorn (1906–1993) himself. Zorn neither stated nor proved it, and repeatedly expressed his preference for not calling it that. He did postulate a closely related principle, and there is a complex web of other statements somewhat like Zorn's lemma, studied by different people in different parts of the world at different times in that era (Figure 9.2). Disentangling exactly who did what when is delicate historical work of a type that few mathematicians can be bothered with. The moral: attributing results or concepts to a single person can be overly simplistic. Most mathematical advances are the outcome of a long-term community effort.

A refinement of Zorn's lemma is often useful.

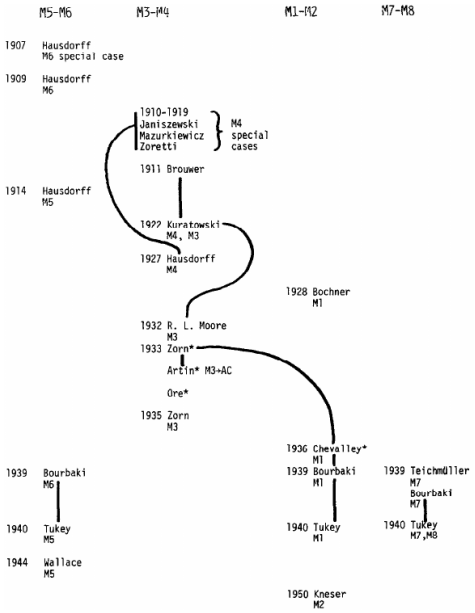



Figure 9.2: A network of Zorn-like principles (Figure 1 of Paul J. Campbell, The origin of "Zorn's lemma", *Historia Mathematica* 5 (1978), 77–89).

**Corollary 9.2.9** *Let $X$ be an ordered set in which every chain has an upper bound. Let $x \in X$. Then $X$ contains a maximal element $m$ such that $m \geq x$.*

**Proof** Write $\uparrow x = \{x' \in X : x' \geq x\}$, with the induced order from $X$. Let us check that every chain $C$ in $\uparrow x$ has an upper bound in $\uparrow x$. If $C$ is empty then $x$ is an upper bound of $C$ in $\uparrow x$. Otherwise, choose some $y \in C$. Since $C$ has an upper bound $u$ in $X$, we have $u \geq y \geq x$, giving $u \in \uparrow x$. So in either case, $C$ has an upper bound in $\uparrow x$. Zorn's lemma now implies that $\uparrow x$ has a maximal element $m$, which is a maximal element of $X$ satisfying $m \geq x$. □

**Example 9.2.10** By Corollary 9.2.9 and what we showed in Example 9.2.7(i), every linearly independent subset of a vector space can be extended to a basis.

We can also use Zorn's lemma to settle a fundamental question about sets: given sets $X$ and $Y$, must there exist either an injection $X \to Y$ or an injection $Y \to X$? Yes!

**Theorem 9.2.11 (Cardinal comparability)** *For all sets $X$ and $Y$, either $X \leq Y$ or $Y \leq X$.*

Cardinal comparability is a companion to the Cantor–Bernstein theorem, that if both $X \leq Y$ and $Y \leq X$ then $X \cong Y$. All in all, $\leq$ is a total order on sets, in the same loose sense as $\preceq$ for well ordered sets (text preceding Lemma 8.2.12).

**Proof** Define a **partial bijection** between $X$ and $Y$ to be a relation $R$ between $X$ and $Y$ such that:

- for all $x \in X$, there is at most one $y \in Y$ such that $xRy$, and
- for all $y \in Y$, there is at most one $x \in X$ such that $xRy$

(Figure 9.3(a)). Let $P \subseteq \mathscr{P}(X \times Y)$ be the set of partial bijections between $X$ and $Y$, ordered by $\subseteq$. We will show that every chain in $P$ has an upper bound, apply Zorn's lemma to obtain a maximal element of $P$, and deduce the theorem.

First we show that every chain $C$ in $P$ has an upper bound. Let

$$S = \bigcup_{R \in C} R \subseteq X \times Y.$$

Then $S$ is an upper bound of $C$ in $P$ as long as $S$ is a partial bijection. By symmetry, it is enough to prove that $S$ satisfies the first of the two bullet points above. So let $x \in X$ and $y, y' \in Y$ with $xSy$ and $xSy'$; we must show that $y = y'$. Since $xSy$, there is some $R \in C$ such that $xRy$, and similarly, there is some $R' \in C$ such that $xR'y'$. Since $C$ is a chain, we may assume without loss of generality that $R' \subseteq R$. Then $xRy$ and $xRy'$. But $R$ is a partial bijection, so $y = y'$, as required.

Zorn's lemma now implies that $P$ has a maximal element $R$.

We show that either $R$ is a functional relation between $X$ and $Y$ or $R^{\mathrm{op}}$ is a functional relation between $Y$ and $X$. That is, we show that at least one of the following statements holds:

- for all $x \in X$, there exists $y \in Y$ such that $xRy$, or
- for all $y \in Y$, there exists $x \in X$ such that $xRy$.

Suppose neither holds. Then there exists $x' \in X$ that is not $R$-related to any element of $Y$, and there exists $y' \in Y$ that is not $R$-related to any element of $X$ (Figure 9.3(b)). In particular, $(x', y') \notin R$. Put $R' = R \cup \{(x', y')\}$. Then $R'$ is a partial bijection, as you can check. But $R$ is a *proper* subset of $R'$, which contradicts $R$ being maximal in the set $P$ of partial bijections. Hence one of the two statements above does hold.

Assume without loss of generality that it is the first. Then $R$ is a functional relation between $X$ and $Y$. Hence there is a function $f : X \to Y$ with graph $R$. The second condition in the definition of partial bijection is that for all $y \in Y$, there is at most one $x \in X$ such that $xRy$. Since $xRy \Leftrightarrow f(x) = y$, this means that $f : X \to Y$ is injective. Thus, $X \leq Y$. □

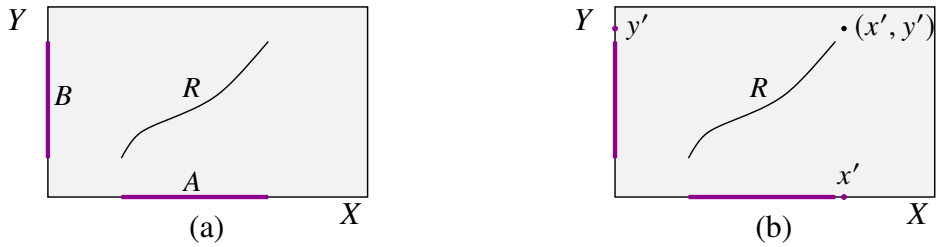



Figure 9.3: (a) A partial bijection $R$ between sets $X$ and $Y$, to be thought of as the graph of a bijection between subsets $A \subseteq X$ and $B \subseteq Y$; (b) the relation $R' = R \cup \{(x', y')\}$ in the proof of Theorem 9.2.11.

## 9.3 Harder equivalents of the axiom of choice

With the work we've done, we can now prove quickly that three important statements are all equivalent to the axiom of choice.

**Theorem 9.3.1** *Each of the following statements is equivalent to the axiom of choice.*

*i. Zorn's lemma: in an ordered set where every chain has an upper bound, there is at least one maximal element;*

*ii. cardinal comparability: for all sets $X$ and $Y$, either $X \leq Y$ or $Y \leq X$;*

*iii. the* **well ordering principle***: for every set $X$, there exists a well ordering on $X$.*

**Proof** We show that (axiom of choice) $\Rightarrow$ (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (axiom of choice).

Axiom of choice $\Rightarrow$ (i): this is Theorem 9.2.4.

(i) $\Rightarrow$ (ii): see the proof of Theorem 9.2.11.

(ii) $\Rightarrow$ (iii): assume cardinal comparability, and let $X$ be a set. By Theorem 8.3.1 (Hartogs), there exists a well ordered set $(W, \leq)$ such that $W \not\leq X$. By cardinal comparability, $X \leq W$, that is, there is an injection $X \hookrightarrow W$. The induced order on $X$ is a well order, by Example 8.1.5(ii).

(iii) $\Rightarrow$ axiom of choice: assuming the well ordering principle, we prove that every equivalence relation $\sim$ on a set $X$ has a system of representatives, which suffices by Proposition 9.1.4. Choose a well order on $X$, and put

$$A = \{x \in X : x \text{ is the least element of } [x]_\sim\}.$$

Since each equivalence class has exactly one least element, $A$ is a system of representatives for $\sim$. □

**Remark 9.3.2** The well ordering principle causes some people to doubt the 'truth' of the axiom of choice (whatever that means). For example, it implies that $\mathbb{R}$ has a well order on it, which might seem counterintuitive. The usual order certainly isn't a well order, and actually *constructing* one is impossible. But if we assume the axiom of choice, we know it's there; we just can't lay our hands on it.

**Digression 9.3.3** If you're doing General Topology, you'll have met Tychonoff's theorem: a product of compact spaces is compact. The version involving a product $X \times Y$ of *two* spaces doesn't need the axiom of choice. But the full theorem, involving the product $\prod_{i \in I} X_i$ of a potentially infinite family of spaces, does. In fact, it can be shown that the full Tychonoff theorem is *equivalent* to the axiom of choice.

Having a well order on a set allows us to fulfil our urge to name the elements as first, second, third, .... We acquire this instinct from working with finite sets (as mentioned in the introduction to Chapter 8), but the well ordering principle gives us a way to extend it to infinite sets.

The well ordering principle also enables us to use results on well ordered sets to deduce facts about ordinary sets. Here is a very important case. The big theorems are coming thick and fast!

**Theorem 9.3.4** *Let $(X_i)_{i \in I}$ be a family of sets, with $I$ nonempty. Then there is some $i \in I$ such that for all $j \in I$, we have $X_i \leq X_j$.*

Cardinal comparability is the case where $I$ only has two elements. Theorem 9.3.4 is much more powerful. Whereas cardinal comparability says that sets are *totally* ordered by $\leq$, Theorem 9.3.4 says that sets are *well* ordered by $\leq$ (all with the same caveats as mentioned before Lemma 8.2.12).

**Proof** For each $i \in I$, the set $\mathrm{WO}(X_i)$ of well orders on $X_i$ is nonempty, by the well ordering principle. Hence the product $\prod_{i \in I} \mathrm{WO}(X_i)$ is nonempty (using the axiom of choice a second time). So, it has an element $(\leq_i)_{i \in I}$. Now $((X_i, \leq_i))_{i \in I}$ is a nonempty family of well ordered sets, so by Theorem 8.2.13, there is some $i \in I$ such that for all $j \in I$,

$$(X_i, \leq_i) \preceq (X_j, \leq_j).$$

In particular, for all $j \in I$, we have $X_i \leq X_j$. □

**Remark 9.3.5** Theorem 9.3.4 is also equivalent to the axiom of choice. For it implies cardinal comparability and is implied by the well ordering principle, both of which are equivalent to the axiom of choice (Theorem 9.3.1).

## 9.4 Unnecessary uses of the axiom of choice

**Warning 9.4.1** This whole section is a warning: the axiom of choice isn't needed as often as you might think!

Broadly speaking, there are three kinds of situation where one might initially think that the axiom of choice is needed, but where it isn't.

- Situations where only a finite number of choices are made.
- Situations where choices can be made in an algorithmic way.
- Situations where it looks like choices need to be made, but they don't.

The last of these categories is particularly relevant to topology, as I will explain in the optional final part of this section. But now I will explain the first two.

Let's begin at the beginning: to show that a nonempty set has an element, you don't need the axiom of choice. Having an element is just the definition of nonempty. Put another way, every surjection $X \xrightarrow{p} \mathbf{1}$ has a section. For $p$ being a surjection means exactly that $X$ has an element, and any element $x$ is a section of $p$.

I emphasize this because an argument that involves picking a particular element of a nonempty set $X$ may involve a phrase such as 'choose an element of $X$', which might seem to signal that the axiom of choice is being used. But the word 'choose' is not always a red flag.

For example, consider Lemma 5.5.3, that every injection with nonempty domain has a retraction. In the proof, we took an injection $i : Y \to X$, and then I wrote 'Assuming $Y$ is nonempty, we can fix an element $b \in Y$.' In other words, I chose an element $b$. This is possible simply because $Y$ *has* an element, by hypothesis. The axiom of choice is not needed.

Here's another way to look at it. The proof of Lemma 5.5.3 constructs, for each $b \in Y$, a retraction of $i$. Since there exists an element of $Y$, there exists a retraction of $i$. And that's it.

Now let's prove that in order to make a *finite* number of choices, the axiom of choice is never needed.

**Definition 9.4.2** A set $I$ is **finite** if there exists $n \in \mathbb{N}$ such that $I \cong \mathbf{n}$.

**Lemma 9.4.3** *Let $p : X \to I$ be a surjection from a set $X$ to a finite set $I$. Then Axioms 1–9 imply that $p$ has a section.*

**Proof** We prove by induction on $n \in \mathbb{N}$ that every surjection into $\mathbf{n}$ has a section, without using the axiom of choice.

Base case: $\mathbf{0}$ is empty, and every function into the empty set is invertible.

Inductive step: let $n \in \mathbb{N}$ and assume the result for $n$. Take a surjection $p\colon X \to \mathbf{n}+\mathbf{1} = \{i \in \mathbb{N} : i \leq n\}$. Define subsets $Y, Z \subseteq X$ by

$$Y = p^{-1}\{0, \ldots, n-1\}, \qquad Z = p^{-1}\{n\}$$

(where of course $\{0, \ldots, n-1\}$ is informal notation for $\{i \in \mathbb{N} : i < n\}$.) Then $X = Y \amalg Z$. The function

$$\begin{array}{rccc} p'\colon & Y & \to & \{0, \ldots, n-1\} \\ & y & \mapsto & p(y) \end{array}$$

is surjective since $p$ is. Hence by inductive hypothesis, $p'$ has a section $h'\colon \{0, \ldots, n-1\} \to Y$. Also, $Z$ is nonempty since $p$ is surjective, so $Z$ has an element $z$. Define $h\colon \mathbf{n}+\mathbf{1} = \{0, \ldots, n\} \to X$ by

$$h(i) = \begin{cases} h'(i) & \text{if } i < n, \\ z & \text{if } i = n. \end{cases}$$

If $i < n$ then $p(h(i)) = p'(h'(i)) = i$, and in the case $i = n$, we have $p(h(n)) = p(z) = n$. Hence $h$ is a section of $p$, completing the induction. □

We've now shown that the axiom of choice is not needed when we only have finitely many choices to make. That was the first scenario in the list of three.

The second is where the axiom of choice is unnecessary because there is an *algorithmic* way of making the choices. This means, more or less, that you can write down a formula. Here are some examples.

**Examples 9.4.4**

i. Let $Y$ and $I$ be sets, and consider the projection $\mathrm{pr}_1 : I \times Y \to I$. If $Y$ is nonempty then $\mathrm{pr}_1$ is surjective, so the axiom of choice implies it has a section. But we can prove that anyway, without choice. Indeed, pick an element $y \in Y$ and define $h\colon I \to I \times Y$ by $h(i) = (i, y)$. Then $h$ is a section of $\mathrm{pr}_1$.

ii. A different take on the same example: let $Y$ be a nonempty set, let $I$ be any set, and consider the constant family $(Y)_{i \in I}$. To prove that its product $\prod_{i \in I} Y$ is nonempty without the axiom of choice, we can simply take an element $y \in Y$ and note that $(y)_{i \in I}$ is an element.

iii. When the choices we have to make are from subsets of a set that can be well ordered, there's no need for the axiom of choice, because we can always

choose the least element of each subset. For example, if $(A_i)_{i \in I}$ is a family of nonempty subsets of $\mathbb{N}$ then we know that $\prod_{i \in I} A_i$ is nonempty even without the axiom of choice: for if we define $a_i$ to be the least element of $A_i$, then we've specified an element $(a_i)_{i \in I}$ of $\prod_{i \in I} A_i$.

Similarly, if you want to prove that every equivalence relation on $\mathbb{N}$ has a system of representatives, you don't need the axiom of choice: just take the representative of each equivalence class to be its least element.

iv. Less obviously, everything I just said about $\mathbb{N}$ and other well ordered sets also holds for $\mathbb{Z}$. Although the *usual* order on $\mathbb{Z}$ is not a well order (Example 8.1.5(iv)), we can define a well order on $\mathbb{Z}$ in the way now described (without using the axiom of choice). Consider the sequence

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

as a function $f : \mathbb{N} \to \mathbb{Z}$. Then $f$ is bijective, so $\mathbb{N} \cong \mathbb{Z}$, and since $\mathbb{N}$ can be well ordered, so can $\mathbb{Z}$. (The property of being well orderable, like everything we do, is isomorphism-invariant. Or explicitly, there is a well order $\trianglelefteq$ on $\mathbb{Z}$ defined by $a \trianglelefteq b \iff f^{-1}(a) \leq f^{-1}(b)$.)

v. Let $(a_n)$ and $(b_n)$ be sequences of real numbers such that $a_n < b_n$ for all $n \in \mathbb{N}$. How do we know that the product of open intervals $\prod_{n \in \mathbb{N}} (a_n, b_n)$ is nonempty? Well, the axiom of choice implies this, but we don't need it: we can explicitly write down an element, such as $\left(\frac{1}{2}(a_n + b_n)\right)_{n \in \mathbb{N}}$.

vi. In the same vein, consider the relation $R$ on $\mathbb{R}$ defined by $x R y \iff \cos x \leq y \leq x^2 + 1$. This is a total relation, since $\cos x \leq x^2 + 1$ for all $x \in \mathbb{R}$. But to prove it can be refined to a function $f$, we don't need the axiom of choice: just put $f(x) = \cos x$ for each $x \in \mathbb{R}$.

*The rest of this section is optional and non-examinable.*

Now we turn to the third and final scenario: where it looks like an infinite number of arbitrary choices need to be made, but in fact, no choices need to be made at all. For some reason, this happens especially often in topology, so I will assume you are taking or have taken General Topology.

**Example 9.4.5** Here is a very useful fact (Exercise 1.6 in this year's General Topology notes). Let $U$ be a subset of a topological space $X$. If for each $x \in U$, there is some open subset $W$ of $X$ such that $x \in W \subseteq U$, then $U$ is open in $X$.

A standard proof goes like this:

> For each $x \in U$, choose an open subset $W_x$ of $X$ such that $x \in W_x \subseteq U$, which we can do by hypothesis. Then $\bigcup_{x \in U} W_x = U$, and $\bigcup_{x \in U} W_x$ is open in $X$ (being a union of open sets), so $U$ is open in $X$.

This proof is correct but uses the axiom of choice, because we are choosing $W_x$ for each point $x \in U$. However, we can tweak the proof to avoid relying on the axiom of choice:

> Let $S$ be the set of open subsets $W$ of $X$ such that $W \subseteq U$. Then $\bigcup_{W \in S} W = U$, by hypothesis. But a union of open sets is open, so $U$ is an open in $X$.

To transform the choicey proof into the choice-free proof, we abandoned the plan of choosing *one* open neighbourhood $W_x$ inside $U$ of each point $x \in X$. Instead, we took *all possible* open sets $W$ inside $U$.

**Example 9.4.6** Here's a similar example: a compact subset $A$ of a Hausdorff space $X$ is closed in $X$. And here's the proof from this year's General Topology notes (Proposition 4.6(ii) there), which is entirely standard:

> We want to show that $X \setminus A$ is open. Let $x \in X \setminus A$. Then for all $y \in A$ there exist disjoint open sets $U_y, V_y$ such that $x \in U_y$ and $y \in V_y$. Then $\{V_y : y \in A\}$ is an open cover of $A$ which hence has a finite subcover $\{V_{y_j} : 1 \leq j \leq n\}$. Then $x$ is in the open set $U_{y_1} \cap \cdots \cap U_{y_n}$ which meets none of the $V_{y_j}$ and hence does not meet $A$. So $X \setminus A$ is open [by Example 9.4.5] and thus $A$ is closed.

Again, this argument uses the axiom of choice, since it requires us to choose for each $y \in A$ the disjoint open sets $U_y$ and $V_y$. But we can rephrase it so as not to use the axiom of choice:

> We want to show that $X \setminus A$ is open. Let $x \in X \setminus A$. Let $S$ be the set of pairs $(U, V)$ of disjoint open sets such that $x \in U$. Then $\{V : (U, V) \in S\}$ is an open cover of $A$, which hence has a finite subcover $\{V_1, \ldots, V_n\}$. Then $x$ is in the open set $U_1 \cap \cdots \cap U_n$, which meets none of the $V_j$ and hence does not meet $A$. So $X \setminus A$ is open (by Example 9.4.5) and thus $A$ is closed.

As in Example 9.4.5, we've eliminated dependence on the axiom of choice by taking all possible $U$s instead of choosing one for each point $x$. Next time you find yourself in a bakery and can't decide what to have, just say 'give me everything!'

Incidentally, the axiom of choice is not needed in order to choose the finite subcover. This is a single choice, just like at the beginning of this section. For any given open cover of a compact space, the set of finite subcovers is nonempty, so it has an element.

Many more examples from elementary topology can be given. If you want a challenge, go through the topology lecture notes and see if you can find more. Then see if you can tweak the proofs so they don't need the axiom of choice. (Warning: some genuinely *do* require choice!)

I mentioned in Digression 9.3.3 that although the full Tychonoff theorem is equivalent to the axiom of choice, the Tychonoff theorem for two spaces does not require choice. This is an excellent example of the situation we're currently discussing. If you want a further challenge, take the proof in the General Topology notes that $X \times Y$ is compact (Theorem 4.18) and try to rephrase it in a way that eliminates its dependence on the axiom of choice.

# Chapter 10

# Cardinal arithmetic

*To read by Monday 18 November: Sections 10.1 and 10.2.*
*To read by Friday 22 November: Sections 10.3 and 10.4.*
*Part of Section 10.4 is labelled as non-examinable.*

The isomorphism classes of finite sets correspond one-to-one with the natural numbers: up to isomorphism, there is one set with 0 elements, one set with 1 element, and so on. Moreover, the set-theoretic operations of coproduct, product and function set correspond to the ordinary arithmetic operations of sum, product and power (Proposition 7.1.14). So the study of isomorphism classes of finite sets, and the behaviour of these set-theoretic operations, is no more or less than number theory.

But coproducts, products and function sets are defined for *all* sets, not just finite ones. So we can try to develop a kind of infinite version of number theory, where we study these operations for sets that may be infinite. This is called **cardinal arithmetic**. And it is dramatically different from number theory, as we will see.

## 10.1 Finite and infinite

If you want to know how sets behave, finite sets can be misleading. In this section, we examine in detail the differences between the finite and the infinite.

Recall from Definition 9.4.2 that a set is finite if and only if it is isomorphic to $\mathbf{n}$ for some $n \in \mathbb{N}$. Here $\mathbf{n}$, also called $B(n)$, was itself defined in Remark 7.1.27; it is $\{0, \ldots, n-1\}$. We'll need some results we proved earlier:

$$\mathbf{m} \leq \mathbf{n} \iff m \leq n, \qquad \mathbf{m} \cong \mathbf{n} \iff m = n \tag{10.1}$$

($m, n \in \mathbb{N}$), by Lemmas 7.1.16 and 7.1.17. A set is **infinite** if it is not finite.

**Remark 10.1.1** The **pigeonhole principle** states that if $m$ pigeons are put into $n$ holes, with $m > n$, then at least one hole contains at least two pigeons. Formally, this means that if $m > n$ then there is no injection $\mathbf{m} \to \mathbf{n}$. An equivalent statement, the contrapositive, is that if $\mathbf{m} \leq \mathbf{n}$ then $m \leq n$. This is part of (10.1).

The **cardinality** or **number of elements** of a finite set $X$, written as $|X|$, is the unique natural number $n$ such that $X \cong \mathbf{n}$. (In particular, $|\mathbf{n}| = n$.) Uniqueness follows from the second part of (10.1), and then (10.1) as a whole implies that for finite sets $X$ and $Y$,

$$X \leq Y \iff |X| \leq |Y|, \qquad X \cong Y \iff |X| = |Y|.$$

(The first left-to-right implication is the pigeonhole principle.) Moreover, when $X$ and $Y$ are finite, Proposition 7.1.14 implies that $X + Y$, $X \times Y$ and $Y^X$ are finite too, with

$$|X + Y| = |X| + |Y|, \qquad |X \times Y| = |X| \cdot |Y|, \qquad |Y^X| = |Y|^{|X|}.$$

Any subset or quotient of a finite set is finite:

**Lemma 10.1.2** *Let $X$ and $Y$ be sets, with $X$ finite. If there exists an injection $Y \to X$ or a surjection $X \to Y$, then $Y$ is also finite.*

**Proof** We may assume that $X = \mathbf{n}$ for some $n \in \mathbb{N}$.

Suppose there is an injection $i \colon Y \to \mathbf{n}$. Give $\mathbf{n}$ its usual order and $Y$ the induced order via $i$ (Example 8.1.5(ii)), which is a well order. By Proposition 8.2.16, $Y \preceq \mathbf{n}$. Then $Y$ is isomorphic to a downset of $\mathbf{n}$, by Lemma 8.2.7. Then by Lemma 8.1.17, $Y$ is isomorphic either to $\mathbf{n}$ itself or to $\downarrow m = \mathbf{m}$ for some $m < n$. In either case, $Y \cong \mathbf{m}$ for some $m \in \mathbb{N}$, so $Y$ is finite.

Now suppose there is a surjection $\mathbf{n} \to Y$. The axiom of choice implies that there is an injection $Y \to \mathbf{n}$, and the result follows from what we have just shown. □

**Digression 10.1.3** In the last part of the proof, we can avoid the axiom of choice as follows. We know that $\mathbf{n} = \{0, \ldots, n-1\}$ has a well order, namely, the one inherited from $\mathbb{N}$. So given a surjection $p \colon \mathbf{n} \to Y$, we can define a section $i$ by taking $i(y)$ to be the least element of $p^{-1}(y)$ for each $y \in Y$. Then $i \colon Y \to \mathbf{n}$ is injective.

If we didn't assume the axiom of choice, cardinal arithmetic would be very different and much more delicate. I will assume it throughout this chapter and use it repeatedly. Here is one way in which it makes life simpler:

**Lemma 10.1.4** *Let $X$ and $Y$ be sets. Then $X \leq Y$ if and only if $X$ is empty or there exists a surjection $Y \to X$.*

**Proof** If $X \leq Y$ and $X$ is nonempty then by Lemma 5.5.3, there is a surjection $Y \to X$. Conversely, if there is a surjection $Y \to X$ then the axiom of choice implies that there is an injection $X \to Y$. □

There are many equivalent characterizations of infiniteness:

**Proposition 10.1.5** *Let $X$ be a set. The following conditions are equivalent:*

*i. $X$ is infinite;*

*ii. $\mathbb{N} \leq X$, that is, there exists an injection $\mathbb{N} \to X$;*

*iii. there exists a surjection $X \to \mathbb{N}$;*

*iv. $X \cong X + \mathbf{1}$;*

*v. there exists a non-surjective injection $X \to X$;*

*vi. there exists a non-injective surjection $X \to X$.*

**Proof** (ii)⇔(iii) is immediate from Lemma 10.1.4.

(v)⇔(vi) is similar. Any non-surjective injection $f : X \to X$ has a retraction $g$ (by Lemma 5.5.3). Then $gf = \mathrm{id}_X$, so $g$ is surjective. If $g$ is also injective then $g$ is invertible, so $f = g^{-1}$, so $f$ is also invertible, contradicting the assumption that $f$ is not surjective. Hence $g$ is not injective. The converse is similar, using the axiom of choice instead of Lemma 5.5.3.

We now prove that (i)⇒(ii)⇒(iv)⇒(v)⇒(i).

(i)⇒(ii): assume (i). By the well ordering principle, we may give $X$ a well order. If $X \prec \omega$ then $X \cong \mathbf{n}$ for some $n \in \mathbb{N}$ (by Lemma 8.2.7), contradicting $X$ being infinite. So by Lemma 8.2.12, $\omega \preceq X$. In particular, there is an injection $\mathbb{N} \to X$, giving (ii).

(ii)⇒(iv): assume (ii). By Lemma 6.4.3, $X \cong Y + \mathbb{N}$ for some set $Y$. Then

$$X + \mathbf{1} \cong Y + \mathbb{N} + \mathbf{1} \cong Y + \mathbb{N} \cong X,$$

using Lemma 7.1.3 in the second isomorphism.

(iv)⇒(v): assuming (iv), there is a coproduct diagram

$$\mathbf{1} \xrightarrow{a} X \xleftarrow{j} X,$$

which is also a disjoint union diagram by Proposition 6.3.7. Then by definition of disjoint union diagram, the function $j : X \to X$ is injective with $a \notin \mathrm{im}\, j$.

(v)⇒(i): assume (v), and suppose for a contradiction that $X \cong \mathbf{n}$ for some $n \in \mathbb{N}$. Then there is a non-surjective injection $i : \mathbf{n} \to \mathbf{n}$. Since $i$ is not surjective,

$n > 0$, so $n = m + 1$ for some $m \in \mathbb{N}$. Thus, $i$ is a non-surjective injection $\mathbf{m+1} \to \mathbf{m+1}$.

Write the unique element of $\mathbf{1}$ as $\star$. Choose some element $y \in \mathbf{m+1}$ such that $y \notin \mathrm{im}(i)$. By Example 5.5.2, there is a bijection $f : \mathbf{m+1} \to \mathbf{m+1}$ that swaps $y$ with $\star$. Then $fi : \mathbf{m+1} \to \mathbf{m+1}$ is an injection such that $\star \notin \mathrm{im}(fi)$. Hence $fi$ corestricts to a function $j : \mathbf{m+1} \to \mathbf{m}$ (by Lemma 5.5.8), which is injective since $fi$ is. So $\mathbf{m+1} \leq \mathbf{m}$, and then by (10.1), $m + 1 \leq m$. This is the desired contradiction. □

**Exercise 10.1.6** Using Proposition 10.1.5, show that a set is infinite if and only if it is isomorphic to a proper subset of itself.

**Remark 10.1.7** Most people have the intuition that there are fewer even numbers than integers, since every even number is an integer but not every integer is even. And there would seem to be fewer perfect squares still, since the squares $n^2$ get sparser and sparser as $n$ increases. But from the set-theoretic point of view, the sets of integers, even integers and square integers are all isomorphic. The apparent paradox of a set being in one-to-one correspondence with a proper subset of itself is exactly what characterizes the infinite sets.

**Corollary 10.1.8** *Every subset of $\mathbb{N}$ is either isomorphic to $\mathbb{N}$ or finite.*

**Proof** Let $A \subseteq \mathbb{N}$. Then $A \leq \mathbb{N}$. If $A$ is infinite then by Proposition 10.1.5, $\mathbb{N} \leq A$, giving $A \cong \mathbb{N}$ by the Cantor–Bernstein theorem. □

**Digression 10.1.9** Corollary 10.1.8 completely classifies the sets $X$ such that $X \leq \mathbb{N}$. However, $\mathbb{N}$ is the largest familiar set for which this is possible. What I mean is that it is impossible for $\mathbf{2}^{\mathbb{N}}$ (which, as we will soon see, is isomorphic to $\mathbb{R}$). Our axioms do not determine whether there are any sets $X$ satisfying $\mathbb{N} < X < \mathbf{2}^{\mathbb{N}}$.

I mentioned this result back in Digression 1.1.1. The statement that there is no such intermediate set $X$ is called the 'continuum hypothesis', and it can neither be proved nor disproved from our axioms.

There's a certain mystique around this phenomenon, but it's really not so strange. For comparison, the abelian group property $xy = yx$ can neither be proved nor disproved from the group axioms, and all that means is that some groups are abelian and some aren't.

## 10.2 Countable and uncountable

Proposition 10.1.5(ii) tells us that the smallest infinite set is $\mathbb{N}$. The sets no bigger than $\mathbb{N}$ are of special interest.

**Definition 10.2.1** A set $X$ is **countable** if $X \leq \mathbb{N}$, and **uncountable** otherwise.

By Corollary 10.1.8, a set is countable if and only if it is either finite or isomorphic to $\mathbb{N}$.

**Warning 10.2.2** In particular, finite sets are countable. But beware that some authors don't call finite sets countable. (Presumably they don't call them uncountable either.) I believe they're in the minority these days; and surely finite sets are the easiest sets of all to count?

**Lemma 10.2.3** *A set $X$ is countable if and only if $X$ is empty or there exists a surjection $\mathbb{N} \to X$.*

**Proof** Follows immediately from Lemma 10.1.4. □

The existence of a surjection $f$ from $\mathbb{N}$ to our set is perhaps the most direct formalization of 'counting' its elements: we can list them as $f(0), f(1), \ldots$, and the whole set is covered that way.

**Corollary 10.2.4** *Let $X$ and $Y$ be sets, with $X$ countable. If there exists an injection $Y \to X$ or a surjection $X \to Y$, then $Y$ is also countable.*

**Proof** Follows from the definition and Lemma 10.2.3. □

One of the themes of this course is the resemblance between the algebra of sets and the algebra of natural numbers: $Z^{X+Y} \cong Z^X \times Z^Y$ and $z^{x+y} = z^x \cdot z^y$, and so on. In a sense, this chapter is all about results where the analogy breaks down, where the behaviour of sets and natural numbers is very different. To put it another way, it is about the essential differences between *finite* sets (which correspond to natural numbers) and *infinite* sets (which go beyond).

The fact that $\mathbb{N} \cong \mathbb{N} + \mathbf{1}$ already demonstrates this difference. There is no natural number $n$ such that $n = n + 1$; equivalently, there is no finite set $X$ such that $X \cong X + \mathbf{1}$. The next result also demonstrates the difference between finite and infinite.

**Proposition 10.2.5** $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$.

**Proof** Certainly $\mathbb{N} \leq \mathbb{N} \times \mathbb{N}$; for example, the diagonal function $n \mapsto (n, n)$ is an injection $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$. So by the Cantor–Bernstein theorem, it suffices to find an injection $i : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

As noted in Example 6.4.12, we can define $i$ by $i(m, n) = 2^m 3^n$, and if we assume uniqueness of prime factorization then it follows that $i$ is injective.

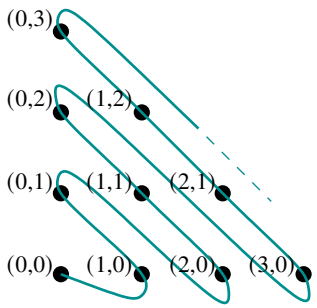



Figure 10.1: A bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$.

If we want to be very careful and use only results that we have proved in this course, we can take $i(m,n) = 2^{m+n} + n$. To show that $i$ is injective, first observe that for all $m, n \in \mathbb{N}$,

$$2^{m+n} \leq i(m,n) \leq 2^{m+n} + m + n < 2^{m+n} + 2^{m+n} = 2^{m+n+1},$$

where the strict inequality follows from Cantor's Theorem 6.4.4 (or an easy induction). Hence $m+n$ is the largest natural number $p$ such that $2^p \leq i(m,n)$. Thus, supposing that $i(m,n) = i(m',n')$, we have $m+n = m'+n'$. But then $2^{m+n} + n = 2^{m+n} + n'$, so $n = n'$ (using Lemma 7.1.22 on cancellation). Since $m+n = m'+n'$, it follows by cancelling again that $m = m'$. □

If you already knew that $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$, maybe you saw it explained using a picture like Figure 10.1. With a bit of work, we can figure out a formula for the bijection shown there. In one direction, it turns out to be

$$(m,n) \mapsto \tfrac{1}{2}(m+n)(m+n+1) + n.$$

With substantially more work, we can show that this function is a bijection.

*But all this work is unnecessary!* If all we want is the *existence* of a bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$, then actually *constructing* one is a really inefficient strategy. The same goes for any pair of sets. Almost always, the easiest way to show they're isomorphic is to prove inequalities in each direction and invoke the Cantor–Bernstein theorem.

**Example 10.2.6** The set $\mathbb{Z}$ of integers is countable. Indeed, $\mathbb{N} \times \mathbb{N}$ is countable by Proposition 10.2.5, and there is a surjection

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \to & \mathbb{Z} \\ (m,n) & \mapsto & m-n, \end{array}$$

so the result follows from Corollary 10.2.4.

To use Proposition 10.2.5 further, it is helpful to have the following lemma on how inequalities interact with products. While we're at it, let's also record some results on how inequalities interact with sums and powers.

**Lemma 10.2.7** *i. For all sets $X, X', Y, Y'$, if $X \leq X'$ and $Y \leq Y'$ then*

$$X + Y \leq X' + Y', \qquad X \times Y \leq X' \times Y'.$$

*ii. For all sets $X, X', Y$, if $X \leq X'$ then*

$$X^Y \leq X'^Y, \qquad Y^X \leq Y^{X'},$$

*the latter under the restriction that $Y$ is nonempty.*

**Proof** Both parts follow from Workshop 4, question 2. The statement on products also follows from Exercise 5.1.4. □

Now here are some consequences of the isomorphism $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$.

**Corollary 10.2.8** *Let $n \geq 1$. Let $X_1, \ldots, X_n$ be countable sets. Then $X_1 \times \cdots \times X_n$ is countable.*

**Proof** We prove this by induction on $n$. For $n = 1$, the product is $X_1$, which is certainly countable. Now take $n \in \mathbb{N}$ and sets $X_1, \ldots, X_n, X_{n+1}$. By inductive hypothesis, $X_1 \times \cdots \times X_n \leq \mathbb{N}$. Also, $X_{n+1} \leq \mathbb{N}$. Hence by Lemma 10.2.7 and Proposition 10.2.5,

$$X_1 \times \cdots \times X_n \times X_{n+1} \leq \mathbb{N} \times \mathbb{N} \cong \mathbb{N},$$

completing the induction. □

Given a set $X$, we define $X^n$ for each $n \in \mathbb{N}$ recursively as follows: $X^0 = \mathbf{1}$, and $X^{n+1} = X^n \times X$ ($n \in \mathbb{N}$). Thus, $X^1 \cong X$, $X^2 \cong X \times X$, and so on.

**Corollary 10.2.9** *Let $X$ be a countable set. Then $X^n$ is countable for all $n \geq 1$.* □

**Examples 10.2.10** i. The set $\mathbb{Q}$ of rational numbers is countable. Indeed, $\mathbb{Z}$ is countable by Example 10.2.6, so the subset $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ is also countable, which implies that $\mathbb{Z} \times \mathbb{Z}^*$ is countable too, by Corollary 10.2.8. Finally, there is a surjection

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z}^* & \to & \mathbb{Q} \\ (a, b) & \mapsto & a/b, \end{array}$$

so $\mathbb{Q}$ is countable by Corollary 10.2.4.

ii. For each $n \geq 0$, the set of polynomials over $\mathbb{Z}$ of degree $\leq n$ (that is, expressions of the form $a_0 + a_1 x + \cdots + a_n x^n$ where $a_i \in \mathbb{Z}$ and $x$ is a formal symbol) is countable. Indeed, this set is isomorphic to $\mathbb{Z}^{n+1}$, which is countable by Corollary 10.2.9.

We've seen that subsets and quotients of countable sets are countable, as are products of finitely many countable sets. A union of any countable family of countable subsets is countable too:

**Lemma 10.2.11** *Let $X$ be a set, and let $(A_i)_{i \in I}$ be a family of subsets of $X$. If $I$ is countable and $A_i$ is countable for each $i \in I$, then so too is $\bigcup_{i \in I} A_i$.*

**Proof** We may assume that each $A_i$ is nonempty. Then by Lemma 10.1.4 and the axiom of choice, we can choose a surjection $f_i \colon \mathbb{N} \to A_i$ for each $i \in I$. This means we can define a function

$$\begin{array}{ccc} \mathbb{N} \times I & \to & \bigcup_{i \in I} A_i \\ (n, i) & \mapsto & f_i(n), \end{array}$$

which is surjective since each $f_i$ is. Hence by Lemma 10.1.4 again, $\bigcup A_i \leq \mathbb{N} \times I$. But $\mathbb{N} \times I$ is countable by Corollary 10.2.8, so $\bigcup A_i$ is countable too. □

**Examples 10.2.12** i. We have already seen that $\mathbb{Z}$ is countable (Example 10.2.6), but here is another proof. Write $-\mathbb{N}$ for the subset $\{-n : n \in \mathbb{N}\} = \{0, -1, -2, \ldots\}$ of $\mathbb{Z}$. Then $-\mathbb{N} \cong \mathbb{N}$ via the bijection $-n \leftrightarrow n$. Now $\mathbb{Z} = -\mathbb{N} \cup \mathbb{N}$, which is the union of two countable sets and is therefore countable, by Lemma 10.2.11.

ii. For each $n \in \mathbb{N}$, the set of polynomials over $\mathbb{Z}$ of degree at most $n$ is countable (Example 10.2.10(ii)), so by Lemma 10.2.11, the set of *all* polynomials over $\mathbb{Z}$ is countable.

iii. Now let $P$ be the set of all polynomials over $\mathbb{Z}$ apart from the zero polynomial, which is countable by (ii). Let

$$\mathbb{A} = \{x \in \mathbb{R} : p(x) = 0 \text{ for some } p \in P\},$$

which is called the set of **algebraic numbers** (or more precisely, the set of real numbers algebraic over $\mathbb{Q}$). It is the union over all $p \in P$ of the set of real roots of $p$, and a nonzero polynomial has only finitely many real roots, so it is a countable union of finite sets. Hence the algebraic numbers are countable.

Every rational number $q = a/b$ is algebraic, since it is a root of the polynomial $bx - a$. So $\mathbb{Q} \subseteq \mathbb{A}$. But most algebraic numbers are not rational; consider, for example, $\sqrt{2}$ or $6 - \sqrt[10]{5/2 - \sqrt{1/3}}$.

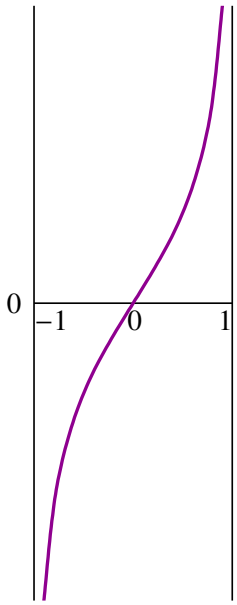



Figure 10.2: An isomorphism between the open interval $(-1, 1)$ and $\mathbb{R}$.

**Warning 10.2.13** A product of finitely many countable sets is countable (Corollary 10.2.8), and a union of countably many countable subsets of a set is countable (Lemma 10.2.11). But a product of *countably* many countable sets is *not* countable, in general. For example, the product

$$\mathbf{2} \times \mathbf{2} \times \cdots = \prod_{n \in \mathbb{N}} \mathbf{2} = \mathbf{2}^{\mathbb{N}}$$

is uncountable, by Cantor's Theorem 6.4.4.

We now turn our attention to the real line.

**Lemma 10.2.14** *$\mathbb{R}$ is isomorphic (as a set) to any real interval with more than one element.*

**Proof** First, $\mathbb{R}$ is isomorphic to the open interval $(-1, 1)$. This can be shown using any bijection $(-1, 1) \to \mathbb{R}$ of the shape shown in Figure 10.2, such as $x \mapsto 2x/(1 - x^2)$ or $x \mapsto \tan(\pi x/2)$. A little calculus shows that these are indeed bijections.

Now let $I$ be any real interval. Since $I \subseteq \mathbb{R}$, certainly $I \leq \mathbb{R}$. Hence by the Cantor–Bernstein theorem, it is enough to prove that $\mathbb{R} \leq I$.

By hypothesis, we can find $a, b \in I$ with $a < b$, and then the open interval $(a, b)$ is a subset of $I$. We can easily find a bijection $(a, b) \to (-1, 1)$ (for example,

one of the form $x \mapsto Cx + D$ for some $C, D \in \mathbb{R}$), so $(a, b) \cong (-1, 1)$. Hence

$$\mathbb{R} \cong (-1, 1) \cong (a, b) \leq I,$$

giving $\mathbb{R} \leq I$, as required. □

To find out more about the real line, we will use arguments involving base $B$ expansions, for various values of $B$. Care is needed over what we ten-fingered animals think of as the recurring 9s phenomenon: some real numbers have two different decimal expansions, such as

$$0.123999\ldots = 0.124000\ldots.$$

Similarly, some numbers have two different binary expansions, one ending in recurring 1s and the other in recurring 0s. This explains the use of base 3 in the following proof.

**Proposition 10.2.15** $\mathbb{R} \cong \mathbf{2}^{\mathbb{N}}$. *In particular,* $\mathbb{R}$ *is uncountable.*

**Proof** The second sentence follows from the first by Cantor's theorem. For the first, we prove inequalities in both directions, and the result will follow by the Cantor–Bernstein theorem.

To show that $\mathbf{2}^{\mathbb{N}} \leq \mathbb{R}$, write the elements of $\mathbf{2}$ as 0 and 1, and define $f\colon \mathbf{2}^{\mathbb{N}} \to \mathbb{R}$ by

$$f\big((a_n)_{n\in\mathbb{N}}\big) = \sum_{n=0}^{\infty} a_n 3^{-(n+1)}$$

($a_n \in \mathbf{2} = \{0, 1\}$). That is, $f$ maps a sequence $(a_n)$ of 0s and 1s to the real number with base 3 expansion $0.a_0a_1\ldots$. Then $f$ is injective, in brief because $0.a_0a_1\ldots$ never ends in recurring 2s. (The full proof involves a few lines of calculus, omitted here.)

To show that $\mathbb{R} \leq \mathbf{2}^{\mathbb{N}}$, first note that there is a surjection $g\colon \mathbf{2}^{\mathbb{N}} \to [0, 1]$ given by

$$g\big((a_n)_{n\in\mathbb{N}}\big) = \sum_{n=0}^{\infty} a_n 2^{-(n+1)}$$

($a_n \in \mathbf{2}$). That is, $g$ maps a sequence $(a_n)$ of 0s and 1s to the real number with binary expansion $0.a_0a_1\ldots$. It is surjective because every number in $[0, 1]$ has a binary expansion of this form. Hence $[0, 1] \leq \mathbf{2}^{\mathbb{N}}$, and so $\mathbb{R} \leq \mathbf{2}^{\mathbb{N}}$ by Lemma 10.2.14. □

**Exercise 10.2.16** In that proof, how would the argument that $\mathbf{2}^{\mathbb{N}} \leq \mathbb{R}$ go wrong if we used base 2 instead of base 3?

**Corollary 10.2.17** *A real interval with more than one element is uncountable.* □

**Digression 10.2.18** You may have seen a proof along the following lines that $\mathbb{R}$ is uncountable. Suppose we could list the real numbers as $x_1, x_2, \ldots$. For example, the list might look as follows, in base 3:

$$\begin{array}{c} 12021.102102\ldots \\ -21.122210\ldots \\ 120.010022\ldots \\ \vdots \end{array}$$

Now let $a$ be the real number with base 3 expansion $0.a_0a_1\ldots$, where $a_n$ is defined as follows: $a_n = 0$ if the $n$th digit after the 'decimal' point of $x_n$ is 1, and $a_n = 1$ otherwise. By comparing the $n$th digit of $a$ with the $n$th digit of $x_n$, and with a pause to consider the fact that a base 3 expression ending in a recurring 2 can also be expressed with a recurring 0, you can convince yourself that $a \neq x_n$. Hence $a \notin \{x_1, x_2, \ldots\}$, a contradiction. It follows that $\mathbb{R}$ is uncountable.

If you've seen this before, most likely it was in base 10. The choice of base doesn't matter, as long as it's at least 3 (since binary doesn't give us enough room for manoeuvre). But the point I want to make is that this argument—the **diagonal argument**—is essentially the same as the argument in the proof of Cantor's Theorem 6.4.4 in the case $X = \mathbb{N}$ (putting aside the complications caused by the 'recurring 9s' problem). There, we proved that there is no surjection from $\mathbb{N}$ to $\mathbf{2}^{\mathbb{N}}$, which is the set of infinite sequences of 0s and 1s. I leave it to you to figure out how the proof of Theorem 6.4.4 in the case $X = \mathbb{N}$ translates into the diagonal argument in the previous paragraph.

**Example 10.2.19** The set of algebraic real numbers is countable (Example 10.2.12(iii)), but $\mathbb{R}$ is not, so not every real number is algebraic.

A real number is said to be **transcendental** if it is not algebraic. We have just proved that the set of transcendental numbers is not empty, but now we'll show it's *uncountable*. Suppose for a contradiction that it is countable. Then $\mathbb{R}$, being the union of the algebraic numbers and the transcendental numbers, both of which are countable, must also be countable. (Here we are using Lemma 10.2.11.) This is a contradiction, so the set of transcendental numbers is uncountable after all.

In that sense, there are far more transcendental numbers than algebraic numbers. If you choose a real number at random (whatever that means), then it is

overwhelmingly likely to be transcendental, even though most of the numbers we deal with directly are algebraic.

**Digression 10.2.20** Proving that a given number is transcendental usually involves some difficult and delicate analysis. For instance, it takes some effort to show that $e$ is transcendental (or even irrational), and $\pi$ is harder still. The first number to be proved transcendental was one constructed specifically for the purpose, $\sum_{n=1}^{\infty} 10^{-n!}$, by Liouville in the mid-19th century.

In contrast, the set-theoretic proof of the existence of transcendental numbers is very quick indeed. It is often said that it is only an *existence* proof, and doesn't actually provide a specific transcendental number. This isn't quite right. By going through the argument above, one can extract a specific transcendental number, in the sense that one could write a computer program that would output its base 3 expansion digit after digit.

What is true is that our set-theoretic argument will never help you show that a *given* number is transcendental. You're not going to be able to use set theory to show that $\pi$ is transcendental, for example.

In fact, we know extraordinarily little about which numbers are transcendental, or even irrational. As a measure of humanity's vast ignorance, get this: for all we know, $\pi + e$ could be rational.

## 10.3 Sums and products

We're now going to think about coproducts $X + Y$ and products $X \times Y$ of sets $X$ and $Y$. For finite sets, these operations correspond to addition and multiplication of natural numbers (Proposition 7.1.14). But for infinite sets, we're in for a surprise: it turns out that $X + Y \cong X \times Y$! And more surprisingly still, $X + Y$ and $X \times Y$ are isomorphic to one of $X$ and $Y$, whichever is the larger.

**Warning 10.3.1** These results are quite different in character from isomorphisms we established earlier like $X \times (Y + Z) \cong (X \times Y) + (X \times Z)$ and $(X^Y)^Z \cong X^{Y \times Z}$. Those isomorphisms are *canonical*, meaning that there's an obvious or natural choice of bijection between the left- and right-hand sides. (This statement can be made precise with the category-theoretic notion of natural isomorphism.) But in the case of $X + Y \cong X \times Y$, there's no natural choice of bijection. We can just prove that one exists.

**Remark 10.3.2** In contexts where we're thinking about sets (or their isomorphism classes) as an extension of the natural number system, we usually say 'sum' rather

than 'coproduct', a synonym that was introduced in Definition 6.3.6 but has barely been used up to now.

The result from which everything else will follow is that $X \times X \cong X$ for all infinite sets $X$. As it's so important, I want to do two things before I show you the proof: first, convince you that it's plausible, and second, explain the strategy of the proof.

To see that it's plausible, let's begin by considering $X + X$ for infinite sets $X$. It's not too hard to see that $\mathbb{N} + \mathbb{N} \cong \mathbb{N}$: we have $\mathbb{N} + \mathbb{N} \cong \mathbf{2} \times \mathbb{N}$, and we can put $\mathbf{2} \times \mathbb{N}$ into bijection with $\mathbb{N}$ by listing its elements as

$$(0,0), (1,0), (0,1), (1,1), (0,2), (1,2), \ldots,$$

where $\mathbf{2} = \{0, 1\}$. (Alternatively, $\mathbf{2} \times \mathbb{N} \leq \mathbb{N} \times \mathbb{N} \cong \mathbb{N}$ and $\mathbb{N} \leq \mathbf{2} \times \mathbb{N}$, so $\mathbf{2} \times \mathbb{N} \cong \mathbb{N}$ by the Cantor–Bernstein theorem.) Also, $X + X \cong X$ if $X$ is an infinite power set: for if $X \cong \mathbf{2}^Y$ then $Y$ must be infinite too, and

$$X + X \cong \mathbf{2} \times X \cong \mathbf{2} \times \mathbf{2}^Y \cong \mathbf{2}^{Y+\mathbf{1}} \cong \mathbf{2}^Y \cong X,$$

using the fact that $Y \cong Y + \mathbf{1}$ (by Proposition 10.1.5). So, $X + X \cong X$ when $X$ is either $\mathbb{N}$ or an infinite power set. This suggests it might be true for all infinite sets.

**Exercise 10.3.3** We just used the fact that $X + X \cong \mathbf{2} \times X$ for all sets $X$. How exactly do we know that?

Now let's consider $X \times X$. We know that $X \times X \cong X$ when $X = \mathbb{N}$ (Proposition 10.2.5). And if $X$ is an infinite power set $\mathbf{2}^Y$ then

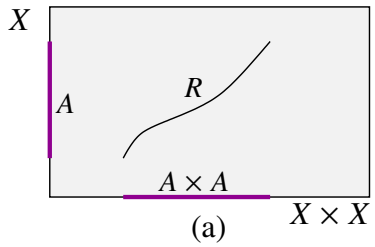
$$X \times X \cong \mathbf{2}^Y \times \mathbf{2}^Y \cong \mathbf{2}^{Y+Y} \cong \mathbf{2}^Y \cong X,$$

using the isomorphism $Y + Y \cong Y$. So it looks as if $X \times X \cong X$ when $X$ is either $\mathbb{N}$ or an infinite power set, again encouraging us to hope that it might be true for all infinite sets.

To prove that $X \times X \cong X$ actually *is* true for all infinite sets $X$, we use the following strategy. Somewhat like in the proof of cardinal comparability (Theorem 9.2.11), we are going to consider partial bijections between $X \times X$ and $X$—but only the ones where the actual bijection involved is of the form $A \times A \to A$ for some subset $A$ of $X$ (Figure 10.3).

The plan is to use Zorn's lemma on the ordered set of such partial bijections. A different way to view it: we take the ordered set whose elements are pairs $(A, f)$ where $A \subseteq X$ and $f : A \times A \to A$ is a bijection, and we define

$$(A, f) \leq (B, g) \iff A \subseteq B \text{ and } f = g|_{A \times A}.$$



(a)

Figure 10.3: A partial bijection $R$ between $X \times X$ and $X$, corresponding to a bijection between subsets $A \times A \subseteq X \times X$ and $A \subseteq X$.

(This is not exactly the formalism we will use, but it's equivalent.) Zorn's lemma will give us a maximal element $(M, h)$ of this ordered set. In other words, it's a partial bijection $h\colon M \times M \to M$, for some subset $M$ of $X$, that cannot be extended any further.

Based on previous uses of Zorn's lemma, you might hope that this maximal element would be an *actual* bijection between $X \times X$ and $X$. That is, you might expect that $M = X$, and the theorem would follow. But it's not quite that simple.

To see why not, consider $X = \mathbb{N}$. Write $\mathbb{N}^+ = \mathbb{N} \setminus \{0\} = \{1, 2, \ldots\}$. Since $\mathbb{N}^+ \cong \mathbb{N}$, we have $\mathbb{N}^+ \times \mathbb{N}^+ \cong \mathbb{N}^+$. Take any bijection $h\colon \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{N}^+$. I claim that $(\mathbb{N}^+, h)$ is maximal in our ordered set: we cannot extend it any further. Indeed, the only subset of $\mathbb{N}$ strictly containing $\mathbb{N}^+$ is $\mathbb{N}$ itself, but no bijection $h\colon \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{N}^+$ can be extended to a bijection $\bar{h}\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. For $\bar{h}$ would have to restrict to a bijection between the complement of $\mathbb{N}^+ \times \mathbb{N}^+$ in $\mathbb{N} \times \mathbb{N}$, which is the infinite set

$$\ldots, (2,0), (1,0), (0,0), (0,1), (0,2), \ldots,$$

and the complement of $\mathbb{N}^+$ in $\mathbb{N}$, which is the one-element set $\{0\}$. This is impossible.

So, it need not be the case that $M = X$. But all is not lost! As long as the sets $M$ and $X$ are *isomorphic*, we have

$$X \times X \cong M \times M \cong M \cong X,$$

which is all we need. In the example just given, the subset $\mathbb{N}^+$ of $\mathbb{N}$ is not the whole of $\mathbb{N}$, but there *is* an isomorphism of sets $\mathbb{N}^+ \cong \mathbb{N}$.

One more thing. For reasons you'll see, we're going to want the set $M$ to be infinite. We could *prove* that when $(M, h)$ is maximal, $M$ must be infinite. But it's actually easier to *force* $M$ to be infinite by using Corollary 9.2.9 of Zorn's lemma, in a sense you'll discover if you read on.

**Proposition 10.3.4** *$X \times X \cong X$ for every infinite set $X$.*

**Proof** *This proof is non-examinable.*

Let $P$ be the subset of $\mathscr{P}(X) \times \mathscr{P}((X \times X) \times X)$ consisting of pairs $(A, R)$ where $A \subseteq X$ and $R$ is a relation between $X \times X$ and $X$ such that

- $R \subseteq (A \times A) \times A$;
- for all $(a, b) \in A \times A$, there exists a unique $c \in A$ such that $(a, b)Rc$;
- for all $c \in A$, there exists a unique $(a, b) \in A \times A$ such that $(a, b)Rc$

(Figure 10.3). Thus, $R$ is the graph of a bijection from $A \times A$ to $A$, but regarded as a subset of $(X \times X) \times X$ rather than the smaller $(A \times A) \times A$. We define a relation $\leq$ on $P$ by

$$(A, R) \leq (B, S) \iff A \subseteq B \text{ and } R = S \cap ((A \times A) \times A).$$

It is easily checked that $\leq$ is an order on $P$.

We show that every chain $C$ in $P$ has an upper bound. Put

$$B = \bigcup_{(A,R)\in C} A, \quad S = \bigcup_{(A,R)\in C} R.$$

Then $(B, S)$ is an upper bound of $C$ in $P$ as long as it is actually an element of $P$. Let us check the three conditions above.

- $S \subseteq (B \times B) \times B$, since $R \subseteq (A \times A) \times A$ for all $(A, R) \in C$.
- Let $(a, b) \in B \times B$. We must prove there exists a unique $c \in B$ such that $(a, b)Sc$.

  *Existence:* $a \in B$, so $a \in A$ for some $(A, R) \in C$, and similarly, $b \in A'$ for some $(A', R') \in C$. Since $C$ is a chain, we may assume without loss of generality that $A' \subseteq A$. Then $(a, b) \in A \times A$. Since $(A, R) \in P$, there is a unique $c \in A$ such that $(a, b)Rc$. But $A \subseteq B$ and $R \subseteq S$, so $c \in B$ with $(a, b)Sc$.

  *Uniqueness:* suppose that $c, c' \in B$ with $(a, b)Sc$ and $(a, b)Sc'$. Then $(a, b)Rc$ for some $(A, R) \in C$, and similarly, $(a, b)R'c'$ for some $(A', R') \in C$. Since $C$ is a chain, we may assume without loss of generality that $(A', R') \leq (A, R)$. Then $A' \subseteq A$ and $R' \subseteq R$, so $(a, b)Rc$ and $(a, b)Rc'$. Since $(A, R) \in P$, it follows that $c = c'$.
- Let $c \in B$. We must show that there exists a unique $(a, b) \in B \times B$ such that $(a, b)Sc$.

  *Existence:* $c \in A$ for some $(A, R) \in C$, so $(a, b)Rc$ for some $(a, b) \in A \times A$. Then $(a, b)Sc$ with $(a, b) \in B \times B$.

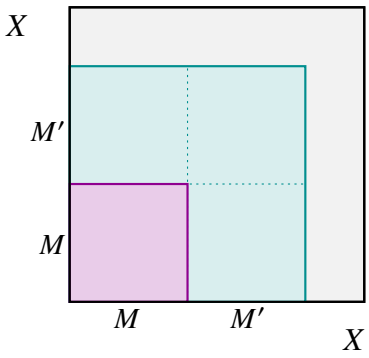



Figure 10.4: The argument that $M \cong X$ in the proof of Proposition 10.3.4.

> *Uniqueness:* suppose that $(a, b), (a', b') \in B \times B$ with $(a, b)Sc$ and $(a', b')Sc$. As in the previous uniqueness argument, there is some $(A, R) \in C$ such that $a, b, a', b', c \in A$ and $(a, b)Rc$ and $(a', b')Rc$. Since $(A, R) \in P$, this implies that $(a, b) = (a', b')$.

We have now shown that every chain in $P$ has an upper bound.

Since $X$ is infinite, there is an injection $\mathbb{N} \hookrightarrow X$ by Proposition 10.1.5. By Proposition 10.2.5, there is a bijection $k : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. The graph of $k$ is a subset of $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, which can be regarded, via the inclusion $\mathbb{N} \hookrightarrow X$, as a subset $Q$ of $(X \times X) \times X$. Then $(\mathbb{N}, Q) \in P$. So by Corollary 9.2.9 of Zorn's lemma, there is a maximal element $(M, T)$ of $P$ such that $(\mathbb{N}, Q) \leq (M, T)$. In particular, there is a maximal element $(M, T)$ of $P$ such that $M$ is infinite.

We now show that $X \setminus M < M$. Suppose for a contradiction that this is false. Then by cardinal comparability, $M \leq X \setminus M$, so $X$ has a subset $M'$ disjoint from $M$ but isomorphic to $M$. Write

$$L = \big((M \amalg M') \times (M \amalg M')\big) \setminus (M \times M)$$

(corresponding to the blue L shape in Figure 10.4). Then

$$\begin{aligned} L &= (M \times M') \amalg (M' \times M) \amalg (M' \times M') \\ &\cong (M \times M) + (M \times M) + (M \times M) \\ &\cong M + M + M \cong \mathbf{3} \times M \\ &\leq M \times M \cong M, \end{aligned}$$

using the fact that $M \times M \cong M$. So $L \leq M$, but also $M \leq M \times M' \leq L$, so $L \cong M$ by Cantor–Bernstein. Hence $L \cong M'$. Choose a bijection $j : L \to M'$. Writing $h : M \times M \to M$ for the bijection with graph $T$, we can extend $h$ to a bijection

$$\bar{h} : (M \amalg M') \times (M \amalg M') \to M \amalg M'$$

by defining

$$\bar{h}(x,y) = \begin{cases} h(x,y) & \text{if } (x,y) \in M \times M, \\ j(x,y) & \text{if } (x,y) \in L \end{cases}$$

($x, y \in M \amalg M'$). Then $(M \amalg M', \Gamma_{\bar{h}})$ is an element of $P$ strictly greater than $(M,T)$, contradicting the maximality of $(M,T)$.

Hence $X \setminus M < M$. It follows that

$$X \cong M + (X \setminus M) \leq M + M \cong \mathbf{2} \times M \leq M \times M \cong M,$$

so $X \leq M$. But also $M \subseteq X$, so $M \leq X$, giving $X \cong M$ by Cantor–Bernstein. Since $M \times M \cong M$, we have $X \times X \cong X$, as required. □

**Corollary 10.3.5** *$X^n \cong X$ for every infinite set $X$ and integer $n \geq 1$.* □

**Example 10.3.6** $\mathbb{R}^n$ and $\mathbb{R}$ are isomorphic as sets for all integers $n \geq 1$. For example, $\mathbb{C}$ and $\mathbb{R}$ are isomorphic as sets, since $\mathbb{C} \cong \mathbb{R}^2$.

(In fact, $\mathbb{R}^n$ and $\mathbb{R}$ are even isomorphic as additive groups! A question on Workshop 5 leads you through a proof.)

For sets $X$ and $Y$, define

$$\max(X,Y) = \begin{cases} X & \text{if } X \geq Y, \\ Y & \text{if } Y \geq X. \end{cases}$$

**Exercise 10.3.7** Which previous theorems are needed in order to guarantee that the definition of $\max(X,Y)$ is logically valid?

**Warning 10.3.8** Like everything else in this course, the max construction is isomorphism-invariant: if $X \cong X'$ and $Y \cong Y'$ then $\max(X,Y) \cong \max(X',Y')$. However, unlike the product and sum constructions, it is not 'functorial'.

What this means is that given functions $f\colon X \to X'$ and $g\colon Y \to Y'$, there is a canonical way of constructing a function $X \times Y \to X' \times Y'$ (namely, $f \times g$) and also a canonical way of constructing a function $X+Y \to X'+Y'$ (which could reasonably be called $f+g$), but there is no canonical way of constructing a function $\max(X,Y) \to \max(X',Y')$.

We come now to the crowning result of the course.

**Theorem 10.3.9** *Let $X$ and $Y$ be nonempty sets, at least one of which is infinite. Then*

$$X \times Y \cong X + Y \cong \max(X, Y).$$

**Proof** By cardinal comparability, we may assume without loss of generality that $X \geq Y$. In particular, $X$ is infinite. We have to prove that $X \times Y \cong X$ and $X + Y \cong X$.

For the result on products,

$$X \times Y \leq X \times X \cong X$$

by Proposition 10.3.4, but also

$$X \cong X \times \mathbf{1} \leq X \times Y$$

since $Y$ is nonempty. Hence by the Cantor–Bernstein theorem, $X \times Y \cong X$.

For the result on sums,

$$X + Y \leq X + X \cong \mathbf{2} \times X \leq X \times X \cong X$$

by Proposition 10.3.4 again, but also $X \leq X + Y$. Hence by Cantor–Bernstein again, $X + Y \cong X$. □

**Digression 10.3.10** Why did we do all that stuff on well ordered sets? Mostly in order to prove the Hartogs theorem. Why did we want the Hartogs theorem? Mostly in order to prove Proposition 8.4.3 on upper bounds of chains, which in turn we wanted in order to prove Zorn's lemma. And why did we want Zorn's lemma? Because it has lots of uses in mathematics, but specifically, because it allows us to prove this fundamental fact: the sum, product and maximum of two infinite sets are all isomorphic.

**Examples 10.3.11**

i. The product $\mathbb{R} \times \mathbb{N}$ and sum $\mathbb{R} + \mathbb{N}$ are both isomorphic to $\mathbb{R}$, or equivalently to $\mathbf{2}^{\mathbb{N}} = \mathscr{P}(\mathbb{N})$.

ii. Any cuboid $[a_1, b_1] \times \cdots \times [a_n, b_n] \subseteq \mathbb{R}^n$ is isomorphic as a set to $\mathbb{R}$, assuming that $n \geq 1$ and $a_i < b_i$ for each $i$. This follows by induction from Lemma 10.2.14 and Theorem 10.3.9.

iii. For any infinite set $X$ and finite sets $A_0, A_1, \ldots, A_n$ (where $n \in \mathbb{N}$), the set

$$A_0 + (A_1 \times X) + (A_2 \times X^2) + \cdots + (A_n \times X^n)$$

is isomorphic to $X$, assuming that $A_1, \ldots, A_n$ are not all empty. This follows from Theorem 10.3.9 by induction.

iv. Lemma 10.2.14 states that $\mathbb{R}$ is isomorphic to any nontrivial real interval, and the proof I gave involved a function like $x \mapsto 2x/(1-x^2)$ or $x \mapsto \tan(\pi x/2)$ and, implicitly, some calculus that we didn't actually do. Here's an alternative proof that doesn't require any calculus.

Much as in the proof of Lemma 10.2.14, it is enough to prove that $\mathbb{R} \cong [0,1]$. There is a surjection

$$\begin{array}{ccc} \mathbb{Z} \times [0,1] & \to & \mathbb{R} \\ (a,x) & \mapsto & a+x, \end{array}$$

so $\mathbb{R} \leq \mathbb{Z} \times [0,1]$. Now $\mathbb{Z} \times [0,1] \cong \max(\mathbb{Z}, [0,1])$ by Theorem 10.3.9, so $\mathbb{R} \leq \max(\mathbb{Z}, [0,1])$. But $\mathbb{R}$ is uncountable, by the first part of the proof of Proposition 10.2.15 (which does not use Lemma 10.2.14), so $\mathbb{Z} < \mathbb{R}$. Since $\mathbb{R} \leq \max(\mathbb{Z}, [0,1])$, the only possibility is that $\mathbb{R} \leq [0,1]$. And $[0,1] \leq \mathbb{R}$, so $[0,1] \cong \mathbb{R}$, as required.

**Remark 10.3.12** I've mentioned a few times that sets can be seen as part of the large mathematical family of sets-with-structure (groups, rings, fields, vector spaces, topological spaces, metric spaces, measure spaces, ...). They're just the extreme case where there's no structure at all. However, the way language has evolved means that mathematicians tend to use different phrasing for sets than for groups, rings, etc.

For example, a typical statement about groups is 'the rotation group of a regular dodecahedron is $A_5$'. Here, 'is' means 'is isomorphic to', and the role played by $A_5$ is that it's a standard group that everyone's supposed to know. If we used language about sets in the same way, we'd say 'the set of polynomials over $\mathbb{Z}$ is $\mathbb{N}$' (Example 10.2.12(ii)).

But that's not how mathematicians actually express themselves. A more normal way to put it would be 'the set of polynomials over $\mathbb{Z}$ has the same cardinality as $\mathbb{N}$'. As explained in Digression 2.2.10, 'has the same cardinality as' is a synonym of 'is isomorphic to'. You can interpret the word 'cardinality' as 'isomorphism type'. But the *most* common way to phrase it would be 'the set of polynomials over $\mathbb{Z}$ has cardinality $\aleph_0$.'

Let me explain what this means. The symbol $\aleph$ is aleph, the first letter of the Hebrew alphabet, and $\aleph_0$ means the isomorphism class of $\mathbb{N}$. In our approach, where everything is isomorphism-invariant, there's really no difference between a set and its isomorphism class, so basically $\aleph_0$ *is* $\mathbb{N}$ (but very emphatically considered up to isomorphism). Like the group $A_5$ in the example above, or like when you say that something is 5cm long, to say that something has cardinality $\aleph_0$ is a way of comparing it with a standard object.

Of course, some sets have cardinalities other than $\aleph_0$! For instance, since $\mathbb{R} \cong \mathbf{2}^{\mathbb{N}}$, one says that $\mathbb{R}$ has cardinality $2^{\aleph_0}$. (This is just different language for the

same thing.) There are also definitions of $\aleph_1$, $\aleph_2$, etc., and even $\aleph_W$ for any well ordered set $W$, but they're not part of this course.

(Personally, I'd argue that the difference in language between sets and other kinds of sets-with-structure is largely an accident of history, and that it doesn't have to be that way. But no matter: it's important that you know how, in practice, mathematicians actually *do* use language.)

**Example 10.3.13** Let $V$ be an infinite-dimensional vector space over an infinite field $K$. By Example 9.2.7(i), we can choose a basis $B$ for $V$. What is the cardinality of $V$ in terms of the cardinalities of $K$ and $B$? In other words, can we determine $V$ as a set (up to isomorphism), in terms of the sets $K$ and $B$?

Every element of $V$ is a finite $K$-linear combination of elements of $B$, say $\alpha_1 b_1 + \cdots + \alpha_n b_n$ with $\alpha_i \in K$ and $b_i \in B$. For each $n \in \mathbb{N}$, the number of such expressions is

$$(K \times B)^n \cong \max(K, B)^n \cong \max(K, B),$$

by Theorem 10.3.9 and Corollary 10.3.5. Now allowing $n$ to vary over $\mathbb{N}$, it follows that

$$V \leq \mathbb{N} \times \max(K, B) \cong \max(\mathbb{N}, K, B) \cong \max(K, B). \tag{10.2}$$

(This is an inequality rather than an isomorphism because there is some redundancy, arising from coefficients of 0 as well as repetition and reordering of basis elements.) On the other hand, since $V$ is nontrivial, it has a one-dimensional subspace, which is in bijection with $K$; hence $K \leq V$. And since $B \subseteq V$, we also have $B \leq V$. Thus, $\max(K, B) \leq V$. Together with (10.2), this implies that $V$ is isomorphic as a set to $\max(K, B)$. Or in more standard mathematical language, the cardinality of $V$ is the maximum of the cardinalities of $K$ and $B$.

## 10.4 Powers and beyond

We saw in the last section that addition and multiplication of infinite sets is, in a sense, rather trivial: they both reduce to the simple operation of taking the maximum. Powers turn out to be much more subtle, and we will only dip our toes in.

By a **power** I mean an expression like $Y^X$. This is, of course, a function set, but from the viewpoint of cardinal arithmetic it is more natural to call it a power, just as we're now calling $X + Y$ a sum rather than a coproduct. In the expression $Y^X$, we call $Y$ the **base** and $X$ the **exponent**.

We begin with finite powers. Given a set $X$ and a natural number $n$, we can consider, on the one hand, the set $\mathbf{n} = \{0, \ldots, n-1\}$ and the power (function set) $X^{\mathbf{n}}$, or, on the other, the product $X^n = X \times \cdots \times X$ defined before Corollary 10.2.9. They're the same:

**Lemma 10.4.1** *Let $X$ be a set. Then $X^{\mathbf{n}} \cong X^n$ for all $n \in \mathbb{N}$.*

**Proof** We prove this by induction on $n$. For $n = 0$,

$$X^{\mathbf{0}} \cong X^{\varnothing} \cong \mathbf{1} \cong X^0.$$

For the inductive step, assuming the result for $n$,

$$X^{\mathbf{n+1}} \cong X^{\mathbf{n}} \times X^{\mathbf{1}} \cong X^{\mathbf{n}} \times X \cong X^n \times X \cong X^{n+1},$$

completing the induction. In both parts of the proof, we have used Proposition 6.3.13(iii). □

**Proposition 10.4.2** *$X^A \cong X$ for all infinite sets $X$ and finite nonempty sets $A$.*

**Proof** This follows from Corollary 10.3.5 and Lemma 10.4.1. □

So, powers of infinite sets are easy when the exponent is finite.

Another easy case is when the base is a power set. To compute $Y^X$ when $Y \cong \mathbf{2}^Z$ for some set $Z$, we simply apply Theorem 10.3.9:

$$Y^X \cong (\mathbf{2}^Z)^X \cong \mathbf{2}^{X \times Z} \cong \mathbf{2}^{\max(X,Z)}.$$

**Example 10.4.3** What is the cardinality of the set of real sequences?

Our task is to find $\mathbb{R}^{\mathbb{N}}$. By Proposition 10.2.15, $\mathbb{R}$ is the power set $\mathbf{2}^{\mathbb{N}}$, so

$$\mathbb{R}^{\mathbb{N}} \cong (\mathbf{2}^{\mathbb{N}})^{\mathbb{N}} \cong \mathbf{2}^{\mathbb{N} \times \mathbb{N}} \cong \mathbf{2}^{\mathbb{N}}.$$

Hence $\mathbb{R}^{\mathbb{N}} \cong \mathbf{2}^{\mathbb{N}}$—or equivalently, if you prefer, $\mathbb{R}^{\mathbb{N}} \cong \mathbb{R}$. There are no more sequences in $\mathbb{R}$ than there are elements of $\mathbb{R}$.

**Warning 10.4.4** You've already seen that $\mathbb{R} + \mathbb{N} \cong \mathbb{R}$ and $\mathbb{R} \times \mathbb{N} \cong \mathbb{R}$, both of which are true because $\mathbb{R} \geq \mathbb{N}$. And you've just seen that $\mathbb{R}^{\mathbb{N}} \cong \mathbb{R}$. So it would be natural to guess that $Y^X \cong Y$ whenever $Y \geq X$ (and both are infinite).

This is false. For example, it fails when $Y = X$: as we'll see in a moment, $X^X$ is *never* isomorphic to $X$. Even if $Y > X$, it can't be proved from our axioms that $Y^X \cong Y$, as discussed later in this section.

Another easy case is where the power is top-heavy: the exponent is bigger than or equal to the base.

**Lemma 10.4.5** *Let $X$ and $Y$ be sets, with $X$ infinite and $X \geq Y \geq \mathbf{2}$. Then $Y^X \cong \mathbf{2}^X$. In particular, $X^X \cong \mathbf{2}^X$ for all infinite sets $X$.*

**Proof** Since $\mathbf{2} \leq Y$, it follows from Lemma 10.2.7 that $\mathbf{2}^X \leq Y^X$. On the other hand,

$$Y^X \leq X^X \leq (\mathbf{2}^X)^X \cong \mathbf{2}^{X \times X} \cong \mathbf{2}^X,$$

since $X$ is infinite. So by the Cantor–Bernstein theorem, $Y^X \cong \mathbf{2}^X$. □

**Examples 10.4.6** i. The set $\mathbb{N}^{\mathbb{N}}$ of sequences of natural numbers is isomorphic to the set $\mathbf{2}^{\mathbb{N}}$ of subsets of the natural numbers.

ii. The set $\mathbb{R}^{\mathbb{R}}$ of functions $\mathbb{R} \to \mathbb{R}$ is isomorphic to $\mathbf{2}^{\mathbb{R}}$, or equivalently to $\mathbf{2}^{\mathbf{2}^{\mathbb{N}}}$.

It's actually quite rare that we want to consider *all* functions $\mathbb{R} \to \mathbb{R}$. More often, we impose some constraint such as continuity, differentiability, linearity, etc., as in the next two examples.

iii. How many continuous functions $\mathbb{R} \to \mathbb{R}$ are there? Write $\mathrm{Cts}(\mathbb{R}, \mathbb{R})$ for the set of continuous functions $\mathbb{R} \to \mathbb{R}$. Two continuous functions on $\mathbb{R}$ that are equal on $\mathbb{Q}$ are equal everywhere, so the function

$$\begin{array}{ccc} \mathrm{Cts}(\mathbb{R}, \mathbb{R}) & \to & \mathbb{R}^{\mathbb{Q}} \\ f & \mapsto & f|_{\mathbb{Q}} \end{array}$$

is injective. Hence

$$\mathrm{Cts}(\mathbb{R}, \mathbb{R}) \leq \mathbb{R}^{\mathbb{Q}} \cong \mathbb{R}^{\mathbb{N}} \cong \mathbb{R},$$

using Examples 10.2.10(i) and 10.4.3. So $\mathrm{Cts}(\mathbb{R}, \mathbb{R}) \leq \mathbb{R}$. But $\mathbb{R} \leq \mathrm{Cts}(\mathbb{R}, \mathbb{R})$ too (consider constant functions), giving $\mathrm{Cts}(\mathbb{R}, \mathbb{R}) \cong \mathbb{R} \cong \mathbf{2}^{\mathbb{N}}$ by Cantor–Bernstein.

Thus, the cardinality of the set of *all* functions from $\mathbb{R}$ to $\mathbb{R}$ is $\mathbf{2}^{\mathbf{2}^{\mathbb{N}}}$, but if we restrict to just the *continuous* ones then it's only $\mathbf{2}^{\mathbb{N}}$.

iv. For integers $n, m \geq 1$, what is the cardinality of the set $\mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m)$ of linear maps $\mathbb{R}^n \to \mathbb{R}^m$? As you learned long ago, the linear maps $\mathbb{R}^n \to \mathbb{R}^m$ are in bijection with the $m \times n$ real matrices. Hence

$$\mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m) \cong \{m \times n \text{ real matrices}\} \cong \mathbb{R}^{mn} \cong \mathbb{R},$$

using Example 10.3.6 in the last step.

Top-heavy powers are easy, but bottom-heavy powers are much harder. Here's the situation. Suppose we have infinite sets $X$ and $Y$ with $X < Y$. Then

$$Y \leq Y^X \leq \mathbf{2}^Y, \tag{10.3}$$

where the second inequality holds because

$$Y^X \leq (\mathbf{2}^Y)^X \cong \mathbf{2}^{X\times Y} \cong \mathbf{2}^Y, \tag{10.4}$$

using $X < Y$ and Theorem 10.3.9. The inequalities (10.3) say that $Y^X$ could perhaps be $Y$, it could perhaps be $\mathbf{2}^Y$, or it could perhaps be somewhere in between.

There are some situations where we can be more specific about the value of $Y^X$. As we've seen, one such situation is where $Y$ is a power set, and there are others that I won't go into here. But in general, it is hard to say more. Understanding the behaviour of powers is one of the most challenging aspects of cardinal arithmetic.

**Exercise 10.4.7** Part of the calculation (10.4) was that $Y^X \leq \mathbf{2}^{X\times Y}$. One can also deduce this from Theorem 5.2.4. How?

*The rest of this section is optional and non-examinable.*

We saw in the last section that sums and products of infinite sets are easy, and in this section that powers can be harder. Another more difficult operation is taking the sum or product of not just *two* sets, but *infinitely many* sets.

What I mean is the following. Take a family of sets $X \xrightarrow{p} I$, written, as usual, as $(X_i)_{i\in I}$. We have seen how to form their product $\prod_{i\in I} X_i$ (Section 9.1). We can also form their **sum** $\sum_{i\in I} X_i$, which is just alternative notation for the set $X$ itself, justified by the fact that each element of $X$ lies in exactly one of the sets $X_i$ (namely, $X_{p(x)}$).

How do sums and products compare? The sum of two infinite sets is isomorphic to their product, but what about the sum and product of infinitely many infinite sets? Are they isomorphic too?

In general, they're not. For example, a power $Y^I$ is a special case of a product of infinitely many sets: it's $\prod_{i\in I} Y$ (Example 9.1.2(ii)). But the sum $\sum_{i\in I} Y$ is $I \times Y$, and in general, $I \times Y < Y^I$. Consider, for instance, $I = Y = \mathbb{N}$.

The fundamental result on sums and products of arbitrarily many sets is König's theorem.

**Theorem 10.4.8 (König)** *Let $(X_i)_{i\in I}$ and $(Y_i)_{i\in I}$ be families of sets indexed over the same set $I$. If $X_i < Y_i$ for all $i \in I$ then $\sum_{i\in I} X_i < \prod_{i\in I} Y_i$.*

The proof is omitted, but it's quite like the proof of Cantor's theorem. In fact, Cantor's theorem is the very special case of König's theorem where $X_i = \mathbf{1}$ and $Y_i = \mathbf{2}$ for all $i \in I$.

**Exercise 10.4.9** What does König's theorem say in the case where $X_i = \varnothing$ for all $i$? Where have you seen this before?

Here's a typical use of König's theorem.

**Corollary 10.4.10** *Let $I$ be an infinite set and $p\colon \mathbf{2}^I \to I$ a function. Then there is some $i \in I$ such that $p^{-1}(i) \cong \mathbf{2}^I$.*

In other words, the fibres of a function $\mathbf{2}^I \to I$ cannot all be strictly smaller than $\mathbf{2}^I$. Cantor's theorem says that no function $\mathbf{2}^I \to I$ can be injective, or equivalently, that at least one fibre has at least two elements. This is the much stronger result that at least one fibre is as big as $\mathbf{2}^I$.

**Proof** Write $X_i = p^{-1}(i)$, and suppose for a contradiction that $X_i < \mathbf{2}^I$ for all $i \in I$. Applying König's theorem with $Y_i = \mathbf{2}^I$ for all $i \in I$, we get

$$\mathbf{2}^I \cong \sum_{i\in I} X_i < \prod_{i\in I} \mathbf{2}^I \cong (\mathbf{2}^I)^I \cong \mathbf{2}^{I\times I} \cong \mathbf{2}^I,$$

a contradiction. Hence $X_i \geq \mathbf{2}^I$ for some $i \in I$, which since $X_i \subseteq \mathbf{2}^I$ implies that $X_i \cong \mathbf{2}^I$. □

Now zooming out and thinking about cardinal arithmetic more generally, here are some questions we might ask ourselves.

- Is there any set bigger than all of $\mathbb{N}, \mathbf{2}^{\mathbb{N}}, \mathbf{2}^{\mathbf{2}^{\mathbb{N}}}, \ldots$?
- Is there any uncountable set $X$ with the property that

  $$Y < X \implies \mathbf{2}^Y < X$$

  for all sets $Y$? For comparison, $Y < \mathbb{N} \implies \mathbf{2}^Y < \mathbb{N}$ (that is, if $Y$ is finite then so is $\mathbf{2}^Y$), but of course $\mathbb{N}$ is countable. Power sets $X$ never have the property above, as if $X \cong \mathbf{2}^Z$ then $Z < X$ but $\mathbf{2}^Z \not< X$. So none of the sets listed in the previous bullet point has this property.
- Is it possible to find an infinite set $X$ and a function $p\colon X \to I$ such that $I < X$ and $p^{-1}(i) < X$ for all $i \in I$? Equivalently, is there a family $(X_i)_{i\in I}$ of sets such that $\sum X_i$ is infinite and all the summands, as well as the indexing set $I$, are strictly smaller than $\sum X_i$?

  Sets $X$ with this property are called **singular**. For example, $\mathbb{N}$ is not singular (it is **regular**), because it cannot be written as a disjoint union of a finite number of finite sets: a finite sum of finite sets is finite.

- Do there exist an infinite set $Y$ and a set $X < Y$ such that $Y^X > Y$? We haven't seen any examples, but I mentioned the possibility just before Exercise 10.4.7. It can be shown that if there is some set larger than all of $\mathbb{N}, \mathbf{2}^{\mathbb{N}}, \mathbf{2}^{\mathbf{2}^{\mathbb{N}}}, \ldots$ (as in the first bullet point), then such sets $X$ and $Y$ do exist.

- For an infinite set $X$, are there any sets $Y$ such that $X < Y < \mathbf{2}^X$? The statement that there are no such sets $Y$ is called the **generalized continuum hypothesis**, the case $X = \mathbb{N}$ being the (ordinary) continuum hypothesis mentioned in Digression 1.1.1.

  Here is another way to look at it. Let $X$ be a set. Cantor's theorem tells us that $\mathbf{2}^X > X$. Theorem 9.3.4 tells us that every nonempty family of sets has a least element. With a bit of thought, these two results together imply that there is a smallest set $X^+$ strictly larger than $X$. That is, $X^+ > X$, and for every set $Y$, if $Y > X$ then $Y \geq X^+$.

  So we now have two ways of enlarging a set $X$: take its power set $\mathbf{2}^X$ or its successor set $X^+$. The generalized continuum hypothesis says that when $X$ is infinite, they're the same. If it's true, then life becomes much simpler.

What these questions have in common is that none of them can be settled on the basis of our axioms. In other words, none of these statements can be proved from our axioms—but none can be disproved either. (Here I'm assuming that our axioms are consistent, meaning that they don't lead to a contradiction. If they're inconsistent then you can prove anything.) Showing this would take us far, far beyond this course. It is the theme of incompleteness mentioned in Digression 1.1.1.

The system of axioms that we have used in this course is powerful. Most mathematicians will never need more. For example, it has been argued that everything needed to prove Fermat's last theorem (tens of thousands of pages, all told) follows from these axioms.

However, other axiom systems are stronger still, and one such system is ZFC (outlined in Section 1.9). We can add to our axiom system an eleventh axiom, called **replacement**, which roughly speaking says the following. Suppose we have a set $I$ and a logical expression that, for each $i \in I$, specifies a set $X_i$ up to isomorphism. Then the axiom states that there exist a set $X$ and a function $p\colon X \to I$ such that $p^{-1}(i) \cong X_i$ for all $i \in I$. More roughly still, replacement says that any family of sets you can describe in ordinary language is a family of sets in the sense of Definition 6.5.4. Once this eleventh axiom is added, our axiom system becomes equivalent to ZFC: a theorem can be proved in one system if and only if it can be proved in the other.

Another way we might consider strengthening our system is by adding new axioms of the type that traditionally go by the name of 'large cardinal' axioms, but

in our isomorphism-invariant approach would better be called 'large set' axioms. Here 'large set' is an informal term for a set that is too large for its existence to be guaranteed by the existing axioms, and a 'large set axiom' is an axiom guaranteeing that it *does* exist.

For example, I mentioned that our axioms don't imply the existence of any set larger than all of $\mathbb{N}, \mathbf{2}^{\mathbb{N}}, \mathbf{2}^{\mathbf{2}^{\mathbb{N}}}, \ldots$. We can add an axiom requiring that such a set does exist. This is a very mild large set axiom. Far, far stronger ones are often discussed.

(It has been joked that set theory is really set theory theory. That is, what set theorists are mostly concerned with is not sets, but set *theories*: the study of what happens when you change the axiom system.)

In the other direction, we can fruitfully consider *weakening* our axiom system. A big selling point of the axioms we've used is that each of them has a life outside set theory. I expanded on this point in Digression 1.4.1, mentioning that a certain subset of our ten axioms characterizes the important class of categories known as toposes, the most prominent examples of which arise in topology and algebraic geometry. A different subset of the axioms characterizes the cartesian closed categories, which are closely related to both the $\lambda$-calculus (a classical topic in logic) and functional programming. Other subsets of the axioms correspond to other important classes of categories, which have interest and applications in different parts of mathematics far away from set theory.

If you're interested in this kind of thing and you're still here next year, you'll probably enjoy the Category Theory course. But for this course on sets, we have reached the end of the road.

* * *