Rational points on varieties

Bjorn Poonen

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: `poonen@math.mit.edu`

URL: `http://math.mit.edu/~poonen/`

Unofficial version for incidental online use

2010 *Mathematics Subject Classification.* Primary 14G05; Secondary 11G35

Key words and phrases. Rational points, descent, étale cohomology, torsors, Brauer–Manin obstruction, descent obstruction

Unofficial version for incidental online use

© 2017 by the American Mathematical Society.
If your use of this book is more than incidental,
please purchase the official print or electronic version.

MathSciNet contains a review of this book,
as well as BibTeX and AMSRefs code for citing this book.

Click here for the errata list.

Contents

Unofficial version for incidental online use

Unofficial version for incidental online use

Unofficial version for incidental online use

Unofficial version for incidental online use

Preface

0.1. Prerequisites

A person interested in reading this book should have the following background:

- Algebraic geometry (e.g., [**Har77**]: up to Chapter II, §8 as a minimum, but familiarity with later chapters is also needed at times)—this is not needed so much in our Chapter 1.
- Algebraic number theory (e.g., [**Cas67**, **Frö67**] or [**Lan94**, Part One] or [**Neu99**, Chapters I and II]).
- Some group cohomology (e.g., [**AW67**] or [**Mil13**, Chapter 2]).

0.2. What kind of book this is

The literature on rational points is vast. To write a book on the subject, an author must

1. write thousands of pages to cover all the topics comprehensively, or
2. focus on one aspect of the subject, or
3. write an extended survey serving as an introduction to many topics, with pointers to the literature for those who want to learn more about any particular one.

Our approach is closest to 3, so as to bring newcomers quickly up to speed while also providing more experienced researchers with directions for further exploration.

This book originated as the lecture notes for a semester-long course, taught during spring 2003 at the University of California, Berkeley, and fall

Unofficial version for incidental online use

2008 and fall 2013 at the Massachusetts Institute of Technology. But it has grown since then; probably now it is about 50% too large for a single semester, unless students are willing to read much of it outside of class.

0.3. The nominal goal

Many techniques have been used to decide whether a variety over a number field has a rational point. Some generalize Fermat's method of infinite descent, some use quadratic reciprocity, and others appear at first sight to be ad hoc. But over the past few decades, it was discovered that nearly all of these techniques could be understood as applications of just two cohomological obstructions, the étale-Brauer obstruction and the descent obstruction. Moreover, while this book was being written, it was proved that the étale-Brauer obstruction and the descent obstruction are equivalent! The topics in this book build up to an explanation of this "grand unified theory" of obstructions.

0.4. The true goal

Our ulterior motive, however, is to introduce readers to techniques that they are likely to need while researching arithmetic geometry more broadly. Along the way, we mention open problems and applications that are interesting in their own right.

0.5. The content

Chapter 1 introduces fields of special interest to arithmetic geometers, and it discusses properties and invariants (the C_r property, cohomological dimension, and the Brauer group) that control the answers to some arithmetic questions about fields in general. Not all of Chapter 1 is needed in future chapters, but the Brauer group plays a key role later on (in Chapters 6 and 8).

Chapter 2 discusses aspects of varieties with particular attention to the case of ground fields that are not algebraically closed. Ultimately, we aim to treat global fields of positive characteristic as well as number fields, so we do not require our ground field to be perfect. Among other topics, this chapter discusses properties of varieties under base extension (e.g., irreducible vs. geometrically irreducible), the functor of points of a scheme, closed points and their relation to field-valued points, and genus change of curves under field extension. A final section introduces the main questions about rational points that motivate the subject, such as the questions of whether the local-global principle and weak approximation hold.

Unofficial version for incidental online use

Chapter 3 begins with morphisms of finite presentation in order to discuss spreading out (e.g., extending a variety over a number field k to a scheme over a ring of S-integers in k). But the heart of the chapter is an extended introduction to smooth and étale morphisms, going beyond the treatment in [**Har77**, III.§10]. This, together with a section on flat morphisms, provides the basis for the definitions of the Grothendieck topologies commonly used for cohomology theories (see Chapter 6). The chapter also includes sections on rational maps and Frobenius morphisms: the latter are used to understand the Weil conjectures in Chapter 7.

The word "descent" has two unrelated meanings in arithmetic geometry. One meaning is as in Fermat's method of infinite descent and its generalizations, in which it is the height of rational points that descends in the course of a proof. The second meaning is that of descent of the ground field: the problem here is to decide whether a variety over a field extension $L \supseteq k$ arises as the base extension of a variety X over k (and to describe all possibilities for X). Chapter 4 studies this problem and its analogue for morphisms, and its generalizations to schemes. It also gives applications to the classification of twists of geometric objects (different k-forms of the same object over a field extension L), and to restriction of scalars, which transforms varieties over a field extension $L \supseteq k$ into varieties over k.

Chapter 5 is a survey on group schemes and algebraic groups over fields. After discussing their general properties, it defines special types of algebraic groups, and it states the classification theorem that decomposes arbitrary smooth algebraic groups into those types. The final section of Chapter 5 introduces torsors, which are needed to define the descent obstruction in Chapter 8. For algebraic groups over global fields, we discuss weak and strong approximation (Section 5.10) and the local-global principle for their torsors (Section 5.12.8).

Chapter 6 is an introduction to étale cohomology and its variants such as fppf cohomology. These cohomology theories are applied to generalize from torsors of algebraic groups over a field to torsors of group schemes over an arbitrary base scheme, and we prove finiteness results for torsors over a global field that are unramified at all but finitely many places. Another application is to generalize the cohomological definition of the Brauer group of a field to Grothendieck's definition of the cohomological Brauer group of a scheme. We end by discussing tools for computing these Brauer groups (the Hochschild–Serre spectral sequence, and residue homomorphisms) and give many examples since these will be needed to understand the Brauer–Manin obstruction in Section 8.2.

Although not needed for the main story of obstructions to rational points, we include in Chapter 7 the motivating application of étale cohomology,

Unofficial version for incidental online use

namely the Weil conjectures on varieties over finite fields. There we also discuss related issues, such as the étale cohomology classes of algebraic cycles and the Tate conjecture.

Chapter 8 defines the cohomological obstructions to the local-global principle and weak approximation for a variety X over a global field; these are expressed as subsets of the set $X(\mathbf{A})$ of adelic points that constrain where k-points may lie. First is the Brauer–Manin obstruction, coming from elements of the Brauer group of X. Next is the descent obstruction coming from torsors of algebraic groups; this is motivated by an example of a genus 2 curve in which the algebraic group is simply a finite group. Next we define hybrids of these two obstructions and compare their strengths for constraining k-points. Finally, we explain why all these obstructions are still not enough to decide whether a variety has a k-point.

Chapter 9 is a survey of the geometry and arithmetic of higher-dimensional varieties, with special attention paid to surfaces. It begins with the crude classification given by Kodaira dimension, and it compares the properties of being rational, unirational, rationally connected, and so on. Next we give the classification of surfaces over an arbitrary ground field, and we discuss the arithmetic of del Pezzo surfaces in some detail since these serve as excellent examples for the techniques presented earlier in the book. We end by discussing very briefly what is proved and conjectured for curves of genus > 1 and more generally for varieties of general type. The reasons for not exploring this in greater detail are first, that it would require a few hundred more pages to develop the required theory of height functions and diophantine approximation, and second, that several books on these topics exist already (we cite some of them).

A few appendices serve various purposes. Appendix A discusses some set theory that is implicitly used when discussing sheafification, for instance. Appendix B defines certain interesting classes of fields that did not make it into Chapter 1. Appendix C contains reference tables with lists of adjectives that can be applied to morphisms, varieties, or algebraic groups; the tables indicate where to find definitions, and propositions about their preservation under base extension, descent, and so on.

Unofficial version for incidental online use

0.6. Anything new in this book?

Almost all of the theorems in this book existed previously in the published literature in some form, but in many places we have tried to make proofs more readable and to organize topics so as to form a coherent exposition. There are a few new results: For example, the finiteness of Selmer sets (see Theorems 6.5.13 and 8.4.6) and Minchev's theorem on the failure of strong approximation (Corollary 8.4.11) were previously known only over number fields, whereas we generalize them to all global fields; these generalizations require extra arguments in the function field case because of the failure of Hermite's finiteness theorem on extensions of bounded degree unramified outside a fixed set of places. A few smaller innovations include an improved proof of Theorem 9.3.1(b)(ii) stating that proper birational morphisms between smooth surfaces factor into blowups at *separable* points, the use of the Lang–Nishimura theorem to avoid general position arguments in the proof of Lemma 9.4.18 on degree 6 del Pezzo surfaces, and the k-rationality of degree 5 del Pezzo surfaces over even the smallest of finite fields (Theorem 9.4.29).

The book whose content overlaps the most with ours is probably [**Sko01**]. That book also discusses torsors and the Brauer–Manin and descent obstructions, and it is written by a leading expert. Our book can serve as preparation for reading that one, since ours includes more background material (on algebraic groups, on étale and fppf cohomology, etc.), while [**Sko01**] goes further in other directions, proving theorems on the Brauer–Manin obstruction for conic bundle surfaces and for homogeneous spaces of simply connected algebraic groups, for instance.

0.7. Standard notation

Following Bourbaki, define

$$\begin{aligned}
\mathbb{N} &:= \text{the set of natural numbers} = \{0, 1, 2, \dots\},\\
\mathbb{Z} &:= \text{the ring of integers} = \{\dots, -2, -1, 0, 1, 2, \dots\},\\
\mathbb{Q} &:= \text{the field of rational numbers} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z},\ n \neq 0 \right\},\\
\mathbb{R} &:= \text{the field of real numbers},\\
\mathbb{C} &:= \text{the field of complex numbers} = \{\, a + bi : a, b \in \mathbb{R} \,\}, \text{ where } i = \sqrt{-1},\\
\mathbb{F}_q &:= \text{the finite field of } q \text{ elements},\\
\mathbb{Z}_p &:= \text{the ring of } p\text{-adic integers} = \varprojlim \mathbb{Z}/p^n\mathbb{Z},\\
\mathbb{Q}_p &:= \text{the field of } p\text{-adic numbers} = \text{the fraction field of } \mathbb{Z}_p.
\end{aligned}$$

The cardinality of a set S is denoted $\#S$ or sometimes $|S|$. If $(A_i)_{i \in I}$ is a collection of sets, and for all but finitely many $i \in I$ a subset $B_i \subseteq A_i$ is specified, then the **restricted product** $\prod'_{i \in I}(A_i, B_i)$ is the set of $(a_i) \in \prod_{i \in I} A_i$ such that $a_i \in B_i$ for all but finitely many i (with no condition being placed at the i for which B_i is undefined).

If $a, b \in \mathbb{Z}$, then $a \mid b$ means that a divides b, that is, that there exists $k \in \mathbb{Z}$ such that $b = ka$. Similarly, $a \nmid b$ means that a does not divide b. Define $\mathbb{Z}_{\geq 1} := \{\, n \in \mathbb{Z} : n \geq 1 \,\}$, and so on.

Unofficial version for incidental use

Rings are associative and have a 1 by definition [**Poo14**]. Suppose that R is a ring. Let $R^\times$ denote the unit group of R. Let $R[t_1, \dots, t_n]$ denote the ring of polynomials in $t_1, \dots, t_n$ with coefficients in R. Let $R[[t_1, \dots, t_n]]$ denote the ring of formal power series in $t_1, \dots, t_n$ with coefficients in R. The ring $R((t)) := R[[t]][t^{-1}]$ is called the ring of formal Laurent series in t with coefficients in R; its elements can be written as formal sums $\sum_{n \in \mathbb{Z}} a_n t^n$, where $a_n \in R$ for all n and $a_n = 0$ for sufficiently negative n. If R is an integral domain, then $\operatorname{Frac} R$ denotes its fraction field.

Suppose that k is a field. The characteristic of k is denoted $\operatorname{char} k$. The **rational function field** $k(t_1, \dots, t_n)$ is $\operatorname{Frac} k[t_1, \dots, t_n]$. The ring $k((t))$ defined above is a field, isomorphic to $\operatorname{Frac} k[[t]]$. Given an extension of fields L/k, a **transcendence basis** for L/k is a subset $S \subset L$ such that S is algebraically independent over k and L is algebraic over $k(S)$; such an S always exists, and $\#S$ is determined by L/k and is called the **transcendence degree** $\operatorname{tr} \deg(L/k)$.

Suppose that R is a ring and $n \in \mathbb{Z}_{\geq 0}$. Then $\mathrm{M}_n(R)$ denotes the R-algebra of $n \times n$ matrices with coefficients in R, and we define the group $\mathrm{GL}_n(R) := \mathrm{M}_n(R)^\times$. If R is commutative, a matrix $A \in \mathrm{M}_n(R)$ belongs to $\mathrm{GL}_n(R)$ if and only if its determinant $\det(A)$ is in $R^\times$.

If $\mathcal{A}$ is a category, then $\mathcal{A}^{\mathrm{opp}}$ denotes the opposite category, with the same objects but with morphisms reversed. We can avoid dealing with an anti-equivalence of categories $\mathcal{A} \to \mathcal{B}$ by rewriting it as an equivalence of categories $\mathcal{A}^{\mathrm{opp}} \to \mathcal{B}$. Let **Sets** be the category whose objects are sets and whose morphisms are functions. Let **Groups** denote the category of groups in which the morphisms are the homomorphisms. Let **Ab** denote the category of abelian groups; this is a full subcategory of **Groups**, where "full" means that for $A, B \in \mathbf{Ab}$, the definition of $\operatorname{Hom}(A, B)$ in **Ab** agrees with the definition of $\operatorname{Hom}(A, B)$ in **Groups**. We work in a fixed universe so that the objects in each category form a *set* (instead of a class); see Appendix A. From now on, we will usually not mention the universe.

0.8. Acknowledgments

I thank Dan Abramovich, Roman Bezrukavnikov, Kęstutis Česnavičius, CheeWhye Chin, Dustin Clausen, Jean-Louis Colliot-Thélène, Brian Conrad, Patrick Corn, David Corwin, Samit Dasgupta, Christopher Davis, Pavel Etingof, E. Victor Flynn, Thomas Graber, David Harari, Yonatan Harpaz, Robin Hartshorne, Ruthi Hortsch, Borys Kadets, Timo Keller, Steven Kleiman, Nikita Kozin, Chu-Wee Lim, William Messing, James Milne, Nghi Nguyen, Pace Nielsen, Arthur Ogus, René Pannekoek, Anatoly Preygel, Bhairav Singh, David Speyer, Padmavathi Srinivasan, Ronald van Luijk,

Unofficial version for incidental online use

Anthony Várilly-Alvarado, John Voight, Jared Weinstein, Olivier Wittenberg, Chenyang Xu, and several referees. In addition, various unpublished notes from the websites of Brian Conrad and James Milne have been very helpful to me. I also thank Yun Hao for converting my hand-drawn figures into Ti*k*Z.

I especially thank Jennifer Wright Sharp for her careful and intelligent copyediting. I thank also the other American Mathematical Society staff, including Marcia Almeida, Barbara Beeton, and Ina Mette, for helping me publish this book.

While writing the book, the author was partially supported by National Science Foundation grants DMS-0301280, DMS-0841321, DMS-1069236, and DMS-1601946; a Packard Fellowship; a Guggenheim Fellowship; and grants from the Simons Foundation (#340694, #402472, and #550033).

Bjorn Poonen
October 4, 2017

Unofficial version for incidental online use

Unofficial version for incidental online use

Chapter 1

Fields

Unofficial version for incidental online use

The first section of this chapter describes some types of fields. The other sections are concerned with questions one can ask about a field k in order to quantify how far it is from being algebraically closed:

(1) How many variables must a degree d homogeneous form over k have before it is guaranteed to have a nontrivial zero? (the C_r property)

(2) How complicated is the absolute Galois group of k? (cohomological dimension)

(3) How complicated is the set of isomorphism classes of finite-dimensional central division algebras over k? (the Brauer group)

1.1. Some fields arising in classical number theory

1.1.1. Closures. Let k be a field. Let $\overline{k}$ denote a fixed algebraic closure of k. Let k_{s} denote the **separable closure** of k in $\overline{k}$, so k_{s} is the maximal separable extension of k contained in $\overline{k}$. Let k^{perf} denote the **perfect closure** of k, so k^{perf} is the smallest perfect field containing k and contained in $\overline{k}$. Equivalently, if $\operatorname{char} k = p > 0$, then, in order to form a more perfect union, one can define $k^{\mathrm{perf}} := \bigcup_{n \geq 1} k^{1/p^n} \subseteq \overline{k}$. The **absolute Galois group** of k is the profinite group $\mathfrak{G}_k := \operatorname{Gal}(k_{\mathrm{s}}/k) \simeq \operatorname{Aut}(\overline{k}/k)$.

1.1.2. Local fields.

(References: [**Frö67**], [**Ser79**], [**RV99**, §4.2])

A **local field** is a field k satisfying one of the following equivalent conditions:

(1) k is a finite extension of $\mathbb{R}$, $\mathbb{Q}_p$, or $\mathbb{F}_p((t))$, for some prime p.

(2) k is isomorphic to one of the following:
- $\mathbb{R}$,
- $\mathbb{C}$,
- a finite extension of $\mathbb{Q}_p$ for some prime p, or
- $\mathbb{F}_q((u))$ for some prime power q.

(3) k is $\mathbb{R}$ or $\mathbb{C}$, or else k is the fraction field of a complete discrete valuation ring with finite residue field.

(4) k is a nondiscrete locally compact topological field (more precisely, k is locally compact and Hausdorff with respect to some nondiscrete topology for which the field operations are continuous).

(5) k is the completion of a global field (see Section 1.1.3) with respect to a nontrivial absolute value.

See Theorem 4-12 in [**RV99**] for a proof of the difficult part of the equivalence, namely that nondiscrete locally compact topological fields satisfy the other conditions.

If k is $\mathbb{R}$ or $\mathbb{C}$, then k is called **archimedean**; other local fields are called **nonarchimedean**.

1.1.3. Global fields.

(Reference: [**Cas67**])

A **number field** is a finite extension of $\mathbb{Q}$. A **global function field** is a finite extension of $\mathbb{F}_p(t)$ for some prime p or, equivalently, is the function field of a geometrically integral curve over a finite field $\mathbb{F}_q$, where q is a power of some prime p. (See Section 2.2 for the meaning of "geometrically integral curve".) When we say that k is a **global field**, we mean that k is either a number field or a global function field.

Equivalently, a global field is the fraction field of a finitely generated $\mathbb{Z}$-algebra that is an integral domain of Krull dimension 1.

By a place of k, we always mean a nontrivial place of k. Let Ω_k be the set of places of k.

Definition 1.1.1. If S is a finite nonempty subset of Ω_k containing all the archimedean places, then the **ring of S-integers in k** is

$$\mathcal{O}_{k,S} := \{ a \in k : v(a) \geq 0 \text{ for all } v \notin S \}.$$

If k is a number field, also define **the ring of integers of** k as $\mathcal{O}_k := \mathcal{O}_{k,S}$ where S is the set of archimedean places.

If v is a place of k, then k_v denotes the **completion** of k at v. Let $\mathcal{O}_v$ be the valuation ring of k_v if v is nonarchimedean, and let $\mathcal{O}_v = k_v$ if v

Unofficial version for incidental online use

is archimedean. Equip k_v and its subset $\mathcal{O}_v$ with the analytic (i.e., v-adic) topology coming from the place.

The **adèle ring** $\mathbf{A} = \mathbf{A}_k$ of k is defined as the restricted product

$$\prod\nolimits'_{v \in \Omega_k} (k_v, \mathcal{O}_v);$$

it is a k-algebra for the diagonal embedding of k, and it is equipped with the unique topology such that

- $\mathbf{A}$ is a topological group under addition,
- the subset $\prod_{v \in \Omega_k} \mathcal{O}_v$ is open, and
- the subspace topology on $\prod_{v \in \Omega_k} \mathcal{O}_v$ agrees with the product topology.

The image of k in $\mathbf{A}$ is discrete, and $\mathbf{A}/k$ is compact.

1.1.4. Other fields. For some other kinds of fields, see Appendix B.

1.2. C_r fields

(References: [**Gre69**], [**Sha72**], [**Pfi95**, Chapter 5])

Definition 1.2.1 ([**Lan52**])**.** Let k be a field, and let $r \in \mathbb{R}_{\geq 0}$. Then k is C_r if and only if every homogeneous form $f(x_1, \dots, x_n)$ of degree $d > 0$ in n variables with $n > d^r$ has a nontrivial zero in k^n. The adjective **quasi-algebraically closed** is a synonym for C_1.

1.2.1. Norm forms and normic forms.

Definition 1.2.2. Let L be a finite extension of a field k. Let $e_1, \dots, e_n$ be a k-basis of L. Write $L' = L(x_1, \dots, x_n)$ and $k' = k(x_1, \dots, x_n)$, where $x_1, \dots, x_n$ are indeterminates. If $N_{L'/k'}$ denotes the norm from L' to k', then $N_{L'/k'}(x_1 e_1 + \cdots + x_n e_n)$ is called a **norm form** for L over k.

Example 1.2.3. Let $k = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{7})$. The norm form for L over k associated to the basis $1, \sqrt{7}$ is $x_1^2 - 7x_2^2$.

Each norm form for L over k is a degree n homogeneous polynomial in $k[x_1, \dots, x_n]$, where $n = [L : k]$. Although it depends on the choice of basis, changing the basis changes the norm form only by an invertible k-linear transformation of the variables. The value of the norm form at a point $(b_1, \dots, b_n) \in k^n$ equals $N_{L/k}(b_1 e_1 + \cdots + b_n e_n)$.

Definition 1.2.4. Let k be a field. A homogeneous form $f \in k[x_1, \dots, x_n]$ is called **normic** if $\deg f = n$ and f has only the trivial zero in k^n.

Any norm form is normic. To construct other normic forms, we introduce some notation. If f and g are homogeneous forms, let $f(g \mid g \mid \cdots \mid g)$ be

Unofficial version for incidental online use

the homogeneous form obtained by substituting a copy of g for each variable in f, except that a new set of variables is used after each occurrence of $|$. If f is of degree d in n variables, and g is of degree e in m variables, then $f(g \mid g \mid \cdots \mid g)$ is of degree de in nm variables. If f and g are normic, then so is $f(g \mid g \mid \cdots \mid g)$.

Lemma 1.2.5. *If k is a field and k is not algebraically closed, then k has normic forms of arbitrarily high degree.*

Proof. Since k is not algebraically closed, it has a finite extension of degree $d > 1$. Let $F_1 = f$ be an associated norm form. For $\ell \geq 2$, let

$$F_\ell = F_{\ell-1}(f \mid f \mid \cdots \mid f).$$

By induction, F_ℓ is normic of degree d^ℓ. □

1.2.2. Systems of forms.

Proposition 1.2.6 (Artin, Lang, Nagata). *Let k be a C_r field, and let $f_1, \ldots, f_s$ be homogeneous forms of the same degree $d > 0$ in n common variables. If $n > sd^r$, then $f_1, \ldots, f_s$ have a nontrivial common zero in k^n.*

Proof. Suppose that k is algebraically closed. Since $n > sd^r \geq s$, the projective dimension theorem [**Har77**, I.7.2] implies that the intersection of the s hypersurfaces $f_i = 0$ in $\mathbb{P}^{n-1}$ contains a point.

Therefore, from now on assume that k is not algebraically closed. Suppose also that the f_i have no nontrivial common zero. We will inductively build forms Φ_m of degree D_m in N_m variables, each having no nontrivial zero, and get a contradiction for large m. By Lemma 1.2.5, we can find a normic form Φ_0 of arbitrarily high degree e (later we will specify how large we need e to be). So $D_0 = N_0 = e$. For $m \geq 1$, define

$$\Phi_m = \Phi_{m-1}(f_1, \ldots, f_s \mid f_1, \ldots, f_s \mid \cdots \mid f_1, \ldots, f_s \mid 0, 0, \ldots, 0),$$

where within each block $f_1, \ldots, f_s$ the same n variables are used, but new variables are used after each $|$, and we use as many blocks as possible (namely, $\lfloor N_{m-1}/s \rfloor$ blocks) and pad with zeros to get the right number of arguments to Φ_{m-1}. Thus $D_m = dD_{m-1}$ and $N_m = n\lfloor N_{m-1}/s \rfloor$. By induction on m, the form Φ_m has no nontrivial zero.

By induction, $D_m = d^m e$. If we could ignore the $\lfloor\ \rfloor$, then N_m would be $(n/s)^m e$, and

$$\frac{N_m}{D_m^r} = \left(\frac{n}{sd^r}\right)^m e^{1-r} > 1$$

for sufficiently large m, since $n > sd^r$. But we cannot quite ignore $\lfloor\ \rfloor$, so we choose $\beta \in \mathbb{R}$ with $d^r < \beta < n/s$ and choose the degree e of the normic form

Unofficial version for incidental online use

Φ_0 so that $n\lfloor x/s\rfloor \geq \beta x$ holds for all $x \geq e$. Then $N_m \geq \beta^m e$ by induction on m, and

$$\frac{N_m}{D_m^r} \geq \left(\frac{\beta}{d^r}\right)^m e^{1-r} > 1$$

for m sufficiently large.

Since k is C_r, the form Φ_m has a nontrivial zero, a contradiction. □

Unofficial version for incidental online use

1.2.3. Transition theorems.

Theorem 1.2.7. *Let k be a C_r field, and let L be a field extension of k.*

(i) *If L is algebraic over k, then L is C_r.*

(ii) *If $L = k(t)$, where t is an indeterminate, then L is C_{r+1}.*

(iii) *If $\operatorname{tr\,deg}(L/k) = s$, then L is C_{r+s}.*

Proof.

(i) Let $f \in L[x_1, \ldots, x_n]$ be a form of degree $d > 0$, where $n > d^r$. Since L is algebraic over k, the coefficients of f generate a finite extension L_0 of k. If we find a nontrivial zero of f over L_0, then the same is a nontrivial zero over L. Thus we reduce to the case where L is a *finite* extension of k.

Choose a basis $e_1, \ldots, e_s$ of L over k. Introduce new variables y_{ij} with $1 \leq i \leq n$ and $1 \leq j \leq s$, and substitute

$$x_i = \sum_{j=1}^{s} y_{ij} e_j$$

for all i into f, so that

$$f(x_1, \ldots, x_n) = F_1 e_1 + \cdots + F_s e_s,$$

where each $F_\ell \in k[\{y_{ij}\}]$ is a form of degree d in ns variables. Since $n > d^r$, we have $ns > sd^r$, so Proposition 1.2.6 implies that the F_ℓ have a nontrivial common zero (y_{ij}) over k. This means that f has a nontrivial zero over L.

(ii) Let $f \in k(t)[x_1, \ldots, x_n]$ be a form of degree $d > 0$, where $n > d^{r+1}$. Multiplying f by a polynomial in $k[t]$ to clear denominators, we may assume that f has coefficients in $k[t]$. Let m be the maximum of the degrees of these coefficients. Choose $s \in \mathbb{Z}_{>0}$ large (later we will say how large), introduce new variables y_{ij} with $1 \leq i \leq n$ and $0 \leq j \leq s$, and substitute

$$x_i = \sum_{j=0}^{s} y_{ij} t^j$$

for all i into f, so that

$$f(x_1, \dots, x_n) = F_0 + F_1 t + \cdots + F_{ds+m} t^{ds+m},$$

where each $F_\ell \in k[\{y_{ij}\}]$ is a form of degree d in $n(s+1)$ variables. Because $n > d^{r+1}$,

$$n(s+1) > (ds+m+1)d^r$$

holds for sufficiently large s, and then Proposition 1.2.6 implies that the F_ℓ have a nontrivial common zero (y_{ij}) over k. This means that f has a nontrivial zero over $k[t]$, hence over $k(t)$.

(iii) This follows from (i) and (ii), by induction on s. □

1.2.4. Examples of C_r fields.

(1) A field is C_0 if and only if it is algebraically closed. For a generalization, see Exercise 1.3.

(2) The following special case of Theorem 1.2.7 is known as **Tsen's theorem**: If L is the function field of a curve over an algebraically closed field k (that is, L is a finitely generated extension of k of transcendence degree 1), then L is C_1.

(3) The **Chevalley–Warning theorem** states that finite fields are C_1. This was conjectured by E. Artin and was proved first by Chevalley [**Che36**], who proved more generally that over a finite field $\mathbb{F}_q$, a (not necessarily homogeneous) polynomial f of total degree d in $n > d$ variables with zero constant term has a nontrivial zero. Warning's proof [**War36**] of this proceeded by showing that the total number of zeros, including the trivial zero, was a multiple of $p := \operatorname{char} \mathbb{F}_q$. Ax [**Ax64**] showed moreover that the number of zeros was divisible by q, and in fact divisible by q^b, where $b = \lceil n/d \rceil - 1$ is the largest integer strictly less than n/d. For an improvement in a different direction, observe that Warning's theorem says that a hypersurface X in $\mathbb{P}^{n-1}$ over $\mathbb{F}_q$ defined by a homogeneous form of degree $d < n$ satisfies $\#X(\mathbb{F}_q) \equiv 1 \pmod{p}$; this can be extended to some varieties that are not hypersurfaces, such as smooth projective rationally chain connected varieties [**Esn03**, Corollary 1.3]; see [**Wit10**] for a survey about this and further generalizations.

(4) Lang proved that if k is complete with respect to a discrete valuation having algebraically closed residue field, then k is C_1. More generally, if k is a henselian discrete valuation field with algebraically closed residue field such that the completion $\widehat{k}$ is separable over k, then k is C_1. (See Section B.3 for the definition of henselian.) This applies in particular if k is the maximal unramified extension of a complete discrete valuation

Unofficial version for incidental online use

field with perfect residue field. For example, the maximal unramified extension $\mathbb{Q}_p^{\mathrm{unr}}$ of $\mathbb{Q}_p$ is C_1. See [**Lan52**] for all these results.

(5) A local field of positive characteristic is C_2; see [**Lan52**, Theorem 8]. More generally, if k is C_r, then $k((t))$ is C_{r+1} [**Gre66**].

1.2.5. Counterexamples. The field $\mathbb{R}$ is not C_r for any r, since for every $n \geq 1$ the equation $x_1^2 + \cdots + x_n^2 = 0$ has no nontrivial solution. The same argument applies to any formally real field.

E. Artin conjectured that nonarchimedean local fields were C_2, the expectation being that if a field k is complete with respect to a discrete valuation with a C_r residue field, then k should be C_{r+1}. That nonarchimedean local fields satisfy the C_2 property *restricted to degree d forms* was proved for $d = 2$ [**Has24**] and $d = 3$ [**Dem50**, **Lew52**]. Also Ax and Kochen [**AK65**] nearly proved that the field $\mathbb{Q}_p$ is C_2: using model theory they showed that for each d, for all primes p *outside a finite set depending on d*, every homogeneous form of degree d in $> d^2$ variables over $\mathbb{Q}_p$ has a nontrivial zero. But then Terjanian [**Ter66**] disproved Artin's conjecture by finding a homogeneous form of degree 4 in 18 variables over $\mathbb{Q}_2$ with no nontrivial zero. Later it was shown that if $[k : \mathbb{Q}_p] < \infty$, then k is not C_r for any r [**AK81**, **Ale85**]. It follows that if k is a number field, then k is not C_r for any r (Exercise 1.8).

1.2.6. Open questions.

Question 1.2.8. Is there a field k and $r \in \mathbb{R}_{\geq 0}$ such that k is C_r but not $C_{\lfloor r \rfloor}$?

Question 1.2.9 (E. Artin)**.** Let $\mathbb{Q}^{\mathrm{ab}}$ be the maximal abelian extension of $\mathbb{Q}$. (The Kronecker–Weber theorem states that $\mathbb{Q}^{\mathrm{ab}}$ is obtained by adjoining all roots of 1 to $\mathbb{Q}$.) Is $\mathbb{Q}^{\mathrm{ab}}$ a C_1 field?

Definition 1.2.10. A field k is called C_r' if whenever one has homogeneous forms $f_1, \ldots, f_s$ in n common variables of degrees $d_1, \ldots, d_s$, respectively, with $n > d_1^r + \cdots + d_s^r$, the forms have a nontrivial common zero in k^n.

Question 1.2.11 ([**Gre69**, p. 21])**.** Is C_r equivalent to C_r'?

By definition, C_r' implies C_r. The converse holds at least for fields k such that for every $d \geq 1$ there exists a homogeneous form of degree d in d^r variables over k with no nontrivial zero [**Lan52**, Theorem 4]. The C_r' property is studied in more detail in [**Pfi95**, Chapter 5].

Question 1.2.12. What general classes of varieties are guaranteed to have a k-point whenever k is C_1?

Question 1.2.13 (Ax)**.** Is every perfect PAC field C_1? (See Section B.5 for the definition of PAC.)

Unofficial version for incidental online use

By [**Kol07a**, Theorem 1], every PAC field of characteristic 0 is C_1, and even C_1'. See [**FJ08**, 21.3.6] for a few other positive partial results toward Question 1.2.13.

1.3. Galois theory

1.3.1. $\mathfrak{G}_k$-sets. Let k be a field. Let $\mathfrak{G}_k$ be the profinite group $\operatorname{Gal}(k_s/k)$. A $\mathfrak{G}_k$-**set** is a set S (with the discrete topology) equipped with a continuous action of $\mathfrak{G}_k$. A morphism of $\mathfrak{G}_k$-sets is a map of sets respecting the $\mathfrak{G}_k$-actions. A $\mathfrak{G}_k$-set is called **finite** if it is finite as a set. For example, if H is an open subgroup of $\mathfrak{G}_k$, then $\mathfrak{G}_k/H$ equipped with the left multiplication action of $\mathfrak{G}_k$ is a finite $\mathfrak{G}_k$-set.

A continuous action of $\mathfrak{G}_k$ on a set S is called **transitive** if $S \neq \emptyset$ and for every $s_1, s_2 \in S$ there exists $g \in \mathfrak{G}_k$ such that $gs_1 = s_2$. In this case, if we fix $s \in S$ and define $H = \operatorname{Stab}_{\mathfrak{G}_k}(s) := \{g \in \mathfrak{G}_k : gs = s\}$, then H is open and the map $\mathfrak{G}_k/H \to S$ sending $gH \in \mathfrak{G}_k/H$ to gs is an isomorphism of $\mathfrak{G}_k$-sets; in particular, S is finite. Every $\mathfrak{G}_k$-set decomposes uniquely as a disjoint union of transitive $\mathfrak{G}_k$-sets, the orbits.

1.3.2. Étale algebras. The problem with field extensions $L \supseteq k$ is that if we change the base by tensoring with a field extension k' of k, the resulting algebra $L \otimes_k k'$ over k' need not be a field. The notion of étale algebra generalizes the notion of finite separable field extension in order to fix this problem.

Definition 1.3.1. A k-algebra L is called **étale** if it satisfies any of the following equivalent conditions:

- L is a direct product of finite separable extensions of k;
- the k_s-algebra $L \otimes_k k_s$ is a finite product of copies of k_s;
- the morphism of schemes $\operatorname{Spec} L \to \operatorname{Spec} k$ is finite and étale in the sense of Section 3.5.8 (see Proposition 3.5.35).

A **morphism** between two étale k-algebras is a homomorphism of k-algebras. If L is an étale k-algebra and k' is any field extension of k, then $L \otimes_k k'$ is an étale k'-algebra.

The following is Grothendieck's restatement and generalization of Galois theory.

Theorem 1.3.2 ([**SGA 1**, V.7 and Proposition V.8.1])**.** *The functors*

$$\begin{aligned}\{\text{finite } \mathfrak{G}_k\text{-sets}\}^{\text{opp}} &\longleftrightarrow \{\text{étale } k\text{-algebras}\},\\ S &\longmapsto \operatorname{Hom}_{\mathfrak{G}_k\text{-sets}}(S, k_s) = \operatorname{Hom}_{\text{sets}}(S, k_s)^{\mathfrak{G}_k}\\ \operatorname{Hom}_{k\text{-algebras}}(L, k_s) &\longleftarrow L\end{aligned}$$

Unofficial version for incidental online use

are inverse equivalences of categories.

Example 1.3.3. If S is a transitive $\mathfrak{G}_k$-set, say $S = \mathfrak{G}_k/H$ for an open subgroup $H \le \mathfrak{G}_k$, then the corresponding étale algebra is the H-fixed subfield $\operatorname{Hom}_{\mathfrak{G}_k\text{-sets}}(\mathfrak{G}_k/H, k_s) = (k_s)^H$ of k_s, i.e., the finite separable extension of k associated to H by classical Galois theory.

In general, a finite $\mathfrak{G}_k$-set S is a finite disjoint union $\coprod S_i$ of transitive $\mathfrak{G}_k$-sets. If S_i corresponds to the finite separable extension L_i, then S corresponds to the étale algebra $\prod L_i$.

Example 1.3.4. If S is a finite set with trivial $\mathfrak{G}_k$-action, the corresponding étale algebra is a finite product of copies of k. Such étale algebras are called **split**.

1.3.3. Galois étale algebras. Just as étale algebras generalize finite separable field extensions, Galois étale algebras generalize finite Galois field extensions:

Definition 1.3.5. Let L be an étale k-algebra with a left action of a finite group G. If $\Omega \supseteq k$ is a field extension, then $L \otimes_k \Omega$ is an étale Ω-algebra with left G-action, and so is $\prod_{g \in G} \Omega = \operatorname{Hom}_{\text{sets}}(G, \Omega)$ via the right translation G-action on G. Call L a **Galois étale k-algebra with Galois group** G if for some field extension $\Omega \supseteq k$ we have $L \otimes_k \Omega \simeq \prod_{g \in G} \Omega$ as étale Ω-algebras with left G-action.

Warning 1.3.6. The group $\operatorname{Aut}(L/k)$ can be larger than G, and in fact G is not determined by L/k. For example, if $L = k \times k \times k \times k$, then L can be equipped with actions of $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ making it a Galois étale algebra, but $\operatorname{Aut}(L/k) \simeq S_4$. This explains why in Definition 1.3.5 the group G and its action on L must be specified in advance.

Remark 1.3.7. If an Ω as in Definition 1.3.5 exists, then one such Ω is k_s.

1.3.4. Galois descent for vector spaces. Let $L \supseteq k$ be a finite Galois extension of fields with Galois group G. An action of G on an L-vector space W is **semilinear** if $\sigma(\ell w) = (\sigma\ell)(\sigma w)$ for all $\sigma \in G$, $\ell \in L$, and $w \in W$.

Example 1.3.8. The coordinatewise action of G on L^n is semilinear. More generally, if V is any k-vector space, then $V \otimes_k L$ is an L-vector space with semilinear G-action.

Let $W^G = \{w \in W : gw = w \text{ for all } g \in G\}$; this is a k-vector space.

Lemma 1.3.9. *Let V be a k-vector space. Then the k-linear map*

$$\begin{aligned} V &\longrightarrow (V \otimes_k L)^G \\ v &\longmapsto v \otimes 1 \end{aligned}$$

Unofficial version for incidental online use

is an isomorphism.

Proof. For $V = k$, this is the Galois theory fact $L^G = k$. Any V is a direct sum of copies of the 1-dimensional space k, and the formation of the map respects direct sums. $\square$

Lemma 1.3.10. *Let W be an L-vector space with semilinear G-action. Then the L-linear map*

$$\begin{aligned} W^G \otimes_k L &\longrightarrow W \\ w \otimes \ell &\longmapsto \ell w \end{aligned}$$

is an isomorphism.

Proof. We will prove that the same holds even if L is only a Galois étale k-algebra with Galois group G (and W is an L-module with semilinear G-action). The advantage of considering this more general statement is that now we can extend the ground field by applying $\otimes_k \Omega$ to k, L, and W. The operation of taking G-invariants and the property of a linear map being an isomorphism are preserved by such a base change, so after renaming Ω as k, we reduce to the split case $L = \prod_{g \in G} k$. Let $e_g = (0, \ldots, 0, 1, 0, \ldots, 0) \in L$, with 1 in the gth coordinate. Then the L-module W is $\prod_{g \in G} W_g$ for some k-vector spaces $W_g := e_g W$. An element $g \in G$ maps e_g to e_1, and hence provides an isomorphism $W_g \xrightarrow{\sim} W_1$. Then W^G is the diagonal image of $W_1 \hookrightarrow \prod_{g \in G} W_g$. Finally, the map $W^G \otimes_k L \to W$ restricts to an isomorphism $W^G \otimes_k k e_g \xrightarrow{\sim} W_g$ for each g, so it is an isomorphism. $\square$

Theorem 1.3.11. *Let $L \supseteq k$ be a finite Galois extension of fields with Galois group G. The functors*

$$\{k\text{-vector spaces}\} \underset{\text{take } G\text{-invariants}}{\overset{\otimes_k L}{\rightleftarrows}} \{L\text{-vector spaces with semilinear } G\text{-action}\}$$

are inverse equivalences of categories.

Proof. The two compositions are isomorphic to the identity functors, by Lemmas 1.3.9 and 1.3.10. $\square$

Corollary 1.3.12. *Let $L \supseteq k$ be a finite Galois extension of fields with Galois group G. For each $r \in \mathbb{Z}_{\geq 0}$, there is only one r-dimensional L-vector space with semilinear G-action, up to isomorphism.*

Proof. The functor $\otimes_k L$ in Theorem 1.3.11 respects dimension: $\dim_k V = \dim_L(V \otimes_k L)$. There is only one r-dimensional k-vector space, up to isomorphism. $\square$

Unofficial version for individual online use

Remark 1.3.13. Theorem 1.3.11 and its proof generalize to the theory of descent developed by Weil and Grothendieck. See Chapter 4.

1.3.5. Hilbert's theorem 90 and generalizations. Let us gather a few fundamental results in Galois cohomology. Let L^+ denote the additive group of a field L. If k is a field, and $n \in \mathbb{Z}_{\geq 1}$ is not divisible by $\operatorname{char} k$, let μ_n denote the group of nth roots of 1 in ${k_s}^\times$.

Definition 1.3.14. If A is a commutative group scheme (see Section 5.1) over a field k, then the notation $\mathrm{H}^q(k, A)$ denotes the Galois cohomology group $\mathrm{H}^q(\mathfrak{G}_k, A(k_s))$. (This definition is made so as to agree with the étale cohomology group $\mathrm{H}^q_{\mathrm{et}}(\operatorname{Spec} k, A)$ of the sheaf defined by A on the étale site of $\operatorname{Spec} k$; see Section 6.4.3.) If A is noncommutative, the same definition is made for $q = 0, 1$.

Proposition 1.3.15. *Let $L \supseteq k$ be a Galois extension of fields.*

(i) *We have* $\mathrm{H}^q(\mathrm{Gal}(L/k), L^+) = 0$ *for all* $q \geq 1$. *In particular, we have* $\mathrm{H}^q(k, \mathbb{G}_a) = 0$ *for all* $q \geq 1$.

(ii) ("Hilbert's theorem 90") *We have* $\mathrm{H}^1(\mathrm{Gal}(L/k), L^\times) = 0$. *In particular,* $\mathrm{H}^1(k, \mathbb{G}_m) = 0$.

(iii) *For each* $r \in \mathbb{Z}_{\geq 0}$, *we have* $\mathrm{H}^1(\mathrm{Gal}(L/k), \mathrm{GL}_r(L)) = 0$. *In particular,* $\mathrm{H}^1(k, \mathrm{GL}_r) = 0$.

Remark 1.3.16. Hilbert's *original* theorem 90 was essentially the special case of (ii) in which $\mathrm{Gal}(L/k)$ is a finite cyclic group; see Exercise 1.10. It was E. Noether who generalized it to arbitrary (finite) Galois extensions.

Proof. We may assume that $[L : k] < \infty$, since the general case then follows by taking a direct limit.

(i) By the normal basis theorem, L^+ is an induced $\mathrm{Gal}(L/k)$-module, so it has trivial cohomology.

(ii) This is the $r = 1$ case of (iii), which we will now prove.

(iii) Let $G = \mathrm{Gal}(L/k)$. Given a 1-cochain (i.e., function) $\xi \colon G \to \mathrm{GL}_r(L)$, let W_ξ be L^r equipped with the function $G \times L^r \to L^r$ sending (σ, w) to $\xi_\sigma(\sigma w)$. Exercise 1.9a shows that this describes a semilinear G-action (i.e., the group action axiom $(\sigma\tau) * w = \sigma * (\tau * w)$ is satisfied) if and only if ξ is a cocycle. Exercise 1.9b shows also that given two 1-cocycles ξ and ξ', we have $W_\xi \simeq W_{\xi'}$ as L-vector spaces with semilinear G-action if and only if ξ and ξ' are cohomologous. Thus we obtain a bijection

$$\mathrm{H}^1(G, \mathrm{GL}_r(L)) \longleftrightarrow \frac{\{r\text{-dimensional } L\text{-vector spaces with semilinear } G\text{-action}\}}{\text{isomorphism}}.$$

Unofficial version for incidental online use

By Corollary 1.3.12, the latter set has one element, so $\mathrm{H}^1(G, \mathrm{GL}_r(L)) = 0$ too. □

Remark 1.3.17. There is an alternative proof of (iii) that proceeds by showing directly that every 1-cocycle $\xi\colon G \to \mathrm{GL}_r(L)$ is cohomologous to the trivial 1-cocycle, by writing down a *Poincaré series*; see [**Ser79**, Chapter X, Proposition 3]. This proof has the advantage of being short and needing little beyond Dedekind's theorem on linear independence of automorphisms, but it is harder to remember and does not readily generalize to give the theory in Chapter 4.

Remark 1.3.18. Suppose that L is an extension of k. Choose an embedding $\iota\colon k_{\mathrm{s}} \hookrightarrow L_{\mathrm{s}}$; we then get an inclusion homomorphism $A(k_{\mathrm{s}}) \to A(L_{\mathrm{s}})$ and a restriction homomorphism $\mathfrak{G}_L \to \mathfrak{G}_k$. Thus we get a homomorphism $\mathrm{H}^q(k, A) \to \mathrm{H}^q(L, A)$, and it is independent of ι, since the conjugation action of a group G on any cohomology group $\mathrm{H}^q(G, M)$ is trivial, as can be proved by dimension shifting.

1.4. Cohomological dimension

(Reference: [**Ser02**])

This section is almost never used in the rest of the book, so it may be skipped upon a first reading.

1.4.1. Definitions. Let G be a profinite group. When we say that A is a G-module, we mean that A is an abelian group with an action of the abstract group G such that the map $G \times A \to A$ giving the action is continuous for the profinite topology on G and the discrete topology on A.

A G-module A is called **torsion** if and only if every element of the abelian group A has finite order. If B is an abelian group and n is an integer, define $B[n] := \{ b \in B : nb = 0 \}$. If p is a prime number, define $B[p^\infty] := \bigcup_{n \geq 1} B[p^n]$.

Definition 1.4.1. Let G be a profinite group, and let p be a prime number.

(i) The **p-cohomological dimension** of G, denoted $\mathrm{cd}_p(G)$, is the smallest $n \in \mathbb{N}$ such that for all *torsion* G-modules A and all integers $q > n$, $\mathrm{H}^q(G, A)[p^\infty] = 0$. If no such n exists, then $\mathrm{cd}_p(G) = +\infty$.

(ii) The **strict p-cohomological dimension** of G, denoted $\mathrm{scd}_p(G)$, is defined in the same way as $\mathrm{cd}_p(G)$, except that the word "torsion" is omitted.

(iii) The **cohomological dimension** of G is $\mathrm{cd}(G) := \sup_p \mathrm{cd}_p(G)$.

(iv) The **strict cohomological dimension** of G is $\mathrm{scd}(G) := \sup_p \mathrm{scd}_p(G)$.

Unofficial version for incidental online use

Proposition 1.4.2. *For any profinite group G and any prime number p, $\operatorname{scd}_p(G)$ equals $\operatorname{cd}_p(G)$ or $\operatorname{cd}_p(G)+1$.*

Proof. Clearly $\operatorname{scd}_p(G) \geq \operatorname{cd}_p(G)$. To complete the proof, we assume that $\operatorname{cd}_p(G) = n < \infty$ and attempt to prove that $\operatorname{scd}_p(G) \leq n+1$.

Let A be a G-module. Take the long exact sequences associated to

$$0 \to A[p] \to A \xrightarrow{p} pA \to 0$$

and

$$0 \to pA \to A \to A/pA \to 0.$$

For $q > n+1$, the hypothesis $\operatorname{cd}_p(G) = n$ implies $\mathrm{H}^q(G, A[p]) = 0$ and $\mathrm{H}^{q-1}(G, A/pA) = 0$, so the long exact sequences give injections $\mathrm{H}^q(G,A) \overset{p}{\hookrightarrow} \mathrm{H}^q(G, pA)$ and $\mathrm{H}^q(G, pA) \hookrightarrow \mathrm{H}^q(G,A)$, respectively. The composition of these injections is multiplication by p on $\mathrm{H}^q(G,A)$, so $\mathrm{H}^q(G,A)[p^\infty] = 0$. Thus $\operatorname{scd}_p(G) \leq n+1$, by definition. $\square$

Recall that if k is a field, then $\mathfrak{G}_k$ denotes the profinite group $\operatorname{Gal}(k_{\mathrm{s}}/k)$.

Definition 1.4.3. If k is a field, then $\operatorname{cd}_p(k) := \operatorname{cd}_p(\mathfrak{G}_k)$. Define $\operatorname{scd}_p(k)$, $\operatorname{cd}(k)$, and $\operatorname{scd}(k)$ similarly.

1.4.2. Transition theorems. The condition $\operatorname{cd}(k) \leq r$ on a field behaves under field extensions similarly to the C_r condition. To prove such results, we need to develop analogous transition theorems for cohomological dimension of groups.

Let us first recall the definition of induced modules, and Shapiro's lemma.

Definition 1.4.4. Suppose that H is a closed subgroup of a profinite group G. Given an H-module A, the **induced module** $\operatorname{Ind}_H^G(A)$ is the group of continuous maps $\phi\colon G \to A$ such that $\phi(hx) = h\phi(x)$ for all $x \in G$ and $h \in H$. Each $g \in G$ acts on $\operatorname{Ind}_H^G(A)$ by $(g\phi)(x) = \phi(xg)$; this makes $\operatorname{Ind}_H^G(A)$ a G-module.

Lemma 1.4.5 (Shapiro's lemma)**.** *Let H be a closed subgroup of a profinite group G. For each H-module A, we have $\mathrm{H}^q(G, \operatorname{Ind}_H^G(A)) \simeq \mathrm{H}^q(H,A)$.*

Next is a transition theorem for cohomological dimension of groups:

Proposition 1.4.6. *Let H be a closed subgroup of a profinite group G, and let p be prime. Then $\operatorname{cd}_p(H) \leq \operatorname{cd}_p(G)$ and $\operatorname{scd}_p(H) \leq \operatorname{scd}_p(G)$. Equality holds in both, if either*

(i) *the index $(G:H)$ is prime to p, or*

(ii) *the subgroup H is open in G and $\operatorname{cd}_p(G) < \infty$.*

Unofficial version for incidental online use

Remark 1.4.7. The condition "$(G : H)$ is prime to p" means that each open subgroup of G containing H has index prime to p. Alternatively (but equivalently), $(G : H)$ can be interpreted as a **supernatural number** [**Ser02**, I.1.3].

Proof of Proposition 1.4.6. Let A be a torsion H-module. Then the G-module $A' := \operatorname{Ind}_H^G(A)$ is torsion, and it satisfies $\mathrm{H}^q(G, A') \simeq \mathrm{H}^q(H, A)$ (Shapiro's lemma). Thus $\operatorname{cd}_p(H) \le \operatorname{cd}_p(G)$ by definition.

Now suppose (i). The corestriction-restriction formula $\operatorname{Cor} \circ \operatorname{Res} = n$ on cohomology for subgroups of finite index n implies that

$$\operatorname{Res}\colon \mathrm{H}^q(G, A)[p^\infty] \to \mathrm{H}^q(H, A)[p^\infty]$$

is injective, at least if $(G : H)$ is finite (and prime to p). In fact, this holds also for $(G : H)$ infinite (and prime to p), by expressing the cohomology as direct limits over cohomology of finite groups. Hence $\operatorname{cd}_p(G) \le \operatorname{cd}_p(H)$.

Now suppose (ii) instead. Let $n = \operatorname{cd}_p(G)$. We may assume $n \ge 1$. Choose a torsion G-module A such that $\mathrm{H}^n(G, A)[p^\infty] \ne 0$. Let $A' = \operatorname{Ind}_H^G(A)$. There is a surjection of G-modules $\pi\colon A' \to A$ mapping ϕ to $\sum_{x \in G/H} x \cdot \phi(x^{-1})$ (where x ranges over a set of coset representatives for H in G). If $B = \ker \pi$, then we have an exact sequence

$$\mathrm{H}^n(G, A') \to \mathrm{H}^n(G, A) \to \mathrm{H}^{n+1}(G, B).$$

These groups are torsion, so taking p-primary parts is exact. Since $\operatorname{cd}_p(G) = n$, we have $\mathrm{H}^{n+1}(G, B)[p^\infty] = 0$, so $\mathrm{H}^n(G, A')[p^\infty] \twoheadrightarrow \mathrm{H}^n(G, A)[p^\infty]$ is surjective. Thus $\mathrm{H}^n(G, A')[p^\infty]$ is nonzero, and Shapiro's lemma identifies this with $\mathrm{H}^n(H, A)[p^\infty]$. Hence $\operatorname{cd}_p(H) \ge n = \operatorname{cd}_p(G)$.

The same proofs work for scd_p. □

Given an algebraic extension $L \supseteq k$, let $[L : k]_{\mathrm{s}}$ denote the **separable degree**; then "$[L : k]_{\mathrm{s}}$ is prime to p" means that every finite separable extension of k inside L has degree prime to p.

Corollary 1.4.8. *Let L be an algebraic extension of k, and let p be prime. Then $\operatorname{cd}_p(L) \le \operatorname{cd}_p(k)$. Equality holds in both, if either*

(i) *$[L : k]_{\mathrm{s}}$ is prime to p, or*

(ii) *$[L : k]_{\mathrm{s}} < \infty$ and $\operatorname{cd}_p(k) < \infty$.*

Corollary 1.4.8 can be strengthened for finite extensions.

Proposition 1.4.9. *Suppose $[L : k] < \infty$. Then $\operatorname{cd}_p(L) = \operatorname{cd}_p(k)$ unless the following are simultaneously satisfied:*

(i) *$p = 2$,*

(ii) *k is formally real, and*

Unofficial version for incidental online use

(iii) $\operatorname{cd}_2(L) < \infty$.

Proof. See [**Ser02**, II.§4.1, Proposition 10′]. $\square$

Remark 1.4.10. We have $\operatorname{cd}_2(\mathbb{R}) = \infty$ but $\operatorname{cd}_2(\mathbb{C}) = 0$, so the "unless" clause in Proposition 1.4.9 cannot be eliminated.

Proposition 1.4.11. *Let L be an extension of k with $\operatorname{tr}\deg(L/k) = s$, and let p be prime. Then $\operatorname{cd}_p(L) \le \operatorname{cd}_p(k) + s$. Equality holds if L is finitely generated over k, $\operatorname{cd}_p(k) < \infty$, and $p \neq \operatorname{char} k$.*

Proof. See [**Ser02**, II.§4.2, Proposition 11]. $\square$

Proposition 1.4.12. *Let L be complete with respect to a discrete valuation with residue field k, and let p be prime. Then $\operatorname{cd}_p(L) \le \operatorname{cd}_p(k) + 1$. Equality holds if $\operatorname{cd}_p(k) < \infty$ and $p \neq \operatorname{char} L$.*

Proof. See [**Ser02**, II.§4.3, Proposition 12]. $\square$

1.4.3. Examples.

(1) If k is a separably closed field, then $\mathfrak{G}_k$ is trivial, so $\operatorname{cd}_p(k) = \operatorname{scd}_p(k) = 0$ for all p.

(2) If k is a finite field, then $\mathfrak{G}_k = \widehat{\mathbb{Z}}$, and $\operatorname{cd}_p(k) = 1$ and $\operatorname{scd}_p(k) = 2$ for all p.

(3) If k is a nonarchimedean local field, then $\operatorname{cd}_p(k) = \operatorname{scd}_p(k) = 2$ for all $p \neq \operatorname{char} k$. (For cd_p this follows from Proposition 1.4.12. For scd_p in the case of finite extensions of $\mathbb{Q}_\ell$, see [**Ser02**, II.§5.3, Proposition 15]. For a proof of the more general fact that an n-dimensional local field k in the sense of Section B.1 has $\operatorname{cd}_p(k) = \operatorname{scd}_p(k) = n + 1$ for $p \neq \operatorname{char} k$, see [**Koy03**].)

(4) Suppose that k is a global field and $p \neq \operatorname{char} k$. If k has a real place, suppose that $p \neq 2$. Then $\operatorname{cd}_p(k) = \operatorname{scd}_p(k) = 2$. (See [**Ser02**, II.§4.4, Proposition 13] and [**NSW08**, Theorems 8.3.17 and 10.2.3].)

(5) Let k_0 be a finite field or a number field. Let p be a prime not equal to $\operatorname{char} k_0$. In the case where k_0 is a number field having a real place, assume in addition that $p \neq 2$. Then for any finitely generated field extension k of k_0,
$$\operatorname{cd}_p(k) = \begin{cases} \operatorname{tr}\deg(k/k_0) + 1 & \text{if } k_0 \text{ is a finite field,} \\ \operatorname{tr}\deg(k/k_0) + 2 & \text{if } k_0 \text{ is a number field.} \end{cases}$$
This follows from the previous examples by using Proposition 1.4.11.

Unofficial version for incidental online use

1.5. Brauer groups of fields

(Reference: [**GS06**])

1.5.1. Azumaya algebras over a field.

Definition 1.5.1. An **Azumaya algebra**[1] over a field k is a k-algebra A (associative and with 1, but possibly noncommutative) such that $A \otimes_k k_{\mathrm{s}}$ is isomorphic as a k_{s}-algebra to the matrix algebra $\mathrm{M}_n(k_{\mathrm{s}})$ for some $n \geq 1$.

Equivalent definitions are given in Proposition 1.5.2. Some of these definitions require additional terminology, which we now provide. Let A be a (possibly noncommutative) k-algebra. Then A is said to be **finite-dimensional** if and only if the dimension of A as a k-vector space is finite. We say that A is **central** if and only if its center is the image of k in A. Finally, A is **simple** if and only if A has exactly two 2-sided ideals, namely 0 and A.

Proposition 1.5.2 (Characterizations of Azumaya algebras)**.** *The following conditions on a k-algebra A are equivalent:*

(i) *There exists a finite separable extension $L \supseteq k$ such that the L-algebra $A \otimes_k L$ is isomorphic to the matrix algebra $\mathrm{M}_n(L)$ for some $n \geq 1$.*
(ii) *The k_{s}-algebra $A \otimes_k k_{\mathrm{s}}$ is isomorphic to the matrix algebra $\mathrm{M}_n(k_{\mathrm{s}})$ for some $n \geq 1$; i.e., A is an Azumaya algebra over k.*
(iii) *There exists a field extension $L \supseteq k$ such that the L-algebra $A \otimes_k L$ is isomorphic to the matrix algebra $\mathrm{M}_n(L)$ for some $n \geq 1$.*
(iv) *The algebra A is a finite-dimensional central simple algebra over k.*
(v) *There is a k-algebra isomorphism $A \simeq \mathrm{M}_r(D)$ for some integer $r \geq 1$ and some finite-dimensional central* division *algebra D over k.*

In (v)*, r and D are uniquely determined by A.*

Sketch of proof. The implications (i) $\Leftrightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) and the implication (v) $\Rightarrow$ (iv) are left as Exercise 1.14. The implication (iv) $\Rightarrow$ (v) and the uniqueness of r and D are a consequence of Wedderburn's theorem [**GS06**, Theorem 2.1.3]: the idea is to choose a simple A-module M, to recover D as $\operatorname{End}_A M$, and to show that the homomorphism $A \to \operatorname{End}_D M$ is an isomorphism. The implication (v) $\Rightarrow$ (ii), or equivalently the statement that a finite-dimensional division algebra over a separably closed field is commutative, is due to Noether and Köthe (for a proof, see [**Bou12**, §13.2, Proposition 3]). □

[1] Azumaya algebras over a field are more commonly called **central simple algebras**, while the term "Azumaya algebra" is reserved for the generalization in which the field is replaced by a ring or scheme. Our reason for calling them Azumaya algebras even over a field is (1) to use a single term consistently for all bases and (2) to highlight that the property of being a twist of a matrix algebra is often more useful or relevant than the properties of being central and simple.

Unofficial version for incidental online use

Let $\mathbf{Az}_k$ be the category of Azumaya algebras over k, with k-algebra homomorphisms as the morphisms. Each A of dimension d can be described by d^3 elements of k expressing the product of each pair from a basis in terms of the basis. It follows that the isomorphism classes in $\mathbf{Az}_k$ form a set (in the universe $\mathcal{U}$ we are working in, as in Appendix A), in contrast with, say, the category of isomorphism classes of arbitrary k-algebras, which is too large to be a set (in $\mathcal{U}$).

The **opposite algebra** A^{opp} of A is the k-algebra with the same underlying k-vector space structure, but with multiplication $\cdot$ defined by $a \cdot b = ba$, the reverse of the original multiplication.

Proposition 1.5.3.

(i) *If $A \in \mathbf{Az}_k$, then $A^{\mathrm{opp}} \in \mathbf{Az}_k$.*

(ii) *If $A, B \in \mathbf{Az}_k$, then $A \otimes_k B \in \mathbf{Az}_k$.*

(iii) *If $A \in \mathbf{Az}_k$ and L is a field extension of k, then $A \otimes_k L \in \mathbf{Az}_L$.*

Proof. We leave this as Exercise 1.15. $\square$

Definition 1.5.4. A **quaternion algebra** over k is a 4-dimensional Azumaya algebra over k.

1.5.2. Splitting fields.

Definition 1.5.5. An Azumaya algebra A is called **split** if it is isomorphic to $\mathrm{M}_n(k)$. A field L such that the L-algebra $A \otimes_k L$ is isomorphic to $\mathrm{M}_n(L)$ for some $n \geq 1$ is called a **splitting field** for A, and then one says that L **splits** A.

Proposition 1.5.6. *Let $A \in \mathbf{Az}_k$. Let L be a field with $k \subseteq L \subseteq A$. Then $[L : k]^2 \leq [A : k]$. If equality holds, then L splits A.*

Proof. Let $n = [L : k]$. View A as a right L-vector space; let r be its dimension. Left multiplication by any $a \in A$ defines an L-endomorphism $A \to A$. Thus we obtain a k-algebra homomorphism $A \otimes_k L \to \operatorname{End}_L A \simeq \mathrm{M}_r(L)$. Since $A \otimes_k L$ is simple, this homomorphism is injective. Thus

$$rn = [A : k] = [A \otimes_k L : L] \leq [\mathrm{M}_r(L) : L] = r^2.$$

Multiply the inequality $rn \leq r^2$ by n/r to obtain $n^2 \leq rn = [A : K]$. If equality holds, then $A \otimes_k L \to \operatorname{End}_L A \simeq \mathrm{M}_r(L)$ must have been an isomorphism. $\square$

Proposition 1.5.7. *Let D be a central division algebra of degree r^2 over a field k. Then D contains a degree r separable field extension $L \supseteq k$.*

Proof. See [**GS06**, Proposition 4.5.4]. $\square$

Unofficial version for incidental online use

1.5.3. Reduced norm and reduced trace. If $A \in \mathbf{Az}_k$, the composition nr_ι of an isomorphism $\iota\colon A \otimes_k k_{\mathrm{s}} \xrightarrow{\sim} \mathrm{M}_r(k_{\mathrm{s}})$ with the determinant map $\mathrm{M}_r(k_{\mathrm{s}}) \to k_{\mathrm{s}}$ is independent of the choice of ι, since any two ι's differ by a k_{s}-algebra automorphism of $\mathrm{M}_r(k_{\mathrm{s}})$, and any such automorphism is given by conjugation by an element of $\mathrm{GL}_r(k_{\mathrm{s}})$. (More generally, any automorphism of an Azumaya algebra over a field is inner, i.e., conjugation by a unit. Even more generally, the **Skolem–Noether theorem** [**GS06**, Theorem 2.7.2] states that for any two k-algebra homomorphisms f, g from a simple k-algebra A to an Azumaya k-algebra B, there exists $b \in B^\times$ such that $f(x) = b\,g(x)\,b^{-1}$ for all $x \in A$.)

If $\sigma \in \mathfrak{G}_k$, then σ acts on $A \otimes_k k_{\mathrm{s}}$ (through the second factor) and on $\mathrm{M}_r(k_{\mathrm{s}})$ (entry-by-entry), so we get a k_{s}-algebra isomorphism ${}^\sigma\iota$, characterized by the fact that it makes the diagram

$$\begin{tikzcd}
A \otimes_k k_{\mathrm{s}} \arrow[r, "\iota"] \arrow[d, "\sigma"'] & \mathrm{M}_r(k_{\mathrm{s}}) \arrow[d, "\sigma"] \\
A \otimes_k k_{\mathrm{s}} \arrow[r, dotted, "{}^\sigma\iota"] & \mathrm{M}_r(k_{\mathrm{s}})
\end{tikzcd}$$

commute. The independence of nr_ι on ι implies that $\mathrm{nr} := \mathrm{nr}_\iota$ is $\mathfrak{G}_k$-equivariant, meaning that ${}^\sigma\mathrm{nr}(x) = \mathrm{nr}({}^\sigma x)$ for all $\sigma \in \mathfrak{G}_k$ and $x \in A \otimes_k k_{\mathrm{s}}$. By Galois theory, nr restricts to a multiplicative map $\mathrm{nr} = \mathrm{nr}_{A/k}\colon A \to k$, called the **reduced norm**. It restricts further to a group homomorphism $A^\times \to k^\times$.

Similarly, one can define the **reduced trace** $\mathrm{tr}_{A/k}\colon A \to k$, by using the trace instead of the determinant. It is a k-linear map.

Example 1.5.8. Let $k = \mathbb{R}$, and let $A = \mathbb{H}$ be Hamilton's ring of quaternions, which is a 4-dimensional $\mathbb{R}$-algebra generated by i and j satisfying $i^2 = -1$, $j^2 = -1$, and $ji = -ij$. There is a $\mathbb{C}$-algebra isomorphism $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\sim} \mathrm{M}_2(\mathbb{C})$ sending $\alpha \otimes 1$ to left-multiplication-by-α on the right $\mathbb{R}(i)$-vector space $\mathbb{H} = \mathbb{R}(i) \oplus j\mathbb{R}(i)$ with basis $1, j$. Explicitly, we have

$$\begin{aligned}
\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} &\xrightarrow{\sim} \mathrm{M}_2(\mathbb{C}) \\
1 \otimes 1 &\longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
i \otimes 1 &\longmapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\
j \otimes 1 &\longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\
ij \otimes 1 &\longmapsto \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.
\end{aligned}$$

Unofficial version for incidental online use

If $\alpha = a + bi + cj + dij$, where $a, b, c, d \in \mathbb{R}$, then

$$\mathrm{nr}_{\mathbb{H}/\mathbb{R}}(\alpha) = \det \begin{pmatrix} a+bi & -c-di \\ c-di & a-bi \end{pmatrix} = a^2 + b^2 + c^2 + d^2,$$

$$\mathrm{tr}_{\mathbb{H}/\mathbb{R}}(\alpha) = \mathrm{tr} \begin{pmatrix} a+bi & -c-di \\ c-di & a-bi \end{pmatrix} = 2a.$$

1.5.4. Definition of the Brauer group. Call two elements $A, B \in \mathbf{Az}_k$ **similar** (or **Brauer equivalent**), and write $A \sim B$, if either of the following equivalent conditions holds:

(1) There exist $m, n \geq 1$ and a division algebra $D \in \mathbf{Az}_k$ such that $A \simeq \mathrm{M}_m(D)$ and $B \simeq \mathrm{M}_n(D)$ as k-algebras.

(2) There exist $m, n \geq 1$ such that $\mathrm{M}_n(A) \simeq \mathrm{M}_m(B)$ as k-algebras.

Define $\mathrm{Br}\, k$ as the set $\mathbf{Az}_k /\!\sim$ of similarity classes. It turns out that the operations $(A, B) \mapsto A \otimes_k B$ and $A \mapsto A^{\mathrm{opp}}$ on $\mathbf{Az}_k$ induce the multiplication and inverse maps for a group structure on $\mathrm{Br}\, k$. The abelian group $\mathrm{Br}\, k$ is called the **Brauer group** of k. (Equivalently, but slightly less elegantly, one can define $\mathrm{Br}\, k$ as the set of isomorphism classes of finite-dimensional central *division* algebras over k, and define the product of D and D' to be the division algebra D'' such that $D \otimes_k D' \simeq \mathrm{M}_n(D'')$ for some $n \geq 1$.)

If L is a field extension of k, then $A \mapsto A \otimes_k L$ induces a group homomorphism $\mathrm{Br}\, k \to \mathrm{Br}\, L$. In fact, Br is a covariant functor from fields to abelian groups.

1.5.5. Cohomological interpretation of the Brauer group.

Proposition 1.5.9. *For each $r \geq 1$, there is a natural injection*

$$\frac{\{\text{Azumaya } k\text{-algebras of dimension } r^2\}}{k\text{-isomorphism}} \quad \hookrightarrow \quad \mathrm{H}^1(\mathfrak{G}_k, \mathrm{PGL}_r(k_{\mathrm{s}})).$$

Proof. Let $A \in \mathbf{Az}_k$ be such that $[A : k] = r^2$. Choose a k_{s}-algebra isomorphism $\phi\colon \mathrm{M}_r(k_{\mathrm{s}}) \xrightarrow{\sim} A \otimes_k k_{\mathrm{s}}$. As in Section 1.5.3, $\mathfrak{G}_k$ acts on such isomorphisms. Define

$$\xi_\sigma := \phi^{-1}\left({}^\sigma\phi\right) \in \mathrm{Aut}_{k_{\mathrm{s}}\text{-algebras}}(\mathrm{M}_r(k_{\mathrm{s}})) \simeq \mathrm{PGL}_r(k_{\mathrm{s}});$$

the last isomorphism is due to the fact that every automorphism of a matrix algebra is inner. If $\sigma, \tau \in \mathfrak{G}_k$, then

$$\xi_{\sigma\tau} = \phi^{-1}\left({}^{\sigma\tau}\phi\right) = \phi^{-1}\left({}^\sigma\phi\right)\left({}^\sigma\phi^{-1}\right)\left({}^{\sigma\tau}\phi\right) = \phi^{-1}\left({}^\sigma\phi\right) \cdot {}^\sigma\!\left(\phi^{-1}\left({}^\tau\phi\right)\right) = \xi_\sigma \cdot {}^\sigma\xi_\tau.$$

In other words, ξ is a 1-cocycle. Changing ϕ (i.e., composing ϕ with an automorphism of $\mathrm{M}_r(k_{\mathrm{s}})$) changes ξ to a cohomologous cocycle, so we get an element of $\mathrm{H}^1(\mathfrak{G}_k, \mathrm{PGL}_r(k_{\mathrm{s}}))$ depending only on A.

Unofficial version for student online use

Finally, we must prove that the map just defined is injective. Suppose that $A, B \in \mathbf{Az}_k$ satisfy $[A : k] = [B : k] = r^2$, and that choices of $\phi\colon \mathrm{M}_r(k_\mathrm{s}) \xrightarrow{\sim} A \otimes_k k_\mathrm{s}$ and $\psi\colon \mathrm{M}_r(k_\mathrm{s}) \xrightarrow{\sim} B \otimes_k k_\mathrm{s}$ give rise to cohomologous cocycles. Then, after changing ψ, the cocycles become *equal*: $\phi^{-1}({}^\sigma\phi) = \psi^{-1}({}^\sigma\psi)$ for all $\sigma \in \mathfrak{G}_k$. Rewriting this as $\psi\phi^{-1} = \left(\psi\phi^{-1}\right)^\sigma$ shows that the k_s-algebra isomorphism $\psi\phi^{-1}\colon A \otimes_k k_\mathrm{s} \xrightarrow{\sim} B \otimes_k k_\mathrm{s}$ restricts to a k-algebra isomorphism $A \xrightarrow{\sim} B$. □

Remark 1.5.10. In fact, the injection of Proposition 1.5.9 is a bijection. This is an elementary special case of descent theory, Theorem 4.5.2 in particular: an Azumaya algebra of dimension r^2 is the same thing as a twist of the matrix algebra $\mathrm{M}_r(k)$.

Taking cohomology of the short exact sequence of $\mathfrak{G}_k$-modules

$$1 \to {k_\mathrm{s}}^\times \to \mathrm{GL}_r(k_\mathrm{s}) \to \mathrm{PGL}_r(k_\mathrm{s}) \to 1$$

and applying Proposition 1.3.15(iii) gives a map of pointed sets

$$\mathrm{H}^1(\mathfrak{G}_k, \mathrm{PGL}_r(k_\mathrm{s})) \to \mathrm{H}^2(\mathfrak{G}_k, {k_\mathrm{s}}^\times). \tag{1.5.11}$$

The latter is denoted $\mathrm{H}^2(k, \mathbb{G}_m)$. Composing Proposition 1.5.9 with (1.5.11) lets us associate to each $A \in \mathbf{Az}_k$ an element $[A] \in \mathrm{H}^2(k, \mathbb{G}_m)$.

Theorem 1.5.12. *The map taking each $A \in \mathbf{Az}_k$ to the associated element of $\mathrm{H}^2(k, \mathbb{G}_m)$ induces an isomorphism of abelian groups $\operatorname{Br} k \xrightarrow{\sim} \mathrm{H}^2(k, \mathbb{G}_m)$.*

Proof. See [**Ser79**, Chapter X, §5]. □

Proposition 1.5.13. *Let k be a field.*

(i) *If $\operatorname{char} k \nmid n$, then $\mathrm{H}^1(k, \mu_n) \simeq k^\times/k^{\times n}$.*
(ii) *If $\operatorname{char} k \nmid n$, then $\mathrm{H}^2(k, \mu_n) \simeq (\operatorname{Br} k)[n]$.*
(iii) *For any Galois extension $L \supseteq k$ of fields,*

$$\mathrm{H}^2(\mathrm{Gal}(L/k), L^\times) \simeq \ker\left(\operatorname{Br} k \to \operatorname{Br} L\right).$$

Proof.

(i) Take the long exact sequence of cohomology associated to

$$0 \to \mu_n \to {k_\mathrm{s}}^\times \to {k_\mathrm{s}}^\times \to 0$$

and apply Hilbert's theorem 90.
(ii) Same proof as (i), but using Theorem 1.5.12.
(iii) Since $\mathrm{H}^1(L, \mathbb{G}_m) = 0$ by (ii), we get an inflation-restriction sequence for H^2,

$$0 \longrightarrow \mathrm{H}^2(\mathrm{Gal}(L/k), L^\times) \xrightarrow{\text{inf}} \mathrm{H}^2(k, \mathbb{G}_m) \xrightarrow{\text{res}} \mathrm{H}^2(L, \mathbb{G}_m).$$

Unofficial version for incidental online use

(To construct this sequence and prove it is exact, one can either use cocycles explicitly or deduce it from the Hochschild–Serre spectral sequence; see Corollary 6.7.4.) Now apply Theorem 1.5.12 to the two groups on the right. □

Remark 1.5.14. Parts (i) and (ii) of Proposition 1.5.13 can be generalized to the case where $\operatorname{char} k \mid n$, but in place of Galois cohomology one must use the fppf cohomology to be introduced in Section 6.4.1.

1.5.6. Period and index.

Definition 1.5.15. The **index** of a finite-dimensional central division algebra D over k is $\sqrt{[D:k]}$, which is a positive integer by Proposition 1.5.2. More generally, the index of $\mathrm{M}_r(D)$ is defined to be the index of D. This makes index a well-defined function $\operatorname{Br} k \to \mathbb{Z}_{>0}$.

Definition 1.5.16. The **period** of an element $A \in \mathbf{Az}_k$ (or of its class $[A]$) is the order of $[A]$ in $\operatorname{Br} k$.

Proposition 1.5.17. *If A is an Azumaya algebra of dimension r^2 over k, then $r[A] = 0$ in $\operatorname{Br} k$. In other words, period divides index.*

Proof. Write $A \simeq \mathrm{M}_n(D)$ for a central division algebra D over k. Then $[D:k]$ divides $[A:k]$, and A and D have the same period and the same index, so we may reduce to the case that A is a central division algebra D. By Proposition 1.5.7, D contains a degree r separable field extension $L \supseteq k$. By Proposition 1.5.6, L is a splitting field for D. Then $[D] \in \ker(\operatorname{Br} k \to \operatorname{Br} L)$. By Exercise 1.19, we have $r[D] = 0$.

For a different proof, see the proof of Theorem 6.6.17(ii). □

Remark 1.5.18. If k is a local or global field, every element of $\operatorname{Br} k$ has period equals index (Theorems 1.5.34(iv) and 1.5.36(iv)), so the injection $\mathrm{H}^1(\mathfrak{G}_k, \mathrm{PGL}_r(k_s)) \to (\operatorname{Br} k)[r]$ is a bijection for each $r \geq 1$.

Warning 1.5.19. For general k, the image of $\mathrm{H}^1(\mathfrak{G}_k, \mathrm{PGL}_r(k_s)) \hookrightarrow \operatorname{Br} k$ need not even be a subgroup! For example, if $r = 2$, the image consists of the classes of quaternion algebras, but a tensor product of quaternion algebras can be a division algebra, in which case it is not similar to another quaternion algebra. Explicitly, if k_0 is a field of characteristic not 2, and $k = k_0(t_1, t_2, t_3, t_4)$, then the k-algebra $(t_1, t_2) \otimes (t_3, t_4)$ (in the notation of Section 1.5.7.4) turns out to be a division algebra [**GS06**, Example 1.5.7]. Its period is 2, but its index is 4.

1.5.7. Cyclic algebras.

Unofficial version for incidental online use

1.5.7.1. *Cyclic algebras from cyclic fields.* Let $L \supseteq k$ be a degree n cyclic extension of fields. Given $a \in k^\times$ and a generator σ of $\operatorname{Gal}(L/k)$, we construct a k-algebra as follows. Let $L[x]_\sigma$ denote the twisted polynomial ring having the same additive group as $L[x]$, but whose multiplication is defined so that $x\ell = ({}^\sigma\ell)\,x$. Let A be the quotient of $L[x]_\sigma$ by the ideal generated by the central element $x^n - a$. Then one can show that $A \in \mathbf{Az}_k$; see Exercise 1.20.

1.5.7.2. *Cyclic algebras from étale algebras.* One can generalize the construction by allowing L to be only an étale k-algebra instead of a field extension.

Start with an element $a \in k^\times$ and a continuous homomorphism $\chi\colon \mathfrak{G}_k \to \mathbb{Z}/n\mathbb{Z}$. Let $S = \mathbb{Z}/n\mathbb{Z}$, and let each $g \in \mathfrak{G}_k$ act on S by $s \mapsto s + \chi(g)$. By Theorem 1.3.2, S corresponds to an étale k-algebra L, and the automorphism $s \mapsto s+1$ of the $\mathfrak{G}_k$-set S corresponds to a k-algebra automorphism σ of L. As in Section 1.5.7.1, form $A := L[x]_\sigma/(x^n - a)$. Again it turns out that $A \in \mathbf{Az}_k$; see Exercise 1.20.

Definition 1.5.20. The k-algebra A just constructed, or its class in $\operatorname{Br} k$, is denoted (a, χ). Such an algebra is called a **cyclic algebra**.

One advantage of allowing L to be an étale algebra instead of insisting on a field is that now if A is a cyclic algebra over k, and $k' \supseteq k$ is a field extension, then $A \otimes_k k'$ is a cyclic algebra over k'.

1.5.7.3. *First cohomological interpretation.* The construction of (a, χ) can also be understood cohomologically. For simplicity, suppose that $\chi\colon \mathfrak{G}_k \to \mathbb{Z}/n\mathbb{Z}$ is surjective, or equivalently that L is a field. Let $G = \operatorname{Gal}(L/k)$, so χ induces $\chi\colon G \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$. By definition of Tate cohomology, $\widehat{\mathrm{H}}^0(G, L^\times) = k^\times/N_{L/k}(L^\times)$, and we may consider the image of a in this group. The generator $\sigma = \chi^{-1}(1)$ of G determines a generator u of the cyclic group $\widehat{\mathrm{H}}^2(G, \mathbb{Z})$, and "cup product with u" gives an isomorphism $\widehat{\mathrm{H}}^0(G, L^\times) \xrightarrow{\sim} \widehat{\mathrm{H}}^2(G, L^\times)$ [**AW67**, §8, Theorem 5]. The latter is isomorphic to $\ker(\operatorname{Br} k \to \operatorname{Br} L)$ by Proposition 1.3.15(iii), and one can show that the composition

$$k^\times \twoheadrightarrow \widehat{\mathrm{H}}^0(G, L^\times) \xrightarrow{\sim} \widehat{\mathrm{H}}^2(G, L^\times) \hookrightarrow \operatorname{Br} k, \tag{1.5.21}$$

maps any $a \in k^\times$ to the class of the cyclic algebra (a, χ), maybe with a sign error, depending on the definition of u. The following two propositions are consequences of this.

Proposition 1.5.22. *Let L and χ be as above. Suppose that $A \in \mathbf{Az}_k$ and that $[A : k] = [L : k]^2$. Then A is split by L if and only if $A \simeq (a, \chi)$ for some $a \in k^\times$.*

Proof. By (1.5.21), A is split by L if and only if it is similar to (a, χ) for some $a \in k^\times$. But A and (a, χ) have the same dimension, so similar is equivalent to isomorphic. $\square$

Unofficial version for incidental online use

Proposition 1.5.23. *Let L and χ be as above. For $a \in k^\times$, the k-algebra (a, χ) is split if and only if $a \in N_{L/k}(L^\times)$.*

Proof. The kernel of the composite homomorphism in (1.5.21) equals the kernel of the first homomorphism, which is $N_{L/k}(L^\times)$. □

1.5.7.4. *Second cohomological interpretation.* We can give a another cohomological interpretation of (a, χ), at least when $\operatorname{char} k \nmid n$. The element a can be mapped to an element of $k^\times/k^{\times n} \xrightarrow{\sim} \mathrm{H}^1(k, \mu_n)$. On the other hand, $\chi \in \operatorname{Hom}(\mathfrak{G}_k, \mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{H}^1(k, \mathbb{Z}/n\mathbb{Z})$. Under the cup product

$$\mathrm{H}^1(k, \mu_n) \times \mathrm{H}^1(k, \mathbb{Z}/n\mathbb{Z}) \to \mathrm{H}^2(k, \mu_n) \simeq (\operatorname{Br} k)[n],$$

a and χ pair to give an element of $(\operatorname{Br} k)[n]$, which turns out to be the class of the cyclic algebra (a, χ), at least up to a sign.

Suppose now that $\operatorname{char} k \nmid n$ and that k contains a primitive nth root of unity, ζ. Then ζ determines an isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mu_n$ of $\mathfrak{G}_k$-modules, so we get an isomorphism $\mathrm{H}^1(k, \mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{H}^1(k, \mu_n) \simeq k^\times/k^{\times n}$. Now given $a, b \in k^\times$, we can take the cup product of their images under

$$\mathrm{H}^1(k, \mu_n) \times \mathrm{H}^1(k, \mathbb{Z}/n\mathbb{Z}) \to \mathrm{H}^2(k, \mu_n) \simeq (\operatorname{Br} k)[n]$$

to get an element of $\operatorname{Br} k$. Alternatively, from a and the étale k-algebra $L = k[t]/(t^n - b)$ equipped with the automorphism σ mapping t to ζt, one can construct a cyclic algebra $(a, b)_\zeta \in \mathbf{Az}_k$ representing the element of $\operatorname{Br} k$ defined in the previous sentence. When $n = 2$, one writes simply (a, b) for $(a, b)_{-1}$.

Remark 1.5.24. Exercise 1.23 shows that every quaternion algebra is cyclic. In particular, if $\operatorname{char} k \neq 2$, then every quaternion algebra D over k is of the form (a, b) for some $a, b \in k^\times$: this algebra has a k-basis $1, i, j, ij$ where $i^2 = a$, $j^2 = b$, and $ji = -ij$. (The elements a and b are not uniquely determined by D.)

1.5.8. Connections with the C_r property and cohomological dimension.

Proposition 1.5.25. *Let k be a field. The following eight conditions are equivalent:*

(i) $\operatorname{cd} k \leq 1$, *and if* $\operatorname{char} k = p > 0$, *then* $(\operatorname{Br} K)[p^\infty] = 0$ *for every algebraic extension K of k.*

(ii) $\operatorname{Br} K = 0$ *for every algebraic extension K of k.*

(iii) *If K is an algebraic extension of k and L/K is a finite Galois extension, then* $\mathrm{H}^q(\operatorname{Gal}(L/K), L^\times) = 0$ *for all $q \geq 1$.*

Unofficial version for nondental online use

(iv) *If K is an algebraic extension of k and L/K is a finite Galois extension, then $N_{L/K}\colon L^\times \to K^\times$ is surjective.*

(i′), (ii′), (iii′), (iv′): *Same as* (i),...,(iv), *but restricted to extensions K that are finite and separable over k.*

Proof. See [**Ser02**, II.§3.1, Proposition 5]. □

Definition 1.5.26. A field k is said to be **of dimension** ≤ 1 if it satisfies the equivalent conditions of Proposition 1.5.25. We then write $\dim k \leq 1$.

Warning 1.5.27. This has nothing to do with the Krull dimension, which is 0 for any field k.

Proposition 1.5.28. *If k is C_1, then* $\operatorname{Br} k = 0$.

Proof. Let D be a finite-dimensional central division algebra over k, so $[D : k] = r^2$ for some $r \geq 1$. An associated reduced norm form is of degree r in r^2 variables and has no nontrivial zero. This contradicts the C_1 property unless $r = 1$. This holds for all D, so $\operatorname{Br} k = 0$. □

Corollary 1.5.29. *If k is C_1, then k is of dimension ≤ 1.*

Proof. We check condition (ii) in Proposition 1.5.25. Let k be C_1. Any algebraic extension K of k is C_1 by Theorem 1.2.7(i), and hence it satisfies $\operatorname{Br} K = 0$ by Proposition 1.5.28. □

Warning 1.5.30. The converse to Corollary 1.5.29 is false. See [**Ser02**, p. 80] for a counterexample, due to Ax [**Ax65**]. In fact, Ax finds a field of dimension ≤ 1 that is not C_r for any r.

Remark 1.5.31. Serre wrote in [**Ser02**, p. 88] that it is probable that for all $r \geq 0$, all C_r fields satisfy $\operatorname{cd} k \leq r$. This is true for $r \leq 2$ (the $r = 2$ case is a theorem of Merkurjev and Suslin). Moreover, [**OVV07**] shows that C_r fields of characteristic 0 satisfy $\operatorname{cd}_2 k \leq r$.

1.5.9. Examples.

Theorem 1.5.32 (Wedderburn)**.** *If k is a finite field, then* $\operatorname{Br} k = 0$.

Proof. The Chevalley–Warning theorem says that k is C_1. Apply Proposition 1.5.28. □

Theorem 1.5.33 (original form of Tsen's theorem)**.** *If k is a field of transcendence degree* 1 *over an algebraically closed field, then* $\operatorname{Br} k = 0$.

Proof. Again k is C_1, so apply Proposition 1.5.28. □

Unofficial version for incidental online use

Theorem 1.5.34 (Brauer group of a local field)**.** *Suppose that k is a local field.*

(i) *There is an injection* $\operatorname{inv}\colon \operatorname{Br} k \to \mathbb{Q}/\mathbb{Z}$, *whose image is*

$$\begin{cases} \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \text{if } k = \mathbb{R}, \\ 0 & \text{if } k = \mathbb{C}, \\ \mathbb{Q}/\mathbb{Z} & \text{if } k \text{ is nonarchimedean.} \end{cases}$$

(ii) *If L is a finite extension of k, then the diagram*

$$\begin{array}{ccc} \operatorname{Br} k & \xrightarrow{\operatorname{inv}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow & & \downarrow{\scriptstyle [L:k]} \\ \operatorname{Br} L & \xrightarrow{\operatorname{inv}} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{1.5.35}$$

commutes.

(iii) *Every Azumaya algebra over k is cyclic.*

(iv) *Every element of* $\operatorname{Br} k$ *has period equal to index.*

Proof. The cases where k is $\mathbb{R}$ or $\mathbb{C}$ are easy, so assume that k is nonarchimedean.

(i) If $\mathbb{F}$ is the residue field of k, one shows that $\operatorname{Br} k \simeq \mathrm{H}^1(\mathbb{F}, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}$; see [**Ser67**, bottom of p. 130].

(ii) See [**Ser67**, Theorem 3].

(iii) Let $m/n \in \mathbb{Q}$ be a rational number in lowest terms, with $n \geq 1$. Let L be the degree n unramified extension of k. Let $\sigma \in \operatorname{Gal}(L/k)$ be the Frobenius automorphism. Choose $a \in k^\times$ of valuation m. By [**Ser67**, p. 138], the cyclic algebra $A := L[x]_\sigma/(x^n - a)$ is a division algebra with $\operatorname{inv} A = m/n \in \mathbb{Q}/\mathbb{Z}$. These m/n cover all possible invariants, so every Azumaya algebra is a matrix algebra over one of these and is cyclic by Exercise 1.24.

(iv) Each A in (iii) has period equal to index. $\square$

If $L \supseteq k$ is a finite extension of global fields, we write $w|v$ to mean that the place w of L lies over the place v of k; in this case, the inclusion $k_v \hookrightarrow L_w$ gives rise to a homomorphism $\operatorname{Br} k_v \to \operatorname{Br} L_w$.

Theorem 1.5.36 (Brauer group of a global field)**.** *Suppose that k is a global field. For each place v of k, let k_v be the completion of k at v, and let* $\operatorname{inv}_v\colon \operatorname{Br} k_v \hookrightarrow \mathbb{Q}/\mathbb{Z}$ *be the injection associated to the local field k_v.*

Unofficial version for incidental online use

(i) *Then the sequence*

$$0 \longrightarrow \operatorname{Br} k \longrightarrow \bigoplus_v \operatorname{Br} k_v \xrightarrow{\sum \operatorname{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0$$

is exact.

(ii) *If L is a finite extension of k, then the diagram*

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Br} k \arrow[r] \arrow[d] & \bigoplus_v \operatorname{Br} k_v \arrow[r, "\sum \operatorname{inv}_v"] \arrow[d] & \mathbb{Q}/\mathbb{Z} \arrow[r] \arrow[d, "{[L:k]}"] & 0 \\ 0 \arrow[r] & \operatorname{Br} L \arrow[r] & \bigoplus_v \bigoplus_{w|v} \operatorname{Br} L_w \arrow[r, "\sum \operatorname{inv}_w"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

commutes.

(iii) *Every Azumaya algebra over k is cyclic.*

(iv) *Every element of* $\operatorname{Br} k$ *has period equal to index.*

Proof.

(i) This follows from [**Tat67**, diagram (9) in Section 11.2, together with Proposition 7.3(b) and Section 11.2(bis)].

(ii) Compare [**Tat67**, diagram (7) in Section 11.2]. The commutativity of the left square follows from functoriality of Br. The commutativity of the right square follows from the identity $\sum_{w|v}[L_w : k_v] = [L : k]$.

(iii) By Exercise 1.24, it suffices to consider a central *division* algebra A over k. Let n be the order of $[A] \in \operatorname{Br} k$. Let S be the finite set of places v such that $\operatorname{inv}_v A \neq 0$. The Grunwald–Wang theorem produces a degree n cyclic extension $L \supseteq k$ such that each local degree $[L_w : k_v]$ above a place $v \in S$ is n if v is nonarchimedean, and is 2 if v is real; see [**AT67**, Chapter 10, Theorem 5]. By Theorem 1.5.34(ii), all local invariants of $A \otimes_k L$ are 0. By the injectivity of the first homomorphism in (i), the extension L splits A. Now

$$n = (\text{period of } A) \leq (\text{index of } A) \leq [L : k] = n, \tag{1.5.37}$$

so equality holds everywhere. In particular, $[A : k] = [L : k]^2$, so A is cyclic by Proposition 1.5.22.

(iv) This follows from the equality in (1.5.37). □

Theorems 1.5.34 and 1.5.36 are byproducts of the cohomological proofs of local and global class field theory; it seems that they cannot be proved without effectively doing a large part of the work toward class field theory.

Unofficial version for incidental online use

Theorem 1.5.38 (Faddeev). *Suppose that k is any field and $K = k(t)$. There is an exact sequence*

$$0 \longrightarrow \operatorname{Br} k \longrightarrow \operatorname{Br} K \xrightarrow{\text{res}} \bigoplus_{f} \mathrm{H}^1\left(k[t]/(f), \mathbb{Q}/\mathbb{Z}\right) \longrightarrow 0,$$

where f ranges over all monic irreducible polynomials in $k[t]$, with the caveat that one must exclude the p-primary parts if k is imperfect of characteristic p.

Proof. See [**Ser02**, II.Appendix.§5] and [**GS06**, 6.4.5] for a proof and a generalization. □

Remark 1.5.39. It is perhaps more natural to let the direct sum range over all closed points of $\mathbb{P}^1_k$. This adds one summand to the direct sum, so one must also add a new term $\mathrm{H}^1(k, \mathbb{Q}/\mathbb{Z})$ to the end of the sequence; the result is a four-term exact sequence.

Theorem 1.5.38 is related to Theorems 6.8.3 and 6.9.7.

Exercises

1.1. (a) Prove that an algebraic extension of a separably closed field is separably closed.
(b) Prove that an algebraic extension of a perfect field is perfect.
(c) Let k be a field. Prove that $\overline{k} = (k_{\mathrm{s}})^{\mathrm{perf}} = (k^{\mathrm{perf}})_{\mathrm{s}} = k^{\mathrm{perf}} \cdot k_{\mathrm{s}}$. (The last expression denotes the subfield of $\overline{k}$ generated by k^{perf} and k_{s}.)

1.2. Let k be a global or local field. Prove that k is perfect if and only if $\operatorname{char} k = 0$.

1.3. For which $r \in \mathbb{R}_{\geq 0}$ is C_r equivalent to being algebraically closed?

1.4. (a) For each finite field $\mathbb{F}_q$ and nonnegative integer n, evaluate the sum $\sum_{a \in \mathbb{F}_q} a^n$.
(b) Prove the Chevalley–Warning theorem, that every finite field $\mathbb{F}_q$ is C_1. (*Hint*: Given a homogeneous polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree $d < n$, evaluate

$$\sum_{(a_1,\ldots,a_n) \in (\mathbb{F}_q)^n} \left(1 - f(a_1, \ldots, a_n)^{q-1}\right) \in \mathbb{F}_q$$

in two different ways.)
(c) Using a similar method, prove directly that $\mathbb{F}_q$ is C_1', without using the paragraph following Question 1.2.11.

1.5. Let $L \supseteq k$ be a finite extension of fields, and let $r \in \mathbb{R}_{\geq 0}$. If L is C_r, must k be C_r?

Unofficial version for incidental online use

1.6. Let k be a C_1 field, and let L be a finite extension. Prove that the norm homomorphism $N_{L/k}\colon L^\times \to k^\times$ is surjective.

1.7. Let k be a field.
(a) Prove that $\{ r \in \mathbb{R}_{\geq 0} : k \text{ is } C_r \}$ has a minimum, if it is nonempty.
(b) Let $r(k)$ denote the real number in Exercise 1.7a, if it exists. Let $k(t)$ be the rational function field over k. Prove that $r(k(t)) = r(k) + 1$, in the sense that if one side is defined, then so is the other, and then they are equal.

1.8. Let k_v be a nonarchimedean completion of a number field k, and let $r \in \mathbb{R}_{\geq 0}$. Assuming (as is true) that k_v is not C_r, prove that k is not C_r.

1.9. Let $L \supseteq k$ be a finite Galois extension with Galois group G. Let $r \in \mathbb{Z}_{\geq 0}$. Given a 1-cochain (i.e., function) $\xi\colon G \to \mathrm{GL}_r(L)$, let W_ξ be L^r equipped with the function $G \times L^r \to L^r$ sending (σ, w) to $\xi_\sigma(\sigma w)$.
(a) Prove that this describes a semilinear G-action (i.e., the group action axiom $(\sigma\tau) * w = \sigma * (\tau * w)$ is satisfied) if and only if ξ is a 1-cocycle.
(b) Prove that given two 1-cocycles ξ and ξ', we have $W_\xi \simeq W_{\xi'}$ as L-vector spaces with semilinear G-action if and only if ξ and ξ' are cohomologous.

1.10. Let $L \supseteq k$ be a finite Galois extension of fields. Suppose that $\mathrm{Gal}(L/k)$ is cyclic, generated by σ. The original Hilbert theorem 90 proved by Hilbert stated that if $a \in L^\times$ satisfies $N_{L/k}(a) = 1$, then there exists $b \in L^\times$ such that $a = \frac{\sigma b}{b}$. Explain why Proposition 1.3.15(ii) is a generalization of this.

1.11. Use the original Hilbert theorem 90 to prove that if $x, y \in \mathbb{Q}$ satisfy $x^2 + y^2 = 1$, then there exist $u, v \in \mathbb{Q}$ not both 0 such that

$$(x, y) = \left(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2} \right).$$

(This can be proved also in more elementary ways.)

1.12. Let A be a torsion abelian group. Prove that $A \simeq \bigoplus_p A[p^\infty]$, where the direct sum is over all prime numbers p.

1.13. Let G be a profinite group, let p be a prime, and let $n \in \mathbb{N}$. Prove that $\mathrm{cd}_p(G) \leq n$ if and only if $\mathrm{H}^{n+1}(G, A) = 0$ for every simple G-module A killed by p. (A G-module A is **simple** if $A \neq 0$ and the only G-submodules of A are 0 and A.)

1.14. (Equivalence of definitions of Azumaya algebra) Prove the implications (i) $\Leftrightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) and the implication (v) $\Rightarrow$ (iv) of Proposition 1.5.2.

Unofficial version for incidental online use

1.15. (Properties of Azumaya algebras) Prove Proposition 1.5.3.

1.16. For a finite-dimensional k-algebra A, the usual norm $N_{A/k}\colon A \to k$ maps a to the determinant of the k-linear endomorphism of A given by $x \mapsto ax$. For $A \in \mathbf{Az}_k$, what is the relationship between $N_{A/k}$ and the reduced norm $\mathrm{nr}_{A/k}$?

1.17. Let $\{K_\alpha\}$ be a directed system of fields, and let $K = \varinjlim K_\alpha$ be the direct limit. Prove that $\operatorname{Br} K = \varinjlim \operatorname{Br} K_\alpha$.

1.18. Prove that if L is an extension of k, the diagram

$$\begin{array}{ccc} \operatorname{Br} k & \longrightarrow & \mathrm{H}^2(k, \mathbb{G}_m) \\ \downarrow & & \downarrow \\ \operatorname{Br} L & \longrightarrow & \mathrm{H}^2(L, \mathbb{G}_m) \end{array}$$

commutes.

1.19. Let $L \supseteq k$ be a field extension of degree n. Prove that the kernel of $\operatorname{Br} k \to \operatorname{Br} L$ is killed by n. (*Hint*: If $L \supseteq k$ is separable, use the identity $\operatorname{Cor} \circ \operatorname{Res} = [L : k]$ of [**AW67**, §6, Proposition 8].)

1.20. Let (a, χ) be a cyclic algebra over a field k. Prove that $(a, \chi) \in \mathbf{Az}_k$.

1.21. Let k be a field. Suppose that $\operatorname{char} k \nmid n$ and that k contains a primitive nth root of unity ζ. Show that

$$\begin{aligned} \frac{k^\times}{k^{\times n}} \times \frac{k^\times}{k^{\times n}} &\longrightarrow (\operatorname{Br} k)[n] \\ a, b &\longmapsto (a, b)_\zeta \end{aligned}$$

is an antisymmetric pairing; that is, $(b, a)_\zeta = -(a, b)_\zeta$ in $\operatorname{Br} k$.

1.22. Let D be a quaternion algebra over a field k. Let tr and nr denote the reduced trace and reduced norm for D/k. Prove that for $\alpha \in D$ one can define $\bar{\alpha} \in D$ such that the following hold:

(a) The map

$$\begin{aligned} D &\to D^{\mathrm{opp}} \\ \alpha &\mapsto \bar{\alpha} \end{aligned}$$

is a k-algebra isomorphism.

(b) $\bar{\bar{\alpha}} = \alpha$.

(c) $\mathrm{tr}(\alpha) = \mathrm{tr}(\bar{\alpha}) = \alpha + \bar{\alpha}$.

(d) $\mathrm{nr}(\alpha) = \mathrm{nr}(\bar{\alpha}) = \alpha\bar{\alpha}$.

(e) If L is an étale k-subalgebra of D and $[L : k] = 2$, then the involution $\alpha \mapsto \bar{\alpha}$ restricts to the nontrivial automorphism of L over k.

1.23. Prove that every quaternion algebra over a field is a cyclic algebra.

Unofficial version for incidental online use

1.24. Show that if A is a cyclic algebra over a field k, then so is $\mathrm{M}_r(A)$ for any $r \geq 1$.

1.25. Describe all Azumaya algebras over $\mathbb{R}$, and show that they are all cyclic algebras.

1.26. Let k be a separably closed field that is not algebraically closed. Let $p = \operatorname{char} k$.

(a) Prove that $\operatorname{Br} k(t) \neq 0$. Better yet, find an element of $\operatorname{Br} k(t)$ whose image in $\operatorname{Br} k((t))$ is nonzero.

(b) Prove that every element of $\operatorname{Br} k(t)$ is killed by some power of p.

1.27. (a) Let k be a global field, and let $a \in \operatorname{Br} k$. Prove that there is a root of unity $\zeta \in \overline{k}$ such that the image of a in $\operatorname{Br} k(\zeta)$ is 0.

(b) Let k be a global field, and let k^{ab} denote its maximal abelian extension. Prove that k^{ab} is of dimension ≤ 1. (So in particular, $\operatorname{Br} k^{\mathrm{ab}} = 0$.)

1.28. Let k be a perfect field.

(a) Prove that if $\operatorname{char} k = p > 0$, then $(\operatorname{Br} k)[p] = 0$.

(b) Prove that $\dim k \leq 1$ if and only if $\operatorname{cd} k \leq 1$.

1.29. Let k be a field.

(a) Show that if t is an indeterminate, the field $k(t)$ has a nontrivial cyclic extension of degree not divisible by $\operatorname{char} k$.

(b) Let k be a field, and let K be the purely transcendental extension $k(t_1, \ldots, t_m)$ for some $m \geq 2$. Use Theorem 1.5.38 to show that $\operatorname{Br} K$ is huge in the following sense: the cardinality of $\operatorname{Br} K$ equals the cardinality of K.

Unofficial version for incidental online use

Chapter 2

Varieties over arbitrary fields

Unofficial version for incidental online use

We refer to [**Har77**] for definitions of standard terms regarding schemes: noetherian, connected, irreducible, reduced, integral,[1] regular, finite type, separated, proper, projective, dimension, rational map, dominant.

Definition 2.0.1. If S is a scheme, an S-**scheme** (X, f) is a scheme X equipped with a morphism of schemes $f \colon X \to S$. The morphism f is called the **structure morphism**.

To simplify notation, we usually write X instead of (X, f). Sometimes it helps to think of $X \to S$ as a family of schemes, one above each point of S.

Definition 2.0.2. An S-**morphism** between S-schemes (X, f) and (Y, g) is a morphism of schemes $\phi \colon X \to Y$ such that

$$\begin{tikzcd} X \arrow[rr, "\phi"] \arrow[dr, "f"'] & & Y \arrow[dl, "g"] \\ & S & \end{tikzcd}$$

commutes.

For a scheme S, let $\mathbf{Schemes}_S$ denote the category whose objects are S-schemes and whose arrows are S-morphisms. If X and Y are S-schemes, let $\operatorname{Hom}_S(X, Y)$ denote the set of S-morphisms from X to Y.

[1]This definition should read as follows: A scheme X is **integral** if it is nonempty and for every nonempty open set $U \subseteq X$, the ring $\mathscr{O}_X(U)$ is an integral domain.

When R is a commutative ring, R may be used as an abbreviation for $\operatorname{Spec} R$; the meaning is usually clear from context. For instance, if X is a scheme (over $\operatorname{Spec} \mathbb{Z}$), then $X \times_{\mathbb{Z}} \mathbb{Q}$ means $X \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathbb{Q}$.

2.1. Varieties

Our definition of variety will be rather inclusive. If we want to consider a more restricted class of varieties, we can apply adjectives (such as "irreducible") as needed.

Definition 2.1.1. A **variety** over a field k is a separated scheme X of finite type over $\operatorname{Spec} k$.

Warning 2.1.2. In [**Har77**, II.§4], varieties must also be integral; we are not including this condition in the definition of variety.

Varieties over a field k may also be called k-**varieties**.

Definition 2.1.3. A **curve** is a variety of pure dimension 1. (**Pure** means that all the irreducible components have the same dimension.) A **surface** is a variety of pure dimension 2. A **3-fold** is a variety of pure dimension 3, and so on.

2.2. Base extension

Definition 2.2.1. If X is an S-scheme and $S' \to S$ is a morphism, then the **base extension** $X_{S'}$ is the S'-scheme $X \times_S S'$. The **base extension** of a *morphism* of S-schemes $X \to Y$ is the S'-morphism $X_{S'} \to Y_{S'}$ induced by the universal property of the fiber product $X \times_S S'$.

Recall some important applications of base extension:

- If X is a k-variety or k-scheme, and L is a field extension of k, then X_L is the scheme defined by the same equations but considered over L instead of k.
- Let X be a k-scheme, and let $\sigma \in \operatorname{Aut} k$. Then the base extension of X by the morphism $\sigma^* \colon \operatorname{Spec} k \to \operatorname{Spec} k$ induced by σ is a new k-scheme ${}^{\sigma}X$. Since σ^* is an isomorphism of schemes, ${}^{\sigma}X$ and X are isomorphic as abstract schemes, but generally they are not isomorphic as *k-schemes*. For instance, if X is an affine variety, then ${}^{\sigma}X$ can be obtained by applying σ to each coefficient in the equations defining X.

$$\begin{tikzcd}
{}^{\sigma}X \arrow[r, dotted] \arrow[d] & X \arrow[d] \\
\operatorname{Spec} k \arrow[r, dotted, "\sigma^*"] & \operatorname{Spec} k
\end{tikzcd}$$

Unofficial version for incidental online use

- Let X be an S-scheme with structure morphism $f\colon X \to S$. If U is an open subscheme of S, then X_U is also written $f^{-1}U$ since its underlying topological space is $f^{-1}U$. The same applies to closed subschemes of S.
- Let $s \in S$. Let $\mathbf{k}(s)$ be the residue field of the local ring $\mathscr{O}_{S,s}$. The scheme $S' := \operatorname{Spec} \mathbf{k}(s)$ has a natural morphism to S. The resulting scheme $X_{S'}$ may also be written X_s or $f^{-1}(s)$ since its underlying topological space is $f^{-1}(s)$. It is called the **fiber** of $X \to S$ above s [**Har77**, p. 89]. If $\mathfrak{p}$ is a prime ideal of a ring A and X is an A-scheme, then the fiber $X_{\mathfrak{p}}$ is also called the **reduction of X modulo $\mathfrak{p}$**.

Example 2.2.2 (Varieties that become isomorphic only after base field extension)**.** Let X be the affine plane curve over $\mathbb{Q}$ defined by the equation $x^2 + y^2 = 1$; that is, $X := \operatorname{Spec} \mathbb{Q}[x,y]/(x^2+y^2-1)$. Let Y be the plane curve over $\mathbb{Q}$ defined by $x^2 + y^2 = -1$. If $L = \mathbb{Q}(i)$, then $X_L \simeq Y_L$ as L-varieties. But $X \not\simeq Y$, because $\mathbb{Q}[x,y]/(x^2+y^2-1)$ admits a $\mathbb{Q}$-algebra homomorphism to $\mathbb{Q}$ while $\mathbb{Q}[x,y]/(x^2+y^2+1)$ does not.

Most properties of morphisms are preserved by base extension. Often they are defined expressly so as to make this so.

Theorem 2.2.3. *Let* blah *denote a property for which a positive answer is listed in the "base extension" column of Table 1 on pp. 302–303. If $X \to S$ is blah, then $X_{S'} \to S'$ is blah for any morphism $S' \to S$.*

$$\begin{tikzcd}
X_{S'} \arrow[r, dotted] \arrow[d, "\text{blah?}"'] & X \arrow[d, "\text{blah}"] \\
S' \arrow[r, dotted] & S
\end{tikzcd}$$

The following properties of a variety can be lost by base extension of the ground field: integral, connected, irreducible, reduced, and regular. This motivates some more definitions.

Definition 2.2.4. Let X be a scheme over a field k. Then X is said to be **geometrically integral** if and only if $X_{\overline{k}}$ is integral. Define **geometrically connected**, **geometrically irreducible**, **geometrically reduced**, and **geometrically regular** similarly.

Remark 2.2.5. When one speaks of the geometry of X, as opposed to the arithmetic of X, one is usually referring to properties of $X_{\overline{k}}$.

Example 2.2.6. Let X be the affine plane curve $x^2 - 2y^2 = 0$ over $\mathbb{Q}$. Then X is irreducible. (In fact, X is integral, since $x^2 - 2y^2$ is an irreducible element of the unique factorization domain $\mathbb{Q}[x,y]$.) But X is not geometrically irreducible, since $X_{\overline{\mathbb{Q}}}$ is the union of the closed subvarieties defined by $x + \sqrt{2}y = 0$ and $x - \sqrt{2}y = 0$.

Unofficial version for incidental online use

Example 2.2.7. Let X be the curve $y^2 = 2$ over $\mathbb{Q}$ in the (x, y)-plane. Then X is connected but not geometrically connected.

Example 2.2.8. Let k be the imperfect field $\mathbb{F}_p(t)$, where t is an indeterminate. Let X be the affine plane curve $y^p = tx^p$ over k. Then X is reduced but not geometrically reduced.

Example 2.2.9. Let L be a finite extension of a field k. View $X = \operatorname{Spec} L$ as a k-variety. Then X is integral. But if the separable degree of L over k is greater than 1 (that is, L is not purely inseparable over k), then X is neither geometrically connected nor geometrically irreducible. And if the inseparable degree of L over k is greater than 1 (that is, L is not separable over k), then X is not geometrically reduced and hence not geometrically regular.

Example 2.2.10. Regular local rings are reduced, so regular implies reduced, and geometrically regular implies geometrically reduced. So if L is a finite inseparable extension of a field k, then $\operatorname{Spec} L$ is a regular k-variety that is not geometrically regular.

For another example of a k-variety that is regular but not geometrically regular, see Example 3.5.23. That example is also geometrically integral.

2.2.1. Function fields.

Definition 2.2.11. If X is an integral finite-type k-scheme, its **function field** $\mathbf{k}(X)$ is the residue field at the generic point of X. Alternatively, $\mathbf{k}(X) := \operatorname{Frac} A$ for any affine open subset $U = \operatorname{Spec} A$ of X.

Remark 2.2.12. Suppose that X is irreducible but not necessarily reduced. Then the first part of Definition 2.2.11 still makes sense. The alternative definition must be modified slightly, however: A might not be a domain, so one should take $\operatorname{Frac}(A/\operatorname{nil}(A))$, where $\operatorname{nil}(A)$ is the nilradical of the ring A.

We can construct varieties with given function field:

Proposition 2.2.13. *Let K be a finitely generated field extension of k. Then there exists a normal projective integral k-variety X with $\mathbf{k}(X) \simeq K$.*

Proof. Let S be a finite set of generators of K as a field extension of k. Let A_0 be the k-subalgebra of K generated by S. Thus A_0 is a domain with $\operatorname{Frac} A_0 = K$. Then $X_0 := \operatorname{Spec} A_0$ is an affine integral k-variety with $\mathbf{k}(X_0) = K$. If we choose a closed immersion $X_0 \hookrightarrow \mathbb{A}^n$ and choose a standard open immersion $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$, then the Zariski closure of X_0 in $\mathbb{P}^n$ is a projective integral k-variety X_1 with $\mathbf{k}(X_1) = K$. Let X be the normalization of X_1. By [**Har77**, Exercise II.3.8], X is finite over X_1, so X is projective. The other properties are immediate. $\square$

Unofficial version for incidental online use

Remark 2.2.14. A weak form of the *resolution of singularities conjecture* states that Proposition 2.2.13 holds with "normal" replaced by the stronger condition "regular". Resolution of singularities was proved by Hironaka [**Hir64**] in the case that k has characteristic 0; see [**Kol07b**] for an exposition of a proof. In arbitrary characteristic it is known in dimension ≤ 2 (i.e., $\operatorname{tr deg}(K/k) \leq 2$); see [**Art86b**] for an exposition of a proof by Lipman [**Lip78**]. Finally, if one can tolerate replacing K by a finite extension, then one can solve the problem in general [**dJ96**]; this suffices for many applications.

2.2.2. Separable and primary field extensions. Section 2.2.3 will show that for an integral k-variety X, the properties of being geometrically irreducible, geometrically reduced, and geometrically integral are equivalent to field-theoretic properties of the extension $\mathbf{k}(X)/k$.

First we define the field-theoretic properties. The following definition of separable agrees with the usual notion for algebraic field extensions.

Definition 2.2.15. A field extension L of k is **separable** if the ring $L \otimes_k k'$ is reduced for all field extensions k' of k.

Proposition 2.2.16. *Let L be a finitely generated field extension of a field k.*

(i) *The field L is separable over k if and only if L is a finite separable extension of a purely transcendental extension $k(t_1, \ldots, t_n)$.*

(ii) *Let $n = \operatorname{tr deg}(L/k)$. Elements $t_1, \ldots, t_n$ of L generate a purely transcendental extension of k over which L is a finite separable extension if and only if $dt_1, \ldots, dt_n$ form a basis for the L-vector space $\Omega_{L/k}$ of Kähler differentials.*

Proof.

(i) See [**Mat80**, (27.F)].

(ii) See the proof of [**Mat80**, (27.B)]. □

Warning 2.2.17. If L is separable over k, then every subextension is separable over k, so in particular every finite subextension is separable over k. But there exist also inseparable field extensions L over k such that all finite subextensions are separable over k. See Exercise 2.2.

Definition 2.2.18. A field extension L of k is **primary** if the largest separable algebraic extension of k contained in L is k itself.

Purely inseparable algebraic field extensions are primary. Purely transcendental field extensions are primary and separable. For equivalent definitions of "primary" and "separable", see [**FJ08**, §2.6].

Unofficial version for incidental online use

2.2.3. Geometric properties determined by the function field.

Proposition 2.2.19. *Let X be a finite-type k-scheme. Then the following are equivalent:*

(i) *X is geometrically irreducible.*
(ii) *There is a separably closed field L containing k such that the L-scheme X_L is irreducible.*
(iii) *For all fields L containing k, the L-scheme X_L is irreducible.*
(iv) *X is irreducible, and the field extension $\mathbf{k}(X)$ of k is primary.*

Sketch of proof. See [**EGA IV**$_2$, 4.5.9]. One shows first that for a field L containing k, the L-scheme $X \times_k L$ is irreducible if and only if the scheme $\operatorname{Spec}(\mathbf{k}(X) \otimes_k L)$ is irreducible. The rest is field theory. □

Proposition 2.2.20. *Let X be a finite-type k-scheme. Then the following are equivalent:*

(i) *X is geometrically reduced.*
(ii) *There is a perfect field L containing k such that the L-scheme X_L is reduced.*
(iii) *For all fields L containing k, the L-scheme X_L is reduced.*
(iv) *X is reduced, and for each irreducible component Z of X, the field extension $\mathbf{k}(Z)$ of k is separable.*

Proof. See [**EGA IV**$_2$, 4.6.1]. □

Combining Propositions 2.2.19 and 2.2.20 leads to equivalent conditions for X to be geometrically integral.

Remark 2.2.21. The property of X being geometrically regular depends on more than the function field, even when X is assumed to be a projective integral variety over an algebraically closed field k. For instance, the cuspidal cubic curve $y^2 z = x^3$ in $\mathbb{P}^2_k$ is not regular at $(0:0:1)$, but it has the same function field as $\mathbb{P}^1_k$, which is regular.

2.2.4. The constant field of a function field. Let K be a finitely generated field extension of k, so $K = \mathbf{k}(X)$ for some integral finite-type k-scheme X. The **constant field** of K or of X is the maximal algebraic extension k' of k contained in K. It is a finite extension of k: in fact, if $t_1, \ldots, t_n$ is a transcendence basis of K/k, then

$$[k' : k] = [k'(t_1, \ldots, t_n) : k(t_1, \ldots, t_n)] \le [K : k(t_1, \ldots, t_n)] < \infty.$$

Proposition 2.2.22. *Let X be an integral finite-type k-scheme. Let $k' \supseteq k$ be its constant field.*

Unofficial version for incidental online use

(i) *If X is geometrically integral, then $k' = k$.*
(ii) *If X is proper, then $\mathscr{O}_X(X)$ is a subfield of k'.*
(iii) *If X is normal, then $k' \subseteq \mathscr{O}_X(X)$.*

Proof.

(i) Proposition 2.2.19 implies that k'/k is primary. Proposition 2.2.20 implies that k'/k is separable. A primary separable finite extension of a field is trivial.
(ii) Let L be the k-algebra $\mathscr{O}_X(X)$. Since X is proper, $\dim_k L < \infty$. Since X is integral, L is an integral domain. Thus L is a finite field extension of k contained in $\mathbf{k}(X)$, so $L \subseteq k'$.
(iii) We have $k \subseteq k' \subseteq \mathbf{k}(X)$, with k' integral over k. For each $x \in X$, the ring $\mathscr{O}_{X,x}$ is integrally closed in its fraction field $\mathbf{k}(X)$ and contains k, so it contains k'. Thus $k' \subseteq \bigcap_{x \in X} \mathscr{O}_{X,x} = \mathscr{O}_X(X)$. $\square$

Remark 2.2.23. The following counterexamples explain why the hypothesis in each part of Proposition 2.2.22 is needed, respectively:

(i) $\mathbb{P}^1_F$ as k-scheme, for any nontrivial finite extension F/k,
(ii) $\mathbb{A}^1_k$, and
(iii) $x^2 - 2y^2 = 0$ over $\mathbb{Q}$.

2.3. Scheme-valued points

2.3.1. Motivation: Rational points on affine varieties over fields. Let X be the subvariety of $\mathbb{A}^n_k$ defined by a system of polynomial equations

$$\begin{aligned} f_1(x_1, \dots, x_n) &= 0 \\ f_2(x_1, \dots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \dots, x_n) &= 0. \end{aligned}$$

In other words, if we define $A := k[x_1, \dots, x_n]/(f_1, \dots, f_m)$, then X is the affine k-variety $\operatorname{Spec} A$. Then a k-**rational point** (or simply k-**point**) on X is an n-tuple $(a_1, \dots, a_n) \in k^n$ such that $f_1(a_1, \dots, a_n) = f_m(a_1, \dots, a_n) = 0$. The set of k-points on X is in bijection with the set $\operatorname{Hom}_{k\text{-algebras}}(A, k)$, which is in bijection with $\operatorname{Hom}_{k\text{-schemes}}(\operatorname{Spec} k, X)$. This motivates the general definition in the next section.

2.3.2. The set of scheme-valued points.

Definition 2.3.1. Let X be an S-scheme. If T is a S-scheme, then **the set of T-points on X** is $X(T) := \operatorname{Hom}_S(T, X)$.

Unofficial version for incidental online use

Warning 2.3.2. The definition of $X(T)$ depends on the structure morphism $X \to S$, even though the notation does not show it explicitly. This is in keeping with our notational convention of using X as abbreviation for the S-scheme (X, f) where $f\colon X \to S$ is the structure morphism.

In the case where $S = \operatorname{Spec} k$ and $T = \operatorname{Spec} L$ for a field extension L of k, an element of $X(L)$ is called an L-**rational point** or simply an L-**point**.

2.3.3. Functor of points, Yoneda's lemma, and representable functors.

(Reference: [**Vis05**, §2.1])

If $T' \to T$ is an S-morphism, then sending each S-morphism $T \to X$ to the composition $T' \to T \to X$ defines a map of sets $X(T) \to X(T')$. In fact, we obtain a functor:

Definition 2.3.3. The **functor of points** of an S-scheme X is the functor

$$\begin{aligned} h_X\colon \mathbf{Schemes}_S^{\mathrm{opp}} &\longrightarrow \mathbf{Sets} \\ T &\longmapsto X(T) := \operatorname{Hom}_S(T, X). \end{aligned}$$

A morphism of S-schemes $f\colon X \to Y$ induces a map of sets $X(T) \to Y(T)$ for each S-scheme T, and whenever $T' \to T$ is an S-morphism, we obtain a commutative square

$$\begin{tikzcd} X(T) \arrow[r] \arrow[d] & Y(T) \arrow[d] \\ X(T') \arrow[r] & Y(T'). \end{tikzcd}$$

In other words, f induces a morphism of functors (i.e., natural transformation) $h_f\colon h_X \to h_Y$.

The following is purely formal, true in any category, not just $\mathbf{Schemes}_S$, but is also very useful:

Lemma 2.3.4 (Yoneda's lemma)**.** *Let X and Y be S-schemes. The function*

$$\begin{aligned} \operatorname{Hom}_S(X, Y) &\longrightarrow \operatorname{Hom}(h_X, h_Y) \\ f &\longmapsto h_f \end{aligned}$$

is a bijection.

Sketch of proof. The inverse map takes a morphism of functors $F\colon h_X \to h_Y$ to the image of the identity $1_X \in \operatorname{Hom}_S(X, X) = X(X)$ under the map $F(X)\colon X(X) \to Y(X)$. $\square$

For a stronger version of Yoneda's lemma, see [**Vis05**, p. 14].

Unofficial version for incidental online use

Remark 2.3.5. Yoneda's lemma implies that X is determined by its functor of points h_X. In fact, X is already determined by the restriction of h_X to *affine* schemes, because $h_X(T) = X(T)$ can be recovered as $\varprojlim X(T_i)$, where (T_i) is the directed system of all affine open subschemes of T ordered by inclusion.

Because no information is lost in passing from X to h_X, it is sometimes convenient to *identify* X with its functor of points h_X! Then more general functors $\mathbf{Schemes}_S^{\mathrm{opp}} \to \mathbf{Sets}$ can be thought of as generalizations of schemes; some of these functors are of the form h_X, and some are not.

Definition 2.3.6. A functor $F\colon \mathbf{Schemes}_S^{\mathrm{opp}} \to \mathbf{Sets}$ is **representable** if it is isomorphic to h_M for some S-scheme M. In this case, one says also that M **represents** F, or that M is a **fine moduli space** for F.

Sometimes when one wants to construct a scheme, at first one can construct only what should be its functor of points F. Then one must ask whether F is actually represented by a scheme. If so, then all the tools of algebraic geometry can be applied to that scheme in order to understand F better. If not, one can hope that F might still be represented by some algebraic object more general than a scheme but close enough to a scheme that some tools of geometry can still be applied. For example, F might be represented by an *algebraic space* or an *algebraic stack*; for an introduction, see [**LMB00**] or [**Ols16**]. Alternatively, if F is not represented by a scheme, so F is not isomorphic to any h_M, then it might be at least *approximated* by a functor h_M in the following sense:

Definition 2.3.7. Let $F\colon \mathbf{Schemes}_S^{\mathrm{opp}} \to \mathbf{Sets}$ be a functor. An S-scheme M equipped with a morphism of functors $F \xrightarrow{\iota} h_M$ is a **coarse moduli space** for F if the following hold:

(i) For every other S-scheme M' with a morphism $F \to h_{M'}$, there is a unique morphism $h_M \to h_{M'}$ (or, equivalently, a unique S-morphism $M \to M'$) such that $F \to h_{M'}$ factors as $F \xrightarrow{\iota} h_M \to h_{M'}$.

(ii) For every algebraically closed field k and morphism $\operatorname{Spec} k \to S$, the map $F(\operatorname{Spec} k) \to M(k)$ given by ι is a bijection.

Intuitively, one can understand Definition 2.3.7 as follows. The set $F(\operatorname{Spec} k)$ is a certain collection of objects. If T is a k-scheme, an element of $F(T)$ may be thought of as a family of such objects parameterized by T. Thus giving F specifies both the objects and also what constitutes a family of objects. If M is a coarse moduli space, then each object in $F(\operatorname{Spec} k)$ has a class in $M(k)$, and condition (ii) says that the objects are in bijection with their classes. The morphism $F \to h_M$ gives in particular that for each T

Unofficial version for incidental online use

there is a map $F(T) \to \operatorname{Hom}_S(T, M)$; it may be thought of as taking a family $\pi\colon \mathcal{X} \to T$ to the morphism $T \to M$ sending each point $t \in T(k)$ to the point of M corresponding to class of the fiber $\pi^{-1}(t)$. Finally, condition (i) requires that M is such that h_M is as close as possible to F; it prevents, for example, replacing the morphism $F \to h_M$ by a composition $F \to h_M \to h_N$ such that $M(k) \to N(k)$ is a bijection. In fact, since condition (i) is a universal property, it guarantees that M is unique if it exists.

Example 2.3.8 (Moduli space of curves)**.** Fix $g \in \mathbb{Z}_{\geq 0}$. For an algebraically closed field k, let $\mathcal{M}_g(k)$ be the set of isomorphism classes of smooth projective geometrically integral curves of genus g over k (see Section 3.5 for the definition of smooth). More generally, for any scheme T, let $\mathcal{M}_g(T)$ be the set of isomorphism classes of smooth proper T-schemes whose fibers are geometrically integral curves of genus g. Then the functor $F := \mathcal{M}_g$ is not represented by a scheme, but it has a coarse moduli space M_g that is a quasi-projective scheme over $\mathbb{Z}$; alternatively, $\mathcal{M}_g$ is represented by an algebraic stack [**DM69**]. Also, the subfunctor $\mathcal{M}_g^0$ parameterizing genus g curves whose automorphism group is trivial *is* represented by a quasi-projective scheme M_g^0, and it is nonempty for $g \geq 3$.

Example 2.3.9 (Moduli space of curves with marked points)**.** More generally, for any $g, n \in \mathbb{Z}_{\geq 0}$, there is a quasi-projective coarse moduli space $M_{g,n}$ whose points over an algebraically closed field parameterize genus g curves with n distinct marked points. The subfunctor parameterizing $(C, p_1, \ldots, p_n)$ such that the group of automorphisms of C fixing $p_1, \ldots, p_n$ is trivial is represented by a quasi-projective scheme $M_{g,n}^0$. For fixed g, we have $M_{g,n} = M_{g,n}^0$ for sufficiently large n; that is, $M_{g,n}$ is a fine moduli space for n large enough relative to g. The symmetric group S_n acts on $M_{g,n}$.

Example 2.3.10 (Moduli space of genus 0 curves with marked points)**.** The group $\operatorname{Aut} \mathbb{P}^1 \simeq \mathrm{PGL}_2$ acts simply transitively on triples of distinct points of $\mathbb{P}^1$. Therefore, for $n \geq 3$, the space $M_{0,n}$ parameterizing $(\operatorname{Aut} \mathbb{P}^1)$-orbits of n-tuples of points on $\mathbb{P}^1$ is a fine moduli space. Let us work over a field k. Then $M_{0,3}$ is a point $\operatorname{Spec} k$. Next, $M_{0,4} \simeq \mathbb{P}^1 - \{0, 1, \infty\}$, since any 4-tuple of distinct geometric points can be moved by an automorphism of $\mathbb{P}^1$ to a unique 4-tuple of the form $(0, 1, \infty, x)$ with $x \notin \{0, 1, \infty\}$. And $M_{0,5}$ is $(\mathbb{P}^1 - \{0, 1, \infty\})^2 - \Delta$, where Δ is the diagonal; see Section 9.4.7 for an application. For each $n \geq 3$, the space $M_{0,n}$ is an open subscheme of $\mathbb{A}^n$.

Example 2.3.11 (Twists of $M_{g,n}$)**.** Over non-algebraically closed fields, we may consider twists of $M_{g,n}$ in the sense of Section 4.5. Start by thinking of $M_{g,n}$ as parameterizing isomorphism classes of genus g curves C equipped with a closed immersion $\operatorname{Spec} k^n \to C$. If L is a degree n étale k-algebra, then there is a coarse moduli space $M_{g,n}^{(L)}$ over k parameterizing genus g curves

Unofficial version for incidental online use

C equipped with a closed immersion $\operatorname{Spec} L \to C$. The varieties $M_{g,n}^{(L)}$ and $M_{g,n}$ become isomorphic after base change to k_s.

Example 2.3.12 (Compactifications of the moduli space of curves)**.** There is a functor $\overline{\mathcal{M}}_g$ that parameterizes isomorphism classes of stable genus g curves; see [**HM98**, Theorem 2.15] for an introduction and for the definition of stable. Knudsen and Mumford proved that $\overline{\mathcal{M}}_g$ has a coarse moduli space $\overline{M}_g$ that is a projective variety containing M_g as an open subvariety: the first proof, published long after its discovery, was that in [**Knu83**, Theorem 6.1], but a simpler proof was given in [**Mum77**, Corollary 5.2]. Similarly one can construct projective varieties $\overline{M}_{g,n}$ and $\overline{M}_{g,n}^{(L)}$.

2.3.4. Functorial properties. If X is an S-scheme and $U \subseteq X$ is an open subscheme, then $U(T) \subseteq X(T)$ for any S-scheme T; see Exercise 2.4.

Remark 2.3.13. Let k be a field, and let X be a k-scheme. If $\{X_i\}$ is an open covering of X, then $\bigcup X_i(k) = X(k)$.

Warning 2.3.14. Remark 2.3.13 holds more generally for a local ring k, but not for an arbitrary ring. It can fail for a polynomial ring, for instance: a morphism $\mathbb{A}^1 \to X$ need not have image contained in any one X_i.

Despite Warning 2.3.2, we do get independence of S if we base change X appropriately:

Proposition 2.3.15. *If X is an S-scheme, $S' \to S$ is a morphism of schemes, and T is an S'-scheme, then $X_{S'}(T) = X(T)$, where on the right we view T as S-scheme via the composition $T \to S' \to S$.*

Proof. The universal property of the fiber product gives $\operatorname{Hom}_{S'}(T, X_{S'}) = \operatorname{Hom}_S(T, X)$. $\square$

2.3.5. Example: Scheme-valued points on projective space. Let X be an S-scheme. By Proposition 2.3.15, $\mathbb{P}^n_S(X) = \mathbb{P}^n_{\mathbb{Z}}(X) := \operatorname{Hom}_{\mathbb{Z}}(X, \mathbb{P}^n_{\mathbb{Z}})$, and the set on the right is described by [**Har77**, Theorem II.7.1]. The outcome is that there is a bijection

$$\mathbb{P}^n_S(X) \longleftrightarrow \left\{ (\mathscr{L}, s_0, \dots, s_n) : \begin{array}{c} \mathscr{L} \text{ is a line bundle on } X \text{, and} \\ s_0, \dots, s_n \in \Gamma(X, \mathscr{L}) \text{ generate } \mathscr{L} \end{array} \right\} / \simeq .$$

By definition, global sections $s_0, \dots, s_n$ **generate** $\mathscr{L}$ if and only if for every $P \in X$, they do not simultaneously vanish when evaluated at P (that is, for every $P \in X$, their images in the 1-dimensional $\mathbf{k}(P)$-vector space stalk $\mathscr{L}_P / \mathfrak{m}_P \mathscr{L}_P$ do not all vanish). On the right, tuples are considered up to isomorphism: $(\mathscr{L}, s_0, \dots, s_n)$ and $(\mathscr{L}', s_0', \dots, s_n')$ are called isomorphic if and only if there is an isomorphism of line bundles $\mathscr{L} \to \mathscr{L}'$ mapping s_i to s_i' for each i.

Unofficial version for incidental online use

Remark 2.3.16. Intuitively, one can think of $(\mathscr{L}, s_0, \dots, s_n)$ as describing the morphism

$$\begin{aligned} X &\longrightarrow \mathbb{P}^n_S \\ P &\longmapsto (s_0(P), \dots, s_n(P)). \end{aligned}$$

Strictly speaking, this does not make sense, since the $s_i(P)$ are not well-defined elements of the field $\mathbf{k}(P)$ (s_i not being a function on X). But at each P, we can fix j such that s_j is nonvanishing at P (that is, $s_j \notin \mathfrak{m}_P \mathscr{L}_P$), and then for every i the *ratio* s_i/s_j may be viewed as a function defined in a neighborhood of P in X.

Example 2.3.17. Let us compute $\mathbb{P}^n(A)$ when A is a principal ideal domain. By [**Har77**, Proposition II.6.2 and Corollary II.6.16], $\operatorname{Pic} A = 0$. That is, the only line bundle on $X := \operatorname{Spec} A$, up to isomorphism, is $\mathscr{O}_X$. Global sections of $\mathscr{O}_X$ are simply elements of A, and a sequence of global sections $a_0, \dots, a_n \in A$ generate $\mathscr{O}_X$ if and only if $a_0, \dots, a_n$ generate the unit ideal. An isomorphism of line bundles $\mathscr{O}_X \to \mathscr{O}_X$ is the same as an A-module isomorphism $A \to A$, which is the same as multiplication by some unit $\lambda \in A^\times$. Hence

$$\mathbb{P}^n(A) = \{ (a_0, \dots, a_n) \in A^{n+1} : a_0, \dots, a_n \text{ generate } (1) \} / \sim,$$

where the equivalence relation $\sim$ is as follows: $(a_0, \dots, a_n) \sim (a'_0, \dots, a'_n)$ if and only if there exists $\lambda \in A^\times$ such that $a'_i = \lambda a_i$ for all i. The equivalence class of $(a_0, \dots, a_n)$ is denoted $(a_0 : \dots : a_n)$.

In the special case where A is a field, this gives the expected description of $\mathbb{P}^n(k)$.

Remark 2.3.18. If A is a principal ideal domain and $K = \operatorname{Frac} A$, it follows from Example 2.3.17 that the natural map $\mathbb{P}^n(A) \to \mathbb{P}^n(K)$ is a bijection. Namely, given $(a_0 : \dots : a_n) \in \mathbb{P}^n(K)$, the fractional ideal generated by $a_0, \dots, a_n$ is principal, and if we choose a generator λ, then scaling all the a_i by λ^{-1} results in an equivalent point that comes from $\mathbb{P}^n(A)$. For a generalization of this remark, see Theorem 3.2.13.

2.3.6. Scheme-valued points on separated schemes.

(Reference: [**EGA IV**$_3$, §11.10])

Definition 2.3.19. A morphism of schemes $f : X \to Y$ is called **dominant** if the set $f(X)$ is dense in the topological space Y; i.e., the only closed subset of Y containing $f(X)$ is Y itself. Call f **scheme-theoretically dominant** (cf. [**EGA IV**$_3$, 11.10.2]) if either of the following equivalent conditions holds:

- Whenever U is an open subscheme of Y, and $f|_{f^{-1}U} : f^{-1}U \to U$ factors as $f^{-1}U \to Z \hookrightarrow U$ for some closed subscheme Z of U, we have $Z = U$.

Unofficial version for incidental online use

- The sheaf homomorphism $\mathscr{O}_Y \to f_*\mathscr{O}_X$ is injective.

Warning 2.3.20. It would be insufficient to require the first condition only for $U = Y$, i.e., to require only that the only closed subscheme of Y through which f factors is Y itself; one really needs to impose the condition for every open subscheme $U \subseteq Y$. See Exercise 2.10.

Scheme-theoretically dominant implies dominant. If Y is reduced, then the notions are equivalent, since then every open subscheme U is reduced too, and the only closed subscheme of U having the same topological space as U is U itself.

Proposition 2.3.21. *Let X be a separated S-scheme. If $T' \to T$ is a scheme-theoretically dominant S-morphism, then $X(T) \to X(T')$ is injective.*

Proof. Let $f, g \in X(T)$, and let e be the morphism $T' \to T$, so we have

$$T' \xrightarrow{e} T \xrightarrow{(f,g)} X \times_S X.$$

Since X is separated over S, the diagonal $\Delta \subseteq X \times_S X$ is a closed subscheme. Let $Z = (f,g)^{-1}\Delta$, which is "the closed subscheme of T on which f and g agree". Let f', g' be the images of f, g in $X(T')$, and let $Z' = (f', g')^{-1}\Delta$. Then $Z' = e^{-1}(Z)$. If $f' = g'$, then $Z' = T'$, but e is scheme-theoretically dominant, so then $Z = T$, which means that $f = g$. This proves injectivity. $\square$

Corollary 2.3.22. *If $R \subseteq R'$ is an inclusion of rings and X is a separated R-scheme, then $X(R) \to X(R')$ is injective.*

Proposition 2.3.21 implies also that, under suitable hypotheses, morphisms agreeing on a dense open subscheme agree everywhere:

Corollary 2.3.23. *Let X be a reduced S-scheme, and let Y be a separated S-scheme. Let U be a dense open subscheme of X. If f and g are morphisms $X \to Y$ such that $f|_U = g|_U$, then $f = g$.*

Proof. Proposition 2.3.21 says that $Y(X) \to Y(U)$ is injective. $\square$

2.3.7. Varieties that are not geometrically integral.

Proposition 2.3.24. *Let k be a field. A connected k-scheme with a k-point is geometrically connected.*

Proof. More generally, if X and Y are connected k-schemes and X has a k-point, then $X \times_k Y$ is connected; see [**EGA IV**$_2$, Corollaire 4.5.14] or [**SGA 3**$_{\mathbf{I}}$, Exposé VI$_{\mathrm{A}}$, Lemma 2.1.2]. $\square$

Unofficial version for incidental online use

Warning 2.3.25. In contrast with Proposition 2.3.24, an irreducible k-variety with a k-point need not be geometrically irreducible: the $\mathbb{Q}$-variety $x^2 - 2y^2 = 0$ in Example 2.2.6 has the rational point $(0,0)$.

But if we have not just one k-point, but a Zariski dense set of k-points, we can say more:

Proposition 2.3.26. *Let X be a finite-type scheme over a field k such that $X(k)$ is Zariski dense in X.*

(i) *If X is irreducible, then X is geometrically irreducible.*
(ii) *If X is reduced, then X is geometrically reduced.*
(iii) *If X is integral, then X is geometrically integral.*

Proof.

(i) Replacing X by its associated reduced subscheme X_{red} affects neither the hypotheses nor the conclusion. Suppose that X is not geometrically irreducible. By Proposition 2.2.19(i)$\Leftrightarrow$(iv), $\mathbf{k}(X)/k$ is not primary, so there exists $\alpha \in \mathbf{k}(X) \setminus k$ separable and algebraic over k. By definition of $\mathbf{k}(X)$, we have $\alpha \in \mathscr{O}(U)$ for some nonempty affine open subscheme $U \subseteq X$. Since $X(k)$ is Zariski dense in X, there exists a k-point in U. This point induces a k-algebra homomorphism $\mathscr{O}(U) \to k$, which restricts to a k-algebra homomorphism $k(\alpha) \to k$, contradicting the fact that field homomorphisms are injective.

(ii) It suffices to prove the statement for each subscheme in an open cover of X. So assume that $X = \operatorname{Spec} A$. Each $x \in X(k)$ corresponds to a k-algebra homomorphism $A \to k$. Putting these together gives a homomorphism $A \to \prod_{x \in X(k)} k$, which is injective since $X(k)$ is Zariski dense and A is reduced. Tensoring with $\overline{k}$ yields an injection

$$A \otimes_k \overline{k} \hookrightarrow \left(\prod_{x \in X(k)} k \right) \otimes_k \overline{k} \subseteq \prod_{x \in X(k)} \overline{k},$$

which shows that $A \otimes_k \overline{k}$ is reduced. Thus X is geometrically reduced.

(iii) Combine (i) and (ii). $\square$

Remark 2.3.27. Proposition 2.3.26 is often applied in its contrapositive form: if X is an integral k-variety that is not geometrically integral, then $X(k)$ is *not* Zariski dense. In this case, the study of $X(k)$ reduces to the study of $Y(k)$ for a lower-dimensional variety Y. For this reason, when studying rational points, we can reduce to the case of geometrically integral varieties.

Unofficial version for incidental online use

2.4. Closed points

Definition 2.4.1. A **closed point** of a scheme X is a point $x \in X$ such that $\{x\}$ is Zariski closed in X.

If X is a variety over an algebraically closed field k, the map

$$\begin{aligned} X(k) &\longrightarrow \{\text{closed points of } X\} \\ (f\colon \operatorname{Spec} k \to X) &\longmapsto f(\operatorname{Spec} k) \end{aligned}$$

is a bijection. The nonclosed points of X are the generic points of the positive-dimensional integral subvarieties of X.

To develop intuition for our generalizations to arbitrary fields k, namely Propositions 2.4.3 and 2.4.6, we begin with an example:

Example 2.4.2. Let $X = \mathbb{A}^1_{\mathbb{R}} = \operatorname{Spec} \mathbb{R}[t]$. The following are in bijection:

(i) The set of closed points of X.
(ii) The set of maximal ideals of $\mathbb{R}[t]$.
(iii) The set of monic irreducible polynomials of $\mathbb{R}[t]$.
(iv) The set of $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-orbits in $X(\mathbb{C}) = \mathbb{C}$.

If $x \in X$ is a closed point corresponding to a monic irreducible polynomial $f \in \mathbb{R}[t]$, then $\mathbf{k}(x) = \mathbb{R}[t]/(f)$, so $[\mathbf{k}(x) : \mathbb{R}] = \deg f$, which may be 1 or 2. Those x with $[\mathbf{k}(x) : k] = 1$ correspond to size 1 orbits in (iv), which correspond to elements of $X(\mathbb{R})$.

Proposition 2.4.3. *Let X be a k-variety, and let $x \in X$. The following are equivalent:*

(i) *The point x is closed.*
(ii) *The dimension of the closure of $\{x\}$ is 0.*
(iii) *The residue field $\mathbf{k}(x)$ is a finite extension of k.*

Proof. The closure $\overline{\{x\}}$ with its reduced structure is irreducible and reduced, so it is an integral k-variety.

(i)$\Rightarrow$(ii): The dimension of a one-point space is 0.

(ii)$\Rightarrow$(i): Suppose that $y \in \overline{\{x\}}$; we must prove that $y = x$. We have irreducible closed subsets $\overline{\{y\}} \subseteq \overline{\{x\}}$, but we are assuming $\dim \overline{\{x\}} = 0$, so $\overline{\{y\}} = \overline{\{x\}}$. In a scheme, an irreducible closed subset has a unique generic point, so $y = x$.

(ii)$\Leftrightarrow$(iii): The function field of $\overline{\{x\}}$ is $\mathbf{k}(x)$, so $\dim \overline{\{x\}} = \operatorname{tr\,deg}(\mathbf{k}(x)/k)$. In particular, $\dim \overline{\{x\}} = 0$ if and only if $\mathbf{k}(x)$ is algebraic over k, which is the same as saying that $\mathbf{k}(x)$ is a finite extension of k since we know in advance that $\mathbf{k}(x)$ is a finitely generated field extension of k. $\square$

Unofficial version for incidental online use

Definition 2.4.4. The **degree** of a closed point x on a k-variety X is $[\mathbf{k}(x) : k]$.

Remark 2.4.5. Schemes of finite type over $\mathbb{Z}$ share many properties with schemes of finite type over a field. In particular, there is an analogue of Proposition 2.4.3 that states that if X is a scheme of finite type over $\mathbb{Z}$ and $x \in X$, the following are equivalent:

(i) The point x is closed.

(ii) The (Krull) dimension of the closure of $\{x\}$ is 0.

(iii) The residue field $\mathbf{k}(x)$ is finite.

The proof of (i)$\Leftrightarrow$(ii) is as before, and (i)$\Leftrightarrow$(iii), which may be called the arithmetic weak Nullstellensatz, is [**EGA IV**$_3$, 10.4.11.1(i)].

Proposition 2.4.6. *Let X be a k-variety. Then the map*

$$\begin{aligned} \{\, \mathfrak{G}_k\text{-orbits in } X(\overline{k}) \,\} &\longrightarrow \{\, \text{closed points of } X \,\} \\ \text{orbit of } \big(f \colon \operatorname{Spec} \overline{k} \to X\big) &\longmapsto f(\operatorname{Spec} \overline{k}) \end{aligned}$$

is a bijection.

Proof. For any field extension L of k, [**Har77**, Lemma II.4.4] gives a bijection

$$X(L) \longleftrightarrow \{\, (x, \iota) \mid x \in X, \text{ and } \iota \colon \mathbf{k}(x) \hookrightarrow L \text{ is a } k\text{-embedding} \,\},$$

in which the x coming from $P \in X(L)$ is the unique point in the image of $\operatorname{Spec} L \to X$. Take $L = \overline{k}$. Suppose that $P \in X(\overline{k})$ corresponds to (x, ι). Since $\mathbf{k}(x)$ is finitely generated over k, it is a finite extension of k, so x is a closed point. Thus we get a bijection

$$X(\overline{k}) \longleftrightarrow \{\, (x, \iota) \mid x \in X \text{ is closed, and } \iota \colon \mathbf{k}(x) \hookrightarrow \overline{k} \text{ is a } k\text{-embedding} \,\}.$$

This bijection is $\mathfrak{G}_k$-equivariant, where σ acts on $X(\overline{k})$ coordinatewise (or, equivalently, by forming the composition $\operatorname{Spec} \overline{k} \xrightarrow{\sigma} \operatorname{Spec} \overline{k} \xrightarrow{P} X$) and acts on the right set by $(x, \iota) \mapsto (x, \iota \circ \sigma)$. For each closed point $x \in X$, the set of k-embeddings $\iota \colon \mathbf{k}(x) \hookrightarrow \overline{k}$ is a nonempty and transitive $\mathfrak{G}_k$-set, so the set of $\mathfrak{G}_k$-orbits on the right-hand side equals the set of closed points x. $\square$

In particular, if X is a k-variety, then k-points of X are in bijection with closed points with residue field k.

Warning 2.4.7. On schemes that are not varieties, closed points can behave strangely. For instance, there exists a nonempty scheme with no closed points at all! See [**Liu02**, Exercise 3.27].

Unofficial version for incidental online use

2.5. Curves

(Reference: [**Liu02**, Chapter 7])

2.5.1. Genus.

(Reference: [**Liu02**, Chapter 7, Definition 3.19])

Let X be a regular, projective, geometrically integral curve over a field k. Its **genus** $g = g(X)$ admits several equivalent definitions:

- The **arithmetic genus** of X is $p_a(X) := \dim_k \mathrm{H}^1(X, \mathscr{O}_X)$.
- Let ω_X° be the dualizing sheaf [**Har77**, III.§7], a line bundle on X. If X is smooth (see Section 3.5), then ω_X° is simply the canonical sheaf $\omega_X = \Omega^1_{X/k}$ [**Har77**, II.§8]. The **geometric genus** of X is $p_g(X) := \dim_k \mathrm{H}^0(X, \omega_X^\circ)$.
- The genus is the integer g that makes the Riemann–Roch theorem (Theorem 2.5.3) hold.
- If $k = \mathbb{C}$, then the compact Riemann surface $X(\mathbb{C})$ can be viewed as a compact orientable 2-dimensional $\mathbb{R}$-manifold, which is a g-holed torus for a unique $g \geq 0$.

The proof of the Serre duality theorem [**Har77**, Corollary III.7.7] works over an arbitrary field k, and shows that the k-vector spaces $\mathrm{H}^1(X, \mathscr{O}_X)$ and $\mathrm{H}^0(X, \omega_X^\circ)$ are dual, so $p_a(X) = p_g(X)$.

If Y is a curve birational to a regular, projective, geometrically integral curve X, define $g(Y) := g(X)$.

2.5.2. Genus change under field extension.

(Reference: [**Tat52**])

Theorem 2.5.1. *Let X be a regular, projective, geometrically integral k-curve. Let $L \supseteq k$ be a field extension. Then*

(a) *We have $g(X_L) \leq g(X)$, with equality if and only if X_L is regular.*
(b) *The difference $g(X) - g(X_L)$ is divisible by $(p-1)/2$.*
(c) *If L is separable over k, then $g(X_L) = g(X)$.*

Sketch of proof.

(a) Let $\widetilde{X}_L$ be the desingularization of X_L. We can define $p_a(X_L)$ as before even if X_L is not regular; in fact, $p_a(X_L) = p_a(X)$ since cohomology commutes with flat base extension [**Har77**, Proposition III.9.3]. But $g(X_L)$ is defined as $p_a(\widetilde{X}_L)$, which is less than or equal to $p_a(X_L)$, with equality if and only if X_L is already regular.

Unofficial version for incidental online use

(b) See [**Tat52**].

(c) If L is separable over k, then X_L is regular (this follows from Proposition 3.5.51(iii)), so this is a special case of (a). □

Example 2.5.2. Let p be an odd prime. Let k be the imperfect field $\mathbb{F}_p(t)$. Let X be the affine curve $y^2 = x^p - t$ over k. One can show that $g(X) = (p-1)/2$. On the other hand, $X_{\overline{k}}$ is isomorphic to the curve $y^2 = x^p$, which is birational to $\mathbb{P}^1_{\overline{k}}$, so $g(X_{\overline{k}}) = 0$.

2.5.3. The Riemann–Roch theorem.

(Reference: [**Liu02**, §7.3])

Let X be a regular, projective, geometrically integral k-curve of genus g. The group $\operatorname{Div} X$ of **Weil divisors** on X is the free abelian group on the set of closed points P of X. Each $D \in \operatorname{Div} X$ gives rise to a line bundle $\mathscr{O}(D)$. By [**Har77**, Corollary II.6.16], this induces an isomorphism from the group of Weil divisors modulo linear equivalence to the **Picard group** $\operatorname{Pic} X$ of isomorphism classes of line bundles. If $D = \sum n_P P \in \operatorname{Div} X$, define $\deg D := \sum n_P \deg P$, where $\deg P$ is as in Definition 2.4.4, and define $\ell(D) := \dim_k \mathrm{H}^0(X, \mathscr{O}(D))$. A **canonical divisor** is a divisor K such that $\omega_X^\circ = \mathscr{O}(K)$.

Theorem 2.5.3 (Riemann–Roch). *Let X and K be as above. Then*

$$\ell(D) - \ell(K - D) = \deg D + 1 - g.$$

Proof. Once one has the Serre duality theorem, this is very similar to the proof of [**Har77**, Theorem IV.1.3], so we leave it as Exercise 2.15. See also [**Liu02**, Chapter 7, Theorem 3.26]. □

2.6. Rational points over special fields

2.6.1. Rational points over finite fields. Let k be a finite field, and let X be a k-variety. Then $X(k)$ is finite. (This is obvious if X is affine, and the general case follows by applying Remark 2.3.13 to an affine open covering.) More will be said in Chapter 7.

2.6.2. Rational points over topological fields.

(Reference: [**Ser55**])

Let k be a topological field (for example, a local field), and let X be a k-variety. We can use the topology of k to define a topology on $X(k)$, called the **analytic topology**, as follows. Give the set $\mathbb{A}^n(k) = k \times \cdots \times k$ the product topology. If X is a closed subvariety of $\mathbb{A}^n$, give $X(k) \subseteq \mathbb{A}^n(k)$ the subspace topology. Finally, if X is obtained by gluing affine open subsets

Unofficial version for incidental online use

$X_1, \ldots, X_m$, then use the same gluing data to glue the topological spaces $X_1(k), \ldots, X_m(k)$. Two different affine open coverings give the same topology on $X(k)$, as one can check by comparison with a common refinement. Any morphism of k-varieties $X \to Y$ induces a continuous map $X(k) \to Y(k)$ of topological spaces.

Proposition 2.6.1. *Let k be a local field. Let X be a k-variety.*

(i) *If X is proper over k, then $X(k)$ is compact.*

(ii) *More generally, if $X \to Y$ is a proper morphism of k-varieties, then $X(k) \to Y(k)$ is a proper map of topological spaces.* (*The latter means that the inverse image of any compact subset of $Y(k)$ is compact.*)

The converses hold when $k = \mathbb{C}$.

Proof. See Serre's "GAGA" paper [**Ser55**]. $\square$

Warning 2.6.2. The converses can fail for $k = \mathbb{R}$; see Exercise 2.16.

Remark 2.6.3. In the case $k = \mathbb{C}$, one can go further by equipping the topological space $X(\mathbb{C})$ with a sheaf of germs of holomorphic functions to get a locally ringed space X^{an}. (If $\dim X > 0$, then X^{an} is not a scheme.) Such locally ringed spaces are special cases of **complex analytic spaces**; see [**Har77**, Appendix B] for a survey with more details, and [**SGA 1**, XII] for a definition of X^{an} as the complex analytic space representing a certain functor. There are also various nonarchimedean analogues [**Con08**].

Remark 2.6.4 (Hilbert's tenth problem over a local field)**.** There is an algorithm that, given a local field k of characteristic 0 and a k-variety X, decides whether $X(k)$ is nonempty. (Strictly speaking, to make sense of this, one should assume that X is given over an explicitly presented finitely generated subfield of k, so that X admits a finite description suitable for input into a Turing machine.) The analogue for $\mathbb{F}_q((t))$ is an open question.

2.6.3. Adelic points.

(Reference: [**Con12a**])

Let k be a global field, and let Ω_k, $\mathcal{O}_{k,S}$, k_v, $\mathcal{O}_v$, and $\mathbf{A}$ be as in Section 1.1.3. Let X be a k-variety. Since $\mathbf{A}$ is a k-algebra, the set $X(\mathbf{A})$ of adelic points is already defined, as the set of k-morphisms $\operatorname{Spec} \mathbf{A} \to X$.

There is a more down-to-earth description of $X(\mathbf{A})$, however, as we now sketch. There exists a finite set S of places and a separated finite-type $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$ such that $\mathcal{X}_k \simeq X$. Then $X(\mathbf{A})$ is in bijection with $\prod'_{v \in \Omega_k} (X(k_v), \mathcal{X}(\mathcal{O}_v))$; see Exercise 3.4.

Unofficial version for incidental online use

This bijection lets us equip $X(\mathbf{A})$ with a topology. First, equip each $X(k_v)$ with the analytic topology. Next, for nonarchimedean $v \notin S$, equip the open and closed subset $\mathcal{X}(\mathcal{O}_v) \subseteq \mathcal{X}(k_v) = X(k_v)$ with the subspace topology. Finally, define the **adelic topology** on $X(\mathbf{A}) \simeq \prod'_{v \in \Omega_k} (X(k_v), \mathcal{X}(\mathcal{O}_v))$ as the restricted product topology, in which the basic open sets are those of the form $\prod_{v \in T} U_v \times \prod_{v \notin T} \mathcal{X}(\mathcal{O}_v)$ for a finite set $T \supseteq S$ and open subsets $U_v \subseteq X(k_v)$ for each $v \in T$.

Remark 2.6.5. If X is a closed subscheme of $\mathbb{A}^n$, the adelic topology on $X(\mathbf{A})$ agrees with the subspace topology obtained by viewing $X(\mathbf{A})$ as a subset of the topological space $\mathbf{A}^n$.

2.6.4. Rational points over global fields. Let k be a global field. Let X be a k-variety. One would like to know the answers to many questions, such as the following.

2.6.4.1. *Existence of rational points.*

Question 2.6.6. Does X have a k-point?

The problem of answering this question given an arbitrary X is equivalent to **Hilbert's tenth problem over** k, which is the problem of finding a general algorithm that takes a multivariable polynomial $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ as input and outputs YES or NO according to whether there exists $\vec{a} \in k^n$ such that $f(\vec{a}) = 0$.

- For each global function field k, no such algorithm exists [**Phe91**, **Shl92**, **Vid94**, **Eis03**].
- On the other hand, for each number field k, it is unknown whether such an algorithm exists. It is not even proved yet that one can decide, given $a \in \mathbb{Q}$, whether $x^3 + y^3 = a$ has a solution in rational numbers.

See [**Poo08**] for more about extensions of Hilbert's tenth problem.

2.6.4.2. *Finiteness of rational points.*

Question 2.6.7. Is $X(k)$ finite or infinite? When $X(k)$ is finite, can one list its elements?

For curves X over number fields, the following theorem of Faltings gives a partial answer. Because of Remark 2.3.27 and the fact that X and its normalization differ in only finitely many points, we may assume that X is nice in the sense of Definition 3.5.68.

Theorem 2.6.8 ([**Fal83**]). *Let X be a nice curve of genus > 1 over a number field k. Then $X(k)$ is finite.*

Unofficial version for incidental online use

For more details and generalizations, see Section 9.5. Question 2.6.7 can be difficult to answer even for specific, simple-looking equations:

Example 2.6.9. Let X be the projective surface in $\mathbb{P}^3_{\mathbb{Q}}$ defined by the homogeneous equation $x^4 + 2y^4 = z^4 + 4w^4$. There are two obvious rational points, given in homogeneous coordinates as $(1 : 0 : \pm 1 : 0)$. The next smallest solutions are

$$(\pm 1484801 : \pm 1203120 : \pm 1169407 : \pm 1157520),$$

according to [**EJ06**]. Are there infinitely many others? (This surface is an example of a K3 surface; see Section 9.3.2.2. It is not known whether there is a K3 surface X over a number field k such that $X(k)$ is nonempty and finite.)

2.6.4.3. *Growth of rational points.* Let us now return to the case of an arbitrary variety X over a global field k. If $X(k)$ is infinite, one can try to "measure its size" in some way. For example, given $P \in \mathbb{P}^n(\mathbb{Q})$, one can write $P = (a_0 : \cdots : a_n)$ with $a_i \in \mathbb{Z}$ and $\gcd(a_0, \ldots, a_n) = 1$, and define the **height** of P as $H(P) := \max |a_i|$. Then, for $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$, one defines

$$N_X(B) := \#\{x \in X(\mathbb{Q}) : H(x) \leq B\}.$$

Question 2.6.10. For $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$, can one predict the rate of growth of $N_X(B)$ as $B \to \infty$?

For a survey on this question, see [**Pey02**].

2.6.4.4. *Zariski density of rational points.*

Question 2.6.11. Is $X(k)$ Zariski dense in X?

Question 2.6.12. Is there a finite extension L of k such that $X(L)$ is Zariski dense (in X_L)? If so, one says that "rational points are **potentially dense** on X".

Campana [**Cam04**, Conjecture 9.20] has conjectured that for a variety X over a number field, potential density is equivalent to a certain *geometric* condition.

2.6.4.5. *Local approximation of rational points.*

Question 2.6.13. Given a place v of k, is $X(k)$ dense in $X(k_v)$ with respect to the v-adic (analytic) topology?

Related to this is the following conjecture of Mazur:

Conjecture 2.6.14 ([**Maz92**]). *If X is a $\mathbb{Q}$-variety, then the closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ with respect to the analytic topology has at most finitely many connected components.*

Unofficial version for mental online use

One strategy for determining whether a variety over global field k has a k-point is to check first whether it has a k_v-point for each completion k_v of k. This motivates the following question:

Question 2.6.15. Does the implication

$$X(k_v) \neq \emptyset \text{ for all places } v \text{ of } k \quad \Longrightarrow \quad X(k) \neq \emptyset$$

hold? If so, one says that X **satisfies the local-global principle** (or **Hasse principle**).

If X satisfies the local-global principle, one can ask whether a stronger condition holds:

Question 2.6.16. Is the image of $X(k) \to \prod_v X(k_v)$ dense with respect to the product of the v-adic topologies? If so, one says that X satisfies **weak approximation**.

Exercise 2.17 explains how weak approximation is about simultaneous approximation of k_v-points for finitely many v by a k-point. Some varieties satisfy the local-global principle and/or weak approximation, and others do not. See [**Har04**] for a survey on weak approximation.

One can ask for even more:

Question 2.6.17. Is the image of $X(k) \to X(\mathbf{A})$ dense with respect to the adelic topology?

This is stronger than weak approximation since the adelic topology on $X(\mathbf{A})$ generally has more open sets than the topology induced on $X(\mathbf{A})$ as a subset of $\prod X(k_v)$ equipped with the product topology. In fact, adelic density is *too* strong to have a chance of holding for many varieties: for instance, if X is affine, then $X(k)$ is discrete in $X(\mathbf{A})$ since k is discrete in $\mathbf{A}$. Therefore we now weaken the condition slightly.

Let S be a finite set of places of k. Define the **prime-to-S adèle ring** $\mathbf{A}^S := \prod'_{v \notin S}(k_v, \mathcal{O}_v)$, so $\mathbf{A} = \left(\prod_{v \in S} k_v\right) \times \mathbf{A}^S$. For any k-variety, define an adelic topology on $X(\mathbf{A}^S)$ as in Section 2.6.3, by viewing $X(\mathbf{A}^S)$ as a restricted product. The weakened question is then:

Question 2.6.18. Is the image of $X(k) \to X(\mathbf{A}^S)$ dense with respect to the adelic topology? If so, one says that X satisfies **strong approximation with respect to S**.

See Section 5.10 for approximation theorems in the case that X is an algebraic group, and see Section 8.4.6 for a way to prove that strong approximation fails for certain varieties.

Unofficial version for incidental online use

Exercises

2.1. Find a field k and a regular integral k-variety X that is neither affine, projective, geometrically connected, geometrically reduced, nor geometrically regular.

2.2. Let $k = \mathbb{F}_p(s,t)$, where s and t are indeterminates. Let X be the k-variety $sx^p + ty^p = 1$ in $\mathbb{A}^2_k$. Let L be the function field of X.
(a) Show that the only finite extension of k contained in L is k itself.
(b) Show that L is not separable over k.

2.3. For any scheme X over a field, if X_{red} is the associated reduced scheme, then the natural map $X_{\mathrm{red}}(k) \to X(k)$ is a bijection. For which schemes S is it true that for every S-scheme X, the map $X_{\mathrm{red}}(S) \to X(S)$ is a bijection?

2.4. Let X be an S-scheme, and let U be an open subscheme. Prove that for any S-scheme T, the set $U(T)$ is the subset of $X(T)$ consisting of S-morphisms $f\colon T \to X$ such that $f(T)$ is contained in U as a set.

2.5. Let F be the functor $\mathbf{Schemes}^{\mathrm{opp}} \to \mathbf{Sets}$ that maps each scheme X to $\mathscr{O}_X(X)^\times$ and that maps a morphism $f\colon X \to Y$ to the natural map $\mathscr{O}_Y(Y)^\times \to \mathscr{O}_X(X)^\times$ induced from the ring homomorphism $\mathscr{O}_Y(Y) \to \mathscr{O}_X(X)$. Prove that F is representable.

2.6. Let S be a scheme with a morphism $\operatorname{Spec} k \to S$ for some algebraically closed field k. Let $F\colon \mathbf{Schemes}_S^{\mathrm{opp}} \to \mathbf{Sets}$ be a functor. Prove that any fine moduli space for F is also a coarse moduli space for F.

2.7. Fix $p, q, r \in \mathbb{Z}_{>0}$. A **primitive** integer solution to the generalized Fermat equation $x^p + y^q = z^r$ is one in which $x, y, z \in \mathbb{Z}$ and $\gcd(x,y,z) = 1$. Let $S = \operatorname{Spec} \mathbb{Z}[x,y,z]/(x^p + y^q - z^r)$, and let T be the closed subscheme $\operatorname{Spec} \mathbb{Z}[x,y,z]/(x,y,z)$. Let $S' = S - T$, which is an open subscheme of S. Prove that $S'(\mathbb{Z})$ is in bijection with the set of primitive integer solutions to $x^p + y^q = z^r$.

2.8. Find a scheme X over $\mathbb{Z}$ such that

$$X(A) \simeq \{\, (a,b) \in A^2 : a, b \text{ generate the unit ideal in } A \,\}$$

functorially in the ring A.

2.9. Give an example of an S-scheme X with open subschemes U and V such that $U \cup V = X$ but $U(S) \cup V(S) \neq X(S)$.

2.10. Let k be a field. Let $Y = \operatorname{Spec} k[t]$. For $n \geq 1$, let X_n be the closed subscheme $\operatorname{Spec} k[t]/(t^n)$. Let X be the disjoint union $\coprod_{n \geq 1} X_n$. Let $f\colon X \to Y$ be the morphism that on each X_n is the inclusion.
(a) Is f dominant?

Unofficial version for incidental online use

(b) Is f scheme-theoretically dominant?
(c) Does f factor through a closed subscheme of Y other than Y itself?

2.11. (Failure of descent) Let $k = \mathbb{Q}(\sqrt{2})$. Prove that there does not exist a variety X over $\mathbb{Q}$ such that X_k is isomorphic to the affine plane curve $x^2 + y^2 = \sqrt{2}$ over k.

2.12. Let X be the curve $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2_{\mathbb{R}}$. Prove that the homomorphism $\operatorname{Pic} X \to (\operatorname{Pic} X_{\mathbb{C}})^{\operatorname{Gal}(\mathbb{C}/\mathbb{R})}$ is not an isomorphism.

2.13. Let X be a scheme of finite type over $\mathbb{F}_q$. Let N_d be the number of degree d closed points on X. Prove that $\sum_{d|n} dN_d = \#X(\mathbb{F}_{q^n})$ for each $n \geq 1$.

2.14. Use Möbius inversion to give a formula for the number of degree n monic irreducible polynomials in $\mathbb{F}_q[t]$.

2.15. Assuming that the Serre duality theorem [**Har77**, Corollary III.7.7] holds over an arbitrary field k (it does), prove the Riemann–Roch theorem (Theorem 2.5.3) for regular, projective, geometrically integral curves over k.

2.16. Give two examples of nonproper $\mathbb{R}$-varieties X such that $X(\mathbb{R})$ is compact in the analytic topology, one with $X(\mathbb{R})$ empty and one with $X(\mathbb{R})$ nonempty.

2.17. Let k be a global field. Let X be a k-variety with a k_v-point for every v. Prove that X satisfies weak approximation if and only if for every finite set S of places and any nonempty open sets $U_v \subseteq X(k_v)$ for $v \in S$, there exists $x \in X(k)$ such that $x \in U_v$ for all $v \in S$.

Unofficial version for incidental online use

Chapter 3

Properties of morphisms

Unofficial version for incidental online use

3.1. Finiteness conditions

3.1.1. Quasi-compact and quasi-separated morphisms.

Definition 3.1.1 ([**Har77**, Exercise II.2.13])**.** A scheme X is **quasi-compact** if one of the following equivalent conditions is satisfied:

(i) The topological space of X is quasi-compact; i.e., every open cover of X has a finite subcover. (One says "quasi-compact" instead of just "compact" for clarity since some authors include "Hausdorff" as part of the latter.)

(ii) The scheme X is a finite union of affine open subsets.

Definition 3.1.2 ([**EGA I**, 6.6.1], [**EGA IV**$_1$, §1.1])**.** A morphism of schemes $f\colon X \to S$ is **quasi-compact** if one of the following equivalent conditions is satisfied:

(i) There is an affine open covering $\{S_i\}$ of S such that for each i, the scheme $f^{-1}S_i$ is quasi-compact.

(ii) For *every* affine open subset $U \subseteq S$, the scheme $f^{-1}U$ is quasi-compact.

Definition 3.1.3 ([**EGA IV**$_1$, §1.2])**.** A morphism of schemes $f\colon X \to S$ is **quasi-separated** if one of the following equivalent conditions is satisfied:

(i) There is an affine open covering $\{S_i\}$ of S such that whenever X_1, X_2 are affine open subsets of $f^{-1}S_i$, the intersection $X_1 \cap X_2$ is a union of finitely many affine open subsets.

(ii) For every affine open $U \subseteq S$ and every affine open subsets $X_1, X_2 \subseteq f^{-1}U$, the intersection $X_1 \cap X_2$ is a union of finitely many affine open subsets.

(iii) The diagonal morphism $X \to X \times_S X$ is quasi-compact.

If X is noetherian, then every open subscheme of X is quasi-compact, so every morphism $X \to S$ is both quasi-compact and quasi-separated. Most theorems about noetherian schemes use only that the schemes are quasi-compact and quasi-separated.

Example 3.1.4. Let A be a polynomial ring $k[x_1, x_2, \ldots]$ in countably many indeterminates over some field k. Let $P \in \operatorname{Spec} A$ be the closed point corresponding to the maximal ideal $(x_1, x_2, \ldots)$. Let U be the open subscheme of $\operatorname{Spec} A$ obtained by removing P. Then the open subsets $D(x_i)$ of $\operatorname{Spec} A$ form an open cover of U with no finite subcover, so U is not quasi-compact.

Example 3.1.5. With notation as in Exercise 3.1.4, let X be "infinite-dimensional affine space with a doubled origin", i.e., the scheme obtained by gluing two copies X_1, X_2 of $\operatorname{Spec} A$ along the copy of U in each. The identity morphisms $X_i \to \operatorname{Spec} A$ glue to give a morphism $X \to \operatorname{Spec} A$ that is not quasi-separated, since X_1 and X_2 are affine open subsets whose intersection is not quasi-compact.

3.1.2. Finitely presented algebras.

Definition 3.1.6 (**[EGA IV**$_1$, 1.4.1]**).** Let A be a commutative ring, and let B be an A-algebra. Then B is said to be a **finitely presented** A-algebra (or **of finite presentation over** A) if B is isomorphic as A-algebra to $A[t_1, \ldots, t_n]/I$ for some $n \in \mathbb{N}$ and some finitely generated ideal I of the polynomial ring $A[t_1, \ldots, t_n]$.

Remark 3.1.7. The only difference between "finitely generated" and "finitely presented" is the requirement in the latter that I be finitely generated as an ideal.

Proposition 3.1.8. *Let A be a commutative ring. If an A-algebra B is finitely presented, then it is finitely generated. The converse holds for noetherian A.*

Proof. Remark 3.1.7 explains why "finitely presented" implies "finitely generated". If A is noetherian, the Hilbert basis theorem says that $A[t_1, \ldots, t_n]$ is noetherian, so any ideal I in it is automatically finitely generated. $\square$

Over non-noetherian rings, the more restrictive notion "finitely presented" has better properties than "finitely generated" (which is synonymous with "of finite type"). Non-noetherian rings do come up in arithmetic geometry; for instance, the adèle ring of a global field is not noetherian.

Unofficial version for incidental online use

Example 3.1.9. Let k be a field, and let $A = k[x_1, x_2, \dots]$. Then the A-ideal $I := (x_1, x_2, \dots)$ is not finitely generated. One can show that the finitely generated A-algebra A/I is not finitely presented; see Exercise 3.1.

3.1.3. Morphisms locally of finite presentation.

Definition 3.1.10 ([**EGA IV**$_1$, 1.4.2])**.** Let $f\colon X \to S$ be a morphism of schemes, let $x \in X$, and let $s = f(x)$. Then one says that f is **locally of finite presentation at** x if there exist affine open neighborhoods $V = \operatorname{Spec} A$ of s and $U = \operatorname{Spec} B$ of x such that B is of finite presentation over A. One says that f is **locally of finite presentation** (or that the S-scheme X is **locally of finite presentation**) if f is locally of finite presentation at every $x \in X$.

Remark 3.1.11. An S-scheme is locally of finite presentation if and only if "its functor of points commutes with taking direct limits of rings". More precisely, an S-scheme X is locally of finite presentation if and only if for every filtered inverse system of affine S-schemes $(\operatorname{Spec} A_i)$, the natural map $\varinjlim X(A_i) \to X(\varinjlim A_i)$ is a bijection [**EGA IV**$_3$, 8.14.2.1]. (See Definition 4.3.2 for the meaning of "affine S-scheme".) This is a version of "spreading out", to be discussed further in Section 3.2.

3.1.4. Morphisms of finite presentation.

Definition 3.1.12 ([**EGA IV**$_1$, 1.6.1])**.** A morphism $f\colon X \to S$ is of **finite presentation** if it is locally of finite presentation, quasi-compact, and quasi-separated.

The three conditions in the definition of "finite presentation" are there so that for each affine open subset $U = \operatorname{Spec} A$ of S, the scheme $f^{-1}U$ admits a finite description, as we now explain. First, the fact that f is locally of finite presentation implies that $f^{-1}U$ is covered by affine open subsets V_i, each of the form $\operatorname{Spec} B$, where B is isomorphic to an A-algebra of the form $A[t_1, \dots, t_n]/(f_1, \dots, f_m)$ for some polynomials $f_1, \dots, f_m$. Second, the fact that f is quasi-compact implies that only finitely many V_i are needed. Third, the fact that f is quasi-separated implies that the intersections $V_i \cap V_j$ are covered by finitely many affine subsets (each of finite presentation over A), so the data needed to glue the V_i to form $f^{-1}U$ are describable by a finite collection of polynomial maps with coefficients in A.

Remark 3.1.13. Suppose that S is locally noetherian. Then by Proposition 3.1.8, a morphism $f\colon X \to S$ is locally of finite presentation if and only if it is locally of finite type, and it is of finite presentation if and only if it is of finite type.

Unofficial version for individual online use

3.2. Spreading out

If X is an affine $\mathbb{Q}$-variety, then for some $N \geq 1$ there exists an affine finite-type scheme $\mathcal{X}$ over $\mathbb{Z}[1/N]$ whose generic fiber $\mathcal{X}_{\mathbb{Q}}$ is isomorphic to X: simply let N be the product of the denominators appearing in the finitely many coefficients appearing in the finitely many polynomials defining X.

We can generalize this by replacing $\mathbb{Z}$ and $\mathbb{Q}$ by any integral scheme S and its generic point, respectively. In general, the principle of "spreading out" is that for schemes of finite presentation, whatever happens over the generic point also happens over some open neighborhood of the generic point.

Theorem 3.2.1 (Spreading out)**.** *Let S be an integral scheme, and let K be its function field. Let* blah *denote a property for which a positive answer is listed in the "Spreading out" column of Table 1 on pp. 302–303.*

(i) (Spreading out schemes) *Suppose that X is a scheme of finite presentation over K. Then there exist a dense open subscheme $U \subseteq S$ and a scheme $\mathcal{X}$ of finite presentation over U such that $\mathcal{X}_K \simeq X$; see Figure 1.*

(ii) (Spreading out properties of schemes) *Suppose that $\mathcal{X} \to S$ is of finite presentation. If $\mathcal{X}_K \to \operatorname{Spec} K$ is blah, then there exists a dense open subscheme $U \subseteq S$ such that $\mathcal{X}_U \to U$ is blah.*

(iii) (Spreading out morphisms) *Suppose that $\mathcal{X}$ and $\mathcal{X}'$ are schemes of finite presentation over S, and $f\colon \mathcal{X}_K \to \mathcal{X}'_K$ is a K-morphism. Then there exists a dense open subscheme $U \subseteq S$ such that f extends to a U-morphism $\mathcal{X}_U \to \mathcal{X}'_U$.*

(iv) (Spreading out properties of morphisms) *Let $f\colon \mathcal{X} \to \mathcal{X}'$ be an S-morphism between schemes of finite presentation over S. If $f\colon \mathcal{X}_K \to \mathcal{X}'_K$ is blah, then there exists a dense open subscheme $U \subseteq S$ such that $f|_U\colon \mathcal{X}_U \to \mathcal{X}'_U$ is blah.*

Sketch of proof. In all parts, we may replace S by an affine open neighborhood of the generic point to assume that $S = \operatorname{Spec} R$.

First we prove (i). Let X be a K-scheme of finite presentation. As in Section 3.1.4, X has a finite description involving only finitely many polynomials over K. Write each coefficient as a fraction of elements of R, and let R' be the localization of R obtained by adjoining the inverses of all the denominators that appear. Then the description of X over K as the scheme obtained by gluing certain affine pieces also makes sense as the description of a scheme $\mathcal{X}$ over $U := \operatorname{Spec} R'$, which is what we needed.

The proof of (iii) is similar to that of (i).

Part (iv), on the other hand, requires a separate proof for each possibility for blah. See Table 1 on pp. 302–303 for references.

Unofficial version for noncommercial online use

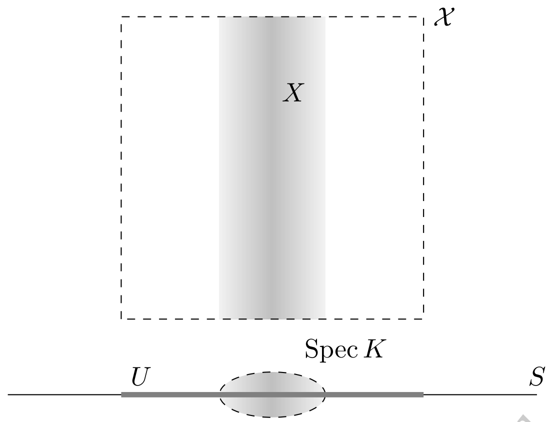

Figure 1. Spreading out X to $\mathcal{X}$

Part (ii) is the special case of (iv) with $\mathcal{X}' = S$. □

Remark 3.2.2 (Spreading out to an open neighborhood of a point)**.** Theorem 3.2.1(i) can be generalized as follows. Let S be any scheme, and let $s \in S$. Then a scheme X of finite presentation over Spec $\mathscr{O}_{S,s}$ can be spread out to a scheme $\mathcal{X}$ of finite presentation over some open neighborhood of s in S. The other parts of Theorem 3.2.1 generalize similarly.

Remark 3.2.3. The ring $\mathscr{O}_{S,s}$ is the injective limit of the coordinate rings of the affine open neighborhoods of s in S, so Spec $\mathscr{O}_{S,s}$ is a projective limit of schemes. This suggests an even more general version of Theorem 3.2.1, for projective limits of schemes. This is the setting considered in [**EGA IV**$_3$, §8.10].

In the following sections, we give some standard applications of spreading out.

3.2.1. Reducing statements to the noetherian case.

Proposition 3.2.4. *Suppose that X is of finite presentation over a commutative ring A. Then there exists a noetherian ring A_0 contained in A and a scheme X_0 of finite presentation over A_0 whose base extension $(X_0)_A$ is isomorphic to X.*

Proof. Any A is the direct limit (union) of its finitely generated subrings A_0. By Remark 3.2.3, $X \simeq (X_0)_A$ for some scheme X_0 of finite presentation over a finitely generated ring A_0. (Concretely, one can take A_0 to be the $\mathbb{Z}$-subalgebra of A generated by the finitely many coefficients in a description of X.) Now $\mathbb{Z}$ is noetherian, so A_0 is noetherian too. □

Unofficial version for incidental online use

3.2.2. Specialization arguments. If X and Y are $\mathbb{Q}$-varieties whose base extensions $X_{\mathbb{Q}(t)}$ and $Y_{\mathbb{Q}(t)}$ are isomorphic, where t is an indeterminate, then one can specialize t to some rational number q, chosen carefully to avoid the poles of the finitely many rational functions appearing in the description of the isomorphism, to obtain an isomorphism $X \to Y$. This idea extends to the following.

Proposition 3.2.5 (Specializing an isomorphism)**.** *Let $k \subseteq L$ be an arbitrary extension of fields. Let X and Y be k-varieties such that $X_L \simeq Y_L$. Then $X_F \simeq Y_F$ for some* finite *extension $F \supseteq k$.*

Proof. Let $f\colon X_L \to Y_L$ be an isomorphism. The field L is the direct limit of its finitely generated k-subalgebras A. By Remark 3.2.3, f is the base extension of an isomorphism $f_A\colon X_A \to Y_A$. Let $\mathfrak{m}$ be a maximal ideal of A, and let $F := A/\mathfrak{m}$. By the weak Nullstellensatz, F is a finite extension of k. Reducing f_A modulo $\mathfrak{m}$ (i.e., taking the base change by $\operatorname{Spec} A/\mathfrak{m} \to \operatorname{Spec} A$) yields an isomorphism $X_F \to Y_F$. □

The same technique reduces many questions about varieties over an arbitrary field to the case in which the field is a number field or a finite field, depending on the characteristic. In fact, by using the arithmetic weak Nullstellensatz (Remark 2.4.5, that the quotient of a finitely generated $\mathbb{Z}$-algebra by a maximal ideal is a finite field), even the characteristic 0 case can often be reduced to the finite field case.

Alternatively, after using spreading out to pass from a general field of characteristic 0 to a finitely generated $\mathbb{Q}$-algebra B, one can embed B into $\mathbb{Q}_p$ for a suitable prime p to reduce to a question over $\mathbb{Q}_p$; see Corollary 7.7.6.

3.2.3. Models over discrete valuation rings. Let R be a discrete valuation ring, with fraction field K, residue field k, and uniformizer π. (For instance, we could have $R = \mathbb{Z}_p$, $K = \mathbb{Q}_p$, $k = \mathbb{F}_p$, $\pi = p$.) Let X be a proper K-variety. We want to make sense of the reduction of X modulo π, which should be a k-variety.

For a projective K-variety X, the lowbrow approach is to scale each defining equation of X by a power of π so that its coefficients lie in R but not all in the maximal ideal (this procedure is sometimes called "chasing denominators"), and then reduce all the coefficients modulo π. The isomorphism class of the k-variety defined by the resulting equations depends not only on the isomorphism class of X, but also on the choice of defining equations.

We want to reinterpret this construction in terms of R-schemes. The scheme $\operatorname{Spec} R$ consists of two points: the **generic point** $\eta = \operatorname{Spec} K$ corresponding to the prime (0) of R, and the **special point** or **closed point** $s = \operatorname{Spec} k$ corresponding to the maximal ideal (π) of R.

Unofficial version for incidental online use

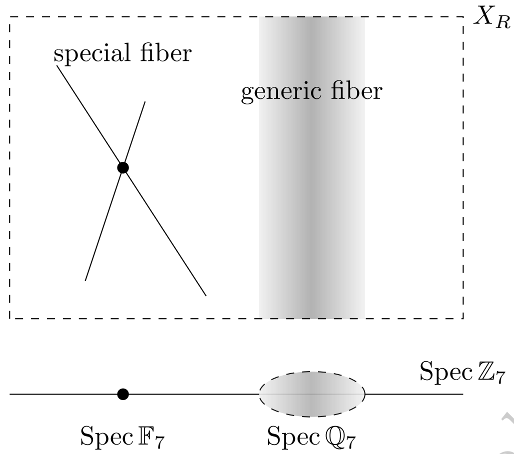

Figure 2. The model $X_R := \operatorname{Proj} \mathbb{Z}_7[x,y,z]/(xy - 7z^2)$ of Example 3.2.9

Definition 3.2.6. Let X_R be an R-scheme. The **generic fiber** of X_R is the K-scheme $X_K = X_R \times_{\operatorname{Spec} R} \operatorname{Spec} K$, and the **special fiber** of X_R is the k-scheme $X_k = X_R \times_{\operatorname{Spec} R} \operatorname{Spec} k$.

Remark 3.2.7. Schemes of finite type over discrete valuation rings or rings of S-integers of number fields are often called **arithmetic schemes** (if they satisfy other technical conditions depending on the author). In the special case where the relative dimension is 1, they are called **arithmetic surfaces**, because the base is a ring of dimension 1.

Definition 3.2.8. Let X be a K-scheme. An R-**model** of X is an R-scheme X_R equipped with an isomorphism $X_R \times_R K \xrightarrow{\sim} X$ of K-schemes.

Example 3.2.9. Let X be the $\mathbb{Q}_7$-curve $\operatorname{Proj} \mathbb{Q}_7[x,y,z]/(xy-7z^2)$. Then the schemes $\operatorname{Proj} \mathbb{Z}_7[x,y,z]/(xy-7z^2)$ and $\operatorname{Proj} \mathbb{Z}_7[x,y,z]/(xy-z^2)$, equipped with suitable isomorphisms, are $\mathbb{Z}_7$-models of X. They are not isomorphic, however, as one can see from their special fibers. See Figure 2.

According to Definition 3.2.8, X itself is yet another $\mathbb{Z}_7$-model of X.

Now, a "reduction modulo π of a K-variety X" can be understood as the special fiber of an R-model of X. Example 3.2.9 shows, however, that to get a reasonable result, one should impose additional restrictions on the model. We will do so in Section 3.5.14.

3.2.4. Models over Dedekind domains and schemes. Definition 3.2.8 makes sense for any integral domain R. A common situation, generalizing the discrete valuation ring case, is where R is a **Dedekind domain**, that is, an integrally closed noetherian domain of dimension ≤ 1. The main examples of such R are

Unofficial version for incidental online use

(1) the integer ring $\mathbb{Z}$, or, more generally, the ring of integers $\mathcal{O}_K$ of a number field,

(2) the coordinate ring of an affine regular integral curve over a field, and

(3) localizations of the above.

A scheme over a Dedekind domain has one generic fiber, and many closed fibers, one for each nonzero prime of R.

Remark 3.2.10. One can generalize even further, to integral Dedekind schemes. A **Dedekind scheme** is a noetherian normal scheme of dimension ≤ 1. Examples include

(i) $\operatorname{Spec} R$ for any Dedekind domain R;

(ii) regular curves over a field; and

(iii) schemes of the form $X - \{x\}$, where X is a normal noetherian local scheme of dimension 2 and x is its closed point. (A scheme X is **local** if it has exactly one closed point x, and x is in the closure of $\{y\}$ for all $y \in X$.) For example, X could be $\operatorname{Spec} k[s,t]_{\mathfrak{m}}$, where k is a field and $\mathfrak{m}$ is the ideal (s,t).

By Lemma 3.2.11(i)$\Rightarrow$(iii) below, any Dedekind scheme X is a disjoint union of integral Dedekind schemes, and their number is finite since X is noetherian. Also, any Dedekind scheme is covered by finitely many open sets of the form $\operatorname{Spec} R$ for Dedekind domains R.

Lemma 3.2.11. *For a locally noetherian scheme X, the following are equivalent:*

(i) *For every $x \in X$, the local ring $\mathscr{O}_{X,x}$ is an integral domain.*

(ii) *The scheme X is **locally integral**: every point has an open neighborhood that is an integral scheme.*

(iii) *The scheme X is a disjoint union of integral schemes.*

Proof. The implications (iii)$\Rightarrow$(ii) and (ii)$\Rightarrow$(i) are trivial. It remains to prove (i)$\Rightarrow$(iii).

Suppose that each local ring $\mathscr{O}_{X,x}$ is an integral domain; then each $\mathscr{O}_{x,x}$ is reduced, so X is reduced. Since irreducible and reduced together imply integral, it remains to show that the irreducible components of X are disjoint. The irreducible components passing through a given point x are in bijection with the the minimal primes of $\mathscr{O}_{X,x}$, of which there is just one (the zero ideal). Thus each x lies in exactly one irreducible component; i.e., the irreducible components are disjoint. $\square$

Unofficial version for incidental online use

3.2.5. Valuative criterion for properness. Return to the setting of Section 3.2.3, where R is a discrete valuation ring. Suppose that we have extended a K-scheme to an R-model. We now wish to speak of reducing K-points on the generic fiber to k-points of the special fiber. There is no homomorphism $K \to k$, so to make sense of this, we must first extend the K-point to an R-point of the model. For a proper scheme over a discrete valuation ring, this extension is always possible (and unique), by the $S = \operatorname{Spec} R$ case of one direction of the following:

Theorem 3.2.12 (Valuative criterion for properness [**Har77**, Theorem II.4.7 and Exercise II.4.11])**.** *Let $f\colon X \to S$ be a morphism of finite type with S noetherian. Then f is proper if and only if whenever* $\operatorname{Spec} R$ *is an S-scheme with R a discrete valuation ring and K its fraction field, the natural map $X(R) \to X(K)$ is bijective.*

We generalize the $S = \operatorname{Spec} R$ case to Dedekind domains as part (ii) of the following:

Theorem 3.2.13. *Let R be an integral domain, and let $K =$ $\operatorname{Frac} R$. Let X be an R-scheme.*

(i) *If X is separated over R, then $X(R) \to X(K)$ is injective.*
(ii) *If X is proper over R and R is a Dedekind domain, then $X(R) \to X(K)$ is bijective.*

Proof.

(i) This is a special case of Corollary 2.3.22.
(ii) Proper schemes over R or K are of finite type, hence of finite presentation, since R and K are noetherian rings. Let $f \in X(K)$. We need to extend $f\colon \operatorname{Spec} K \to X$ to an R-morphism $\operatorname{Spec} R \to X$. Apply Theorem 3.2.1(iii) to find a dense open subscheme $U \subseteq \operatorname{Spec} R$ such that f extends to a U-morphism $f_U\colon U \to X_U$, or equivalently, an R-morphism $f_U\colon U \to X$. Since R is noetherian of dimension ≤ 1, the complement $(\operatorname{Spec} R) - U$ is a finite union of closed points $\mathfrak{p}$. It suffices to extend f_U to $U \cup \{\mathfrak{p}\} \to X$ for *one* $\mathfrak{p}$, since then we can repeat the extension argument for each missing point.

    By Theorem 3.2.12, we can extend f to a morphism $\operatorname{Spec} R_{\mathfrak{p}} \to X$. Next, apply Remark 3.2.2 to spread this morphism out to an R-morphism $f_V\colon V \to X_V \subseteq X$ for some dense open $V \subseteq \operatorname{Spec} R$. The restrictions of f_U and f_V to $U \cap V$ must agree, by part (i) applied to each ring used in an affine cover of $U \cap V$. Thus we can glue to obtain an extension of f to $U \cap V$, which contains both U and $\mathfrak{p}$. $\square$

Remark 3.2.14. The same argument proves Theorem 3.2.13 more generally when R is replaced by an integral Dedekind scheme with function field

Unofficial version for incidental online use

K. Even more generally, if X is a separated (resp. proper) S-scheme, T is an integral Dedekind scheme with a morphism to S, and $K = \mathbf{k}(T)$, then $X(T) \to X(K)$ is an injection (resp. bijection); this statement can be reduced to the previous sentence by Proposition 2.3.15. For an important application, see Proposition 3.6.5(b).

Warning 3.2.15. Theorem 3.2.13(ii) does not hold for arbitrary integral domains R; see Exercise 3.3.

3.3. Flat morphisms

3.3.1. Flat modules.

(References: [**Har77**, III.§9] and [**BLR90**, §2.4])

Definition 3.3.1. Let A be a commutative ring, and let B be an A-module. Then B is **flat** if the functor $\otimes_A B$ is exact; that is, whenever

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is an exact sequence of A-modules, the induced sequence

$$0 \longrightarrow M' \otimes_A B \longrightarrow M \otimes_A B \longrightarrow M'' \otimes_A B \longrightarrow 0$$

is exact.

Examples 3.3.2.

(i) Free modules are flat. In particular, any module over a field k (that is, a vector space) is flat.
(ii) A module over a discrete valuation ring or Dedekind domain is flat if and only if it is torsion-free.
(iii) Any localization $S^{-1}A$ of A is flat.

3.3.2. Flat and faithfully flat morphisms.

Definition 3.3.3. A morphism of schemes $f\colon X \to Y$ is **flat at a point** $x \in X$ if $\mathscr{O}_{X,x}$ is flat as an $\mathscr{O}_{Y,f(x)}$-module. Also, f is called **flat** if f is flat at every $x \in X$.

Definition 3.3.4. A morphism of schemes $f\colon X \to Y$ is **faithfully flat** if f is flat and surjective.

Remark 3.3.5. Let $A \to B$ be a homomorphism of commutative rings. Then $\operatorname{Spec} B \to \operatorname{Spec} A$ is flat if and only if B is flat over A. Also, $\operatorname{Spec} B \to \operatorname{Spec} A$ is faithfully flat if and only if B is flat over A and for any nonzero A-module M one has $M \otimes_A B \neq 0$. This explains the use of the word "faithfully".

Unofficial version for incidental online use

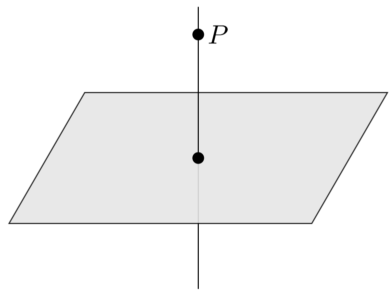

Figure 3. Dimension of a variety at a point; see Example 3.3.9

3.3.3. Dimension and relative dimension.

Definition 3.3.6 ([**EGA IV**$_1$, Chapter 0, 14.1.2]). Let X be a topological space. Its **dimension** $\dim X \in \{-\infty, 0, 1, 2, \ldots, \infty\}$ is the supremum of the set of nonnegative integers n for which there exists an n-step chain $X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$ of irreducible closed subsets of X. If $x \in X$, define the **dimension of** X **at** x as

$$\dim_x X := \inf\{\, \dim U : U \text{ is an open neighborhood of } x \text{ in } X\,\}.$$

Remark 3.3.7. The empty space is not irreducible. We have $\dim X = -\infty$ if and only if $X = \emptyset$.

Warning 3.3.8. The definition of $\dim_x X$ differs from the definition in [**Har77**, Proposition III.9.5] for schemes, where it is defined as $\dim \mathscr{O}_{X,x}$. For example, if x is the generic point of an integral k-variety X, then $\dim_x X = \dim X$ according to the definition above from [**EGA IV**$_1$, Chapter 0, 14.1.2], but $\dim \mathscr{O}_{X,x} = 0$ since $\mathscr{O}_{X,x}$ is a field. See Theorem 3.3.10 for the relationship more generally.

Example 3.3.9. Let $X \subseteq \mathbb{A}^3_k = \operatorname{Spec} k[x,y,z]$ be the union of the plane $z = 0$ and the line $x = y = 0$ over a field k. Let P be the point $(0,0,1)$ of X. Then $\dim X = 2$, but $\dim_P X = 1$. See Figure 3.

Theorem 3.3.10. *Let X be a scheme that is locally of finite type over a field k. Let $x \in X$. Then*

$$\dim_x X = \dim \mathscr{O}_{X,x} + \operatorname{tr\,deg}(\mathbf{k}(x)/k).$$

Proof. See [**EGA IV**$_2$, 5.2.3]. □

Definition 3.3.11. If $f\colon X \to S$ is a continuous map of topological spaces, and $x \in X$, define the **relative dimension of** X **over** S **at** x as

$$\dim_x f := \dim_x f^{-1}(f(x)).$$

Unofficial version for incidental online use

Proposition 3.3.12. *Let $f: X \to S$ be a flat k-morphism between irreducible k-varieties. Then $\dim_x f = \dim X - \dim S$. In particular, $\dim_x f$ is independent of x.*

Proof. This is a special case of [**Har77**, Corollary III.9.6]. □

3.4. Fppf and fpqc morphisms

(Reference: [**Vis05**, §2.3])

The notions in this section will play an important role in the definition of "topologies" finer than the Zariski topology, for use in faithfully flat descent (Chapter 4) and in the construction of cohomology theories (Chapter 6).

Definition 3.4.1. A morphism of schemes $X \to Y$ is **fppf** if it is faithfully flat and locally of finite presentation.

Proposition 3.4.2. *A morphism $f: X \to Y$ that is flat and locally of finite presentation is **open**; i.e., for every open subset $U \subseteq X$, the set $f(U)$ is open in Y.*

Proof. Here is a very brief sketch:

(1) Reduce to proving that $f(X)$ is open in Y when X and Y are affine and $X \to Y$ is of finite presentation.
(2) Use Proposition 3.2.4 to assume moreover that Y is noetherian.
(3) Chevalley's theorem states for a finite-type morphism between noetherian schemes, $f(X)$ is **constructible**, i.e., a finite boolean combination of open subsets.
(4) Flatness implies that $f(X)$ is **stable under generization** (one says that y_1 is a **generization** of y_2 if y_2 belongs to the closure of $\{y_1\}$ in Y, and the conclusion here means that any generization of a point of $f(X)$ is again in $f(X)$).
(5) In a noetherian scheme, a subset is open if and only if it is constructible and stable under generization [**Har77**, Exercise II.3.18(c)].

See [**EGA IV**$_2$, 2.4.6] for details. □

Definition 3.4.3 (Kleiman [**Vis05**, 2.34])**.** A morphism of schemes $X \to Y$ is **fpqc** if it is faithfully flat and every quasi-compact open subset of Y is the image of a quasi-compact open subset of X.

Example 3.4.4. Let Y be a positive-dimensional k-variety. For each point $y \in Y$, there is a morphism $\operatorname{Spec} \mathscr{O}_{Y,y} \to Y$. Let X be the disjoint union $\coprod_{y \in Y} \operatorname{Spec} \mathscr{O}_{Y,y}$. Then the natural morphism $X \to Y$ is faithfully flat but not fpqc.

Unofficial version for incidental online use

Remark 3.4.5. Both fppf and fpqc are French acronyms: fppf stands for "fidèlement plat de présentation finie" and fpqc stands for "fidèlement plat quasi-compact". Our (slightly nonstandard) definitions of fppf and fpqc are less restrictive than a direct translation would suggest; this is so that fppf and fpqc morphisms include Zariski open covering morphisms. See Proposition 3.8.2.

3.5. Smooth and étale morphisms

(Reference: [**MO15**, 5.3–5.4], [**Ray70a**], [**BLR90**, §2.2])

Section I.5 of [**Har77**] gives two equivalent definitions of "nonsingular" for varieties over an algebraically closed field. These definitions disagree over imperfect fields, so we will avoid the term "nonsingular" and instead use "regular" and "smooth" for the two distinct notions.

3.5.1. Regular schemes.

Recall the following definition:

Definition 3.5.1. A scheme X is **regular** if X is locally noetherian and $\mathscr{O}_{X,x}$ is a regular local ring for every $x \in X$.

Remark 3.5.2. The localization of a regular local ring at a prime ideal is a regular local ring [**Eis95**, 19.14]. Thus, for X locally of finite type over a field or over $\mathbb{Z}$, one gets an equivalent definition if one checks the local rings at only the *closed* points x.

Remark 3.5.3. Definition 3.5.1 agrees with the definitions of nonsingular given in [**Har77**, p. 32] for quasi-projective integral varieties over an algebraically closed field and [**Har77**, p. 177] for arbitrary integral varieties over an algebraically closed field.

Remark 3.5.4. "Regular" is an absolute notion: if X is an S-scheme, the question of whether X is regular ignores the structure morphism $X \to S$. In contrast, "smooth" is relative: we will speak of an S-scheme X being smooth over S, and this does depend on more than the structure of X as a scheme.

Proposition 3.5.5. *A regular scheme is a disjoint union of integral schemes.*

Proof. Regular local rings are integral domains [**Eis95**, Corollary 10.14]. Apply Lemma 3.2.11. □

Corollary 3.5.6. *A connected regular scheme is integral.*

Unofficial version for incidental online use

3.5.2. Inspiration from differential geometry. (This section is purely motivational.) The notion of smooth variety is an algebraic version of the notion of (smooth) manifold. In particular, we want the definition to have the following property: for a $\mathbb{C}$-variety X,

$$X \text{ is smooth over } \mathbb{C} \iff X^{\text{an}} \text{ is a manifold,} \tag{3.5.7}$$

where the condition on the right means that X^{an} can be covered by open subsets isomorphic *as complex analytic spaces* to open subsets of $\mathbb{C}^n$.

Warning 3.5.8. It is not enough to require that $X(\mathbb{C})$ be locally isomorphic as *topological space* to open subsets of $\mathbb{C}^n$: one problem with this is that this would not distinguish X from its associated reduced variety X_{red}. Nonreduced varieties should never be considered smooth.

Stupid Idea 3.5.9. We might try adapting the definition of manifold to the algebraic setting and come up with the following "definition":

> "A $\mathbb{C}$-variety is smooth of dimension r if and only if it is covered by Zariski open subschemes each isomorphic to an open subscheme of $\mathbb{A}^r_{\mathbb{C}}$."

But this would be wrong, in the sense that it would violate (3.5.7): If X is defined by $x^3 + y^3 = 1$ in $\mathbb{A}^2_{\mathbb{C}}$, then X^{an} is a manifold, so X should be smooth, but it turns out that X is not birational to affine space, so it does not satisfy the "definition". The Zariski topology is simply too coarse: It does not have enough open sets.

Remark 3.5.10. Stupid Idea 3.5.9 actually works if one uses the étale topology instead of the Zariski topology. But the definition of the étale topology requires the notion of étale morphism, which we have not yet defined. And in fact, one definition of étale morphism depends on the definition of smooth.

There is a different characterization of manifolds that does adapt well to the algebraic setting. A subset $X \subseteq \mathbb{C}^n$ is a complex manifold of dimension r if and only if in a neighborhood of each $x \in X$ it is locally the intersection of $n - r$ analytic hypersurfaces $H_{r+1}, \ldots, H_n$ meeting transversely. Here each H_i is defined as the zero set of a holomorphic function g_i defined on a neighborhood of x in $\mathbb{C}^n$. The condition that the hypersurfaces meet transversely at x means that the $n - r$ tangent spaces $T_x H_i$ at x (each a subspace of codimension ≤ 1 of the tangent space $T_x \mathbb{C}^n$) intersect in a subspace of codimension $n - r$, that is, dimension r. Dually, this means that the differentials $dg_i(x)$ evaluated at x are linearly independent in the cotangent space of $\mathbb{C}^n$ at x. In terms of coordinates $t_1, \ldots, t_n$ on $\mathbb{C}^n$, this means that the rows of the $(n - r) \times n$ **Jacobian matrix** J with entries $J_{ij} := \partial g_i / \partial t_j$ evaluated at x are independent. In other words, J has rank $n - r$ when evaluated at x.

Unofficial version for incidental online use

Remark 3.5.11. It is the implicit function theorem which shows that the linear independence of differentials makes X a manifold. More explicitly, if one extends the list $g_{r+1}, \ldots, g_n$ to a list of holomorphic functions $g_1, \ldots, g_n$ in a neighborhood of x in $\mathbb{C}^n$ such that $dg_1(x), \ldots, dg_n(x)$ form a *basis* for the cotangent space of $\mathbb{C}^n$ at x, then $(g_1, \ldots, g_r)$ defines a biholomorphic map between an open neighborhood of x in X and an open subset of $\mathbb{C}^r$. The functions $g_1, \ldots, g_r$ restricted to X (or rather, to the open neighborhood of x in X on which they are defined) are called **local coordinates** at x, because they correspond under the biholomorphic map to the standard coordinates on (an open subset of) $\mathbb{C}^n$.

3.5.3. Summary of the definitions of smooth. A definition of "smooth" for morphisms $X \to S$ between schemes of finite type over a field is given in [**Har77**, III.§10], but in arithmetic geometry it is sometimes necessary to work in greater generality: for instance, S might be $\operatorname{Spec} \mathbb{Z}_p$.

So we want to define what it means for a morphism of schemes $f\colon X \to S$ to be smooth, or in other words, what it means for an S-scheme X to be smooth (over S). There are several approaches, yielding equivalent definitions, each with its own virtues. We summarize three of them here:

(1) *Generalize the differential criterion given at the beginning of* [**Har77**, I.§5] *to make everything relative to a base scheme S instead of* $\operatorname{Spec} k$. This definition yields a practical criterion for testing smoothness. A variant of it is used as a starting point in [**BLR90**, §2.2]. See Section 3.5.4.

(2) *Work fiber by fiber.* Roughly, first define a k-variety X to be smooth if and only if it is geometrically regular; then define a morphism $f\colon X \to S$ to be smooth if and only if the fiber $f^{-1}(s)$ is smooth over the residue field $\mathbf{k}(s)$ for each $s \in S$. Actually, in the first step one should work more generally with X *locally of finite type* over a field, and then for morphisms to an arbitrary S one needs technical conditions (locally of finite presentation, and flat) to make sure that the fibers are locally of finite type and that the fibers form a decent family, respectively. This definition provides perhaps the clearest visualization of what a smooth S-scheme looks like, but it is not as useful as a starting point for proving things. See Section 3.5.6.

(3) *Characterize smooth morphisms by the "infinitesimal lifting property".* This definition, due to Grothendieck, is elegant, though less intuitive. Also, variants give definitions of the related adjectives G-unramified and étale. See Section 3.5.12.

3.5.4. Definition 1 of smooth: The differential criterion.

Unofficial version for internal online use

Definition 3.5.12. Let $r \in \mathbb{N}$. Let $f\colon X \to S$ be a morphism of schemes, and let $x \in X$.

(i) (Special case) Suppose that f is

$$\operatorname{Spec} \frac{A[t_1, \ldots, t_n]}{(g_{r+1}, \ldots, g_n)} \quad \longrightarrow \quad \operatorname{Spec} A.$$

Then f is **obviously smooth of relative dimension** r **at** x if and only if the matrix

$$\left(\frac{\partial g_i}{\partial t_j}(x)\right) \quad \in \quad \mathrm{M}_{(n-r)\times n}(\mathbf{k}(x))$$

has rank $n-r$.

(ii) (General case) An arbitrary f is **smooth of relative dimension** r **at** x if and only if there exist open neighborhoods $U \subseteq X$ of x and $V \subseteq S$ of $f(x)$ such that $f(U) \subseteq V$ and $f|_U\colon U \to V$ is isomorphic to a morphism that is obviously smooth of relative dimension r at x.

Remark 3.5.13. For an A-morphism

$$X := \operatorname{Spec} \frac{A[t_1, \ldots, t_n]}{(g_{r+1}, \ldots, g_n)} \xrightarrow{f} \quad \operatorname{Spec} A,$$

f is smooth of relative dimension r at x if and only if f is obviously smooth of relative dimension r at x. (One way to prove this is to give an intrinsic characterization of "obviously smooth": e.g., f as above is obviously smooth of relative dimension r at x if and only if $\mathscr{O}_{X_{\mathbf{k}(x)},x}$ is a regular local ring.) Thus we can dispense with the made-up terminology "obviously smooth" and just say "smooth" from now on.

Definition 3.5.14. Let $f\colon X \to S$ be a morphism of schemes. We say that X is **smooth over** S, or that X is a **smooth** S**-scheme**, or that f is **smooth**, if at each $x \in X$ the morphism is smooth of some relative dimension.

Remark 3.5.15. If $f\colon X \to S$ is smooth of relative dimension r at x, then f is of relative dimension r at x. (In proving this, one can reduce first to the special case, and then to the case where $S = \operatorname{Spec} k$ for a field k.)

Definition 3.5.16. The **smooth locus** of $f\colon X \to S$ is the subset

$$X^{\mathrm{smooth}} := \{\, x \in X : \ f \text{ is smooth at } x \,\} \quad \subseteq X.$$

Its complement $X^{\mathrm{sing}} := X - X^{\mathrm{smooth}}$ is called the **singular locus** or **non-smooth locus**.

Proposition 3.5.17. *The subset X^{smooth} is open in X.*

Proof. We may assume we are in the special case of Definition 3.5.12. If the matrix of derivatives has maximal rank $n-r$ at a point x, then some

Unofficial version for incidental online use

$(n-r) \times (n-r)$ minor is nonvanishing at x, and will be nonvanishing in some open neighborhood U of x. Then $U \subseteq X^{\text{smooth}}$. $\square$

Warning 3.5.18. The smooth locus can be empty, even for nonempty varieties over a field. See Example 3.5.65.

Proposition 3.5.19. *If $X \to S$ is smooth of relative dimension r, then the $\mathscr{O}_X$-module $\Omega_{X/S}$ is locally free of rank r.*

Proof. The construction of $\Omega_{X/S}$ is local on X and S, so we may reduce to the special case of Definition 3.5.12, and we may assume that a particular $(n-r) \times (n-r)$ minor of $\left(\frac{\partial g_i}{\partial t_j}(x)\right)$ is a unit in the ring

$$B := A[t_1, \ldots, t_n]/(g_{r+1}, \ldots, g_n).$$

By [**Eis95**, §16.1], $\Omega_{B/A}$ is the quotient of the free B-module with basis $dt_1, \ldots, dt_n$ by the relations $\sum_{j=1}^{n} \frac{\partial g_i}{\partial t_j} dt_j$ for $i = r+1, \ldots, n$. This quotient is a free B-module of rank r, with basis consisting of the dt_j for which the index j is not involved in the $(n-r) \times (n-r)$ minor above. $\square$

Remark 3.5.20. There is a partial converse to Proposition 3.5.19. Suppose that $f \colon X \to S$ is a flat morphism between irreducible k-varieties. Let $r := \dim X - \dim S$. Then f is smooth of relative dimension r if and only if $\Omega_{X/S}$ is locally free of rank r.

Warning 3.5.21. If $\Omega_{X/S}$ is locally free of the wrong rank, then the morphism $X \to S$ is not smooth. For example, if k is a field of characteristic p, then the 0-dimensional irreducible k-scheme $X := \operatorname{Spec} k[\epsilon]/(\epsilon^p)$ is such that $\Omega_{X/k}$ is locally free of rank 1. This X is not smooth of any relative dimension over k.

3.5.5. Smooth vs. regular. The relationship between "smooth" and "regular" over arbitrary fields is given by the following generalization of [**Har77**, Theorem I.5.1]:

Proposition 3.5.22. *Let X be locally of finite type over a field k.*

(i) *X is smooth if and only if X is geometrically regular.*

(ii) *If X is smooth, then X is regular; the converse holds if k is perfect.*

(iii) *For a closed point $x \in X$ with $\mathbf{k}(x)/k$ separable, the variety X is smooth at x if and only if X is regular at x (i.e., $\mathscr{O}_{X,x}$ is a regular local ring).*

Proof. See [**BLR90**, §2.2, Proposition 15] and its proof. $\square$

Example 3.5.23 (Regular variety that is not smooth)**.** Let k be the imperfect field $\mathbb{F}_p(t)$, where p is odd and t is an indeterminate. Let X be the curve

Unofficial version for incidental online use

$y^2 = x^p - t$ in $\mathbb{A}^2_k$, so $X = \operatorname{Spec} k[x,y]/(f)$ with $f := y^2 - (x^p - t)$. Since f is irreducible even in $\overline{k}[x,y]$, the curve X is geometrically integral. We will show that X is regular but not smooth. Let P be the closed point of X corresponding to the maximal ideal $(x^p - t, y)$ of $k[x,y]$. The subscheme of X defined by $f = \partial f/\partial x = \partial f/\partial y = 0$ is $\{P\}$, so X is smooth everywhere except at P (where it is definitely not smooth). This implies that X is regular except possibly at P, but we will find that X is regular even at P. Let $\mathfrak{m}_P$ be the maximal ideal of $\mathscr{O}_{X,P}$, so $\mathbf{k}(P) := \mathscr{O}_{X,P}/\mathfrak{m}_P \simeq k[x,y]/(x^p - t, y)$. We must compute the $\mathbf{k}(P)$-dimension of

$$\frac{\mathfrak{m}_P}{\mathfrak{m}_P^2} \simeq \frac{(x^p - t, y)}{(x^p - t, y)^2 + (f)}.$$

Now $\frac{(x^p - t, y)}{(x^p - t, y)^2}$ is a 2-dimensional $\mathbf{k}(P)$-vector space spanned by $x^p - t$ and y (not surprising, given that $\mathbb{A}^2_k$ is regular of dimension 2), and the image of f in this vector space is nonzero, so

$$\dim \frac{\mathfrak{m}_P}{\mathfrak{m}_P^2} = \dim \frac{(x^p - t, y)}{(x^p - t, y)^2 + (f)} = 1 = \dim X = \dim \mathscr{O}_{X,P}.$$

Thus $\mathscr{O}_{X,P}$ is a regular local ring. So X is regular at P.

To summarize, X is regular, and smooth everywhere except at P. By Proposition 3.5.22, X is not geometrically regular; this can also be checked directly, by examining the point on $X_{\overline{k}}$ corresponding to the maximal ideal $(x - t^{1/p}, y)$ of $\overline{k}[x,y]$.

Example 3.5.24. Let k be a field, let $S = \mathbb{A}^1_k = \operatorname{Spec} k[t]$, and let X be the S-scheme $\operatorname{Spec} k[t][x,y]/(xy - t)$. In other words, X is a family of hyperbolas depending on a parameter t, which degenerates to a union of two lines when $t = 0$. The Jacobian matrix for $X \to S$ is $\begin{pmatrix} y & x \end{pmatrix}$. Thus the nonsmooth locus of $X \to S$ is the subscheme $y = x = xy - t = 0$ of $\operatorname{Spec} k[t][x,y] = \mathbb{A}^3_k$. This consists of the single point $(0,0,0) \in \mathbb{A}^3(k)$. In other words, all the fibers of $X \to S$ are smooth except for the fiber above $t = 0$, which has a single singularity.

Although X is not smooth over S, we have $k[t][x,y]/(xy - t) \simeq k[x,y]$, so $X \simeq \mathbb{A}^2_k$ (the projection $\mathbb{A}^3_k \to \mathbb{A}^2_k$ to the (x,y)-plane maps X isomorphically to its image); thus X is smooth over k. In particular X is regular, even geometrically regular.

Example 3.5.25. Let $X = \operatorname{Spec} \mathbb{Z}[x,y]/(xy - 7)$, and let π be the unique morphism from X to $\operatorname{Spec} \mathbb{Z}$. The same computation as in the previous example shows that the nonsmooth locus of π consists of the single point given by the maximal ideal $(x, y, 7)$ of $\mathbb{Z}[x,y]$; in geometric terms, it is the point $(0,0)$ on the fiber above the prime (7) of $\operatorname{Spec} \mathbb{Z}$. If U is the open subset $\operatorname{Spec} \mathbb{Z}[1/7]$ of $\operatorname{Spec} \mathbb{Z}$, then $\pi^{-1}U \to U$ is smooth.

Unofficial version for incidental online use

Again, one can check that X is regular.

3.5.6. Definition 2 of smooth: Geometrically regular fibers. For a morphism that is flat and locally of finite presentation, smoothness can be tested fiberwise:

Proposition 3.5.26. *Let $f: X \to S$ be a morphism that is locally of finite presentation. Let $x \in X$, and let $s = f(x)$. Let X_s be the fiber $f^{-1}(s)$. Then f is smooth of relative dimension r at x if and only if f is flat at x and X_s is smooth of relative dimension r over the residue field $\mathbf{k}(s)$ at x.*

Proof. See [**BLR90**, §2.4, Proposition 8]. □

Combining Propositions 3.5.26 and 3.5.22 shows that Definition 3.5.12 is equivalent to the following:

Definition 3.5.27 (cf. [**EGA IV**$_2$, §6.8.1]). A morphism of schemes $f: X \to S$ is **smooth** if all of the following hold:

- f is flat;
- f is locally of finite presentation; and
- for all $s \in S$, the fiber X_s over $\mathbf{k}(s)$ is geometrically regular.

For $x \in X$, the morphism f is called **smooth at** x if there is an open neighborhood U of x such that $f|_U: U \to S$ is smooth.

3.5.7. Unramified morphisms. Let $A \hookrightarrow B$ be an inclusion of discrete valuation rings, with uniformizers π_A and π_B, respectively. In algebraic number theory, the extension B over A is called **unramified** if and only if the maximal ideal (π_B) of B is generated by π_A and the residue field extension $B/(\pi_B)$ over $A/(\pi_A)$ is a finite separable extension (or separable algebraic if one is considering infinite extensions).

This definition can be generalized to local rings. Recall that a homomorphism $f: A \to B$ between local rings with maximal ideals $\mathfrak{m}_A$ and $\mathfrak{m}_B$ is called **local** if $f^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$ [**Har77**, p. 73].

Definition 3.5.28. A local homomorphism of local rings $f: A \to B$ with maximal ideals $\mathfrak{m}_A$ and $\mathfrak{m}_B$ is **unramified** if $f(\mathfrak{m}_A)B = \mathfrak{m}_B$ and $B/\mathfrak{m}_B$ is a finite separable extension of $A/\mathfrak{m}_A$.

Example 3.5.29. Let $A = \mathbb{C}[[z]]$, and let $B = A[\sqrt{z}] = \mathbb{C}[[\sqrt{z}]]$. Let $f: A \to B$ be the inclusion. Then $\mathfrak{m}_A = (z)$, but $f(\mathfrak{m}_A)B = (\sqrt{z})^2 B \neq (\sqrt{z})B = \mathfrak{m}_B$, so B is not unramified over A.

Remark 3.5.30. Definition 3.5.28 relates to the ordinary English meaning of "ramified" as "branched", as we now explain. Example 3.5.29 is related to the

Unofficial version for incidental online use

fact that there is no single-valued branch of $\sqrt{z}$ defined in a neighborhood of the origin; the map from the associated Riemann surface down to the complex plane is generically 2-to-1, with "the branches coming together" above $z = 0$.

Definition 3.5.31 ([**SP**, Tag 02G4])**.** Let $f\colon X \to S$ be a morphism of schemes, and let $x \in X$. Then f is **unramified at** x if f is locally of finite type at x and $\mathscr{O}_{S,f(x)} \to \mathscr{O}_{X,x}$ is an unramified homomorphism of local rings. Also, f is called **unramified** if f is unramified at every $x \in X$.

Warning 3.5.32. There is a variant in which "locally of finite type" is replaced by "locally of finite presentation". Following [**SP**, Tag 02G4], we reserve the adjective **G-unramified** for this more restrictive variant. In fact, the original definition of unramified in [**EGA IV**$_4$, 17.3.1] is what we are calling G-unramified. The decision to require only "locally of finite type" was made in [**Ray70a**, Chapitre I, Définition 4].

Example 3.5.33. Open and closed immersions are unramified. But not all closed immersions are G-unramified; this is one of the advantages of unramified over G-unramified.

See [**BLR90**, §2.2, Definition 1 and Proposition 2] for some equivalent definitions.

3.5.8. Étale morphisms.

Definition 3.5.34. A morphism $f\colon X \to S$ is **étale at a point** $x \in X$ if it is flat at x and G-unramified at x. Also, f is **étale** if f is étale at every $x \in X$.

Étale morphisms can be thought of as the algebraic analogue of locally biholomorphic maps in differential geometry. In fact, a morphism of $\mathbb{C}$-varieties $X \to Y$ is étale if and only if the induced morphism $X^{\mathrm{an}} \to Y^{\mathrm{an}}$ between complex analytic spaces is locally biholomorphic (that is, each point $x \in X^{\mathrm{an}}$ has an open neighborhood that is mapped isomorphically to its image).

Alternatively, étale morphisms can be thought of as generalizations of finite separable extensions of fields, as the following proposition suggests.

Proposition 3.5.35. *Let k be a field, and let X be a k-scheme. The following are equivalent:*

(i) *X is unramified over k.*
(ii) *X is étale over k.*
(iii) *X is a disjoint union of k-schemes of the form* $\operatorname{Spec} L$ *where each L is a finite separable extension of k.*

Unofficial version for incidental online use

Proof.

(i)$\Leftrightarrow$(ii): Over a field, flatness is automatic, and "locally of finite type" coincides with "locally of finite presentation".

(iii)$\Rightarrow$(i): Immediate from the definition of unramified.

(i)$\Rightarrow$(iii): By definition, X is locally of finite type. The question is local on X, so we may assume that $X = \operatorname{Spec} A$ for some finitely generated k-algebra A. The definition of unramified implies that each local ring $\mathscr{O}_{X,x}$ is a finite separable extension of k, so $\dim A = 0$. Hence A is artinian [**AM69**, Theorem 8.5] and is a finite product of local artinian rings [**AM69**, Theorem 8.7], each of which is a finite separable extension of k. $\square$

Corollary 3.5.36. *If $f\colon X \to S$ is an unramified morphism of schemes, then the relative dimension $\dim_x f$ is 0 for all $x \in X$.*

Proof. Let $s = f(x)$. Unramified morphisms are stable under base change, so the fiber X_s is unramified over $\operatorname{Spec} \mathbf{k}(s)$. Then $\dim X_s = 0$ by Proposition 3.5.35. $\square$

The following characterization of étale morphisms is sometimes taken as a definition.

Proposition 3.5.37. *A morphism $f\colon X \to S$ is étale at a point $x \in X$ if and only if it is smooth of relative dimension 0 at x.*

Proof. This follows from [**BLR90**, §2.4, Proposition 8]. $\square$

The primitive element theorem states that a finite separable extension of a field k is generated by one element. Proposition 3.5.39 is a generalization.

Definition 3.5.38. Let A be a commutative ring. Let $p \in A[t]$ be a monic polynomial. Let $B = A[t]/(p)$. Let $C = B[q^{-1}]$ for some $q \in B$. If the image of $p'(t)$ in C is in $C^\times$, then $\operatorname{Spec} C \to \operatorname{Spec} A$ is called a **standard étale morphism**.

Geometrically, the condition $p'(t) \in C^\times$ says that the fiber above each point of $\operatorname{Spec} A$ looks like the set of zeros of a separable polynomial; see Figure 4, in which we view q as an element of $A[t]$ instead of its image in $A[t]/(p)$.

Proposition 3.5.39 (Local structure of an étale morphism)**.** *Let $f\colon X \to S$ be a morphism of schemes, let $x \in X$, and let $s = f(x) \in S$. Then f is étale at x if and only if there exist affine open neighborhoods $X' \subseteq X$ of x and $S' \subseteq S$ of s with $f(X') \subseteq S'$ such that $f|_{X'}\colon X' \to S'$ is a standard étale morphism.*

Unofficial version for incidental online use

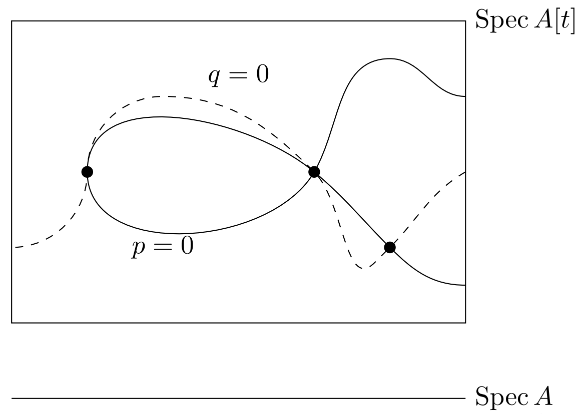

Figure 4. A standard étale morphism

Proof. The proof relies on Zariski's main theorem; see [**Ray70a**, V.§1, Théorème 1] and [**BLR90**, §2.3, Proposition 3]. □

3.5.9. Fundamental groups.

(Reference: [**Sza09**])

3.5.9.1. *Fundamental groups in topology.* Let X be a topological space that is reasonably nice (e.g., path connected, locally path connected, and locally simply connected). A **cover** of X is a map of topological spaces $Y \xrightarrow{p} X$ such that X can be covered by open subsets U such that $p^{-1}U \to U$ is isomorphic to a disjoint union of copies of U each mapping by the identity to U. A **morphism of covers** is a map of topological spaces over X. The covers of X form a category $\mathbf{Covers}_X$. For $x \in X$, the **fiber functor**

$$F_x \colon \mathbf{Covers}_X \to \mathbf{Sets}$$

is the functor sending a cover $Y \xrightarrow{p} X$ to the fiber $p^{-1}(x)$.

Theorem 3.5.40. *The following groups are naturally isomorphic:*

(i) *the group of homotopy classes of loops in X based at x;*

(ii) *the group of deck transformations of the universal cover $\widetilde{X} \to X$;*

(iii) *the automorphism group of the fiber functor F_x.*

The **fundamental group** $\pi_1(X, x)$ of the pointed topological space (X, x) is any of the three groups in Theorem 3.5.40. Then F_x can be upgraded to a functor $F'_x \colon \mathbf{Covers}_X \to \{\pi_1(X, x)\text{-sets}\}$, which turns out to be an equivalence of categories.

Unofficial version for incidental online use

The space X is called **simply connected** if the only connected cover of X is given by the identity map $X \to X$. For any $x \in X$, this condition is equivalent to $\pi_1(X, x) = \{1\}$.

There is a variant of $\pi_1(X, x)$ in which $\mathbf{Covers}_X$ is replaced by the category $\mathbf{FCovers}_X$ of covers with finite fibers. The universal cover may not exist in $\mathbf{FCovers}_X$ (consider $X = \mathbb{C}^\times$; for each $n \geq 1$ the nth power map $\mathbb{C}^\times \xrightarrow{n} \mathbb{C}^\times$ defines a cover, and no finite cover can dominate them all). So the variant of the fundamental group should be defined either as the inverse limit of the deck transformation groups of the finite Galois covers of X or as the automorphism group of the restriction $F_x|_{\mathbf{FCovers}_X}$. Both approaches lead to the same group $\widehat{\pi}_1(X, x)$. This group $\widehat{\pi}_1(X, x)$ is isomorphic to the **profinite completion** of $\pi_1(X, x)$, i.e., the inverse limit of all finite quotients of $\pi_1(X, x)$.

3.5.9.2. *The étale fundamental group.* Which of the three definitions in Theorem 3.5.40 works best in the algebraic setting? Not (i): loops are not a good notion in a space with the Zariski topology. For (ii) or (iii), we need an algebraic analogue of covers. Ideally, the analogue should be such that algebraic covers of a $\mathbb{C}$-variety X roughly correspond to covers of the topological space $X(\mathbb{C})$.

A first attempt might be to apply the topological definition of cover directly to X with the Zariski topology. But there are often not enough Zariski locally trivial covers. For example, the complex manifold $\mathbb{C}^\times$ has universal cover $\mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times$ and fundamental group $\mathbb{Z}$, but the corresponding algebraic variety $\mathbb{A}^1_\mathbb{C} \setminus \{0\}$ has no connected Zariski locally trivial cover.

Étale morphisms come to the rescue. Actually, étale morphisms are not quite restrictive enough, since they include open immersions like $\mathbb{A}^1_\mathbb{C} \setminus \{0\} \hookrightarrow \mathbb{A}^1_\mathbb{C}$ that do not induce a cover of topological spaces. Instead we use *finite* étale morphisms. (The morphism $\mathbb{A}^1_\mathbb{C} \setminus \{0\} \hookrightarrow \mathbb{A}^1_\mathbb{C}$ has finite fibers, but it is not finite, since $k[x, x^{-1}]$ is not a finite $k[x]$-module.)

To explain why a finite étale morphism is the algebraic analogue of a topological cover with finite fibers, we state the generalized Riemann existence theorem. Let X be a $\mathbb{C}$-variety. Let X^{an} be the associated complex analytic space; its underlying topological space is $X(\mathbb{C})$. Let $\mathbf{FEt}_X$ be the category of finite étale covers of X. There is a corresponding notion of finite étale cover of X^{an}, and we let $\mathbf{FEt}_{X^{\mathrm{an}}}$ be the corresponding category.

Theorem 3.5.41 (Generalized Riemann existence theorem)**.** *For each $\mathbb{C}$-variety X, the natural functors*

$$\mathbf{FEt}_X \to \mathbf{FEt}_{X^{\mathrm{an}}} \to \mathbf{FCovers}_{X(\mathbb{C})}$$

are equivalences of categories.

Unofficial version for incidental online use

Proof. See [**SGA 1**, Théorème XII.5.1]. □

Remark 3.5.42. In Theorem 3.5.41 it is necessary to restrict to finite covers. *Infinite* topological covers such as $\mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times$ have no algebraic analogue. They can at best be *approximated* by their finite subcovers.

Now we are prepared to define the algebraic analogue of the fundamental group. Let X be any scheme. Let x be a **geometric point** of X, i.e., a morphism $x\colon \operatorname{Spec}\Omega \to X$ for some separably closed field Ω. Pulling back a finite étale morphism $Y \xrightarrow{p} X$ by $x\colon \operatorname{Spec}\Omega \to X$ yields a finite disjoint union of copies of $\operatorname{Spec}\Omega$ (Proposition 3.5.35), and forgetting the scheme structure yields a set $p^{-1}(x)$. The **fiber functor** $F_x\colon \mathbf{FEt}_X \to \mathbf{Sets}$ sends an object $Y \xrightarrow{p} X$ to $p^{-1}(x)$.

Definition 3.5.43. The **étale fundamental group** $\pi_1^{\mathrm{et}}(X, x)$ is the group $\operatorname{Aut} F_x$. (Alternative terminology/notation: **algebraic fundamental group**, $\pi_1^{\mathrm{alg}}(X, x)$, $\widehat{\pi}_1(X, x)$.)

For a connected scheme X with a geometric point x, as (Y, y) varies over pointed connected (finite) Galois étale covers of (X, x), the Galois groups $\operatorname{Gal}(Y/X)$ form an inverse system whose inverse limit is $\pi_1^{\mathrm{et}}(X, x)$, so $\pi_1^{\mathrm{et}}(X, x)$ is a profinite group.

Example 3.5.44. If X is a $\mathbb{C}$-variety and $x \in X(\mathbb{C})$, then the generalized Riemann existence theorem (Theorem 3.5.41) shows that $\pi_1^{\mathrm{et}}(X, x)$ is the profinite completion of $\pi_1(X(\mathbb{C}), x)$.

Definition 3.5.45. Let X be a connected variety over a separably closed field. Then X is **algebraically simply connected** if it has no nontrivial connected finite étale cover. For any geometric point $x\colon \operatorname{Spec}\Omega \to X$, this is equivalent to the condition that $\pi_1^{\mathrm{et}}(X, x) = \{1\}$.

Warning 3.5.46. There exists an algebraically simply connected $\mathbb{C}$-variety X such that the topological space $X(\mathbb{C})$ is not simply connected. That is, there exists a connected $\mathbb{C}$-variety such that $\pi_1(X, x)$ is nontrivial but has trivial profinite completion. To see this, combine Example 3.5.44 with the following two facts:

1. There exists an infinite finitely presented group G with no nontrivial finite quotients [**Hig51**].
2. For any finitely presented group G, there exist an integral $\mathbb{C}$-variety X and $x \in X(\mathbb{C})$ such that $\pi_1(X(\mathbb{C}), x) \simeq G$ [**Sim11**, Theorem 12.1].

Remark 3.5.47. Toledo [**Tol93**] found a smooth projective integral variety X over $\mathbb{C}$ and $x \in X(\mathbb{C})$ such that $\pi_1(X, x) \to \pi_1^{\mathrm{et}}(X, x)$ fails to be injective. It is not known if there exists such an (X, x) with $\pi_1(X, x) \neq \{1\}$ and $\pi_1^{\mathrm{et}}(X, x) = \{1\}$.

Unofficial version for incidental online use

3.5.10. Local coordinates. The following proposition should be compared with the discussion in Remark 3.5.11.

Proposition 3.5.48. *Let $f \colon X \to S$ be smooth of relative dimension r at a point $x \in X$, and let $s = f(x)$. Then the following are equivalent for elements $g_1, \ldots, g_r \in \mathscr{O}_{X,x}$:*

(i) *The differentials $dg_1(x), \ldots, dg_r(x)$ form a basis for the (r-dimensional) cotangent space $\Omega_{X/S,x} \otimes \mathbf{k}(x)$.*

(ii) *There is an open neighborhood U of x in X to which the g_i extend, such that the S-morphism $(g_1, \ldots, g_r) \colon U \to \mathbb{A}^r_S$ is étale.*

Moreover, such $g_1, \ldots, g_r$ exist.

Proof. See [**BLR90**, §2.2, Proposition 11 and Remark 12]. □

Definition 3.5.49. An r-tuple $(g_1, \ldots, g_r)$ satisfying the equivalent conditions of Proposition 3.5.48 is called a **system of local coordinates at** x.

Remark 3.5.50. Suppose that in the setting of Proposition 3.5.48, we have $S = \operatorname{Spec} k$ and $x \in X(k)$. Then we have an isomorphism of r-dimensional k-vector spaces

$$\begin{aligned} \mathfrak{m}_x/\mathfrak{m}_x^2 &\to \Omega_{X/k,x} \otimes \mathbf{k}(x) \\ g &\mapsto dg(x). \end{aligned}$$

Thus for $g_1, \ldots, g_r$ vanishing at x, we have that $g_1, \ldots, g_r$ are local coordinates at x if and only if their images in $\mathfrak{m}_x/\mathfrak{m}_x^2$ form a basis.

Local coordinates can be used to reduce questions about smooth schemes to the case of étale schemes. For example:

Proposition 3.5.51. *Let $X \to S$ be a smooth morphism of schemes.*

(i) *If S is reduced, then X is reduced.*

(ii) *If S is normal, then X is normal.*

(iii) *If S is regular, then X is regular.*

Sketch of proof. Each statement is local on X. Proposition 3.5.48 says that locally $X \to S$ factors into an étale morphism and a morphism of the type $\mathbb{A}^n_S \to S$. Thus we reduce to proving the statements for étale morphisms of the type described in Proposition 3.5.39 and for morphisms of the type $\operatorname{Spec} A[t] \to \operatorname{Spec} A$. For these, it is a calculation; see [**Ray70a**, VII.§2] for some more details. □

3.5.11. Example: Étale schemes over a normal scheme.

(Reference: [**SGA 1**, I.10])

Unofficial version for incidental online use

We now classify étale schemes Y over a normal locally noetherian scheme X. By Proposition 3.5.51(ii), any such Y is normal and locally noetherian too. We may assume that X and Y are connected, and hence integral by Lemma 3.2.11(i)$\Rightarrow$(iii). For simplicity, we also restrict to the case where $Y \to X$ is separated; otherwise, we could get more étale X-schemes by doubling some closed points of Y, for example.

Theorem 3.5.52. *Let X be a normal connected locally noetherian scheme. Let $K = \mathbf{k}(X)$.*

(a) *Let K' be a finite separable extension of K. Let X' be the normalization of X in K'. Then $X' \to X$ is finite.*

(b) *Let $X' \to X$ be as in* (a). *Let $U' \subseteq X'$ be a nonempty open subscheme. If U' is unramified over X, then U' is a separated connected étale X-scheme ("separated" here means "separated over X").*

$$\begin{tikzcd} U' \arrow[r, hook, "\text{open}"] \arrow[dr, dotted, "\text{étale?}"'] & X' \arrow[d, "\text{normalization}"] \\ & X \end{tikzcd} \qquad \begin{tikzcd} K' \arrow[d, dash, "\text{finite separable extension}"] \\ K \end{tikzcd}$$

(c) *Every separated connected étale X-scheme Y arises as in* (b).

(d) *An étale X-scheme U' as in* (b) *is finite over X if and only if $U' = X'$.*

Proof.

(a) The question is local on X, so assume that X is affine. Now this is [**Ser79**, I.§4, Proposition 8].

(b) For the proof that $U' \to X$ is étale, see [**SGA 1**, I.9.11]. The composition $U' \to X' \to X$ of an open immersion and finite morphism is separated. Since U' is a nonempty open subscheme of the integral scheme X', it is connected.

(c) An étale morphism is locally quasi-finite, so this follows from Zariski's main theorem; see [**EGA IV**$_3$, 8.12.11].

(d) If $U' = X'$, then U' is finite over X by (a). Conversely, if U' is finite over X, then U' is finite over X', and hence proper over X', so the open subscheme U' is closed in X'. Since X' is connected, $U' = X'$. □

Definition 3.5.53. In the context of Theorem 3.5.52(a), call $K' \supseteq K$ **unramified above** X if the normalization $X' \to X$ is unramified.

Corollary 3.5.54 (Fundamental group of a normal scheme)**.** *Let X be a normal connected locally noetherian scheme. Let $K = \mathbf{k}(X)$. Let Ω be a separably closed field containing K. Let $\eta\colon \operatorname{Spec}\Omega \to X$ be the associated geometric point. Let L be the compositum of all finite separable extensions of K in Ω that are unramified above X. Then $\pi_1^{\mathrm{et}}(X, \eta) \simeq \operatorname{Gal}(L/K)$.*

Unofficial version for incidental online use

Proof. By Theorem 3.5.52(c,d), the finite étale X-schemes are the normalizations of X in finite separable extensions K' of K, so $\pi_1^{\mathrm{et}}(X, \eta)$ is the inverse limit of the groups $\operatorname{Gal}(K'/K)$ for the finite Galois extensions of this type. $\square$

Example 3.5.55. Let k be a field. A choice of separable closure gives a geometric point $\eta\colon \operatorname{Spec} k_{\mathrm{s}} \to \operatorname{Spec} k$, and $\pi_1(\operatorname{Spec} k, \eta) \simeq \operatorname{Gal}(k_{\mathrm{s}}/k)$.

Example 3.5.56. Let $\mathcal{O}_{K,S}$ be a ring of S-integers in a global field K (Definition 1.1.1). Fix a geometric point $\eta\colon \operatorname{Spec} K_{\mathrm{s}} \to \operatorname{Spec} \mathcal{O}_{K,S}$. In this case, the field $L \subseteq K_{\mathrm{s}}$ of Corollary 3.5.54 is classically called the maximal Galois extension of K unramified outside S. Then $\pi_1^{\mathrm{et}}(\operatorname{Spec} \mathcal{O}_{K,S}, \eta) \simeq \operatorname{Gal}(L/K)$.

The following will be used in Section 8.4.6:

Lemma 3.5.57 (cf. [**Har00**, proof of Lemma 5.2(1)]). *For a normal geometrically integral k-variety X with a k-point x, the following are equivalent:*

(i) $X_{k_{\mathrm{s}}}$ *is* not *algebraically simply connected; i.e.,* $\pi_1^{\mathrm{et}}(X_{k_{\mathrm{s}}}, x) \neq \{1\}$.

(ii) $X_{k_{\mathrm{s}}}$ *has a nontrivial connected finite étale cover.*

(iii) $X_{k_{\mathrm{s}}}$ *has a nontrivial geometrically integral finite étale cover.*

(iv) X *has a nontrivial geometrically integral finite étale cover.*

Proof. For each finite separable extension $L \supseteq k$, the variety X_L is normal by Proposition 3.5.51(ii). so X_{k_s} is normal too.

(iv)⇒(iii): If $Y \to X$ is a nontrivial geometrically integral finite étale cover, then so is $Y_{k_{\mathrm{s}}} \to X_{k_{\mathrm{s}}}$.

(iii)⇒(ii): Geometrically integral implies connected.

(i)⇔(ii): This is the definition of algebraically simply connected.

(ii)⇒(iii): We show that every connected finite étale cover $\mathcal{Y} \to X_{k_{\mathrm{s}}}$ is geometrically integral. First, $\mathcal{Y}$ is integral by the arguments preceding Theorem 3.5.52, so $\mathcal{Y}$ is geometrically irreducible by Proposition 2.2.19(ii)⇒(i). On the other hand, $\mathcal{Y}_{\overline{k}}$ is étale over the reduced variety $X_{\overline{k}}$, so $\mathcal{Y}_{\overline{k}}$ is reduced by Proposition 3.5.51(i). Thus $\mathcal{Y}$ is geometrically integral.

(iii)⇒(iv): By Theorem 3.5.52(c,d), nontrivial connected finite étale covers of X are the normalizations of X in the finite separable extensions of $\mathbf{k}(X)$ unramified above X, and likewise for $X_{k_{\mathrm{s}}}$. Let $\mathcal{Y} \to X_{k_{\mathrm{s}}}$ be a nontrivial geometrically integral finite étale cover. By replacing $\mathbf{k}(\mathcal{Y})$ by its Galois closure over $\mathbf{k}(X)$, and $\mathcal{Y}$ by the corresponding normalization of X, we may assume that $\mathbf{k}(\mathcal{Y})$ is Galois over $\mathbf{k}(X)$; by the proof of (ii)⇒(iii), $\mathcal{Y}$ is still geometrically integral.

We claim that $\mathcal{Y} \to X_{k_{\mathrm{s}}}$ is the base change of a geometrically integral finite étale cover $Y \to X$. To construct $Y \to X$, we will construct $\mathbf{k}(Y)$

Unofficial version for insitutional online use

and then take the normalization of X in $\mathbf{k}(Y)$. First, the tower of fields $\mathbf{k}(\mathcal{Y}) \supseteq \mathbf{k}(X_{k_s}) \subseteq \mathbf{k}(X)$ yields an exact sequence

(3.5.58)
$$1 \to \mathrm{Gal}(\mathbf{k}(\mathcal{Y})/\mathbf{k}(X_{k_s})) \to \mathrm{Gal}(\mathbf{k}(\mathcal{Y})/\mathbf{k}(X)) \to \mathrm{Gal}(\mathbf{k}(X_{k_s})/\mathbf{k}(X)) \to 1.$$

Define the fiber $\mathcal{Y}_x$ as the set of points in $\mathcal{Y}(k_s)$ above x. The group $\mathrm{Gal}(\mathbf{k}(\mathcal{Y})/\mathbf{k}(X))$ acts on $\mathcal{Y}_x$, and its subgroup $\mathrm{Gal}(\mathbf{k}(\mathcal{Y})/\mathbf{k}(X_{k_s}))$ acts simply transitively since $\mathcal{Y} \to X_{k_s}$ is Galois étale. Therefore a choice of $y \in \mathcal{Y}_x$ splits (3.5.58): the stabilizer $S := \mathrm{Stab}_{\mathrm{Gal}(\mathbf{k}(\mathcal{Y})/\mathbf{k}(X))}(y)$ maps isomorphically to $\mathrm{Gal}(\mathbf{k}(X_{k_s})/\mathbf{k}(X))$. Thus the extension $\mathbf{k}(\mathcal{Y}) \supseteq \mathbf{k}(X_{k_s})$ arises from $\mathbf{k}(\mathcal{Y})^S \supseteq \mathbf{k}(X_{k_s})^S = \mathbf{k}(X)$ by base change, i.e., by applying $\otimes_{\mathbf{k}(X)}\mathbf{k}(X_{k_s})$ or, equivalently, $\otimes_k k_s$. Taking normalizations of X in these fields shows that $\mathcal{Y} \to X_{k_s}$ is the base change of some $Y \to X$. Since $\mathcal{Y} \to X_{k_s}$ is finite étale and nontrivial, so is $Y \to X$. Since $\mathcal{Y}$ is geometrically integral, so is Y. □

3.5.12. Definition 3 of smooth: The infinitesimal lifting property.

Here is yet another equivalent definition of smooth:

Definition 3.5.59. [**EGA IV**$_4$, §17.1.1, 17.3.1]. A morphism $f\colon X \to S$ is **smooth** if and only if both of the following hold:

(i) f is locally of finite presentation; and
(ii) for every affine scheme $\operatorname{Spec} A$ equipped with a morphism to S and for every nilpotent ideal $I \subset A$, the natural map $X(A) \to X(A/I)$ is surjective.

(Here we think of X, $\operatorname{Spec} A$, and $\operatorname{Spec} A/I$ as S-schemes, so for instance, $X(A/I)$ should be interpreted as $\operatorname{Hom}_S(\operatorname{Spec} A/I, X)$. To say that I is nilpotent means that $I^n = 0$ for some n.)

For a proof that Definition 3.5.59 is equivalent to Definition 3.5.12, see [**BLR90**, §2.2, Proposition 6] or [**EGA IV**$_4$, §17.5.2].

Remark 3.5.60. Property (ii) is called the **infinitesimal lifting property**, and a morphism satisfying it alone is called **formally smooth**. One gets an equivalent condition if one allows only ideals I for which $I^2 = 0$.

Example 3.5.61. Let k be a field, and let X be the k-variety $xy = 0$ in $\mathbb{A}^2_k$. We will show that X does not satisfy property (ii), and hence is not smooth. Take $A = k[\epsilon]/(\epsilon^3)$ and $I = (\epsilon^2) \subseteq A$, so $A/I = k[\epsilon]/(\epsilon^2)$. Then the point $(\epsilon, \epsilon) \in \mathbb{A}^2(A/I)$ lies on $X(A/I)$, but there is no way to lift this to a point in $X(A)$: such a lift would have to be of the form $(\epsilon + a\epsilon^2, \epsilon + b\epsilon^2)$ for some $a, b \in k$, but $(\epsilon + a\epsilon^2)(\epsilon + b\epsilon^2) = \epsilon^2 \neq 0$ in A.

This example can be interpreted geometrically. Let $A_n := k[\epsilon]/(\epsilon^n)$. Giving an element of $X(A_2)$, i.e., a morphism $\operatorname{Spec} A_2 \to X$, is the same as giving a point $P \in X(k)$ with a tangent vector at P. More generally,

Unofficial version for incidental online use

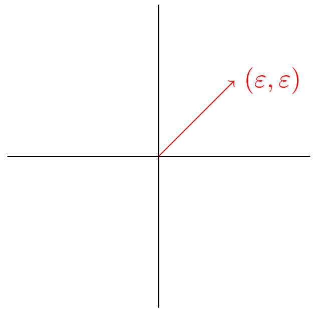

Figure 5. Failure of the infinitesimal lifting property: a tangent vector to $xy = 0$ that does not extend to a higher order jet; see Example 3.5.61

for any n, morphisms $\operatorname{Spec} A_n \to X$ are called **jets**. Let P be the origin $(0,0) \in X(k)$; then the tangent space $T_{X,P} = T_{\mathbb{A}^2,P}$ is 2-dimensional. The element $(\epsilon, \epsilon) \in X(A_2)$ corresponds to a tangent vector at P pointing along the line $y = x$; see Figure 5. Such a tangent vector, lying along neither of the two branches of X at P, will not extend to a higher order jet in X.

Remark 3.5.62. If one replaces "surjective" in Theorem 3.5.59 by "injective" or "bijective", one gets equivalent definitions for the concepts of G-unramified or étale morphisms, respectively [**EGA IV**$_4$, §17.1.1, 17.3.1].

Theorem 3.5.63 (Hensel's lemma)**.** *Let A be a complete noetherian local ring with maximal ideal $\mathfrak{m}$.*

(a) *If X is smooth over* $\operatorname{Spec} A$*, then the reduction map $X(A) \to X(A/\mathfrak{m})$ is surjective.*

(b) *If X is étale over* $\operatorname{Spec} A$*, then the reduction map $X(A) \to X(A/\mathfrak{m})$ is bijective.*

To see what Theorem 3.5.63 has to do with the Hensel's lemma in algebraic number theory, see what it says when $A = \mathbb{Z}_p$ and $X = \operatorname{Spec} \mathbb{Z}_p[t]/(f)$ where $f \in \mathbb{Z}_p[t]$ is a monic polynomial such that f modulo p is a separable polynomial in $\mathbb{F}_p[t]$.

Proof of Theorem 3.5.63. If X is smooth (resp. étale) over $\operatorname{Spec} A$, then by the infinitesimal lifting property, $X(A/\mathfrak{m}^{n+1}) \to X(A/\mathfrak{m}^n)$ is surjective (resp. bijective) for each $n \geq 1$. The theorem will follow if we can verify the technical point $X(A) = \varprojlim X(A/\mathfrak{m}^n)$. (The reader is invited to skip the rest of this proof.)

For any local ring A and scheme X, there is a bijection

$$\left\{ \begin{array}{c} \text{morphisms} \\ \operatorname{Spec} A \to X \end{array} \right\} = \left\{ (x, \phi) \;\middle|\; \begin{array}{l} x \in X, \text{ and} \\ \phi\colon \mathscr{O}_{X,x} \to A \text{ is a local homomorphism} \end{array} \right\};$$

Unofficial version for incidental online use

given a morphism $\operatorname{Spec} A \to X$, the image of the closed point of $\operatorname{Spec} A$ in X is the point x in the associated pair (x, ϕ) [**EGA I**, 2.4.4]. Thus, for our A-scheme X,

$$X(A) = \left\{ (x, \phi) \;\middle|\; \begin{array}{l} x \in X, \text{ and} \\ \phi\colon \mathscr{O}_{X,x} \to A \text{ is a local } A\text{-algebra homomorphism} \end{array} \right\},$$

and

$$X(A/\mathfrak{m}^n) = \left\{ (x, \phi) \;\middle|\; \begin{array}{l} x \in X, \text{ and} \\ \phi\colon \mathscr{O}_{X,x} \to A/\mathfrak{m}^n \text{ is a local } A\text{-alg. homomorphism} \end{array} \right\}$$

for any $n \geq 1$. This, together with the fact that A is the projective limit of $A/\mathfrak{m}^n$ in the category of rings, implies that the natural map

$$X(A) \longrightarrow \varprojlim X(A/\mathfrak{m}^n)$$

is bijective. □

3.5.13. Smooth varieties over a field.

Proposition 3.5.64. *The smooth locus of a geometrically reduced k-variety X is open and dense in X.*

Proof. Openness was proved in Proposition 3.5.17. For the denseness, see [**BLR90**, §2.2, Proposition 16]. □

Example 3.5.65. Here we show that the "geometrically reduced" hypothesis in Proposition 3.5.64 cannot be dropped. Let k be the imperfect field $\mathbb{F}_p(t)$. Let X be the curve $x^p - ty^p = 0$ in $\mathbb{A}^2_k$. The Jacobian matrix is identically zero, so $X^{\text{smooth}} = \emptyset$.

Proposition 3.5.66. *Let k be a field, and let X be a k-variety. Suppose that X is smooth at the point $x \in X(k)$, and let $t_1, \ldots, t_r$ be local coordinates at x. Replace t_i by $t_i - t_i(x)$ to make each new t_i vanish at x. Then the natural map $k[[t_1, \ldots, t_r]] \to \widehat{\mathscr{O}}_{X,x}$ from the formal power series ring to the completion of the local ring of X at x is an isomorphism.*

Proof. The local ring $\mathscr{O}_{X,x}$ is a regular local ring of dimension r containing its residue field k. Therefore its completion $\widehat{\mathscr{O}}_{X,x}$ is too, and the Cohen structure theorem implies $\widehat{\mathscr{O}}_{X,x} \simeq k[[t_1, \ldots, t_r]]$ (see [**Mat80**, Corollary 2 to 28.J].) □

Proposition 3.5.67. *If a k-variety is smooth and geometrically connected, then it is geometrically integral.*

Proof. Let X be the variety. By Proposition 3.5.22(i), smooth is equivalent to geometrically regular, so Corollary 3.5.6 applies to $X_{\overline{k}}$. □

Unofficial version for incidental online use

For convenience, we make the following definition:

Definition 3.5.68. A k-variety is **nice** if it is smooth, projective, and geometrically integral.

Remark 3.5.69. The literature contains many theorems about varieties that are "smooth, projective, and geometrically connected". These hypotheses look weaker than "nice", but in fact they are equivalent, by Proposition 3.5.67.

3.5.13.1. *Separably closed fields.*

Proposition 3.5.70. *If X is a smooth k-variety over a separably closed field k, then $X(k)$ is Zariski dense in X.*

Proof. The question is local on X, so by Proposition 3.5.48, we may assume that there is an étale morphism $g\colon X \to \mathbb{A}^r_k$. We may also assume that X is nonempty. It suffices to prove $X(k) \neq \emptyset$, since then we can apply the same argument to each dense open subscheme of X.

By Proposition 3.4.2, $g(X)$ is open in $\mathbb{A}^r_k$. Since separably closed fields are infinite, $\mathbb{A}^r(k)$ is dense in $\mathbb{A}^r_k$. In particular, there is a k-point v in $g(X)$. The nonempty étale k-scheme $g^{-1}(v)$ is a disjoint union of k-points by Proposition 3.5.35. Thus X has a k-point. □

The hypothesis of Proposition 3.5.70 can be weakened slightly:

Corollary 3.5.71. *If X is a geometrically reduced k-variety over a separably closed field k, then $X(k)$ is Zariski dense in X.*

Proof. Combine Propositions 3.5.64 and 3.5.70. □

Example 3.5.72. Here we show that the "geometrically reduced" hypothesis in Corollary 3.5.71 cannot be dropped. Let k be an imperfect separably closed field. Choose $t \in k - k^p$. Let X be the curve $x^p - ty^p = 0$ in $\mathbb{A}^2_k$. Then $X(k)$ consists of the single point $(0,0)$, and hence $X(k)$ is not Zariski dense in X.

3.5.13.2. *Local fields.*

Proposition 3.5.73. *Let k be a local field. Let $f\colon Y \to X$ be a morphism between k-varieties.*

(i) *If f is étale, then the induced map of topological spaces $Y(k) \to X(k)$ is a local homeomorphism (for the analytic topology).*
(ii) *If f is smooth, then the map $Y(k) \to X(k)$ is open.*

Proof.

Unofficial version for incidental online use

(i) By Proposition 3.5.39 we may assume that $f\colon Y \to X$ is a standard étale morphism $\operatorname{Spec}(A[t]/(p))[q^{-1}] \to \operatorname{Spec} A$ as in Definition 3.5.38, where A is a quotient of a polynomial ring $R := k[x_1, \dots, x_n]$. Lift $p \in A[t]$ to some $\tilde{p} \in R[t]$. Then there is an affine open subset of $\operatorname{Spec} R[t]/(\tilde{p})$ whose projection to $\operatorname{Spec} R = \mathbb{A}^n$ is a standard étale morphism whose restriction above $\operatorname{Spec} A$ is f. So we reduce to the case of a standard étale morphism $Y \to X = \mathbb{A}^n$. The result now is a special case of the implicit function theorem over k.

(ii) Proposition 3.5.48 lets us reduce to proving openness for étale morphisms and projections $X \times \mathbb{A}^n \to X$. The étale case follows from (i), and the projection case follows from the definition of the product topology. □

The classical Krasner's lemma [**Lan94**, II, §2, Proposition 3] is a statement about local fields k that implies that if the coefficients of a monic separable polynomial are perturbed, then the multiset of zeros varies continuously, irreducibility is locally preserved, and the field extension generated by the zeros is locally constant [**Lan94**, II, §2, Proposition 4]. Since any monic separable polynomial in $\mathbb{Q}_p[x]$ can be approximated by monic polynomials in $\mathbb{Q}[x]$, this implies that any degree d extension of $\mathbb{Q}_p$ is $\mathbb{Q}_p(\alpha)$ for some α that is algebraic of degree d over $\mathbb{Q}$. In particular, the copy of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$ is dense, and the homomorphism $\operatorname{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sending σ to $\sigma|_{\overline{\mathbb{Q}}}$ is injective (its image is a decomposition group).

The following is a generalization of the statement above that the field extension generated by the zeros is locally constant.

Proposition 3.5.74 (Krasner's lemma)**.** *Let k be a local field. Let $f\colon Y \to X$ be a finite étale morphism of k-varieties. Then the isomorphism type of the étale k-scheme $f^{-1}(x)$ is locally constant as x varies over $X(k)$ in the analytic topology.*

Proof. We may assume that X is connected, so that f has constant degree, say d. Let $x_0 \in X(k)$. Let $L \supseteq k$ be a finite Galois extension over which $f^{-1}(x_0)$ splits, say into points $y_1, \dots, y_d \in Y(L)$. Let $f_L\colon Y(L) \to X(L)$ be the map on L-points. By Proposition 3.5.73(i), there exist open neighborhoods $Y_i \subseteq Y(L)$ of y_i and $U_i \subseteq X(L)$ of x_0 such that f_L restricts to a homeomorphism $Y_i \to U_i$. We may assume that $\sigma Y_i = Y_j$ whenever $\sigma \in \operatorname{Gal}(L/k)$ and $\sigma y_i = y_j$. By shrinking the U_i (and correspondingly the Y_i), we may assume that the Y_i are disjoint and that the U_i are all equal, say to U. The disjoint union of the homeomorphisms $f_L|_{Y_i}\colon Y_i \to U \simeq U \times \{y_i\}$ is a $\operatorname{Gal}(L/k)$-equivariant homeomorphism $h\colon \bigcup Y_i \to U \times f_L^{-1}(x_0)$ of degree d covers of U. Thus if $u \in U \cap X(k)$, then restricting the domain and codomain of h to the fibers above u yields an isomorphism of $\operatorname{Gal}(L/k)$-sets,

Unofficial version for individual online use

so the corresponding étale k-schemes are isomorphic too; these are $f^{-1}(u)$ and $f^{-1}(x_0)$ since both have degree d. $\square$

Proposition 3.5.75. *Let k be a local field. Let X be an irreducible k-variety. If X has a smooth k-point x, then $X(k)$ is Zariski dense in X.*

Proof. By Proposition 3.5.48, we may replace X by an open subscheme to assume that there is an étale morphism $\pi\colon X \to \mathbb{A}^r_k$. By Proposition 3.5.73(ii), the image $\pi(X(k))$ is a nonempty open subset of $\mathbb{A}^r(k)$. No nonzero polynomial can vanish on such an open subset, so $\pi(X(k))$ is Zariski dense in $\mathbb{A}^r_k$. So if Y is the Zariski closure of $X(k)$ in X, then $\dim \pi(Y) = r$. This implies $\dim Y \geq r$, so $Y = X$. $\square$

Remark 3.5.76. One can strengthen the conclusion of Proposition 3.5.75 to assert that any open neighborhood U of x in $X(k)$ contains k-points outside any given countable union of closed subvarieties $Y_i \subsetneq X$. To prove this, after reducing to the case $X = \mathbb{A}^r$ as before, one can proceed in any of the following ways:

- apply the Baire category theorem to the nowhere dense subsets $Y_i(k)$ of $X(k)$;
- equip $\mathbb{A}^r(k)$ with Haar measure and observe that U has positive measure while each set $Y_i(k)$ has measure 0; or
- use induction on r, by fibering $\mathbb{A}^r(k)$ into lines and using the uncountability of any nonempty open subset of each line $\mathbb{A}^1(k)$.

This strengthening will be used in the proof of Theorem 7.7.4.

3.5.14. Good reduction.

3.5.14.1. *Discrete valuation rings.*

Definition 3.5.77. Let R be a discrete valuation ring, and let $K = \operatorname{Frac} R$. Let X be a smooth proper K-variety. We say that X has **good reduction** if there exists a smooth proper R-model of X.

In this case, the special fiber is a smooth proper variety over the residue field.

Example 3.5.78. The K-variety in Example 3.2.9 has good reduction, because the scheme $\operatorname{Proj} \mathbb{Z}_7[x,y,z]/(xy - z^2)$ is a smooth proper R-model.

Warning 3.5.79. Let X be a smooth proper K-variety. Let $\widehat{R}$ and $\widehat{K}$ denote the completions of R and K, respectively. If X_R is a smooth proper R-model of K, then $X_R \times_R \widehat{R}$ is a smooth proper $\widehat{R}$-model for $X_{\widehat{K}}$. So if X has good reduction, then so does $X_{\widehat{K}}$. But the converse can fail, as we now explain by modifying [**Mat15**, Example 5.3]. Let p, a, b, c, F be as in

Unofficial version for incidental online use

[**Mat15**, Example 5.3], except with c a nonsquare integer that becomes a square in $\mathbb{Z}_p$. Let $R = \mathbb{Z}_{(p)}$. Let $\mathcal{X} = \operatorname{Proj} \mathbb{Z}_{(p)}[x, y, z, w]/(F)$. Then

(i) the generic fiber is a smooth quartic surface $X \subseteq \mathbb{P}^3_{\mathbb{Q}}$ (a K3 surface) with $\operatorname{Pic} X \simeq \mathbb{Z}$;

(ii) the special fiber is a singular quartic surface over $\mathbb{F}_p$ whose singularities are ordinary double points; and

(iii) there are non-Cartier Weil divisors $\mathcal{C}_+$ and $\mathcal{C}_-$ on $\mathcal{X}_{\mathbb{Z}_p}$ (defined, in fact, on $\mathcal{X}_{\mathbb{Z}_{(p)}[\sqrt{c}]}$) such that blowing up either results in a smooth proper scheme over $\mathbb{Z}_p$.

Facts (i) and (ii) imply that X does not extend to a smooth proper scheme over $\mathbb{Z}_{(p)}$, by the argument in [**Art74**, p. 330]. Fact (iii) says that $X_{\mathbb{Q}_p}$ does extend to a smooth proper scheme over $\mathbb{Z}_p$.

Remark 3.5.80. In the context of Definition 3.5.77, it can happen that X does not extend to a smooth proper R-scheme but does extend to a smooth proper R-*algebraic space* [**Art74**]. In fact, the notion of good reduction would have better properties if it were defined in terms of algebraic spaces; see [**Mat15**] for more examples of this.

3.5.14.2. *Dedekind domains.*

Definition 3.5.81. Let R be a Dedekind domain, and let $K = \operatorname{Frac} R$. Let $\mathfrak{p}$ be a nonzero prime of R. A smooth proper K-variety X has **good reduction at $\mathfrak{p}$** if X has a smooth proper $R_{\mathfrak{p}}$-model. And X has **good reduction** if it has good reduction at every $\mathfrak{p}$.

3.5.15. Regular proper models. When a smooth proper model does not exist, one can seek models with weaker properties.

For example, if R is a complete discrete valuation ring and X is a nice K-curve, then X always has a regular proper R-model. Let us sketch a construction. Choose an embedding of X in $\mathbb{P}^n_K$ for some n. We have $\mathbb{P}^n_K \hookrightarrow \mathbb{P}^n_R$, and the Zariski closure of X in $\mathbb{P}^n_R$ is a proper R-model X'_R of X. But X'_R need not be smooth. The normalization of X'_R is finite over X_R, so it is another proper R-model X''_R, but now it is regular except at isolated closed points. By *resolution of singularities for arithmetic surfaces*, alternately blowing up singularities and normalizing eventually produces a regular proper model. (In fact, it is even projective.) See [**Art86b**] for an exposition of Lipman's proof of an even more general version.

If moreover X has genus ≥ 1, then among all regular proper R-models, there is a unique one satisfying a certain minimality property; see Section 9.3.1.6. It is called the **minimal regular proper model**. This result

Unofficial version for incremental online use

is analogous to the theory of minimal models for surfaces over fields, which is discussed in [**Har77**, pp. 418–419].

It is conjectured that a nice K-variety X of any dimension has a regular proper R-model. This conjecture is a version of what could be called *resolution of singularities for arithmetic schemes*.

3.5.16. Néron models.

(References: [**BLR90**], [**LT16**])

Let R be a discrete valuation ring. Let $K = \operatorname{Frac} R$. Let X be a nice K-variety. If X has good reduction, i.e., X has a smooth proper R-model $\mathcal{X}$, then $\mathcal{X}(R) \simeq X(K)$ by the valuative criterion for properness. But even if X has bad reduction, it might have a smooth not-necessarily-proper R-model $\mathcal{N}$ satisfying $\mathcal{N}(R) \simeq X(K)$. To determine $\mathcal{N}$ uniquely, we would want to specify not just $\mathcal{N}(R)$, but the whole functor of points. Actually, if we insist that $\mathcal{N}$ be smooth over R, then it suffices to specify its functor of points *restricted to smooth R-schemes*, by Yoneda's lemma (Lemma 2.3.4) applied in the category of smooth R-schemes. This motivates the following definition, which we give in the more general context of Dedekind domains (and which could be generalized further to integral Dedekind schemes):

Definition 3.5.82. Let R be a Dedekind domain. Let $K = \operatorname{Frac} R$. Let X be a smooth K-variety. A **Néron model** of X is a smooth R-scheme $\mathcal{N}$ with an isomorphism $\mathcal{N}_K \simeq X$ such that for every smooth R-scheme T, the induced map $\mathcal{N}(T) \to X(T_K)$ is a bijection. (Some authors write "Néron lft-model" for the above, and write "Néron model" only if $\mathcal{N}$ is also of finite type [**LT16**]; here lft stands for "locally of finite type".)

As mentioned above, Yoneda's lemma implies that $\mathcal{N}$ is unique if it exists. Moreover, if X is a group scheme (see Section 5.1) and $\mathcal{N}$ exists, then the functor of points of $\mathcal{N}$ factors through **Groups**, so $\mathcal{N}$ is a group object in the category of smooth R-schemes; that is, $\mathcal{N}$ is a smooth group scheme over R.

Néron has his name attached to the concept because in 1964 he proved that $\mathcal{N}$ exists when X is an abelian variety over the fraction field of a discrete valuation ring; see Section 5.7.5. Here is a more recent result, in a different direction:

Theorem 3.5.83 (Liu and Tong)**.** *Let S be an integral Dedekind scheme. Let $K = \mathbf{k}(S)$. Let X be a nice curve over K of positive genus. Let $\mathcal{X} \to S$ be the minimal regular proper model of X (see Section 9.3.1.6). Then the smooth locus $\mathcal{X}^{\text{smooth}}$ of $\mathcal{X} \to S$ is a Néron model of X.*

Proof. See [**LT16**, Theorem 1.1]. $\square$

Unofficial version for internet online use

3.6. Rational maps

3.6.1. Rational maps and domain of definition.

(Reference: [**EGA I**, §7])

Definition 3.6.1 ([**EGA I**, 7.1.2])**.** Let X and Y be S-schemes. Consider pairs (U, ϕ) in which U is a dense open subscheme of X and $\phi\colon U \to Y$ is an S-morphism. Call pairs (U, ϕ) and (V, ψ) equivalent if ϕ and ψ agree on a dense open subscheme of $U \cap V$. A **rational map** $X \dashrightarrow Y$ is an equivalence class of such pairs. In other words,

$$\{\text{rational maps } X \dashrightarrow Y\} := \varinjlim_{U} \operatorname{Hom}_S(U, Y),$$

where U ranges over dense open subschemes of X ordered by reverse inclusion.

Definition 3.6.2 ([**EGA I**, 7.2.1])**.** The **domain of definition** of a rational map is the union of the U as (U, ϕ) ranges over the equivalence class. It is an open subscheme of X.

Definition 3.6.2 is useful mainly when X is reduced and Y is separated:

Proposition 3.6.3. *Let W be the domain of definition of a rational map $X \dashrightarrow Y$, where X is reduced and Y is separated. Then there is a unique $\xi\colon W \to Y$ such that (W, ξ) belongs to the equivalence class.*

Proof. If (U, ϕ) and (V, ψ) are equivalent, so ϕ and ψ agree on a dense open subscheme of $U \cap V$, then by Corollary 2.3.23 they agree on all of $U \cap V$. Therefore all the (U, ϕ) can be glued to give (W, ξ). $\square$

Remark 3.6.4. One can drop the hypothesis that X is reduced in Proposition 3.6.3 if one replaces "dense" by the stronger property "scheme-theoretically dense" everywhere in Definition 3.6.1. This leads to the notion of **pseudo-morphism**, a variant of the notion of rational map; see [**EGA IV**$_4$, 20.2.1].

3.6.2. Rational points over a function field.

Proposition 3.6.5. *Let X be an integral k-variety, and let Y be an arbitrary k-variety. Let $K = \mathbf{k}(X)$.*

(a) *The natural map*

$$\{\text{rational maps from } X \text{ to } Y\} \longrightarrow Y(K)$$

$$[\phi\colon U \to Y] \longmapsto (\text{the composition } \operatorname{Spec} K \hookrightarrow U \xrightarrow{\phi} Y)$$

is a bijection.

Unofficial version for incidental online use

(b) *If moreover X is a regular curve and Y is proper, then we get bijections*

$$\operatorname{Hom}_k(X,Y) \quad \tilde{\to} \quad \{\text{rational maps from } X \text{ to } Y\} \quad \tilde{\to} \quad Y(K).$$

Proof.

(a) Every dense open subscheme of X contains a dense affine open subscheme; i.e., the inverse system $(\operatorname{Spec} A_i)$ of dense affine open subschemes of X is cofinal in the system of all dense open subschemes. Thus we have bijections

$$\begin{aligned} \{\text{rational maps from } X \text{ to } Y\} &= \varinjlim_U Y(U) && \text{(by definition)} \\ &\simeq \varinjlim Y(A_i) && \text{(by cofinality)} \\ &\simeq Y(\varinjlim A_i) && \text{(by Remark 3.1.11)} \\ &= Y(K) && \text{(since } \varinjlim A_i = K\text{).} \end{aligned}$$

(b) The first bijection comes from the valuative criterion for properness: The map $Y(X) \to Y(K)$ is bijective by Remark 3.2.14. The second bijection was given already in (a). ☐

Unofficial version for incidental online use

3.6.3. Dominant rational maps.

Definition 3.6.6. A rational map $X \dashrightarrow Y$ is **dominant** if and only if for some (or equivalently, for each) representative (U, ϕ), the image $\phi(U)$ is dense in Y.

Corollary 3.6.7 (cf. [**Har77**, Theorem I.4.4])**.** *The functor*

$$\left\{\begin{matrix}\text{integral } k\text{-varieties,} \\ \text{dominant rational maps}\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{finitely generated field extensions of } k, \\ k\text{-algebra homomorphisms}\end{matrix}\right\}^{\text{opp}}$$

$$X \longmapsto \mathbf{k}(X)$$

is an equivalence of categories.

Proof. A rational map $X \dashrightarrow Y$ is dominant if and only if it maps the generic point of X to the generic point of Y; thus we have a functor from left to right. Restricting the bijection in Proposition 3.6.5(a) to the dominant rational maps $X \dashrightarrow Y$ shows that the functor is fully faithful. Every finitely generated field extension of k is isomorphic to the function field of an integral k-variety (cf. Proposition 2.2.13); i.e., the functor is essentially surjective. ☐

Definition 3.6.8. If X is an integral k-variety, the set of birational maps $X \dashrightarrow X$ forms a group $\operatorname{Bir} X$. By Corollary 3.6.7, $\operatorname{Bir} X$ is isomorphic to the group $\operatorname{Aut}(\mathbf{k}(X)/k)$ of automorphisms of the function field over k.

Example 3.6.9. The group $\operatorname{Bir} \mathbb{P}^n$ is also called the **Cremona group**.

Definition 3.6.10. If $\pi\colon X \to Y$ is a dominant rational map between integral k-varieties of the same dimension, then $\mathbf{k}(X)$ may be viewed as a finite extension of $\mathbf{k}(Y)$, and we define the **degree** of π as $\deg \pi := [\mathbf{k}(X) : \mathbf{k}(Y)]$.

3.6.4. Lang–Nishimura theorem. If $\pi\colon X \to Y$ is a morphism of k-varieties and X has a k-point x, then Y has a k-point, namely $\pi(x)$. If π is only a rational map, this argument fails, since π might be undefined at x, but surprisingly the same conclusion can be drawn, under mild hypotheses. The following theorem is due to Lang [**Lan54**] and Nishimura [**Nis55**].

Theorem 3.6.11 (Lang–Nishimura theorem)**.** *Let $X \dashrightarrow Y$ be a rational map between k-varieties, where Y is proper. If X has a smooth k-point, then Y has a k-point.*

Proof. Let x be the given smooth k-point on X. Replacing X by an open neighborhood of x, we may assume that X is integral. Let $n = \dim X$. Proposition 3.5.66 gives the isomorphism in the chain of embeddings

$$\mathscr{O}_{X,x} \hookrightarrow \widehat{\mathscr{O}}_{X,x} \simeq k[[t_1, \ldots, t_n]] \hookrightarrow F := k((t_1))((t_2)) \cdots ((t_n)).$$

Since F is a field (an iterated formal Laurent series field), the fraction field $\operatorname{Frac} \mathscr{O}_{X,x} = \mathbf{k}(X)$ embeds in F. By Proposition 3.6.5(a), the rational map gives an element of $Y(\mathbf{k}(X))$, and hence an element of $Y(F)$. Applying Lemma 3.6.12 n times shows that Y has a k-point. $\square$

Lemma 3.6.12. *Let Y be a proper k-variety. Let L be a field extension of k, and let $L((t))$ be the formal Laurent series field over L. If Y has an $L((t))$-point, then Y has an L-point.*

Proof. By the valuative criterion for properness (Theorem 3.2.12), the element of $Y(L((t)))$ extends to an element of $Y(L[[t]])$, which reduces modulo t to an element of $Y(L)$. $\square$

Remark 3.6.13. The Lang–Nishimura theorem can be explained geometrically as follows. If $\dim_x X > 0$, then one can show that X contains an integral curve C such that

- x is a smooth point of C, and
- C meets the domain of definition of the rational map ϕ.

The valuative criterion for properness shows that $\phi|_C\colon C \dashrightarrow Y$ extends to be defined at x. It maps x to a k-point of Y. (The reason that we did not present the proof this way is that the existence of C is not immediate.)

Remark 3.6.14. For another proof of Theorem 3.6.11, see Exercise 3.11.

Remark 3.6.15. In Theorem 3.6.11 one cannot conclude that Y has a *smooth* k-point.

Unofficial version for incidental online use

The Lang–Nishimura theorem implies that the property of having a k-point is a birational invariant of smooth, proper, integral k-varieties:

Corollary 3.6.16. *Let X and Y be smooth, proper, integral k-varieties that are birational to each other. Then X has a k-point if and only if Y has a k-point.*

3.7. Frobenius morphisms

(Reference: [**SGA 5**, XV])

Let p be a prime number. Let X be a scheme of characteristic p, i.e., a scheme with $p\mathscr{O}_X = 0$. Then the **absolute Frobenius morphism** is the morphism of schemes $F_X : X \to X$ that is the identity on topological spaces and that induces the pth-power homomorphism $f \mapsto f^p$ on each ring $\mathscr{O}_X(U)$.

Now let S be a scheme of characteristic p, and let X be an S-scheme. Let $X^{(p)}$ be the base extension of X by F_S. Then the universal property of the fiber product gives a morphism $F_{X/S} : X \to X^{(p)}$ called the **relative Frobenius morphism**:

(3.7.1)
$$\begin{tikzcd}
X \arrow[dr, dotted, "F_{X/S}"] \arrow[drr, bend left, "F_X"] \arrow[ddr, bend right] & & \\
& X^{(p)} \arrow[r, "\alpha"] \arrow[d] & X \arrow[d] \\
& S \arrow[r, "F_S"] & S
\end{tikzcd}$$

As the diagram shows, $F_{X/S}$ is an S-morphism, but F_X is generally not an S-morphism because it lies over $F_S : S \to S$ instead of the identity 1_S.

Example 3.7.2. Let k be a field of characteristic p. Let $S = \operatorname{Spec} k$, and let X be a k-variety. Then $X^{(p)}$ is the k-variety obtained by replacing the coefficients in the equations defining X by their pth powers. We then write $F_{X/k} = F_{X/S}$. On regular functions, the three morphisms along the top of (3.7.1) act as follows:

$F_{X/k}$: identity on elements of k, raises variables to the pth power;

α : raises elements of k to the pth power, identity on variables;

F_X : raises *everything* to the pth power.

Of these three morphisms, usually only $F_{X/k}$ is a morphism of k-varieties; it is a finite morphism.

Remark 3.7.3. If X is an integral variety over a field k of characteristic p, then the degree of $F_{X/k} : X \to X^{(p)}$ is $p^{\dim X}$ (see Definition 3.6.10). In

Unofficial version for incidental online use

particular, if $\dim X > 0$, then $F_{X/k}$ is not an isomorphism, and hence not an automorphism even if $X^{(p)} \simeq X$ over k.

Remark 3.7.4. If we specialize (3.7.1) to the case where $S = \operatorname{Spec} \mathbb{F}_p$, then F_S is the identity, so $X^{(p)} \simeq X$ as an $\mathbb{F}_p$-scheme via α.

The following will be used later, in the proof of Proposition 7.5.17.

Lemma 3.7.5. *If $X \to S$ is an étale morphism of schemes of characteristic p, then the diagram*

$$\begin{array}{ccc} X & \xrightarrow{F_X} & X \\ \downarrow & & \downarrow \\ S & \xrightarrow{F_S} & S \end{array}$$

is cartesian; that is, the upper left X is the fiber product of the rest of the diagram.

Proof. By [**SGA 5**, XV, Proposition 2(c)(2)], $F_{X/S}$ is an isomorphism. □

Remark 3.7.6. Let $q = p^n$ for some $n \geq 1$. Under the same hypotheses as above, one can define an absolute q-power Frobenius morphism $X \to X$, a scheme $X^{(q)}$, and a relative q-power Frobenius morphism $X \to X^{(q)}$ over S in the same way, by replacing p by q.

3.8. Comparisons

Given a collection of schemes $(X_i)_{i \in I}$, we may glue the X_i along their empty subschemes to obtain the disjoint union scheme $\coprod X_i$. Given a collection of morphisms $(X_i \to Y)_{i \in I}$, we may glue them to obtain a a single morphism $\coprod X_i \to Y$.

Definition 3.8.1. A **Zariski open covering morphism** is a morphism of schemes $\coprod X_i \to Y$ obtained as a disjoint union of open immersions $X_i \to Y$ whose images form an open covering of Y. (This terminology is not standard, but it will be convenient to have.)

Proposition 3.8.2. *Let $f\colon X \to Y$ be a morphism of schemes. Each of the following statements implies the next:*

- *f is a Zariski open covering morphism.*
- *f is étale and surjective.*
- *f is fppf.*
- *f is fpqc.*

Proof. We leave this to the reader, as Exercise 3.13. □

Unofficial version for incidental online use

Proposition 3.8.2 suggests that fpqc morphisms may be considered generalizations of open coverings. This point of view will prevail in Chapters 4 and 6.

Exercises

3.1. Let A be a commutative ring. Let I be an ideal in the polynomial ring $A[t_1, \dots, t_n]$ for some $n \geq 0$. Prove that $A[t_1, \dots, t_n]/I$ is a finitely presented A-algebra if and only if I is a finitely generated ideal.

3.2. Which of the following morphisms are flat? Faithfully flat?
(a) $\operatorname{Spec} \mathbb{Z}[1/2] \to \operatorname{Spec} \mathbb{Z}$.
(b) $\operatorname{Spec}\left(\mathbb{Z} \times \frac{\mathbb{Z}}{6\mathbb{Z}}\right) \to \operatorname{Spec} \mathbb{Z}$.
(c) $\operatorname{Spec} \mathbb{C}[x, y]/(xy - 1) \to \operatorname{Spec} \mathbb{C}[x]$.
(d) $\operatorname{Spec} \mathbb{C}[x, y]/(xy) \to \operatorname{Spec} \mathbb{C}[x]$.
(e) $\operatorname{Spec} \mathbb{C}[x, y]/(y^2 - x^3) \to \operatorname{Spec} \mathbb{C}[x]$.
(f) $X \to \mathbb{A}^2_{\mathbb{C}}$, where X is the blowup of $\mathbb{A}^2_{\mathbb{C}}$ at the origin.

3.3. Give an example of an integral domain R and fraction field K such that the natural map $\mathbb{P}^1(R) \to \mathbb{P}^1(K)$ is not a bijection.

3.4. Let k be a global field, and let Ω_k, $\mathcal{O}_{k,S}$, k_v, $\mathcal{O}_v$, and $\mathbf{A}$ be as in Section 1.1.3. Let X be a k-variety.
(a) Prove that there is a finite subset $S \subset \Omega_k$, a separated scheme $\mathcal{X}$ of finite type over $\mathcal{O}_{k,S}$, and an isomorphism $\mathcal{X}_k \simeq X$; fix these.
(b) Explain why $\mathcal{X}(\mathcal{O}_v)$ may be identified with a subset of $X(k_v)$ for each $v \notin S$.
(c) Prove that there is a bijection

$$X(\mathbf{A}) \longrightarrow {\prod}'_{v \in \Omega_k} (X(k_v), \mathcal{X}(\mathcal{O}_v)).$$

(*Hint*: Use Remark 3.1.11 and prove the following.

Lemma. *If Y is a quasi-compact and quasi-separated A-scheme for some ring A, and $(R_i)_{i \in I}$ is a collection of local A-algebras, then the natural map $Y(\prod R_i) \to \prod Y(R_i)$ is a bijection.*

Even with this hint, the problem is hard.)
(d) Prove that if moreover X is proper over k, then the natural map

$$X(\mathbf{A}) \longrightarrow \prod_{v \in \Omega_k} X(k_v)$$

is a bijection.

Unofficial version for incidental online use

3.5. Give an example of a prime p and a nice $\mathbb{Q}_p$-variety X with proper $\mathbb{Z}_p$-models $\mathcal{X}$ and $\mathcal{X}'$ such that their special fibers are isomorphic and such that $\mathcal{X}$ is regular and $\mathcal{X}'$ is not.

3.6. Let X be a variety over a field k. Show that it is possible to find finitely many locally closed subvarieties Y_i of X (i.e., open subvarieties of closed subvarieties) such that each Y_i is smooth and geometrically integral and $\bigcup Y_i(k) = X(k)$.

3.7. Give an example of a prime p and a geometrically integral curve X over $\mathbb{Q}_p$ such that $X(\mathbb{Q}_p)$ consists of a single point.

3.8. Let R be a Dedekind domain, let $K = \operatorname{Frac} R$, and let X be a smooth proper K-scheme. Suppose that for each nonzero prime $\mathfrak{p}$ of R, the scheme X has good reduction at $\mathfrak{p}$. Prove that there is a smooth proper R-model of X.

3.9. Let $\phi\colon X \dashrightarrow Y$ be a rational map from a regular k-variety to a proper k-variety. Prove that there is a closed subset $Z \subseteq X$ of codimension ≥ 2 in X such that ϕ extends to a morphism from $X - Z$ to Y.

3.10. For a proper variety X over a global field k, explain why strong approximation with respect to $\emptyset$ is equivalent to weak approximation.

3.11. Give a proof of the Lang–Nishimura theorem by induction on $\dim X$, along the following lines: Blow up the smooth k-point on X and apply the inductive hypothesis to the restriction of the rational map to the exceptional divisor E. (This proof is due to János Kollár and Endre Szabó [**RY00**, Proposition A.6].)

3.12. Show that the Lang–Nishimura theorem can fail if either of the following changes is made:
(a) The assumption that Y is proper is dropped.
(b) The given k-point on X is not assumed to be smooth.

3.13. Prove Proposition 3.8.2 comparing Zariski open covering, étale and surjective, fppf, and fpqc morphisms.

3.14. The inclusions $k[x] \hookrightarrow k[x, x^{-1}]$ and $k[x] \hookrightarrow k[[x]]$ define a morphism f from the disjoint union $X := \operatorname{Spec} k[x, x^{-1}] \amalg \operatorname{Spec} k[[x]]$ to the scheme $Y := \operatorname{Spec} k[x]$. Show that f is fpqc but not fppf.

Unofficial version for mendeleev online use

Chapter 4

Faithfully flat descent

(References: [**Gro95a**] and [**BLR90**, Chapter 6])

Suppose that one wants to carry out a construction of a variety over a base field k. Sometimes all one can do directly is to construct its analogue X' over some field extension k'. Then one is faced with deciding whether X' is the base extension of some k-variety X, and if so, to construct X. This is a special case of the problem known as **descent**.

Weil gave necessary and sufficient conditions for descending a quasi-projective variety over a Galois extension $k' \supseteq k$. Later, Grothendieck noticed that these conditions were analogous to the conditions for reconstructing an object from local data by gluing; this led him to a common generalization.

4.1. Motivation: Gluing sheaves

4.1.1. A gluing problem. Let S be a topological space, and let $\{S_i\}_{i\in I}$ denote an open covering of S. Suppose we are given a sheaf $\mathscr{F}_i$ on S_i for each i. Under what conditions is there a sheaf $\mathscr{F}$ on S such that $\mathscr{F}|_{S_i} \simeq \mathscr{F}_i$? (Cf. [**Har77**, Exercise II.1.22].)

4.1.2. Solution: The gluing conditions. If $\mathscr{F}$ exists, then the restrictions of $\mathscr{F}|_{S_i}$ and $\mathscr{F}|_{S_j}$ to $S_{ij} := S_i \cap S_j$ must be isomorphic (both isomorphic to $\mathscr{F}|_{S_{ij}}$). Thus we should at least insist that

(4.1.1) for all i and j, we are given an isomorphism $\phi_{ij} \colon \mathscr{F}_i|_{S_{ij}} \to \mathscr{F}_j|_{S_{ij}}$.

Can we then glue the $\mathscr{F}_i$ via the ϕ_{ij}? On a triple intersection $S_{ijk} := S_i \cap S_j \cap S_k$, the sheaves $\mathscr{F}_i|_{S_{ijk}}$, $\mathscr{F}_j|_{S_{ijk}}$, $\mathscr{F}_k|_{S_{ijk}}$ are identified in pairs by ϕ_{ij}, ϕ_{jk}, and ϕ_{ik}, forming a triangle of identifications. For these identifications

Unofficial version for incidental online use

to be compatible, we should insist that the composition of two sides of the triangle gives the third, i.e., that we have the following "cocycle condition":

(4.1.2) for all i, j, k, we have $\phi_{jk} \circ \phi_{ij} = \phi_{ik}$ on S_{ijk}.

In the case where $\mathscr{F}$ exists, each ϕ_{ij} is the identity, so these are automatically satisfied. The gluing theorem states that given sheaves $\mathscr{F}_i$ on S_i, if there exist isomorphisms as in (4.1.1) satisfying (4.1.2), then up to isomorphism there exists a unique sheaf $\mathscr{F}$ on S with isomorphisms $\phi_i\colon \mathscr{F}|_{S_i} \to \mathscr{F}_i$ such that ϕ_i and ϕ_j identify the identity on $\mathscr{F}_{S_{ij}}$ with ϕ_{ij}.

Example 4.1.3. Let k be a field, and let $S = \mathbb{P}^1_k$, which is covered by two affine open subsets $S_1 = \operatorname{Spec} k[t] \simeq \mathbb{A}^1_k$ and $S_2 = \operatorname{Spec} k[t^{-1}] \simeq \mathbb{A}^1_k$ whose intersection is $S_{12} = \operatorname{Spec} k[t,t^{-1}] \simeq \mathbb{A}^1_k - \{0\}$. Let $M_1 = k[t]$ and $M_2 = k[t^{-1}]$ be free rank 1 modules over $k[t]$ and $k[t^{-1}]$, respectively. Let $\mathscr{F}_1 = \widetilde{M_1}$ and $\mathscr{F}_2 = \widetilde{M_2}$ be the corresponding sheaves on S_1 and S_2. Let $d \in \mathbb{Z}$. The $k[t,t^{-1}]$-module isomorphism

$$M_1 \otimes_{k[t]} k[t,t^{-1}] = k[t,t^{-1}] \xrightarrow{t^{-d}} k[t,t^{-1}] = M_2 \otimes_{k[t^{-1}]} k[t,t^{-1}]$$

given by multiplication by t^{-d} induces a sheaf isomorphism

$$\phi_{12}\colon \mathscr{F}_1|_{S_{12}} \longrightarrow \mathscr{F}_2|_{S_{12}}.$$

Let ϕ_{11} and ϕ_{22} be the identity, and let ϕ_{21} be ϕ_{12}^{-1}. Then (4.1.2) is trivially satisfied, so we can glue to get a sheaf $\mathscr{F}$ on $\mathbb{P}^1_k$. In fact, $\mathscr{F}$ is $\mathscr{O}(d)$.

Remark 4.1.4. One can also glue *morphisms* of sheaves, in the following sense. Let S be a topological space, and let $\{S_i\}_{i\in I}$ denote an open covering of S. Let $\mathscr{F}$ and $\mathscr{G}$ be two sheaves on S. For each $i \in I$, let $\phi_i\colon \mathscr{F}|_{S_i} \to \mathscr{G}|_{S_i}$ be a morphism of sheaves. If for every $i,j \in I$, the restrictions of ϕ_i and ϕ_j to S_{ij} are equal, then there exists a unique morphism $\phi\colon \mathscr{F} \to \mathscr{G}$ such that $\phi|_{S_i} = \phi_i$ for each $i \in I$. (In fact, this statement holds very generally, for sheaves on any site [**SP**, Tag 04TQ].)

4.1.3. Rewriting the gluing conditions. We can restate the gluing conditions by introducing the disjoint union $S' := \coprod S_i$. Let $\pi\colon S' \to S$ be the "open covering morphism" that on each S_i is the inclusion. To give the $\mathscr{F}_i$ on all the S_i is equivalent to giving a single sheaf $\mathscr{F}'$ on S'. The question is whether there exists a sheaf $\mathscr{F}$ on S such that the sheaf $\pi^{-1}\mathscr{F}$ on S' is isomorphic to the given $\mathscr{F}'$.

The fiber product $S'' := S' \times_S S'$ equals the disjoint union of $S_i \times_S S_j = S_i \cap S_j =: S_{ij}$ over all i,j. Let $p_1\colon S'' \to S'$ and $p_2\colon S'' \to S'$ be the two projections. The sheaf $p_1^{-1}\mathscr{F}'$ restricted to the piece indexed by ij corresponds to the sheaf $\mathscr{F}_i|_{S_{ij}}$. Thus, asking for isomorphisms ϕ_{ij} as in (4.1.1)

Unofficial version for incidental online use

is equivalent to asking that

(4.1.5)

we are given an isomorphism $\phi\colon p_1^{-1}\mathscr{F}' \to p_2^{-1}\mathscr{F}'$ of sheaves on S''.

Let $S''' := S' \times_S S' \times_S S'$. Let $p_{13} : S''' \to S''$ be the projection onto the first and third coordinates, and so on. Then $p_{13}^{-1}\phi$ is an isomorphism of sheaves on S'''. The cocycle condition (4.1.2) can now be rewritten as

$$p_{13}^{-1}\phi = p_{23}^{-1}\phi \circ p_{12}^{-1}\phi.$$

4.2. Faithfully flat descent for quasi-coherent sheaves

The idea behind faithfully flat descent is that, in the context of schemes, in place of the Zariski open covering morphisms $S' \to S$ of Section 4.1.3, one can use the much more general fpqc morphisms defined in Section 3.4. We develop this first for quasi-coherent sheaves, by analogy with the conditions in Section 4.1.3. The operation p^{-1} on sheaves is replaced by p^*, which is the appropriate operation for quasi-coherent sheaves.

4.2.1. Descent data. Let $p\colon S' \to S$ be an fpqc morphism of schemes. Let $\mathscr{F}'$ denote a quasi-coherent S'-module (that is, a quasi-coherent sheaf of $\mathscr{O}_{S'}$-modules). Define S'' and S''' as in Section 4.1.3, using fiber product of schemes instead of fiber products of topological spaces. Define the projections p_1, p_{13}, and so on as before.

Definition 4.2.1. With notation as in the previous paragraph, a **descent datum** on $\mathscr{F}'$ is an isomorphism $\phi\colon p_1^*\mathscr{F}' \to p_2^*\mathscr{F}'$ of S''-modules satisfying the cocycle condition

$$p_{13}^*\phi = p_{23}^*\phi \circ p_{12}^*\phi.$$

A **morphism of quasi-coherent S'-modules with descent data** $(\mathscr{F}', \phi) \to (\mathscr{G}', \psi)$ is a morphism of S'-modules $f\colon \mathscr{F}' \to \mathscr{G}'$ such that

$$\begin{array}{ccc} p_1^*\mathscr{F}' & \xrightarrow{p_1^* f} & p_1^*\mathscr{G}' \\ {\scriptstyle\phi}\big\downarrow & & \big\downarrow{\scriptstyle\psi} \\ p_2^*\mathscr{F}' & \xrightarrow{p_2^* f} & p_2^*\mathscr{G}' \end{array}$$

commutes.

Remark 4.2.2. There is an elegant reinterpretation of the notion of descent datum in terms of simplicial schemes. See [**SP**, Tag 0248] for an introduction.

If $\mathscr{F}$ is a quasi-coherent S-module, then $p^*\mathscr{F}$ has a natural descent datum $\phi_{\mathscr{F}}$, consisting of the canonical isomorphism

$$p_1^*(p^*\mathscr{F}) \simeq (p \circ p_1)^*\mathscr{F} = (p \circ p_2)^*\mathscr{F} \simeq p_2^*(p^*\mathscr{F}).$$

Unofficial version for incidental online use

4.2.2. The descent theorem for quasi-coherent sheaves. We now have the main theorem of descent theory, in the context of quasi-coherent modules.

Theorem 4.2.3 (Grothendieck)**.** *If* $p\colon S' \to S$ *is an fpqc morphism, then the functor*

$$\{\text{quasi-coherent } S\text{-modules}\} \longrightarrow \{\text{quasi-coherent } S'\text{-modules with descent data}\},$$
$$\mathscr{F} \longmapsto (p^*\mathscr{F}, \phi_{\mathscr{F}})$$

is an equivalence of categories.

The proof takes only a few pages. It reduces to a statement about modules over rings generalizing Theorem 1.3.11. See [**Gro95a**, Theorem 1] or [**BLR90**, §6.1] for details.

4.3. Faithfully flat descent for schemes

We now consider the problem of descending schemes instead of quasi-coherent sheaves. Let $p\colon S' \to S$ be fpqc. Let X' be an S'-scheme. Under what conditions is X' isomorphic to an S'-scheme of the form p^*X for some S-scheme X? (We use the notation $p^*X = X \times_S S'$.)

4.3.1. Descent data for schemes. The answer is almost the same as for sheaves. A **descent datum** on an S'-scheme X' is an S''-isomorphism $\phi\colon p_1^*X' \to p_2^*X'$ satisfying the usual cocycle condition. The pairs (X', ϕ) are the objects of a category as before. If X is an S-scheme, then p^*X has a canonical descent datum ϕ_X. Call ϕ **effective** if $(X', \phi) \simeq (p^*X, \phi_X)$ for some S-scheme X. Ideally every descent datum would be effective, as happened for quasi-coherent sheaves, but this is not quite true for schemes; see [**BLR90**, §6.7] for a counterexample.

4.3.2. Open subschemes stable under a descent datum.

Definition 4.3.1. Let X' be an S'-scheme, and let $\phi\colon p_1^*X' \to p_2^*X'$ be a descent datum. An open subscheme $U' \subseteq X'$ is called **stable under** ϕ if ϕ induces a descent datum on U', that is, if ϕ restricts to an isomorphism $p_1^*U' \to p_2^*U'$ of S''-schemes.

The idea behind this definition is that the stable open subschemes of X' are the ones that are supposed to be of the form p^*U for an open subscheme U of X, if X exists.

4.3.3. The descent theorem for schemes.

Definition 4.3.2 ([**EGA II**, 1.6.1])**.** A morphism $f\colon X \to S$ is **affine** if $f^{-1}S_0$ is affine for each affine open subscheme S_0 of S. In this case, we call X an **affine** S**-scheme**.

Unofficial version for incidental online use

Warning 4.3.3. An affine S-scheme is not necessarily affine as a scheme; "relatively affine" might be clearer terminology.

Definition 4.3.4 ([**EGA II**, 5.1.1])**.** A scheme is **quasi-affine** if it is an open subscheme of an affine scheme and is quasi-compact. A morphism $f\colon X \to S$ is **quasi-affine** if $f^{-1}S_0$ is quasi-affine for each affine open subscheme S_0 of S.

Theorem 4.3.5. *Let $p\colon S' \to S$ be an fpqc morphism of schemes.*

(i) *The functor $X \mapsto p^*X$ from S-schemes to S'-schemes with descent data is fully faithful.*

(ii) *The functor $X \mapsto p^*X$ from* quasi-affine *S-schemes to* quasi-affine *S'-schemes with descent data is an equivalence of categories.*

(iii) *Suppose that S and S' are affine. Then a descent datum ϕ on an S'-scheme X' is effective if and only if X' can be covered by quasi-affine open subschemes which are stable under ϕ.*

Remark 4.3.6. Parts (ii) and (iii) hold also if "quasi-affine" is replaced by "affine" everywhere. Part (iii) will be used primarily to show that certain descent data *are* effective (the "if" part), so it is preferable to have the more widely applicable criterion.

The proof of Theorem 4.3.5 reduces to the proof of Theorem 4.2.3. See [**Gro95a**, B.1, Theorem 2], [**BLR90**, §6.1, Theorem 6], and [**SP**, Tag 0247] for details.

4.3.4. Descending properties of morphisms. When an S-scheme X is base extended to an S'-scheme X', we know that X' inherits many properties from X. Conversely, when an S'-scheme X' is descended to an S-scheme X, one hopes that X inherits properties from X'. Fortunately, this is the case in fpqc descent, for many properties.

Theorem 4.3.7. *Let* blah *denote a property for which a positive answer is listed in the "fpqc descent" column of Table 1 on pp. 302–303. Let $S' \to S$ be an fpqc morphism. For any S-scheme X, let $X' = X_{S'}$.*

(i) *Let X be an S-scheme. If the base extension $X' \to S'$ is blah, then the original morphism $X \to S$ is blah.*

(ii) *More generally, if $X \to Y$ is a morphism of S-schemes and its base extension $X' \to Y'$ by $S' \to S$ is blah, then the original morphism*

Unofficial version for incidental online use

$X \to Y$ is blah.

$$\begin{tikzcd}
X' \arrow[rr, dotted] \arrow[dr, "\text{blah}"] \arrow[dd] & & X \arrow[dr, "\text{blah?}"] \arrow[dd] & \\
& Y' \arrow[rr, dotted] \arrow[dl] & & Y \arrow[dl] \\
S' \arrow[rr, dotted, "\text{fpqc}"] & & S &
\end{tikzcd}$$

Proof.

(i) See the references in Table 1.

(ii) Since the morphism $S' \to S$ is fpqc, Table 1 implies that its base extension $Y' \to Y$ is fpqc. Now the result follows from (i). $\square$

Remark 4.3.8. It is easy to understand why the surjectivity implicit in fpqc is a hypothesis for a statement like Theorem 4.3.7(i). If $S' \to S$ were not surjective, the morphism $X \to S$ could have bad behavior above points of S not in the image of S', and this behavior would not be seen in the base extension $X' \to S'$.

4.4. Galois descent

Let k be a field, and let k' be a finite Galois extension of k. Let $S = \operatorname{Spec} k$ and $S' = \operatorname{Spec} k'$. Then $S' \to S$ is fpqc, so we can apply Theorem 4.3.5(iii) to say something about descending k'-schemes to k-schemes.

Remark 4.4.1. This case was developed by Weil. Later Grothendieck generalized it to the fpqc descent we presented first.

Let $G = \operatorname{Gal}(k'/k)$. The left action of G on k' induces a right action of G on S'; each $\sigma \in G$ induces an automorphism σ^* of S'.

Proposition 4.4.2.

(i) *Giving a descent datum on a k'-scheme X' is equivalent to giving a right action of G on X' compatible with the right action of G on S', i.e., to giving a collection of isomorphisms $\tilde{\sigma}\colon X' \to X'$ for $\sigma \in G$ such that*

$$\begin{tikzcd}
X' \arrow[r, dotted, "\tilde{\sigma}"] \arrow[d] & X' \arrow[d] \\
S' \arrow[r, "\sigma^*"] & S'
\end{tikzcd}$$

commutes for each $\sigma \in G$ and $\widetilde{\sigma\tau} = \tilde{\tau}\tilde{\sigma}$ for all $\sigma, \tau \in G$.

(ii) *An isomorphism between k'-schemes with descent data is a k'-isomorphism that is equivariant for the G-actions in part* (i).

Unofficial version for incidental online use

(iii) *An open subscheme U' of a k'-scheme X' is stable under a descent datum described as in part* (i) *if and only if $\tilde{\sigma}(U') = U'$ for all $\sigma \in G$.*

Proof. Since k'/k is Galois, we have an isomorphism

$$\begin{aligned} k' \underset{k}{\otimes} k' &\xrightarrow{\sim} \prod_{\sigma \in G} k' \\ a \otimes b &\mapsto (a \cdot {}^{\sigma}b)_{\sigma \in G}. \end{aligned}$$

This induces isomorphisms

$$\begin{aligned} S'' &\simeq \coprod_{\sigma \in G} \operatorname{Spec} k' =: S' \times G, \\ S''' &\simeq S' \underset{S}{\times} S'' \simeq S' \underset{S}{\times} S' \times G \simeq S' \times G \times G. \end{aligned} \tag{4.4.3}$$

Plugging these into the definition of descent datum and doing some straightforward calculations yields the results. See [**BLR90**, §6.2B] for the details. □

The morphisms $\tilde{\sigma}$ are not morphisms of k'-schemes, since they lie over the σ^* instead of the identity. If desired, we can rewrite the conditions in Proposition 4.4.2 in terms of k'-morphisms. Recall from Section 2.2 that we can transform a k'-scheme by an element $\sigma \in G$.

Proposition 4.4.4. *Let X' be a k'-scheme.*

(i) *Giving a descent datum on X' is equivalent to giving a collection of k'-isomorphisms $f_\sigma \colon {}^{\sigma}X' \to X'$ for $\sigma \in G$ satisfying the "cocycle condition" $f_{\sigma\tau} = f_\sigma \cdot {}^{\sigma}(f_\tau)$ for all $\sigma, \tau \in G$.*

(ii) *An isomorphism between varieties with descent data, say X' with $(f_\sigma)_{\sigma \in G}$ and Y' with $(g_\sigma)_{\sigma \in G}$, is a k'-isomorphism $b \colon X' \to Y'$ such that $f_\sigma = b^{-1} g_\sigma({}^{\sigma}b)$ for all $\sigma \in G$.*

(iii) *An open subscheme $U' \subseteq X'$ is stable under a descent datum described as in part* (i) *if and only if $f_\sigma\left({}^{\sigma}U'\right) = U'$ for all $\sigma \in G$.*

Proof. We will use Proposition 4.4.2.

(i) Because of the isomorphism ${}^{\sigma}X' \to X'$ lying over σ^*, giving an isomorphism $\tilde{\sigma} \colon X' \to X'$ over σ^* is equivalent to giving a k'-isomorphism

Unofficial version for incidental online use

$f_\sigma\colon {}^\sigma X' \to X'$ fitting into the commutative diagram

(4.4.5)
$$\begin{tikzcd}
X' \arrow[dr, "\tilde\sigma"] & \\
{}^\sigma X' \arrow[u, dotted, "f_\sigma"] \arrow[r] \arrow[d] & X' \arrow[d] \\
S' \arrow[r, "\sigma^*"] & S'.
\end{tikzcd}$$

(Squares are cartesian, and we use dotted arrows to denote k'-morphisms.) The diagram

$$\begin{tikzcd}
X' \arrow[dr, "\tilde\sigma"] \arrow[drr, bend left, "\widetilde{\sigma\tau}"] & & \\
{}^\sigma X' \arrow[u, dotted, "f_\sigma"] \arrow[r] & X' \arrow[dr, "\tilde\tau"] & \\
{}^{\sigma\tau} X' \arrow[u, dotted, "{}^\sigma f_\tau"] \arrow[uu, dotted, bend left=60, "f_{\sigma\tau}"] \arrow[r] \arrow[d] & {}^\tau X' \arrow[u, dotted, "f_\tau"] \arrow[r] \arrow[d] & X' \arrow[d] \\
S' \arrow[r, "\sigma^*"] \arrow[rr, bend right, "(\sigma\tau)^*"'] & S' \arrow[r, "\tau^*"] & S'
\end{tikzcd}$$

shows that $\widetilde{\sigma\tau} = \tilde\tau\tilde\sigma$ is equivalent to $f_{\sigma\tau} = f_\sigma \cdot {}^\sigma(f_\tau)$.

(ii) A k'-isomorphism $b\colon X' \to Y'$ is G-equivariant if and only if for every $\sigma \in G$, the 3-dimensional diagram formed by two copies of (4.4.5), one for X' and one for Y', connected by vertical isomorphisms given by $b\colon X' \to Y'$ and ${}^\sigma b\colon {}^\sigma X' \to {}^\sigma Y'$, commutes, or equivalently,

$$\begin{tikzcd}
{}^\sigma X' \arrow[r, dotted, "f_\sigma"] \arrow[d, dotted, "{}^\sigma b"] & X' \arrow[d, dotted, "b"] \\
{}^\sigma Y' \arrow[r, dotted, "g_\sigma"] & Y'
\end{tikzcd}$$

commutes.

(iii) The diagram (4.4.5) shows that $\tilde\sigma(U') = U'$ if and only if $f_\sigma({}^\sigma U') = U'$. $\square$

Corollary 4.4.6. *Let k'/k be a finite Galois extension of fields. Let X' be a quasi-projective k'-scheme. Suppose that we are given k'-isomorphisms $f_\sigma\colon {}^\sigma X' \to X'$ for $\sigma \in G$ satisfying $f_{\sigma\tau} = f_\sigma \cdot {}^\sigma(f_\tau)$ for all $\sigma, \tau \in G$. Then $X' = X_{k'}$ for some k-scheme X.*

Unofficial version for incidental online use

Proof. As in the proof of Proposition 4.4.4, giving the f_σ is equivalent to giving a right action of G on X'. By Theorem 4.3.5, it suffices to show that X' can be covered by G-invariant quasi-affine open subsets. Fix an embedding $X' \hookrightarrow \mathbb{P}^n_{k'}$. Given $x' \in X'$, we can choose a hypersurface $H \subset \mathbb{P}^n_{k'}$ that does not meet the G-orbit of x'. (In fact, if k' is infinite, then a hyper*plane* suffices.) Let $U' = X' - H$. Then $\bigcap_{\sigma \in G} \tilde{\sigma}(U')$ is a quasi-affine open subset of X' containing x'. $\square$

Remark 4.4.7. More generally, a finite and faithfully flat morphism of schemes $p\colon S' \to S$ equipped with a finite group G of automorphisms of S' as an S-scheme (acting on the right) is called a **Galois covering with Galois group** G if the morphism $S' \times G \to S''$ given by (id, σ) on the piece $S' \times \{\sigma\}$ for each $\sigma \in G$ is an isomorphism of schemes (cf. (4.4.3)). Propositions 4.4.2 and 4.4.4 continue to hold in this setting. Corollary 4.4.6 holds too, provided that we assume that S is affine (so that S' is affine too); this condition is used to construct the hypersurface H in the proof.

Remark 4.4.8. Sometimes the scheme X' to be descended to k is over k_{s} instead of a finite Galois extension of k. In that case, assuming that X' is finitely presented, we may use that k_{s} is the direct limit of its finite Galois subextensions to obtain X' as the base extension of a scheme over a finite Galois extension of k before applying Galois descent.

4.5. Twists

(Reference: [**Ser02**, III.§1])

Let X be a quasi-projective k-variety. Let k'/k be a Galois extension of fields, and let $\mathfrak{G} = \mathrm{Gal}(k'/k)$.

Definition 4.5.1. A k'/k-**twist** (or k'/k-**form**) of X is a k-variety Y such that there exists an isomorphism $\phi\colon X_{k'} \xrightarrow{\sim} Y_{k'}$. A **twist** of X is a k_{s}/k-twist of X.

The set of k-isomorphism classes of k'/k-twists of X is a pointed set, with neutral element given by the isomorphism class of X. The action of $\mathfrak{G}$ on k' induces an action of $\mathfrak{G}$ on the automorphism group $\operatorname{Aut} X_{k'}$.

Theorem 4.5.2. *There is a natural bijection of pointed sets*

$$\frac{\{k'/k\text{-twists of } X\}}{k\text{-isomorphism}} \xrightarrow{\sim} \mathrm{H}^1(\mathfrak{G}, \operatorname{Aut} X_{k'}).$$

Warning 4.5.3. It is the automorphism group of $X_{k'}$, not X, that appears. Also, the group $\operatorname{Aut} X_{k'}$ may be nonabelian, so it may be necessary to use nonabelian group cohomology as in [**Ser02**, I.§5].

Unofficial version for incidental online use

Proof of Theorem 4.5.2. We may assume that k'/k is finite, since at the end we can take a direct limit of both sides.

For each $\sigma \in \mathfrak{G}$, we identify ${}^{\sigma}X_{k'}$ with $X_{k'}$. To give a k'/k-twist of X is to descend $X_{k'}$ to a k-variety. By Theorem 4.3.5 and the fact that $X_{k'}$ is quasi-projective, this is the same as giving a descent datum on $X_{k'}$. By Proposition 4.4.4(i) this is the same as giving a 1-cocycle $\mathfrak{G} \to \operatorname{Aut} X_{k'}$.

By Theorem 4.3.5(i), two such twists are k-isomorphic if and only if the descent data are isomorphic, which by Proposition 4.4.4(ii) holds if and only if the 1-cocycles are cohomologous. □

Remark 4.5.4. Explicitly, given a k'/k-twist Y, an associated 1-cocycle is constructed as follows: choose a k'-isomorphism $\phi\colon X_{k'} \xrightarrow{\sim} Y_{k'}$, and define

$$f_\sigma := \phi^{-1}\,({}^{\sigma}\phi) \quad \in \operatorname{Aut} X_{k'}.$$

Warning 4.5.5. Given an element of $\mathrm{H}^1(\mathfrak{G}, \operatorname{Aut} X_{k'})$, one gets an isomorphism class of k'/k-twists, but there is no natural way to select a particular twist in that isomorphism class. Thus, strictly speaking, it is incorrect to speak of "the twist associated to a cohomology class". To determine a twist, one should select a cocycle representing that cohomology class.

Important Remark 4.5.6. Although we used quasi-projective k-varieties in Theorem 4.5.2, an analogous result holds for twists of many other "k-objects", where $\operatorname{Aut} X_{k'}$ now denotes the automorphism group of $X_{k'}$ as a k'-object. (To make this precise, one should specify a category of k-objects, a corresponding category of k'-objects, a notion of base extension, etc., satisfying certain axioms.) To get injectivity of the natural map in Theorem 4.5.2, one needs that $\mathfrak{G}$-invariant morphisms between base extensions of k-objects descend. To get surjectivity, one needs that descent data on k'-objects be effective. These conditions (especially the latter) can sometimes fail.

4.5.1. Severi–Brauer varieties.

Definition 4.5.7. A **Severi–Brauer variety** over k is a twist of the k-variety $\mathbb{P}^{n-1}_k$ for some $n \geq 1$.

Example 4.5.8. The 1-dimensional Severi–Brauer varieties over k are exactly the nice genus 0 curves over k.

Because Severi–Brauer varieties are twists, it is natural (but not necessary [**Kol16**]) to use cohomology to study them. First, $\operatorname{Aut} \mathbb{P}^{n-1}_{k_{\mathrm{s}}}$ equals $\mathrm{PGL}_n(k_{\mathrm{s}})$, which is also the automorphism group of the matrix algebra $\mathrm{M}_n(k_{\mathrm{s}})$. Applying Theorem 4.5.2 and recalling material from Section 1.5.5,

Unofficial version for individual online use

we get

$$\begin{tikzcd}
\{(n-1)\text{-dimensional Severi–Brauer varieties}/k\} \arrow[d, leftrightarrow] & \\
\mathrm{H}^1(\mathfrak{G}_k, \mathrm{PGL}_n(k_s)) \arrow[r, hook] \arrow[d, leftrightarrow] & \mathrm{Br}\, k. \\
\{n^2\text{-dimensional Azumaya } k\text{-algebras}\} &
\end{tikzcd}$$

Remark 4.5.9. One can show also that if X is a k-variety such that $X_{\overline{k}} \simeq \mathbb{P}^{n-1}_{\overline{k}}$, then $X_{k_s} \simeq \mathbb{P}^{n-1}_{k_s}$ already; i.e., X is a Severi–Brauer variety. This can be viewed as a consequence of the triviality of the fppf cohomology set $\mathrm{H}^1(k_s, \mathrm{PGL}_n)$ (cf. Remark 6.6.3 and Theorem 6.4.6(iii)), or it can be related to the fact that an Azumaya algebra over a separably closed field is split.

Proposition 4.5.10 (Châtelet)**.** *The following are equivalent for an $(n-1)$-dimensional Severi–Brauer variety X over a field k:*

(i) $X \simeq \mathbb{P}^{n-1}_k$.

(ii) X *is birational to* $\mathbb{P}^{n-1}_k$.

(iii) $X(k) \neq \emptyset$.

Proof.

(i)$\Rightarrow$(ii): Trivial.

(ii)$\Rightarrow$(iii): This follows from the Lang–Nishimura theorem; see Corollary 3.6.16.

(iii)$\Rightarrow$(i): Choose $x \in X(k)$. Since X is a Severi–Brauer variety, there exists an isomorphism $X_{k_s} \xrightarrow{\sim} \mathbb{P}^{n-1}_{k_s}$. Compose it with an automorphism of $\mathbb{P}^{n-1}_{k_s}$ so that it maps x to the point $P := (1 : 0 : \cdots : 0) \in \mathbb{P}^{n-1}(k)$. Then (X, x) may be viewed as a twist of the pointed variety $(\mathbb{P}^{n-1}_k, P)$. The automorphisms of $(\mathbb{P}^{n-1}_k, P)$ over k_s are the automorphisms of $\mathbb{P}^{n-1}_{k_s}$ that fix P. They form a subgroup of $\mathrm{PGL}_n(k_s)$:

$$\mathrm{Aut}(\mathbb{P}^{n-1}_{k_s}, P) \quad = \quad \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix} \bmod {k_s}^{\times} \quad \simeq \quad \begin{pmatrix} 1 & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix}.$$

The "forget the first row and column" map is a homomorphism from the group on the right onto $\mathrm{GL}_{n-1}(k_s)$, and we obtain a $\mathfrak{G}_k$-equivariant exact sequence

$$0 \longrightarrow (k_s)^{n-1} \longrightarrow \mathrm{Aut}(\mathbb{P}^{n-1}_{k_s}, P) \longrightarrow \mathrm{GL}_{n-1}(k_s) \longrightarrow 0.$$

Unofficial version for incidental online use

By Proposition 1.3.15(i,iii), the H^1 of the group at each end is trivial, so in the middle $\mathrm{H}^1\left(\mathfrak{G}_k, \operatorname{Aut}(\mathbb{P}^{n-1}_{k_s}, P)\right)$ is trivial too. Equivalently, by Theorem 4.5.2, the pointed variety $(\mathbb{P}^{n-1}_k, P)$ has no nontrivial twists. Thus $(X,x) \simeq (\mathbb{P}^{n-1}_k, P)$. In particular, $X \simeq \mathbb{P}^{n-1}_k$. □

Theorem 4.5.11 (Châtelet)**.** *Severi–Brauer varieties over global fields satisfy the local-global principle.*

Proof. Let X be the variety, and let x be the corresponding element of $\operatorname{Br} k$. Let $n-1 = \dim X$. By Proposition 4.5.10,

$$X(k) \neq \emptyset \quad \Longleftrightarrow \quad X \simeq \mathbb{P}^{n-1}_k \quad \Longleftrightarrow \quad x = 0.$$

The variety X_{k_v} is a Severi–Brauer variety over k_v corresponding to the image x_v of x in $\operatorname{Br} k_v$, so we similarly have

$$X(k_v) \neq \emptyset \quad \Longleftrightarrow \quad x_v = 0.$$

Thus the result follows from the injectivity of

$$\operatorname{Br} k \longrightarrow \bigoplus_v \operatorname{Br} k_v,$$

which was mentioned in Section 1.5.9. □

4.5.1.1. *Rational maps between Severi–Brauer varieties.*

Proposition 4.5.12. *Let X and Y be positive-dimensional Severi–Brauer varieties over a field k. Let $x, y \in \operatorname{Br} k$ be the corresponding Brauer classes. Let $f\colon X \dashrightarrow Y$ be a rational map. Let $U \subseteq X$ be the domain of definition of f. The composition*

$$\mathbb{Z} = \operatorname{Pic} Y_{k_s} \xrightarrow{f^*} \operatorname{Pic} U_{k_s} \xleftarrow{\sim} \operatorname{Pic} X_{k_s} = \mathbb{Z}$$

(*in which the identifications at each end associate* 1 *to the ample generator* $\mathscr{O}(1)$ *of the Picard group of each projective space over* k_s) *is multiplication by some nonnegative integer m. Then $y = mx$.*

Sketch of proof. For any nice k-variety X, the exact sequences

$$0 \longrightarrow \frac{\mathbf{k}(X_{k_s})^\times}{{k_s}^\times} \longrightarrow \operatorname{Div} X_{k_s} \longrightarrow \operatorname{Pic} X_{k_s} \longrightarrow 0,$$

$$0 \longrightarrow {k_s}^\times \longrightarrow \mathbf{k}(X_{k_s})^\times \longrightarrow \frac{\mathbf{k}(X_{k_s})^\times}{{k_s}^\times} \longrightarrow 0$$

define connecting homomorphisms

$$\mathrm{H}^0(\mathfrak{G}_k, \operatorname{Pic} X_{k_s}) \longrightarrow \mathrm{H}^1\left(\mathfrak{G}_k, \frac{\mathbf{k}(X_{k_s})^\times}{{k_s}^\times}\right) \longrightarrow \mathrm{H}^2(\mathfrak{G}_k, {k_s}^\times)$$

Unofficial version for incidental online use

whose composition is a homomorphism $(\operatorname{Pic} X_{k_s})^{\mathfrak{G}_k} \to \operatorname{Br} k$. Moreover, given a rational map $X \dashrightarrow Y$, we obtain a commutative diagram

(4.5.13)
$$\begin{tikzcd} (\operatorname{Pic} Y_{k_s})^{\mathfrak{G}_k} \arrow[r] \arrow[d] & \operatorname{Br} k \arrow[d, equal] \\ (\operatorname{Pic} X_{k_s})^{\mathfrak{G}_k} \arrow[r] & \operatorname{Br} k \end{tikzcd}$$

Finally, in the case where X is a positive-dimensional Severi–Brauer variety corresponding to an Azumaya algebra A, we have $(\operatorname{Pic} X_{k_s})^{\mathfrak{G}_k} \simeq \mathbb{Z}$, and a computation proves a theorem of Lichtenbaum stating that the class of $\mathscr{O}(1)$ (corresponding to $1 \in \mathbb{Z}$) maps to the class of A in $\operatorname{Br} k$; see [**GS06**, 5.4.10]. Chasing elements in diagram (4.5.13) yields

$$\begin{tikzcd} 1 \arrow[r, mapsto] \arrow[d, mapsto, "m"'] & y \arrow[d, equal] \\ m \arrow[r, mapsto] & mx. \end{tikzcd}$$ ☐

Warning 4.5.14. The quantity m appearing in Proposition 4.5.12 acts strangely:

- It is not directly related to the notion of degree in Definition 3.6.10.
- It is not multiplicative with respect to composition of rational maps.
- For a birational map, m need not be 1.

Example 4.5.15. If $f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ is the quadratic transformation

$$(x : y : z) \mapsto \left(\frac{1}{x} : \frac{1}{y} : \frac{1}{z}\right) = (yz : zx : xy),$$

then $m = 2$. But $f \circ f$ is the identity, which has $m = 1$.

Corollary 4.5.16. *Let X and Y be Severi–Brauer varieties over a field k. Let $x, y \in \operatorname{Br} k$ be the corresponding Brauer classes. If X and Y are birational, then x and y generate the same subgroup of $\operatorname{Br} k$.*

Remark 4.5.17. Amitsur [**Ami55**] conjectured a converse to Corollary 4.5.16, namely, that if X and Y are Severi–Brauer varieties of the same dimension whose classes generate the same subgroup of $\operatorname{Br} k$, then X and Y are birational. For some partial results toward Amitsur's conjecture, see [**Roq64**, **Tre91**].

Remark 4.5.18. Integral varieties X and Y are called **stably birational** if $X \times \mathbb{P}^m$ and $Y \times \mathbb{P}^n$ are birational for some $m, n \geq 0$. Even over $\mathbb{C}$, stably birational varieties of the same dimension need not be birational [**BCTSSD85**]. Exercise 4.6 asks for a proof of the following weak form of Amitsur's conjecture: if X and Y are Severi–Brauer varieties of the same dimension whose

Unofficial version for incidental online use

classes generate the same subgroup of $\operatorname{Br} k$, then X and Y are stably birational.

4.6. Restriction of scalars

(Reference: [**BLR90**, §7.6])

Let $L \supseteq k$ be a finite extension of fields, and let X be an L-variety. We want to construct a k-variety $\mathcal{X}$ whose arithmetic over k mimics the arithmetic of X over L. In particular, we want a bijection $\mathcal{X}(k) \simeq X(L)$. But this condition is not enough to determine $\mathcal{X}$ uniquely.

Definition 4.6.1. Let L be a finite extension of a field k, and let X be an L-variety. The **restriction of scalars** (also called **Weil restriction**) $\mathcal{X} = \operatorname{Res}_{L/k}(X)$, if it exists, is a k-variety characterized by the existence of bijections $\mathcal{X}(S) \to X(S \times_k L) = \operatorname{Hom}_L(S \times_k L, X)$, for each k-scheme S, varying functorially in S.

"Functorially in S" means that for any k-morphism $f \colon S \to T$, the diagram

$$\begin{array}{ccc} \mathcal{X}(T) & \longrightarrow & X(T \times_k L) \\ \big\downarrow & & \big\downarrow \\ \mathcal{X}(S) & \longrightarrow & X(S \times_k L) \end{array}$$

induced by f and its base extension $f_L \colon S \times_k L \to T \times_k L$ commutes. In other words, the restriction of scalars, if it exists, is a k-scheme representing the functor $S \mapsto X(S \times_k L)$.

If X is an affine L-variety, then $\mathcal{X} := \operatorname{Res}_{L/k} X$ exists as an affine k-variety, and can be described explicitly as follows. Write

$$X = \operatorname{Spec} L[x_1, \ldots, x_n]/(f_1, \ldots, f_m).$$

Choose a basis $e_1, \ldots, e_s$ of L over k. Introduce new variables y_{ij} with $1 \le i \le n$ and $1 \le j \le s$, and substitute

$$x_i = \sum_{j=1}^{s} y_{ij} e_j$$

for all i into f_r for each r, so that

$$f_r(x_1, \ldots, x_n) = F_{r,1} e_1 + \cdots + F_{r,s} e_s$$

for some polynomials $F_{r,\ell} \in k[\{y_{ij}\}]$. Then $\mathcal{X} = \operatorname{Spec} k[\{y_{ij}\}]/(\{F_{r,\ell}\})$.

Unofficial version for incidental online use

Example 4.6.2. Let $k = \mathbb{Q}$, let $L = \mathbb{Q}(\sqrt{2})$, and let X be the curve in $\mathbb{A}^2_L$ defined by $x_1x_2 + (5 + 7\sqrt{2}) = 0$. Substituting

$$x_1 = y_{11} + y_{12}\sqrt{2},$$
$$x_2 = y_{21} + y_{22}\sqrt{2},$$

we get

$$(y_{11}y_{21} + 2y_{12}y_{22} + 5) + (y_{11}y_{22} + y_{12}y_{21} + 7)\sqrt{2} = 0,$$

so $\mathcal{X}$ is the surface in $\mathbb{A}^4_{\mathbb{Q}}$ defined by the system of equations

$$y_{11}y_{21} + 2y_{12}y_{22} + 5 = 0,$$
$$y_{11}y_{22} + y_{12}y_{21} + 7 = 0.$$

The fact that $\mathcal{X}(\mathbb{Q})$ equals $X(L)$ is almost a tautology. To show more generally that $\mathcal{X}(S)$ equals $X(S_L)$ for any k-scheme S, one uses the fact that $\mathscr{O}_{S_L}(S_L) = \mathscr{O}_S(S) \otimes_k L$, which follows easily from the construction of the fiber product.

For non-affine varieties, the restriction of scalars is harder to construct, and sometimes it even fails to exist!

Proposition 4.6.3. *Let $L \supseteq k$ be a finite extension of fields, and let X be an L-variety. If every finite subset of X is contained in some affine open subset of X, then $\operatorname{Res}_{L/k} X$ exists.*

Proof. This is a special case of [**BLR90**, §7.6, Theorem 4]. The idea of the proof is to take the restriction of scalars of *each* affine subvariety of X, and then to use descent to show that they can be glued. □

Remark 4.6.4. To see why one must use affine open subvarieties containing finite subsets instead of just affine open subvarieties forming a covering of X, do Exercise 4.8.

Important Remark 4.6.5. Any quasi-projective variety X over L satisfies the hypothesis of Proposition 4.6.3.

Restriction of scalars can often be used to reduce questions about varieties over a large field to questions about (higher-dimensional) varieties over smaller fields. For example, it is known [**Mil72**, Theorem 1] that if L is a finite separable extension of a global field k and A is an abelian variety over L, then the full Birch and Swinnerton-Dyer conjecture holds for A over L (see Conjecture 5.7.33 and Remark 5.7.34) if and only if it holds for the abelian variety $\operatorname{Res}_{L/k} A$ over k. This lets one reduce the conjecture for abelian varieties over global fields to the conjecture for abelian varieties over $\mathbb{Q}$ and $\mathbb{F}_p(t)$.

Unofficial version for incidental online use

Remark 4.6.6. One can generalize the notion of restriction of scalars to $\operatorname{Res}_{S'/S}$ where S' is a finite and locally free scheme over a base scheme S. (Our discussion corresponds to the special case $S = \operatorname{Spec} k$ and $S' = \operatorname{Spec} L$.)

Remark 4.6.7 (Greenberg transform)**.** Let R be a discrete valuation ring, with uniformizer π and perfect residue field k. Let $R_n = R/\pi^n R$. For example, R_n could be the ring $W_n(k)$ of length n Witt vectors (see [**Ser79**, II.§6]). The level n Greenberg functor takes a scheme X locally of finite type over R_n and returns a k-scheme $\mathcal{X}$, called the **Greenberg transform**; see [**BLR90**, p. 276] for more details. The Greenberg transform acts very much like the restriction of scalars, but cannot be considered as a special case even of the generalized restriction of scalars in Remark 4.6.6, because R_n need not be a k-algebra.

Example 4.6.8 (Jet spaces)**.** If X is a finite-type scheme over a field k and $A := k[[t]]/(t^{n+1})$, then $\operatorname{Res}_{A/k} X_A$ exists as a finite-type k-scheme and is called the n**th jet space** of X [**BLR90**, p. 276]. This could also be viewed as a special case of the Greenberg transform, at least when k is perfect.

Exercises

4.1. (Field of moduli not a field of definition) Let $\sigma \in \operatorname{Gal}(\mathbb{C}/\mathbb{R})$ denote complex conjugation. Let $a_0, \ldots, a_6$ be complex numbers such that ${}^\sigma a_{6-j} = (-1)^{j+1} a_j$ for $0 \le j \le 6$. Let $f(x) = a_6 x^6 + \cdots + a_0$. Assume that $f(x)$ is a separable polynomial of degree 6. Let X be the smooth projective model of the affine curve $y^2 = f(x)$ over $\mathbb{C}$. Assume that the only nontrivial automorphism of X is the hyperelliptic involution ι, induced by the automorphism $(x, y) \mapsto (x, -y)$ of the affine curve.

(a) Prove that X is isomorphic to ${}^\sigma X$ as a $\mathbb{C}$-variety, where σ is the nontrivial element of $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$.

(b) Prove that X is not the base extension of a curve defined over $\mathbb{R}$.

(c) Prove that the hypotheses of the problem can actually be satisfied! (*Hint*: For a suitable choice of a_i, prove $\operatorname{Aut} X = \{1_X, \iota\}$ by using that any automorphism of X induces an automorphism of $X/\iota \simeq \mathbb{P}^1$ preserving the six branch points.)

4.2. (Twists of a superelliptic curve) Let k be a field, and let n be a positive integer such that $\operatorname{char} k \nmid n$. Fix $f(x) \in k[x]$ such that $y^n - f(x) = 0$ defines a geometrically integral affine curve over k; let X be its smooth projective model. Assuming that every automorphism of $X_{\overline{k}}$ fixes the rational function x, describe the set of twists of X up to k-isomorphism.

Unofficial version for incidental online use

4.3. (Rational points on a quadratic twist of an elliptic curve) Let k be a field. Let E be an elliptic curve over k with equation $y^2 = x^3 + ax + b$; i.e., E is the projective closure of that affine curve, and E is smooth (so $\operatorname{char} k \neq 2$). Let $d \in k^\times \setminus k^{\times 2}$, let $L = k(\sqrt{d})$, and let σ be the nontrivial element of $\operatorname{Gal}(L/k)$. Let E' be the elliptic curve over k with equation $dy^2 = x^3 + ax + b$. Prove that $E'(k)$ is isomorphic to the group $\{P \in E(L) : {}^\sigma P = -P\}$.

4.4. Let k be a field. Let $k(t)$ be the rational function field over k. Let E be an elliptic curve over k with Weierstrass equation $y^2 = x^3 + ax + b$. Let E' be the elliptic curve over $k(t)$ with Weierstrass equation

$$(t^3 + at + b)y^2 = x^3 + ax + b.$$

Prove that $E'(k(t)) \simeq (\operatorname{End} E) \oplus E[2](k)$ as abelian groups.

4.5. Let X be a nice genus 0 curve over a global field k. Use the description of $\operatorname{Br} k$ to prove the following:

(a) The curve X has a k-point if and only if X has a k_v-point for every place v of k.

(b) The number of places v for which $X(k_v) = \emptyset$ is finite and even.

4.6. Let X and Y be Severi–Brauer varieties of dimension $n-1$ whose classes in $\operatorname{Br} k$ generate the same subgroup. Prove that $X \times \mathbb{P}^{n-1}$, $X \times Y$, and $Y \times \mathbb{P}^{n-1}$ are all birational to each other. (*Hint*: Use Proposition 4.5.10.)

4.7. Let $L \supseteq k$ be a finite Galois extension of fields, with Galois group G. Let X be an L-variety. Assume that the k-variety $\mathcal{X} := \operatorname{Res}_{L/k} X$ exists. Prove that $\mathcal{X}_L \simeq \prod_{\sigma \in G} {}^\sigma X$ as L-varieties.

4.8. Let $X = \mathbb{P}^1_{\mathbb{C}}$. Let $U = X - \{0\}$ and $V = X - \{\infty\}$ be the standard copies of $\mathbb{A}^1_{\mathbb{C}}$ whose union is X. Prove that the union of the open subschemes $\operatorname{Res}_{\mathbb{C}/\mathbb{R}} U$ and $\operatorname{Res}_{\mathbb{C}/\mathbb{R}} V$ does *not* equal $\operatorname{Res}_{\mathbb{C}/\mathbb{R}} X$.

4.9. (Inseparable restriction of scalars) Let $L = \mathbb{F}_p(t)$ and $k = \mathbb{F}_p(t^p)$. Let X be the L-scheme $\operatorname{Spec} L[x]/(x^p - t)$. Compute $\operatorname{Res}_{L/k} X$. (The answer may surprise you!)

Unofficial version for incidental online use

Unofficial version for incidental online use

Chapter 5

Algebraic groups

Unofficial version for incidental online use

5.1. Group schemes

(References: [**Vis05**, §2.2], [**Wat79**])

5.1.1. Category-theoretic definition of groups. Let pt be an empty product of sets; in other words, pt is a terminal object in the category **Sets**, i.e., a one-element set.

A **group** can be interpreted as a set G equipped with maps $m\colon G\times G \to G$ (multiplication), $i\colon G \to G$ (inverse), and $e\colon \mathrm{pt} \to G$ (identity) satisfying the group axioms, namely the commutativity of the following diagrams, in which $1\colon G \to G$ is the identity on G.

- Associativity:

$$\begin{tikzcd} G\times G\times G \arrow[r, "m\times 1"] \arrow[d, "1\times m"] & G\times G \arrow[d, "m"] \\ G\times G \arrow[r, "m"] & G. \end{tikzcd}$$

- Identity (left and right):

$$\begin{tikzcd} \mathrm{pt}\times G \arrow[r, "e\times 1"] \arrow[dr, equal] & G\times G \arrow[d, "m"] \\ & G \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} G\times \mathrm{pt} \arrow[r, "1\times e"] \arrow[dr, equal] & G\times G \arrow[d, "m"] \\ & G. \end{tikzcd}$$

- Inverse (left and right):

$$\begin{tikzcd} G \arrow[r, "(i,1)"] \arrow[d] & G \times G \arrow[d, "m"] \\ \mathrm{pt} \arrow[r, "e"] & G \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} G \arrow[r, "(1,i)"] \arrow[d] & G \times G \arrow[d, "m"] \\ \mathrm{pt} \arrow[r, "e"] & G. \end{tikzcd}$$

The definitions of commutativity, group homomorphism, (right or left) action of a group on a set (i.e., G-set), and G-equivariant map (i.e., morphism of G-sets) are category-theoretic too.

5.1.2. Group objects. Let $\mathcal{C}$ be a category with **finite products**: i.e., for any $n \geq 0$ and for any objects $G_1, \ldots, G_n$ of $\mathcal{C}$, there is an object G equipped with a morphism to each G_i such that any other object H equipped with a morphism to each G_i admits a unique morphism to G compatible with the morphisms $G \to G_i$. For $n = 0$, an empty product is the same thing as a terminal object of $\mathcal{C}$.

Then a **group object** in $\mathcal{C}$ is an object G equipped with morphisms m, i, e satisfying the group axioms listed in Section 5.1.1.

Example 5.1.1. A group object in **Sets** is a group.

Example 5.1.2. A group object in the category of topological spaces with continuous maps is a **topological group**. (Actually, many authors require a topological group to be Hausdorff; if one wants this, one should start with the full subcategory of Hausdorff topological spaces.)

The definitions of commutative group object, homomorphism of group objects, action of a group object G on an object, and G-equivariant morphism are defined by the same diagrams used for **Sets**. In particular, the group objects in $\mathcal{C}$ form their own category.

5.1.3. Group schemes.

Definition 5.1.3. A **group scheme** G over a scheme S is a group object in the category of S-schemes.

In the category of S-schemes, products are fiber products over S, and the terminal object is the S-scheme S. So, for example, a **homomorphism of group schemes** $G \to H$ over S is an S-morphism respecting the multiplication morphisms m_G and m_H, that is, an S-morphism $\phi\colon G \to H$ making

$$\begin{tikzcd} G \times_S G \arrow[r, "m_G"] \arrow[d, "(\phi,\phi)"'] & G \arrow[d, "\phi"] \\ H \times_S H \arrow[r, "m_H"] & H \end{tikzcd}$$

Unofficial version for incidental online use

commute.

Remark 5.1.4. If $S = \operatorname{Spec} R$, and $G = \operatorname{Spec} A$ is an *affine* group scheme over R, then m, i, e correspond to R-algebra homomorphisms with their own names,

$$\begin{aligned} \Delta\colon A &\to A \otimes_R A && (\textbf{comultiplication}), \\ S\colon A &\to A && (\textbf{antipode}), \\ \epsilon\colon A &\to R && (\textbf{counit}), \end{aligned}$$

satisfying opposite axioms. Together with the R-algebra structure on A, given by the structure homomorphism $R \to A$ and multiplication $A \otimes_R A \to A$, this makes A into a **commutative Hopf algebra** over R. In fact, the axioms defining commutative Hopf algebra are such that one obtains an equivalence of categories

$$\{\text{affine group schemes over } R\}^{\text{opp}} \to \{\text{commutative Hopf algebras over } R\}.$$

Definition 5.1.5. A **subgroup scheme** of a group scheme G is a group scheme H that is also a closed subscheme of G, and for which the inclusion $H \to G$ is a homomorphism.

Definition 5.1.6. If k is a field, a **group variety** over k is a group object in the category of k-varieties.

Group varieties form a full subcategory of the category of group schemes.

5.1.4. Functor of points of a group scheme. Intuitively, to make a k-variety G into a group scheme, one would want a morphism $G \times G \to G$ giving the set $G(k)$ the structure of a group; this is a valid description if k is algebraically closed and G is reduced. More generally, to describe a group law on an S-scheme G, one should use the whole functor of points instead of just $G(S)$. This leads to an equivalent definition of group scheme that is perhaps closer to geometric intuition:

Proposition 5.1.7. *Let G be an S-scheme. Equipping G with the structure of a group scheme over S is equivalent to equipping the set $G(T)$ with a group structure for each S-scheme T such that for any S-morphism $T' \to T$, the map of sets $G(T) \to G(T')$ is a group homomorphism. Equivalently, making G a group scheme over S is equivalent to giving a functor $\mathcal{G}\colon$* $\mathbf{Schemes}_S^{\text{opp}} \to$ $\mathbf{Groups}$ *completing the commutative diagram*

$$\begin{tikzcd} \mathbf{Schemes}_S^{\text{opp}} \arrow[rr, "h_G"] \arrow[dr, dashed, "\mathcal{G}"'] & & \mathbf{Sets}\,. \\ & \mathbf{Groups} \arrow[ur, "\text{forgetful}"'] & \end{tikzcd}$$

Unofficial version for incidental online use

Proof. This is just Yoneda's lemma (Lemma 2.3.4): To give compatible multiplication maps $G(T)\times G(T) \to G(T)$ is to give an S-morphism $G\times G \to G$, and so on. □

Homomorphisms of group schemes, group scheme actions, and equivariant morphisms can be described similarly. For example, giving a right action of a group scheme G on an S-scheme X is equivalent to giving a collection of compatible group actions $X(T)\times G(T) \to X(T)$ (in the category of sets), one for each S-scheme T. Such an action is **faithful** if for every S-scheme T and $g \in G(T)$ not equal to 1, there exists $T' \to T$ and $x \in X(T')$ such that $gx \neq x$ (here gx is defined by mapping g to an element of $G(T')$ before acting).

Warning 5.1.8. If G acts faithfully on X, it does not follow that $G(T)$ acts faithfully on $X(T)$ for each T. A group scheme G acting on a nontrivial torsor X gives a counterexample (see Definition 5.12.3).

Various properties of a group scheme are also conveniently described in terms of its functor of points. For instance, a subgroup scheme H of G is **normal** if and only if $H(T)$ is a normal subgroup of $G(T)$ for every S-scheme T.

Unofficial version for incidental online use

5.1.5. Examples of group schemes.

(1) The additive group scheme $\mathbb{G}_a$ over a ring A is $\mathbb{A}^1_A = \operatorname{Spec} A[t]$ with $m\colon \mathbb{G}_a \times \mathbb{G}_a \to \mathbb{G}_a$ given in coordinates by $(t_1, t_2) \mapsto t_1 + t_2$; that is, m corresponds to the A-algebra homomorphism

$$\begin{aligned} A[t] &\to A[t_1] \otimes_A A[t_2] \\ t &\mapsto t_1 \otimes 1 + 1 \otimes t_2. \end{aligned}$$

Similarly i is given by $t \mapsto -t$, and e corresponds to the ring homomorphism $A[t] \to A$ mapping t to 0.

(2) The multiplicative group scheme $\mathbb{G}_m$ over A is defined the same way, but using $\operatorname{Spec} A[t, t^{-1}]$ with m given in coordinates by $(t_1, t_2) \mapsto t_1 t_2$, and so on.

(3) For each $n \geq 0$, the group scheme GL_n over a ring A is

$$\operatorname{Spec} A[x_{11}, x_{12}, \ldots, x_{nn}, 1/\det],$$

where det is the determinant of the $n \times n$ matrix with indeterminate entries $x_{11}, \ldots, x_{nn}$. (One defines m, i, and e in the obvious way.) One has $\mathrm{GL}_1 \simeq \mathbb{G}_m$.

(4) Similarly, the group scheme SL_n over a ring A is

$$\operatorname{Spec} A[x_{11}, x_{12}, \ldots, x_{nn}]/(\det -1).$$

(5) Let U_n be the closed subgroup scheme of GL_n such that for every scheme S, the set $\mathrm{U}_n(S)$ is the set of upper triangular matrices in $\mathrm{GL}_n(S)$ with every diagonal entry equal to 1.

(6) When one has a group scheme over $\mathbb{Z}$, one can base extend to get a corresponding group scheme over any scheme S. Thus for instance, one can define $\mathbb{G}_{a,S}$, $\mathrm{SL}_{n,S}$, and so on.

(7) Let G be a group, and let S be a scheme. For each $\sigma \in G$, let S_σ be a copy of S. Then $\coprod_{\sigma \in G} S_\sigma$ can be made a group scheme over S, by letting m map $S_\sigma \times_S S_\tau$ isomorphically to $S_{\sigma\tau}$ for each $\sigma, \tau \in G$. This is called a **constant group scheme**.

(8) An elliptic curve over a field k is an example of a group scheme of finite type over k.

Definition 5.1.9. If G is a group scheme over S such that $\mathscr{O}_G$ is locally free of rank r as an $\mathscr{O}_S$-module, then the **order** of G is $\#G := r$.

Example 5.1.10. If G_S is the constant group scheme over S associated to a finite group G, then $\#G_S = \#G$.

Example 5.1.11. If G is a finite group scheme over a field k, then $G = \operatorname{Spec} A$ for some finite-dimensional k-algebra A, and $\#G = \dim_k A$.

5.1.6. Kernels.

Definition 5.1.12. The **kernel** K of a homomorphism of group schemes $\phi\colon G \to H$ is $\phi^{-1}(e)$, where $e\colon S \to H$ is the identity of H. More explicitly, $\ker \phi$ is the S-group scheme $G \times_H S$, where the S in the fiber product is viewed as an H-scheme via e. The m, i, e for $\ker \phi$ are induced from the m, i, e of G by base extension. Alternatively, one can describe K as the group scheme whose functor of points is given by $K(T) := \ker(G(T) \to H(T))$. Sometimes one thinks of the kernel as the inclusion morphism from K into G, instead of as a group scheme in isolation.

Example 5.1.13. Let $\mathbb{G}_m$ be the multiplicative group scheme over $\mathbb{Z}$. Let $n \in \mathbb{Z}_{>0}$. Then we have an endomorphism $[n]\colon \mathbb{G}_m \to \mathbb{G}_m$ given in coordinates by $t \mapsto t^n$. Its kernel is called $\boldsymbol{\mu}_n$. As a scheme, $\boldsymbol{\mu}_n = \operatorname{Spec} \mathbb{Z}[t]/(t^n - 1)$. The multiplication is given by $(t, u) \mapsto tu$, as for $\mathbb{G}_m$. For any commutative ring R, the group $\boldsymbol{\mu}_n(R)$ is $\{r \in R : r^n = 1\}$ under multiplication.

Let G be a group scheme over a field k of characteristic p. Then the relative Frobenius morphism $F_{G/k}\colon G \to G^{(p)}$ is a homomorphism of group schemes over k. If G is the base change of a group scheme over $\mathbb{F}_p$, then $G^{(p)} \simeq G$, so $F_{G/k}$ can be viewed as an *endomorphism* of G, the **Frobenius endomorphism**.

Unofficial version for incidental online use

Example 5.1.14. Let k be a field of characteristic p. Let $\mathbb{G}_a$ be the additive group scheme over k. The Frobenius endomorphism $\mathbb{G}_a \to \mathbb{G}_a$ is described in coordinates by $t \mapsto t^p$. Its kernel is called $\boldsymbol{\alpha}_p$. As a scheme, $\boldsymbol{\alpha}_p = \operatorname{Spec} k[t]/(t^p)$. The "multiplication" is given by $(t,u) \mapsto t+u$. We have $\#\boldsymbol{\alpha}_p = p$. For any k-algebra R, the group $\boldsymbol{\alpha}_p(R)$ is $\{r \in R : r^p = 0\}$ under addition.

5.1.7. Quotients and cokernels.

Warning 5.1.15. The notions of quotient and cokernel are trickier to define, because even when A is a normal subgroup scheme of a group scheme B, the functor $T \mapsto B(T)/A(T)$ might not be representable.

Example 5.1.16. Let $\mathbb{G}_m$ be the multiplicative group scheme over $\mathbb{Q}$. The squaring map $\mathbb{G}_m \xrightarrow{2} \mathbb{G}_m$ is scheme-theoretically surjective, so it should be considered a surjective homomorphism, but it is certainly not true that every $q \in \mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^\times$ is in the image of $\mathbb{G}_m(\mathbb{Q}) \xrightarrow{2} \mathbb{G}_m(\mathbb{Q})$. What is true is that each $q \in \mathbb{G}_m(\mathbb{Q})$ is in the image of $\mathbb{G}_m(k) \xrightarrow{2} \mathbb{G}_m(k)$ for some finite extension $k \supseteq \mathbb{Q}$ depending on q. Similarly, we want to consider

$$1 \to \boldsymbol{\mu}_2 \to \mathbb{G}_m \xrightarrow{2} \mathbb{G}_m \to 1$$

to be exact, even though the resulting sequence of rational points is only left exact. One can show that the functor $T \mapsto \mathbb{G}_m(T)/\boldsymbol{\mu}_2(T)$ is not representable, but the quotient group scheme $\mathbb{G}_m/\boldsymbol{\mu}_2$ should be defined so that it is isomorphic to $\mathbb{G}_m$.

Important Remark 5.1.17. Over an arbitrary base scheme, fppf base extensions play the role of the finite extension of fields $k \supseteq \mathbb{Q}$ in Example 5.1.16.

Motivated by Example 5.1.16, we make the following definitions; we work in the context of **fppf group schemes** over S (i.e., group schemes G over S such that the structure morphism $G \to S$ is fppf).

Definition 5.1.18. A homomorphism $B \to C$ of fppf group schemes over S is **surjective** if for every S-scheme T and element $c \in C(T)$, there is an fppf morphism $T' \to T$ such that the image of c in $C(T')$ is the image of some $b \in B(T')$. Call a sequence of homomorphisms of fppf group schemes

$$A \xrightarrow{f} B \xrightarrow{g} C$$

exact (at B) if $g \circ f$ is the trivial homomorphism and the induced homomorphism $A \to \ker g$ is surjective. If A is the kernel of a surjective homomorphism of fppf group schemes $B \to C$, then define the **quotient** B/A to be C, and call B an **extension** of C by A; in this case,

$$1 \to A \to B \to C \to 1$$

Unofficial version for incidental online use

is exact. More generally, the **cokernel** of a homomorphism $A \to B$ of fppf group schemes is an fppf group scheme C equipped with a homomorphism $B \to C$ such that

$$A \to B \to C \to 1$$

is exact.

Warning 5.1.19. For a homomorphism of group schemes to be surjective, it is not enough that it induce a surjection on the underlying topological spaces. For example, over a field of characteristic p, the homomorphism from the trivial group scheme to $\boldsymbol{\mu}_p$ is not surjective.

Warning 5.1.20. As in Example 5.1.16, a surjective homomorphism need not induce a surjective map on rational points, and an exact sequence of S-group schemes need not induce an exact sequence of their groups of S-points. We will see in Chapter 6 that the obstruction can be measured by cohomology.

5.2. Fppf group schemes over a field

(References: [**Bor91**], [**PR94**], [**Spr98**])

Let k be a field. Flatness over k is automatic, and k is noetherian, so a k-scheme is fppf if and only if it is locally of finite type.

Definition 5.2.1. An **algebraic group** over a field k is a group scheme of finite type over k.

Warning 5.2.2. Some authors require also that the group scheme be *smooth* over k.

5.2.1. Connected component.

Definition 5.2.3. The **connected component** (or **identity component**) G^0 of an fppf group scheme G over a field k is the connected component of G containing the identity point 1.

Proposition 5.2.4. *If G is an fppf group scheme over k, then G^0 is a closed and open normal subgroup scheme of G. Moreover, G^0 is of finite type (an algebraic group) and is geometrically irreducible.*

Proof. If any two irreducible components of $G_{\overline{k}}$ intersected, then there would be some $\overline{k}$-points in the intersection of two such components, and some not, contradicting the fact that the group $G(\overline{k})$ acts transitively by translations on $G(\overline{k})$. Thus irreducible components of $G_{\overline{k}}$ are the same as connected components of $G_{\overline{k}}$. Since G^0 has a k-point 1, Proposition 2.3.24 shows that G^0 is geometrically connected, and hence geometrically irreducible by the

Unofficial version for incidental online use

previous sentence. In a scheme locally of finite type over a field, any connected component is open and closed, and any irreducible component is of finite type, so G^0 has these properties.

The proof of Proposition 2.3.24 shows that $G^0 \times G^0$ is connected, so the multiplication $m\colon G \times G \to G$ maps $G^0 \times G^0$ into the connected component containing $m(1,1) = 1$, which is G^0. Similarly, the inverse morphism $i\colon G \to G$ restricts to a morphism $G^0 \to G^0$, and $1 \in G^0(k)$. These make G^0 a subgroup scheme of G.

The conjugation action $G \times G \to G$ sending (g,h) to ghg^{-1} maps $\{g\} \times G^0$ into G^0 for every $g \in G(k)$, and the same holds after arbitrary field extension, so it maps $G \times G^0$ into G^0. In other words, G^0 is normal in G. $\square$

Because of Proposition 5.2.4, the theory of fppf group schemes over a field k is almost the same as the theory of algebraic groups over k.

5.2.2. Quotients.

Theorem 5.2.5 (Existence of quotient group schemes)**.** *If A is a closed normal subgroup scheme of an fppf group scheme B over a field k, then the closed immersion $A \to B$ fits in a uniquely determined exact sequence of fppf group schemes*

$$1 \to A \to B \to C \to 1.$$

Proof. This is a special case of [**SGA** $3_{\mathbf{I}}$, $\mathrm{VI_A}$ 3.2]. One constructs C by first constructing its functor of points h_C as the fppf sheafification (see Definition 6.3.21) of the functor $T \mapsto B(T)/A(T)$ on k-schemes. $\square$

Remark 5.2.6. One can generalize Theorem 5.2.5 to the case where the subgroup scheme A is not normal in B. Then the quotient $C := B/A$ is not a group scheme, but only a k-scheme with a left B-action, a left homogeneous space of B with a k-point; see Remark 5.12.7 for the definition of homogeneous space.

Proposition 5.2.7. *Let $1 \to A \to B \to C \to 1$ be an exact sequence of fppf group schemes over a field k. Then*

(a) (Properties inherited by quotients) *For any of the following properties, if B has it, so does C: connected, reduced, finite type, smooth, étale, unramified, finite, affine.*

(b) (Properties inherited by extensions) *Let* blah *be a property that is stable under composition, base extension, and fpqc descent* (*see Table 1 on pp. 302–303*)*. If A and C are blah (over k), so is B.*

Proof.

Unofficial version for incidental online use

(a) Any image of a connected space is connected. For reduced, see [**SGA** $3_{\mathbf{I}}$, VI_{B} 9.2(ix)]. For finite type, smooth, étale, unramified, and finite (which over a field is equivalent to quasi-finite), see [**SGA** $3_{\mathbf{I}}$, VI_{B} 9.2(xii)]. For affine, see [**SGA** $3_{\mathbf{I}}$, VI_{B} 11.7].

(b) The diagram

$$\begin{tikzcd}
A \arrow[d, "\text{blah}"'] & A \times B \arrow[l, "\mathrm{pr}_1"'] \arrow[r, "m"] \arrow[d, "\mathrm{pr}_2"] & B \arrow[d] \\
\operatorname{Spec} k & B \arrow[l] \arrow[r, "\text{fpqc}"] & C \arrow[d, "\text{blah}"] \\
 & & \operatorname{Spec} k
\end{tikzcd}$$

is cartesian (for the square on the right, check on T-valued points). If the first vertical arrow $A \to \operatorname{Spec} k$ is blah, then so are the second (base extension) and the third (fpqc descent). If $C \to \operatorname{Spec} k$ is blah too, then the composition $B \to C \to \operatorname{Spec} k$ is blah. □

Definition 5.2.8. Let G be an algebraic group. A **(finite) composition series** of G is a chain of subgroups

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

in which G_i is a closed normal subgroup scheme of G_{i+1} for $0 \leq i < n$. The groups G_{i+1}/G_i are called the **successive quotients** of the composition series.

5.2.3. Quotients and homomorphisms.

Theorem 5.2.9. *Let $f\colon G \to H$ be a homomorphism of algebraic groups. Then f factors into homomorphisms*

$$G \overset{q}{\twoheadrightarrow} \frac{G}{\ker f} \overset{i}{\hookrightarrow} H,$$

where q is the canonical quotient homomorphism, and i is a closed immersion.

Proof. See [**Gro62**, page 212-17, Corollary 7.4]. □

Corollary 5.2.10. *Let $f\colon G \to H$ be a homomorphism of algebraic groups. Then* $\ker f$ *is the trivial group scheme if and only if f is a closed immersion.*

Proof. If $\ker f$ is trivial, then f equals the closed immersion i in Theorem 5.2.9. Conversely, if f is a closed immersion, then $f\colon G(S) \to H(S)$ is injective for every k-scheme S, so $\ker f$ is trivial. □

Unofficial version for incidental online use

Definition 5.2.11. A homomorphism satisfying the equivalent conditions of Corollary 5.2.10 is called an **embedding** of algebraic groups.

Theorem 5.2.12. *The category of* commutative *algebraic groups over a field k (a full subcategory of the category of group schemes over k) is an* abelian *category.*

Proof. This is a consequence of Theorem 5.2.9; see [**SGA** $3_{\mathbf{I}}$, VI_{A} 5.4, Théorème]. ◻

5.2.4. Center, centralizer, and normalizer. Let k be a field. Let H be a subgroup scheme of an fppf group scheme G over k. Let S be a k-scheme. Let $g \in G(S)$. If T is an S-scheme and $g' \in G(T)$, we interpret $gg' \in G(T)$ by mapping g into $G(T)$ before multiplying. Say that g **centralizes** H if for every S-scheme T and every $h \in H(T)$, the identity $gh = hg$ holds in $G(T)$. Say that g **normalizes** H if for every S-scheme T and every $h \in H(T)$, we have $ghg^{-1} \in H(T)$. Let $C_G(H)$ be the functor sending a k-scheme S to $\{g \in G(S) : g \text{ centralizes } H\}$. Let $N_G(H)$ be the functor sending a k-scheme S to $\{g \in G(S) : g \text{ normalizes } H\}$.

Theorem 5.2.13. *The functors $C_G(H)$ and $N_G(H)$ are represented by closed subgroup schemes of G, called the* ***centralizer of** H **in** G and the **normalizer of** H **in** G.*

Proof. See [**SGA** $3_{\mathbf{II}}$, VIII.6.7]. ◻

The **center** of G is the closed subgroup scheme $Z := C_G(G)$.

Warning 5.2.14. The group $Z(k)$ might be smaller than the center of $G(k)$; see Exercise 5.1.

Remark 5.2.15. Because centralizers, normalizers, and centers are defined functorially, their formation automatically respects base field extension.

5.2.5. Smoothness.

Theorem 5.2.16. *For an fppf group scheme G over a field k, the following are equivalent:*

(i) *G is smooth over k.*

(ii) *G is geometrically reduced.*

(iii) *The local ring of $G_{\overline{k}}$ at the identity is reduced.*

(iv) *Either* $\operatorname{char} k = 0$, *or* $\operatorname{char} k = p > 0$ *and $F_{G/k} \colon G \to G^{(p)}$ is surjective.*

Unofficial version for incidental online use

Proof. None of the conditions are affected by base field extension, so assume that k is algebraically closed.

(i)⇒(ii): Smooth implies reduced by Proposition 3.5.51(i).

(ii)⇒(iii): Trivial.

(iii)⇒(ii): Translating by elements of $G(k)$ shows that the local ring of G at *each* k-point is reduced. For algebraically closed k, this implies that G is reduced.

(ii)⇒(i): By Proposition 3.5.64, the smooth locus is open and dense. In particular, G is smooth at some k-point. By translation, G is smooth at every k-point. Since k is algebraically closed, the only open subscheme of G containing $G(k)$ is G itself.

(i)⇔(iv): See [**SGA** $3_{\mathbf{I}}$, $\mathrm{VII_A}$ 8.3.1]. □

Remark 5.2.17. In (iv), one could replace the relative p-power Frobenius morphism by the relative q-power Frobenius morphism for any power q of p.

Corollary 5.2.18 (Cartier)**.** *Every fppf group scheme over a field of characteristic* 0 *is smooth.*

More generally:

Proposition 5.2.19. *Any fppf group scheme G over a field k is an extension of a smooth group scheme by a finite group scheme.*

Sketch of proof. If $\operatorname{char} k = 0$, the result follows from Corollary 5.2.18. Therefore, assume that $\operatorname{char} k = p > 0$. Let $F_n \colon G \to G^{(p^n)}$ denote the relative p^n-power Frobenius morphism, which is a homomorphism. Then the group scheme $\ker F_n$ is finite, and one shows that $G/\ker F_n$ is smooth for sufficiently large n: for G is of finite type, this is [**SGA** $3_{\mathbf{I}}$, $\mathrm{VII_A}$ 8.3], and in general one may replace G by its connected component G^0, which is of finite type by Proposition 5.2.4. □

5.2.6. Quasi-projectivity.

Theorem 5.2.20. *Every algebraic group over a field k is quasi-projective.*

Proof. Chow proved that *smooth* algebraic groups (and even their homogeneous spaces) are quasi-projective [**Cho57**]. This can be extended to arbitrary algebraic groups G by using Proposition 5.2.19; see [**Con02**, Corollary 1.2]. □

Because of Theorem 5.2.20, fpqc descent involving algebraic groups is automatically effective.

Unofficial version for incidental online use

5.3. Affine algebraic groups

An algebraic group whose underlying scheme is affine is also called a **linear algebraic group**, because of the following.

Theorem 5.3.1. *An algebraic group G is affine if and only if it embeds in GL_n for some $n \geq 0$.*

Proof. Since GL_n itself is affine, any closed subgroup of GL_n is affine.

Conversely, suppose that G is affine, say $G = \operatorname{Spec} A$. Let A^* be the space of k-linear functionals $A \to k$. Below, fiber products and tensor products are over k. For any k-vector space V and k-algebra R, let $V_R = V \otimes R$. The proof will proceed in three steps.

1. *Find a finite-type affine k-scheme $X = \operatorname{Spec} B$ with a faithful right G-action.* Let X be G with the right translation action. For later use, note that we have the translation action of $G(k)$ on A and B, and the induced action on A^*.
2. *Show that each $b \in B$ is contained in a finite-dimensional G-invariant subspace $V \subseteq B$; here "G-invariant" means that for each k-algebra R, the $G(R)$-action on B_R preserves V_R.* The action morphism $X \times G \to X$ corresponds to a homomorphism $B \to A \otimes B$, which induces $A^* \otimes B \to B$. Let V be the image of the composition

$$A^* \xrightarrow{\otimes b} A^* \otimes B \longrightarrow B. \tag{5.3.2}$$

   Let each $g \in G(k)$ act as $g \otimes 1$ on $A \otimes B$ and $A^* \otimes B$. The associative axiom for the G-action on X shows that $B \to A \otimes B$ is $G(k)$-equivariant, so the maps in (5.3.2) are $G(k)$-equivariant. Thus V is $G(k)$-invariant. The construction of V respects base change to any k-algebra R, and the same argument shows that V_R is $G(R)$-invariant.

   The identity in $G(k)$ is a k-morphism $\operatorname{Spec} k \to G$, so it corresponds to a k-algebra homomorphism $A \to k$, which may be viewed as an element of A^*. It is mapped by (5.3.2) to b. Thus $b \in V$.

   Concretely, if $B \to A \otimes B$ maps b to $\sum a_i \otimes b_i$, where the a_i are chosen to be k-independent, then V is the k-span of the b_i, so V is finite-dimensional.
3. *Find a finite-dimensional subspace $W \subseteq B$ such that $G(R)$ acts faithfully on W_R for all R.* Let B_0 be a finite set of generators for B as a k-algebra. For each $b \in B_0$, construct a $V = V_b$ as in step 2, and let W be their sum. If $g \in G(R)$ acts trivially on W_R, then g acts trivially on B_0 and on the R-algebra B_R it generates, but G acts faithfully on X, so $g = 1$.

Yoneda's lemma now produces a homomorphism $G \to \mathrm{GL}_{\dim W}$. By Corollary 5.2.10, it is an embedding. $\square$

Unofficial version for incidental online use

Remark 5.3.3. It is not known whether affine finite-type group schemes over $k[\epsilon]/(\epsilon^2)$ embed in GL_n over that ring.

5.4. Unipotent groups

5.4.1. Powers of the additive group. Algebraic groups isomorphic to $\mathbb{G}_a^n := (\mathbb{G}_a)^n$ for some $n \in \mathbb{N}$ are sometimes called **vector groups** or **vectorial groups**.

Proposition 5.4.1. *If k is a field of characteristic 0, then $\mathbb{G}_a^n$ as an algebraic group has no nontrivial twists.*

Proof. An endomorphism of $\mathbb{G}_a$ is a polynomial map $t \mapsto f(t)$ such that the polynomial $f \in k[t]$ satisfies $f(t+u) = f(t)+f(u)$ in $k[t,u]$. Since $\operatorname{char} k = 0$, the binomial theorem shows that the only such f are the homogeneous linear polynomials. In other words, $\operatorname{End} \mathbb{G}_a = k$. Similarly, $\operatorname{End} \mathbb{G}_{a,k_\mathrm{s}} = k_\mathrm{s}$. Thus $\operatorname{End} \mathbb{G}_{a,k_\mathrm{s}}^n = \mathrm{M}_n(k_\mathrm{s})$, and $\operatorname{Aut} \mathbb{G}_{a,k_\mathrm{s}}^n = (\mathrm{M}_n(k_\mathrm{s}))^\times = \mathrm{GL}_n(k_\mathrm{s})$. Finally, $\mathrm{H}^1(\mathfrak{G}_k, \mathrm{GL}_n(k_\mathrm{s})) = 0$ by Remark 1.3.16. $\square$

Remark 5.4.2. A more difficult argument shows that Proposition 5.4.1 holds also for fields of characteristic $p > 0$. This follows from [**KMT74**, Theorem 1.5.1, proof of Lemma 2.1.1].

Warning 5.4.3. There exists an *inseparable* extension of fields $L \supseteq k$ and an algebraic group $G \not\simeq \mathbb{G}_a$ over k such that $G_L \simeq \mathbb{G}_{a,L}$; see Exercise 5.4 and [**Rus70**]. More generally, [**KMT74**, Section 2.6] classifies, over any field k, all algebraic groups over k that become isomorphic to $\mathbb{G}_a^n$ after base extension to $\overline{k}$.

5.4.2. Unipotent elements.

Definition 5.4.4. Let k be a field. An element u of $\mathrm{GL}_n(k)$ is called **unipotent** if it satisfies one of the following equivalent conditions:

- The eigenvalues of u are all 1.
- One has $(u-1)^n = 0$.
- The element u is conjugate in $\mathrm{GL}_n(k)$ to a matrix in $\mathrm{U}_n(k)$.

More generally, if G is an affine algebraic group, an element $u \in G(\overline{k})$ is called **unipotent** if for every n and every homomorphism $G_{\overline{k}} \to (\mathrm{GL}_n)_{\overline{k}}$, the image of u in $\mathrm{GL}_n(\overline{k})$ is unipotent.

Remark 5.4.5. To check that an element $u \in G(\overline{k})$ is unipotent, it suffices to check that its image under any *one* embedding $G_{\overline{k}} \hookrightarrow (\mathrm{GL}_n)_{\overline{k}}$ is unipotent. This follows from the "multiplicative Jordan decomposition"; see [**Spr98**, Theorem 2.4.8 and Corollary 2.4.9].

Unofficial version for incidental online use

5.4.3. Unipotent groups.

Definition 5.4.6. Let G be an algebraic group over k. Then G is called **unipotent** if $G_{\overline{k}}$ admits a composition series in which each successive quotient is isomorphic to a closed subgroup of $\mathbb{G}_{a,\overline{k}}$.

Examples 5.4.7.

(i) Any power of $\mathbb{G}_a$ is unipotent.

(ii) For each $n \geq 0$, the algebraic group U_n in Section 5.1.5 is unipotent.

(iii) If $\operatorname{char} k = p > 0$, then the constant group scheme $\mathbb{Z}/p\mathbb{Z}$ is unipotent.

(iv) If $\operatorname{char} k = p > 0$, then $\boldsymbol{\alpha}_p$ is unipotent.

(v) Suppose that $\operatorname{char} k = p$. For $n \geq 0$, there is a connected algebraic group (even a ring scheme) W_n over $\mathbb{F}_p$ such that for each $\mathbb{F}_p$-algebra A, the group $\mathrm{W}_n(A)$ is the additive group of length-n Witt vectors with coordinates in A; see [**Ser79**, p. 44]. It is unipotent by induction on n: there is a surjective homomorphism $\mathrm{W}_{n+1} \to \mathrm{W}_n$ with kernel isomorphic to $\mathbb{G}_a$ (not surprising, given that there is a surjective homomorphism $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ with kernel isomorphic to $\mathbb{F}_p$ as an abelian group).

Theorem 5.4.8 (Characterizations of unipotent groups)**.** *The following three conditions are equivalent for an algebraic group G over a field k:*

(i) *The group G is unipotent.*

(ii) *There is an embedding of G in U_n for some $n \geq 0$.*

(iii) *The group G admits a composition series (over k) such that*
   (a) *if $\operatorname{char} k = 0$, then each successive quotient is $\mathbb{G}_a$; and*
   (b) *if $\operatorname{char} k = p$, then each successive quotient is one of $\boldsymbol{\alpha}_p$, $\mathbb{G}_a$, or a twist of $(\mathbb{Z}/p\mathbb{Z})^n$ for some $n \geq 1$.*

These conditions imply

(iv) *Every element of $G(\overline{k})$ is unipotent in the sense of Definition 5.4.4.*

If G is smooth, then all four conditions are equivalent.

Proof.

(i)$\Leftrightarrow$(ii)$\Leftrightarrow$(iii): See [**SGA 3$_{\mathbf{II}}$**, XVII, Théorème 3.5(i, ii, v)]. Stronger statements about the composition series are available in [**SGA 3$_{\mathbf{II}}$**, XVII, Théorème 3.5(iii, iv)]. A standard specialization argument [**SGA 3$_{\mathbf{II}}$**, XVII, Proposition 1.2] shows that unipotence is unchanged by extension of the ground field, so we now know that (iii) and (iv) are unchanged as well.

(iii)$\Rightarrow$(iv): If $g \in G(\overline{k}) \leq \mathrm{U}_n(\overline{k})$, then g is unipotent by Remark 5.4.5.

(iv)$\Rightarrow$(iii) for smooth G: Since both (ii) and (iii) are unchanged by base extension from k to $\overline{k}$, we may assume that k is algebraically closed. Now see

Unofficial version for incidental online use

[**Spr98**, Proposition 2.4.12] (which applies only to smooth algebraic groups over an algebraically closed field). □

Warning 5.4.9. Condition (iv) does not necessarily imply the others if G is not smooth. For example, suppose that G is $\boldsymbol{\mu}_p$ over a field k of characteristic $p > 0$. Then $G(\overline{k}) = \{1\}$, so (iv) holds. But G is a group scheme of prime order, so G is simple, and therefore G violates (iii).

Proposition 5.4.10. *If* $\operatorname{char} k = 0$ *and* G *is a commutative unipotent group over* k*, then* $G \simeq \mathbb{G}_a^n$ *for some* $n \geq 0$*.*

Sketch of proof. First of all, G must be connected, since otherwise it would have a nontrivial finite quotient embedding in some GL_n, and the elements of the image over $\overline{k}$ would not be unipotent.

Let $\operatorname{Lie} G$ be the power of $\mathbb{G}_a$ corresponding to the tangent space of G at the origin. For a unipotent group $G \leq \mathrm{U}_n$, the exponential map gives an isomorphism $\operatorname{Lie} G \to G$ of varieties, the inverse being given by

$$1 + u \longmapsto \log(1 + u) := u - \frac{u^2}{2} + \frac{u^3}{3} - \cdots ,$$

which is a finite series for any nilpotent matrix u. If G is also commutative, then the exponential map and its inverse are also homomorphisms of group schemes. □

Warning 5.4.11. The hypothesis "commutative" in Proposition 5.4.10 is necessary: consider U_3.

Warning 5.4.12. The hypothesis "$\operatorname{char} k = 0$" in Proposition 5.4.10 is necessary too. For example, the constant group scheme $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{F}_p$ is a counterexample: it embeds in $\mathbb{G}_a \simeq \mathrm{U}_2$, so it is unipotent. One can also give a connected counterexample: the underlying variety of the Witt group scheme W_n is $\mathbb{A}^n$, but if $n \geq 2$, then W_n is not isomorphic to $\mathbb{G}_a^n$ since the group $\mathrm{W}_n(\mathbb{F}_p) \simeq \mathbb{Z}/p^n\mathbb{Z}$ is not killed by p.

Trying to classify all unipotent groups up to isomorphism is like trying to classify finite p-groups: hopeless.

5.5. Tori

(Reference: [**Spr98**, §3.2])

5.5.1. Homomorphisms between powers of the multiplicative group.

Unofficial version for incidental online use

Lemma 5.5.1. *Consider the multiplicative group scheme* $\mathbb{G}_m = \operatorname{Spec} k[t,t^{-1}]$ *over a field* k. *We have*

$$\operatorname{End}\mathbb{G}_m \simeq \mathbb{Z}, \quad \operatorname{Hom}(\mathbb{G}_m^n, \mathbb{G}_m^p) \simeq \mathrm{M}_{p\times n}(\mathbb{Z}), \quad \operatorname{Aut}\mathbb{G}_m^n \simeq \mathrm{GL}_n(\mathbb{Z}),$$

computed in the category of k*-group schemes.*

Proof. An endomorphism of $\mathbb{G}_m$ is given by $t \mapsto f(t)$, where $f \in k[t,t^{-1}]^\times$ satisfies $f(tu) = f(t)f(u)$ in $k[t,t^{-1},u,u^{-1}]$ (respecting the comultiplications amounts to this identity). Elements of $k[t,t^{-1}]^\times$ are monomials, and the only ones satisfying $f(tu) = f(t)f(u)$ are $f(t) = t^n$ for some $n \in \mathbb{Z}$. Thus $\operatorname{End}\mathbb{G}_m \simeq \mathbb{Z}$. The other two claims follow from this: in particular, the unit group of $\mathrm{M}_n(\mathbb{Z})$ is $\mathrm{GL}_n(\mathbb{Z})$. □

5.5.2. Tori.

Definition 5.5.2. Let k be a field. A **torus** over k is a twist of $\mathbb{G}_m^n$ (as a group scheme) for some $n \in \mathbb{N}$. It is called a **split torus** if it is actually *isomorphic* to $\mathbb{G}_m^n$.

Example 5.5.3. Let T be the affine variety $x^2+2y^2 = 1$ in $\mathbb{A}^2_{\mathbb{Q}}$. We secretly think of a point (x,y) on T as representing $x + y\sqrt{-2}$ and hence define

$$\begin{aligned} m\colon T \times T &\longrightarrow T \\ (x_1,y_1),(x_2,y_2) &\longmapsto (x_1x_2 - 2y_1y_2, x_1y_2 + y_1x_2). \end{aligned}$$

Then one can show that T is a nonsplit 1-dimensional torus over $\mathbb{Q}$.

Example 5.5.4. If $L \supseteq k$ is a finite separable extension of fields and T is a torus over L, then the restriction of scalars $\operatorname{Res}_{L/k} T$ is a torus over k.

Example 5.5.5. If $L \supseteq k$ is a finite separable extension of fields, then the norm homomorphism $L^\times \to k^\times$ is the map on k-points of a homomorphism of tori $\operatorname{Res}_{L/k}\mathbb{G}_m \xrightarrow{N} \mathbb{G}_m$. The kernel of N is a torus $\operatorname{Res}^1_{L/k}\mathbb{G}_m$ of dimension $[L:k]-1$ over k. For example, $\operatorname{Res}^1_{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}\mathbb{G}_m$ is the torus T in Example 5.5.3.

5.5.3. Character groups.

Definition 5.5.6. The **character group** of a k-torus T is the $\mathfrak{G}_k$-module

$$\mathrm{X}(T) := \operatorname{Hom}_{k_{\mathrm{s}}\text{-group schemes}}\left(T_{k_{\mathrm{s}}}, \mathbb{G}_{m,k_{\mathrm{s}}}\right).$$

If T is an n-dimensional torus, then Lemma 5.5.1 implies that $\mathrm{X}(T)$ stripped of its $\mathfrak{G}_k$-action is a free abelian group of rank n.

5.5.4. Classification of tori.

Unofficial version for incidental online use

Theorem 5.5.7. *The functor*

$$\begin{array}{ccc} \{\text{tori}/k\} & \longleftrightarrow & \{\mathfrak{G}_k\text{-modules that are free of finite rank over } \mathbb{Z}\}^{\text{opp}} \\ T & \longmapsto & \mathrm{X}(T) \end{array}$$

is an equivalence of categories.

Proof. If $k = k_{\mathrm{s}}$, then the $\mathfrak{G}_k$-action is irrelevant, and the result follows from Lemma 5.5.1. For arbitrary k, equipping a finite-rank free $\mathbb{Z}$-module with a $\mathfrak{G}_k$-action corresponds to equipping a corresponding torus over k_{s} with a descent datum as in Proposition 4.4.4(i), since $\mathfrak{G}_k$ acts trivially on $\operatorname{Aut} \mathbb{G}^n_{m,k_{\mathrm{s}}} \simeq \mathrm{GL}_n(\mathbb{Z})$, so the result for k follows from the result from k_{s}. (Strictly speaking, Proposition 4.4.4(i) is for a finite Galois extension, so it would be better to proceed as in the proof of Theorem 4.5.2 by first showing that k-tori which split over a fixed finite Galois extension k' are classified by $\mathrm{Gal}(k'/k)$-modules that are free of finite rank, and then taking a direct limit.) □

Remark 5.5.8. Here is another way of thinking about Theorem 5.5.7: Theorem 4.5.2 gives a bijection

$$\begin{aligned} &\{n\text{-dimensional tori}/k\} \\ &= \{\text{twists of } \mathbb{G}_m^n\} \\ &= \mathrm{H}^1\left(\mathfrak{G}_k, \operatorname{Aut} \mathbb{G}^n_{m,k_{\mathrm{s}}}\right) \\ &= \mathrm{H}^1(\mathfrak{G}_k, \mathrm{GL}_n(\mathbb{Z})) \quad (\text{where } \mathfrak{G}_k \text{ acts trivially on } \mathrm{GL}_n(\mathbb{Z})) \\ &= \mathrm{Hom}_{\mathrm{conts}}(\mathfrak{G}_k, \mathrm{GL}_n(\mathbb{Z}))/\text{conjugacy} \\ &= \{\mathfrak{G}_k\text{-modules that are free of rank } n \text{ over } \mathbb{Z}\}, \end{aligned}$$

where each set is really a set of isomorphism classes.

5.5.5. Rationality. Whether a given n-dimensional torus T is k-rational (i.e., birational to projective space over k) is a subtle question. By enumerating the possibilities for the action of $\mathfrak{G}_k$ on the character group, Voskresenskii proved that if $n \leq 2$, then T is k-rational [**Vos67**]. On the other hand, Chevalley showed that there is a 3-dimensional torus over $\mathbb{Q}_p$ that is not $\mathbb{Q}_p$-rational, namely $\mathrm{Res}^1_{K/\mathbb{Q}_p} \mathbb{G}_m$ for any Galois extension $K/\mathbb{Q}_p$ with $\mathrm{Gal}(K/\mathbb{Q}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ [**Che54**, §5].

5.5.6. Groups of multiplicative type. The additive category of tori is not an abelian category because, for instance, the squaring homomorphism $\mathbb{G}_m \xrightarrow{2} \mathbb{G}_m$ is an epimorphism that is not a cokernel of any homomorphism $T \to \mathbb{G}_m$. This motivates enlarging the category slightly.

Definition 5.5.9. A **group of multiplicative type** over k is an algebraic group G that after base extension to k_{s} is isomorphic to a product of groups

Unofficial version for incidental online use

each isomorphic to either $\mathbb{G}_m$ or $\boldsymbol{\mu}_n$ for some n. (Some authors extend the notion also to group schemes that are not of finite type.)

Groups of multiplicative type *do* form an abelian category; see [**SGA** $3_{\mathbf{II}}$, IX, Corollaire 2.8] for a generalization. Moreover, one can define the character group $\mathrm{X}(G)$ as for tori, and there is a generalization of the classification theorem (Theorem 5.5.7):

Theorem 5.5.10. *The functor*

$$\begin{aligned}\{\text{groups of multiplicative type}/k\} &\leftrightarrow \left\{\begin{matrix}\mathfrak{G}_k\text{-modules that are}\\ \text{finitely generated as } \mathbb{Z}\text{-modules}\end{matrix}\right\}^{\mathrm{opp}}\\ G &\mapsto \mathrm{X}(G)\end{aligned}$$

is an equivalence of abelian categories.

Proof. See [**SGA** $3_{\mathbf{II}}$, X, Proposition 1.4]. □

Corollary 5.5.11. *Each group G of multiplicative type contains a unique maximal torus T of the same dimension.*

Proof. Theorem 5.5.10 translates this into a statement about character groups. The torus T is the one for which $\mathrm{X}(T) = \mathrm{X}(G)/\mathrm{X}(G)_{\mathrm{tors}}$. □

Over a separably closed field, groups of multiplicative type are exactly the algebraic groups that for some n embed into the torus in GL_n consisting of diagonal matrices.

5.5.7. Maximal tori. Every algebraic group G contains a maximal torus T (usually not normal in G); moreover, any such T remains maximal after base field extension. Call G **split** if G contains a split maximal torus.

5.6. Semisimple and reductive algebraic groups

(Reference: [**Kne67**])

5.6.1. Radical and unipotent radical.

Definition 5.6.1. The **commutator subgroup** $[G, G]$ of an algebraic group is the intersection of all algebraic subgroups containing the (scheme-theoretic) image of the morphism $G \times G \to G$ sending $g, h \in G(T)$ to $ghg^{-1}h^{-1} \in G(T)$ for each k-scheme T.

Definition 5.6.2. Let G be a smooth affine algebraic group. The **derived series** of G is the sequence of algebraic subgroups

$$G = G^0 \rhd G^1 \rhd G^2 \rhd \cdots ,$$

Unofficial version for incidental online use

each normal in the preceding one, defined by $G^0 := G$ and $G^{i+1} := [G^i, G^i]$ for $i \geq 0$. Call G **solvable** if G^n is trivial for some n. (It turns out that this condition is equivalent to solvability of the abstract group $G(K)$ for any algebraically closed field K containing k [**SGA** $3_{\mathbf{I}}$, $\mathrm{VI_B}$ 8.3(i)$\Leftrightarrow$(iii)].)

Let G be a smooth affine algebraic group. One can show that G contains a unique maximal smooth connected solvable *normal* subgroup $\mathscr{R}(G)$, called the **radical** of G. Also, G contains a unique maximal smooth connected unipotent *normal* subgroup $\mathscr{R}_u(G)$, called the **unipotent radical** of G.

Remark 5.6.3 (Radicals under field extension)**.** For any field extension $L \supseteq k$, by definition $\mathscr{R}(G)_L \subseteq \mathscr{R}(G_L)$. If L is a separable algebraic extension of k, then descent theory shows that equality holds. On the other hand, equality sometimes fails if L is inseparable over k. Analogous statements hold for the unipotent radical $\mathscr{R}_u(G)$.

5.6.2. Semisimple and reductive groups.

Definition 5.6.4. Let G be a smooth affine algebraic group over a field k. Call G **semisimple** if $\mathscr{R}(G_{\overline{k}}) = \{1\}$. Call G **reductive** if $\mathscr{R}_u(G_{\overline{k}}) = \{1\}$.

Warning 5.6.5. Many authors also require a semisimple or reductive group to be connected.

Warning 5.6.6. Definition 5.6.4 uses the *geometric* radicals, i.e., the radical or unipotent radical of $G_{\overline{k}}$ instead of G. Remark 5.6.3 shows that this makes no difference if k is perfect. But if k is imperfect, it matters; see Section 5.9.3.

By Theorem 5.4.8, smooth connected unipotent groups are solvable, so the unipotent radical is contained in the radical. In particular, semisimple groups are reductive.

Example 5.6.7. The algebraic group SL_n is semisimple.

Example 5.6.8. The algebraic group GL_n is reductive but not semisimple. Its radical is a copy of $\mathbb{G}_m$, consisting of the scalar multiples of the identity.

Remark 5.6.9. Although GL_n contains nontrivial smooth connected unipotent subgroups (e.g., U_n), they are not normal. Similarly, SL_n contains nontrivial smooth connected solvable subgroups (e.g., the torus consisting of diagonal matrices of determinant 1), but they are not normal.

5.6.3. Center of a reductive group.

Theorem 5.6.10. *The center of a connected reductive group is a group of multiplicative type.*

Unofficial version for incidental online use

Sketch of proof. Let G be a connected reductive group over k. For any maximal torus $T \leq G$, we have $C_G(T) = T$ [**SGA** $3_{\mathbf{III}}$, XIX, 2.8]. The center Z of G is a closed subgroup of $C_G(T) = T$, so Z is of multiplicative type. □

Corollary 5.6.11. *The center of a connected semisimple group is a* finite *group of multiplicative type.*

Proof. Let G be a connected semisimple group. Let Z be its center. By Theorem 5.6.10, Z is a group of multiplicative type. Let T be the maximal torus in Z given by Corollary 5.5.11. Since $T \subseteq Z$, the group T is normal in G, so $T \subseteq \mathscr{R}(G) = \{1\}$, since G is semisimple. Hence $T = \{1\}$. Now $\dim Z = \dim T = 0$, so Z is finite. □

Example 5.6.12. The center of the reductive group GL_n is $\mathbb{G}_m$.

Example 5.6.13. The center of the semisimple group SL_n is $\boldsymbol{\mu}_n$.

5.6.4. Isogenies. An **isogeny** between connected algebraic groups is a surjective homomorphism $G \to H$ whose kernel is finite. If the kernel of an isogeny is (scheme-theoretically) contained in the center of G, then it is called a **central isogeny**, and G is called a **central cover** of H.

Example 5.6.14. Let $n \geq 1$. The inclusion $\mathrm{SL}_n \hookrightarrow \mathrm{GL}_n$ is not surjective, so it is not an isogeny. The projection $\mathrm{GL}_n \twoheadrightarrow \mathrm{PGL}_n$ has a kernel that is not finite, so it is not an isogeny. But their composition $\mathrm{SL}_n \to \mathrm{PGL}_n$ is a central isogeny with kernel $\boldsymbol{\mu}_n$.

Proposition 5.6.15. *Every isogeny whose kernel is étale is central. In particular, every isogeny over a field of characteristic* 0 *is central.*

Proof. Let $f \colon G \to H$ be an isogeny with étale kernel K. We may assume that k is algebraically closed, so K consists of a finite disjoint union of points (Proposition 3.5.35). The conjugation action of G on K defines a homomorphism from G to a finite group $\operatorname{Aut} K$, but G is connected, so this homomorphism must be trivial. In other words, K is contained in the center of G. □

Example 5.6.16. If G is a smooth connected algebraic group over a field k of characteristic $p > 0$, then the relative Frobenius morphism $F_{G/k} \colon G \to G^{(p)}$ is an isogeny, but not necessarily a central isogeny.

5.6.5. Simply connected and adjoint groups. Call a central cover $G' \xrightarrow{f} G$ trivial if f is an isomorphism.

Definition 5.6.17. A connected semisimple group G is called **simply connected** if G has no nontrivial central cover.

Unofficial version for incidental online use

Warning 5.6.18. Let G be a connected semisimple group over a separably closed field k. If $\operatorname{char} k = 0$, then G is simply connected in the sense of Definition 5.6.17 if and only if G is algebraically simply connected in the sense of Definition 3.5.45. But if $\operatorname{char} k = p > 0$, the notion of simply connected is more restrictive. For example, PGL_p is algebraically simply connected but not simply connected: it has no nontrivial finite étale cover, but $\mathrm{SL}_p \to \mathrm{PGL}_p$ is a nontrivial central cover with kernel $\boldsymbol{\mu}_p$.

Proposition 5.6.19. *Let G be a connected semisimple group. Then the following are equivalent:*

(i) *The group G is not a nontrivial central cover of any other group G'.*

(ii) *The center Z of G is trivial.*

Proof. If $G \xrightarrow{f} G'$ is a nontrivial central cover, then $\{1\} \neq \ker f \subseteq Z$, so Z is nontrivial. Conversely, if Z is nontrivial, then $G \to G/Z$ is a nontrivial central cover. $\square$

Definition 5.6.20. A connected semisimple group G is called **adjoint** if it satisfies the conditions of Proposition 5.6.19.

Proposition 5.6.21. *Let G be a connected semisimple group.*

(a) *Among all connected semisimple groups that centrally cover G, there is a maximal one $\widetilde{G}$ that centrally covers all others. This $\widetilde{G}$ is unique up to isomorphism (as a group equipped with a central isogeny to G) and is simply connected.*

(b) *Among all connected semisimple groups that G centrally covers, there is a minimal one G^{ad} that is centrally covered by all others. This G^{ad} is unique up to isomorphism (as a group equipped with a central isogeny from G to it) and is adjoint. If Z is the center of G, then $G^{\mathrm{ad}} \simeq G/Z$.*

The formation of $\widetilde{G}$ and G^{ad} commutes with base field extension.

Proof.

(a) See [**CGP10**, Corollary A.4.11].

(b) By Corollary 5.6.11, Z is a finite group of multiplicative type, so the connected semisimple groups centrally covered by G are the quotients G/Z' for $Z' \leq Z$. In particular, G/Z is the minimal such quotient. By [**SGA 3$_{\mathbf{III}}$**, XXII, Proposition 4.3.5], the center of G/Z is trivial. $\square$

Unofficial version for incidental online use

$$\begin{tikzcd} & \widetilde{G} \arrow[dl, dotted] \arrow[d] \arrow[dr, dotted] & & \text{simply connected} & \mathrm{SL}_n \arrow[dd, "\text{central isogeny with kernel } \boldsymbol{\mu}_n"] \\ {} \arrow[dr, dotted] & G \arrow[d] & {} \arrow[dl, dotted] & & \\ & G^{\mathrm{ad}} & & \text{adjoint} & \mathrm{PGL}_n \end{tikzcd}$$

Example 5.6.22. The connected semisimple group SL_n is simply connected. Its center is $\boldsymbol{\mu}_n$, and the quotient $(\mathrm{SL}_n)^{\mathrm{ad}} = \mathrm{SL}_n / \boldsymbol{\mu}_n$ is isomorphic to the adjoint group PGL_n.

Corollary 5.6.23. *For a connected semisimple group, the properties of being simply connected or adjoint are unchanged by base field extension.*

Remark 5.6.24. Let us explain how the use of the word "adjoint" here relates to other uses of the word. Each $g \in G(k)$ induces an automorphism $x \mapsto gxg^{-1}$ of G, which in turn induces an automorphism of its Lie algebra $\mathfrak{g}$. This construction works with S-valued points as well as k-valued points, so we get a homomorphism of algebraic groups $\mathrm{Ad}\colon G \to \mathrm{GL}(\mathfrak{g})$, called the **adjoint homomorphism**. The kernel of Ad turns out to be the center Z of G, so the image G^{ad} of Ad is isomorphic to G/Z.

Because of Proposition 5.6.21(a), to classify all connected semisimple groups, it suffices to classify the simply connected semisimple groups G; then for each such G compute the center Z, compute the finitely many subgroup schemes $Z' \subseteq Z$, and consider the quotients G/Z'.

5.6.6. Almost simple groups. A **simple** algebraic group is a connected semisimple group G that has exactly two normal subgroup schemes, $\{1\}$ and G. If k is an algebraically closed field of characteristic 0, then an algebraic group G is simple if and only if the abstract group $G(k)$ is simple.

It is not true that every connected semisimple group is a product of simple groups. For example, if $n \geq 2$, then SL_n is not simple (it has $\boldsymbol{\mu}_n$ as a normal subgroup scheme), but it is not a nontrivial product either. Therefore we define a less restrictive concept: an **almost simple** algebraic group is a connected semisimple group G such that the quotient G/Z of G by its center Z is simple. (Recall that Z is finite; see Corollary 5.6.11.)

Remark 5.6.25. What we call "simple" is what other authors might call "k-simple": the notion is relative to the ground field, and might be lost if the base field is extended. The same applies to "almost simple".

Unofficial version for incidental online use

Theorem 5.6.26 (Classification of almost simple groups)**.** *Fix a separably closed field k. Almost simple groups over k up to the equivalence relation generated by central isogenies are in bijection with connected Dynkin diagrams. In particular, for each connected Dynkin diagram $\mathcal{D}$, there is one simply connected group and one adjoint group of type $\mathcal{D}$.*

Call G **geometrically almost simple** (or **absolutely almost simple**) if G_{k_s} is almost simple. For each field k, let $\mathscr{S}(k)$ be the set of isomorphism classes of split geometrically almost simple simply connected groups over k.

Theorem 5.6.27. *For any field extension $L \supseteq k$, the map $\mathscr{S}(k) \to \mathscr{S}(L)$ is a bijection.*

Thus among geometrically almost simple simply connected groups over k of a given type $\mathcal{D}$, there is exactly one that is split, and all others are twists of that one.

5.6.7. Decomposition of a semisimple group.

Theorem 5.6.28. *Every simply connected semisimple group is uniquely expressible as a product of almost simple groups.*

By taking the quotients by the centers, we find that every adjoint semisimple group is uniquely expressible as a product of adjoint simple groups.

Example 5.6.29. For $n > 1$, embed $\boldsymbol{\mu}_n$ diagonally in $\mathrm{SL}_n \times \mathrm{SL}_n$, and let $G = (\mathrm{SL}_n \times \mathrm{SL}_n)/\boldsymbol{\mu}_n$. Then G is not a product of almost simple groups, but $\widetilde{G} = \mathrm{SL}_n \times \mathrm{SL}_n$, and $G^{\mathrm{ad}} = \mathrm{PGL}_n \times \mathrm{PGL}_n$.

Decompositions over k and over k_s are related, as we now explain. Let G be a simply connected semisimple group over k. Write $G_{k_s} = \prod_{i \in I} G_i$ for some almost simple groups G_i over k_s. The Galois group $\mathfrak{G}_k$ acts on G_{k_s} and hence also on I. For each $i \in I$, the stabilizer of i is $G_{L_i} \le \mathfrak{G}_k$ for some finite separable extension $L_i \supseteq k$ contained in k_s, and G_i descends to an algebraic group H_i over L_i. For each $\mathfrak{G}_k$-orbit $J \subseteq I$, the product $\prod_{i \in J} G_i$ descends to an almost simple group G_J over k. Thus the decomposition of G over k corresponds to the decomposition of I into $\mathfrak{G}_k$-orbits. Finally, if $i \in J$, then $G_J \simeq \operatorname{Res}_{L_i/k} H_i$. Thus the classification of simply connected groups reduces to the classification of *geometrically* almost simple simply connected groups over finite separable extensions.

5.6.8. Decomposition of a reductive group. The following theorem says that a reductive group is almost a direct product of a semisimple group and a torus.

Unofficial version for incidental online use

Theorem 5.6.30. *Let G be a connected reductive group. Let T be the maximal torus in the center of G (see Corollary 5.5.11). Let $G' = [G, G]$ be the commutator subgroup. Then G' is semisimple, and the multiplication map $G' \times T \to G$ is surjective with finite kernel isomorphic to $G' \cap T$.*

Proof. We may assume that k is algebraically closed. In this case, the result is contained in [**PR94**, Theorem 2.4]. $\square$

Let us summarize how to build all reductive groups over a field k.

(1) Given a Dynkin diagram $\mathcal{D}$ and a finite separable extension $L \supseteq k$, construct the unique split geometrically almost simple simply connected group over L of type $\mathcal{D}$.
(2) Use Galois cohomology to classify its twists over L; these are all geometrically almost simple simply connected groups over L of type $\mathcal{D}$.
(3) Apply $\operatorname{Res}_{L/k}$ to these twists (for all $\mathcal{D}$ and L) to obtain the almost simple simply connected groups over k.
(4) Take a finite product to obtain the simply connected groups over k.
(5) Divide by a subgroup scheme of the center to obtain the connected semisimple groups over k.
(6) Take the product with a torus, and divide again by a subgroup scheme of the center to obtain the connected reductive groups over k.

Remark 5.6.31. Semisimple and reductive groups can also be understood in terms of reduced root data.

5.7. Abelian varieties

(Reference: [**Mum70**, §3.2])

Definition 5.7.1. An algebraic group over a field k is called an **abelian variety** if it is smooth, proper, and connected.

Example 5.7.2. A 0-dimensional abelian variety is the same thing as the trivial algebraic group. A 1-dimensional abelian variety is the same thing as an elliptic curve.

Proposition 5.7.3. *Abelian varieties are nice.*

Proof. Let A be an abelian variety. By Theorem 5.2.20, A is quasi-projective. Quasi-projective and proper imply projective. Since A has a k-point (the identity), connected implies geometrically connected (Proposition 2.3.24). Smooth and geometrically connected imply geometrically integral (Proposition 3.5.67). $\square$

Unofficial version for incidental online use

Abelian varieties are also commutative; see [**Mum70**, pp. 41–44] for two proofs.

Proposition 5.7.4. *Let A be an abelian variety over a field k, and let m be an integer such that $\operatorname{char} k \nmid m$. Then the multiplication-by-m map $A \stackrel{m}{\to} A$ is étale.*

Sketch of proof. Because of Theorem 4.3.7(ii), we may assume that k is algebraically closed. The set of points where the map is étale is open, so it suffices to check that it is étale at each $a \in A(k)$. By translating, it suffices to check that it is étale at $a = 0$. One can show that its derivative at 0 equals multiplication-by-m as an endomorphism of the tangent space of A at 0. If $\operatorname{char} k \nmid m$, then this linear map is invertible. $\square$

Definition 5.7.5. A **semiabelian variety** is an extension G of an abelian variety A by a torus T:

$$0 \to T \to G \to A \to 0.$$

5.7.1. Jacobian varieties.

(References: [**Mil86b**], [**BLR90**, Chapters 8 and 9], [**Kle05**])

Let X be a nice k-curve. Recall that there is a homomorphism

$$\deg \colon \operatorname{Pic} X \to \mathbb{Z}$$

and that $\operatorname{Pic}^0 X$ is defined as its kernel.

Theorem 5.7.6. *Let X be a nice k-curve of genus g. Assume that X has a k-point. Then there is a g-dimensional abelian variety $J = \operatorname{Jac} X$, called the **Jacobian** of X, such that $J(k) \simeq \operatorname{Pic}^0 X$ as groups, and more generally $J(L) \simeq \operatorname{Pic}^0 X_L$ for every field extension $L \supseteq k$, functorially in L.*

Proof. See [**Mil86b**]. $\square$

Remark 5.7.7. In fact, [**Mil86b**] contains a stronger version of Theorem 5.7.6 that specifies not only $J(L)$ for field extensions $L \supseteq k$, but also $J(T)$ for every k-scheme T, i.e., the entire functor of points. This is needed if one wants to determine the group scheme J uniquely up to isomorphism. Under the hypotheses of Theorem 5.7.6, if $\pi \colon X \times_k T \longrightarrow T$ denotes the second projection, X_t denotes the fiber $\pi^{-1}(t)$ for each $t \in T$, and $\mathscr{L}_t \in \operatorname{Pic} X_t$ denotes the restriction of an element $\mathscr{L} \in \operatorname{Pic}(X \times_k T)$ to X_t, then

(5.7.8)
$$J(T) \simeq \frac{\{\mathscr{L} \in \operatorname{Pic}(X \times_k T) : \text{for every } t \in T, \text{ we have } \deg \mathscr{L}_t = 0\}}{\pi^* \operatorname{Pic} T}.$$

Elements of $J(T)$ can be thought of as families of degree 0 line bundles on X parameterized by the points of T; the pullback of a line bundle on T restricts

Unofficial version for incidental online use

to the trivial line bundle on each fiber since the map from a fiber to T factors through a point.

Remark 5.7.9. In both Theorem 5.7.6 and Remark 5.7.7, the assumption that X has a k-point can be weakened to the assumption that X has a degree 1 divisor, or equivalently X has closed points of degrees whose gcd is 1.

Warning 5.7.10. If X does not have a degree 1 divisor, then the conclusions of Theorem 5.7.6 and Remark 5.7.7 can sometimes fail. The problem is that for any k-scheme J and for any Galois field extension $L \supseteq k$, there is a bijection $J(k) \to J(L)^{\mathrm{Gal}(L/k)}$, but in general $\operatorname{Pic}^0 X \to (\operatorname{Pic}^0 X_L)^{\mathrm{Gal}(L/k)}$ is only injective; see Corollary 6.7.8 for a related fact, and see Exercise 2.12 for an example. In general, the Jacobian J still exists, but the correct description of its points over a field $L \supseteq k$ is $J(L) \simeq (\operatorname{Pic}^0 X_{L_s})^{\mathrm{Gal}(L_s/L)}$, functorially in L. The correct generalization of this to T-valued points for an arbitrary k-scheme T is that the functor of points of J is the *fppf sheafification* (see Section 6.3.4) of the functor on the right-hand side of (5.7.8).

Remark 5.7.11. The functor has a variant using Pic instead of Pic^0. It is represented by the **Picard scheme $\mathbf{Pic}_{X/k}$**, a group scheme that is only *locally* of finite type over k. It has countably many connected components $\mathbf{Pic}^n_{X/k}$, indexed by $n \in \mathbb{Z}$, and each $\mathbf{Pic}^n_{X/k}$ is a nice k-variety. Moreover, $\mathbf{Pic}^0_{X/k}$ is isomorphic to the Jacobian J, and there is an exact sequence

$$0 \to J \to \mathbf{Pic}_{X/k} \to \mathbb{Z} \to 0,$$

where the $\mathbb{Z}$ on the right denotes a constant group scheme over k.

Remark 5.7.12. Even more generally, given an S-scheme X, the **relative Picard functor $\mathbf{Pic}_{X/S}$** is defined as the fppf sheafification of the functor

$$T \mapsto \operatorname{Pic}(X \times_S T)$$

on S-schemes T. (The sheafification process automatically trivializes pullbacks of line bundles on T, so it is not necessary to take the quotient as in (5.7.8).) Here are two criteria for representability of $\mathbf{Pic}_{X/S}$:

- If $X \to S$ is flat, projective, and finitely presented with geometrically reduced fibers, then $\mathbf{Pic}_{X/S}$ is represented by a scheme that is locally of finite presentation over S.
- If X is a proper k-scheme, then $\mathbf{Pic}_{X/k}$ is represented by a scheme that is locally of finite type over k.

5.7.2. Albanese varieties.

(References: [**Ser60**], [**Wit10**, §2 and Appendix A])

Unofficial version for incidental online use

The notion of Jacobian of a curve generalizes in two different ways to higher-dimensional varieties, as we discuss in this section and the next.

Let X be a geometrically integral variety over a field k. Is there a morphism to an abelian variety, $f\colon X \to A$, such that every other such morphism $f'\colon X \to A'$ factors uniquely as f followed by a homomorphism $A \to A'$? Not quite: for instance, if $x \in X(k)$ is such that $f(x) = 0$, and f' is f followed by a nonzero translation, then $f'(x) \neq 0$, but any homomorphism $A \to A'$ must map 0 to 0.

If a point $x \in X(k)$ is fixed, however, and we restrict attention to morphisms that send x to 0, then the answer becomes yes. This can be reformulated as follows:

Theorem 5.7.13 (Existence of Albanese varieties)**.** *Let $\mathcal{C}_{X,x}$ be the category of pairs (A, f), where A is an abelian variety over k, and $f\colon X \to A$ is a morphism such that $f(x) = 0$; a morphism from (A, f) to (A', f') is a homomorphism $\alpha\colon A \to A'$ making the triangle*

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "f'"'] & A \arrow[d, "\alpha"] \\ & A' \end{tikzcd}$$

commute. Then $\mathcal{C}_{X,x}$ has an initial object $(\mathrm{Alb}_{X/k}, \iota)$.

Proof. See [**Ser60**, Théorème 5] for the case where k is algebraically closed, and [**Wit10**, Appendix A] for the general case. □

Definition 5.7.14. The abelian variety $\mathrm{Alb}_{X/k}$ is called the **Albanese variety** of X.

Remark 5.7.15. For a variant that does not require a k-point x, see Example 5.12.11. It will follow from Exercise 5.16 that $\mathrm{Alb}_{X/k}$ is independent of x.

Remark 5.7.16. There is also a variant using semiabelian varieties instead of only abelian varieties; see [**Ser60**, Théorème 7] and [**Wit08**, Appendix A].

5.7.3. Picard varieties.

(References: [**Gro95b**], [**Kle05**])

Let X be a nice k-variety. The group scheme $\mathbf{Pic}^0_{X/k}$ is proper over k [**Gro95b**, Théorème 2.1(ii)], but in general it may happen that it is not reduced and hence not an abelian variety. The **Picard variety** of X is the associated reduced subscheme $\mathbf{Pic}^0_{X/k,\mathrm{red}}$.

Unofficial version for incidental online use

Theorem 5.7.17 ([**Gro95b**, Corollaire 3.2])**.** *The scheme* $\mathbf{Pic}^0_{X/k,\mathrm{red}}$ *is a subgroup scheme of* $\mathbf{Pic}^0_{X/k}$*, and it is an abelian variety.*

Sketch of proof. In general, for an algebraic group G over a field k of characteristic $p > 0$, it can happen that G_{red} is not a subgroup scheme; see Exercise 5.11. But if G is commutative, proper, and connected, then Proposition 5.2.19 and its proof imply that G is an extension of an abelian variety A by a finite commutative connected group scheme F of order p^n for some n; then it turns out that $p^n F = 0$, so $p^n G$ (the scheme-theoretic image of multiplication-by-p^n) is isomorphic to $p^n A = A$, so $p^n G$ is a closed subgroup of G whose underlying scheme is G_{red}. Apply this to $G := \mathbf{Pic}^0_{X/k}$. □

Remark 5.7.18. The group scheme $\mathbf{Pic}^0_{X/k}$ is an abelian variety even before passing to the reduced subscheme if any of the following hold:

- $\operatorname{char} k = 0$;
- X is a curve; or
- X is an abelian variety.

But there exist nice varieties X of dimension ≥ 2 over an algebraically closed field k of characteristic p such that $\mathbf{Pic}^0_{X/k}$ is not reduced; see Example 5.7.22 for an example and [**Kle05**, Remark 9.5.15] for discussion.

Definition 5.7.19. If X is an abelian variety, then $\mathbf{Pic}^0_{X/k}$ is called the **dual abelian variety**.

Theorem 5.7.20 (Albanese–Picard duality)**.** *Let* X *be a nice* k*-variety. Then* $\mathbf{Pic}^0_{X/k,\mathrm{red}}$ *is the dual abelian variety of* $\mathrm{Alb}_{X/k}$.

Proof. See [**Gro95b**, Théorème 3.3(iii)]. □

Remark 5.7.21. Let X be a nice k-variety. Let 0 be the identity point of $\mathbf{Pic}^0_{X/k}$, and let $T_0 \mathbf{Pic}^0_{X/k}$ be the tangent space there. Then it turns out that $T_0 \mathbf{Pic}^0_{X/k} \simeq \mathrm{H}^1(X, \mathscr{O}_X)$. In particular, if $\dim \mathbf{Pic}^0_{X/k} < \dim \mathrm{H}^1(X, \mathscr{O}_X)$, then $\mathbf{Pic}^0_{X/k}$ is not smooth at 0, and hence not reduced (see Theorem 5.2.16).

Example 5.7.22 ([**Igu55**])**.** Let k be a field of characteristic 2. Let E and E' be elliptic curves over k such that E has a k-point e of order 2. Let ι be the order 2 automorphism of $E \times E'$ given by $(x, y) \mapsto (x + e, -y)$. Then ι has no fixed points, so the quotient variety $X := (E \times E')/\iota$ is a nice surface. One can show that $\mathrm{Alb}_{X/k}$ is the quotient of E by the subgroup generated by e; in particular, $\dim \mathbf{Pic}^0_{X/k} = \dim \mathrm{Alb}_{X/k} = 1$. On the other hand, it turns out that $\dim \mathrm{H}^1(X, \mathscr{O}_X) = 2$. Thus, by Remark 5.7.21, $\mathbf{Pic}^0_{X/k}$ is not reduced. (For other examples, see [**Ser58**, §20].)

Unofficial version for incidental online use

5.7.4. Abelian schemes.

(Reference: [**Mil86a**, §20])

Definition 5.7.23. A group scheme $\mathcal{A} \to S$ is an **abelian scheme** if it is smooth and proper and has connected fibers.

An abelian scheme over S may be thought of as a family of abelian varieties parameterized by the points of S.

Remark 5.7.24. Let R be a discrete valuation ring, and let $K = \operatorname{Frac} R$. Let A be an abelian variety over K. If A has good reduction in the sense of Section 3.5.14, so there exists a smooth proper R-model $\mathcal{A}$, then it turns out that $\mathcal{A} \to \operatorname{Spec} R$ is automatically an abelian scheme. Thus A has good reduction if and only if it is the generic fiber of an abelian scheme over $\operatorname{Spec} R$.

5.7.5. Néron models of abelian varieties.

(Reference: [**BLR90**])

Recall the notion of Néron model from Section 3.5.16.

Theorem 5.7.25 (Néron)**.** *Let R be a discrete valuation ring. Let $K = \operatorname{Frac} R$. Let A be an abelian variety over K. Then A has a Néron model $\mathcal{N}$, and $\mathcal{N}$ is of finite type over R.*

Proof. See [**Art86a**, Theorem 1.2] or [**BLR90**, §1.3, Corollary 2]. □

Proposition 5.7.26. *Let $R, K, A, \mathcal{N}$ be as in Theorem 5.7.25. Let T be a smooth R-scheme. Then any K-rational map $T_K \dashrightarrow A$ extends to an R-morphism $T \to \mathcal{N}$.*

Proof. According to [**Wei48b**, §2, No. 15, Théorème 6], any K-rational map $T_K \dashrightarrow A$ is a K-morphism. Next, the Néron property says that any K-morphism $T_K \to A$ extends to an R-morphism $T \to \mathcal{N}$. □

Remark 5.7.27. Theorem 5.7.25 extends to the case where R is replaced by an integral Dedekind scheme, and K is its function field. See [**BLR90**, §1.4, Theorem 3]. For example, an abelian variety over $\mathbb{Q}$ has a Néron model over $\mathbb{Z}$.

Remark 5.7.28. Theorem 5.7.25 can be extended also in a different direction, to the case where A is a *semiabelian* variety over a discrete valuation ring. See [**Art86a**, Theorem 1.9] or [**BLR90**, §10.2, Theorem 2]. But these Néron models are generally no longer of finite type. For example, if $A = \mathbb{G}_{m,K}$ and $\pi \in R$ is a uniformizer, then $A(K) = K^\times = R^\times \times \pi^{\mathbb{Z}}$, and the Néron model $\mathcal{N}$ can be constructed by gluing copies of $\mathbb{G}_{m,R}$ indexed by

Unofficial version for incidental online use

$n \in \mathbb{Z}$ along their generic fibers, with the nth generic fiber glued to the 0th by multiplication-by-π^n on $\mathbb{G}_{m,K}$; see [**BLR90**, §10.1, Example 5].

It is not yet known if Remarks 5.7.27 and 5.7.28 can be combined; see [**BLR90**, §10.3].

5.7.6. Néron models of elliptic curves.

(References: [**BLR90**, §1.5], [**Liu02**, §10.2], [**Con15**])

Here we describe in more explicit terms the Néron model of an elliptic curve E, and we relate it to Weierstrass equations. Let R be a discrete valuation ring, and let $K = \operatorname{Frac} R$. Let $v\colon K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ be the discrete valuation.

Start with an elliptic curve E over K. If $\operatorname{char} K$ is not 2 or 3, then E is the closure in $\mathbb{P}^2_K$ of an affine plane curve $y^2 = x^3 + Ax + B$ with $A, B \in K$ such that $4A^3 + 27B^2 \neq 0$. Without restriction on the characteristic, E is the curve in $\mathbb{P}^2_K$ defined by a **Weierstrass equation**

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{5.7.29}$$

such that a certain polynomial Δ in a_1, a_2, a_3, a_4, a_6 is nonzero [**Sil09**, III.§1]. A **Weierstrass model** of E is a closed subscheme of $\mathbb{P}^2_R$ cut out by an equation (5.7.29) with $a_1, a_2, a_3, a_4, a_6 \in R$ whose generic fiber over K is isomorphic to E. Among all such models, any one that minimizes $v(\Delta)$ is called a **minimal Weierstrass model**; cf. [**Sil09**, Chapter VII].

Let W be a minimal Weierstrass model, so W is a proper R-scheme. If $v(\Delta) = 0$, then W is an abelian scheme over R; this is the case in which E has good reduction. If $v(\Delta) > 0$, then the special fiber W_k has a nonsmooth point, so $W \to \operatorname{Spec} R$ is not smooth, but W might be regular. In any case, one can iteratively blow up nonregular points until one reaches a regular proper model $\mathcal{E}$, which in fact is the minimal regular proper model in the sense of Section 9.3.1.6 (usually constructing the minimal regular proper model requires normalizations as well as blowups, and requires blowing down some exceptional curves, but this turns out to be unnecessary for elliptic curves; see the end of [**Con15**]). Although $\mathcal{E}$ is regular, it need not be smooth over R. Removing from $\mathcal{E}$ all nonsmooth points of the special fiber $\mathcal{E}_k$ (which may include removing entire irreducible components of $\mathcal{E}_k$ if they are of multiplicity > 1) yields the smooth locus $\mathcal{E}^{\text{smooth}}$. Similarly, removing from W the nonsmooth point of the special fiber W_k (if there is one) yields the smooth locus W^{smooth}.

Theorem 5.7.30. *Let R be a discrete valuation ring. Let $K = \operatorname{Frac} R$. Let E be an elliptic curve over K. Let W, $\mathcal{E}$, and $\mathcal{N}$ be, respectively, a minimal Weierstrass model, the minimal regular proper model, and the Néron model.*

Unofficial version for incidental online use

Let $\mathcal{N}^0$ be the open subscheme of $\mathcal{N}$ obtained by removing the non-identity components of the special fiber of $\mathcal{N}$. Then $\mathcal{E}^{\mathrm{smooth}} \xrightarrow{\sim} \mathcal{N}$ and $W^{\mathrm{smooth}} \xrightarrow{\sim} \mathcal{N}^0$.

Proof. See [**Con15**, Theorems 5.4 and 5.5]. The morphisms come from the Néron property. For example, the identity $E \to E$ extends to $\mathcal{E}^{\mathrm{smooth}} \to \mathcal{N}$. □

The first conclusion in Theorem 5.7.30 generalizes to higher genus; see Theorem 3.5.83.

5.7.7. Arithmetic of abelian varieties.

Theorem 5.7.31 (Mordell–Weil theorem)**.** *Let A be an abelian variety over a global field k. Then the abelian group $A(k)$ is finitely generated.*

Sketch of proof. Fix $m \in \mathbb{Z}_{\geq 2}$ not divisible by $\operatorname{char} k$. Theorem 5.7.31 implies the "weak Mordell–Weil theorem" that $A(k)/mA(k)$ is finite, but in fact, all known proofs of Theorem 5.7.31 involve proving the weak Mordell–Weil theorem (or some variant) first. For a proof of the weak Mordell–Weil theorem, see Theorem 8.4.9. Combining this with the theory of height functions completes the proof; see [**Ser97**, 4.3]. □

Let A be an abelian variety over a global field k. To A one can attach two objects that are conjecturally related to $A(k)$:

- The **Shafarevich–Tate group**[1] of A is
$$Ш(A) := \ker\Big(\mathrm{H}^1(k, A) \to \prod_{v \in \Omega_k} \mathrm{H}^1(k_v, A)\Big).$$
Because $Ш(A)$ is a subgroup of a Galois cohomology group, it is a torsion abelian group.
- The **L-function** of A is
$$L(A, s) := \prod_{\text{finite } v} \det\left(1 - q_v^{-s} \operatorname{Frob}_v |(V_\ell A)^{I_v}\right)^{-1},$$
where q_v is the order of the residue field, $\operatorname{Frob}_v \in \mathfrak{G}_k$ is a Frobenius element, $V_\ell A$ is as in Example 7.5.5, and $I_v \leq \mathfrak{G}_k$ is an inertia group. It turns out that the product converges for $\operatorname{Re} s > 3/2$, and conjecturally it has an analytic continuation to all of $\mathbb{C}$ [**Tat95a**, p. 216].

Conjecture 5.7.32 (Shafarevich–Tate conjecture [**Tat63**, Conjecture 4.1])**.** *For every abelian variety A over a global field k, the group $Ш(A)$ is finite.*

[1] Or should we say Tate–Shafarevich group? In the Cyrillic alphabet, the first letter Ш of Shafarevich comes *after* T.

Unofficial version for incidental online use

Conjecture 5.7.32 is open even for elliptic curves A over $\mathbb{Q}$: this case has been proved only under the additional hypothesis that the order of vanishing of its L-function at $s = 1$ is at most 1.

Conjecture 5.7.33 (Birch and Swinnerton-Dyer conjecture, rank part)**.** *Let A be an abelian variety over a global field k. Then* $\operatorname{ord}_{s=1} L(A, s) = \operatorname{rk} A(k)$.

Remark 5.7.34. The *full* Birch and Swinnerton-Dyer conjecture predicts that the leading coefficient in the Taylor series of $L(A, s)$ at $s = 1$ equals a product of certain arithmetic invariants of A, including $\#Ш(A)$; it may be considered an analogue of the Dirichlet analytic class number formula. The conjecture was formulated for elliptic curves over $\mathbb{Q}$ by Birch and Swinnerton-Dyer [**BSD65**, **SD67**] and generalized to abelian varieties over global fields by Tate [**Tat95a**].

Conjecture 5.7.33 is known for all elliptic curves A over $\mathbb{Q}$ satisfying $\operatorname{ord}_{s=1} L(A, s) \leq 1$.

5.8. Finite étale group schemes

A smooth algebraic group of dimension 0 over k is the same thing as a finite étale group scheme over k.

A $\mathfrak{G}_k$-**group** is a discrete group equipped with a continuous action of $\mathfrak{G}_k$. A $\mathfrak{G}_k$-**module** is a discrete *abelian* group equipped with a continuous action of $\mathfrak{G}_k$. A $\mathfrak{G}_k$-group or $\mathfrak{G}_k$-module is finite if it is finite as a set. The following gives a concrete way to study finite étale group schemes over k:

Theorem 5.8.1. *The functors*

$$\begin{aligned} \{\text{finite étale group schemes over } k\} &\longleftrightarrow \{\text{finite } \mathfrak{G}_k\text{-groups}\} \\ G &\longmapsto G(k_s) \\ \operatorname{Spec} \operatorname{Hom}_{\text{sets}}(A, k_s)^{\mathfrak{G}_k} &\longleftarrow\!\shortmid A \end{aligned}$$

are inverse equivalences of categories, and they restrict to equivalences of categories

$$\{\text{commutative finite étale group schemes over } k\} \longleftrightarrow \{\text{finite } \mathfrak{G}_k\text{-modules}\}.$$

Proof. The first equivalence arises from taking the group objects on both sides of Theorem 1.3.2 and using the anti-equivalence between affine k-schemes and k-algebras. Then imposing commutativity on both sides yields the second equivalence. □

5.9. Classification of smooth algebraic groups

(Reference: [**Kne67**])

Unofficial version for incidental online use

5.9.1. Classification over perfect fields. Let G be a *smooth* algebraic group over a *perfect* field k. We will define a chain of smooth algebraic subgroups in G, each normal in G.

The connected component $G_{\mathrm{conn}} = G^0$ of G is a closed and open normal subgroup of G (Proposition 5.2.4), and G/G_{conn} is a finite étale group scheme, called the **component group** of G (this holds even if k is not necessarily perfect and G is not necessarily smooth). Next, *Chevalley's theorem* states that there is a unique exact sequence of smooth connected algebraic groups

$$0 \to G_{\mathrm{affine}} \to G_{\mathrm{conn}} \to A \to 0, \tag{5.9.1}$$

where G_{affine} is affine and A is an abelian variety; in fact, G_{affine} is the unique maximal smooth connected affine algebraic subgroup of G_{conn} (or of G). As mentioned in Section 5.6, the radical $G_{\mathrm{solv}} := \mathscr{R}(G_{\mathrm{affine}})$ is the unique maximal smooth connected solvable *normal* subgroup of G_{affine}; the quotient $G_{\mathrm{affine}}/G_{\mathrm{solv}}$ is semisimple. As mentioned in Section 5.6, the unipotent radical $G_{\mathrm{unip}} := \mathscr{R}_u(G_{\mathrm{affine}}) = \mathscr{R}_u(G_{\mathrm{solv}})$ is the unique maximal smooth connected unipotent *normal* subgroup of G_{affine}; then $G_{\mathrm{solv}}/G_{\mathrm{unip}}$ is a torus.

To summarize, we have the following chain of normal algebraic subgroups of G:

$$\begin{tikzcd}
G \arrow[d, dash, "\text{finite étale}"'] \arrow[dd, dash, bend left, "\text{proper}"] \\
G_{\mathrm{conn}} \arrow[d, dash, "\text{abelian variety}"'] \\
G_{\mathrm{affine}} \arrow[d, dash, "\text{semisimple}"'] \arrow[dd, dash, bend left, "\text{reductive}"] \\
G_{\mathrm{solv}} \arrow[d, dash, "\text{torus}"'] \\
G_{\mathrm{unip}} \arrow[d, dash, "\text{unipotent}"'] \\
\{1\}.
\end{tikzcd}$$

Each label between groups indicates the type of group that arises as the quotient.

5.9.2. Functorial properties.

Proposition 5.9.2. *If $L \supseteq k$ is an extension of perfect fields, then the chain for G_L is obtained by base-extending each group in the chain for G.*

Unofficial version for internal online use

Proof. For G_{conn} it follows since G_{conn} is geometrically connected (Proposition 5.2.4). For G_{affine} it follows from the uniqueness of (5.9.1), since base-extending (5.9.1) yields a sequence with the same properties over L. For G_{solv}, this has been mentioned already in Remark 5.6.3. For G_{unip} see [**CGP10**, Proposition 1.1.9(1)]. $\square$

Proposition 5.9.3. *Let $f\colon G \to H$ be a homomorphism of smooth algebraic groups. Then*

(a) *f restricts to a homomorphism $G_{\text{conn}} \to H_{\text{conn}}$, and*

(b) *f restricts to a homomorphism $G_{\text{affine}} \to H_{\text{affine}}$.*

Proof.

(a) The image of G_{conn} is connected and contains the identity point 1 of H.

(b) Let I be the image of the composititition

$$G_{\text{affine}} \hookrightarrow G_{\text{conn}} \to H_{\text{conn}} \twoheadrightarrow H_{\text{conn}}/H_{\text{affine}}.$$

By Theorem 5.2.9, I is both a quotient of the smooth affine connected group G_{affine} and a closed subgroup of the abelian variety $H_{\text{conn}}/H_{\text{affine}}$. The former shows that I is smooth, affine, and connected (Proposition 5.2.7(a)), and the latter shows that I is proper. Thus I is trivial. $\square$

Warning 5.9.4. A homomorphism $f\colon G \to H$ of smooth algebraic groups does not necessarily restrict to $G_{\text{solv}} \to H_{\text{solv}}$ and $G_{\text{unip}} \to H_{\text{unip}}$. (For a counterexample, let f be the embedding $\mathrm{U}_n \hookrightarrow \mathrm{SL}_n$ for some $n \geq 2$.)

5.9.3. Imperfect fields.

(Reference: [**CGP10**])

A few aspects of the classification fail over imperfect fields k. Let G be a smooth connected affine algebraic group.

- As in Remark 5.6.3, if k is not perfect, the unipotent radical of $G_{\overline{k}}$ need not descend to an algebraic group over k; thus $\mathscr{R}_u(G_{\overline{k}})$ can be strictly larger than $\mathscr{R}_u(G)_{\overline{k}}$. In fact, it can happen that $\mathscr{R}_u(G_{\overline{k}}) \neq \{1\}$ while $\mathscr{R}_u(G) = \{1\}$; see Exercise 5.13. Call G **pseudo-reductive** if $\mathscr{R}_u(G) = \{1\}$ [**CGP10**, Definition 1.1.1]; this is weaker than being reductive.
- There are similar issues with the radical $\mathscr{R}(G)$. Moreover, it turns out that semisimplicity condition $\mathscr{R}(G_{\overline{k}}) = \{1\}$ implies $[G, G] = G$, but the weaker condition $\mathscr{R}(G) = \{1\}$ does not, so it is natural to require $[G, G] = G$ separately. Therefore call G **pseudo-semisimple** if $\mathscr{R}(G) = \{1\}$ and $[G, G] = G$ [**CGP10**, Definition 11.2.2].

Unofficial version for incidental online use

- Chevalley's theorem above must be modified as follows: A connected algebraic group G contains a smallest connected affine normal subgroup scheme G_{affine} such that G/G_{affine} is an abelian variety. But G_{affine} need not be smooth; see [**BLR90**, 9.2, Theorem 1]. In particular, the formation of G_{affine} does not commute with inseparable base extension.

There is an alternative to Chevalley's theorem that works over any field, but is backward in that the affine group is the quotient instead of the subgroup. Call an algebraic group A **anti-affine** if $\mathscr{O}(A) = k$. Anti-affine algebraic groups are smooth, connected, and commutative; see [**Bri09**] and the references listed there for these and more properties of these groups.

Theorem 5.9.5. *A smooth connected algebraic group G over a field k fits in an exact sequence of smooth connected algebraic groups*

$$0 \to A \to G \to L \to 0$$

in which A is anti-affine and L is affine.

Sketch of proof. Let $L = \operatorname{Spec} \mathscr{O}(G)$, and use the group structure on G to define a group structure on L. See [**DG70**, III, §3, no. 8] for the rest of the proof. $\square$

For cohomological purposes, Theorem 5.9.5 is superior to the original Chevalley theorem in that the commutative group is on the left.

5.10. Approximation theorems

(References: [**PR94**, Chapter 7] and [**Rap14**])

Recall from Section 2.6.4.5 the notions of weak and strong approximation for varieties over a global field.

5.10.1. Weak approximation. Recall from Section 2.6.2 that for any variety X over $\mathbb{R}$ (or a subfield), the set $X(\mathbb{R})$ can be equipped with the analytic topology.

Theorem 5.10.1 (Real approximation theorem)**.** *Let G be a connected affine algebraic group over $\mathbb{Q}$. Then $G(\mathbb{Q})$ is dense in $G(\mathbb{R})$.*

Theorem 5.10.1 is implied by the case $k = \mathbb{Q}$ of Theorem 5.10.4(a) below.

Warning 5.10.2. The conclusion of Theorem 5.10.1 can fail if G is not connected; see Exercise 5.14. It can fail also if G is not affine: consider a rank 0 elliptic curve over $\mathbb{Q}$.

Warning 5.10.3. There exists a connected semisimple algebraic group G over $\mathbb{Q}$ such that $G(\mathbb{Q})$ is not dense in $G(\mathbb{Q}_2)$ [**San81**, Exemple 5.8].

Unofficial version for incidental online use

Theorem 5.10.4 (Weak approximation theorem)**.** *Let G be a connected affine algebraic group over a number field k.*

(a) *There exists a finite set of finite places T of k such that $G(k)$ is dense in $\prod_{v \notin T} G(k_v)$.*
(b) *The closure of $G(k)$ in $\prod_{v \in \Omega_k} G(k_v)$ is an open normal subgroup, and the quotient is a finite abelian group.*
(c) *If G is a simply connected or adjoint group, then G satisfies weak approximation.*

Proof.

(a) Let $L \supseteq k$ be a finite Galois extension such that G_L is split. Let T be the set of $v \in \Omega_k$ for which a decomposition group of v in $\operatorname{Gal}(L/k)$ is not cyclic. Thus T is a subset of the set of ramified finite primes in the extension $L \supseteq k$. It turns out that T satisfies the conclusion [**San81**, Corollaire 3.5(ii)]. The proof reduces to the case of tori, which is attributed to Serre. (In general, a variety over a global field that satisfies weak approximation away from finitely many places is said to satisfy **weak weak approximation**!)
(b) See [**San81**, Corollaire 3.5(i)]. The quotient is called the **defect of weak approximation**.
(c) See [**PR94**, Theorem 7.8]. □

Remark 5.10.5. If instead k is a global function field, (c) still holds [**Har67**, Satz 2.2.4], but (a) and (b) can fail. For example, if p is odd, $k = \mathbb{F}_p(t)$, and $G \leq \mathbb{G}_a^2$ is defined by $y^p = tx^p + x$ over k, then $G(k)$ is finite by [**Vol91**, Theorem 3], but $G(k_v)$ is infinite for every v by Proposition 3.5.75.

For more on weak approximation in algebraic groups, see [**PR94**, §7.3].

5.10.2. Strong approximation.

Theorem 5.10.6 (Strong approximation theorem)**.** *Let G be a connected semisimple algebraic group over a global field k. Let S be a finite set of places of k. Then $G(k)$ is dense in $G(\mathbf{A}^S)$ if and only if G is simply connected and for each almost simple factor G_i of G, there exists $v \in S$ such that $G_i(k_v)$ is noncompact.*

Proof. See the original sources [**Kne66**, **Pla69**, **Pra77**, **Mar77**], or see [**PR94**, §7.4]. □

See Theorem 8.4.10 for the reason for the simply connected hypothesis.

Unofficial version for incidental online use

Remark 5.10.7. If k is a number field, there is a more general statement, applicable to any algebraic group G over k. Namely, G satisfies strong approximation if and only if G is connected and affine, the torus $G_{\mathrm{solv}}/G_{\mathrm{unip}}$ is trivial, and the semisimple quotient G/G_{solv} satisfies the criterion of Theorem 5.10.6.

5.11. Inner twists

Let G be a smooth algebraic group over k. The action of G on itself by inner automorphisms defines a homomorphism

$$G(k_{\mathrm{s}}) \to \operatorname{Aut} G_{k_{\mathrm{s}}}.$$

This induces a map of pointed sets

$$\mathrm{H}^1(k, G) \to \mathrm{H}^1(k, \operatorname{Aut} G_{k_{\mathrm{s}}}). \tag{5.11.1}$$

The image of an element $\tau \in \mathrm{H}^1(k, G)$ under (5.11.1) (or, more precisely, a cocycle representing this image) defines a twist G^τ of the algebraic group G, called an **inner twist**. It is another smooth algebraic group over k.

5.12. Torsors

(Reference: [**BLR90**, §6.4], Chapter 2 of [**Sko01**])

5.12.1. Warmup: Torsors of groups. Let G be a group.

Definition 5.12.1. A (right) G-**torsor** (also called **torsor under** G or **principal homogeneous space of** G) is a right G-set isomorphic to

G with the right action of G by translation.

In other words, a G-torsor is a set X with a simply transitive G-action (**simply transitive** means that X is nonempty and that for every $x, x' \in X$ there exists a *unique* $g \in G$ such that $xg = x'$).

If X is a G-torsor, then a choice of $x \in X$ determines an isomorphism of G-sets

$$\begin{aligned} G &\longrightarrow X \\ g &\longmapsto xg. \end{aligned}$$

Example 5.12.2. If G is a subspace of a vector space V, and X is a translate of G, then X is a G-torsor. Here X is not *canonically* isomorphic to G, but a choice of $x \in X$ determines a translation isomorphism $G \to X$ sending 0 to x.

Unofficial version for incidental online use

5.12.2. Torsors under algebraic groups. Let k be a field. Let G be a smooth algebraic group over k. The **trivial G-torsor over k**, which for convenience we denote by $\mathbf{G}$, is

the underlying variety of G equipped with
the right action of G by translation.

Definition 5.12.3. A **G-torsor over k** (also called **torsor under G** or **principal homogeneous space of G**) is a k-variety X equipped with a right action of G such that X_{k_s} *equipped with its right G_{k_s}-action* is isomorphic to $\mathbf{G}_{k_s}$ (the isomorphism is required to respect the right actions of G_{k_s}). A **morphism of G-torsors** is a G-equivariant morphism of k-schemes.

Remark 5.12.4. The definition can be generalized to nonsmooth G, but then one should use $\overline{k}$ instead of k_s. We restrict to smooth G for now so that Galois cohomology suffices in Section 5.12.4. For a generalization, see Section 6.5.

Remark 5.12.5. If X is a G-torsor over k, then $X(k_s)$ is a $G(k_s)$-torsor in the sense of Section 5.12.1.

Warning 5.12.6. A k-variety X equipped with a right G-action making $X(k_s)$ a $G(k_s)$-torsor is not necessarily a G-torsor. For example, if G is a smooth algebraic group over $\mathbb{F}_p$, then X could be G with the action

$$\begin{aligned} X \times G &\longrightarrow X \\ (x, g) &\longmapsto x \cdot F(g), \end{aligned}$$

where $F\colon G \to G$ is the Frobenius endomorphism; this X is not a G-torsor if $\dim G > 0$.

Remark 5.12.7. The notion of torsor can be generalized to the notion of homogeneous space. First suppose that G is a group. A right G-set X decomposes as a disjoint union of G-orbits. If X consists of exactly one G-orbit, then X is called a **homogeneous space of G**. If H is a subgroup of G, then $H\backslash G$ is a homogeneous space; conversely, if X is a homogeneous space, and H is the stabilizer of some $x \in X$, then $X \simeq H\backslash G$ as homogeneous spaces.

Now suppose that G is a smooth algebraic group. A k-variety X equipped with a right G-action is called a **homogeneous space** if there exists $x \in X(k_s)$ such that

$$\begin{aligned} G_{k_s} &\longrightarrow X_{k_s} \\ g &\longmapsto xg \end{aligned}$$

is surjective, or equivalently if there exists a closed subgroup $H \leq G_{k_s}$ such that $X_{k_s} \simeq H\backslash G_{k_s}$ as k_s-varieties equipped with right G_{k_s}-action.

Unofficial version for incidental online use

5.12.3. Examples.

Example 5.12.8. Let T be the torus $x^2 + 2y^2 = 1$ of Example 5.5.3. Then the affine variety X defined by $x^2 + 2y^2 = -3$ in $\mathbb{A}^2_{\mathbb{Q}}$ can be viewed as a T-torsor over $\mathbb{Q}$. It is a nontrivial torsor, since $X(\mathbb{Q}) = \emptyset$.

Example 5.12.9. Let $L \supseteq k$ be a finite Galois extension of fields. Let G be the constant group scheme over k associated to $\operatorname{Gal}(L/k)$; see Section 5.1.5. Then the left action of $\operatorname{Gal}(L/k)$ on L induces a right action of G on $\operatorname{Spec} L$ that makes $\operatorname{Spec} L$ a G-torsor over k.

Example 5.12.10. Let A be a smooth closed subgroup of a smooth algebraic group B. Let $\phi\colon B \to C := B/A$ be the natural surjective morphism to the quotient (which in general is only a k-variety, since we did not assume that A was normal). Let $c \in C(k)$. Then the closed subscheme $\phi^{-1}(c) \subseteq B$ is an A-torsor over k.

Example 5.12.11 (Albanese torsor)**.** Let X be a geometrically integral variety over a field k. Let $\mathcal{C}_X$ be the category of triples (A, T, f), where A is an abelian variety over k, and T is an A-torsor, and $f\colon X \to T$ is a morphism; a morphism from (A, T, f) to (A', T', f') consists of a homomorphism $\alpha\colon A \to A'$ and a morphism of varieties $\tau\colon T \to T'$ such that the diagrams

$$\begin{tikzcd} T \times A \arrow[r] \arrow[d, "(\alpha,\tau)"'] & T \arrow[d, "\tau"] \\ T' \times A' \arrow[r] & T' \end{tikzcd} \qquad \text{and} \qquad \begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "f'"'] & T \arrow[d, "\tau"] \\ & T' \end{tikzcd}$$

commute. Then $\mathcal{C}_X$ has an initial object $(\operatorname{Alb}_{X/k}, \operatorname{Alb}^1_{X/k}, \iota)$; see [**Wit08**, Appendix A].

The abelian variety $\operatorname{Alb}_{X/k}$ is called the **Albanese variety** of X, and its torsor $\operatorname{Alb}^1_{X/k}$ is called the **Albanese torsor** of X. In the case that X has a k-point x, the abelian variety $\operatorname{Alb}_{X/k}$ defined using $\mathcal{C}_{X,x}$ in Theorem 5.7.13 coincides with the abelian variety $\operatorname{Alb}_{X/k}$ defined using $\mathcal{C}_X$; see Exercise 5.16.

As in Remark 5.7.16, there is a semiabelian variant: see [**Wit08**, Appendix A].

Example 5.12.12. Let X be a nice genus 1 curve, so $\operatorname{Alb}_{X/k}$, the Jacobian of X, is a 1-dimensional abelian variety, an elliptic curve. One can show that the morphism $X \to \operatorname{Alb}^1_{X/k}$ is an isomorphism, so X is a torsor under the elliptic curve $\operatorname{Alb}_{X/k}$.

Unofficial version for incidental online use

5.12.4. Classification of torsors. For any fixed smooth algebraic group G over k, we have bijections

$$
\begin{aligned}
\{\, G\text{-torsors over } k \,\} = \{\, \text{twists of } \mathbf{G} \,\} &\leftrightarrow \mathrm{H}^1(k, \operatorname{Aut} \mathbf{G}_{k_s}) \quad \text{(by Theorems 4.5.2 and 5.2.20)} \\
&= \mathrm{H}^1(k, G(k_s)) \qquad \text{(see Exercise 5.15)} \\
&=: \mathrm{H}^1(k, G).
\end{aligned}
$$

(the first two sets should really be sets of *k-isomorphism classes*). Given a G-torsor X, let $[X]$ denote its class in $\mathrm{H}^1(k, G)$.

Remark 5.12.13. The cohomology class of a torsor can also be constructed explicitly. Given a G-torsor X, choose $x \in X(k_s)$, and define $g_\sigma \in G(k_s)$ by ${}^\sigma x = x \cdot g_\sigma$; then $\sigma \mapsto g_\sigma$ is a 1-cocycle representing the class of X in $\mathrm{H}^1(k, G)$.

A G-torsor is analogous to a coset of a group G in some larger group, or to a translate of a subspace G in some larger vector space. To trivialize a torsor T, one must choose a point in T to be translated back to the identity of G, but such a point might not exist over the ground field. With this intuition, the following should not be a surprise:

Proposition 5.12.14 (Trivial torsors)**.** *Let G be a smooth algebraic group over a field k. Let X be a G-torsor over k. The following are equivalent:*

(i) *X is isomorphic to the trivial torsor $\mathbf{G}$.*

(ii) *$X(k) \neq \emptyset$.*

(iii) *$[X] \in \mathrm{H}^1(k, G)$ is the neutral element.*

Proof.

(i)$\Leftrightarrow$(iii): This is a general fact about twists.

(i)$\Rightarrow$(ii): The set $\mathbf{G}(k)$ contains the identity.

(ii)$\Rightarrow$(iii): This follows from the explicit construction of a cocycle above. □

Exercise 5.22 gives another way of thinking about torsors when G is commutative.

5.12.5. Geometric operations on torsors. Throughout this section, G is a smooth algebraic group over k. When G is commutative, $\mathrm{H}^1(k, G)$ is an abelian group. The group operations can be expressed in purely geometric terms, as we now explain. In fact, some versions of the operations make sense even when G is not commutative.

Unofficial version for incidental online use

5.12.5.1. *Inverse torsors.* Let $\mathbf{G}$ be the trivial right G-torsor. It also has a left action of $\mathcal{G} := G$, so one says that $\mathbf{G}$ is a $\mathcal{G}$-G-**bitorsor**:

$$^{\mathcal{G}} \circlearrowright \mathbf{G} \circlearrowleft {}^{G}.$$

The automorphism group scheme of the right G-torsor $\mathbf{G}$ is $\mathcal{G}$ acting on the left.

Now let $\tau \in \mathrm{H}^1(k, \mathcal{G})$. The left action of $\mathcal{G}$ on $\mathbf{G}$ does not commute with the left action of other elements of $\mathcal{G}$, so if we twist $\mathbf{G}$ by (a cocycle representing) τ to get the corresponding right G-torsor T, then the left action of $\mathcal{G}$ must be twisted too. The result is that T is a $\mathcal{G}^\tau$-G-bitorsor, where $\mathcal{G}^\tau$ is the inner twist (see Section 5.11):

$$^{\mathcal{G}^\tau} \circlearrowright T \circlearrowleft {}^{G}.$$

The same k-scheme T has a left action of G defined by $g \cdot t := tg^{-1}$ and a right action of $\mathcal{G}^\tau$ defined by $t \cdot g := g^{-1}t$. The resulting G-$\mathcal{G}^\tau$-bitorsor is denoted T^{-1}, and is called the **inverse torsor**:

$$^{G} \circlearrowright T^{-1} \circlearrowleft {}^{\mathcal{G}^\tau}.$$

Example 5.12.15. If G is commutative, then $\mathcal{G}^\tau = G$ and $[T^{-1}] = -[T]$ in the abelian group $\mathrm{H}^1(k, G)$.

5.12.5.2. *Contracted products.* Let T be a right G-torsor; let $\tau \in \mathrm{H}^1(k, G)$ be its class. Let X be a quasi-projective k-variety equipped with a *left* G-action. This action defines a homomorphism $G(k_\mathrm{s}) \to \operatorname{Aut} X_{k_\mathrm{s}}$ and hence a map $\mathrm{H}^1(k, G) \to \mathrm{H}^1(k, \operatorname{Aut} X_{k_\mathrm{s}})$. The image of (a cocycle representing) τ under this map corresponds to a twist of X, called the **contracted product** $T \overset{G}{\times} X$. Geometrically, it is the quotient of $T \times_k X$ by the G-action in which $g \in G$ acts by $(t, x) \mapsto (tg^{-1}, gx)$.

In a similar way, if T is a *left* G-torsor and Z is a quasi-projective variety with a right G-action, then we can construct the contracted product $Z \overset{G}{\times} T$.

Example 5.12.16. If G is commutative and Z also is a G-torsor, then $Z \overset{G}{\times} T$ is another G-torsor, and $[Z \overset{G}{\times} T] = [Z] + [T]$ in the abelian group $\mathrm{H}^1(k, G)$.

Example 5.12.17. If Z is a right G-torsor, and T is a G-H-bitorsor, then $Z \overset{G}{\times} T$ is a right H-torsor.

5.12.5.3. *Subtraction of torsors.* Let Z and T be two right G-torsors; let $\zeta, \tau \in \mathrm{H}^1(k, G)$ be their classes. As in Section 5.12.5.1, T^{-1} is a G-G^τ-bitorsor. By Example 5.12.17, $Z \overset{G}{\times} T^{-1}$ is then a right G^τ-torsor. If we fix

Unofficial version for incidental online use

T, then the "subtraction-of-τ" map

$$\begin{aligned} \mathrm{H}^1(k,G) &\xrightarrow{-\tau} \mathrm{H}^1(k,G^\tau) \\ [Z] &\longmapsto [Z \overset{G}{\times} T^{-1}] \end{aligned}$$

is a bijection, the inverse bijection being subtraction-of-$[T^{-1}]$.

Example 5.12.18. If G is commutative, then $G^\tau = G$ and the class of the right G-torsor $Z \overset{G}{\times} T^{-1}$ is $\zeta - \tau$ by Examples 5.12.15 and 5.12.16.

5.12.6. Torsors over fields of dimension ≤ 1. The following theorem shows that certain algebraic groups over certain fields have no nontrivial torsors:

Theorem 5.12.19.

(a) (Lang) *Let k be a finite field, and let G be a smooth connected algebraic group over k. Then $\mathrm{H}^1(k,G) = 0$.*

(b) (Steinberg) *Let k be a perfect field. Then $\dim k \le 1$ if and only if $\mathrm{H}^1(k,G) = 0$ for all smooth connected* affine *algebraic groups G over k.*

Proof.

(a) We follow the original proof of [**Lan56**]. An element of $\mathrm{H}^1(k,G)$ corresponds to a G-torsor X. By Proposition 5.12.14, it suffices to show that X has a k-point.

Fix $x \in X(\overline{k})$. Then every other point of $X(\overline{k})$ is of the form xg for some $g \in G(\overline{k})$, and to say that xg is a k-point is to say that it is fixed by the Frobenius automorphism $\sigma \in \mathrm{Gal}(\overline{k}/k)$. Thus we must find $g \in G(\overline{k})$ such that ${}^\sigma(xg) = xg$, or equivalently ${}^\sigma x\, {}^\sigma g\, g^{-1} = x$. Since X is a torsor, there exists $b \in G(\overline{k})$ such that ${}^\sigma x\, b = x$, so it suffices to show the following:

(5.12.20) Every $b \in G(\overline{k})$ is of the form ${}^\sigma g\, g^{-1}$.

(Alternatively, we could have reduced to proving (5.12.20) by using the definition of nonabelian H^1.)

Let $q = \#k$. Let $F\colon G \to G$ be the q-power Frobenius endomorphism; it acts on $\overline{k}$-points in the same way as σ. There is a left action of G on $T := G$ in which g acts as $t \mapsto F(g)\, t\, g^{-1}$. Then (5.12.20) is equivalent to b being in the $G(\overline{k})$-orbit of 1.

Fix $t \in T(\overline{k})$ and define a morphism

$$\begin{aligned} \phi\colon G_{\overline{k}} &\longrightarrow T_{\overline{k}} \\ g &\longmapsto F(g)\, t\, g^{-1}. \end{aligned}$$

Unofficial version for incidental online use

The derivative of F is everywhere 0, so the derivative of ϕ at $g = 1$ equals the derivative of the invertible morphism $g \mapsto tg^{-1}$ at $g = 1$; thus the derivative of ϕ at $g = 1$ is invertible. If a morphism between smooth varieties $V \to W$ of the same dimension has invertible derivative somewhere, its image contains a nonempty Zariski open subset of W. Applying this to $\phi\colon G_{\overline{k}} \to T_{\overline{k}}$ shows that an arbitrary $G(\overline{k})$-orbit in $T(\overline{k})$ contains a nonempty Zariski open subset of $G(\overline{k})$. Since also G is connected, and hence geometrically connected, any two orbits will intersect. But orbits are disjoint, so there can be only one. In particular, b is in the $G(\overline{k})$-orbit of 1, as required.

(b) See [**Ste65**, Theorem 1.9], or the reproduction in Theorem 1′ of III.§2 and III.Appendix 1 of [**Ser02**]. □

Remark 5.12.21. The same proof shows that Theorem 5.12.19(a) remains true if the smoothness hypothesis is dropped and one interprets $\mathrm{H}^1(k, G)$ as the Čech fppf cohomology set defined in Section 6.4.4.

Corollary 5.12.22. *A nice genus* 1 *curve X over a finite field k has a k-point.*

Proof. Let E be the Jacobian of X. As discussed in Example 5.12.12, X is an E-torsor. By Theorem 5.12.19(a), $\mathrm{H}^1(k, E) = 0$, so X is a trivial torsor. By Proposition 5.12.14(i)⇒(ii), X has a k-point. □

Remark 5.12.23. The first proof of Corollary 5.12.22 used the Riemann–Roch theorem; see [**Sch31**, Satz 20]. Corollary 5.12.22 can also be viewed as a consequence of the Hasse–Weil bound; see Corollary 7.2.1.

5.12.7. Torsors over local fields.

Theorem 5.12.24. *Let k be a local field.*

(a) (Borel–Serre) *Let G be an affine algebraic group over k. If* $\operatorname{char} k = 0$ *or G is connected and reductive, then $\mathrm{H}^1(k, G)$ is finite.*

(b) (Kneser, Bruhat–Tits) *If $k \not\simeq \mathbb{R}$, and G is a simply connected semisimple algebraic group over k, then $\mathrm{H}^1(k, G) = 0$.*

(c) (Tate) *If A is an abelian variety over k, then*

$$\mathrm{H}^1(k, A) \simeq \mathrm{Hom}_{\mathrm{conts}}(A(k), \mathbb{Q}/\mathbb{Z}).$$

Proof.

(a) See [**BS64**, Théorème 6.1] and [**Ser02**, III.§4.3, Remark 2].

(b) This was proved in [**Kne65a**, **Kne65b**] using the classification of such groups when k is a finite extension of $\mathbb{Q}_p$. It was extended to local fields of characteristic p in [**BT87**], which gave a classification-free proof.

Unofficial version for incidental online use

(c) See [**Tat95b**]. □

Warning 5.12.25. With regard to Theorem 5.12.24(a), it is not true that $\mathrm{H}^1(k,G)$ is finite for every affine algebraic group G over a local field k of characteristic p, even if k is commutative and smooth. For example, $\mathrm{H}^1(k,\mathbb{Z}/p\mathbb{Z})$ is infinite in this case, since if $t \in k$ is a uniformizer, then each positive integer n not divisible by p gives rise to a $\mathbb{Z}/p\mathbb{Z}$-extension $k[y]/(y^p - y - t^{-n})$ of k, and these are distinct because their discriminants are distinct. For a connected pseudo-reductive example, see [**CGP10**, Example 11.3.3].

Warning 5.12.26. Theorem 5.12.24(a) can fail if the affineness assumption is dropped. For example, if A is a nonzero abelian variety, then Theorem 5.12.24(c) implies that $\mathrm{H}^1(k,A)$ is infinite.

Warning 5.12.27. Theorem 5.12.24(b) is false for $k=\mathbb{R}$. For example, $\#\mathrm{H}^1(\mathbb{R},\mathrm{Spin}_n) \to \infty$ as $n \to \infty$, as can be deduced from the fact that the number of isomorphism types of rank n quadratic forms over $\mathbb{R}$ grows with n. Nevertheless, the group $\mathrm{H}^1(\mathbb{R},G)$ can be described explicitly for every simply connected group over $\mathbb{R}$ [**Bor88**].

For more results along the lines of Theorems 5.12.19 and 5.12.24, see [**Ser02**, Chapter III].

5.12.8. Local-global principle for torsors. Let G be an algebraic group over a global field k. Let X be a right G-torsor, and let $[X]$ denote its class in $\mathrm{H}^1(k,G)$ (throughout this section, if $\operatorname{char} k = p$ and G is not smooth, then interpret $\mathrm{H}^1(k,G)$ as the Čech fppf cohomology set defined in Section 6.4.4). By Proposition 5.12.14, X has a k-point if and only if $[X]$ is the neutral element 0. Similarly, X has a k_v-point if and only if the image $[X_{k_v}]$ of $[X]$ under $\mathrm{H}^1(k,G) \to \mathrm{H}^1(k_v,G)$ is 0. Thus the statement that X satisfies the local-global principle is the statement

If $[X]$ maps to 0 in $\mathrm{H}^1(k_v,G)$ for every v, then $[X]=0$ in $\mathrm{H}^1(k,G)$.

Hence the statement that *all* right G-torsors satisfy the local-global principle is the statement that the kernel

$$Ш^1(k,G) := \ker\big(\mathrm{H}^1(k,G) \to \prod_v \mathrm{H}^1(k_v,G)\big)$$

is trivial.

If G is noncommutative, then a stronger statement is that the map

$$\mathrm{H}^1(k,G) \longrightarrow \prod_v \mathrm{H}^1(k_v,G) \tag{5.12.28}$$

Unofficial version for mental online use

is injective. For each $\tau \in \mathrm{H}^1(k,G)$, we have an inner twist G^τ of G, and the subtraction-of-τ bijection $\mathrm{H}^1(k,G) \to \mathrm{H}^1(k,G^\tau)$ of Section 5.12.5.3 identifies the fiber of (5.12.28) containing τ with $\text{Ш}^1(k,G^\tau)$. Thus injectivity of (5.12.28) is equivalent to the statement that $\text{Ш}^1(k,G^\tau) = 0$ for every inner twist G^τ of G. There are also variants in which v ranges not over all places of k, but only over places outside a fixed finite subset S; one defines

$$\text{Ш}^1_S(k,G) := \ker\big(\mathrm{H}^1(k,G) \to \prod_{v \notin S} \mathrm{H}^1(k_v,G)\big).$$

None of the injectivity statements are true in general, but the following weaker result holds:

Theorem 5.12.29. *Let k be a global field. Let S be a finite set of places of k. Let G be an affine algebraic group over k. Then $\mathrm{H}^1(k,G) \to \prod_{v\notin S} \mathrm{H}^1(k_v,G)$ has finite fibers.*

Proof. The number field case was proved by Borel and Serre [**BS64**, Theorem 7.1]. For the global function field case, see [**Nis79**], [**BP90**, §4], [**Oes84**, IV, 2.6, Proposition(a)], and [**Con12b**, Theorem 1.3.3(i)]. □

Remark 5.12.30. The analogue of Theorem 5.12.29 for abelian varieties is a conjecture; see Conjecture 5.7.32.

Theorem 5.12.31 (Kneser, Harder, Chernousov)**.** *Let G be a simply connected semisimple group over a global field k. Then the map*

$$\mathrm{H}^1(k,G) \longrightarrow \prod_v \mathrm{H}^1(k_v,G) \simeq \prod_{\text{real } v} \mathrm{H}^1(k_v,G)$$

is a bijection. In particular, if k is a totally imaginary number field or a global function field, then $\mathrm{H}^1(k,G) = 0$.

Proof. By Theorem 5.12.24(b), $\mathrm{H}^1(k_v,G)$ is trivial for each nonreal place v. For the number field case, see [**PR94**, Theorem 6.6]. The statement $\mathrm{H}^1(k,G) = 0$ for a global function field is proved in [**Har75**]. □

Theorem 5.12.32 (Voskresenskii)**.** *Let T be a torus of dimension at most 2 over a global field k. Then $\text{Ш}^1(k,T) = 0$.*

Sketch of proof. One classifies all finite subgroups of $\mathrm{GL}_d(\mathbb{Z})$ for $d \leq 2$ to classify all possibilities for T, and one checks the result in each case; see [**Vos65**] for the details. □

Unofficial version for inidental online use

Exercises

5.1. (Center of a group scheme vs. center of its group of points) Over a field k, let $\{\pm 1\}$ denote the constant group scheme associated to a two-element group (view 1 and -1 as symbols that are distinct even if $\operatorname{char} k = 2$). Let $\{\pm 1\}$ act on $\mathbb{G}_m$ so that -1 acts as $x \mapsto x^{-1}$. Let G be the semidirect product $\mathbb{G}_m \rtimes \{\pm 1\}$ over k. Let Z be the center of G.

(a) Prove that $Z \simeq \boldsymbol{\mu}_2$.

(b) Show that if $k = \mathbb{F}_2$, then $Z(k)$ is strictly smaller than the center of $G(k)$.

5.2. Let S be a scheme.

(a) Prove that the group schemes $\mathrm{U}_{n,S}$ and $\mathbb{G}_{a,S}^{n(n-1)/2}$ over S have the same underlying S-scheme.

(b) Prove that if S is nonempty and $n \geq 3$, they are not isomorphic as group schemes.

5.3. (Group schemes of order p) Let k be a field of characteristic p. Show that $\boldsymbol{\mu}_p$, $\boldsymbol{\alpha}_p$, and the constant group scheme $\mathbb{Z}/p\mathbb{Z}$ over k are pairwise nonisomorphic as group schemes over k.

5.4. ("Inseparable twist" of $\mathbb{G}_a$) Let k be a field of characteristic p, and suppose that $t \in k - k^p$. (So in particular, k is not perfect.) Let G be the k-subvariety of $\mathbb{G}_a^2$ defined by the equation $y^p = tx^p + x$. Prove that

(a) G is a subgroup scheme of $\mathbb{G}_a^2$.

(b) $G_{\overline{k}} \simeq \mathbb{G}_{a,\overline{k}}$ as $\overline{k}$-group schemes.

(c) G is not isomorphic to the k-group scheme $\mathbb{G}_a$.

(d) G as a k-variety (without group structure) is not isomorphic to $\mathbb{A}^1$.

(e) G is birational to $\mathbb{A}^1$ over k if and only if $p = 2$.

5.5. (Coordinate-free variant of GL_n) Let k be a field, and let V be a finite-dimensional k-vector space. For each k-algebra A, define $\mathrm{GL}_V(A)$ to be the group of A-module automorphisms of $V \otimes_k A$. Prove that the functor GL_V is represented by an algebraic group.

5.6. (Representations of $\mathbb{G}_m$) Let G be an algebraic group over a field k. A (finite-dimensional) **representation** of G is a finite-dimensional k-vector space V equipped with a homomorphism $G \to \mathrm{GL}_V$ of algebraic groups. Prove that giving a representation of $\mathbb{G}_m$ on a vector space V is equivalent to giving a direct sum decomposition $V = \bigoplus_{n \in \mathbb{Z}} V_n$ into subspaces indexed by $\mathbb{Z}$. (*Hint*: Given a decomposition, define an

Unofficial version for incidental online use

action of $\mathbb{G}_m$ on V such that each $a \in k$ act as multiplication-by-a^n on V_n and likewise for elements of k-algebras.)

5.7. (Hodge structures [**Del71**, 2.1])

(a) Define the **Deligne torus** $\mathbb{S} := \operatorname{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m$. Prove that there is a unique isomorphism $\mathbb{S}_{\mathbb{C}} \xrightarrow{\sim} \mathbb{G}_m \times \mathbb{G}_m$ of algebraic groups over $\mathbb{C}$ such that the induced homomorphism

$$\mathbb{C}^\times = \mathbb{S}(\mathbb{R}) \hookrightarrow \mathbb{S}(\mathbb{C}) \longrightarrow (\mathbb{G}_m \times \mathbb{G}_m)(\mathbb{C}) = \mathbb{C}^\times \times \mathbb{C}^\times$$

is $z \mapsto (z, \bar{z})$.

(b) Let V be an $\mathbb{R}$-vector space. Complex conjugation acts on the space $V_{\mathbb{C}} := V \otimes_{\mathbb{R}} \mathbb{C}$ through the second factor. Let W be a $\mathbb{C}$-subspace of $V_{\mathbb{C}}$. Let $\overline{W}$ be the image of W under complex conjugation. Prove that $\overline{W}$ is another $\mathbb{C}$-subspace of $V_{\mathbb{C}}$.

(c) A **Hodge structure** over $\mathbb{R}$ is a finite-dimensional representation of $\mathbb{S}$. Prove that giving a Hodge structure is the same as giving a finite-dimensional $\mathbb{R}$-vector space V equipped with a direct sum decomposition $V_{\mathbb{C}} = \bigoplus_{(p,q)\in\mathbb{Z}^2} V^{pq}$ into $\mathbb{C}$-subspaces V^{pq} such that $V^{qp} = \overline{V^{pq}}$ for all $(p,q) \in \mathbb{Z}^2$.

5.8. The **cocharacter group** of a k-torus T is the $\mathfrak{G}_k$-module

$$\mathrm{Y}(T) := \operatorname{Hom}_{k_{\mathrm{s}}\text{-group schemes}}(\mathbb{G}_{m,k_{\mathrm{s}}}, T_{k_{\mathrm{s}}}).$$

(a) Describe the abelian group $\mathrm{Y}(T)$ stripped of its $\mathfrak{G}_k$-action.

(b) Define a bilinear $\mathfrak{G}_k$-equivariant pairing

$$\mathrm{X}(T) \times \mathrm{Y}(T) \to \mathbb{Z},$$

and show that it identifies each of $\mathrm{X}(T)$ and $\mathrm{Y}(T)$ with the $\mathbb{Z}$-dual of the other.

(c) Restate Theorem 5.5.7 using $\mathrm{Y}(T)$ instead of $\mathrm{X}(T)$.

(*Remark*: One advantage of $\mathrm{X}(T)$ over $\mathrm{Y}(T)$ is that it can be used also in the generalization given in Theorem 5.5.10.)

5.9. Compute $\operatorname{Hom}(\boldsymbol{\mu}_n, \mathbb{G}_m)$ in the category of algebraic groups over a field k.

5.10. Let T be a group of multiplicative type over a field k. Prove that T is smooth if and only if either $\operatorname{char} k = 0$, or $\operatorname{char} k = p$ and $\mathrm{X}(T)$ has no nontrivial elements of order p.

5.11. Let $k = \mathbb{F}_2(t)$. Let $f\colon \mathbb{G}_a \to \mathbb{G}_a$ be the homomorphism $x \mapsto x^4 - tx^2$. Let $G = \ker f$.

(a) Prove that $G^0 \simeq \boldsymbol{\alpha}_2$.

(b) Prove that G_{red} is not a subgroup scheme of G.

5.12. Let k be a field. Let $n \geq 1$. Let $A = k[\epsilon]/(\epsilon^n)$. Let $G = \operatorname{Res}_{A/k} \mathbb{G}_m$. Prove that there exists a unipotent group U of dimension $n-1$ and

Unofficial version for incidental online use

an exact sequence

$$1 \to U \to G \to \mathbb{G}_m \to 1$$

of smooth algebraic groups.

5.13. (Example of a pseudo-reductive group) Let k be a separably closed field of characteristic p having a field extension L of degree p. Let $G = \operatorname{Res}_{L/k} \mathbb{G}_m$.
(a) Prove that $\dim \mathscr{R}_u(G_{\overline{k}}) = p - 1$.
(b) Prove that $G(k)$ has no nontrivial elements of order p.
(c) Prove that $\mathscr{R}_u(G) = \{1\}$.
(d) Deduce that G is pseudo-reductive but not reductive.
For a generalization, see [**CGP10**, Example 1.1.3].

5.14. (Failure of real approximation) Let T be the torus $x^2 + 2y^2 = 1$ of Example 5.5.3. Let G be the kernel of the cubing map $T \xrightarrow{3} T$. Prove that $G(\mathbb{Q})$ is not dense in $G(\mathbb{R})$.

5.15. Let G be a smooth algebraic group over a field k. Let $\mathbf{G}$ be the trivial right G-torsor. Prove that there is an isomorphism $G(k) \simeq \operatorname{Aut} \mathbf{G}$.

5.16. Let X be a geometrically integral k-variety with a k-point x. Prove that the category $\mathcal{C}_{X,x}$ of Section 5.7.2 is equivalent to the category $\mathcal{C}_X$ of Example 5.12.11, and that the two definitions of $\operatorname{Alb}_{X/k}$ are compatible.

5.17. Let k be a field. (Assume $\operatorname{char} k \neq 2$ if you want to make the problem easier.)
(a) Find explicit equations for all 1-dimensional tori T over k.
(b) For each T, find explicit equations for all T-torsors over k.

5.18. Prove that any smooth connected algebraic group G over a field k is geometrically integral.

5.19. Use Theorem 5.12.19(a) to give another proof of Wedderburn's theorem that every finite division ring is commutative, or equivalently, that the Brauer group of a finite field is trivial.

5.20. In [**Lan56**], Lang proved a stronger version of Theorem 5.12.19(a). Specifically, he proved that any *homogeneous space* X of a smooth connected algebraic group G over a finite field k has a k-point. Prove this.

5.21. Let k be a finite field. Let G be an algebraic group over k.
(a) Prove that $\mathrm{H}^1(k, G)$ is finite.
(*Hint*: To handle the noncommutative case, use [**Ser02**, I.§5.5, Corollary 2].)
(b) Give an example to show that $\mathrm{H}^1(k, G)$ can have more than one element.

Unofficial version for incidental online use

5.22. (Extensions and torsors) Let G be a smooth *commutative* algebraic group over a field k, with group law written additively. An **extension** of the constant group scheme $\mathbb{Z}$ by G (in the category of commutative k-group schemes) is a commutative k-group scheme E fitting in an exact sequence

$$0 \to G \to E \to \mathbb{Z} \to 0.$$

A **morphism of extensions** is a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & G \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & G \arrow[r] & E' \arrow[r] & \mathbb{Z} \arrow[r] & 0. \end{tikzcd}$$

Given an extension, write $E = \coprod_{n\in\mathbb{Z}} E_n$, where E_n is the inverse image under $E \to \mathbb{Z}$ of the point corresponding to the integer n.

(a) Prove that each E_n is a G-torsor.

(b) Prove that

$$\begin{aligned} \{\,\text{extensions of } \mathbb{Z} \text{ by } G\,\} &\longrightarrow \{\,G\text{-torsors over } k\,\} \\ (0 \to G \to E \to \mathbb{Z} \to 0) &\longmapsto E_1 \end{aligned}$$

defines an equivalence of categories. Deduce that the set of isomorphism classes of extensions is in bijection with $\mathrm{H}^1(k, G)$.

(c) Prove that any extension induces an exact sequence of $\mathfrak{G}_k$-modules

$$0 \to G(k_{\mathrm{s}}) \to E(k_{\mathrm{s}}) \to \mathbb{Z} \to 0$$

and that the image of n under the coboundary homomorphism $\mathbb{Z} = \mathrm{H}^0(\mathfrak{G}_k, \mathbb{Z}) \to \mathrm{H}^1(k, G)$ is $[E_n]$.

(*Remark*: Similarly, a 2-**extension**

$$0 \to G \to E_1 \to E_0 \to \mathbb{Z} \to 0$$

gives rise to a class in $\mathrm{H}^2(k, G)$, and so on; this is related to the notion of **gerbe**.)

Unofficial version for incidental online use

Unofficial version for incidental online use

Chapter 6

Étale and fppf cohomology

(References: [**SGA** $4\frac{1}{2}$], [**Mil80**], [**FK88**], [**Tam94**])

Étale cohomology was developed by M. Artin and Grothendieck for reasons to be discussed in Section 6.1. To set up the foundations of étale cohomology properly would require a whole book. In fact, there are several books about this, cited above. We will only introduce some of the key concepts and definitions. Many results will be cited without proof.

In this chapter, schemes are assumed to be separated and locally noetherian.

Unofficial version for incidental online use

6.1. The reasons for étale cohomology

6.1.1. Generalization of Galois cohomology. Étale cohomology over $\operatorname{Spec} k$ is the same as Galois cohomology, so étale cohomology over more general schemes can be thought of as a generalization of Galois cohomology. More precisely, it will turn out that any abelian sheaf $\mathscr{F}$ for the étale topology on $\operatorname{Spec} k$ gives rise to a continuous $\mathfrak{G}_k$-module called $\mathscr{F}(k_s)$ (and vice versa), and the étale cohomology group $\mathrm{H}^i_{\mathrm{et}}(\operatorname{Spec} k, \mathscr{F})$ equals the Galois cohomology group $\mathrm{H}^i(\mathfrak{G}_k, \mathscr{F}(k_s))$. See Theorem 6.4.6.

For instance, in Section 5.12 we saw that torsors under a smooth algebraic group A over k could be classified by the Galois cohomology set $\mathrm{H}^1(\mathfrak{G}_k, A(k_s))$. To classify torsors under group schemes over a more general scheme S we need étale cohomology.

One can also generalize the cohomological description of the Brauer group of a field, to define the Brauer group of an arbitrary scheme.

6.1.2. Comparison with classical cohomology theories. Given a compact complex manifold X, one can define singular cohomology groups $\mathrm{H}^i(X, \mathbb{Z})$, $\mathrm{H}^i(X, \mathbb{Z}/n\mathbb{Z})$, and so on. One can also define cohomology of coherent analytic sheaves; this can be useful in proving the existence of global meromorphic functions on compact complex manifolds, for instance. These cohomology theories use the analytic topology on X.

It would be nice if these cohomology theories worked for varieties over other fields. But one does not usually have an analytic topology on such a variety, so one needs to find substitutes. To measure the success of a cohomology theory, we check whether for proper $\mathbb{C}$-varieties it gives the same answers as the classical topological cohomology theories such as singular cohomology.

It turns out that the Zariski topology on a proper variety gives the right answers for cohomology of coherent sheaves; see [**Ser55**] or [**Har77**, Theorem B.2.1]. But the Zariski topology is not fine enough to give the right answers for constant coefficients. For instance, if X is a nice $\mathbb{C}$-curve of genus g, then the singular cohomology group $\mathrm{H}^1(X(\mathbb{C}), \mathbb{Z})$ and the sheaf cohomology group $\mathrm{H}^1(X^{\mathrm{an}}, \mathbb{Z})$ for the analytic topology both give $\mathbb{Z}^{2g}$, which should be considered the right answer; but if we use the Zariski topology on X, and let $\mathbb{Z}$ be the constant sheaf $\mathbb{Z}$ on X, then $\mathrm{H}^1(X, \mathbb{Z}) = 0$ since $\mathbb{Z}$ is flasque [**Har77**, Proposition III.2.5]. Again, the problem is that the Zariski topology has too few open subsets in comparison with the analytic topology.

To obtain a sufficiently fine topology on a scheme, one must be open-minded about what a topology is, and in particular about what open subsets and open coverings are; see Section 6.2. The "topologies" that follow are not topologies in the usual sense.

The étale topology on X, which is finer than the Zariski topology, is a substitute for the analytic topology, and has an associated cohomology theory. Étale cohomology does not give the right answer for $\mathrm{H}^1(X, \mathbb{Z})$, but it does give the right answers for cohomology with a finite abelian group as coefficients, at least when the order of the group is not divisible by the characteristic. For instance, if X is a nice curve of genus g over an algebraically closed field k, and n is an integer not divisible by $\operatorname{char} k$, then we get the right answer $\mathrm{H}^1_{\mathrm{et}}(X, \mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$. One can also define an even finer topology, the fppf topology, which lets one remove the restriction on the characteristic.

Unofficial version for incidental online use

Étale cohomology with coefficients in some rings of characteristic 0 can be defined by taking an inverse limit; for instance,

$$\mathrm{H}^i_{\mathrm{et}}(X, \mathbb{Z}_\ell) := \varprojlim_n \mathrm{H}^i_{\mathrm{et}}(X, \mathbb{Z}/\ell^n\mathbb{Z}).$$

This is important for an application to the Weil conjectures; see Chapter 7. Other applications of étale and fppf cohomology, to torsors and to Brauer groups of schemes, are given toward the end of Chapter 6.

6.2. Grothendieck topologies

(Reference: [**Vis05**, §2.3])

Before the notion of a topology on a set was invented, people studied metric spaces. Then people noticed that many properties of metric spaces could be defined without reference to the metric; for many purposes, just knowing which subsets were open was enough. This led to the definition of a topology on a set, in which an arbitrary collection of subsets could be decreed to be the open sets, provided that the collection satisfied some axioms modeled after the *theorems* about open sets in metric spaces. (See [**Moo08**] for the history.)

Grothendieck took this one step further by observing that sometimes one does not even need to know the open subsets: for many purposes (for instance, the concept of a sheaf), it suffices to have a notion of *open covering*. This led to the notion of a Grothendieck topology, which is usually not a topology in the standard sense. Just as an open set in a topological space need not be open relative to any metric, an open covering in a Grothendieck topology need not consist of actual open subsets!

This relaxation of the notion of open covering is necessary to obtain a sufficiently fine topology on a scheme.

Remark 6.2.1. This point of view was used already in Chapter 4.

Definition 6.2.2. Let $\mathcal{C}$ be a category. (Our set-theoretic conventions are such that the collection of objects in each category is a set; see Section A.4.) We consider all families of morphisms $\{U_i \to U\}_{i \in I}$ in $\mathcal{C}$ having a common target. A **Grothendieck (pre)topology** on $\mathcal{C}$ is a set $\mathcal{T}$ whose elements are *some* of these families (the families that do belong to $\mathcal{T}$ are called the **open coverings**), satisfying the following axioms:

(i) Isomorphisms are open coverings: If $U' \to U$ is an isomorphism, then the one-element family $\{U' \to U\}$ belongs to $\mathcal{T}$.

(ii) An open covering of an open covering is an open covering: If $\{U_i \to U\}$ belongs to $\mathcal{T}$ and $\{V_{ij} \to U_i\}$ belongs to $\mathcal{T}$ for each i, then $\{V_{ij} \to U\}$ belongs to $\mathcal{T}$.

Unofficial version for incidental online use

(iii) A base extension of an open covering is an open covering: If $\{U_i \to U\}$ belongs to $\mathcal{T}$ and $V \to U$ is a morphism, then the fiber products $V \times_U U_i$ exist and $\{V \times_U U_i \to V\}$ belongs to $\mathcal{T}$.

Remark 6.2.3. There is another approach, using **sieves**, which has advantages and disadvantages, one disadvantage being that it is farther from geometric intuition. The definition of Grothendieck topology in [**SGA** $4_{\mathbf{I}}$, II.1.1] is in terms of sieves. A Grothendieck pretopology gives rise to a Grothendieck topology, and all the Grothendieck topologies we will use arise this way. From now on, we will abuse terminology and call a pretopology a topology, as is commonly done.

Definition 6.2.4. A pair $(\mathcal{C}, \mathcal{T})$ consisting of a category $\mathcal{C}$ and a Grothendieck topology $\mathcal{T}$ on $\mathcal{C}$ is called a **site**.

6.2.1. The Zariski site. Let X be a topological space. Let $\mathcal{C}$ be the category whose objects are the open sets in X, and such that for any $U, V \in \mathcal{C}$,

$$\operatorname{Hom}(U,V) = \begin{cases} \{i\}, & \text{if } U \subseteq V, \text{ and } i\colon U \to V \text{ is the inclusion,} \\ \emptyset, & \text{otherwise.} \end{cases}$$

Let $\mathcal{T}$ be the collection of families $\{U_i \to U\}$ such that $\bigcup_i U_i = U$. Then $\mathcal{T}$ is a Grothendieck topology on $\mathcal{C}$, called the **classical Grothendieck topology**.

Let X be a scheme. The **(small) Zariski site** X_{Zar} is the site associated to the underlying topological space $\operatorname{sp}(X)$.

6.2.2. The (small) étale site. Fix a scheme X. Take $\mathcal{C}$ to be the category $\mathbf{Et}_X$ whose objects are schemes U equipped with an étale morphism $U \to X$ and whose morphisms are X-morphisms. (These morphisms will automatically be étale [**SP**, Tag 02GW].) Call a family $\{\phi_i\colon U_i \to U\}$ of morphisms in $\mathcal{C}$ an open covering if $\bigcup_i \phi_i(U_i) = U$ as topological spaces. This defines the **(small) étale site** X_{et}.

Remark 6.2.5. For the **big étale site**, one would take $\mathcal{C} = \mathbf{Schemes}_X$. Open coverings are defined as families of étale morphisms $\{\phi_i\colon U_i \to U\}$ such that $\bigcup_i \phi_i(U_i) = U$. The definitions of sheaves and cohomology (see Sections 6.3.2 and 6.4.1) make sense for both the small and the big étale sites. But the cohomology of a big étale sheaf equals the cohomology of its restriction to the small étale site [**SP**, Tag 03YX], and the small étale site is easier to work with, so the small étale site is generally preferred.

6.2.3. The (big) fppf and fpqc sites. Fix a scheme X. Take $\mathcal{C} = \mathbf{Schemes}_X$. An open covering is a family $\{\phi_i\colon U_i \to U\}$ of X-morphisms such that $\coprod U_i \to U$ is fppf (respectively, fpqc). This defines the **(big) fppf site** X_{fppf} (respectively, the **(big) fpqc site** X_{fpqc}).

Unofficial version for incidental online use

Remark 6.2.6. By the étale site, we will always mean the *small* étale site. By the fppf or fpqc site, we will always mean the *big* site. (Here is one reason for this. For the small étale site, morphisms between objects are automatically étale [**SP**, Tag 02GW], as mentioned already in Section 6.2.2. But if one considered the small fppf site, by taking $\mathcal{C}$ to be the category of fppf X-schemes with X-morphisms, it would not be automatic that X-morphisms between objects were fppf—for example, all k-varieties are fppf over $\operatorname{Spec} k$, but a k-morphism between two k-varieties need not be flat. The same problem arises with fpqc.)

6.2.4. Continuous maps of sites.

Definition 6.2.7. A **continuous map of sites** $(\mathcal{C}', \mathcal{T}') \to (\mathcal{C}, \mathcal{T})$ is a functor in the *opposite direction* $F \colon \mathcal{C} \to \mathcal{C}'$ respecting open coverings, in the following sense:

(1) for every open covering $\{U_i \to U\}$ in $\mathcal{T}$, collection $\{FU_i \to FU\}$ is an open covering in $\mathcal{T}'$, and
(2) for every open covering $\{U_i \to U\}$ in $\mathcal{T}$ and $\mathcal{C}$-morphism $V \to U$, the $\mathcal{C}'$-morphism $F(V \times_U U_i) \to FV \times_{FU} FU_i$ is an isomorphism.

The reversal of direction makes the definition compatible with maps of topological spaces:

Example 6.2.8. Let $f \colon X' \to X$ be a continuous map of topological spaces. Equip the categories of open subsets of X and X' with the classical Grothendieck topologies to obtain sites $(\mathcal{C}, \mathcal{T})$ and $(\mathcal{C}', \mathcal{T}')$. Then f induces a continuous map of sites $(\mathcal{C}', \mathcal{T}') \to (\mathcal{C}, \mathcal{T})$: the functor $\mathcal{C} \to \mathcal{C}'$ takes an open subset U of X to the open subset $f^{-1}U$ of X'.

If a set X is equipped with topologies $\mathcal{T}'$ and $\mathcal{T}$ (in the usual sense) and $\mathcal{T}'$ is finer (more open sets) than $\mathcal{T}$, then the identity map $(X, \mathcal{T}') \to (X, \mathcal{T})$ is a continuous map of topological spaces. Similarly:

Example 6.2.9. For any scheme X, Proposition 3.8.2 yields continuous maps

$$X_{\mathrm{fpqc}} \to X_{\mathrm{fppf}} \to X_{\mathrm{et}} \to X_{\mathrm{Zar}}.$$

Remark 6.2.10. There is a more restrictive notion, called a **morphism of sites**. This is a continuous map of sites for which the inverse image functor on the categories of sheaves is exact; see [**SP**, Tag OOX1]. The maps in Example 6.2.9 are morphisms of sites.

6.3. Presheaves and sheaves

6.3.1. Presheaves.

Unofficial version for incidental online use

Definition 6.3.1. A **presheaf of abelian groups** (or **abelian presheaf**) $\mathscr{F}$ on a category $\mathcal{C}$ is a functor

$$\begin{aligned} \mathcal{C}^{\mathrm{opp}} &\longrightarrow \mathbf{Ab} \\ U &\longmapsto \mathscr{F}(U). \end{aligned}$$

An element of $\mathscr{F}(U)$ is called a **section of $\mathscr{F}$ over U**. A **morphism of presheaves** is a morphism of functors.

Remark 6.3.2. Similarly, one may define a **presheaf of sets**, a **presheaf of groups**, and so on.

Example 6.3.3. If $\mathcal{C}$ is the category of open subsets of a topological space (Section 6.2.1), then we get the same notion of presheaf as in [**Har77**, II.§1]. (The condition $\mathscr{F}(\emptyset) = 0$ there is unnatural and should be deleted.) For this reason, for arbitrary $\mathcal{C}$, the homomorphism $\mathscr{F}(U) \to \mathscr{F}(V)$ induced by a morphism $V \to U$ of $\mathcal{C}$ is called the **restriction** from U to V and is denoted $s \mapsto s|_V$, even though V might not be an actual subset of U.

Example 6.3.4. Let A be an abelian group. The **constant presheaf** A on a category $\mathcal{C}$ is the functor $\mathscr{F}$ such that $\mathscr{F}(U) = A$ for all $U \in \mathcal{C}$, and such that $\mathscr{F}$ takes each morphism in $\mathcal{C}$ to the identity $A \to A$.

6.3.2. Sheaves.

Definition 6.3.5. Let A, B, C be sets, and let $f \colon A \to B$, $g \colon B \to C$, and $h \colon B \to C$ be functions. Then

$$A \xrightarrow{f} B \underset{h}{\overset{g}{\rightrightarrows}} C$$

is called **exact** if

(i) f is injective, and
(ii) $f(A)$ equals the **equalizer** $\{b \in B : g(b) = h(b)\}$ of g and h.

Example 6.3.6. If A, B, C are abelian groups and f, g, h are homomorphisms, then

$$A \xrightarrow{f} B \underset{h}{\overset{g}{\rightrightarrows}} C$$

is exact if and only if the sequence of abelian groups

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g-h} C$$

is exact.

Definition 6.3.7. Let $\mathscr{F}$ be a presheaf on a site $(\mathcal{C}, \mathcal{T})$. Then $\mathscr{F}$ is a **sheaf** if and only if

$$\mathscr{F}(U) \to \prod_i \mathscr{F}(U_i) \rightrightarrows \prod_{i,j} \mathscr{F}(U_i \times_U U_j) \qquad (6.3.8)$$

Unofficial version for internal online use

is exact for all open coverings $\{U_i \to U\}$ in $\mathcal{T}$. (Here the two arrows on the right correspond to the two projections, from $U_i \times_U U_j$ to U_i and to U_j.) A **morphism of sheaves** $\mathscr{F} \to \mathscr{G}$ is simply a morphism of presheaves.

Example 6.3.9. If $\mathcal{T}$ is the classical Grothendieck topology on a topological space, then the sheaf condition says

(i) an element $s \in \mathscr{F}(U)$ is determined by its restriction to an open covering, and

(ii) given elements $s_i \in \mathscr{F}(U_i)$ for an open covering $\{U_i \to U\}$ that are compatible (they agree on pairwise intersections), one can glue to obtain an element $s \in \mathscr{F}(U)$ whose restriction to U_i is s_i for each i.

Remark 6.3.10. Suppose that $\{U_i \to U\}$ is an open covering in one of the sites X_{et}, X_{fppf}, or X_{fpqc}. Let $U' = \coprod U_i$ and $U'' = U' \times_U U'$. If a presheaf $\mathscr{F}$ already satisfies $\mathscr{F}(U') = \prod \mathscr{F}(U_i)$, then exactness of (6.3.8) is equivalent to exactness for the open covering consisting of the single morphism $U' \to U$, the exactness of

$$\mathscr{F}(U) \to \mathscr{F}(U') \rightrightarrows \mathscr{F}(U''). \tag{6.3.11}$$

Definition 6.3.12. An **abelian sheaf** is a sheaf of abelian groups. A **group sheaf** is a sheaf of groups.

6.3.3. Examples of sheaves. Here we show that some presheaves arising commonly in algebraic geometry are fpqc sheaves. The sheaf property in each case turns out to be a consequence of fpqc descent.

Definition 6.3.13. Let X be a scheme, and let $\mathcal{C}$ be a subcategory of $\mathbf{Schemes}_X$. Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module; in particular, $\mathscr{F}$ is a sheaf on X_{Zar}. Define a presheaf $\mathscr{F}_{\mathcal{C}}$ on $\mathcal{C}$ by

$$\mathscr{F}_{\mathcal{C}}(U) := (p^*\mathscr{F})(U) = \operatorname{Hom}(p^*\mathscr{O}_X, p^*\mathscr{F})$$

for each object $U \xrightarrow{p} X$ of $\mathcal{C}$.

Example 6.3.14. Take $\mathcal{C}$ to be the underlying category of X_{fpqc}; then Definition 6.3.13 extends a quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ to a presheaf $\mathscr{F}_{\text{fpqc}}$ on X_{fpqc}.

Proposition 6.3.15. *Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module on a scheme X. Then the presheaf $\mathscr{F}_{\text{fpqc}}$ on X_{fpqc} in Example 6.3.14 is an abelian sheaf. (And hence the same is true on X_{Zar}, X_{et}, and X_{fppf}. Of course, this is trivial for X_{Zar}, on which $\mathscr{F}_{\text{Zar}} = \mathscr{F}$.)*

Proof. By Remark 6.3.10, it suffices to check exactness of (6.3.11) for each fpqc morphism $p\colon S' \to S$ of X-schemes. For this, we may replace $\mathscr{F}$ by

Unofficial version for incidental online use

its restriction to S, which we now rename $\mathscr{F}$. Let $S'' = S' \times_S S'$, and let $q\colon S'' \to S$ be the projection. Then (6.3.11) for $\mathscr{F}_{\mathrm{fpqc}}$ is

$$\operatorname{Hom}(\mathscr{O}_S, \mathscr{F}) \to \operatorname{Hom}(p^*\mathscr{O}_S, p^*\mathscr{F}) \rightrightarrows \operatorname{Hom}(q^*\mathscr{O}_S, q^*\mathscr{F}).$$

This is exact, because Theorem 4.2.3 implies that the functor from quasi-coherent S-modules to quasi-coherent S'-modules with descent data is fully faithful. □

Proposition 6.3.16. *Let S be a scheme, and let X and Y be S-schemes. Then the functor $U \mapsto \operatorname{Hom}_U(X_U, Y_U)$ is a sheaf of sets on S_{fpqc}, denoted* $\mathbf{Hom}(X, Y)$.

Proof. Remark 6.3.10 lets us reduce to showing that for each fpqc morphism $p\colon U' \to U$ of S-schemes, if $U'' := U' \times_U U'$, then

$$\operatorname{Hom}_U(X_U, Y_U) \to \operatorname{Hom}_{U'}(X_{U'}, Y_{U'}) \rightrightarrows \operatorname{Hom}_{U''}(X_{U''}, Y_{U''}) \tag{6.3.17}$$

is exact. The map from $\operatorname{Hom}_U(X_U, Y_U)$ to the equalizer sends a U-morphism $X_U \to Y_U$ to the morphism between the associated U'-schemes with descent data; this map is a bijection by Theorem 4.3.5(i). Thus (6.3.17) is exact. □

Corollary 6.3.18. *Let S be a scheme, and let X be an S-scheme. The functor $U \mapsto \operatorname{Aut}_U(X_U)$ is a group sheaf on S_{fpqc}.*

Proof. By Proposition 6.3.16, the monoid presheaf $\mathbf{Hom}(X, X)$ is a sheaf. Take the subgroup of invertible elements in each monoid. □

Recall from Definition 2.3.3 that if X is a scheme and Y is an X-scheme, then the functor of points $h_Y\colon \mathbf{Schemes}_X^{\mathrm{opp}} \to \mathbf{Sets}$ is defined by $h_Y(U) := \operatorname{Hom}_X(U, Y)$.

Proposition 6.3.19. *Let S be a scheme, and let X be an S-scheme. Then the functor of points h_X, viewed as a presheaf on the fpqc site S_{fpqc}, is a sheaf (and hence the same is true for the Zariski, étale, fppf sites).*

Proof. Remark 6.3.10 lets us reduce to showing that for each fpqc morphism $p\colon U' \to U$ of S-schemes, if $U'' := U' \times_U U'$, then

$$\operatorname{Hom}_S(U, X) \to \operatorname{Hom}_S(U', X) \rightrightarrows \operatorname{Hom}_S(U'', X)$$

is exact. Applying Proposition 2.3.15 to each term rewrites this as

$$\operatorname{Hom}_U(U, X_U) \to \operatorname{Hom}_{U'}(U', X_{U'}) \rightrightarrows \operatorname{Hom}_{U''}(U'', X_{U''}),$$

which, as a special case of (6.3.17), is exact. □

Remark 6.3.20. If G is a *group* scheme over X, then h_G is a *group* sheaf. We sometimes write G when we mean the associated sheaf. For instance, the abelian sheaf $\mathbb{G}_a$ on X_{Zar} is the same as $\mathscr{O}_X$, and the abelian sheaf $\mathbb{G}_a$

Unofficial version for incidental online use

on X_{fpqc} is the same as $(\mathscr{O}_X)_{\text{fpqc}}$. Another example is the abelian sheaf $\mathbb{G}_m$ on X_{fpqc} sending each U to $\mathscr{O}_U(U)^\times$.

6.3.4. Sheafification.

Definition 6.3.21. A **sheafification** of a presheaf $\mathscr{F}$ is a sheaf $\mathscr{F}^+$ equipped a morphism $i\colon \mathscr{F} \to \mathscr{F}^+$ such that every presheaf morphism from $\mathscr{F}$ to a sheaf factors uniquely through i.

The definition implies that a sheafification is unique if it exists.

Proposition 6.3.22 (cf. [**Har77**, Proposition-Definition II.1.2])**.** *Let $\mathscr{F}$ be a presheaf on a site. Then the sheafification of $\mathscr{F}$ exists.*

Sketch of proof. Let $\mathscr{F}$ be a presheaf. Call two sections $s, t \in \mathscr{F}(U)$ equivalent if there exists an open covering $\{U_i \to U\}$ such $s|_{U_i} = t|_{U_i}$ for all i. This defines an equivalence relation. Let $\mathscr{F}_1(U)$ be the set of equivalence classes. Then $\mathscr{F}_1$ is another presheaf.

Loosely speaking, a section of $\mathscr{F}^+$ is something that is locally (for some open covering in the Grothendieck topology) a section of $\mathscr{F}_1$. More precisely, one should define $\mathscr{F}^+(U) := \check{\mathrm{H}}^0(U, \mathscr{F}_1)$ (the notation $\check{\mathrm{H}}^0$ is explained in Section 6.4.4). □

Remark 6.3.23. The Zariski, étale, and fppf topologies are *independent of the choice of universe* in the sense that

(1) any open covering can be refined to one in which all the morphisms $U_i \to U$ are open immersions, étale morphisms of finite presentation, or flat morphisms of finite presentation, respectively, and
(2) for any U, the isomorphism classes of such morphisms form a set that does not grow as one enlarges the universe.

The same is not true for fpqc morphisms. For instance, over $\operatorname{Spec} k$ one has the fpqc morphism $\operatorname{Spec} L \to \operatorname{Spec} k$, where L is the purely transcendental extension $k(\{t_i : i \in I\})$ for a set I of arbitrary cardinality, bounded only by the size of the universe. In the fpqc topology, even the sheafification of a presheaf can depend on the choice of universe [**Wat75**, Theorem 5.5, Remark (c)]. Because of this, in situations requiring sheafification, the fppf topology is preferred over the fpqc topology.

Definition 6.3.24. The constant presheaf A (on a Zariski, étale, fppf, or fpqc site) is usually not a sheaf, so we define the **constant sheaf** to be the sheafification of the constant presheaf.

Unofficial version for incidental online use

6.3.5. Exact sequences.

Definition 6.3.25. Let $\alpha\colon \mathscr{G} \to \mathscr{H}$ be a morphism of abelian sheaves on a site. Its **kernel** $\ker(\alpha)$ is defined as the presheaf $U \longmapsto \ker(\mathscr{G}(U) \to \mathscr{H}(U))$. It turns out to be a sheaf.

Warning 6.3.26. In contrast, the presheaf image $U \longmapsto \operatorname{im}(\mathscr{G}(U) \to \mathscr{H}(U))$ need not be a sheaf.

Definition 6.3.27. A sequence of abelian sheaves

$$\mathscr{F} \xrightarrow{\alpha} \mathscr{G} \xrightarrow{\beta} \mathscr{H}$$

on a site $(\mathcal{C}, \mathcal{T})$ with $\beta \circ \alpha = 0$ is called **exact** (at $\mathscr{G}$) if $\ker(\beta)$ is a sheafification of the presheaf image of α (for the natural morphism from this presheaf image to $\ker(\beta)$). In other words, the sequence is exact if for each $U \in \mathcal{C}$ and for each $g \in \mathscr{G}(U)$, we have $\beta(g) = 0$ if and only if there exist an open covering $\{U_i \to U\}$ and $f_i \in \mathscr{F}(U_i)$ with $\alpha(f_i) = g|_{U_i}$ for each i.

Remark 6.3.28. Let A, B, C be fppf group schemes over a scheme S. A sequence

$$A \to B \to C$$

of homomorphisms of group schemes over S is exact in the sense of Definition 5.1.18 if and only if the associated sequence of sheaves on S_{fppf} is exact. (One can make sense of this even if A, B, and C are noncommutative.)

6.4. Cohomology

6.4.1. The derived functor definition.

In this section we fix a scheme X and an element $\bullet$ of $\{\text{Zar}, \text{et}, \text{fppf}\}$, so that $X_\bullet$ is one of the sites we have defined. It turns out that the category of abelian sheaves on $X_\bullet$ has enough injectives.

Definition 6.4.1 (cf. [**Har77**, III.§1])**.** For $q \in \mathbb{N}$, define the functor

$$\begin{aligned} \{\text{abelian sheaves on } X_\bullet\} &\longrightarrow \mathbf{Ab} \\ \mathscr{F} &\longmapsto \mathrm{H}^q_\bullet(X, \mathscr{F}) \end{aligned}$$

as the qth right derived functor of the (left exact) global sections functor

$$\begin{aligned} \{\text{abelian sheaves on } X_\bullet\} &\longrightarrow \mathbf{Ab} \\ \mathscr{F} &\longmapsto \mathscr{F}(X). \end{aligned}$$

If $\mathscr{F}$ is an abelian sheaf on $X_\bullet$, then the abelian group $\mathrm{H}^q_\bullet(X, \mathscr{F})$ is called the q**th** $\begin{cases} \textsf{Zariski} \\ \textsf{étale} \\ \textsf{fppf} \end{cases}$ **cohomology group** of $\mathscr{F}$.

Unofficial version for incidental online use

In particular, for any exact sequence of abelian sheaves on $X_\bullet$

$$0 \to \mathscr{F} \to \mathscr{G} \to \mathscr{H} \to 0,$$

we get a long exact sequence

$$\begin{aligned}0 &\longrightarrow \mathrm{H}^0_\bullet(X,\mathscr{F}) \longrightarrow \mathrm{H}^0_\bullet(X,\mathscr{G}) \longrightarrow \mathrm{H}^0_\bullet(X,\mathscr{H})\\ &\longrightarrow \mathrm{H}^1_\bullet(X,\mathscr{F}) \longrightarrow \mathrm{H}^1_\bullet(X,\mathscr{G}) \longrightarrow \mathrm{H}^1_\bullet(X,\mathscr{H})\\ &\longrightarrow \cdots .\end{aligned}$$

Remark 6.4.2. For each abelian sheaf $\mathscr{F}$ on $X_\bullet = (\mathcal{C}, \mathcal{T})$ and for each "open subset" $U \in \mathcal{C}$, one can define $\mathrm{H}^q_\bullet(U,\mathscr{F})$ by taking the derived functors of $\Gamma(U,-)$. There is a canonical "pullback" homomorphism $\mathrm{H}^q_\bullet(X,\mathscr{F}) \to \mathrm{H}^q_\bullet(U,\mathscr{F})$. In fact,

$$\begin{aligned}\mathcal{C}^{\mathrm{opp}} &\longrightarrow \mathbf{Ab}\\ U &\longmapsto \mathrm{H}^q_\bullet(U,\mathscr{F})\end{aligned}$$

defines a presheaf called $\mathscr{H}^q(\mathscr{F})$.

Alternatively, one can restrict $\mathscr{F}$ to the site $U_\bullet$ and take $\mathrm{H}^q_\bullet(U,\mathscr{F}|_U)$. There is a canonical isomorphism

$$\mathrm{H}^q_\bullet(U,\mathscr{F}) \simeq \mathrm{H}^q_\bullet(U,\mathscr{F}|_U),$$

because one can show that the functor $\mathscr{F} \mapsto \mathscr{F}|_U$ takes injective sheaves on $X_\bullet$ to injective sheaves on $U_\bullet$; see [**Mil80**, III.1.10 and III.1.11].

6.4.2. Étale cohomology and limits. Exercise 1.17 stated that for a direct limit of fields $K = \varinjlim K_\alpha$, we have $\operatorname{Br} K = \varinjlim \operatorname{Br} K_\alpha$. There are various versions of this for schemes and étale cohomology, discussed in [**SGA** $4_{\mathbf{II}}$, VII, §5]. Here is one:

Theorem 6.4.3. *Let $(X_i)_{i\in I}$ be a filtered inverse system of schemes. Suppose that the X_i are quasi-compact and quasi-separated, and that the morphisms in the system are affine.*

(a) *The limit $X := \varprojlim X_i$ exists in the category of schemes.*

(b) *Suppose that $0 \in I$ and G_0 is a commutative group scheme of finite presentation over X_0. For $i \geq 0$, let $G_i = G_0 \times_{X_0} X_i$. Let $G = G_0 \times_{X_0} X$. For each $q \in \mathbb{N}$, the natural homomorphism*

$$\varinjlim \mathrm{H}^q_{\mathrm{et}}(X_i, G_i) \longrightarrow \mathrm{H}^q_{\mathrm{et}}(X, G)$$

is an isomorphism.

Proof. See [**SGA** $4_{\mathbf{II}}$, VII, Corollaire 5.9]. □

6.4.3. Étale cohomology and Galois cohomology. For this section, we fix a field k and a separable closure k_{s}. By Proposition 3.5.35, the only field

Unofficial version for incidental online use

extensions L of k for which $\operatorname{Spec} L \to \operatorname{Spec} k$ is étale are the finite separable extensions.

Definition 6.4.4. If $\mathscr{F}$ is a sheaf on $(\operatorname{Spec} k)_{\mathrm{et}}$, define $\mathscr{F}(k_{\mathrm{s}}) := \varinjlim \mathscr{F}(L)$, where the direct limit is over all finite separable extensions $L \supseteq k$ contained in k_{s}, and $\mathscr{F}(L)$ means $\mathscr{F}(\operatorname{Spec} L)$.

Remark 6.4.5. We get the same direct limit if we take only finite Galois extensions $L \supseteq k$. Then $\mathfrak{G}_k$ acts continuously on each L, hence on each $\mathscr{F}(L)$. Thus $\mathscr{F}(k_{\mathrm{s}})$ is naturally a $\mathfrak{G}_k$-set.

Theorem 6.4.6 (Étale cohomology over a field)**.**

(i) *The functor*

$$\begin{aligned} \{\text{ sheaves of sets on } (\operatorname{Spec} k)_{\mathrm{et}} \} &\longrightarrow \{ \mathfrak{G}_k\text{-sets} \} \\ \mathscr{F} &\longmapsto \mathscr{F}(k_{\mathrm{s}}) \end{aligned}$$

is an equivalence of categories. The global section functor $\mathscr{F} \mapsto \mathscr{F}(k)$ *corresponds to functor that takes a* $\mathfrak{G}_k$*-set* M *to the set of invariants* $M^{\mathfrak{G}_k}$.

(ii) *The equivalence in part* (i) *restricts to an equivalence*

$$\{\text{ abelian sheaves on } (\operatorname{Spec} k)_{\mathrm{et}} \} \longrightarrow \{ \mathfrak{G}_k\text{-modules} \}.$$

(iii) *There are natural isomorphisms*

$$\mathrm{H}^q_{\mathrm{et}}(\operatorname{Spec} k, \mathscr{F}) \simeq \mathrm{H}^q(\mathfrak{G}_k, \mathscr{F}(k_{\mathrm{s}}))$$

for all $q \in \mathbb{N}$.

Proof.

(i) We describe an inverse functor. Let S be a $\mathfrak{G}_k$-set. For each finite separable extension $L \supseteq k$ contained in k_{s}, define $\mathscr{F}(L) = S^{\operatorname{Gal}(k_{\mathrm{s}}/L)}$. By Proposition 3.5.35, every étale k-scheme U is a disjoint union of k-schemes of the form $\operatorname{Spec} L$, and we define $\mathscr{F}(U)$ as the corresponding product of the sets $\mathscr{F}(L)$. The restriction morphisms are products of inclusion morphisms

$$\mathscr{F}(L) = S^{\operatorname{Gal}(k_{\mathrm{s}}/L)} \hookrightarrow S^{\operatorname{Gal}(k_{\mathrm{s}}/M)} = \mathscr{F}(M)$$

for finite separable extensions L/M of finite separable extensions of k contained in k_{s}. The rest of the proof of (i) is easy.

(ii) This is obvious from (i).

(iii) Under (ii), the global sections functor corresponds to the $\mathfrak{G}_k$-invariants functor. Take derived functors on both sides. $\square$

Unofficial version for incidental online use

6.4.4. Čech cohomology. Let $\mathcal{U} = \{U_i \to U\}_{i\in I}$ be an open covering on some site $\mathcal{S}$. For $(i_0, \dots, i_p) \in I^{p+1}$, define

$$U_{i_0\dots i_p} := U_{i_0} \underset{U}{\times} U_{i_1} \underset{U}{\times} \cdots \underset{U}{\times} U_{i_p}.$$

If $(i_0, \dots, i_p) \in I^{p+1}$ and $j \in \{0, \dots, p\}$, then forgetting the jth factor gives a projection $U_{i_0\dots i_p} \to U_{i_0\dots\widehat{i_j}\dots i_p}$, where the $\widehat{\ }$ means that that index is omitted. We obtain

$$\textstyle\coprod_{i_0} U_{i_0} \leftleftarrows \coprod_{i_0 i_1} U_{i_0 i_1} \;\substack{\leftarrow\\ \leftarrow\\ \leftarrow}\; \coprod_{i_0 i_1 i_2} U_{i_0 i_1 i_2} \;\substack{\leftarrow\\ \leftarrow\\ \leftarrow\\ \leftarrow}\; \cdots .$$

Let $\mathscr{F}$ be an abelian presheaf on $\mathcal{S}$. Then we obtain

$$\textstyle\prod_{i_0} \mathscr{F}(U_{i_0}) \rightrightarrows \prod_{i_0 i_1} \mathscr{F}(U_{i_0 i_1}) \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow}\; \prod_{i_0 i_1 i_2} \mathscr{F}(U_{i_0 i_1 i_2}) \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow\\ \rightarrow}\; \cdots .$$

Relabel these products as C^0, C^1, and so on, and combine each stack of arrows by taking their alternating sum to obtain homomorphisms d^q:

$$C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \xrightarrow{d^2} \cdots .$$

Definition 6.4.7. The elements of C^q, $\ker(d^q)$, $\operatorname{im}(d^{q-1})$, respectively, are called **Čech q-cochains**, **Čech q-cocycles**, and **Čech q-coboundaries**.

One can check that the composition $d^q \circ d^{q-1}$ of any two successive homomorphisms is zero, so we have a *complex*. Take the cohomology groups of this complex, and denote them

$$\check{\mathrm{H}}^q(\mathcal{U}, \mathscr{F}) = \frac{\ker d^q}{\operatorname{im} d^{q-1}},$$

where we interpret $\operatorname{im} d^{q-1}$ as 0 if $q = 0$.

Warning 6.4.8. In the case of the Zariski site, one obtains the same group $\check{\mathrm{H}}^q(\mathcal{U}, \mathscr{F})$ if one fixes a well ordering on I and takes products only over $(p+1)$-tuples satisfying $i_0 < i_1 < \cdots < i_p$, as in [**Har77**, III.§4]. But for the étale site and other sites, this approach gives the wrong cohomology groups because the fiber products contain new information even when some of the indices are equal.

Definition 6.4.9. Let $\mathcal{U} = \{U_i \to U\}_{i\in I}$ and $\mathcal{V} = \{V_j \to U\}_{j\in J}$ be open coverings with respect to some site $(\mathcal{C}, \mathcal{T})$. Then $\mathcal{U}$ is called a **refinement** of $\mathcal{V}$ if there exists a map $\pi\colon I \to J$ and a morphism $U_i \to V_{\pi(i)}$ for each $i \in I$.

If $\mathcal{U}$ is a refinement of $\mathcal{V}$, then there is an induced morphism $\check{\mathrm{H}}^q(\mathcal{V}, \mathscr{F}) \to \check{\mathrm{H}}^q(\mathcal{U}, \mathscr{F})$ for each $q \geq 0$.

Definition 6.4.10. Let $\mathscr{F}$ be an abelian presheaf on a site $(\mathcal{C}, \mathcal{T})$, let $U \in \mathcal{C}$, and let $q \in \mathbb{N}$. The **qth Čech cohomology group of U with coefficients in $\mathscr{F}$** is

$$\check{\mathrm{H}}^q(U, \mathscr{F}) := \varinjlim \check{\mathrm{H}}^q(\mathcal{U}, \mathscr{F}),$$

Unofficial version for incidental online use

where the direct limit is taken over all open coverings of U, ordered by refinement.

Warning 6.4.11. The abelian groups $\check{\mathrm{H}}^q(U, \mathscr{F})$ and $\mathrm{H}^q(U, \mathscr{F})$ need not be isomorphic.

Proposition 6.4.12. *If $\mathscr{F}$ is an abelian* sheaf *on a site $(\mathcal{C}, \mathcal{T})$, and $U \in \mathcal{C}$, then we have*

$$\begin{aligned} \check{\mathrm{H}}^0(U, \mathscr{F}) &\xrightarrow{\sim} \mathrm{H}^0(U, \mathscr{F}) \quad = \quad \mathscr{F}(U) \\ \check{\mathrm{H}}^1(U, \mathscr{F}) &\xrightarrow{\sim} \mathrm{H}^1(U, \mathscr{F}) \\ \check{\mathrm{H}}^2(U, \mathscr{F}) &\hookrightarrow \mathrm{H}^2(U, \mathscr{F}). \end{aligned}$$

Sketch of proof. The first line is immediate from the definition of $\check{\mathrm{H}}^0(U, \mathscr{F})$ and the sheaf property of $\mathscr{F}$. For the second and third lines, let $\mathscr{H}(\mathscr{F})$ be the presheaf of Remark 6.4.2, and use Proposition 6.7.1 for the **spectral sequence of Čech cohomology**

$$E_2^{pq} := \check{\mathrm{H}}^p(U, \mathscr{H}^q(\mathscr{F})) \implies \mathrm{H}^{p+q}(U, \mathscr{F}),$$

and use the fact $\check{\mathrm{H}}^0(U, \mathscr{H}^q(\mathscr{F})) = 0$; see [**Sha72**, pp. 200–201]. □

Theorem 6.4.13 (M. Artin). *Let X be a quasi-compact scheme such that every finite subset of X is contained in an affine open subset. (This is automatic if X is quasi-projective over an affine scheme.) Let $\mathscr{F}$ be an abelian sheaf on X_{et}. Then there are canonical isomorphisms $\check{\mathrm{H}}^q_{\mathrm{et}}(X, \mathscr{F}) \xrightarrow{\sim} \mathrm{H}^q_{\mathrm{et}}(X, \mathscr{F})$ for all $q \in \mathbb{N}$.*

Proof. See the original reference [**Art71**], or see [**Mil80**, III.2.17]. □

Important Remark 6.4.14. In group cohomology, one can define $\mathrm{H}^0(G, A)$ and $\mathrm{H}^1(G, A)$ even when the group A is nonabelian. Similarly, one can define $\check{\mathrm{H}}^0(X, \mathscr{F})$ and $\check{\mathrm{H}}^1(X, \mathscr{F})$ for a presheaf $\mathscr{F}$ of possibly nonabelian groups; see [**Mil80**, p. 122].

Unofficial version for incidental online use

6.5. Torsors over an arbitrary base

(Reference: [**Mil80**, III.§4])

Torsors under a group scheme G over a general base scheme can be thought of as families of torsors. (In differential geometry, such objects are sometimes called principal G-bundles.)

6.5.1. Definition of torsors.

Definition 6.5.1. Let $G \to S$ be an fppf group scheme. An G-**torsor over** S (or simply G-**torsor**) is an fppf S-scheme X equipped with a right G-action

$$X \times_S G \longrightarrow X$$

such that one of the following equivalent conditions holds:

(i) There exists an fppf base change $S' \to S$ such that

$$X_{S'} \text{ with its right } G_{S'}\text{-action}$$

is isomorphic over S' to

$$G_{S'} \text{ with the right translation } G_{S'}\text{-action.}$$

(ii) The morphism

$$\begin{aligned} X \times_S G &\longrightarrow X \times_S X \\ (x, g) &\longmapsto (x, xg) \end{aligned}$$

is an isomorphism.

Proof of equivalence.

(ii)⇒(i): Take $S' = X$. Then (ii) backward says that $S' \times_S X \simeq S' \times_S G$. In other words, $X_{S'} \simeq G_{S'}$. Moreover, the right G-actions correspond: this is simply the formula $(xg)h = x(gh)$ coming from the definition of right G-action on X.

(i)⇒(ii): Let ϕ be the morphism

$$\begin{aligned} X \times_S G &\longrightarrow X \times_S X \\ (x, g) &\longmapsto (x, xg). \end{aligned}$$

Base extend ϕ by $S' \to S$ and use (i) to replace $X_{S'}$ by $G_{S'}$. This gives

$$\begin{aligned} \phi_{S'} \colon G_{S'} \times_{S'} G_{S'} &\longrightarrow G_{S'} \times_{S'} G_{S'} \\ (x, g) &\longmapsto (x, xg). \end{aligned}$$

Since G is a group scheme, $\phi_{S'}$ is an isomorphism. But $S' \to S$ is fppf, hence fpqc, so fpqc descent (Theorem 4.3.7(ii)) implies that ϕ was an isomorphism to begin with. □

Remark 6.5.2. Let X be an G-torsor over S. By fpqc descent (Theorem 4.3.7(i)), many properties of G are inherited by X. For instance, if G is smooth over S, then X is smooth over S.

6.5.2. Trivial torsors. The following generalizes Proposition 5.12.14.

Proposition 6.5.3. *Let $G \to S$ be an fppf group scheme, and let X be a G-torsor over S. The following are equivalent:*

Unofficial version for incidental online use

(i) *X is isomorphic to the trivial torsor (G with right translation action).*

(ii) *$X(S) \neq \emptyset$; i.e., $X \to S$ admits a section.*

(iii) *X corresponds to the neutral element of $\check{\mathrm{H}}^1_{\mathrm{fppf}}(S, G)$ (see Section 6.5.5).*

Proof.

(i)⇒(ii): This is because $G \to S$ has the identity section.

(ii)⇒(i): The second definition of torsor gives us an isomorphism $X_X \simeq G_X$ of G_X-torsors over X. If we have a section $S \to X$, we can further base extend by this to get $X_S \simeq G_S$; in other words, $X \simeq G$ as G-torsors over S.

(i)⇔(iii): This follows from the definition of the correspondence given in Section 6.5.5. □

6.5.3. Examples. Generalizing Example 5.12.9, we have:

Example 6.5.4. Let G be a finite group. A Galois covering $S' \to S$ with Galois group G in the sense of Remark 4.4.7 is the same thing as a torsor under the constant S-group scheme corresponding to G.

Example 6.5.5. Let $\mathscr{L}$ be a invertible sheaf on a scheme S. Let $L \to S$ be the corresponding line bundle, i.e., $L := \mathbf{Spec}\,\mathrm{Sym}(\mathscr{L})$ (some authors use $\mathscr{L}^{-1}$ instead). Thus there exists a finite cover of S by open subsets U such that $L_U \to U$ is isomorphic to $U \times \mathbb{A}^1 \to U$. Let Z be the zero section of the line bundle, viewed as a closed subscheme of L. Then the open subscheme $X := L - Z$ of L is an $\mathbb{G}_{m,S}$-torsor over S. This torsor is trivial if and only if $\mathscr{L} \simeq \mathscr{O}_S$.

Example 6.5.6. The same construction as in Example 6.5.5 associates to any locally free rank n sheaf a GL_n-torsor.

6.5.4. Torsor sheaves. Recall that a scheme gives rise to its functor of points, which is a sheaf of sets. Thus sheaves of sets can be viewed as a generalization of schemes. Similarly, group sheaves can be viewed as a generalization of group schemes.

Definition 6.5.7. Let G be a group sheaf on a site with final object S (e.g., the étale site on a scheme S). A G-**torsor sheaf** T is a sheaf of sets equipped with a right action $T(U) \times G(U) \to T(U)$ for each $U \in \mathcal{C}$, functorially in U, such that there exists an open covering $\{U_i \to S\}$ and an isomorphism $T|_{U_i} \xrightarrow{\sim} G|_{U_i}$ identifying the right $G|_{U_i}$-action on $T|_{U_i}$ with the right action of $G|_{U_i}$ on itself by translations.

Definition 6.5.8. Say that an open covering $\{V_i \to S\}$ **trivializes** a torsor sheaf T if there exist isomorphisms $T|_{V_i} \simeq G|_{V_i}$ respecting the right G-actions for all i.

Unofficial version for incidental online use

6.5.5. Torsors and H^1. Section 5.12 used Galois descent to show that (scheme) torsors under a smooth algebraic group G over k are classified by $\mathrm{H}^1(k,G)$. The generalization to base schemes S other than $\operatorname{Spec} k$ breaks up into two steps:

(1) Relate $\check{\mathrm{H}}^1(S,G)$ to torsor *sheaves*. By definition, giving a sheaf locally is the same as giving a sheaf, so the question of descent does not come up.

(2) Ask whether torsor sheaves are represented by (scheme) torsors. This is the delicate part, because it involves descent of schemes, which is not always effective.

The following handles the first step:

Proposition 6.5.9. *Let G be a group sheaf on a site with final object S. Then there is a isomorphism of pointed sets*

$$\frac{\{G\text{-torsor sheaves}\}}{\text{isomorphism}} \quad \stackrel{\sim}{\to} \quad \check{\mathrm{H}}^1(S,G).$$

Proof. The construction is similar to the construction of a 1-cocycle from a twist in Remark 4.5.4, as we now demonstrate.

Let T be a G-torsor sheaf. Choose an open covering $\mathcal{U} := \{U_i \to S\}$ and isomorphisms $f_i\colon G|_{U_i} \simeq T|_{U_i}$. Then on the overlaps $U_{ij} = U_i \times_S U_j$ the transition maps $f_i^{-1} f_j\colon G|_{U_{ij}} \stackrel{\sim}{\to} G|_{U_{ij}}$ are given by left multiplication by some $g_{ij} \in G(U_{ij})$. The g_{ij} form a Čech 1-cocycle. Changing the isomorphisms f_i corresponds to replacing the 1-cocycle by a cohomologous one. In this way, we get an isomorphism of pointed sets

$$\frac{\{G\text{-torsor sheaves trivialized by } \mathcal{U}\}}{\text{isomorphism}} \quad \stackrel{\sim}{\to} \quad \check{\mathrm{H}}^1(\mathcal{U},\mathscr{F}).$$

Taking the direct limit over all open coverings gives the desired isomorphism. □

Fortunately, it is often true that torsor sheaves are represented by torsor schemes:

Theorem 6.5.10. *Let G be an fppf group scheme over a locally noetherian scheme S. Then we have*

$$\frac{\{G\text{-torsors}\}}{\text{isomorphism}} \hookrightarrow \frac{\{G\text{-torsor sheaves}\}}{\text{isomorphism}} \stackrel{\sim}{\to} \check{\mathrm{H}}^1_{\mathrm{fppf}}(S,G) \stackrel{\sim}{\dashrightarrow} \mathrm{H}^1_{\mathrm{fppf}}(S,G),$$

where the last term and the last isomorphism should be included only if G is commutative (since otherwise $\mathrm{H}^1_{\mathrm{fppf}}(S,G)$ is not defined). Moreover, the first injection is a bijection in any of the following cases:

(i) *$G \to S$ is an affine morphism.*

Unofficial version for incidental online use

(ii) *G is of finite presentation and separated over S, and* $\dim S \leq 1$.

(iii) *$G \to S$ is an abelian scheme, and G is locally factorial.*

Proof. For the last isomorphism, see [**Mil80**, III.4.7]. Case (i) follows from Theorem 4.3.5(ii). Case (ii) follows from [**Ray70b**, Théorème XI.3.1(1)] in the smooth case, and [**Ana73**, Théorème 4.D] in general. Case (iii) is a special case of [**Ray70b**, Théorème XI.3.1(2)]. In [**Ray70b**, XI and XIII] one can find other hypotheses that guarantee that the injection is a bijection. On the other hand, [**Ray70b**, XII] contains some counterexamples. □

Remark 6.5.11. To avoid the delicate issue of representability by a scheme, one can enlarge the category of schemes to the category of *algebraic spaces*. Under the hypotheses of Theorem 6.5.10 (or the weaker hypothesis that $G \to S$ is a group algebraic space over an algebraic space), a G-torsor sheaf for the fppf topology on S is always represented by a G-torsor algebraic space, because the definition of algebraic space is fppf local; see [**LMB00**, 10.4.2] and [**SP**, Tag 04SK].

To simplify notation, we write $\mathrm{H}^1(S,G)$ for $\check{\mathrm{H}}^1_{\mathrm{fppf}}(S,G)$ from now on.

6.5.6. Geometric operations on torsors over schemes. The notions of inner twist, inverse torsors, contracted product, and subtraction of torsors in Sections 5.11 and 5.12.5 can be generalized to base schemes S other than $\operatorname{Spec} k$. The idea in each case is that the construction is easy in the case where the torsor $T \to S$ involved is trivial, so we do the construction after fppf base change and then descend the result to S. We will only state the results here; see [**Sko01**, pp. 20–21] for more details.

Let G be an fppf group scheme over a scheme S. Assume that G is *affine over S*; this is to ensure that descent is effective, so that we can work with torsors as schemes instead of only as sheaves.

6.5.6.1. *Inner twists.* Given $\tau \in \mathrm{H}^1(S,G)$ (perhaps the class of a G-torsor $T \to S$), one obtains another fppf group scheme G^τ affine over S.

6.5.6.2. *Inverse torsors.* Let $T \to S$ be a right G-torsor, and let τ be its class in $\mathrm{H}^1(S,G)$. Then T may be viewed as a G^τ-G-bitorsor, and the same S-scheme may be viewed as a G-G^τ-bitorsor T^{-1}.

6.5.6.3. *Contracted products.* Let $G \to S$ be an fppf group scheme. Let X be an S-scheme that is affine over S and equipped with a right G-action (but X is not necessarily a torsor). Let T be a *left* G-torsor over S. The **contracted product** $X \overset{G}{\times} T$ is the quotient of $X \times_S T$ by the G-action in which $g \in G$ acts by $(x,t) \mapsto (xg, g^{-1}t)$. The result is an S-scheme that is affine over S.

Unofficial version for incidental online use

6.5.6.4. *Subtraction of torsors.* Let Z and T be two right G-torsors over S. Let $\tau = [T] \in \mathrm{H}^1(S, G)$ be their classes. Then $Z \overset{G}{\times} T^{-1}$ is a right G^τ-torsor over S.

Example 6.5.12 (Twisted torsor)**.** Let k be a field. Let S be a k-scheme. Let G be an affine algebraic group over k. Then G_S is an fppf group scheme over S that is affine over S. Suppose that $f := Z \to S$ is a right G_S-torsor, but $T \to \operatorname{Spec} k$ is a right G-torsor. Define

$$Z^\tau := Z \overset{G_S}{\times}_S T_S = Z \overset{G}{\times}_k T$$

and let $f^\tau \colon Z^\tau \to S$ be its structure morphism. Then Z^τ is a right G^τ-torsor over S (i.e., a right $(G^\tau)_S$-torsor).

6.5.7. Unramified torsors. This section will be essential for the finiteness of Selmer sets in Section 8.4.4. Let k be a global field. Let S be a finite nonempty set of places of k containing all the archimedean places. Let $\mathcal{O}_{k,S}$ be the ring of S-integers in k. For $v \notin S$, let $\mathcal{O}_{k,v}$ be the local ring of $\mathcal{O}_{k,S}$ at v, let $\mathcal{O}_v$ be its completion, and let $k_v = \operatorname{Frac} \mathcal{O}_v$, so k_v is the completion of k at v. Let $\mathcal{G}$ be a smooth finite-type affine group scheme over $\mathcal{O}_{k,S}$. Affineness guarantees that every element of H^1 is actually represented by a torsor scheme (Theorem 6.5.10(i)). Let $G = \mathcal{G} \times_{\mathcal{O}_{k,S}} k$.

Let $\tau \in \mathrm{H}^1(k, G)$ and $v \notin S$. Let τ_v be the image of τ in $\mathrm{H}^1(k_v, G)$. Call τ **unramified at** v if τ is in the image of $\mathrm{H}^1(\mathcal{O}_{k,v}, \mathcal{G}) \to \mathrm{H}^1(k, G)$, or equivalently, if τ_v is the image of $\mathrm{H}^1(\mathcal{O}_v, \mathcal{G}) \to \mathrm{H}^1(k_v, G)$ (the equivalence follows from a fancy version of fpqc descent; see [**BLR90**, §6.2, Proposition D.4(b)]). Call τ **unramified outside** S if τ is unramified at every $v \notin S$. In this case, τ comes from an element of $\mathrm{H}^1(\mathcal{O}_{k,S}, \mathcal{G})$: first, the torsor corresponding to τ spreads out over $\mathcal{O}_{k,S'}$ for some finite $S' \supseteq S$; then apply fpqc descent to $\operatorname{Spec} \mathcal{O}_{k,S'} \amalg \coprod_{v \in S' \setminus S} \operatorname{Spec} \mathcal{O}_{k,v} \to \operatorname{Spec} \mathcal{O}_{k,S}$. Let $\mathrm{H}^1_S(k, \mathcal{G})$ be the set of $\tau \in \mathrm{H}^1(k, G)$ that are unramified outside S.

As in Section 5.9.1, we have an exact sequence of smooth algebraic groups over k

$$1 \to G^0 \to G \to F \to 1,$$

where G^0 is the connected component of G, and F is finite étale over k. Enlarging S if necessary, we get a corresponding exact sequence of smooth finite-type separated group schemes over $\mathcal{O}_{k,S}$

$$1 \to \mathcal{G}^0 \to \mathcal{G} \to \mathcal{F} \to 1$$

in which $\mathcal{G}^0$ has connected fibers and $\mathcal{F}$ is finite étale of order n. The map $\mathrm{H}^1(k, G) \to \mathrm{H}^1(k, F)$ restricts to a map $h \colon \mathrm{H}^1_S(k, \mathcal{G}) \to \mathrm{H}^1_S(k, \mathcal{F})$.

Theorem 6.5.13. *Under the hypotheses above,*

Unofficial version for incidental online use

(a) *the maps* $\mathrm{H}^1_S(k,\mathcal{G}) \xrightarrow{h} \mathrm{H}^1_S(k,\mathcal{F}) \longrightarrow \prod_{v\in S} \mathrm{H}^1(k_v,F)$ *have finite fibers;*

(b) *if k is a number field, then* $\mathrm{H}^1_S(k,\mathcal{G})$ *itself is finite.*

Proof.

Step 1: For each $v \notin S$, the kernel of $\mathrm{H}^1(\mathcal{O}_v,\mathcal{F}) \to \mathrm{H}^1(k_v,F)$ *is trivial.*

If T is an $\mathcal{F}$-torsor over $\mathcal{O}_v$, then T is finite over $\mathcal{O}_v$ by Remark 6.5.2, so T is proper over $\mathcal{O}_v$, and hence $T(\mathcal{O}_v) = T(k_v)$ by the valuative criterion for properness. Thus $T(\mathcal{O}_v) \neq \emptyset$ if and only if $T(k_v) \neq \emptyset$. That is, T is trivial if and only if T_{k_v} is trivial.

Step 2: $\mathrm{H}^1(\mathcal{O}_v,\mathcal{G}^0) = 0$.

Let $T \to \operatorname{Spec}\mathcal{O}_v$ be a $\mathcal{G}^0$-torsor. Its special fiber $T_{\mathbf{k}(v)}$ over the residue field corresponds to an element of $\mathrm{H}^1(\mathbf{k}(v),\mathcal{G}^0_{\mathbf{k}(v)})$, which is trivial by Lang's theorem (Theorem 5.12.19(a)). Thus $T_{\mathbf{k}(v)}$ has a $\mathbf{k}(v)$-point. Since $\mathcal{G}^0$ is smooth over $\mathcal{O}_v$, so is T (Remark 6.5.2). Hence we may apply Hensel's lemma (Theorem 3.5.63(a)) to deduce that T has an $\mathcal{O}_v$-point. Thus T is a trivial torsor.

Step 3: The kernel of h is finite.

For each $v \notin S$, we have the following commutative diagram in which the maps labelled Step 1 and Step 2 have trivial kernel:

$$\begin{tikzcd}
& \mathrm{H}^1(k,G) \arrow[r] \arrow[d] & \mathrm{H}^1(k,F) \arrow[d] \\
& \mathrm{H}^1(k_v,G) \arrow[r] & \mathrm{H}^1(k_v,F) \\
\mathrm{H}^1(\mathcal{O}_v,\mathcal{G}) \arrow[ur] \arrow[r, "\text{Step 2}"'] & \mathrm{H}^1(\mathcal{O}_v,\mathcal{F}). \arrow[ur, "\text{Step 1}"'] &
\end{tikzcd}$$

Suppose $\tau \in \ker h$. By definition of $\mathrm{H}^1_S(k,\mathcal{G})$, for each $v \notin S$, the element τ_v comes from some $\tau_{\mathcal{O}_v} \in \mathrm{H}^1(\mathcal{O}_v,\mathcal{G})$. The diagram shows that $\tau_{\mathcal{O}_v}$ maps to 0 in $\mathrm{H}^1(k_v,F)$. Step 1 shows that $\tau_{\mathcal{O}_v}$ maps to 0 already in $\mathrm{H}^1(\mathcal{O}_v,\mathcal{F})$. Step 2 shows that $\tau_{\mathcal{O}_v} = 0$. Thus $\tau_v = 0$.

Hence $\ker h$ is contained in

$$Ш^1_S(k,G) := \ker\left(\mathrm{H}^1(k,G) \to \prod_{v\notin S} \mathrm{H}^1(k_v,G)\right),$$

which is finite by Theorem 5.12.29 since G is affine.

Step 4: Every fiber of h is finite.

Unofficial version for incidental online use

Given a nonempty fiber $h^{-1}(\phi)$ with $\phi \in \mathrm{H}^1_S(k, \mathcal{F})$, choose $\tau \in h^{-1}(\phi) \subseteq \mathrm{H}^1_S(k, \mathcal{G})$. Then τ comes from an element of $\mathrm{H}^1(\mathcal{O}_{k,S}, \mathcal{G})$. Call this element τ also.

If G were commutative, then $h^{-1}(\phi)$ would be in bijection with $h^{-1}(0)$ via the subtraction-of-τ map. In the general case, subtraction-of-τ and subtraction-of-ϕ (see Section 5.12.5.3) identify the top row of

$$\begin{tikzcd}
\mathrm{H}^1_S(k, \mathcal{G}) \arrow[r, "h"] \arrow[d, "-\tau"'] & \mathrm{H}^1_S(k, \mathcal{F}) \arrow[d, "-\phi"] \\
\mathrm{H}^1_S(k, \mathcal{G}^\tau) \arrow[r, "h^\tau"] & \mathrm{H}^1_S(k, \mathcal{F}^\phi)
\end{tikzcd}$$

with the bottom row, and $h^{-1}(\phi)$ is identified with $(h^\tau)^{-1}(0)$. By Step 3 applied to $\mathcal{G}^\tau$, the latter is finite. Thus $h^{-1}(\phi)$ is finite.

Step 5: The map $\mathrm{H}^1_S(k, \mathcal{F}) \to \prod_{v \in S} \mathrm{H}^1(k_v, F)$ has finite fibers.

Fix $\xi_v \in \mathrm{H}^1(k_v, F)$ for each $v \in S$. Consider $\tau \in \mathrm{H}^1_S(k, \mathcal{F})$ mapping to ξ_v for all v. By Theorem 4.3.7(i), the torsor $T \to \operatorname{Spec} k$ corresponding to τ is finite étale. By Proposition 3.5.35, T as k-scheme is a disjoint union of k-schemes of the form $\operatorname{Spec} L$ for some separable field extensions $L \supseteq k$ of degree bounded by $n := \#F$. For $v \notin S$, the class τ_v comes from $\mathrm{H}^1(\mathcal{O}_v, \mathcal{F})$, so the base extension T_{k_v} comes from a finite étale $\mathcal{O}_v$-scheme, which by Theorem 3.5.52 is a disjoint union of $\mathcal{O}_v$-schemes $\operatorname{Spec} R$, where each R is the valuation ring of a finite unramified extension of k_v. This implies that each $L \supseteq k$ above is unramified outside S. For finite $v \in S$, the v-adic valuation of the discriminant of each L/K may be nonzero, but it is bounded given ξ_v. A variant of Hermite's theorem [**Ser97**, 4.1] says that k has only finitely many separable extensions of degree $\leq n$ and bounded discriminant. Let k' be the compositum of them all, so $k' \supseteq k$ is a finite Galois extension. Then $T(k')$ is nonempty, so τ maps to 0 in $\mathrm{H}^1(k', F)$. Thus τ comes from $\mathrm{H}^1(\mathrm{Gal}(k'/k), F(k'))$ in the inflation-restriction sequence of Galois cohomology

$$0 \longrightarrow \mathrm{H}^1(\mathrm{Gal}(k'/k), F(k')) \longrightarrow \mathrm{H}^1(k, F) \longrightarrow \mathrm{H}^1(k', F).$$

Since $\mathrm{Gal}(k'/k)$ and $F(k')$ are finite, the set $\mathrm{H}^1(\mathrm{Gal}(k'/k), F(k'))$ is finite, so there are only finitely many possibilities for τ. This completes the proof of (a).

Step 6: If k is a number field, then $\mathrm{H}^1_S(k, \mathcal{G})$ is finite.

If k is a number field, then (an elementary case of) Theorem 5.12.24(a) shows that $\mathrm{H}^1(k_v, F)$ is finite for each of the finitely many v in S. Thus the conclusion follows from (a). $\square$

Unofficial version for incidental online use

6.6. Brauer groups

(References: [**Gro68b**, **Gro68c**, **Gro68d**] and [**Mil80**, IV])

6.6.1. Cohomology of $\mathbb{G}_m$.

Proposition 6.6.1. *Let X be a scheme. Then*

(i) $\mathrm{H}^0_{\mathrm{Zar}}(X, \mathbb{G}_m) \simeq \mathrm{H}^0_{\mathrm{et}}(X, \mathbb{G}_m) \simeq \mathrm{H}^0_{\mathrm{fppf}}(X, \mathbb{G}_m) \simeq \mathscr{O}_X(X)^\times$.

(ii) $\mathrm{H}^1_{\mathrm{Zar}}(X, \mathbb{G}_m) \simeq \mathrm{H}^1_{\mathrm{et}}(X, \mathbb{G}_m) \simeq \mathrm{H}^1_{\mathrm{fppf}}(X, \mathbb{G}_m) \simeq \operatorname{Pic} X$ (*generalization of Hilbert's theorem* 90).

Proof.

(i) This is true by definition.

(ii) For each Zariski open covering $\mathcal{U} = \{U_i \to X\}$, we have

$$\frac{\{\text{line bundles trivialized by } \mathcal{U}\}}{\text{isomorphism}} \simeq \check{\mathrm{H}}^1_{\mathrm{Zar}}(\mathcal{U}, \mathbb{G}_m),$$

because the transition maps needed to describe a line bundle are invertible functions on the pairwise intersections. Taking the direct limit over open coverings, we get the first of the isomorphisms in

$$\operatorname{Pic} X \simeq \check{\mathrm{H}}^1_{\mathrm{Zar}}(X, \mathbb{G}_m) \simeq \mathrm{H}^1_{\mathrm{Zar}}(X, \mathbb{G}_m),$$

and the second isomorphism comes from Proposition 6.4.12.

If we repeat the argument using the étale topology instead of the Zariski topology, we get an isomorphism

$$\operatorname{Pic} X_{\mathrm{et}} \simeq \mathrm{H}^1_{\mathrm{et}}(X, \mathbb{G}_m),$$

where $\operatorname{Pic} X_{\mathrm{et}}$ is the group of isomorphism classes of "étale line bundles", that is, sheaves $\mathscr{L}$ on X_{et} such that there exists an étale open covering $\{U_i \to X\}$ such that $\mathscr{L}|_{U_i} \simeq \mathscr{O}_{U_i}$ for all i.

We claim that for any étale surjective morphism $X' \to X$, the maps

$$\begin{tikzcd} \left\{\begin{matrix}\text{line bundles on } X \\ \text{trivialized by } X'\end{matrix}\right\} \arrow[r, "\text{fpqc descent}"] & \left\{\begin{matrix}\text{trivial line bundles on } X' \\ \text{with descent datum}\end{matrix}\right\} \arrow[d] \\ \left\{\begin{matrix}\text{line bundles on } X_{\mathrm{et}} \\ \text{trivialized by } X'_{\mathrm{et}}\end{matrix}\right\} \arrow[r, "\text{étale gluing}"] & \left\{\begin{matrix}\text{trivial line bundles on } X'_{\mathrm{et}} \\ \text{with descent datum,}\end{matrix}\right\}, \end{tikzcd}$$

where each set denotes a set of isomorphism classes, are bijections. The top horizontal map is a bijection by Theorem 4.2.3 on fpqc descent of quasi-coherent sheaves: one can show that descending a line bundle yields a line bundle. The right vertical map is the functor of Definition 6.3.13: it gives a bijection, because the descent data are given by

Unofficial version for incidental online use

isomorphisms of trivial line bundles, and the automorphism groups of the trivial line bundle $\mathscr{O}_X$ and $\mathscr{O}_{X_{\mathrm{et}}}$ are both equal to $\mathscr{O}_X(X)^\times$ for every scheme X. The bottom horizontal map is a bijection because an étale sheaf is uniquely determined by its restriction to an étale open cover with gluing data.

Finally, taking the limit of the bijection between the sets on the left over all $X' \to X$ yields $\operatorname{Pic} X \simeq \operatorname{Pic} X_{\mathrm{et}}$, since every line bundle (on X or X_{et}) is trivialized by some X'. Thus $\operatorname{Pic} X$, $\operatorname{Pic} X_{\mathrm{et}}$, $\mathrm{H}^1_{\mathrm{Zar}}(X, \mathbb{G}_m)$, $\mathrm{H}^1_{\mathrm{et}}(X, \mathbb{G}_m)$ are all isomorphic.

The same proof shows that $\operatorname{Pic} X \simeq \mathrm{H}^1_{\mathrm{fppf}}(X, \mathbb{G}_m)$. □

Remark 6.6.2. Specializing part (ii) to the case $X = \operatorname{Spec} k$ with the étale topology gives $\mathrm{H}^1(\mathfrak{G}_k, k_s^\times) = 0$, which is (Noether's generalization of) Hilbert's theorem 90.

Remark 6.6.3. More generally, for any smooth commutative group scheme G over a scheme X, there is an isomorphism $\mathrm{H}^q_{\mathrm{et}}(X, G) \xrightarrow{\sim} \mathrm{H}^q_{\mathrm{fppf}}(X, G)$ [**Gro68d**, Théorème 11.7]. The analogue for smooth *noncommutative* G holds too, as far as it makes sense: $\check{\mathrm{H}}^1_{\mathrm{et}}(X, G) \simeq \check{\mathrm{H}}^1_{\mathrm{fppf}}(X, G)$ [**Gro68d**, Remarque 11.8(3)].

6.6.2. The cohomological Brauer group.

For a field k, Theorems 1.5.12 and 6.4.6(iii) yield

$$\operatorname{Br} k \simeq \mathrm{H}^2(\mathfrak{G}_k, k_s^\times) \simeq \mathrm{H}^2_{\mathrm{et}}(\operatorname{Spec} k, \mathbb{G}_m).$$

The right-hand side makes sense when $\operatorname{Spec} k$ is replaced by an arbitrary scheme, so we are led to the following definition:

Definition 6.6.4. For any scheme X, define the **(cohomological) Brauer group** as

$$\operatorname{Br} X := \mathrm{H}^2_{\mathrm{et}}(X, \mathbb{G}_m).$$

If R is a commutative ring, define $\operatorname{Br} R := \operatorname{Br}(\operatorname{Spec} R)$.

Warning 6.6.5. Some authors use $\operatorname{Br} X$ instead to denote the Brauer group defined using Azumaya algebras as in Definition 6.6.14, and use $\operatorname{Br}' X$ to denote the cohomological Brauer group. Some instead use $\operatorname{Br}' X$ to denote the *torsion subgroup* of the cohomological Brauer group, because of Theorem 6.6.17(iii).

Remark 6.6.6. For any scheme X, we have $\operatorname{Br} X \simeq \mathrm{H}^2_{\mathrm{fppf}}(X, \mathbb{G}_m)$, by Remark 6.6.3.

Unofficial version for horizontal online use

If $X \to Y$ is a morphism of schemes, then there is an induced homomorphism $\operatorname{Br} Y \to \operatorname{Br} X$, and we obtain a functor

$$\begin{aligned}\mathbf{Schemes}^{\mathrm{opp}} &\longrightarrow \mathbf{Ab} \\ X &\longmapsto \operatorname{Br} X.\end{aligned}$$

Proposition 6.6.7 (Brauer group of a regular integral noetherian scheme)**.** *Let X be a regular integral noetherian scheme. Then*

(i) $\operatorname{Br} X \to \operatorname{Br} \mathbf{k}(X)$ *is injective.*

(ii) $\operatorname{Br} X$ *is a torsion abelian group.*

Proof.

(i) This is a special case of [**Gro68c**, Corollaire 1.10].

(ii) Since $\operatorname{Br} \mathbf{k}(X)$ is a Galois cohomology group, it is torsion. So (i) implies (ii). $\square$

Warning 6.6.8. Without regularity, Proposition 6.6.7 can fail: Exercise 6.6 gives a counterexample to (i) from [**AG60**, p. 388]. Part (ii) can fail too; see Warning 6.6.18(i).

For an extension of Proposition 6.6.7(i), see Theorem 6.8.3.

Corollary 6.6.9. *If $X \to Y$ is a birational morphism of regular integral noetherian schemes, then* $\operatorname{Br} Y \to \operatorname{Br} X$ *is injective.*

Proof. Functoriality of Br yields a commutative diagram

$$\begin{tikzcd} \operatorname{Br} X \arrow[r] & \operatorname{Br} \mathbf{k}(X) \arrow[d, equal] \\ \operatorname{Br} Y \arrow[u] \arrow[r] & \operatorname{Br} \mathbf{k}(Y), \end{tikzcd}$$

and the horizontal homomorphisms are injective by Proposition 6.6.7(i). $\square$

See Corollary 6.8.5 for a partial refinement of Corollary 6.6.9.

Proposition 6.6.10 (Brauer group of a limit)**.** *Let $(X_i)_{i \in I}$ be a filtered inverse system of schemes. Suppose that the X_i are quasi-compact and quasi-separated, and that the morphisms in the system are affine. Let $X = \varprojlim X_i$. Then $\operatorname{Br} X \simeq \varinjlim \operatorname{Br} X_i$.*

Proof. Take $G_0 = \mathbb{G}_m$ and $q = 2$ in Theorem 6.4.3. $\square$

Proposition 6.6.10 is useful for spreading out Brauer group elements:

Unofficial version for incidental online use

Corollary 6.6.11. *Let X be a variety over a global field k. Let $A \in \operatorname{Br} X$. Then for some finite set S of places of k, there exist a finite-type $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$, an element $\mathcal{A} \in \operatorname{Br} \mathcal{X}$ and a morphism $X \hookrightarrow \mathcal{X}$ identifying X with the generic fiber $\mathcal{X}_k$ such that $\operatorname{Br} \mathcal{X} \to \operatorname{Br} X$ maps $\mathcal{A}$ to A.*

Proof. Theorem 3.2.1 lets us spread out X to a finite-type $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$. The open subschemes $\mathcal{X}_{\mathcal{O}_{k,T}}$, as T ranges over finite sets of places with $T \supseteq S$, form a filtered inverse system and $\varprojlim \mathcal{X}_{\mathcal{O}_{k,T}} \simeq X$. By Proposition 6.6.10, $\operatorname{Br} X \simeq \varinjlim \operatorname{Br} \mathcal{X}_{\mathcal{O}_{k,T}}$. Thus A comes from an element of $\operatorname{Br} \mathcal{X}_{\mathcal{O}_{k,T}}$ for some T. Rename T as S, and rename $\mathcal{X}_{\mathcal{O}_{k,T}}$ as $\mathcal{X}$. □

6.6.3. Azumaya algebras. A matrix algebra over a field k is $\operatorname{End} V$ for some finite-dimensional vector space over k. The generalization of this over a scheme X is the $\mathscr{O}_X$-algebra $\mathbf{End}_{\mathscr{O}_X}(\mathscr{E}) := \mathbf{Hom}_{\mathscr{O}_X}(\mathscr{E}, \mathscr{E})$ for some locally free $\mathscr{O}_X$-module $\mathscr{E}$.

An Azumaya algebra over k is a k-algebra that becomes isomorphic to an $r \times r$ matrix algebra for some $r \in \mathbb{Z}_{>0}$ after finite separable base extension. The generalization of this is the following:

Definition 6.6.12 (**[Gro68b**, Théorème 5.1]). An **Azumaya algebra** on a scheme X is an $\mathscr{O}_X$-algebra $\mathcal{A}$ that is coherent as an $\mathscr{O}_X$-module with $\mathcal{A}_x \neq 0$ for all $x \in X$, and that satisfies one of the following equivalent conditions:

(i) There is an open covering $\{U_i \to X\}$ in the étale topology such that for each i there exists $r_i \in \mathbb{Z}_{>0}$ such that $\mathcal{A} \otimes_{\mathscr{O}_X} \mathscr{O}_{U_i} \simeq \mathrm{M}_{r_i}(\mathscr{O}_{U_i})$.

(ii) There is an open covering $\{U_i \to X\}$ in the fppf topology such that for each i there exists $r_i \in \mathbb{Z}_{>0}$ such that $\mathcal{A} \otimes_{\mathscr{O}_X} \mathscr{O}_{U_i} \simeq \mathrm{M}_{r_i}(\mathscr{O}_{U_i})$.

(iii) $\mathcal{A}$ is locally free as an $\mathscr{O}_X$-module, and the fiber $\mathcal{A}(x) := \mathcal{A} \otimes_{\mathscr{O}_X} \mathbf{k}(x)$ is an Azumaya algebra over the residue field $\mathbf{k}(x)$ for each $x \in X$.

(iv) $\mathcal{A}$ is locally free as an $\mathscr{O}_X$-module, and the canonical homomorphism $\mathcal{A} \otimes_{\mathscr{O}_X} \mathcal{A}^{\mathrm{opp}} \to \mathbf{End}_{\mathscr{O}_X}(\mathcal{A})$ is an isomorphism.

6.6.3.1. *The Azumaya Brauer group.*

Definition 6.6.13. Two Azumaya algebras $\mathcal{A}$ and $\mathcal{A}'$ on X are **similar** (and we then write $\mathcal{A} \sim \mathcal{A}'$) if there exist locally free coherent $\mathscr{O}_X$-modules $\mathscr{E}$ and $\mathscr{E}'$ of positive rank at each $x \in X$ such that

$$\mathcal{A} \underset{\mathscr{O}_X}{\otimes} \mathbf{End}_{\mathscr{O}_X}(\mathscr{E}) \simeq \mathcal{A}' \underset{\mathscr{O}_X}{\otimes} \mathbf{End}_{\mathscr{O}_X}(\mathscr{E}').$$

Definition 6.6.14. Let X be a scheme. The **Azumaya Brauer group** $\operatorname{Br}_{\mathrm{Az}} X$ is the the set of similarity classes of Azumaya algebras on X. The multiplication is induced by $\mathcal{A}, \mathcal{B} \mapsto \mathcal{A} \otimes_{\mathscr{O}_X} \mathcal{B}$, the inverse is induced by $\mathcal{A} \mapsto \mathcal{A}^{\mathrm{opp}}$, and the identity is the class of $\mathscr{O}_X$.

Unofficial version for incidental online use

Then $\mathrm{Br}_{\mathrm{Az}}$ is a functor from $\mathbf{Schemes}^{\mathrm{opp}}$ to $\mathbf{Ab}$, just as Br was.

6.6.3.2. *Cyclic Azumaya algebras.* The cyclic algebra constructions from Section 1.5.7 generalize in a straightforward way to an arbitrary base scheme X. Namely, suppose that $a \in \Gamma(X, \mathscr{O}_X^\times)$ is a global unit and that $Y \to X$ is a $\mathbb{Z}/n\mathbb{Z}$-torsor. As in Section 1.5.7, we define a twisted polynomial algebra $\mathscr{O}_Y[x]_\sigma$, where σ acts as the generator of $\mathbb{Z}/n\mathbb{Z}$, and $x\ell = ({}^\sigma\ell)\,x$ for all sections ℓ of $\mathscr{O}_Y$. Then the $\mathscr{O}_X$-algebra $\mathscr{O}_Y[x]_\sigma/(x^n - a)$ turns out to be an Azumaya $\mathscr{O}_X$-algebra, split by the étale cover $Y \to X$.

There is a cohomological version of this construction. The exact sequence

$$1 \longrightarrow \boldsymbol{\mu}_n \longrightarrow \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \longrightarrow 1$$

lets us map a to an element of $\mathrm{H}^1(X, \boldsymbol{\mu}_n)$. On the other hand, the torsor $Y \to X$ has a class in $\mathrm{H}^1(X, \mathbb{Z}/n\mathbb{Z})$. The cup product yields an element of $\mathrm{H}^2(X, \boldsymbol{\mu}_n)$, which can be mapped to an element of $\mathrm{H}^2(X, \mathbb{G}_m) =: \mathrm{Br}\, X$.

The two constructions above are related: the homomorphism (6.6.16) defined in the next section maps the class of $\mathscr{O}_Y[x]_\sigma/(x^n - a)$ to the element of $\mathrm{Br}\, X$.

Remark 6.6.15. Suppose that X is a scheme over $\mathbb{Z}[1/n, \zeta_n]$, so $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\boldsymbol{\mu}_n$ over X. Then we may form a cyclic algebra from two units $a, b \in \Gamma(X, \mathscr{O}_X^\times)$, by reinterpreting the $\boldsymbol{\mu}_n$-torsor $\mathbf{Spec}\, \mathscr{O}_X[x]/(x^n - b) \longrightarrow X$ as a $\mathbb{Z}/n\mathbb{Z}$-torsor and proceeding as before.

6.6.4. Comparison of the two definitions of the Brauer group. Just as Azumaya algebras of dimension n^2 over a field k are classified up to isomorphism by $\mathrm{H}^1(k, \mathrm{PGL}_n)$, Azumaya algebras of rank n^2 over a scheme X are classified by $\mathrm{H}^1(X, \mathrm{PGL}_n)$: a Čech 1-cocycle gives the transition data needed to glue sheaves of matrix algebras using fpqc descent.

The exact sequence

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \mathrm{GL}_n \longrightarrow \mathrm{PGL}_n \longrightarrow 0$$

of sheaves on X_{et} (or X_{fppf}) gives rise to a map

$$\mathrm{H}^1(X, \mathrm{PGL}_n) \longrightarrow \mathrm{H}^2(X, \mathbb{G}_m) = \mathrm{Br}\, X$$

so each Azumaya algebra $\mathcal{A}$ of rank n^2 gives rise to an element of $\mathrm{Br}\, X$. If the rank of $\mathcal{A}$ is not constant, one can apply the same construction on each open and closed subset of X where the rank is constant. It turns out that this induces a map

$$\mathrm{Br}_{\mathrm{Az}}\, X \longrightarrow \mathrm{Br}\, X, \tag{6.6.16}$$

functorial in X.

Theorem 6.6.17.

Unofficial version for incidental online use

(i) *For any scheme X, the natural map*

$$\operatorname{Br}_{\mathrm{Az}} X \longrightarrow \operatorname{Br} X := \mathrm{H}^2_{\mathrm{et}}(X, \mathbb{G}_m)$$

is an injective homomorphism.

(ii) *An Azumaya algebra $\mathcal{A}$ on X that is locally free of rank n^2 defines an element of $\operatorname{Br}_{\mathrm{Az}} X$ that is killed by n. In particular, if X has at most finitely many connected components, $\operatorname{Br}_{\mathrm{Az}} X$ is torsion.*

(iii) *If X has an ample invertible sheaf (e.g., X is quasi-projective over* $\operatorname{Spec} A$ *for some noetherian ring A), then the injection in* (i) *induces an isomorphism*

$$\operatorname{Br}_{\mathrm{Az}} X \xrightarrow{\sim} (\operatorname{Br} X)_{\mathrm{tors}}.$$

Proof.

(i) See [**Gro68b**, equation (2.1)].

(ii) We have a commutative diagram of fppf group schemes

$$\begin{tikzcd} 0 \arrow[r] & \boldsymbol{\mu}_n \arrow[r] \arrow[d] & \mathrm{SL}_n \arrow[r] \arrow[d] & \mathrm{PSL}_n \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mathbb{G}_m \arrow[r] & \mathrm{GL}_n \arrow[r] & \mathrm{PGL}_n \arrow[r] & 0. \end{tikzcd}$$

The snake lemma, together with the surjectivity of $\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m$, shows that $\mathrm{PSL}_n \to \mathrm{PGL}_n$ is an isomorphism. Taking cohomology gives a commutative diagram

$$\begin{tikzcd} \mathrm{H}^1(X, \mathrm{PSL}_n) \arrow[r] \arrow[d, equal] & \mathrm{H}^2(X, \boldsymbol{\mu}_n) \arrow[d] \\ \mathrm{H}^1(X, \mathrm{PGL}_n) \arrow[r] & \mathrm{H}^2(X, \mathbb{G}_m). \end{tikzcd}$$

Now $\mathcal{A}$ corresponds to an element of $\mathrm{H}^1(X, \mathrm{PGL}_n)$. The diagram shows that its image in $\mathrm{H}^2(X, \mathbb{G}_m)$ comes from an element of $\mathrm{H}^2(X, \boldsymbol{\mu}_n)$ and is hence killed by n. By (i), the class of A in $\operatorname{Br}_{\mathrm{Az}} X$ is killed by n too.

(iii) This is an unpublished theorem of Gabber. A different proof, using *α-twisted sheaves*, was found by de Jong [**dJ05**]. □

Warning 6.6.18.

(i) Mumford constructed a normal singular surface X over $\mathbb{C}$ such that $\operatorname{Br} X$ is not torsion [**Gro68c**, Remarque 1.11b]. But $\operatorname{Br}_{\mathrm{Az}} X$ is torsion. This shows the necessity of taking the torsion subgroup on the right-hand side of Theorem 6.6.17(iii).

(ii) There is a nonseparated normal surface with $\operatorname{Br}_{\mathrm{Az}} X \subsetneq (\operatorname{Br} X)_{\mathrm{tors}}$, namely the cone $\operatorname{Spec} \mathbb{C}[x, y, z]/(xy - z^2)$ with a doubled vertex. The

Unofficial version for incidental online use

original reference is [**EHKV01**, Corollary 3.11]; see [**Ber05**, §3] for a simpler proof.

Corollary 6.6.19. *If X is a regular quasi-projective variety over a field, then* $\operatorname{Br}_{\mathrm{Az}} X \simeq (\operatorname{Br} X)_{\mathrm{tors}} = \operatorname{Br} X$.

Proof. The first isomorphism comes from Theorem 6.6.17(iii). By Proposition 3.5.5, the variety X is a finite disjoint union of integral varieties, and applying Proposition 6.6.7(ii) to each shows that $\operatorname{Br} X$ is torsion. □

6.6.5. Computing Brauer groups. Two main methods for computing Brauer groups are

- the Hochschild–Serre spectral sequence in étale cohomology (see Corollary 6.7.8), and
- residue homomorphisms (see Theorem 6.8.3).

6.7. Spectral sequences

(References: [**Mil80**, Appendix B], [**Sha72**, II.§4], [**Wei94**, Chapter V])

Suppose that one has left exact functors between abelian categories

$$\mathcal{A} \xrightarrow{f} \mathcal{B} \xrightarrow{g} \mathcal{C}.$$

Then the composite functor $gf\colon \mathcal{A} \to \mathcal{C}$ is also left exact. If $\mathcal{A}$ and $\mathcal{B}$ have enough injectives, one can form the derived functors $R^n f$, $R^n g$, and $R^n(gf)$. If moreover f takes injectives to g-acyclics (that is, $R^q g(f(A)) = 0$ for any injective object $A \in \mathcal{A}$ and any $q \in \mathbb{Z}_{>0}$), then there is a **spectral sequence**

$$E_2^{p,q} := (R^p g)(R^q f)(A) \implies (R^{p+q}(gf))(A)$$

that sometimes lets one compute $R^n(gf)$ in terms of the other two derived functors.

The notation

$$E_2^{p,q} \implies L^{p+q}$$

used above means all of the following:

- For each $r \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, there is a **page** r consisting of objects $E_r^{p,q}$ of $\mathcal{C}$ for $p, q \in \mathbb{Z}$ such that $E_r^{p,q} = 0$ when $p < 0$ or $q < 0$. (The objects on a given page are usually displayed in a table.)
- The objects $E_2^{p,q}$ on page 2 are the ones given in the notation.
- For $r \in \mathbb{Z}_{\geq 2}$, one has morphisms "of degree $(r, 1-r)$": this means that there is a morphism

$$d_r^{p,q}\colon E_r^{p,q} \to E_r^{p+r,q+1-r}$$

Unofficial version for incidental online use

for each $p, q \in \mathbb{Z}$. For example, page 2 has the form

$$\begin{tikzcd}
\vdots & \vdots & \vdots & \vdots & \vdots & \\
E_2^{0,3} \arrow[drr] & E_2^{1,3} \arrow[drr] & E_2^{2,3} \arrow[drr] & E_2^{3,3} & E_2^{4,3} & \cdots \\
E_2^{0,2} \arrow[drr] & E_2^{1,2} \arrow[drr] & E_2^{2,2} \arrow[drr] & E_2^{3,2} & E_2^{4,2} & \cdots \\
E_2^{0,1} \arrow[drr] & E_2^{1,1} \arrow[drr] & E_2^{2,1} \arrow[drr] & E_2^{3,1} & E_2^{4,1} & \cdots \\
E_2^{0,0} & E_2^{1,0} & E_2^{2,0} & E_2^{3,0} & E_2^{4,0} & \cdots.
\end{tikzcd}$$

- For each $r \in \mathbb{Z}_{\geq 2}$, the morphisms on page r form complexes:
$$d_r^{p,q} \circ d_r^{p-r,q+r-1} = 0$$
for all $p, q \in \mathbb{Z}$.
- For each $r \in \mathbb{Z}_{\geq 2}$, the objects on page $r+1$ are the cohomology objects of the complexes on page r:
$$E_{r+1}^{p,q} = \frac{\ker d_r^{p,q}}{\operatorname{im} d_r^{p-r,q+r-1}}.$$
- For fixed $p, q \in \mathbb{Z}$, the page ∞ object $E_\infty^{p,q}$ is equal to $E_r^{p,q}$ for sufficiently large r. (Note that for r sufficiently large, the d_r morphisms coming into and out of $E_r^{p,q}$ extend outside the nonnegative quadrant, so they are automatically zero, and hence $E_r^{p,q} = E_{r+1}^{p,q} = E_{r+2}^{p,q} = \cdots$.)
- The "limit objects" L^n for $n \in \mathbb{N}$ are objects of $\mathcal{C}$.
- The object L^n has a filtration
$$L^n = L_0^n \supseteq L_1^n \supseteq \cdots \supseteq L_n^n \supseteq 0$$
such that the quotients of successive terms equal (respectively) the objects
$$E_\infty^{0,n}, E_\infty^{1,n-1}, \ldots, E_\infty^{n,0}$$
along a diagonal on page ∞. (Thus $E_\infty^{0,n}$ is a subobject of L_n.)

One says that $E_2^{p,q}$ **converges to** (or **abuts to**) L^{p+q}.

Proposition 6.7.1. *Suppose that*

$$E_2^{p,q} \implies L^{p+q}$$

Unofficial version for incidental online use

is a spectral sequence. Abbreviate $E_2^{p,q}$ as $E^{p,q}$. Then there is an exact sequence

$$0 \to E^{1,0} \to L^1 \to E^{0,1} \xrightarrow{d} E^{2,0} \longrightarrow \ker\left(L^2 \to E^{0,2}\right) \longrightarrow E^{1,1} \to E^{3,0}.$$

Remark 6.7.2. Spectral sequences also arise in some situations not having to do with the composition of left exact functors. For instance, cohomology of the total complex of a double complex is the limit of a spectral sequence starting with page 1.

6.7.1. The Hochschild–Serre spectral sequence in group cohomology.

Theorem 6.7.3. *Let G be a profinite group, and let H be a normal closed subgroup of G. Then there is a spectral sequence*

$$E_2^{p,q} := \mathrm{H}^p(G/H, \mathrm{H}^q(H, A)) \implies \mathrm{H}^{p+q}(G, A)$$

for each (continuous) G-module A.

Sketch of proof. The composition of the left exact functors

$$\begin{array}{ccccc} \{G\text{-modules}\} & \longrightarrow & \{G/H\text{-modules}\} & \longrightarrow & \mathbf{Ab} \\ M & \longmapsto & M^H & & \\ & & N & \longmapsto & N^{G/H} \end{array}$$

equals $M \mapsto M^G$ (all group actions are assumed continuous). One checks that the first functor takes injectives to acyclics. $\square$

Applying Proposition 6.7.1 to Theorem 6.7.3, one gets the following extension of the inflation-restriction sequence:

Corollary 6.7.4 (Inflation-restriction sequence)**.** *Let G be a profinite group, and let H be a normal closed subgroup of G. Then for any G-module A, there is an exact sequence*

$$\begin{aligned} 0 &\to \mathrm{H}^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(G, A) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(H, A)^{G/H} \\ &\to \mathrm{H}^2(G/H, A^H) \longrightarrow \ker\left(\mathrm{H}^2(G, A) \to \mathrm{H}^2(H, A)\right) \longrightarrow \mathrm{H}^1(G/H, \mathrm{H}^1(H, A)) \\ &\to \mathrm{H}^3(G/H, A^H). \end{aligned}$$

6.7.2. The Hochschild–Serre spectral sequence in étale cohomology. Recall from Example 6.5.4 that a Galois covering of schemes $X' \to X$ with Galois group G (assumed finite) is the same thing as a torsor under the constant group scheme associated to G. Then $X' \to X$ is finite and surjective, so it is fpqc. Since $X' \to X$ becomes étale after base extension by $X' \to X$, it was étale to begin with (Theorem 4.3.7(ii)).

Unofficial version for incidental online use

Theorem 6.7.5. *Let $X' \to X$ be a Galois covering of schemes with Galois group G. Let $\mathscr{F}$ be a sheaf on X_{et}. Then there is a spectral sequence*

$$\mathrm{H}^p(G, \mathrm{H}^q_{\mathrm{et}}(X', \mathscr{F})) \implies \mathrm{H}^{p+q}_{\mathrm{et}}(X, \mathscr{F}).$$

Sketch of proof. The right G-action on X' makes $\mathscr{F}(X')$ a left G-module. The sheaf condition for the open covering $\{X' \to X\}$ implies that the composition of the left exact functors

$$\begin{array}{ccccc} \{\text{sheaves on } X_{\mathrm{et}}\} & \longrightarrow & \{G\text{-modules}\} & \longrightarrow & \mathbf{Ab} \\ \mathscr{F} & \longmapsto & \mathscr{F}(X') & & \\ & & N & \longmapsto & N^G \end{array}$$

equals $\mathscr{F} \mapsto \mathscr{F}(X)$. Moreover, the first functor takes injectives to acyclics. $\square$

Remark 6.7.6. A common application of Theorem 6.7.5 is to the case where X is a k-variety and $X' = X_L$ for some finite Galois extension L of k. By taking a direct limit, one obtains an analogous spectral sequence for an *infinite* Galois extension, such as k_{s} over k.

Theorem 6.7.5 and Remark 6.7.6 help us compute Brauer groups of varieties over non-algebraically closed fields.

Definition 6.7.7. If X is a variety over a field k, let $X^{\mathrm{s}} = X_{k_{\mathrm{s}}}$ and define the **algebraic part of the Brauer group** of X by

$$\mathrm{Br}_1 X := \ker\left(\mathrm{Br}\, X \to \mathrm{Br}\, X^{\mathrm{s}}\right).$$

Corollary 6.7.8. *Let X be a proper and geometrically integral variety over a field k. Then there is an exact sequence*

$$0 \to \mathrm{Pic}\, X \to (\mathrm{Pic}\, X^{\mathrm{s}})^{\mathfrak{G}_k} \to \mathrm{Br}\, k \to \mathrm{Br}_1 X \to \mathrm{H}^1(\mathfrak{G}_k, \mathrm{Pic}\, X^{\mathrm{s}}) \to \mathrm{H}^3(k, \mathbb{G}_m).$$

Proof. We apply Theorem 6.7.5 and Remark 6.7.6 with $\mathscr{F} = \mathbb{G}_m$, and plug

$$\begin{aligned} \mathrm{H}^0_{\mathrm{et}}(X^{\mathrm{s}}, \mathbb{G}_m) &= k_{\mathrm{s}}^{\times} && \text{(Proposition 2.2.22)}, \\ \mathrm{H}^1_{\mathrm{et}}(X^{\mathrm{s}}, \mathbb{G}_m) &= \mathrm{Pic}\, X^{\mathrm{s}} && \text{(Proposition 6.6.1)}, \\ \mathrm{H}^2_{\mathrm{et}}(X^{\mathrm{s}}, \mathbb{G}_m) &= \mathrm{Br}\, X^{\mathrm{s}} && \text{(by definition)}, \\ \mathrm{H}^1_{\mathrm{et}}(X, \mathbb{G}_m) &= \mathrm{Pic}\, X && \text{(Proposition 6.6.1)}, \\ \mathrm{H}^2_{\mathrm{et}}(X, \mathbb{G}_m) &= \mathrm{Br}\, X && \text{(by definition)}, \\ \mathrm{H}^1(\mathfrak{G}_k, k_{\mathrm{s}}^{\times}) &= 0 && \text{(Hilbert's theorem 90)}, \\ \mathrm{H}^2(\mathfrak{G}_k, k_{\mathrm{s}}^{\times}) &= \mathrm{Br}\, k && \text{(Theorem 1.5.12)} \end{aligned}$$

into the exact sequence of Proposition 6.7.1. $\square$

Remark 6.7.9. For a nice k-variety X, the homomorphism

$$(\mathrm{Pic}\, X^{\mathrm{s}})^{\mathfrak{G}_k} \longrightarrow \mathrm{Br}\, k$$

Unofficial version for incidental online use

given in Corollary 6.7.8 is the same as the homomorphism constructed in the proof of Proposition 4.5.12.

Remark 6.7.10. The cohomological approach to class field theory gives as a byproduct that if k is a local or global field, then $\mathrm{H}^3(k, \mathbb{G}_m) = 0$. The local case is obtained by taking a direct limit of [**NSW08**, 7.2.2]. The number field case is [**NSW08**, 8.3.11(iv)] applied to the set S of all places of k. The function field case follows from the fact $\operatorname{scd} k \leq 2$ [**NSW08**, 8.3.17].

6.8. Residue homomorphisms

(References: [**GS06**, Chapter 6], [**Gro68d**, §2])

6.8.1. Residue homomorphisms for discrete valuation rings. Given an integral divisor D on a variety X, one has the associated discrete valuation ring R inside the function field $K := \mathbf{k}(X)$. An element of $K^\times$ need not come from the subgroup $R^\times$; the obstruction is measured by the valuation $K^\times \to \mathbb{Z}$; in other words, a rational function has no zero or pole along D if and only if its valuation is 0. Analogously, an element of $\operatorname{Br} K$ need not come from the subgroup $\operatorname{Br} R$; the obstruction is measured by a certain **residue homomorphism**:

Proposition 6.8.1. *If R is a discrete valuation ring with fraction field K and residue field k, then there is an exact sequence*

$$0 \longrightarrow \operatorname{Br} R \longrightarrow \operatorname{Br} K \xrightarrow{\text{res}} \mathrm{H}^1(k, \mathbb{Q}/\mathbb{Z}),$$

with the caveat that one must exclude the p-primary parts from all the groups if k is imperfect of characteristic p.

Proof. This is a special case of [**Gro68d**, Proposition 2.1]. □

The residue homomorphism can be defined as follows. First, we may replace R by its completion. Let K^{unr} be the maximal unramified extension of K. If k is perfect, then Example 4 in Section 1.2.4 implies that K^{unr} is C_1, so $\operatorname{Br} K^{\text{unr}} = 0$ by Proposition 1.5.28. If k is imperfect of characteristic p, then [**Gro68d**, Corollaire 1.3] implies that $\operatorname{Br} K^{\text{unr}} = 0$ still holds after the p-primary part is excluded; in the rest of this paragraph, we exclude p-primary parts in this case. Proposition 1.3.15(iii) applied to the extension K^{unr} of K implies that $\operatorname{Br} K \simeq \mathrm{H}^2(\operatorname{Gal}(K^{\text{unr}}/K), (K^{\text{unr}})^\times)$, which maps to $\mathrm{H}^2(\operatorname{Gal}(K^{\text{unr}}/K), \mathbb{Z})$ via the valuation. Also, $\operatorname{Gal}(K^{\text{unr}}/K) \simeq \mathfrak{G}_k$. Finally, the long exact sequence associated to the exact sequence of groups

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

Unofficial version for incidental online use

with trivial $\mathfrak{G}_k$-action yields an isomorphism $\mathrm{H}^1(k, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathrm{H}^2(k, \mathbb{Z})$. The composition

$$\begin{aligned} \operatorname{Br} K &\simeq \mathrm{H}^2(\operatorname{Gal}(K^{\mathrm{unr}}/K), (K^{\mathrm{unr}})^\times) \\ &\longrightarrow \mathrm{H}^2(\operatorname{Gal}(K^{\mathrm{unr}}/K), \mathbb{Z}) \simeq \mathrm{H}^2(k, \mathbb{Z}) \simeq \mathrm{H}^1(k, \mathbb{Q}/\mathbb{Z}) \end{aligned}$$

is the residue homomorphism.

Warning 6.8.2. The caveat in Proposition 6.8.1 cannot be dropped. For example, if $k = k_{\mathrm{s}} \neq \overline{k}$ and $R = k[[t]]$, then $\operatorname{Br} R \simeq \operatorname{Br} k = 0$ (Proposition 6.9.1 below), and $\mathrm{H}^1(k, \mathbb{Q}/\mathbb{Z}) = 0$ (since $\mathfrak{G}_k = \{1\}$), but $\operatorname{Br} k((t)) \neq 0$ (Exercise 1.26).

6.8.2. Residue homomorphisms for regular integral schemes, and purity. For any discrete valuation v on a field K with residue field k, applying Proposition 6.8.1 to the valuation ring gives a homomorphism $\operatorname{Br} K \overset{\mathrm{res}}{\to} \mathrm{H}^1(k, \mathbb{Q}/\mathbb{Z})$, modulo the caveat. On a regular integral noetherian scheme X, each integral divisor defines a discrete valuation v on $\mathbf{k}(X)$, and the integral divisors are in bijection with the set $X^{(1)}$ of codimension 1 points of X. Taking all the associated residue homomorphisms yields the following global variant of Proposition 6.8.1, saying roughly that an element of $\operatorname{Br} \mathbf{k}(X)$ belongs to the subgroup $\operatorname{Br} X$ if and only if it has "no poles" along any integral divisor of X.

Theorem 6.8.3. *Let X be a regular integral noetherian scheme. Then the sequence*

$$0 \longrightarrow \operatorname{Br} X \longrightarrow \operatorname{Br} \mathbf{k}(X) \xrightarrow{\mathrm{res}} \bigoplus_{x \in X^{(1)}} \mathrm{H}^1(\mathbf{k}(x), \mathbb{Q}/\mathbb{Z})$$

is exact, with the caveat that one must exclude the p-primary part of all the groups if X is of dimension ≤ 1 and some $\mathbf{k}(x)$ is imperfect of characteristic p, or if X is of dimension ≥ 2 and some $\mathbf{k}(x)$ is of characteristic p.

Proof. This is a consequence of [**Gro68d**, Proposition 2.1] and Grothendieck's *absolute cohomological purity*" conjecture, proved by Gabber; see [**Fuj02**]. □

Warning 6.8.4. The caveat in Theorem 6.8.3 cannot be removed completely. For example, suppose that $k = k_{\mathrm{s}} \neq \overline{k}$ and $X := \mathbb{P}^1_k$. Then $\operatorname{Br} X = 0$ (Theorem 6.9.7 below) and $\mathrm{H}^1(\mathbf{k}(x), \mathbb{Q}/\mathbb{Z}) = 0$ for every $x \in X^{(1)}$, but $\operatorname{Br} k(X) \neq 0$ (Exercise 1.26). On the other hand, it might be that excluding the p-primary parts for p such that some $\mathbf{k}(x)$ is imperfect of characteristic p is enough even when $\dim X \geq 2$.

Unofficial version for incidental online use

Corollary 6.8.5. *Let X be a regular integral noetherian scheme. Let Z be a closed subscheme of codimension ≥ 2, and let $U = X - Z$. Then the homomorphism $\operatorname{Br} X \to \operatorname{Br} U$ is an isomorphism, with the caveat that one considers only the ℓ-primary parts for primes ℓ invertible on X.*

Proof. Theorem 6.8.3 describes $\operatorname{Br} X$ and $\operatorname{Br} U$ as the same subgroup of $\operatorname{Br} \mathbf{k}(X)$. □

Remark 6.8.6. The caveat in Corollary 6.8.5 might be unnecessary.

Corollary 6.8.7. *Let X and X' be nice varieties over a field k. If X and X' are birational, then $\operatorname{Br} X$ and $\operatorname{Br} X'$ are isomorphic, with the caveat that one considers only the prime-to-p parts if $\operatorname{char} k = p > 0$.*

Proof. We give the proof when $\operatorname{char} k = 0$; the same proof applies to the prime-to-p parts if $\operatorname{char} k = p > 0$. The domain of definition U of the birational map $X \dashrightarrow X'$ is the complement of a closed subscheme of codimension ≥ 2 in X. Corollary 6.8.5 implies that $\operatorname{Br} X \to \operatorname{Br} U$ is an isomorphism. The composition

$$\operatorname{Br} X' \to \operatorname{Br} U \xleftarrow{\sim} \operatorname{Br} X$$

is compatible with the embeddings of all three groups in $\operatorname{Br} \mathbf{k}(X) = \operatorname{Br} \mathbf{k}(X')$. Thus $\operatorname{Br} X' \subseteq \operatorname{Br} X$. Similarly $\operatorname{Br} X \subseteq \operatorname{Br} X'$. □

Remark 6.8.8. If in Corollary 6.8.7 we assume moreover that $\dim X = \dim X' \leq 2$, then $\operatorname{Br} X \simeq \operatorname{Br} X'$; i.e., the caveat becomes unnecessary. See [**Gro68d**, Corollaire 7.5].

6.9. Examples of Brauer groups

6.9.1. Local rings and fields.

Proposition 6.9.1. *Let R be a complete local ring with residue field k. Then the quotient homomorphism $R \to k$ induces an isomorphism $\operatorname{Br} R \to \operatorname{Br} k$.*

Proof. The (equivalent) analogue for $\operatorname{Br}_{\mathrm{Az}}$ was first proved in [**Azu51**, Theorem 31]. See [**Mil80**, III.3.11(a)] for a proof for Br. □

Remark 6.9.2. Proposition 6.9.1 holds more generally for henselian local rings [**Mil80**, IV.2.13]. (See Section B.3 for the definition of henselian.) Even more generally, if R is henselian local ring with residue field k, and G is a smooth commutative group scheme over R, then $\mathrm{H}^q(R, G) \xrightarrow{\sim} \mathrm{H}^q(k, G)$ for all $q \geq 1$; see [**Gro68d**, equation (2.6)] for the case where R is a henselian discrete valuation ring, and [**Mil80**, III.3.11(b)] for the general case. For $q = 1$, we can formulate the same statement for *noncommutative* G, and it is true [**SGA 3$_{\mathbf{III}}$**, XXIV, Proposition 8.1].

Unofficial version for incidental online use

Corollary 6.9.3. *Let R be the valuation ring of a nonarchimedean local field K. Then* $\operatorname{Br} R = 0$.

Proof. The residue field k is finite, so $\operatorname{Br} k = 0$ by Theorem 1.5.32. Now use Proposition 6.9.1. □

For R and K as in Corollary 6.9.3, we have

$$\mathrm{H}^1(k, \mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}_{\text{conts}}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z},$$

so the exact sequence of Proposition 6.8.1 becomes

$$0 \longrightarrow 0 \longrightarrow \operatorname{Br} K \xrightarrow{\text{res}} \mathbb{Q}/\mathbb{Z}.$$

In fact, res is (up to sign) the homomorphism $\operatorname{inv}\colon \operatorname{Br} K \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ in Theorem 1.5.34.

6.9.2. Rings of S-integers and arithmetic schemes.

Example 6.9.4. Let k be a global field. Let S be a nonempty set of places of k containing all the archimedean places. Let $\mathcal{O}_{k,S}$ be as in Definition 1.1.1. For $v \notin S$, let $\mathbb{F}_v$ be the residue field. Theorem 6.8.3 yields an exact sequence

$$0 \longrightarrow \operatorname{Br} \mathcal{O}_{k,S} \longrightarrow \operatorname{Br} k \xrightarrow{\text{res}} \bigoplus_{v \notin S} \mathrm{H}^1(\mathbb{F}_v, \mathbb{Q}/\mathbb{Z}).$$

By the previous discussion, the homomorphism $\operatorname{Br} k \to \mathrm{H}^1(\mathbb{F}_v, \mathbb{Q}/\mathbb{Z})$ is the same as the homomorphism $\operatorname{inv}_v\colon \operatorname{Br} k \to \mathbb{Q}/\mathbb{Z}$. Comparing with the description of $\operatorname{Br} k$ in Theorem 1.5.36(i) yields an exact sequence

$$0 \longrightarrow \operatorname{Br} \mathcal{O}_{k,S} \longrightarrow \bigoplus_{v \in S} \operatorname{Br} k_v \xrightarrow{\sum \operatorname{inv}_v} \mathbb{Q}/\mathbb{Z}. \tag{6.9.5}$$

Question 6.9.6 (M. Artin)**.** If X is proper over $\mathbb{Z}$, must $\operatorname{Br} X$ be finite? [**Mil80**, IV.2.19]

A positive answer to Question 6.9.6 in the special case of nice surfaces over finite fields would already have significant implications; see Theorem 7.6.8.

6.9.3. Curves.

Theorem 6.9.7. *If X is a proper curve over a separably closed field k, then* $\operatorname{Br} X = 0$.

Proof. If k is algebraically closed and X is nice, then this follows from Proposition 6.6.7(i) and Tsen's theorem. For the general case, see [**Gro68d**, Corollaire 5.8]; the proof uses fppf cohomology. □

Unofficial version for incidental online use

6.9.4. Rational varieties. The following lemma will allow us to compute the Brauer groups of $\mathbb{P}^n_k$ and other rational varieties.

Lemma 6.9.8. *Let $\pi\colon X \to B$ be a morphism of regular integral noetherian schemes. Suppose that π has a section $s\colon B \to X$, and that the generic fiber of π is isomorphic to $\mathbb{P}^1_{\mathbf{k}(B)}$ as a $\mathbf{k}(B)$-scheme. Then $\pi^*\colon \operatorname{Br} B \to \operatorname{Br} X$ is an isomorphism.*

Proof. By functoriality, we have a diagram

$$\begin{tikzcd} \operatorname{Br}\mathbb{P}^1_{\mathbf{k}(B)} & \operatorname{Br} X \arrow[l] \arrow[d, bend right, "s^*"'] \\ \operatorname{Br}\mathbf{k}(B) \arrow[u] & \operatorname{Br} B \arrow[l] \arrow[u, bend right, "\pi^*"'] \end{tikzcd}$$

containing two commutative squares. By Proposition 6.6.7(i), we may view $\operatorname{Br} B$ as a subgroup of $\operatorname{Br}\mathbf{k}(B)$. By Corollary 6.6.9, $\operatorname{Br} X \to \operatorname{Br}\mathbb{P}^1_{\mathbf{k}(B)}$ is injective. The left vertical homomorphism is an isomorphism by Theorem 6.9.7. Hence all four groups in the diagram may be viewed as subgroups of $\operatorname{Br}\mathbb{P}^1_{\mathbf{k}(B)}$. Then π^* shows that $\operatorname{Br} B \subseteq \operatorname{Br} X$, and s^* shows that $\operatorname{Br} X \subseteq \operatorname{Br} B$. Thus $\operatorname{Br} B = \operatorname{Br} X$. $\square$

Proposition 6.9.9. *Let k be a field. Let $n \in \mathbb{Z}_{\geq 0}$. Then $\operatorname{Br} k \xrightarrow{\sim} \operatorname{Br}\mathbb{P}^n_k$.*

Proof. We use induction on n. The case $n = 0$ is trivial, so suppose that $n \geq 1$. Let $P = (1 : 0 : \cdots : 0) \in \mathbb{P}^n(k)$, and let X be the blowup of $\mathbb{P}^n$ at P. Projection from P is a rational map $\mathbb{P}^n \dashrightarrow \mathbb{P}^{n-1}$ sending $(x_0 : x_1 : \cdots : x_n)$ to $(x_1 : \cdots : x_n)$, and it has a rational section sending $(x_1 : \cdots : x_n)$ to $(1 : x_1 : \cdots : x_n)$. Resolving the indeterminacy yields a morphism $X \to \mathbb{P}^{n-1}$ with a section. Lemma 6.9.8 shows that $\operatorname{Br} X \simeq \operatorname{Br}\mathbb{P}^{n-1}$, and the inductive hypothesis yields $\operatorname{Br}\mathbb{P}^{n-1} \simeq \operatorname{Br} k$, so $\operatorname{Br} X \simeq \operatorname{Br} k$.

By functoriality we have $\operatorname{Br} k \to \operatorname{Br}\mathbb{P}^n \hookrightarrow \operatorname{Br} X$, with the injectivity coming from Corollary 6.6.9. The previous paragraph showed that the composition is an isomorphism, so $\operatorname{Br} k \to \operatorname{Br}\mathbb{P}^n$ is an isomorphism too. $\square$

Proposition 6.9.10. *Let X be a nice variety over a field k. If X is birational to $\mathbb{P}^n_k$ for some $n \geq 0$, then $\operatorname{Br} k \xrightarrow{\sim} \operatorname{Br} X$.*

Proof. If $\operatorname{char} k = 0$, this follows from Proposition 6.9.9 and Corollary 6.8.7. For the general case, see [**Sal85**, Proposition 1.7 and the paragraph after Lemma 1.2]. $\square$

Corollary 6.9.11. *Let X be a nice variety over a field k. If $X_{k_{\mathrm{s}}}$ is birational to $\mathbb{P}^n_{k_{\mathrm{s}}}$ for some $n \geq 0$, then $\operatorname{Br} X_{k_{\mathrm{s}}} = 0$ and $\operatorname{Br}_1 X = \operatorname{Br} X$.*

Unofficial version for incidental online use

6.9.5. Quadrics. A **quadric** over a field k is a degree 2 hypersurface in $\mathbb{P}^n_k$ for some $n \geq 2$.

Proposition 6.9.12. *If X is a smooth quadric over a field k, then the homomorphism $\operatorname{Br} k \to \operatorname{Br} X$ is surjective.*

Proof. By Proposition 3.5.67, the variety X is geometrically integral. By Corollary 6.7.8, it suffices to prove that $\operatorname{Br} X^{\mathrm{s}} = 0$ and $\mathrm{H}^1(\mathfrak{G}_k, \operatorname{Pic} X^{\mathrm{s}}) = 0$. Corollary 6.9.11 yields $\operatorname{Br} X^{\mathrm{s}} = 0$.

By [**Har77**, Exercise II.6.5(c) and Corollary II.6.16],

$$\operatorname{Pic} X^{\mathrm{s}} \simeq \begin{cases} \mathbb{Z} \times \mathbb{Z} & \text{if } \dim X = 2, \\ \mathbb{Z} & \text{if } \dim X = 1 \text{ or } \dim X \geq 3. \end{cases}$$

with $\mathscr{O}_{X^{\mathrm{s}}}(1)$ corresponding to 2 if $\dim X = 1$, to $(1,1)$ if $\dim X = 2$, and to 1 if $\dim X \geq 3$. If $\dim X = 1$ or $\dim X \geq 3$, then the Galois action on $\operatorname{Pic} X^{\mathrm{s}} \simeq \mathbb{Z}$ is trivial (ampleness must be preserved), so $\mathrm{H}^1(\mathfrak{G}_k, \operatorname{Pic} X^{\mathrm{s}}) = 0$. Now suppose that $\dim X = 2$. If the $\mathfrak{G}_k$-action on $\operatorname{Pic} X^{\mathrm{s}} \simeq \mathbb{Z} \times \mathbb{Z}$ is trivial, then $\mathrm{H}^1(\mathfrak{G}_k, \operatorname{Pic} X^{\mathrm{s}}) = 0$ again. If not, then $\operatorname{Pic} X^{\mathrm{s}} \simeq \mathbb{Z}[\mathfrak{G}_k/\mathfrak{G}_L]$ for some quadratic extension L of k, so by Shapiro's lemma, $\mathrm{H}^1(\mathfrak{G}_k, \operatorname{Pic} X^{\mathrm{s}}) = \mathrm{H}^1(\mathfrak{G}_L, \mathbb{Z}) = 0$. $\square$

6.9.6. Quadric bundles.

Lemma 6.9.13. *Let k be a field of characteristic 0. Let $\pi\colon X \to B$ be a flat morphism of regular integral k-varieties. Let η be the generic point of B. For $x \in X^{(1)}$ mapped by π to some $b \in B^{(1)}$, the inclusion $\mathbf{k}(b) \to \mathbf{k}(x)$ induces a homomorphism $i_x\colon \mathrm{H}^1(\mathbf{k}(b), \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^1(\mathbf{k}(x), \mathbb{Q}/\mathbb{Z})$; also let $e_{x/b} \in \mathbb{Z}_{\geq 1}$ be the ramification index, and let $\epsilon_{x,b} = e_{x/b} i_x$. If $x \in X^{(1)}$ and $b \in B^{(1)}$ satisfy $\pi(x) \neq b$, then let $\epsilon_{x,b} = 0$. Together, these $\epsilon_{x,b}$ define a homomorphism ϵ in the diagram*

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Br} B \arrow[r] \arrow[d] & \operatorname{Br} \mathbf{k}(B) \arrow[r, "\mathrm{res}"] \arrow[d] & \bigoplus_{b \in B^{(1)}} \mathrm{H}^1(\mathbf{k}(b), \mathbb{Q}/\mathbb{Z}) \arrow[d, "\epsilon"] \\ 0 \arrow[r] & \operatorname{Br} X \arrow[r] & \operatorname{Br} X_\eta \arrow[r, "\mathrm{res}"] & \bigoplus_{\substack{x \in X^{(1)} \\ \pi(x) \neq \eta}} \mathrm{H}^1(\mathbf{k}(x), \mathbb{Q}/\mathbb{Z}). \end{tikzcd} \tag{6.9.14}$$

This diagram commutes and has exact rows.

Proof. The first row is exact by Theorem 6.8.3. By Theorem 6.8.3, $\operatorname{Br} X_\eta$ is cut out in $\operatorname{Br} \mathbf{k}(X)$ by the residue homomorphisms for $x \in X^{(1)}$ lying above η, while $\operatorname{Br} X$ is cut out in $\operatorname{Br} \mathbf{k}(X)$ by the residue homomorphisms for all

Unofficial version for incidental online use

$x \in X^{(1)}$; thus the second row of (6.9.14) is exact. The first square commutes since Br is a functor. The second square commutes by Exercise 6.12. □

Proposition 6.9.15. *Let k be a field of characteristic 0. Let $\pi\colon X \to B$ be a flat morphism of regular integral k-varieties. Suppose that every fiber of π has an irreducible component of multiplicity 1 that is geometrically integral. Suppose also that the generic fiber $X_{\mathbf{k}(B)}$ is a smooth quadric over $\mathbf{k}(B)$. Then the homomorphism $\operatorname{Br} B \to \operatorname{Br} X$ is surjective.*

Proof. Proposition 6.9.12 shows that the middle vertical homomorphism of (6.9.14) is surjective. Surjectivity of the left vertical homomorphism will follow from the four-lemma if the homomorphism ϵ in (6.9.14) is injective.

Suppose that $b \in B^{(1)}$. By hypothesis, the fiber X_b has an irreducible component Z of multiplicity 1 that is a geometrically integral $\mathbf{k}(b)$-variety. Let x be the generic point of Z. By flatness, $x \in X^{(1)}$. By Proposition 2.2.19(i)⇒(iv), the extension $\mathbf{k}(x) \supseteq \mathbf{k}(b)$ is primary, so the largest separable algebraic extension of $\mathbf{k}(b)$ in $\mathbf{k}(x)$ is $\mathbf{k}(b)$. Equivalently, by Galois theory, if we choose compatible separable closures $\mathbf{k}(b)_{\mathrm{s}} \subseteq \mathbf{k}(x)_{\mathrm{s}}$, then the restriction homomorphism of absolute Galois groups $G_{\mathbf{k}(x)} \to G_{\mathbf{k}(b)}$ is surjective. Applying $\operatorname{Hom}_{\mathrm{conts}}(-, \mathbb{Q}/\mathbb{Z})$ shows that i_x is injective. Also, $e_{x/b}$ is the multiplicity of Z, which is 1. Thus $\epsilon_{x,b} = e_{x,b} i_x = i_x$, which is injective. Since for every $b \in B^{(1)}$ there exists an x as above, ϵ is injective. □

Exercises

6.1. (Kummer sequence) Let X be a scheme, and let $n \in \mathbb{Z}_{\geq 1}$. Consider the sequence of sheaves

$$1 \longrightarrow \boldsymbol{\mu}_n \longrightarrow \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \longrightarrow 1$$

on either X_{et} or X_{fppf}, where $\boldsymbol{\mu}_n(U) \hookrightarrow \mathbb{G}_m(U)$ is the inclusion, and $\mathbb{G}_m(U) \to \mathbb{G}_m(U)$ is the nth-power homomorphism.
(a) Prove that the sequence is exact when considered as a sequence of sheaves on X_{fppf}.
(b) Give an example to show that it need not be exact when considered as a sequence of sheaves on X_{et}.
(c) Prove that if $1/n \in \mathscr{O}_X$ (that is, the image of n under $\mathbb{Z} \to \mathscr{O}_X(X)$ is invertible), then the sequence is exact on X_{et}.

6.2. Is it true that the groups $\mathrm{H}^q_{\mathrm{Zar}}(X, \mathbb{G}_m)$ and $\mathrm{H}^q_{\mathrm{et}}(X, \mathbb{G}_m)$ are isomorphic for all schemes X and all $q \geq 0$?

6.3. Show that the general definition of "G-torsor over S" is equivalent, in the case where $S = \operatorname{Spec} k$ and G is a smooth algebraic group over k,

Unofficial version for noncommercial online use

to the definition of "G-torsor over k" given earlier. (*Hint*: Use the fact that smoothness is preserved by base extension and fpqc descent.)

6.4. Let k be an imperfect field of characteristic p. Fix $a \in k - k^p$, and let $X = \operatorname{Spec} k(a^{1/p})$.
(a) Prove that X can be made an $\boldsymbol{\alpha}_p$-torsor over k.
(b) Prove that X can also be made a $\boldsymbol{\mu}_p$-torsor over k.

6.5. Let k be a global field. Let S be a finite nonempty set of places of k containing all the archimedean places. Let $\mathcal{O}_{k,S}$ be the ring of S-integers. Use familiar theorems of algebraic number theory to prove that $\mathrm{H}^1_{\mathrm{fppf}}(\operatorname{Spec} \mathcal{O}_{k,S}, \boldsymbol{\mu}_n)$ is finite for each $n \geq 1$.

6.6. Let $\mathbb{H}$ be as in Example 1.5.8. Let $A = \mathbb{R}[x,y]/(x^2+y^2)$, and let $K = \operatorname{Frac} A$. Prove that the class h of the Azumaya A-algebra $\mathbb{H} \otimes_{\mathbb{R}} A$ is a nonzero element of $\ker(\operatorname{Br} A \to \operatorname{Br} K)$.

6.7. Let k be an algebraically closed field. Let X be a nice k-curve of genus g. Let n be a positive integer not divisible by $\operatorname{char} k$. Using that $\operatorname{Br} X = 0$, calculate $\mathrm{H}^q_{\mathrm{et}}(X, \boldsymbol{\mu}_n)$ for $q = 0, 1, 2$. (You may assume the following fact: if A is an abelian variety of dimension g over an algebraically closed field k and $\operatorname{char} k \nmid n$, then the multiplication-by-n homomorphism $A(k) \xrightarrow{n} A(k)$ is surjective and has kernel isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$.)

6.8. Let $\mathcal{O}$ be the ring of integers of a number field k. Using (6.9.5), show that $\operatorname{Br} \mathcal{O}$ is a finite abelian group, and compute its structure.

6.9. Let k be a finite field. Let X be a nice k-curve. Show that $\operatorname{Br} X = 0$.

6.10. Let X be a proper and geometrically integral variety over a field k. Assume that $X(k) \neq \emptyset$.
(a) Prove that the homomorphism $\operatorname{Br} k \to \operatorname{Br} X$ is injective.
(b) Prove that the homomorphism $\operatorname{Pic} X \to (\operatorname{Pic} X^{\mathrm{s}})^{\mathfrak{G}_k}$ is an isomorphism.
(c) Show that the same two conclusions hold if k is a global field and the hypothesis "$X(k) \neq \emptyset$" is weakened to "$X(k_v) \neq \emptyset$ for all places v of k".

6.11. (Brauer group of a conic) Let k be a field. Let X be a nice genus 0 curve over k. Let $c \in \operatorname{Br} k$ be the class of X viewed as a 1-dimensional Severi–Brauer variety. Prove that the homomorphism $\operatorname{Br} k \to \operatorname{Br} X$ is surjective with kernel generated by c. (*Hint*: Use the theorem of Lichtenbaum mentioned in the proof of Proposition 4.5.12.)

6.12. (Functoriality of residue homomorphisms) Let $K \subseteq K'$ be an inclusion of fields. Suppose that $v\colon K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ and $v'\colon K' \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ are discrete valuations such that $v'|_K = ev$ for some $e \in \mathbb{Z}_{\geq 1}$ (called the ramification index). Let R be the valuation ring in K, and let k be

Unofficial version for incidental online use

the residue field. Let R' be the valuation ring in K', and let k' be the residue field. The inclusion $k \hookrightarrow k'$ induces a homomorphism $i\colon \mathrm{H}^1(k, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^1(k', \mathbb{Q}/\mathbb{Z})$. Then the diagram

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Br} R \arrow[r] \arrow[d] & \operatorname{Br} K \arrow[r, "\mathrm{res}"] \arrow[d] & \mathrm{H}^1(k, \mathbb{Q}/\mathbb{Z}) \arrow[d, "ei"] \\ 0 \arrow[r] & \operatorname{Br} R' \arrow[r] & \operatorname{Br} K' \arrow[r, "\mathrm{res}"] & \mathrm{H}^1(k', \mathbb{Q}/\mathbb{Z}) \end{tikzcd} \tag{6.9.16}$$

commutes. (This result may be viewed as a generalization of Theorem 1.5.34(ii).)

Unofficial version for incidental online use

Chapter 7

The Weil conjectures

(References: [**Har77**, Appendix C], [**FK88**])

The Weil conjectures give information about the number of points on varieties over finite fields. All of them have been proved.

7.1. Statements

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let $\overline{\mathbb{Z}}$ be the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$.

Theorem 7.1.1 (Weil conjectures)**.**

(i) *Let X be a scheme of finite type over $\mathbb{F}_q$. Then there exist $\alpha_1, \ldots, \alpha_r$, $\beta_1, \ldots, \beta_s \in \overline{\mathbb{Z}}$ such that*

$$\#X(\mathbb{F}_{q^n}) = \alpha_1^n + \cdots + \alpha_r^n - \beta_1^n - \cdots - \beta_s^n$$

for all $n \geq 1$.

(ii) *If X is a smooth proper variety of dimension d over $\mathbb{F}_q$, then the plus and minus terms can be grouped as follows in alternating batches according to the absolute value of the terms:*

$$\#X(\mathbb{F}_{q^n}) = \sum_{j=1}^{b_0} \alpha_{0j}^n - \sum_{j=1}^{b_1} \alpha_{1j}^n + \sum_{j=1}^{b_2} \alpha_{2j}^n - \cdots + \sum_{j=1}^{b_{2d}} \alpha_{2d,j}^n,$$

where

- *the $b_i \in \mathbb{N}$ are the* ℓ-adic Betti numbers, *and they satisfy $b_{2d-i} = b_i$ for $i = 0, \ldots, 2d$ (the terminology will be explained in Section 7.5);*
- *the $\alpha_{ij} \in \overline{\mathbb{Z}}$ are such that the $\alpha_{2d-i,*}$ in the $(2d-i)$-th batch equal the values $q^d/\alpha_{i,*}$ in some order;*

Unofficial version for incidental online use

- $|\alpha_{ij}| = q^{i/2}$ *for all* i *and* j*, for any archimedean absolute value* $|\ |$ *on the number field* $\mathbb{Q}(\alpha_{ij})$ *(this is called the* ***Riemann hypothesis*** *for* X *because of an analogy to be explained in Remark 7.4.4).*

If moreover X *is geometrically irreducible, then*

$$b_0 = 1 \qquad\qquad b_{2d} = 1$$
$$\alpha_{01} = 1 \qquad\qquad \alpha_{2d,1} = q^d.$$

(iii) *Let* X *be a smooth proper scheme over a finitely generated subring* R *of* $\mathbb{C}$*. Let* $\mathfrak{m}$ *be a maximal ideal of* R*, so* $R/\mathfrak{m}$ *is a finite field by Remark 2.4.5, and the reduction* $X_{R/\mathfrak{m}}$ *is a smooth proper scheme over* $R/\mathfrak{m}$*. Then for* $i = 0, \ldots, 2d$*, the* b_i *in* (ii) *for* $X_{R/\mathfrak{m}}$ *equals* $\operatorname{rk} \mathrm{H}^i(X(\mathbb{C}), \mathbb{Z})$*, the* $\mathbb{Z}$*-rank of the singular cohomology group.*

A typical choice of R in (iii) is the ring of S-integers of a number field embedded in $\mathbb{C}$. Part (iii) is especially intriguing, in that it hints at a connection between singular cohomology and varieties over finite fields. This will be explained in Section 7.5.

Unofficial version for incidental online use

7.2. The case of curves

If X is a nice genus g curve over $\mathbb{C}$, then

$$\begin{aligned} \mathrm{H}^0(X(\mathbb{C}), \mathbb{Z}) &\simeq \mathbb{Z}, \\ \mathrm{H}^1(X(\mathbb{C}), \mathbb{Z}) &\simeq \mathbb{Z}^{2g}, \\ \mathrm{H}^2(X(\mathbb{C}), \mathbb{Z}) &\simeq \mathbb{Z}. \end{aligned}$$

Analogously, if X is a nice genus g curve over $\mathbb{F}_q$, then it turns out that the ℓ-adic Betti numbers of X are

$$\begin{aligned} b_0 &= 1, \\ b_1 &= 2g, \\ b_2 &= 1. \end{aligned}$$

The Weil conjectures in this case say that there exist $\lambda_1, \ldots, \lambda_{2g} \in \overline{\mathbb{Z}}$ with $|\lambda_j| = q^{1/2}$ and $\lambda_{g+i} = q/\lambda_i$ for $i = 1, \ldots, g$, such that for all $n \geq 1$,

$$\#X(\mathbb{F}_{q^n}) = 1 - (\lambda_1^n + \cdots + \lambda_{2g}^n) + q^n.$$

Corollary 7.2.1 (Hasse–Weil bound)**.** *Let* X *be a nice genus* g *curve over* $\mathbb{F}_q$*. Then*

$$\#X(\mathbb{F}_q) = q + 1 - \epsilon,$$

where the "error" ϵ *is an integer satisfying* $|\epsilon| \leq 2g\sqrt{q}$*.*

7.3. Zeta functions

(References: [**Ser65**, **Tat65**, **Tat94**])

7.3.1. The prototype: the Riemann zeta function.

(Reference: [**Ahl78**, Chapter 5, §4])

Definition 7.3.1. The **Riemann zeta function** is the meromorphic continuation of the holomorphic function defined for $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$ by

$$\zeta(s) := \sum_{n \geq 1} n^{-s}.$$

For future comparison to zeta functions of schemes, we recall some basic properties of $\zeta(s)$.

Proposition 7.3.2.

(i) *The function $\zeta(s)$ is holomorphic on $\mathbb{C}$ except for a simple pole at $s = 1$.*

(ii) *There is a* ***functional equation*** *relating $\zeta(s)$ to $\zeta(1-s)$. More precisely, if Γ denotes the* ***gamma function*** [**Ahl78**, Chapter 5, §2.4], *then the function $\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$ is entire and satisfies $\xi(s) = \xi(1-s)$.*

(iii) *The function $\zeta(s)$ vanishes at every negative even integer. The negative even integers are called the* ***trivial zeros****.*

(iv) *All other zeros of $\zeta(s)$ lie in the interior of the* ***critical strip*** *defined by $0 \leq \operatorname{Re}(s) \leq 1$. The (unproven)* ***Riemann hypothesis*** *is the statement that these nontrivial zeros lie on the* ***critical line*** *defined by $\operatorname{Re}(s) = 1/2$.*

Proof.

(i) See [**Ahl78**, Chapter 5, §4.2].

(ii) See [**Ahl78**, Chapter 5, §4.3].

(iii) See [**Ahl78**, Chapter 5, end of §4.2].

(iv) See [**Ahl78**, Chapter 5, §4.4]. □

For $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$, the unique factorization of positive integers and the formula for an infinite geometric series allow us to rewrite $\zeta(s)$ as

Unofficial version for incidental online use

an **Euler product**:

$$\begin{aligned}\zeta(s) &:= \sum_{n\geq 1} n^{-s}\\ &= \prod_{\text{primes } p} \left(1-p^{-s}\right)^{-1}\\ &= \prod_{\text{maximal ideals } \mathfrak{m}\subseteq\mathbb{Z}} \left(1-(\#(\mathbb{Z}/\mathfrak{m}))^{-s}\right)^{-1}\\ &= \prod_{\text{closed points } P\in\operatorname{Spec}\mathbb{Z}} \left(1-(\#\mathbf{k}(P))^{-s}\right)^{-1}.\end{aligned}$$

Remark 7.3.3. The factor $\pi^{-s/2}\Gamma(s/2)$ appearing in Proposition 7.3.2(ii) should be viewed as the analogue for the infinite place of $\mathbb{Q}$ of the Euler factor $(1-p^{-s})^{-1}$ for a finite prime p.

7.3.2. Schemes of finite type over $\mathbb{Z}$.

Definition 7.3.4. If X is a scheme of finite type over $\mathbb{Z}$, one defines the **zeta function** of X as

$$\zeta_X(s) := \prod_{\text{closed } P\in X} \left(1-(\#\mathbf{k}(P))^{-s}\right)^{-1}.$$

Remark 7.3.5. It is easy to show that $\zeta_X(s)$ converges in the half-plane $\{s\in\mathbb{C} : \operatorname{Re}(s) > r\}$ for some $r\in\mathbb{R}$ depending on X (see Exercise 7.2), but it is less easy to find the smallest such r.

The Riemann zeta function $\zeta(s)$ is then $\zeta_{\operatorname{Spec}\mathbb{Z}}(s)$. More generally, if k is a number field and $\mathcal{O}_k$ is its ring of integers, then $\zeta_{\operatorname{Spec}\mathcal{O}_k}(s)$ is called the **Dedekind zeta function** of k.

7.3.3. Schemes of finite type over a finite field. For schemes over a finite type over a finite field, there is a closely related definition.

Definition 7.3.6. Let X be a scheme of finite type over $\mathbb{F}_q$. Define

$$Z_X(T) := \exp\left(\sum_{n\geq 1} \#X(\mathbb{F}_{q^n})\frac{T^n}{n}\right) \quad\in\quad \mathbb{Q}[[T]].$$

Equivalently, $Z_X(T)$ is characterized by the equations

$$Z_X(0)=1, \qquad T\frac{d}{dT}\log Z_X(T) = \sum_{n\geq 1}\#X(\mathbb{F}_{q^n})T^n. \tag{7.3.7}$$

Because of the following proposition, $Z_X(T)$ too is called the zeta function of X.

Unofficial version for incidental online use

Proposition 7.3.8. *If X is a scheme of finite type over $\mathbb{F}_q$, then X is also of finite type over $\mathbb{Z}$, and we have $\zeta_X(s) = Z_X(q^{-s})$.*

Proof. See Exercise 7.3. $\square$

7.4. The Weil conjectures in terms of zeta functions

We can reformulate the Weil conjectures in terms of $Z_X(T)$, and in fact this is how they were originally expressed [**Wei49**, p. 507]:

Theorem 7.4.1 (Restatement of Weil conjectures)**.**

(i) *Let X be a scheme of finite type over $\mathbb{F}_q$. Then the power series $Z_X(T)$ is (the Taylor series of) a rational function in $\mathbb{Q}(T)$. The rational function will be of the form*
$$\frac{(1-\beta_1 T)\cdots(1-\beta_s T)}{(1-\alpha_1 T)\cdots(1-\alpha_r T)}$$
for some $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in \overline{\mathbb{Z}}$.

(ii) *If X is a smooth proper variety of dimension d over $\mathbb{F}_q$, then*
$$Z_X(T) = \frac{P_1(T)P_3(T)\cdots P_{2d-1}(T)}{P_0(T)P_2(T)P_4(T)\cdots P_{2d}(T)},$$
where $P_i \in 1 + T\mathbb{Z}[T]$ factors over $\mathbb{C}$ as $\prod_{j=1}^{b_i}(1-\alpha_{ij}T)$, with $|\alpha_{ij}| = q^{i/2}$ for any archimedean absolute value $|\ |$ on the number field $\mathbb{Q}(\alpha_{ij})$ ("Riemann hypothesis"). Also, we have the **functional equation**

$$Z_X\left(\frac{1}{q^d T}\right) = \pm q^{d\chi/2} T^{\chi} Z_X(T), \tag{7.4.2}$$

where $\chi := b_0 - b_1 + b_2 - \cdots + b_{2d} \in \mathbb{Z}$ is the **Euler characteristic** *of X. (Equation* (7.4.2) *can be equivalently expressed as a functional equation relating $\zeta_X(s)$ to $\zeta_X(d-s)$, in analogy with Proposition 7.3.2*(ii)*. The sign is specified in Exercise 7.4.) If in addition X is geometrically irreducible, then $P_0(T) = 1 - T$ and $P_{2d}(T) = 1 - q^d T$.*

(iii) *Same as in Theorem 7.1.1.*

Remark 7.4.3. The Euler characteristic χ can also be defined geometrically, without reference to Betti numbers: it equals the self-intersection number $\Delta.\Delta$ where $\Delta \subseteq X \times X$ is the **diagonal** (the graph of the identity morphism $X \to X$).

Remark 7.4.4 (Riemann hypothesis for a curve over a finite field)**.** If X is a smooth proper curve, then the zeros of $Z_X(T)$ satisfy $|T| = q^{-1/2}$, so Proposition 7.3.8 implies that the zeros of $\zeta_X(s)$ satisfy $\mathrm{Re}(s) = 1/2$, in

Unofficial version for incidental online use

analogy with Proposition 7.3.2(iv).) This explains the use of the terminology "Riemann hypothesis" for varieties over finite fields.

7.5. Cohomological explanation

(Reference: [**Del74**, §1 and §2])

7.5.1. History.

(References: [**Die75**], [**Roq02**, **Roq04**, **Roq06**])

Before Weil's work, the Weil conjectures were known for *curves* over finite fields, by work of E. Artin, Hasse, and Schmidt, except that the Riemann hypothesis was known only for curves of genus ≤ 1. Weil was led to his conjectures by this work, and by his own proof of the Riemann hypothesis for curves of arbitrary genus [**Wei48a**] and for certain varieties of higher dimension such as diagonal hypersurfaces [**Wei49**].

Weil's proof for curves proceeded by adapting the theory of correspondences to varieties in characteristic p. As Hasse observed in 1936, the problem of determining $\#X(\mathbb{F}_{q^n})$ can be converted into a purely geometric problem; namely, if F is the relative q-power Frobenius morphism on $X_{\overline{\mathbb{F}}_q}$, then $\#X(\mathbb{F}_{q^n})$ equals the number of fixed points of F^n. Weil reinterpreted this number as the intersection number of two curves in $X \times X$, namely, the graphs of the identity and F^n.

On the other hand, Lefschetz and Hopf had given a topological "trace formula" for the number of fixed points of a map from a compact manifold to itself, in terms of the action of the map on the associated singular cohomology spaces; this showed that the number of fixed points of powers of an endomorphism of a *complex* projective variety (assuming nondegeneracy) would be given by a formula such as that in Theorem 7.1.1(i). Weil's hope was that the theory of correspondences would serve in characteristic p as a *substitute* for the singular cohomology theory, given that correspondences had served him so well in the case of curves. Such a "motivic" approach (to use anachronistic terminology), however, has never been completed.

Instead, others, starting with Serre and Grothendieck in the 1950s, sought to develop an algebraic analogue of singular cohomology rich enough to accommodate a trace formula that would explain the Weil conjectures. It was this thinking that motivated the development of étale cohomology by Grothendieck, M. Artin, Verdier, and Deligne. Étale cohomology eventually proved the conjectures in full, even though the first of the conjectures, the rationality, was originally proved by a different method without cohomology, by Dwork [**Dwo60**].

Unofficial version for individual online use

7.5.2. The Lefschetz trace formula in topology. Let X be a compact differentiable real manifold of dimension d. Let $f\colon X \to X$ be a differentiable map. A **fixed point** of f is a point $x \in X$ such that $f(x) = x$. At such a point, the derivative df_x is an endomorphism of the tangent space T_xX. Call a fixed point $x \in X$ **nondegenerate** if $1 - df_x$ is invertible, where 1 is the identity endomorphism; this condition should be thought of as saying that the fixed point is of "multiplicity 1".

For $i \geq 0$, the singular cohomology group $\mathrm{H}^i(X, \mathbb{Z})$ is a finitely generated abelian group, and tensoring with $\mathbb{Q}$ yields a finite-dimensional $\mathbb{Q}$-vector space isomorphic to $\mathrm{H}^i(X, \mathbb{Q})$. Its dimension b_i is called the ith **Betti number** of X. Then f induces a $\mathbb{Q}$-linear endomorphism f^* of each $\mathrm{H}^i(X, \mathbb{Q})$, and its trace is an integer because the endomorphism comes from an endomorphism of $\mathrm{H}^i(X, \mathbb{Z})$.

Theorem 7.5.1 (Lefschetz trace formula)**.** *With notation as above, if all fixed points of f are nondegenerate, then*

$$\#\{\text{fixed points of } f\} = \sum_{i \geq 0} (-1)^i \operatorname{tr}\left(f^* | \mathrm{H}^i(X, \mathbb{Q})\right).$$

The alternating sum of traces is actually a finite sum since $\mathrm{H}^i(X, \mathbb{Q}) = 0$ for $i > d = \dim X$.

Definition 7.5.2. From now on, in this and similar situations, we use the abbreviations

$$\operatorname{tr}(f | \mathrm{H}^*(X, \mathbb{Q})) := \sum_{i \geq 0} (-1)^i \operatorname{tr}\left(f^* | \mathrm{H}^i(X, \mathbb{Q})\right),$$

$$\det(1 - Tf | \mathrm{H}^*(X, \mathbb{Q})) := \prod_{i \geq 0} \det\left(1 - Tf^* | \mathrm{H}^i(X, \mathbb{Q})\right)^{(-1)^i},$$

where T is an indeterminate.

The following is a simplified version of Poincaré duality, stated in a form suitable for adaptation to the étale setting.

Theorem 7.5.3 (Poincaré duality)**.** *If X is an oriented connected compact real differentiable manifold of dimension d, then $\mathrm{H}^d(X, \mathbb{Q}) \simeq \mathbb{Q}$, and there are cup-product pairings*

$$\mathrm{H}^i(X, \mathbb{Q}) \times \mathrm{H}^{d-i}(X, \mathbb{Q}) \longrightarrow \mathrm{H}^d(X, \mathbb{Q}) \simeq \mathbb{Q}$$

that are perfect pairings for each i. In particular, $b_i = b_{d-i}$ for each i.

If X is a connected compact *complex* manifold of complex dimension d, then X is automatically oriented, and its dimension as a real manifold is $2d$.

Unofficial version for incidental online use

7.5.3. Some ℓ-adic cohomology. If $n \in \mathbb{Z}$, we write $1/n \in \mathscr{O}_X$ to mean that the image of n in $\Gamma(X, \mathscr{O}_X)$ is a unit, or equivalently, that each point of X has residue field of characteristic not dividing n.

Definition 7.5.4. Let X be a scheme. Fix a prime ℓ with $1/\ell \in \mathscr{O}_X$. For $i \in \mathbb{N}$, define

$$\mathrm{H}^i(X, \mathbb{Z}_\ell) := \varprojlim_n \mathrm{H}^i_{\mathrm{et}}(X, \mathbb{Z}/\ell^n\mathbb{Z}).$$

(To simplify notation, we omit the subscript $_{\mathrm{et}}$.) When equipped with the profinite topology, this is a continuous $\mathbb{Z}_\ell$-module. Also define a $\mathbb{Q}_\ell$-vector space

$$\mathrm{H}^i(X, \mathbb{Q}_\ell) := \mathrm{H}^i(X, \mathbb{Z}_\ell) \underset{\mathbb{Z}_\ell}{\otimes} \mathbb{Q}_\ell.$$

These definitions will be applied especially when X is a variety over a *separably closed* field, since it is this case that most closely models the singular cohomology of a complex variety. If X is a variety over a smaller field, typically one forms the base extension X_K for some separably closed field $K \supseteq k$ before taking its cohomology. One can show that the resulting cohomology is unchanged upon passing from one separably closed field to a larger one, so it does not matter much which K is chosen.

Example 7.5.5. Let A be a g-dimensional abelian variety over a field k. Let ℓ be a prime not equal to $\operatorname{char} k$. The **Tate module** of A is defined by

$$T_\ell A := \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(k_{\mathrm{s}})) = \varprojlim_n A(k_{\mathrm{s}})[\ell^n],$$

where each homomorphism $A(k_{\mathrm{s}})[\ell^{n+1}] \to A(k_{\mathrm{s}})[\ell^n]$ in the inverse system is multiplication-by-ℓ. It turns out that $T_\ell A$ is a free $\mathbb{Z}_\ell$-module of rank $2g$ equipped with a continuous action of $\mathfrak{G}_k$. It acts as if it were an "étale homology group $\mathrm{H}_1^{\mathrm{et}}(A_{k_{\mathrm{s}}}, \mathbb{Z}_\ell)$" in the sense that its $\mathbb{Z}_\ell$-dual $\operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A, \mathbb{Z}_\ell)$ is canonically isomorphic to $\mathrm{H}^1(A_{k_{\mathrm{s}}}, \mathbb{Z}_\ell)$, as it turns out. See Exercise 7.5 for another way in which $T_\ell A$ acts like homology. One also defines a $\mathbb{Q}_\ell$-vector space $V_\ell A := (T_\ell A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

Remark 7.5.6. More generally, it turns out that for any smooth proper variety X over a separably closed field k, for any prime $\ell \neq \operatorname{char} k$, and any $i \geq 0$, the $\mathbb{Z}_\ell$-module $\mathrm{H}^i(X, \mathbb{Z}_\ell)$ is finitely generated. Its rank, which by definition equals $\dim_{\mathbb{Q}_\ell} \mathrm{H}^i(X, \mathbb{Q}_\ell)$, is called the ith **ℓ-adic Betti number** b_i of X. This is in analogy with Section 7.5.2.

If k is not separably closed, one generally base-extends X to k_{s} or $\overline{k}$ before defining its Betti numbers.

Remark 7.5.7. There is another approach to defining étale cohomology with $\mathbb{Z}_\ell$ or $\mathbb{Q}_\ell$ coefficients, via the pro-étale topology; see **[BS15]**.

Unofficial version for incidental online use

7.5.4. Tate twists. There is a "twisted" variant of ℓ-adic cohomology:

Definition 7.5.8. Let X be a scheme, and let $n \in \mathbb{Z}_{>0}$ be such that $1/n \in \mathscr{O}_X$. For $m \in \mathbb{Z}$, the **Tate twist** $(\mathbb{Z}/n\mathbb{Z})(m)$ is a sheaf on X_{et} defined as follows:

$$(\mathbb{Z}/n\mathbb{Z})(m) := \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{if } m = 0, \\ (\boldsymbol{\mu}_n)^{\otimes m} & \text{if } m > 0, \\ \mathbf{Hom}((\boldsymbol{\mu}_n)^{\otimes(-m)}, \mathbb{Z}/n\mathbb{Z}) & \text{if } m < 0. \end{cases}$$

Again fix a prime ℓ with $1/\ell \in \mathscr{O}_X$. Also fix $m \in \mathbb{Z}$. For each $n \geq 0$, there is a natural surjection $(\mathbb{Z}/\ell^{n+1}\mathbb{Z})(m) \to (\mathbb{Z}/\ell^n\mathbb{Z})(m)$. (For example, when $m = 1$, it is the ℓth-power homomorphism $\boldsymbol{\mu}_{\ell^{n+1}} \to \boldsymbol{\mu}_{\ell^n}$.) For $i \in \mathbb{N}$ and $m \in \mathbb{Z}$, define

$$\begin{aligned} \mathrm{H}^i(X, \mathbb{Z}_\ell(m)) &:= \varprojlim_n \mathrm{H}^i_{\text{et}}(X, (\mathbb{Z}/\ell^n\mathbb{Z})(m)), \\ \mathrm{H}^i(X, \mathbb{Q}_\ell(m)) &:= \mathrm{H}^i(X, \mathbb{Z}_\ell(m)) \underset{\mathbb{Z}_\ell}{\otimes} \mathbb{Q}_\ell. \end{aligned}$$

When $X = \operatorname{Spec} k$, one can also view $(\mathbb{Z}/n\mathbb{Z})(m)$, $\mathbb{Z}_\ell(m)$, and $\mathbb{Q}_\ell(m)$ as continuous $\mathfrak{G}_k$-modules. In particular, $\mathbb{Q}_\ell(m)$ is a 1-dimensional continuous character of $\mathfrak{G}_k$, and $\mathbb{Q}_\ell(1)$ is called the **cyclotomic character**.

Suppose that k is separably closed. Then k contains all ℓ-power roots of unity. If we choose generators ζ_{ℓ^n} of the abelian group μ_{ℓ^n} for all $n \geq 1$ compatibly (i.e., such that $\zeta_{\ell^{n+1}}^\ell = \zeta_{\ell^n}$), then we obtain compatible isomorphisms $\mathbb{Z}/\ell^n\mathbb{Z} \to \boldsymbol{\mu}_{\ell^n}$ and $\mathbb{Z}_\ell \to \mathbb{Z}_\ell(1)$ and $\mathbb{Q}_\ell \to \mathbb{Q}_\ell(1)$. Thus the Tate twists do nothing.

Now let k be an arbitrary field. The previous paragraph shows that $\mathrm{H}^i(X_{k_s}, \mathbb{Q}_\ell(m))$ and $\mathrm{H}^i(X_{k_s}, \mathbb{Q}_\ell)$ are isomorphic *as abelian groups*. But they may differ when the action of $\mathfrak{G}_k$ is taken into account. The precise relationship is as follows:

Proposition 7.5.9. *There is an isomorphism of $\mathbb{Q}_\ell$-representations of $\mathfrak{G}_k$*

$$\mathrm{H}^i(X_{k_s}, \mathbb{Q}_\ell(m)) \simeq \mathrm{H}^i(X_{k_s}, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell(m).$$

Proof. On X_{k_s}, we may identify $(\mathbb{Z}/\ell^n\mathbb{Z})(m)$ with $\mathbb{Z}/\ell^n\mathbb{Z}$ by choosing a generator ζ of the $\mathfrak{G}_k$-module $(\mathbb{Z}/\ell^n\mathbb{Z})(m)$. Hence we obtain an isomorphism of abelian groups

$$\mathrm{H}^i(X_{k_s}, \mathbb{Z}/\ell^n\mathbb{Z}) \otimes_{\mathbb{Z}/\ell^n\mathbb{Z}} (\mathbb{Z}/\ell^n\mathbb{Z})(m) \longrightarrow \mathrm{H}^i(X_{k_s}, (\mathbb{Z}/\ell^n\mathbb{Z})(m)).$$

This isomorphism is independent of the choice of ζ, so it is $\mathfrak{G}_k$-equivariant. Take inverse limits and tensor with $\mathbb{Q}_\ell$. $\square$

Unofficial version for personal online use

7.5.5. The Lefschetz trace formula in étale cohomology. If X is a scheme of finite type over a separably closed field, and $d := \dim X$, then it turns out that $\mathrm{H}^i(X, \mathbb{Q}_\ell) = 0$ for all i outside the range $0 \le i \le 2d$ (this is a consequence of [**SGA** $4_{\mathbf{III}}$, X, Corollaire 4.3]).

Theorem 7.5.10 (Grothendieck–Lefschetz trace formula)**.** *Let X be a smooth proper variety over an algebraically closed field k. Fix a prime $\ell \neq \operatorname{char} k$. Let $f \colon X \to X$ be a k-morphism such that each fixed point in $X(k)$ is nondegenerate* (*in the same sense as in Section 7.5.2, but using the Zariski tangent space*)*. Then*

$$\#\{\text{fixed points of } f \text{ in } X(k)\} = \operatorname{tr}\left(f|\mathrm{H}^*(X, \mathbb{Q}_\ell)\right)$$

in $\mathbb{Q}_\ell$, where the right-hand side is defined as in Definition 7.5.2.

Proof. See [**SGA** $4\frac{1}{2}$, Cycle, Corollaire 3.7]. □

Remark 7.5.11. More generally, without the nondegeneracy hypothesis, the formula remains true if we replace the left-hand side by the intersection number $\Gamma.\Delta$ computed in $X \times X$, where Γ is the graph of f and Δ is the diagonal [**SGA** $4\frac{1}{2}$, Cycle, Corollaire 3.7].

Theorem 7.5.12 (Poincaré duality in ℓ-adic cohomology)**.** *Let X be a smooth proper integral variety of dimension d over a separably closed field k. Fix a prime $\ell \neq \operatorname{char} k$.*

(a) *There is a natural isomorphism $\mathrm{H}^{2d}(X, \mathbb{Q}_\ell(d)) \simeq \mathbb{Q}_\ell$.*

(b) *Cup product defines a perfect pairing*

$$\mathrm{H}^r(X, \mathbb{Q}_\ell(i)) \times \mathrm{H}^{2d-r}(X, \mathbb{Q}_\ell(d-i)) \longrightarrow \mathrm{H}^{2d}(X, \mathbb{Q}_\ell(d)) \simeq \mathbb{Q}_\ell$$

for each $r, i \in \mathbb{Z}$.

Proof. This is a consequence of [**Mil80**, VI.11.2]. □

Remark 7.5.13. As at the end of Section 7.5.4, the Tate twists do not change the $\mathbb{Q}_\ell$-vector spaces; they only change the Galois action in the setting that X comes from a variety defined over a subfield $k_0 \le k$. For fixed r, Proposition 7.5.9 shows that if Theorem 7.5.12 holds for some i, then it holds for all i.

7.5.6. Arithmetic and geometric Frobenius. Fix a power q of a prime p. Define the **arithmetic Frobenius** σ to be the *field* automorphism of $\overline{\mathbb{F}}_q$ given by $\sigma(a) = a^q$. Write σ also for the induced morphism $\operatorname{Spec} \overline{\mathbb{F}}_q \to \operatorname{Spec} \overline{\mathbb{F}}_q$.

Unofficial version for incidental online use

Let X be a smooth proper variety over $\mathbb{F}_q$. Let $\overline{X} = X \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. The field automorphism σ gives rise to an automorphism

$$\overline{X} = X \underset{\mathbb{F}_q}{\times} \overline{\mathbb{F}}_q \xrightarrow{1\times\sigma} X \underset{\mathbb{F}_q}{\times} \overline{\mathbb{F}}_q = \overline{X}.$$

Let $F_{\overline{X}} \colon \overline{X} \to \overline{X}$ be the absolute q-power Frobenius morphism. Finally, let $F = F_{\overline{X}/\overline{\mathbb{F}}_q} \colon \overline{X} \to \overline{X}$ be the relative q-power Frobenius morphism (Remark 3.7.6).

The diagram (3.7.1) for $\overline{X} \to \operatorname{Spec} \overline{\mathbb{F}}_q$ (with q in place of p) is

(7.5.14)
$$\begin{tikzcd}
\overline{X} \arrow[dr, dotted, "F"] \arrow[drr, bend left, "F_{\overline{X}}"] \arrow[ddr, bend right] & & \\
& \overline{X} \arrow[r, "1\times\sigma"] \arrow[d] & \overline{X} \arrow[d] \\
& \operatorname{Spec}\overline{\mathbb{F}}_q \arrow[r, "\sigma"] & \operatorname{Spec}\overline{\mathbb{F}}_q .
\end{tikzcd}$$

Warning 7.5.15. Of the three morphisms F, $F_{\overline{X}}$, and $1 \times \sigma$, only F is a morphism of $\overline{\mathbb{F}}_q$-varieties, and usually only $1 \times \sigma$ is an automorphism.

Warning 7.5.16. Diagram (7.5.14) for $\overline{X} \to \operatorname{Spec} \overline{\mathbb{F}}_q$ is not the same as the base extension by $\operatorname{Spec} \overline{\mathbb{F}}_q \to \operatorname{Spec} \mathbb{F}_q$ of the corresponding diagram for $X \to \operatorname{Spec} \mathbb{F}_q$. For example, the absolute Frobenius $F_{\overline{X}}$ is different from the base extension of F_X.

The $\mathbb{Q}_\ell$-vector space $\mathrm{H}^i(\overline{X}, \mathbb{Q}_\ell)$ is finite-dimensional by Remark 7.5.6. By contravariant functoriality, each morphism of schemes $\overline{X} \to \overline{X}$ (not necessarily an $\overline{\mathbb{F}}_q$-morphism) induces a $\mathbb{Q}_\ell$-linear endomorphism of $\mathrm{H}^i(\overline{X}, \mathbb{Q}_\ell)$. We compare these for the three morphisms at the top of (7.5.14).

Proposition 7.5.17. *Let X be a smooth proper variety over $\mathbb{F}_q$. With notation as above, the endomorphism of $\mathrm{H}^i(\overline{X}, \mathbb{Q}_\ell)$ induced by the relative Frobenius morphism F is the* inverse *of the endomorphism induced by $1 \otimes \sigma$.*

Proof. Lemma 3.7.5 applied to étale morphisms to $\overline{X}$ implies that $F_{\overline{X}}$ acts as the identity on the category of étale $\overline{X}$-schemes, and hence as the identity on $\mathrm{H}^i(\overline{X}, \mathbb{Q}_\ell)$. Now the result follows from (7.5.14). $\square$

Because of Proposition 7.5.17, the field automorphism $\sigma^{-1} \in \operatorname{Aut} \overline{\mathbb{F}}_q$ and the corresponding automorphism $1 \times \sigma^{-1}$ of $\overline{X}$ are both called **geometric Frobenius** (cf. [**Del74**, 1.15]).

Unofficial version for incidental online use

7.5.7. Deducing the Weil conjectures. Let X be a smooth proper variety of dimension d over $\mathbb{F}_q$. Let $\overline{X} = X_{\overline{\mathbb{F}}_q}$. Let $F\colon \overline{X} \to \overline{X}$ be the relative q-power Frobenius morphism. Then $\#X(\mathbb{F}_{q^n})$ is the number of fixed points of the nth iterate F^n. Also, the derivative of F is everywhere 0, so fixed points of F and its powers are automatically nondegenerate. So applying the Grothendieck–Lefschetz trace formula (Theorem 7.5.10) to $\overline{X}$ and F^n yields

$$\#X(\mathbb{F}_{q^n}) = \operatorname{tr}\left(F^n|\mathrm{H}^*(\overline{X},\mathbb{Q}_\ell)\right). \tag{7.5.18}$$

Thus

$$\begin{aligned}
Z_X(T) &= \exp\left(\sum_{n\geq 1} \#X(\mathbb{F}_{q^n})\frac{T^n}{n}\right) && \text{(Definition 7.3.6)}\\
&= \exp\left(\sum_{n\geq 1} \operatorname{tr}\left(F^n|\mathrm{H}^*(\overline{X},\mathbb{Q}_\ell)\right)\frac{T^n}{n}\right)\\
&= \det\left(1 - TF|\mathrm{H}^*(\overline{X},\mathbb{Q}_\ell)\right)^{-1} && \text{(by Exercise 7.6)}\\
&= \frac{P_1(T)\,P_3(T)\cdots P_{2d-1}(T)}{P_0(T)\,P_2(T)\,P_4(T)\cdots P_{2d}(T)},
\end{aligned}$$

where

$$P_i(t) := \det\left(1 - TF|\mathrm{H}^i(\overline{X},\mathbb{Q}_\ell)\right) \in \mathbb{Q}_\ell[T].$$

In particular, $Z_X(T)$ is a rational function in $\mathbb{Q}_\ell(T)$. But $Z_X(T)$ is also in $1 + T\mathbb{Z}[[T]]$ by Proposition 7.3.8, so $Z_X(T) \in \mathbb{Q}(T)$.

For each i, let $b_i = \dim \mathrm{H}^i(\overline{X},\mathbb{Q}_\ell)$, and let $\alpha_{i1},\ldots,\alpha_{i,b_i}$ be the eigenvalues of $F^*|\mathrm{H}^i(\overline{X},\mathbb{Q}_\ell)$ counted with multiplicity; then

$$P_i(t) = \prod_{j=1}^{b_i}(1 - \alpha_{ij}T).$$

The α_{ij} turn out to be nonzero, so $\deg P_i = b_i$.

The identity $1_X\colon X \to X$ induces the identity on each space $\mathrm{H}^i(\overline{X},\mathbb{Q}_\ell)$, so Remark 7.5.11 applied to 1_X yields

$$\Delta.\Delta = \sum_{i=0}^{2d}(-1)^i b_i = \chi,$$

as claimed in Remark 7.4.3.

Now suppose in addition that $\overline{X}$ is integral. Twisting the isomorphism in Theorem 7.5.12(a) by $-d$ shows that

$$\mathrm{H}^{2d}(\overline{X},\mathbb{Q}_\ell) \simeq \mathbb{Q}_\ell(-d).$$

Unofficial version for incidental online use

In particular, $b_{2d} = 1$. With notation as in Section 7.5.6, Proposition 7.5.17 shows that F^* acts on $\mathrm{H}^{2d}(\overline{X}, \mathbb{Q}_\ell)$ as σ^{-1} acts on $\mathbb{Q}_\ell(-d)$, i.e., as multiplication by q^d. The Galois equivariance of the perfect pairing in Theorem 7.5.12(b) shows that the eigenvalues $\alpha_{2d-i,*}$ of F^* (or σ^{-1}) acting on the space $\mathrm{H}^{2d-i}(\overline{X}, \mathbb{Q}_\ell)$ are the *inverses* of the eigenvalues of σ^{-1} acting on $\mathrm{H}^i(\overline{X}, \mathbb{Q}_\ell(d))$; the latter eigenvalues are α_i/q^d, because of the twist. This explains the functional equation.

The relationship between ℓ-adic Betti numbers and classical Betti numbers arises from a theorem comparing ℓ-adic and singular cohomology for a $\mathbb{C}$-variety, and a theorem about how $\mathrm{H}^i(\overline{X}, \mathbb{Q}_\ell)$ behaves under specialization.

All that remains is to prove that each eigenvalue α_{ij} is an algebraic integer with $|\alpha_{ij}| = q^{i/2}$. This was shown by Deligne using further properties of ℓ-adic cohomology; see [**Del74**, Théorème 1.6] and [**Del80**, Théorème 2]. See also [**Kat76**] for an overview of the proof.

7.5.8. Nonproper varieties.

Remark 7.5.19. The cohomological approach generalizes to $\mathbb{F}_q$-varieties that are not proper. The Grothendieck–Lefschetz trace formula holds for a variety over a separably closed field once one replaces $\mathrm{H}^r(X, \mathbb{Q}_\ell)$ with "cohomology with compact support" $\mathrm{H}^r_c(X, \mathbb{Q}_\ell)$; cf. [**Gro68a**] and [**Del74**, Théorème 2.8]. And for a smooth integral variety of dimension d over a separably closed field, Poincaré duality gives a perfect pairing

$$\mathrm{H}^r_c(X, \mathbb{Q}_\ell(i)) \times \mathrm{H}^{2d-r}(X, \mathbb{Q}_\ell(d-i)) \longrightarrow \mathrm{H}^{2d}_c(X, \mathbb{Q}_\ell(d)) \simeq \mathbb{Q}_\ell$$

involving both kinds of cohomology; cf. [**SGA** $4_{\mathbf{III}}$, XVIII, Théorème 2.14 and (3.2.6.2)].

Lemma 7.5.20. *Let X be a d-dimensional variety over a separably closed field k. If $U \subseteq X$ is a dense open subscheme, then the restriction map $\mathrm{H}^{2d}_c(X, \mathbb{Q}_\ell(d)) \to \mathrm{H}^{2d}_c(U, \mathbb{Q}_\ell(d))$ is an isomorphism.*

Proof. This is a consequence of [**SGA** $4_{\mathbf{III}}$, XVIII, Lemme 2.1]. □

Corollary 7.5.21. *Let X be a d-dimensional variety over a separably closed field k. Then $\mathrm{H}^{2d}_c(X, \mathbb{Q}_\ell(d))$ is naturally the $\mathbb{Q}_\ell$-vector space having as basis the set of d-dimensional irreducible components of X.*

Proof. Lemma 7.5.20 lets us replace X by a dense open subscheme so that its irreducible components are disjoint. Then the statement reduces to the irreducible case already mentioned in Remark 7.5.19. □

Unofficial version for incidental online use

7.6. Cycle class homomorphism

In this section, X is a variety that is smooth of dimension d over a field k. We will occasionally impose more restrictive conditions.

7.6.1. Algebraic cycles.

(Reference: [**Ful98**, Chapter 1])

The group $\operatorname{Pic} X$ may be identified with the group of Weil divisors modulo linear equivalence. And by definition, a Weil divisor is an integer combination of integral closed subschemes of codimension 1. We now generalize to higher codimension.

For $r \in \mathbb{N}$, **the group of codimension r cycles**, denoted $\mathscr{Z}^r(X)$, is defined as the free abelian group on the set of codimension r integral closed subschemes of X. For instance, $\mathscr{Z}^1(X)$ is the group of Weil divisors on X. If $r > d$, then $\mathscr{Z}^r(X) = 0$.

For each codimension r integral closed subscheme Z, let $[Z] \in \mathscr{Z}^r(X)$ denote the basis element corresponding to Z. More generally, if $Y \subseteq X$ is any closed subscheme whose irreducible components Y_i are of codimension r in X, let y_i be the generic point of Y_i, let ℓ_i be the length of the artinian ring $\mathscr{O}_{Y,y_i}$, and define $[Y] := \sum \ell_i [Y_i] \in \mathscr{Z}^r(X)$.

There is a notion of **rational equivalence** of cycles that for $r = 1$ becomes linear equivalence of divisors. The **Chow group** $\mathrm{CH}^r(X)$ is the group of codimension r cycles modulo rational equivalence; see [**Ful98**, §1.3 and §1.6], where $\mathrm{CH}^r(X)$ is denoted by $A^r(X)$. For instance, $\mathrm{CH}^1(X) = \operatorname{Pic} X$.

7.6.2. Changing the base field. Given a field extension $L \supseteq k$, there is a base change homomorphism $\mathscr{Z}^r(X) \to \mathscr{Z}^r(X_L)$ sending each basis element $[Z]$ to $[Z_L]$. Even though Z is integral, Z_L might not be, so $[Z_L]$ must be defined in terms of lengths as in Section 7.6.1.

Proposition 7.6.1. *Let $L \supseteq k$ be an extension of fields. Let X be a smooth k-variety. Let $r \in \mathbb{N}$.*

(a) *The homomorphism $\mathscr{Z}^r(X) \to \mathscr{Z}^r(X_L)$ is injective.*
(b) *If L is Galois over k with Galois group G, then the homomorphism $\mathscr{Z}^r(X) \to \mathscr{Z}^r(X_L)^G$ is an isomorphism.*

Proof.

(a) For Z varying over codimension r integral closed subschemes of X, the subschemes Z_L are nonempty and do not share irreducible components, so the classes $[Z_L]$ are linearly independent.

Unofficial version for individual online use

(b) Consider a G-orbit of codimension r integral closed subscheme of X_L, and let Y be their union, a closed subscheme of X_L. Although descent of schemes is not effective in general, in the present setting we can descend the ideal sheaf of Y to show that $Y = Z_L$ for some closed subscheme $Z \subseteq X$. If Z were not reduced, then Y would not be reduced either. If Z were not irreducible, then Y would not consist of exactly one G-orbit. Thus Z is integral, and $[Z]$ maps to $[Y]$. Such classes $[Y]$ form a basis of $\mathcal{Z}^r(X_L)^G$, so $\mathcal{Z}^r(X) \to \mathcal{Z}^r(X_L)^G$ is an isomorphism. $\square$

7.6.3. Cohomology classes of divisors. Taking cohomology of the Kummer sequence

$$1 \longrightarrow \boldsymbol{\mu}_{\ell^n} \longrightarrow \mathbb{G}_m \xrightarrow{\ell^n} \mathbb{G}_m \longrightarrow 1$$

of sheaves on X_{et} yields a connecting homomorphism

$$\operatorname{Pic} X = \mathrm{H}^1(X, \mathbb{G}_m) \longrightarrow \mathrm{H}^2(X, (\mathbb{Z}/\ell^n\mathbb{Z})(1)).$$

These are compatible as n varies, so we obtain homomorphisms

$$\operatorname{Pic} X \longrightarrow \mathrm{H}^2(X, \mathbb{Z}_\ell(1)) \longrightarrow \mathrm{H}^2(X, \mathbb{Q}_\ell(1)), \tag{7.6.2}$$

whose composition will be denoted $\mathrm{cl}_{\mathrm{et}}$.

7.6.4. Cohomology classes of higher-codimension cycles. In this section, k is algebraically closed. Let $Z \subseteq X$ be an integral closed subscheme of codimension r, so $\dim Z = d - r$. Our goal is to define a cohomology class $\mathrm{cl}_{\mathrm{et}}(Z) \in \mathrm{H}^{2r}(X, \mathbb{Q}_\ell(r))$.

Case 1: X and Z are nice. The inclusion $Z \hookrightarrow X$ induces

$$\mathrm{H}^{2d-2r}(X, \mathbb{Q}_\ell(d-r)) \longrightarrow \mathrm{H}^{2d-2r}(Z, \mathbb{Q}_\ell(d-r)) \simeq \mathbb{Q}_\ell, \tag{7.6.3}$$

by Theorem 7.5.12(a) for Z. By Theorem 7.5.12(b) for X, this linear functional corresponds to an element of $\mathrm{H}^{2r}(X, \mathbb{Q}_\ell(r))$ denoted $\mathrm{cl}_{\mathrm{et}}(Z)$.

Case 2: X and Z are smooth and integral. Replace (7.6.3) by

$$\mathrm{H}_c^{2d-2r}(X, \mathbb{Q}_\ell(d-r)) \longrightarrow \mathrm{H}_c^{2d-2r}(Z, \mathbb{Q}_\ell(d-r)) \simeq \mathbb{Q}_\ell,$$

which again by Poincaré duality (Remark 7.5.19) defines an element $\mathrm{cl}_{\mathrm{et}}(Z) \in \mathrm{H}^{2r}(X, \mathbb{Q}_\ell(r))$. (In fact, Case 1 was unnecessary since it is subsumed by Case 2.)

Case 3: X is smooth and integral, and Z is integral. Let $X' = X - Z^{\mathrm{sing}}$ and $Z' = Z - Z^{\mathrm{sing}}$. Case 2 defines $\mathrm{cl}_{\mathrm{et}}(Z') \in \mathrm{H}^{2r}(X', \mathbb{Q}_\ell(r))$. Using the fact that X' differs from X only in a subset of codimension $> r$, one can show that the map $\mathrm{H}^{2r}(X, \mathbb{Q}_\ell(r)) \to \mathrm{H}^{2r}(X', \mathbb{Q}_\ell(r))$ is an isomorphism (cf. [**SGA** $4\frac{1}{2}$, Cycle, 2.2.10]). Let $\mathrm{cl}_{\mathrm{et}}(Z)$ be the element of $\mathrm{H}^{2r}(X, \mathbb{Q}_\ell(r))$ corresponding to $\mathrm{cl}_{\mathrm{et}}(Z') \in \mathrm{H}^{2r}(X', \mathbb{Q}_\ell(r))$.

Unofficial version for incremental online use

Case 4: X is smooth, and Z is integral (*the general case*). Extending $\mathbb{Z}$-linearly, and taking direct sums over the components of X if X is not integral, we obtain a **cycle class homomorphism**

$$\mathrm{cl}_{\mathrm{et}} \colon \mathscr{Z}^r(X) \longrightarrow \mathrm{H}^{2r}(X, \mathbb{Q}_\ell(r)).$$

Rationally equivalent cycles have the same image under $\mathrm{cl}_{\mathrm{et}}$; in other words, $\mathrm{cl}_{\mathrm{et}}$ factors through the quotient $\mathrm{CH}^r(X)$. Even better, *algebraically* equivalent cycles have the same image under $\mathrm{cl}_{\mathrm{et}}$ [**SGA** $4\frac{1}{2}$, Cycle, Remarque 2.3.10].

The homomorphism $\mathrm{CH}^1(X) \to \mathrm{H}^2(X, \mathbb{Q}_\ell(1))$ is the same as the homomorphism (7.6.2).

7.6.5. The Tate conjecture.

(Reference: [**Tat94**])

Which cohomology classes in $\mathrm{H}^{2r}(X, \mathbb{Q}_\ell(r))$ are in the image of $\mathrm{cl}_{\mathrm{et}}$, or at least in the $\mathbb{Q}_\ell$-span of the image? The Tate conjecture attempts to answer this question. It is analogous to the Hodge conjecture, which, for a smooth projective $\mathbb{C}$-variety, attempts to describe the $\mathbb{Q}$-span of the image of the analogous cycle class homomorphism from $\mathscr{Z}^r(X)$ to the singular cohomology group $\mathrm{H}^{2r}(X(\mathbb{C}), \mathbb{Q})$.

Let X be a nice variety over a field k that is not necessarily algebraically closed. Let $\mathfrak{G} = \mathrm{Gal}(k_{\mathrm{s}}/k) = \mathrm{Aut}(\overline{k}/k)$. Fix $r \geq 0$. The homomorphisms

$$\mathscr{Z}^r(X_{k_{\mathrm{s}}}) \longrightarrow \mathscr{Z}^r(X_{\overline{k}}) \xrightarrow{\mathrm{cl}_{\mathrm{et}}} \mathrm{H}^{2r}(X_{\overline{k}}, \mathbb{Q}_\ell(r)) \simeq \mathrm{H}^{2r}(X_{k_{\mathrm{s}}}, \mathbb{Q}_\ell(r))$$

are $\mathfrak{G}$-equivariant, and taking $\mathfrak{G}$-invariants yields a homomorphism

$$\mathscr{Z}^r(X) \longrightarrow \mathrm{H}^{2r}(X_{k_{\mathrm{s}}}, \mathbb{Q}_\ell(r))^{\mathfrak{G}},$$

by Proposition 7.6.1(b). Extending $\mathbb{Q}_\ell$-linearly yields a $\mathbb{Q}_\ell$-linear cycle class homomorphism

$$\mathscr{Z}^r(X) \otimes \mathbb{Q}_\ell \xrightarrow{\mathrm{cl}_{\mathrm{et}}} \mathrm{H}^{2r}(X_{k_{\mathrm{s}}}, \mathbb{Q}_\ell(r))^{\mathfrak{G}}. \tag{7.6.4}$$

Conjecture 7.6.5 (Tate conjecture)**.** *Let k be a* finitely generated *field (i.e., finitely generated as a field over $\mathbb{F}_p$ or $\mathbb{Q}$). Let X be a nice variety over k. Then the cycle class homomorphism* (7.6.4) *is surjective.*

Conjecture 7.6.5 implies a variant for $X_{k_{\mathrm{s}}}$ instead of X, as we explain in the rest of this section.

Definition 7.6.6. The space of **algebraic classes** is the image of

$$\mathscr{Z}^r(X_{k_{\mathrm{s}}}) \otimes \mathbb{Q}_\ell \xrightarrow{\mathrm{cl}_{\mathrm{et}}} \mathrm{H}^{2r}(X_{k_{\mathrm{s}}}, \mathbb{Q}_\ell(r)).$$

Unofficial version for incidental online use

The space of **Tate classes** is

$$\bigcup_{\text{open } H \leq \mathfrak{G}} \mathrm{H}^{2r}(X_{k_s}, \mathbb{Q}_\ell(r))^H,$$

where the union is over all (finite-index) open subgroups H of the Galois group $\mathfrak{G}$.

Every algebraic class is a Tate class. If Conjecture 7.6.5 holds for X_L for every finite separable extension $L \supseteq k$ contained in k_s, then the converse holds.

Remark 7.6.7. Like the Hodge conjecture, the Tate conjecture is interesting because it predicts the existence of algebraic cycles in situations where there is no known way to construct them.

7.6.6. The Tate conjecture and the Birch and Swinnerton-Dyer conjecture.

(References: [**Tat95a**], [**KT03**])

Theorem 7.6.8. *The following statements are equivalent:*

(i) *The Tate conjecture for divisors* (*the* $r = 1$ *case*) *on nice surfaces over finite fields holds.*

(ii) *For every nice surface* X *over a finite field,* $\operatorname{Br} X$ *is finite.*

(iii) *For every abelian variety* A *over a global function field,* $Ш(A)$ *is finite.*

(iv) *The rank part of the Birch and Swinnerton-Dyer conjecture* (*the formula* $\operatorname{ord}_{s=1} L(A, s) = \operatorname{rk} A(K)$) *holds for abelian varieties over global function fields.*

(v) *The full Birch and Swinnerton-Dyer conjecture (Remark 5.7.34) holds for abelian varieties over global function fields.*

Sketch of proof. Artin and Tate proved the equivalence of these statements in the 1960s, except that they required additional assumptions and needed to exclude the p-parts of some groups, where p is the characteristic [**Tat95a**]. Since then the work of many people [**Gro68d**, **Mil75**, **Mil81**, **Sch82**, **Bau92**, **KT03**] proved the equivalence in full generality, as we now sketch.

(i)⇔(ii): For each nice surface X over a finite field k and for each prime $\ell \neq \operatorname{char} k$, the truth of the Tate conjecture for divisors on X in ℓ-adic cohomology is equivalent to the finiteness of $(\operatorname{Br} X)[\ell^\infty]$ [**Tat95a**, Theorem 5.2(i)⇔(ii)], and the finiteness of $(\operatorname{Br} X)[\ell^\infty]$ implies the finiteness of the whole group $\operatorname{Br} X$ (see [**Mil75**, Theorem 4.1] and [**LLR05**, p. 674, footnote]).

Unofficial version for incidental online use

(iii)⇒(ii): Let X be a nice surface over a finite field k. There exists a nice curve B over k and a rational map $f: X \dashrightarrow B$ whose generic fiber X_η (a variety over the global function field $\mathbf{k}(B)$) is nice. In proving finiteness of $\operatorname{Br} X$, Remark 6.8.8 lets us replace X by a blowup, so we may assume that f is a morphism. Let J be the Jacobian of X_η. In this context, $\operatorname{Br} X$ is finite if and only if $Ш(J)$ is finite [**Gro68d**, §4].

(ii)⇒(iii): Suppose that A is an abelian variety over a global function field K. By [**Gab01**, Proposition 2.4], A is a quotient of the Jacobian J of some nice curve C over K. Spread out C to show that $C = X_\eta$ for some $X \dashrightarrow B$ as in the previous paragraph. Then finiteness of $\operatorname{Br} X$ implies finiteness of $Ш(J)$, which implies finiteness of $Ш(A)$ (because J is isogenous to $A \times A'$ for some A', and finiteness of Ш is invariant under isogeny).

(iii)⇔(iv) and (iv)⇔(v): See [**KT03**, 1.8, Theorem]. □

Unofficial version for incidental online use

7.7. Applications to varieties over global fields

7.7.1. Uniform estimates for the number of points over finite fields. The following application of the Weil conjectures is a variant of [**LW54**, Theorem 1].

Theorem 7.7.1 (Lang–Weil). *Let $\pi: X \to Y$ be a morphism between schemes of finite type over $\mathbb{Z}$. For what follows, let q be a prime power, let $y \in Y(\mathbb{F}_q)$, let X_y be the fiber $\pi^{-1}(y)$ (i.e., the $\mathbb{F}_q$-scheme obtained by pulling back π by* $\operatorname{Spec}\mathbb{F}_q \xrightarrow{y} Y$*), and let $d = \dim X_y$. All implied constants below depend on $\pi: X \to Y$ but not on q, y, or d. Then*

(i) *We have $\#X_y(\mathbb{F}_q) = O(q^d)$.*
(ii) *If the $\mathbb{F}_q$-scheme X_y is geometrically irreducible, then*
$$\#X_y(\mathbb{F}_q) = q^d + O(q^{d-1/2}).$$
(iii) *If q is sufficiently large and X_y is geometrically irreducible, then X_y has an $\mathbb{F}_q$-point.*
(iv) *If q is sufficiently large and X_y is geometrically integral, then X_y has a* smooth *$\mathbb{F}_q$-point.*

Sketch of proof.

(i) We may assume that X and Y are affine; then in particular each X_y is separated. We may also assume that a prime ℓ is invertible on X and Y, because in each, the open subschemes where two different ℓ are invertible cover the whole scheme. The result now follows from
   - the generalized Lefschetz trace formula of Remark 7.5.19,

- a uniform bound on $\dim \mathrm{H}^i_c(\overline{X}_y, \mathbb{Q}_\ell)$ as y varies [**Kat01**, Theorem 1], and
- the bound $q^{i/2}$ on the absolute values of the eigenvalues of the relative q-power Frobenius morphism on the space $\mathrm{H}^i_c(\overline{X}_y, \mathbb{Q}_\ell)$ [**Del80**, Théorème 1].

Alternatively, by fibering a variety into curves and using induction on the dimension, one can reduce to the case in which $X \to Y$ is a family of curves, in which case one does not need the ingredients above, but just the Weil conjectures for curves; this is the original argument of [**LW54**].

(ii) Combine the proof of (i) with the isomorphism $\mathrm{H}^{2d}_c(\overline{V}, \mathbb{Q}_\ell(d)) \simeq \mathbb{Q}_\ell$ of Corollary 7.5.21 for a d-dimensional geometrically irreducible finite-type $\mathbb{F}_q$-scheme V. (Alternatively, one can again follow [**LW54**] and reduce to the case of curves.)

(iii) If q is sufficiently large, then $q^d + O(q^{d-1/2}) > 0$.

(iv) Let U be the smooth locus of $X \to Y$. If X_y is geometrically integral, then so is its smooth locus U_y, by Proposition 3.5.64. So (iv) follows from (iii) for $U \to Y$. $\square$

7.7.2. Existence of local points. Recall the notation for global fields introduced in Section 1.1.3.

Theorem 7.7.2. *Let k be a global field. Let X be a geometrically integral k-variety. Then $X(k_v)$ is nonempty for all but finitely many $v \in \Omega_k$.*

Proof. There exists a finite subset $S \subseteq \Omega_k$ containing all archimedean places such that X spreads out to a separated finite-type $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$ with geometrically integral fibers. By Theorem 7.7.1(iv), for almost all $v \in \operatorname{Spec} \mathcal{O}_{k,S}$, there is a point in $\mathcal{X}(\mathbb{F}_v)$ at which the morphism $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_{k,S}$ is smooth. By Hensel's lemma (Theorem 3.5.63(a)), this point lifts to an element of $\mathcal{X}(\mathcal{O}_v) \subseteq \mathcal{X}(k_v) = X(k_v)$. $\square$

Remark 7.7.3. Given X as in Theorem 7.7.2, one can algorithmically determine a finite subset $S \subseteq \Omega_k$ such that $X(k_v)$ is nonempty for all $v \notin S$ (in practice, it might be easiest to begin by replacing X by a geometrically integral curve in X). If k is a number field, then in principle one can also determine whether $X(k_v)$ is nonempty for each of the finitely many $v \in S$; this was mentioned already in Remark 2.6.4.

7.7.3. Embedding finitely generated algebras into local fields.

(Reference: [**Cas86**, Chapter 5])

Theorem 7.7.4. *Let A be an integral domain of characteristic 0 that is finitely generated as a $\mathbb{Z}$-algebra. Let k be the constant field of* $\operatorname{Frac} A$*, so k*

Unofficial version for incidental online use

is a finite extension of $\mathbb{Q}$ *(see Section 2.2.4). Then for all but finitely many* $v \in \Omega_k$*, there exists an embedding* $A \hookrightarrow \mathcal{O}_v$*.*

Proof. Let $\mathcal{X} = \operatorname{Spec} A$. Let $X = \operatorname{Spec}(\mathbb{Q}A)$, which is a geometrically integral k-variety by Propositions 2.2.19 and 2.2.20. We may replace A by $A[f^{-1}]$ for some nonzero $f \in A$ to assume that $\mathcal{X}$ is as in the proof of Theorem 7.7.2, so $\mathcal{X}^{\text{smooth}}$ has an $\mathcal{O}_v$-point for all but finitely many v. For any such v, Remark 3.5.76 yields a point in the open subset $\mathcal{X}(\mathcal{O}_v)$ of $X(k_v)$ lying outside the countably many subvarieties $g = 0$ defined by nonzero $g \in A$. Any such $\mathcal{O}_v$-point is a homomorphism $A \to \mathcal{O}_v$ killing no nonzero $g \in A$. $\square$

Corollary 7.7.5. *Let* A *be an integral domain of characteristic* 0 *that is finitely generated as a* $\mathbb{Z}$*-algebra. Then there are infinitely many primes* p *such that* A *embeds in* $\mathbb{Z}_p$*.*

Proof. With notation as in Theorem 7.7.4, there are infinitely many places v of k that are unramified of degree 1 over $\mathbb{Q}$; then $\mathcal{O}_v \simeq \mathbb{Z}_p$. There are only finitely many v above each p, so infinitely many primes p occur. $\square$

In the context of Corollary 7.7.5, for some applications one would like to force particular nonzero elements $a_1, \ldots, a_n \in A$ to map to units in $\mathbb{Z}_p$. To arrange this, apply Corollary 7.7.5 to $A[a_1^{-1}, \ldots, a_n^{-1}]$.

Corollary 7.7.6. *Let* B *be an integral domain that is also a finitely generated* $\mathbb{Q}$*-algebra. Then there are infinitely many primes* p *such that* B *embeds in* $\mathbb{Q}_p$*.*

Proof. Choose $\mathbb{Q}$-algebra generators of B, and let A be the $\mathbb{Z}$-subalgebra they generate. Apply Corollary 7.7.5 to A. If A embeds in $\mathbb{Z}_p$, then its localization $B = \mathbb{Q}A$ embeds in $\mathbb{Q}\mathbb{Z}_p = \mathbb{Q}_p$. $\square$

Corollaries 7.7.5 and 7.7.6 make it possible to reduce many questions over characteristic 0 fields to questions over $\mathbb{Z}_p$ or $\mathbb{Q}_p$. See Exercises 7.9 and 7.10 for examples.

Unofficial version for incidental online use

Exercises

7.1. Find the smallest $g \geq 0$ such that there exists a finite field $\mathbb{F}_q$ and a nice curve X of genus g over $\mathbb{F}_q$ such that $X(\mathbb{F}_q)$ is empty.

7.2. (Convergence of zeta functions) Let X be a scheme of finite type over $\mathbb{Z}$.

(a) Prove that there is a polynomial $f(x)$ such that for every $q \geq 1$, the number of closed points $P \in X$ with $\#\mathbf{k}(P) = q$ is less than or equal to $f(q)$.

(b) Deduce that there exists $r \in \mathbb{R}$ such that the product defining $\zeta_X(s)$ converges for all $s \in \mathbb{C}$ with $\operatorname{Re}(s) > r$.

7.3. Use Exercise 2.13 to prove Proposition 7.3.8.

7.4. Let notation be as in Theorem 7.4.1(ii). Let μ be the multiplicity of $-q^{d/2}$ as a zero of $P_d(T)$. Assuming Theorem 7.1.1(ii), prove that

$$Z_X\left(\frac{1}{q^d T}\right) = (-1)^{\chi+\mu} q^{d\chi/2} T^{\chi} Z_X(T).$$

7.5. Let A be an abelian variety over $\mathbb{C}$. Then $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ for some rank $2g$ discrete $\mathbb{Z}$-submodule Λ in $\mathbb{C}^g$, and $\Lambda \simeq \mathrm{H}_1(A(\mathbb{C}), \mathbb{Z})$. Let ℓ be any prime. Prove that there is a natural $\mathbb{Z}_\ell$-module isomorphism $T_\ell A \simeq \Lambda \otimes \mathbb{Z}_\ell$. ("Natural" means that it should be functorial with respect to abelian variety homomorphisms $A \to B$.)

7.6. Let V be a finite-dimensional vector space over a field k of characteristic 0. Let $F\colon V \to V$ be an endomorphism. Then

$$\exp\left(\sum_{n\geq 1} \operatorname{tr}(F^n)\frac{T^n}{n}\right) = \det(1 - TF)^{-1}$$

in $k[[T]]$.

7.7. Prove that given $n \geq 1$, if p is sufficiently large (relative to n), then for any $\epsilon_1, \ldots, \epsilon_n \in \{1, -1\}$, there exists $x \in \mathbb{Z}$ such that for all $i \in \{1, 2, \ldots, n\}$, the Legendre symbol $\left(\frac{x+i}{p}\right)$ equals ϵ_i.

7.8. Generalize Theorem 7.7.1(ii): Show that if the hypothesis that X_y is geometrically irreducible is dropped, then

$$\#X_y(\mathbb{F}_q) = Cq^d + O(q^{d-1/2}),$$

where C is the number of d-dimensional irreducible components of X_y that are geometrically irreducible.

Unofficial version for incidental online use

7.9. (a) Let p be an odd prime, and let $n \geq 1$. Let $N \in \mathrm{M}_n(\mathbb{Z}_p)$. For each $r \geq 1$, prove that $(1+p^r N)^p \equiv 1 + p^{r+1}N \pmod{p^{r+2}}$.

(b) Prove that the group $1+p\,\mathrm{M}_n(\mathbb{Z}_p)$ of $\mathrm{GL}_n(\mathbb{Z}_p)$ is torsion-free; that is, its only element of finite order is the identity.

(c) (Selberg) Let k be a field of characteristic 0. Prove that any finitely generated subgroup G of $\mathrm{GL}_n(k)$ has a torsion-free finite-index subgroup.

(d) Does the previous statement hold for all fields of all characteristics?

7.10. (a) Let p be an odd prime. Let $b \in 1 + p\mathbb{Z}_p$. Prove that there is a p-adic power series $f \in \mathbb{Z}_p[[n]]$ with radius of convergence greater than 1 such that $f(n) = b^n$ for all $n \in \mathbb{Z}$. (*Hint*: Use properties of the p-adic logarithm and exponential maps in [**Kob84**, IV.1].)

(b) Let $b \in \mathbb{Z}_p^\times$. Prove that there are p-adic power series $f_0, \ldots, f_{p-2} \in \mathbb{Z}_p[[n]]$ such that $f_c(n) = b^{(p-1)n+c}$ for all $c \in \{0, \ldots, p-2\}$ and $n \in \mathbb{Z}$.

(c) A sequence $(a_n)_{n\geq 0}$ in a field k is called a **linear recursive sequence** if there exist $r \geq 1$ and $c_{r-1}, \ldots, c_0 \in k$ such that

$$a_{n+r} = c_{r-1}a_{n+r-1} + \cdots + c_0 a_n$$

for all $n \geq 0$. Prove that if $\operatorname{char} k = 0$, then there exist a nonnegative integer s, polynomials $p_1, \ldots, p_s \in \overline{k}[n]$, and elements $b_1, \ldots, b_s \in \overline{k}^\times$ such that

$$a_n = p_1(n)\, b_1^n + \cdots + p_s(n)\, b_s^n$$

for all sufficiently large n.

(d) The **Skolem–Mahler–Lech theorem** states that for any linear recursive sequence (a_n) in a field k of characteristic 0, the set $\{n : a_n = 0\}$ is a finite union of arithmetic progressions and singletons. Prove it. (*Hint*: A p-adic power series with radius of convergence greater than 1 is either identically zero or has only finitely many zeros in $\mathbb{Z}_p$.)

(e) Give an algorithm that takes as input the specification $(r, c_0, \ldots, c_{r-1}, a_0, \ldots, a_{r-1})$ of a linear recursive sequence $(a_n)_{n\geq 0}$ of integers, and outputs YES if there exists n such that $a_n = 0$ and NO otherwise. (*Warning*: This is an unsolved problem! No such algorithm is known, and it may be that no such algorithm exists—that is, it could be undecidable.)

Unofficial version for incidental online use

Chapter 8

Cohomological obstructions to rational points

Unofficial version for incidental online use

In 1970, Manin [**Man71**] explained how, for a variety X over a global field k, elements of $\operatorname{Br} X$ could produce obstructions to the local-global principle. Meanwhile, Fermat's method of infinite descent was generalized to show how a torsor under an algebraic group G over X could give rise to an obstruction, by Chevalley and Weil [**CW30**] for finite G, by Colliot-Thélène and Sansuc [**CTS77**, **CTS80**, **CTS87**] for commutative G, and by Harari and Skorobogatov [**HS02**] for general G. In this chapter, we will explain these and related obstructions.

8.1. Obstructions from functors

8.1.1. The F-obstruction to the local-global principle. Let k be a global field, and let $\mathbf{A}$ be its adèle ring. Let $F\colon \mathbf{Schemes}_k^{\mathrm{opp}} \to \mathbf{Sets}$ be a functor. For a k-algebra L, write $F(L)$ for $F(\operatorname{Spec} L)$. Let X be a k-variety.

Suppose that $A \in F(X)$. For each k-algebra L, define $\mathrm{ev}_A\colon X(L) \to F(L)$ as follows: Given $x \in X(L)$, the corresponding morphism $\operatorname{Spec} L \xrightarrow{x} X$ induces a map $F(X) \to F(L)$, sending A to some element of $F(L)$ called

$\mathrm{ev}_A(x)$ or $A(x)$. Then the diagram

$$\begin{tikzcd} X(k) \arrow[r, hook] \arrow[d, "\mathrm{ev}_A"'] & X(\mathbf{A}) \arrow[d, "\mathrm{ev}_A"'] \\ F(k) \arrow[r] & F(\mathbf{A}) \end{tikzcd} \tag{8.1.1}$$

commutes. Let $X(\mathbf{A})^A$ be the subset of $X(\mathbf{A})$ consisting of elements whose image in $F(\mathbf{A})$ lies in the image of $F(k) \to F(\mathbf{A})$. Then (8.1.1) shows that $X(k) \subseteq X(\mathbf{A})^A$. In other words, A puts constraints on the locus in $X(\mathbf{A})$ where k-points can lie.

Imposing the constraints for all $A \in F(X)$ yields the subset

$$X(\mathbf{A})^F = X(\mathbf{A})^{F(X)} := \bigcap_{A \in F(X)} X(\mathbf{A})^A,$$

again containing $X(k)$.

Definition 8.1.2. If $X(\mathbf{A}) \neq \emptyset$ but $X(\mathbf{A})^F = \emptyset$, then we say that there is an F-**obstruction to the local-global principle**; in this case $X(k) = \emptyset$.

8.1.2. The F-obstruction to weak approximation. We have $X(\mathbf{A}) \subseteq X(\prod k_v) = \prod X(k_v)$; cf. Exercise 3.4. (If X is proper, then all three sets are equal.) There is a variant of Definition 8.1.2 in which $X(\mathbf{A})$ is replaced by $X(\prod k_v) = \prod X(k_v)$ and $F(\mathbf{A})$ is replaced by $\prod F(k_v)$ in (8.1.1); call the resulting set $X(\prod k_v)^F$.

Definition 8.1.3. If $X(\prod k_v)^F \neq X(\prod k_v)$, then we say that there is an F-**obstruction to weak approximation**. Usually this terminology is used in a context where $X(\prod k_v)^F$ is known to be closed in $X(\prod k_v)$, in which case such an F-obstruction would imply that $X(k)$ is not dense in $X(\prod k_v)$.

8.1.3. Examples. In order for the F-obstruction to be nontrivial, F must be such that $F(k) \to F(\mathbf{A})$ is not surjective. In order for the F-obstruction to be useful, the image of $F(k) \to F(\mathbf{A})$ must be describable in some way. This is so in the following two examples, as will be explained in subsequent sections.

Example 8.1.4. Taking $F = \mathrm{Br}$ defines the **Brauer set** $X(\mathbf{A})^{\mathrm{Br}}$.

Example 8.1.5. Taking $F = \mathrm{H}^1(-, G)$ for an affine algebraic group G over k defines a set $X(\mathbf{A})^{\mathrm{H}^1(X,G)}$.

Remark 8.1.6. To avoid having to understand the Brauer group of a non-noetherian ring like $\mathbf{A}$, in Section 8.2 we will replace $\mathrm{Br}\,\mathbf{A}$ in (8.1.1) by $\bigoplus_v \mathrm{Br}\, k_v$ when defining $X(\mathbf{A})^{\mathrm{Br}}$; in fact, the Brauer–Manin obstruction was originally defined using $\bigoplus_v \mathrm{Br}\, k_v$. It turns out that the natural homomorphism $\mathrm{Br}\,\mathbf{A} \to \bigoplus_v \mathrm{Br}\, k_v$ is an isomorphism [**Česk15**, Theorem 2.13],

Unofficial version for incidental online use

so the resulting set $X(\mathbf{A})^{\mathrm{Br}}$ is the same. Similarly, we replace $\mathrm{H}^1(\mathbf{A}, G)$ by $\prod_v \mathrm{H}^1(k_v, G)$ in Section 8.4; the natural map $\mathrm{H}^1(\mathbf{A}, G) \to \prod_v \mathrm{H}^1(k_v, G)$ is an injection (a consequence of [**Čes15**, Theorem 2.18]), so again the resulting set $X(\mathbf{A})^{\mathrm{H}^1(X,G)}$ is the same.

Question 8.1.7. Are there other functors that one could use to obtain obstructions?

8.1.4. Functoriality. The proofs of the following three statements are left to the reader as Exercise 8.1.

Proposition 8.1.8. *Let $\pi \colon X' \to X$ be a morphism of k-varieties. Let $x' \in X'(L)$ for some k-algebra L, and let $A \in F(X)$. Then the two ways of evaluating A on x' yield the same result: If we define $x := \pi(x) \in X(L)$ and $A' := \pi^* A \in F(X')$, then $A'(x') = A(x)$ in $F(L)$.*

Corollary 8.1.9. *The assignment $X \mapsto X(\mathbf{A})^F$ is functorial in X.*

Corollary 8.1.10. *Let $\pi \colon X' \to X$ be a morphism of k-varieties. If the map $F(X) \to F(X')$ is surjective, then $X'(\mathbf{A})^F$ is the inverse image of $X(\mathbf{A})^F$ under $X'(\mathbf{A}) \to X(\mathbf{A})$.*

8.2. The Brauer–Manin obstruction

Throughout this section, k is a field, and X is a k-variety.

8.2.1. Evaluation. Let $A \in \operatorname{Br} X$. If L is a k-algebra and $x \in X(L)$, then $\operatorname{Spec} L \xrightarrow{x} X$ induces a homomorphism $\operatorname{Br} X \to \operatorname{Br} L$, which maps A to an element of $\operatorname{Br} L$ that we call $A(x)$; cf. Section 8.1.1.

8.2.2. The Brauer set.

(Reference: [**Sko01**, §5.2])

Now suppose that k is a global field. Fix $A \in \operatorname{Br} X$.

Proposition 8.2.1. *If $(x_v) \in X(\mathbf{A})$, then $A(x_v) = 0$ for almost all v.*

Proof. By Corollary 6.6.11, for some finite set of places S (containing all the archimedean places), we can spread out X to a finite-type $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$ and spread out A to an element $\mathcal{A} \in \operatorname{Br} \mathcal{X}$. Enlarging S if necessary, we may also assume that $x_v \in \mathcal{X}(\mathcal{O}_v)$ for all $v \notin S$. Then $A(x_v)$ comes from an element $\mathcal{A}(x_v) \in \operatorname{Br} \mathcal{O}_v$. But $\operatorname{Br} \mathcal{O}_v = 0$ by Corollary 6.9.3. □

Thus A determines a map

$$\begin{aligned} X(\mathbf{A}) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ (x_v) &\longmapsto (A, (x_v)) := \sum_v \operatorname{inv}_v(A(x_v)). \end{aligned}$$

Unofficial version for incidental online use

Proposition 8.2.2. *If $x \in X(k) \subseteq X(\mathbf{A})$, then $(A, x) = 0$.*

Proof. Use the commutativity of

$$\begin{tikzcd} & X(k) \arrow[r, hook] \arrow[d] & X(\mathbf{A}) \arrow[d] & & \\ 0 \arrow[r] & \operatorname{Br} k \arrow[r] & \bigoplus_v \operatorname{Br} k_v \arrow[r, "\sum \operatorname{inv}_v"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0. \end{tikzcd} \tag{8.2.3}$$

□

Remark 8.2.4. Compare (8.2.3) with (8.1.1).

Definition 8.2.5. For $A \in \operatorname{Br} X$, define

$$X(\mathbf{A})^A := \{ (x_v) \in X(\mathbf{A}) : (A, (x_v)) = 0 \}.$$

Also define

$$X(\mathbf{A})^{\mathrm{Br}} := \bigcap_{A \in \operatorname{Br} X} X(\mathbf{A})^A.$$

This agrees with the definition in Example 8.1.4, because of Remark 8.1.6.

Corollary 8.2.6. *We have $X(k) \subseteq X(\mathbf{A})^{\mathrm{Br}}$.*

Proof. This is a restatement of Proposition 8.2.2. □

8.2.3. The Brauer–Manin obstruction to the local-global principle.

Definition 8.2.7. One says that there is a **Brauer–Manin obstruction to the local-global principle** for X if $X(\mathbf{A}) \neq \emptyset$, but $X(\mathbf{A})^{\mathrm{Br}} = \emptyset$.

Definition 8.2.8. For a class of nice varieties X over global fields, one says that **the Brauer–Manin obstruction to the local-global principle is the only one** if the implication

$$X(\mathbf{A})^{\mathrm{Br}} \neq \emptyset \quad \Longrightarrow \quad X(k) \neq \emptyset$$

holds.

See Conjecture 9.2.27 for a setting in which it is conjectured that the Brauer–Manin obstruction to the local-global principle is the only one.

8.2.4. Brauer evaluation is locally constant.

Proposition 8.2.9. *Let k be a local field, and let X be a k-variety. Let $A \in \operatorname{Br} X$.*

(a) *The map $X(k) \to \operatorname{Br} k$ sending x to $A(x)$ is locally constant with respect to the analytic topology on $X(k)$.*

(b) *If $k = \mathbb{R}$, the map $X(\mathbb{R}) \to \operatorname{Br} \mathbb{R}$ is constant on each connected component of $X(\mathbb{R})$.*

Unofficial version for incidental online use

Proof.

(a) Given $\alpha \in \operatorname{Br} k$, we need to show that $\{x \in X(k) : A(x) = \alpha\}$ is open in $X(k)$. The structure morphism $X \to \operatorname{Spec} k$ induces a homomorphism $\operatorname{Br} k \to \operatorname{Br} X$, which sends α to a "constant" element $\alpha_X \in \operatorname{Br} X$. Replacing A by $A - \alpha_X$ subtracts α from all the values $A(x)$. Thus we may reduce to showing that $\{x \in X(k) : A(x) = 0\}$ is open in $X(k)$.

Let $x_0 \in X(k)$. Consider pairs (Y, y) where Y is an étale X-scheme, Y is affine, and $y \in Y(k)$ maps to $x_0 \in X(k)$. Let R be the direct limit of $\mathscr{O}(Y)$ over the system of such (Y, y). Then R is the henselization of the local ring $\mathscr{O}_{X,x_0}$, so R is a henselian local ring with residue field k (see Section B.3). For each (Y, y), we have morphisms $\operatorname{Spec} k \to \operatorname{Spec} R \to Y \to X$, inducing homomorphisms $\operatorname{Br} X \to \operatorname{Br} Y \to \operatorname{Br} R \to \operatorname{Br} k$, the composition of which sends A to $A(x_0) = 0$. By Remark 6.9.2, the homomorphism $\operatorname{Br} R \to \operatorname{Br} k$ is an isomorphism, so A maps to 0 already in $\operatorname{Br} R$. By Theorem 6.4.3, A maps to 0 in $\operatorname{Br} Y$ for some (Y, y). Let $\pi \colon Y \to X$ be the structure morphism, which is étale. By functoriality as in Proposition 8.1.8, $A(\pi(y)) = 0$ for every $y \in Y(k)$. Since $\pi \colon Y \to X$ is étale, Proposition 3.5.73 shows that $\pi(Y(k))$ is open in $X(k)$, and it contains x_0.

(b) A locally constant map is constant on connected components. □

Remark 8.2.10. The proof of (b) works for every local field k. But if k is nonarchimedean, then each connected component of $X(k)$ is a point. And if $k = \mathbb{C}$, then $\operatorname{Br} k = 0$. So only the case $k = \mathbb{R}$ is interesting.

Corollary 8.2.11. *Let k be a global field. Let X be a k-variety.*

(a) *For any $A \in \operatorname{Br} X$, the map $X(\mathbf{A}) \to \mathbb{Q}/\mathbb{Z}$ sending (x_v) to $(A, (x_v))$ is locally constant.*

(b) *For any $A \in \operatorname{Br} X$, the set $X(\mathbf{A})^A$ is open and closed in $X(\mathbf{A})$.*

(c) *The set $X(\mathbf{A})^{\mathrm{Br}}$ is closed in $X(\mathbf{A})$.*

(d) *Let $\overline{X(k)}$ be the closure of $X(k)$ in $X(\mathbf{A})$. Then $\overline{X(k)} \subseteq X(\mathbf{A})^{\mathrm{Br}}$.*

(e) *If X is proper and $X(\mathbf{A})^{\mathrm{Br}} \neq X(\mathbf{A})$, then weak approximation for X fails. In this case, one says that there is a* ***Brauer–Manin obstruction to weak approximation for*** *X.*

Proof.

(a) Combine Propositions 8.2.1 and 8.2.9.

(b) A fiber of a locally constant map is open and closed.

(c) The set $X(\mathbf{A})^{\mathrm{Br}}$ is the intersection of the closed sets $X(\mathbf{A})^A$ as A varies.

(d) This follows from (c) and Corollary 8.2.6.

Unofficial version for incidental online use

(e) If $\overline{X(k)} \subseteq X(\mathbf{A})^{\mathrm{Br}} \subsetneq X(\mathbf{A})$, then $\overline{X(k)} \neq X(\mathbf{A})$, while $X(\mathbf{A}) = \prod_v X(k_v)$ if X is proper. Thus weak approximation for X fails. $\square$

Remark 8.2.12. Suppose that X is a *proper* variety over a global field k. For a place v of k, what does a locally constant function f on $X(k_v)$ look like?

- Suppose that v is archimedean. Then f is constant on each connected component of $X(k_v)$.
- Suppose that v is nonarchimedean. Let $\mathcal{O}_v$ be the valuation ring, and let $\pi_v \in \mathcal{O}_v$ be a uniformizer. Then $X(k_v) = X(\mathcal{O}_v) = \varprojlim_n X(\mathcal{O}_v/\pi_v^n)$, which is compact, and f factors through the finite set $X(\mathcal{O}_v/\pi_v^n)$ for some n.

Now suppose that $A \in \operatorname{Br} X$. Then the remarks above apply to the evaluation map $X(k_v) \to \operatorname{Br} k_v$ given by A for each v, and this map is 0 for all but finitely many v, by Proposition 8.2.1. Thus the map $X(\mathbf{A}) \to \mathbb{Q}/\mathbb{Z}$ sending (x_v) to $(A, (x_v))$ admits a finite explicit description, in principle. In Section 8.2.5, we will see an example of this.

8.2.5. Example: Iskovskikh's conic bundle with 4 singular fibers.

(References: [**Isk71**], [**Sko01**, Chapter 7])

Let U be the smooth, affine, geometrically integral surface

$$y^2 + z^2 = (3 - x^2)(x^2 - 2)$$

over $\mathbb{Q}$. We will construct a nice $\mathbb{Q}$-surface X containing U as an open subscheme, and then we will show that there is a Brauer–Manin obstruction to the local-global principle for X.

8.2.5.1. *Conic bundles.* The X above will be a conic bundle. Before constructing it, let us discuss conic bundles more generally.

A (possibly degenerate) **conic** over a field k is the zero locus in $\mathbb{P}^2$ of a nonzero degree 2 homogeneous polynomial s in $k[x_0, x_1, x_2]$. It is a **diagonal conic** if s is $ax_0^2 + bx_1^2 + cx_2^2$ for some $a, b, c \in k$ not all zero.

The generalization to conic bundles will be easier if we first re-express the situation over k in a coordinate-free way. If E is the k-vector space with basis x_0, x_1, x_2, then $\mathbb{P}^2 = \operatorname{Proj} k[x_0, x_1, x_2] = \operatorname{Proj} \operatorname{Sym} E =: \mathbb{P}E$, and a degree 2 homogeneous polynomial s is an element of $\operatorname{Sym}^2 E$. We have $E = L_0 \oplus L_1 \oplus L_2$, where $L_i = kx_i$. To say that $s = 0$ is a diagonal conic is to say that $s = s_0 + s_1 + s_2$ for some $s_i \in kx_i^2 = L_i^{\otimes 2}$ not all zero.

If B is a k-scheme, then a **conic bundle** over B is the zero locus of s in $\mathbb{P}\mathscr{E} := \mathbf{Proj} \operatorname{Sym} \mathscr{E}$, where $\mathscr{E}$ is a rank 3 vector bundle on B, and $s \in \Gamma(B, \operatorname{Sym}^2 \mathscr{E})$ is a section vanishing nowhere on B. In the special case

Unofficial version for incidental online use

where $\mathscr{E} = \mathscr{L}_0 \oplus \mathscr{L}_1 \oplus \mathscr{L}_2$ for some line bundles $\mathscr{L}_i$ on B, and $s = s_0+s_1+s_2$ for some $s_i \in \Gamma(B, \mathscr{L}_i^{\otimes 2})$ such that s_0, s_1, s_2 do not simultaneously vanish anywhere on B, the zero locus of s is called a **diagonal conic bundle**.

8.2.5.2. *Châtelet surfaces.* We now specialize further to the following setting:

$$\begin{aligned} k &: \text{ field of characteristic not 2,} & & \\ B &:= \mathbb{P}^1_k, & & \\ \mathscr{L}_0 &:= \mathscr{O}, & s_0 &:= 1, \\ \mathscr{L}_1 &:= \mathscr{O}, & s_1 &:= -a, \\ \mathscr{L}_2 &:= \mathscr{O}(2), & s_2 &:= -F(w,x), \end{aligned}$$

where $a \in k^\times$, and $F(w,x) \in \Gamma(\mathbb{P}^1_k, \mathscr{O}(4))$ is a separable homogeneous polynomial of degree 4 in the homogeneous coordinates w, x on $B = \mathbb{P}^1$. The result is a nice k-surface X containing the affine surface

$$y^2 - az^2 = f(x)$$

as an open subscheme, where $f(x)$ is the dehomogenization $F(1,x)$. Such a surface X is called a **Châtelet surface**. It has a map to $B = \mathbb{P}^1$, and the fibers of $X \to \mathbb{P}^1$ are conics. In fact, all the fibers of $X \to \mathbb{P}^1$ above points in $\mathbb{P}^1(\overline{k})$ are *nice* conics, except above four points (the zeros of F) where the fiber degenerates to the union of two intersecting lines in $\mathbb{P}^2$.

8.2.5.3. *Iskovskikh's example.* Iskovskikh's surface is the Châtelet surface X over $\mathbb{Q}$ given by the choices $a := -1$ and $f(x) := (3-x^2)(x^2-2) \in \mathbb{Q}[x]$.

Remark 8.2.13. One could choose other nice compactifications X' of the affine surface

$$U\colon y^2 + z^2 = (3-x^2)(x^2-2).$$

For instance, one could let X' be the blowup of X at a closed point of $X - U$. But the question of whether such a compactification has a rational point is independent of the choice, by Corollary 3.6.16.

Let $K = \mathbf{k}(X)$. As explained in Section 1.5.7.4, given two elements $a, b \in K^\times$, one can define a quaternion algebra with class $(a,b) \in (\operatorname{Br} K)[2]$. Let $A = (3-x^2, -1) \in \operatorname{Br} K$. By Proposition 6.6.7(i), we may view $\operatorname{Br} X$ as a subgroup of $\operatorname{Br} K$.

Proposition 8.2.14. *The element $A \in \operatorname{Br} K$ lies in the subgroup $\operatorname{Br} X$.*

Proof. By Theorem 6.8.3, we need only check that A has no residue along any integral divisor on X. Therefore it will suffice to find a Zariski open covering $\{U_i\}$ of X such that A extends to an element of $\operatorname{Br} U_i$ for each i.

To accomplish this, we rewrite A in other ways. Define $B := (x^2-2, -1)$ and $C := (3/x^2 - 1, -1)$ in $\operatorname{Br} K$. Then $A + B = (y^2+z^2, -1) = 0$ by

Unofficial version for incidental online use

Proposition 1.5.23 since $y^2 + z^2 = N_{K(\sqrt{-1})/K}(y + z\sqrt{-1})$. Also, $A - C = (x^2, -1) = 0$ since x^2 is a square in K. But A, B, C are all killed by 2, so $A = B = C$.

Let P_{3-x^2} and P_{x^2-2} be the closed points of $\mathbb{P}^1_{\mathbb{Q}}$ given by $3 - x^2 = 0$ and $x^2 - 2 = 0$, respectively. Now $A = (3 - x^2, -1)$ represents a quaternion Azumaya algebra on all of X except along integral divisors where $3 - x^2$ or -1 has a zero or pole. Thus A comes from $\operatorname{Br} U_A$, where

$$U_A := X - (\text{fiber above } \infty) - (\text{fiber above } P_{3-x^2}).$$

Similarly, $B \in \operatorname{Br} U_B$, where

$$U_B := X - (\text{fiber above } \infty) - (\text{fiber above } P_{x^2-2}),$$

and $C \in \operatorname{Br} U_C$, where

$$U_C := X - (\text{fiber above } 0) - (\text{fiber above } P_{3-x^2}).$$

Since $U_A \cup U_B \cup U_C = X$ (in fact, $U_B \cup U_C = X$), the element $A = B = C \in \operatorname{Br} K$ belongs to $\operatorname{Br} X$. $\square$

From now on, we consider A as an element of $\operatorname{Br} X$. To evaluate A at a point $P \in X(k)$ for any field $k \supset \mathbb{Q}$, choose one of

$$(3 - x^2, -1), \quad (x^2 - 2, -1), \quad (3/x^2 - 1, -1)$$

such that the rational function of x is defined and nonzero at P, so that A extends to an element of the Brauer group of an open subset U_A, U_B, or U_C containing P, and replace the rational function by its value at P. For example, if $P \in U_A(\mathbb{Q}_p)$ for some $p \leq \infty$, then

$$\begin{aligned} \operatorname{inv}_p A(P) &= \operatorname{inv}_p(3 - x(P)^2, -1) \\ &= \begin{cases} 0 & \text{if } 3 - x(P)^2 \in N_{\mathbb{Q}_p(\sqrt{-1})/\mathbb{Q}_p}(\mathbb{Q}_p(\sqrt{-1})^\times), \\ 1/2 & \text{otherwise,} \end{cases} \end{aligned}$$

by Proposition 1.5.23.

Proposition 8.2.15. *We have $X(\mathbf{A}) \neq \emptyset$, but $X(\mathbf{A})^A = \emptyset$. In particular, $X(\mathbb{Q}) = \emptyset$, and there is a Brauer–Manin obstruction to the local-global principle for X.*

Proof. A computation involving Hensel's lemma (Theorem 3.5.63(a)) shows that $X(\mathbf{A}) \neq \emptyset$.

Suppose that $P \in X(\mathbb{Q}_p)$ for some $p \leq \infty$. If $p \neq \infty$, let $v_p \colon \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ denote the p-adic valuation. Let $x = x(P) \in \mathbb{Q}_p \cup \{\infty\}$.

Case I: $p \notin \{2, \infty\}$. If $v_p(x) < 0$ (or $x = \infty$), then $3/x^2 - 1 \in \mathbb{Z}_p^\times$. If $v_p(x) \geq 0$, then either $3 - x^2$ or $x^2 - 2$ is in $\mathbb{Z}_p^\times$ because their sum is 1. In

Unofficial version for incidental online use

either case, $A(P)$ has the form (u_1, u_2) with $u_1, u_2 \in \mathbb{Z}_p^\times$, so $A(P) \in \operatorname{Br} \mathbb{Z}_p$ (this uses $p \neq 2$). But $\operatorname{Br} \mathbb{Z}_p = 0$ by Corollary 6.9.3, so $\operatorname{inv}_p A(P) = 0$.

Case II: $p = \infty$. The leading coefficient of $(3 - x^2)(x^2 - 2)$ is not a sum of squares in $\mathbb{R}$, so any $P \in X(\mathbb{R})$ satisfies $x(P) \neq \infty$. Then $x(P)^2 < 3$ or $x(P)^2 > 2$, so $3 - x(P)^2$ or $x(P)^2 - 2$ is in $\mathbb{R}_{>0} = N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times)$. Thus $\operatorname{inv}_\infty A(P) = 0$.

Case III: $p = 2$. Let $P \in X(\mathbb{Q}_2)$. Let $x = x(P)$. Then

$$\begin{aligned} v_2(x) > 0 &\implies 3 - x^2 \equiv 3 \equiv -1 \pmod 4) \\ v_2(x) = 0 &\implies x^2 - 2 \equiv -1 \pmod 4) \\ v_2(x) < 0 &\implies 3/x^2 - 1 \equiv -1 \pmod 4). \end{aligned}$$

But an element of $\mathbb{Z}_2$ that is $-1 \bmod 4$ is not of the form $a^2 + b^2$ with $a, b \in \mathbb{Q}_2$, so it is not a norm from $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$. Thus $\operatorname{inv}_2 A(P) = 1/2$.

Cases I, II, III imply that if $(P_p) \in X(\mathbf{A})$, then $(A, (P_p)) = 1/2 \neq 0$. Thus $X(\mathbf{A})^A = \emptyset$. □

Remark 8.2.16. Iskovskikh's original proof that $X(\mathbb{Q}) = \emptyset$ used only ad hoc methods based on quadratic reciprocity. Ironically, according to [**CTPS16**, §1], Iskovskikh's intention was to produce an example that the Brauer–Manin obstruction could not explain! It was only a few years later that it was realized that the Brauer–Manin obstruction *could* explain it, as above.

Remark 8.2.17. Theorem B of [**CTSSD87a**, **CTSSD87b**] shows that for *any* Châtelet surface over a number field, the Brauer–Manin obstruction to the local-global principle is the only one, and even better, the Brauer–Manin obstruction to weak approximation is the only one; that is, $X(k)$ is dense in $X(\mathbf{A})^{\mathrm{Br}}$. These results were generalized in [**Sal90**, **CT90**, **SS91**] to conic bundle surfaces over $\mathbb{P}^1$ with at most five degenerate fibers. Moreover, Schinzel's hypothesis on prime values of polynomials would imply the same when the number of degenerate fibers is arbitrary, and more generally for "generalized Severi–Brauer bundles over $\mathbb{P}^1$" [**CTSD94**, Theorem 4.2]. A key ingredient in these works is the *fibration method*; for an introduction, see [**CT92**, §3] and [**CT98**, §2], and for examples of the further development of this method, see [**Har94**, **Har97**, **Lia14**, **HW16**].

Unofficial version for incidental online use

8.2.6. Effectivity. Let X be a nice variety over a global field k. One can imagine the following procedure for attempting to decide whether X has a k-point:

- by day, search for k-points;
- by night, search for a finite set of Azumaya $\mathscr{O}_X$-algebras that obstructs k-points.

If the Brauer–Manin obstruction to the local-global principle is the only one for X, then this procedure terminates successfully. See [**Poo06**, Remark 5.3] for more details.

Under additional assumptions on X, one can give more reasonable algorithms and even compute a kind of finite description of $X(\mathbf{A})^{\mathrm{Br}}$; see [**KT08**, **KT11**].

Unofficial version for incidental online use

8.3. An example of descent

Suppose (as in [**Fly00**, §6]) that we want to find the rational solutions to

$$y^2 = (x^2+1)(x^4+1). \tag{8.3.1}$$

Write $x = X/Z$, where X, Z are integers with gcd 1. Then $y = Y/Z^3$ for some integer Y with $\gcd(Y, Z) = 1$. We get

$$Y^2 = (X^2+Z^2)(X^4+Z^4).$$

If a prime p divides both X^2+Z^2 and X^4+Z^4, then

$$\begin{aligned} Z^2 &\equiv -X^2 \pmod p, \\ Z^4 &\equiv -X^4 \pmod p, \end{aligned}$$

so

$$2Z^4 = (Z^2)^2 + Z^4 \equiv (-X^2)^2 + (-X^4) = 0 \pmod p,$$

and similarly

$$2X^4 = (X^2)^2 + X^4 \equiv (-Z^2)^2 + (-Z^4) = 0 \pmod p.$$

But $\gcd(X, Z) = 1$, so this forces $p = 2$. (Alternatively, the resultant of the homogeneous forms X^2+Z^2 and X^4+Z^4 is 4, so the only prime p modulo which these forms have a common nontrivial zero is $p = 2$.)

Each odd prime p divides at most one of X^2+Z^2 and X^4+Z^4, but the product $(X^2+Z^2)(X^4+Z^4)$ is a square, so the exponent of p in each must be even. In other words,

$$X^4 + Z^4 = cW^2$$

for some $c \in \{\pm 1, \pm 2\}$. Since X, Z are not both zero, the left-hand side is positive, so $c > 0$. Thus $c \in \{1, 2\}$.

Dividing by Z^4 and setting $w = W/Z^2$, we obtain a rational point on one of the following smooth curves:

$$\begin{aligned} Y_1\colon &\quad w^2 = x^4 + 1, \\ Y_2\colon &\quad 2w^2 = x^4 + 1. \end{aligned}$$

Each curve Y_c is of geometric genus g where $2g+2=4$; i.e., $g=1$. The point $(x,w)=(0,1)$ belongs to $Y_1(\mathbb{Q})$, and $(1,1)$ belongs to $Y_2(\mathbb{Q})$, so both Y_1 and Y_2 are open subsets of elliptic curves.

One can show that Y_1 and Y_2 are birational to the curves

$$\begin{aligned} \text{32A2:} \quad & y^2 = x^3 - x, \\ \text{64A1:} \quad & y^2 = x^3 - 4x, \end{aligned}$$

where the labels are as in **[Cre97]**. A "2-descent" (or a glance at **[Cre97**, Table 1]!) shows that both elliptic curves have rank 0. One also can compute that their torsion subgroups are isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus the nice models of Y_1 and Y_2 have four rational points each. It follows that rational points on Y_1 satisfy $x=0$ (there are two more rational points at infinity), and rational points on Y_2 satisfy $x \in \{\pm 1\}$. So (8.3.1) has six solutions, namely,

$$(0,1), (0,-1), (1,2), (1,-2), (-1,2), (-1,-2).$$

8.3.1. Explanation. We are asked to find $U(\mathbb{Q})$, where U is the smooth affine curve

$$y^2 = (x^2+1)(x^4+1)$$

in $\mathbb{A}^2_{\mathbb{Q}}$. Let X be the nice genus 2 curve over $\mathbb{Q}$ containing U as an open subscheme; explicitly, $X = \operatorname{Proj} k[x,y,z]/(y^2 - (x^2+z^2)(x^4+z^4))$, where $\deg x = \deg z = 1$ and $\deg y = 3$. This description shows also that $X - U$ consists of two rational points. In particular, finding $U(\mathbb{Q})$ is equivalent to finding $X(\mathbb{Q})$, and the latter is finite by Faltings's theorem (Theorem 2.6.8).

Let Z be the nice curve over $\mathbb{Q}$ birational to the curve in (x,y,w)-space defined by the system

$$\begin{aligned} y^2 &= (x^2+1)(x^4+1), \\ w^2 &= x^4+1, \end{aligned}$$

so $\mathbf{k}(Z) = \mathbb{Q}(x, \sqrt{x^2+1}, \sqrt{x^4+1})$. For $c \in \mathbb{Q}^\times$, let Z_c be the twist of Z that is birational to the curve

$$\begin{aligned} y^2 &= (x^2+1)(x^4+1), \\ cw^2 &= x^4+1. \end{aligned}$$

For each c, there is a degree 2 morphism

$$\begin{aligned} Z_c &\longrightarrow X \\ (x,y,w) &\longmapsto (x,y). \end{aligned}$$

The argument of the previous section can be reinterpreted as follows:

- Each point in $X(\mathbb{Q})$ is the image of $f_c \colon Z_c(\mathbb{Q}) \to X(\mathbb{Q})$ for some $c \in \mathbb{Q}^\times$.

Unofficial version for incidental online use

- Up to multiplying c by $\mathbb{Q}^{\times 2}$, there are only finitely many $c \in \mathbb{Q}^\times$ for which Z_c has $\mathbb{Q}_p$-points for all $p \leq \infty$. Moreover, such a finite set of c's can be computed effectively.

The finite set of c's turned out to be $\{1, 2\}$. Thus the problem of determining $X(\mathbb{Q})$ was reduced to the problem of determining $Z_c(\mathbb{Q})$ for $c \in \{1, 2\}$.

If Y_c is the nice genus 1 curve birational to

$$cy^2 = x^4 + 1,$$

then we have a morphism

$$\begin{aligned} \pi_c \colon Z_c &\longrightarrow Y_c \\ (x, y, w) &\longmapsto (x, w). \end{aligned}$$

Fortunately, for $c \in \{1, 2\}$, the curve Y_c is an elliptic curve of rank 0, so $Y_c(\mathbb{Q}) = Y_c(\mathbb{Q})_{\text{tors}}$ is a computable finite set. We determine the $\mathbb{Q}$-points in the 0-dimensional preimage $\pi_c^{-1}(Y_c(\mathbb{Q})) \subset Z_c$; this gives $Z_c(\mathbb{Q})$. Finally we compute $X(\mathbb{Q}) = \bigcup_{c \in \{1,2\}} f_c(Z_c(\mathbb{Q}))$.

Remark 8.3.2. The elliptic curve

$$E\colon \quad y^2 = (t + 1)(t^2 + 1)$$

is dominated by X, by the morphism

$$\begin{aligned} \phi \colon X &\longrightarrow E \\ (x, y) &\longmapsto (x^2, y). \end{aligned}$$

Unfortunately, the approach of computing $E(\mathbb{Q})$ and then computing $\phi^{-1}(P)$ for each $P \in E(\mathbb{Q})$ cannot be carried out directly, since $E(\mathbb{Q})$ is infinite, of rank 1. Moreover, one can show that the Jacobian J of X is isogenous to $E \times E$, so $\operatorname{rk} J(\mathbb{Q}) = 2$ is not less than $g(X) = 2$, so Chabauty's method (see [**Ser97**, §5.1] or [**MP12**]) cannot be applied directly to X. On the other hand, X has two independent maps to E, so the Demyanenko–Manin method [**Ser97**, §5.2] could be applied to determine $X(\mathbb{Q})$.

8.3.2. Galois covering. One of the key points is the argument was that there are only finitely many c such that Z_c has $\mathbb{Q}_p$-points for all $p \leq \infty$. What makes this work is the fact that $Z \to X$ is a Galois covering.

Let us first explain why $f \colon Z \to X$ is étale. Over the affine open subset V_1 of $U \subseteq X$ where $x^4 + 1$ is nonvanishing, the open subset $f^{-1}V_1 \subseteq Z$ is obtained by adjoining $\sqrt{x^4 + 1}$ to the affine coordinate ring; this is an étale extension. Similarly, over the affine open subset V_2 of U where $x^2 + 1$ is nonvanishing, $f^{-1}V_2$ is obtained by adjoining $\sqrt{x^2 + 1}$. Since V_1 and V_2 cover U, it follows that f is étale above U. A similar argument shows that f is étale above the other affine open piece U' of X. Thus $f \colon Z \to X$ is étale.

Unofficial version for incidental online use

Remark 8.3.3. The argument that f is étale is a special case of the proof of Abhyankar's lemma [**SGA 1**, X.3.6]. It is analogous to the proof that the field $\mathbb{Q}(\sqrt{15}, \sqrt{3}) = \mathbb{Q}(\sqrt{15}, \sqrt{5})$ is an everywhere unramified extension of $\mathbb{Q}(\sqrt{15})$.

In fact, the following shows that $Z \to X$ is a Galois covering with Galois group $\mathbb{Z}/2\mathbb{Z}$:

Proposition 8.3.4. *Let $Z \to X$ be an étale morphism between nice k-curves. If $\mathbf{k}(Z)/\mathbf{k}(X)$ is a Galois extension of field with Galois group G, then $Z \to X$ is a Galois covering with Galois group G.*

Proof. By the equivalence of categories between curves and function fields, the left G-action on $\mathbf{k}(Z)$ induces a right G-action on Z considered as an X-scheme. Since $\mathbf{k}(Z)/\mathbf{k}(X)$ is Galois, the X-morphism

$$\psi\colon Z \times G \longrightarrow Z \times_X Z$$

is an isomorphism above the generic point of X. By spreading out (Theorem 3.2.1(iv)), ψ gives an isomorphism from an open dense subscheme of $Z \times G$ to an open dense subscheme of $Z \times_X Z$. Both $Z \times G$ and $Z \times_X Z$ are smooth, proper, and 1-dimensional over k, so any birational maps between their components are isomorphisms. □

8.4. Descent

(Reference: [**Sko01**, §5.3])

In our example, Z was a $\mathbb{Z}/2\mathbb{Z}$-torsor over X. We now generalize by replacing $\mathbb{Z}/2\mathbb{Z}$ by an arbitrary smooth affine algebraic group G over k. When we speak of a G-torsor over X, we mean a right fppf G_X-torsor over X, where G_X is the base extension. Throughout the rest of Chapter 8, all cohomology is fppf cohomology, and we use $\mathrm{H}^1(X, G)$ as an abbreviation for the pointed set $\check{\mathrm{H}}^1_{\mathrm{fppf}}(X, G)$ (which is a group if G is commutative). By Theorem 6.5.10(i), isomorphism classes of G-torsors over X are in bijection with $\mathrm{H}^1(X, G)$.

8.4.1. Evaluation. Let k be a field. Let X be a k-variety. Let G be a smooth algebraic group over k. Let $Z \xrightarrow{f} X$ be an G-torsor over X, and let ζ be its class in $\mathrm{H}^1(X, G)$. If $x \in X(k)$, then the fiber $Z_x \to \{x\}$ is a G-torsor over k, and its class in $\mathrm{H}^1(k, G)$ will be denoted $\zeta(x)$. Equivalently,

Unofficial version for incidental online use

x determines a morphism in cohomology mapping ζ to $\zeta(x)$:

$$\begin{aligned} x\colon \operatorname{Spec} k &\longrightarrow X \\ \mathrm{H}^1(k,G) &\longleftarrow \mathrm{H}^1(X,G) \\ \zeta(x) &\longleftarrow\!\shortmid \zeta. \end{aligned}$$

Thus the torsor $Z \to X$ gives rise to an "evaluation" map

$$\begin{aligned} X(k) &\longrightarrow \mathrm{H}^1(k,G) \\ x &\longmapsto \zeta(x). \end{aligned}$$

In other words, $Z \to X$ can be thought of as a family of torsors parameterized by X, and $\zeta(x)$ gives the class of the fiber above x.

8.4.2. The fibers of the evaluation map. We may partition $X(k)$ according to the class of the fiber above each rational point:

$$X(k) = \coprod_{\tau \in \mathrm{H}^1(k,G)} \{\, x \in X(k) : \zeta(x) = \tau \,\}.$$

The following key theorem reinterprets the right-hand side.

Theorem 8.4.1. *Let k be a field. Let X be a k-variety. Let G be a smooth affine algebraic group. Suppose that $f\colon Z \to X$ is a G-torsor over X, and let $\zeta \in \mathrm{H}^1(X,G)$ be its class. For each $\tau \in \mathrm{H}^1(k,G)$, let $f^\tau : Z^\tau \to X$ be the twisted torsor constructed in Example 6.5.12. Then*

$$\{\, x \in X(k) : \zeta(x) = \tau \,\} \quad = \quad f^\tau(Z^\tau(k)).$$

In particular,

$$X(k) = \coprod_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(k)).$$

Proof. For each $x \in X(k)$, we have the following equivalences:

$$\begin{aligned} & x \in f^\tau(Z^\tau(k)) \\ \iff\ & \text{the fiber } Z^\tau_x \text{ is a trivial } \mathcal{G}^\tau\text{-torsor over } k \quad \text{(Proposition 5.12.14)} \\ \iff\ & Z_x \overset{G}{\times} T^{-1} \text{ is a trivial } \mathcal{G}^\tau\text{-torsor over } k \\ \iff\ & Z_x \simeq T \text{ as } G\text{-torsor} \\ & \qquad \text{(by taking the contracted product with } T \text{ on the right)} \\ \iff\ & \zeta(x) = \tau. \end{aligned}$$

□

8.4.3. The evaluation map over a local field.

Proposition 8.4.2. *Let k be a local field. Let X be a proper k-variety. Let F be a finite étale algebraic group over k. Let $f\colon Z \to X$ be an F-torsor over X. Then the image of $X(k) \to \mathrm{H}^1(k,F)$ is finite.*

Unofficial version for incidental online use

Proof. For each $x \in X(k)$, the fiber $f^{-1}(x)$ is $\operatorname{Spec} L$ for some étale k-algebra L. By Krasner's lemma (Proposition 3.5.74), there exists an open neighborhood U of x in $X(k)$ such that for $u \in U$, the fiber $f^{-1}(u)$ is isomorphic to $f^{-1}(x)$ as a k-scheme. In other words, if $\mathrm{H}^1(k, F)$ is given the discrete topology, then the evaluation map $X(k) \to \mathrm{H}^1(k, F)$ is continuous.

On the other hand, X is proper, so Proposition 2.6.1(i) shows that $X(k)$ is compact. Thus the image of $X(k) \to \mathrm{H}^1(k, F)$ is compact and hence finite. $\square$

Remark 8.4.3. If $\operatorname{char} k = 0$, then the whole set $\mathrm{H}^1(k, F)$ is finite, by Theorem 5.12.24(a).

8.4.4. The Selmer set. Return to the notation of Theorem 8.4.1, but assume moreover that k is a global field. For each place v of k, the inclusion $k \hookrightarrow k_v$ induces a homomorphism of fppf cohomology groups $\mathrm{H}^1(k, G) \to \mathrm{H}^1(k_v, G)$. (Equivalently, it is the restriction homomorphism of Galois cohomology associated with the inclusion of $\operatorname{Gal}(k_v^s/k_v)$ as a decomposition group in $\operatorname{Gal}(k_{\mathrm{s}}/k)$.) If $\tau \in \mathrm{H}^1(k, G)$, let $\tau_v \in \mathrm{H}^1(k_v, G)$ be its image.

Definition 8.4.4. The **Selmer set** is the following subset of $\mathrm{H}^1(k, G)$:

$$\operatorname{Sel}_Z(k, G) := \left\{ \tau \in \mathrm{H}^1(k, G) : \tau_v \in \operatorname{im}\left(X(k_v) \to \mathrm{H}^1(k_v, G)\right) \text{ for all } v \in \Omega_k \right\}.$$

Remark 8.4.5. This terminology and notation is compatible with the notion of the Selmer group, in the case where $f : Z \to X$ is an isogeny between abelian varieties, viewed as a torsor under $G := \ker f$. For instance, if $f : E \to E$ is the multiplication-by-2 map on an elliptic curve over a number field, then $\operatorname{Sel}_E(k, E[2]) \subseteq \mathrm{H}^1(k, E[2])$ is the 2-Selmer group defined in [**Sil92**, X.§4].

By Theorem 8.4.1 applied over each k_v, we have

$$\begin{aligned} \operatorname{Sel}_Z(k, G) &= \{ \tau \in \mathrm{H}^1(k, G) : Z^\tau(k_v) \neq \emptyset \text{ for all } v \in \Omega_k \} \\ &\supseteq \{ \tau \in \mathrm{H}^1(k, G) : Z^\tau(k) \neq \emptyset \}. \end{aligned}$$

In particular,

$$X(k) = \coprod_{\tau \in \operatorname{Sel}_Z(k, G)} f^\tau(Z^\tau(k)).$$

Theorem 8.4.6. *If X is a proper variety over a global field k, then $\operatorname{Sel}_Z(k, G)$ is finite.*

Proof. Let F be the component group of G. For a suitable finite nonempty subset $S \subseteq \Omega_k$ containing the archimedean places, Theorem 3.2.1 lets us spread out G to a smooth finite-type separated group scheme $\mathcal{G}$ over $\mathcal{O}_{k,S}$,

Unofficial version for incidental online use

spread out X to a proper scheme $\mathcal{X}$ over $\mathcal{O}_{k,S}$, and spread out Z to a $\mathcal{G}$-torsor over $\mathcal{X}$. Let $\tau \in \mathrm{H}^1(k,G)$. For $v \notin S$, the commutative diagram

$$\begin{tikzcd}
 & \mathrm{H}^1(k,G) \arrow[d] & \tau \arrow[d, mapsto] \\
X(k_v) \arrow[r] \arrow[d, equal, "\substack{\text{valuative criterion}\\ \text{for properness}}"'] & \mathrm{H}^1(k_v,G) & \tau_v \\
\mathcal{X}(\mathcal{O}_v) \arrow[r] & \mathrm{H}^1(\mathcal{O}_v,\mathcal{G}) \arrow[u] &
\end{tikzcd}$$

shows that if τ_v comes from $X(k_v)$, then τ_v also comes from $\mathrm{H}^1(\mathcal{O}_v,\mathcal{G})$. Thus $\mathrm{Sel}_Z(k,G)$ is contained in $\mathrm{H}^1_S(k,\mathcal{G})$. Moreover, for each $v \in S$, the image of $X(k_v) \to \mathrm{H}^1(k_v,F)$ is finite by Proposition 8.4.2, so the image of $\mathrm{Sel}_Z(k,G)$ in $\prod_{v\in S}\mathrm{H}^1(k_v,F)$ is finite. The preceding two sentences combined with Theorem 6.5.13(a) show that $\mathrm{Sel}_Z(k,G)$ is finite. $\square$

Remark 8.4.7. One can show that $\mathrm{Sel}_Z(k,G)$ is not only finite, but also effectively computable, even if one does not know $X(k)$. This makes it potentially useful for the determination of $X(k)$.

Corollary 8.4.8. *There exists a finite separable extension k' of k such that $X(k) \subseteq f(Z(k'))$.*

Proof. For each $\tau \in \mathrm{H}^1(k,G)$, there exists a finite separable extension k' such that the image of τ in $\mathrm{H}^1(k',G)$ is trivial. By taking a compositum, one can find a k' that works simultaneously for all $\tau \in \mathrm{Sel}_Z(k,G)$. Extending the base from k to k' makes $Z^\tau \xrightarrow{f^\tau} X$ isomorphic to $Z \xrightarrow{f} X$. $\square$

8.4.5. The weak Mordell–Weil theorem.

The Mordell–Weil theorem states that for any abelian variety A over a global field k, the abelian group $A(k)$ is finitely generated. The following weaker statement is proved along the way to proving the Mordell–Weil theorem:

Theorem 8.4.9 (Weak Mordell–Weil theorem)**.** *Let A be an abelian variety over a global field k, and let m be a positive integer not divisible by* $\operatorname{char} k$*. Then $A(k)/mA(k)$ is finite.*

Proof of Theorem 8.4.9. By Proposition 5.7.4, the multiplication-by-m map $A \xrightarrow{m} A$ is étale, so it is locally surjective in the étale topology. Thus we get an exact sequence of sheaves on $(\operatorname{Spec} k)_{\mathrm{et}}$

$$0 \to A[m] \to A \xrightarrow{m} A \to 0$$

Unofficial version for internal online use

(or equivalently of $\mathfrak{G}_k$-modules), where $A[m]$ is the kernel of $A \stackrel{m}{\to} A$. Taking cohomology gives

$$A(k) \xrightarrow{m} A(k) \longrightarrow \mathrm{H}^1(k, A[m]).$$

On the other hand, we may view $[m]\colon A \to A$ as a torsor under the smooth affine algebraic group $A[m]$, and hence we get an evaluation map

$$\begin{aligned} A(k) &\longrightarrow \mathrm{H}^1(k, A[m]) \\ a &\longmapsto \text{class of the torsor } [m]^{-1}(a). \end{aligned}$$

Its image is contained in the Selmer set, which is finite by Theorem 8.4.6.

One checks that the two maps $A(k) \to \mathrm{H}^1(k, A[m])$ coincide. Comparing images shows that $A(k)/mA(k)$ is isomorphic to the image of the evaluation map, and we proved already that the latter image is finite. $\square$

8.4.6. Application of descent to failure of strong approximation. We will use an integral point analogue of descent to prove a theorem of Minchev [**Min89**, Theorem 1] on the failure of strong approximation. Minchev worked over number fields, but with a little more work we can generalize to global fields.

Theorem 8.4.10. *Let k be a global field. Let S be a finite set of places of k. Let $f\colon Y \to X$ be a finite étale morphism of geometrically integral k-varieties. If $X(\mathbf{A}^S) \neq \emptyset$ and f is not an isomorphism, then the image of the inclusion $X(k) \to X(\mathbf{A}^S)$ is not dense; that is, X does not satisfy strong approximation with respect to S.*

Proof. Let $n = \dim X = \dim Y$. Let $d = \deg f > 1$. Use Theorem 3.2.1 to enlarge S so that f spreads out to a finite étale morphism $F\colon \mathcal{Y} \to \mathcal{X}$ of separated $\mathcal{O}_{k,S}$-schemes such that $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_{k,S}$ and $\mathcal{Y} \to \operatorname{Spec} \mathcal{O}_{k,S}$ have geometrically integral fibers and $\mathcal{X}(\mathcal{O}_v) \neq \emptyset$ for $v \notin S$. For any nonarchimedean $v \in S$, as x_v varies over the compact set $\mathcal{X}(\mathcal{O}_v)$, there are only finitely many possibilities for the finite étale $\mathcal{O}_v$-scheme $F^{-1}(x_v)$, by Krasner's lemma (Proposition 3.5.74). Therefore, as x varies over $\mathcal{X}(\mathcal{O}_{k,S})$, the finite étale $\mathcal{O}_{k,S}$-scheme $F^{-1}(x)$ has bounded degree and bounded ramification over S, so there are only finitely many possibilities for $F^{-1}(x)$. In particular, there exists an infinite set T of nonarchimedean $v \notin S$ such that v splits in $F^{-1}(x)$ for every $x \in \mathcal{X}(\mathcal{O}_{k,S})$.

Let $\mathcal{X}'$ be the smooth locus of $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_{k,S}$, and let $\mathcal{Y}' = F^{-1}\mathcal{X}'$. For $v \notin S$, let $\mathbb{F}_v$ be the residue field, and let $q_v = \#\mathbb{F}_v$. By Theorem 7.7.1(ii), $\#\mathcal{X}'(\mathbb{F}_v)$ and $\#\mathcal{Y}'(\mathbb{F}_v)$ are both $q_v^n + O(q_v^{n-1/2})$ as $q_v \to \infty$. In particular, we may choose $w \in T$ such that $\#\mathcal{Y}'(\mathbb{F}_w) < d \cdot \#\mathcal{X}'(\mathbb{F}_w)$. Thus there exists a point $\bar{a}_w \in \mathcal{X}'(\mathbb{F}_w)$ that does not split in $\mathcal{Y}'$. By Hensel's lemma (Theorem 3.5.63(a)), $\bar{a}_w$ lifts to some $a_w \in \mathcal{X}'(\mathcal{O}_w)$. By Krasner's lemma

Unofficial version for incidental online use

(Proposition 3.5.74), the set $U_w := \{u_w \in \mathcal{X}'(\mathcal{O}_w) : F^{-1}(u_w) \simeq F^{-1}(a_w)\}$ is an open neighborhood of a_w in $X(k_w)$. Let U be the nonempty open set $U_w \times \prod_{v \notin S \cup \{w\}} \mathcal{X}(\mathcal{O}_{k,S})$ of $X(\mathbf{A}^S)$. If $x \in X(k) \cap U$, then $x \in \mathcal{X}'(\mathcal{O}_{k,S})$, so the definition of T implies that w splits in $F^{-1}(x)$, but the definition of U_w implies that w does not split in $F^{-1}(x)$. Thus $X(k) \cap U = \emptyset$, so $X(k)$ is not dense in $X(\mathbf{A}^S)$. □

Corollary 8.4.11 (cf. [**Min89**, Theorem 1])**.** *Let k be a global field. Let S be a finite set of places of k. Let X be a normal geometrically integral k-variety. If $X(\mathbf{A}^S) \neq \emptyset$ and X_{k_s} is not algebraically simply connected, then X does not satisfy strong approximation with respect to S.*

Proof. If $X(k)$ is empty, strong approximation fails by definition. If $X(k)$ is nonempty, apply Lemma 3.5.57 to obtain a nontrivial geometrically integral finite étale cover $Y \to X$, and apply Theorem 8.4.10. □

Remark 8.4.12. Corollary 8.4.11 can fail if X is not normal. For example, if X is a nodal cubic curve in $\mathbb{P}^2$ over a global field such that the tangent lines to the branches at the node have irrational slope, then X is not algebraically simply connected, but X satisfies strong approximation with respect to any finite S, because there is a dominant morphism $\mathbb{P}^1 \twoheadrightarrow X$.

8.4.7. The descent obstruction to the local-global principle. Let k be a global field. Let X be a k-variety. One can show that there is an injection $X(\mathbf{A}) \hookrightarrow \prod_v X(k_v)$, so an element of $X(\mathbf{A})$ will be written as a sequence (x_v) indexed by the places v of k. The set $X(k)$ embeds diagonally into $X(\mathbf{A})$.

A torsor $Z \xrightarrow{f} X$ under a smooth affine algebraic group G over k restricts the locations in $X(\mathbf{A})$ where rational points can lie. Namely, the commutativity of

(8.4.13)
$$\begin{tikzcd} X(k) \arrow[r, hook] \arrow[d] & X(\mathbf{A}) \arrow[d] \\ \mathrm{H}^1(k,G) \arrow[r] & \prod_v \mathrm{H}^1(k_v,G) \end{tikzcd}$$

(cf. (8.1.1)) shows that $X(k)$ is contained in the subset $X(\mathbf{A})^f \subseteq X(\mathbf{A})$ consisting of points of $X(\mathbf{A})$ whose image in $\prod_v \mathrm{H}^1(k_v, G)$ comes from $\mathrm{H}^1(k,G)$. One can show also that

$$X(\mathbf{A})^f = \bigcup_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(\mathbf{A})),$$

and that $X(\mathbf{A})^f$ is closed in $X(\mathbf{A})$ if X is proper; see Exercise 8.7. Moreover, one can replace $\mathrm{H}^1(k,G)$ by its subset $\mathrm{Sel}_Z(k,G)$ in either of the two

Unofficial version for incidental online use

descriptions of $X(\mathbf{A})^f$ above. The condition $X(\mathbf{A})^f = \emptyset$ is equivalent to $\mathrm{Sel}_Z(k, G) = \emptyset$.

One can constrain the possible locations of rational points further by using *many* torsors:

$$X(\mathbf{A})^{\mathrm{H}^1(X,G)} := \bigcap_{\text{all } G\text{-torsors } f\colon Z \to X} X(\mathbf{A})^f,$$
$$X(\mathbf{A})^{\mathrm{descent}} := \bigcap_{\text{all smooth affine } G} X(\mathbf{A})^{\mathrm{H}^1(X,G)}.$$

Then

$$X(k) \subseteq X(\mathbf{A})^{\mathrm{descent}} \subseteq X(\mathbf{A}).$$

Recall that one says that the local-global principle holds for X if and only if the implication

$$X(\mathbf{A}) \neq \emptyset \quad \Longrightarrow \quad X(k) \neq \emptyset$$

holds.

Definition 8.4.14. One says that there is a **descent obstruction to the local-global principle** if $X(\mathbf{A}) \neq \emptyset$ but $X(\mathbf{A})^{\mathrm{descent}} = \emptyset$.

Sometimes we wish to study the adelic subset cut out by torsors under a subset of the possible smooth affine algebraic groups. In particular, we define

$$X(\mathbf{A})^{\mathrm{et}} := \bigcap_{\text{finite étale } G} X(\mathbf{A})^{\mathrm{H}^1(X,G)},$$
$$X(\mathbf{A})^{\mathrm{conn}} := \bigcap_{\text{smooth connected affine } G} X(\mathbf{A})^{\mathrm{H}^1(X,G)},$$
$$X(\mathbf{A})^{\mathrm{PGL}} := \bigcap_{n \geq 1} X(\mathbf{A})^{\mathrm{H}^1(X,\mathrm{PGL}_n)}.$$

8.5. Comparing the descent and Brauer–Manin obstructions

8.5.1. Descent is stronger than Brauer–Manin.

(Reference: [**Sko01**, Proposition 5.3.4])

Proposition 8.5.3 below shows that the Brauer–Manin obstruction is equivalent to the special case of the descent obstruction using only PGL_n-torsors for all n.

Recall from Section 6.6.4 that for any scheme X, we have a map of sets

$$\mathrm{H}^1(X, \mathrm{PGL}_n) \longrightarrow (\mathrm{Br}\, X)[n]. \tag{8.5.1}$$

(We used Theorem 6.6.17(ii) to know that the image is killed by n.)

Unofficial version for incidental online use

Lemma 8.5.2. *Let k be a global field. Let X be a k-variety. Let $Z \xrightarrow{f} X$ be a PGL_n-torsor for some $n \geq 1$. Its class in $\mathrm{H}^1(X, \mathrm{PGL}_n)$ is mapped by (8.5.1) to some $A \in \operatorname{Br} X$. Then $X(\mathbf{A})^f = X(\mathbf{A})^A$.*

Proof. Let $(x_v) \in X(\mathbf{A})$. Then we have a commutative diagram

$$\begin{tikzcd}
\mathrm{H}^1(X, \mathrm{PGL}_n) \arrow[r] \arrow[d, "(x_v)"'] & (\operatorname{Br} X)[n] \arrow[d, "(x_v)"] \\
\prod_v \mathrm{H}^1(k_v, \mathrm{PGL}_n) \arrow[r, "\sim"] & \prod_v (\operatorname{Br} k_v)[n] \\
\mathrm{H}^1(k, \mathrm{PGL}_n) \arrow[r, "\sim"] \arrow[u, "\mathrm{res}_1"] & (\operatorname{Br} k)[n] \arrow[u, "\mathrm{res}_2"']
\end{tikzcd}$$

in which the downward maps are evaluation at (x_v), the upward maps $\mathrm{res}_1, \mathrm{res}_2$ are restriction maps induced by $k \to k_v$, and the horizontal maps are given by (8.5.1). The lower two horizontal maps are bijections by Remark 1.5.18.

The middle horizontal bijection identifies $\operatorname{im}(\mathrm{res}_1)$ with $\operatorname{im}(\mathrm{res}_2)$, so the class of f in $\mathrm{H}^1(X, \mathrm{PGL}_n)$ maps down into $\operatorname{im}(\mathrm{res}_1)$ if and only if the element $A \in (\operatorname{Br} X)[n]$ maps down into $\operatorname{im}(\mathrm{res}_2)$. In other words, $(x_v) \in X(\mathbf{A})^f$ if and only if $(x_v) \in X(\mathbf{A})^A$. $\square$

Proposition 8.5.3. *Let k be a global field. Let X be a regular quasi-projective k-variety. Then*

$$X(\mathbf{A})^{\mathrm{descent}} \subseteq X(\mathbf{A})^{\mathrm{PGL}} = X(\mathbf{A})^{\mathrm{Br}}.$$

Proof. By Corollary 6.6.19, every $A \in \operatorname{Br} X$ is in the image of (8.5.1) for some n. So intersecting the equality of Lemma 8.5.2 over all PGL_n-torsors over X yields $X(\mathbf{A})^{\mathrm{PGL}} = X(\mathbf{A})^{\mathrm{Br}}$. The inclusion $X(\mathbf{A})^{\mathrm{descent}} \subseteq X(\mathbf{A})^{\mathrm{PGL}}$ holds by definition since each PGL_n is a smooth affine algebraic group. $\square$

8.5.2. The étale-Brauer set.

(References: [**Poo10**, **Dem09**, **Sko09**])

Let k be a global field. Let X be a k-variety. Let G be a smooth affine algebraic group. Recall that if $Z \xrightarrow{f} X$ is a G-torsor, the determination of $X(k)$ can be reduced to the determination of $Z^\tau(k)$ for various twists Z^τ of Z:

$$X(k) = \coprod_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(k)) \subseteq \bigcup_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(\mathbf{A})).$$

We can produce a possibly better "upper bound" on $X(k)$ by replacing $Z^\tau(\mathbf{A})$ by $Z^\tau(\mathbf{A})^{\mathrm{Br}}$. If we do so for every G-torsor for every finite étale group scheme

Unofficial version for incidental online use

G, we are led to define the **étale-Brauer set**

$$X(\mathbf{A})^{\mathrm{et,Br}} := \bigcap_{\substack{\text{finite étale } G \\ \text{all } G\text{-torsors } f\colon Z \to X}} \bigcup_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(\mathbf{A})^{\mathrm{Br}}),$$

which is the upper bound on $X(k)$ obtained from applying the Brauer–Manin obstruction to étale covers. A priori, the subset

$$X(\mathbf{A})^{\mathrm{et,descent}} := \bigcap_{\substack{\text{finite étale } G \\ \text{all } G\text{-torsors } f\colon Z \to X}} \bigcup_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(\mathbf{A})^{\mathrm{descent}})$$

could be even smaller.

8.5.3. Étale-Brauer equals descent.

(References: [**Dem09**, **Sko09**])

The proof of the following theorem combines work of Demarche, Harari, Skorobogatov, and Stoll.

Theorem 8.5.4. *Let k be a number field. Let X be a nice k-variety. Then*

$$X(\mathbf{A})^{\mathrm{et,Br}} = X(\mathbf{A})^{\mathrm{et,descent}} = X(\mathbf{A})^{\mathrm{descent}}.$$

Sketch of proof. It suffices to prove

$$X(\mathbf{A})^{\mathrm{descent}} \subseteq X(\mathbf{A})^{\mathrm{et,descent}} \subseteq X(\mathbf{A})^{\mathrm{et,Br}} \subseteq X(\mathbf{A})^{\mathrm{descent}}.$$

The first inclusion is [**Sko09**, Theorem 1.1], which generalizes [**Sto07**, Proposition 5.17] (a statement that we would write as $X(\mathbf{A})^{\mathrm{et}} = X(\mathbf{A})^{\mathrm{et,et}}$). The idea in both results is, roughly speaking, to show that if $Y \to X$ is an torsor under a finite étale group scheme, and $Z \to Y$ is a torsor under a smooth affine algebraic group, then $Z \to X$ is dominated by some torsor under an even larger smooth affine algebraic group over X; this is analogous to the fact that a Galois extension of a Galois extension of a field k is contained in some even larger Galois extension of k.

The second inclusion is deduced by applying Proposition 8.5.3 to the étale covers of X.

The third inclusion is the main result of [**Dem09**], which generalizes the equality $X(\mathbf{A})^{\mathrm{conn}} = X(\mathbf{A})^{\mathrm{Br}}$ of [**Har02**, Théorème 2, 2., and Remarque 4]. (The latter already is striking in that it implies that the torsors under all smooth connected affine algebraic groups give no more information than the torsors under all the groups PGL_n.) □

Unofficial version for incidental online use

8.5.4. Iterated descent obstruction. In the hope of obtaining an obstruction beyond the descent obstruction one might define

$$X(\mathbf{A})^{\text{descent,descent}} := \bigcap_{\substack{\text{all smooth affine } G \\ \text{all } G\text{-torsors } f\colon Z \to X}} \bigcup_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(\mathbf{A})^{\text{descent}})$$

and similarly $X(\mathbf{A})^{\text{descent,descent,descent}}$, and so on. But Cao, answering a question of the author, proved the following:

Theorem 8.5.5 ([**Cao17**, Corollaire 1.2])**.** *For any smooth quasi-projective geometrically integral variety X over a number field,*

$$X(\mathbf{A})^{\text{descent,descent}} = X(\mathbf{A})^{\text{descent}}.$$

Corollary 8.5.6. *For any smooth quasi-projective geometrically integral variety X over a number field,*

$$X(\mathbf{A})^{\text{descent}} = X(\mathbf{A})^{\text{descent,descent}} = X(\mathbf{A})^{\text{descent,descent,descent}} = \cdots .$$

Proof. Use induction on the number of descents! Apply the inductive hypothesis to all the torsors Z^τ over X. $\square$

8.6. Insufficiency of the obstructions

8.6.1. A bielliptic surface.

(Reference: [**Sko99**])

Skorobogatov proved that the Brauer–Manin obstruction is insufficient to explain all counterexamples to the local-global principle:

Theorem 8.6.1 ([**Sko99**])**.** *There exists a nice $\mathbb{Q}$-variety X such that $X(\mathbf{A})^{\mathrm{Br}} \neq \emptyset$ but $X(\mathbb{Q}) = \emptyset$.*

The proof is involved, so we only outline it. First, we describe the kind of variety used.

Definition 8.6.2. A **bielliptic surface** over an algebraically closed field k is a surface isomorphic to $(E_1 \times E_2)/G$ for some elliptic curves E_1 and E_2 and some finite group scheme G such that G is a subgroup scheme of E_1 acting by translations on E_1 and G acts on E_2 so that the quotient E_2/G is isomorphic to $\mathbb{P}^1$. (Since G acts freely on E_1, it acts freely on $E_1 \times E_2$; i.e., $E_1 \times E_2 \to (E_1 \times E_2)/G$ is G-torsor.) A surface over an arbitrary field k is called bielliptic if $X_{\overline{k}}$ is bielliptic.

Warning 8.6.3. Some authors use the term **hyperelliptic surface** to mean bielliptic surface, but these surfaces have nothing to do with hyperelliptic curves.

Unofficial version for incidental online use

Skorobogatov's example was a bielliptic surface $X := Y/G$, where Y was a product of two genus 1 curves over $\mathbb{Q}$, and G was a group generated by a fixed-point free automorphism of order 2 of Y. Explicitly, his X was birational to the affine surface defined by

$$(x^2+1)y^2 = (x^2+2)z^2 = 3(t^4 - 54t^2 - 117t - 243).$$

To show that $X(\mathbb{Q}) = \emptyset$, Skorobogatov proved $X(\mathbf{A})^{\mathrm{et,Br}} = \emptyset$, by applying the Brauer–Manin obstruction to the étale cover $Y \to X$ and its twists.

Remark 8.6.4. Because $X(\mathbf{A})^{\mathrm{et,Br}} = X(\mathbf{A})^{\mathrm{descent}}$, the nonexistence of rational points must also be explained by a descent obstruction. In fact, it can be explained by the obstruction from a single torsor under a noncommutative finite étale group scheme [**HS02**, §5.1].

8.6.2. A quadric bundle over a curve.

(References: [**Poo10**], [**CTPS16**])

We next construct an "even worse" example:

Theorem 8.6.5 ([**Poo10**]). *There exists a nice $\mathbb{Q}$-variety X such that $X(\mathbf{A})^{\mathrm{et,Br}} \neq \emptyset$ but $X(\mathbb{Q}) = \emptyset$.*

Combined with Theorem 8.5.4, this shows that even the descent obstruction is not enough to explain all counterexamples to the local-global principle. In the original proof of Theorem 8.6.5, X was a Châtelet surface bundle over a curve of positive genus. We will present a simpler variant, based on [**CTPS16**, §3.1], using quadrics instead of Châtelet surfaces. In this section, all varieties are over $\mathbb{Q}$.

Start with a nice curve C such that $C(\mathbb{Q})$ consists of a single point c. (For example, C could be the elliptic curve $y^2 = x^3 - 3$, named 972B1 in [**Cre97**].) Let $f\colon C \to \mathbb{P}^1$ be a morphism that is étale at c (for instance, take f corresponding to a uniformizing parameter at c). Compose with an automorphism of $\mathbb{P}^1$ to assume that $f(c) = \infty$. Let U be a connected open neighborhood of c in $C(\mathbb{R})$. By the implicit function theorem, $f(U)$ contains an open neighborhood of ∞ in $\mathbb{P}^1(\mathbb{R})$. Compose f with a translation automorphism of $\mathbb{P}^1$ to assume that $1 \in f(U)$ and that f is étale above $0, 1 \in \mathbb{P}^1$.

Next we construct a quadric bundle $Y \to \mathbb{P}^1$. View $\mathbb{P}^1$ as the result of gluing $\mathbb{A}^1_t := \operatorname{Spec} \mathbb{Q}[t]$ and $\mathbb{A}^1_T := \operatorname{Spec} \mathbb{Q}[T]$ using $t = 1/T$. In $\mathbb{P}^4 \times \mathbb{A}^1_t$, define the closed subscheme

$$Y^{(t)}\colon \quad t(t-1)x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0.$$

Similarly, in $\mathbb{P}^4 \times \mathbb{A}^1_T$, define the closed subscheme

$$Y^{(T)}\colon \quad (1-T)X_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0.$$

Unofficial version for incidental online use

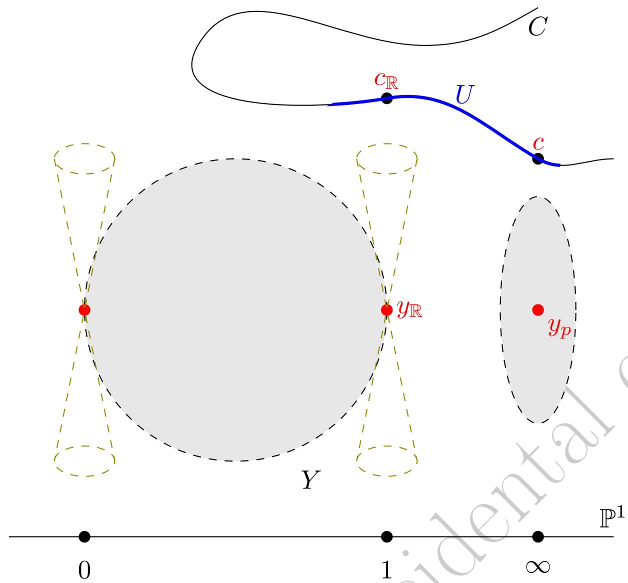

Figure 6. Real points of the varieties C and Y over $\mathbb{P}^1$ are shown in solid black and gray. The open subset U of $C(\mathbb{R})$ is shown as a thicker curve. The dotted lines indicate some fibers of $Y \to \mathbb{P}^1$ with imaginary points.

Glue $Y^{(t)} \to \mathbb{A}^1_t$ and $Y^{(T)} \to \mathbb{A}^1_T$ using $t = 1/T$ and $x_0 = T/X_0$ to obtain $Y \to \mathbb{P}^1$. Alternatively, if $\mathscr{E}$ denotes the rank 5 vector bundle $\mathscr{O}(1) \oplus \mathscr{O}^{\oplus 4}$ on $\mathbb{P}^1$, then Y is the zero locus in $\mathbb{P}\mathscr{E} := \mathbf{Proj}\,\operatorname{Sym}\mathscr{E}$ of a section of $\operatorname{Sym}^2 \mathscr{E}$; in particular, Y is projective over $\mathbb{Q}$. A calculation shows that $Y^{(t)}$ and $Y^{(T)}$ are smooth over $\mathbb{Q}$, so Y is smooth over $\mathbb{Q}$. Thus Y is a family of 3-dimensional quadrics over the base $\mathbb{P}^1$, with two degenerate fibers, above 0 and 1. For each $t \in \mathbb{P}^1$, let Y_t denote the fiber above t. In particular, the locus in $Y^{(T)}$ above $T = 0$ is the fiber

$$Y_\infty\colon \quad X_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0,$$

a smooth quadric in $\mathbb{P}^4$. See Figure 6.

Let $\pi\colon X \to C$ be the base extension of $Y \to \mathbb{P}^1$ by f:

$$\begin{tikzcd} X \arrow[r] \arrow[d, "\pi"'] & Y \arrow[d] \\ C \arrow[r, "f"] & \mathbb{P}^1. \end{tikzcd}$$

Proposition 8.6.6. *The $\mathbb{Q}$-variety X is nice.*

Unofficial version for incidental online use

Proof. Since $Y \to \mathbb{P}^1$ is projective with geometrically integral fibers, the same is true of $X \to C$; in particular, X is a projective and geometrically integral $\mathbb{Q}$-variety. The morphism $Y \to \mathbb{P}^1$ is smooth above all points except $0, 1$, so $X \to C$ is smooth above all points of C outside those above $0, 1 \in \mathbb{P}^1$; since C is smooth over $\mathbb{Q}$, this implies that X is smooth over $\mathbb{Q}$ outside the points above $0, 1 \in \mathbb{P}^1$. Similarly, $C \to \mathbb{P}^1$ is smooth above $0, 1$, so $X \to Y$ is smooth at the points above $0, 1$; since Y is smooth over $\mathbb{Q}$, this implies that X is smooth over $\mathbb{Q}$ also at the points above $0, 1 \in \mathbb{P}^1$. Thus X is nice. $\square$

Proposition 8.6.7. *We have* $X(\mathbb{Q}) = \emptyset$.

Proof. The sole point of $C(\mathbb{Q})$ maps to $\infty \in \mathbb{P}^1$, but Y_∞ has no $\mathbb{Q}$-points. $\square$

As a warm-up to proving that $X(\mathbf{A})^{\text{et,Br}} \neq \emptyset$, we prove that $X(\mathbf{A})^{\text{Br}} \neq \emptyset$.

For each finite prime p, any quadratic form over $\mathbb{Q}_p$ of rank ≥ 5 has a nontrivial zero [**Ser73**, IV.2.2, Theorem 6], so we may choose $y_p \in Y_\infty(\mathbb{Q}_p)$ and let $x_p = (y_p, c) \in X(\mathbb{Q}_p)$. Let $y_\mathbb{R}$ be the unique point in $Y_1(\mathbb{R})$, let $c_\mathbb{R} \in U \subseteq C(\mathbb{R})$ be such that $f(c_\mathbb{R}) = 1 \in \mathbb{P}^1(\mathbb{R})$, and let $x_\mathbb{R} = (y_\mathbb{R}, c_\mathbb{R}) \in X(\mathbb{R})$ (we use the subscript $\mathbb{R}$ for the archimedean place to avoid confusion with the point $\infty \in \mathbb{P}^1$). Together, these define $x = (x_v) \in X(\mathbf{A})$.

Proposition 8.6.8. *We have* $x \in X(\mathbf{A})^{\text{Br}}$.

Proof. The adeles $\pi(x)$ and c agree except for their archimedean parts $c_\mathbb{R}$ and c, which lie in the same connected component of $C(\mathbb{R})$. By this and Proposition 8.2.9, any $A \in \operatorname{Br} C$ takes the same value at $\pi(x)$ as at $c \in C(\mathbb{Q})$; by Proposition 8.2.2, that value is 0. Thus $\pi(x) \in C(\mathbf{A})^{\text{Br}}$. Also, the homomorphism $\operatorname{Br} C \to \operatorname{Br} X$ is surjective by Proposition 6.9.15. Corollary 8.1.10 then implies $x \in X(\mathbf{A})^{\text{Br}}$. $\square$

To generalize Proposition 8.6.8 to prove that $x \in X(\mathbf{A})^{\text{et,Br}}$, we must understand the category $\mathbf{FEt}(X)$ of finite étale covers of X.

Lemma 8.6.9. *The morphism* $X \to C$ *induces an equivalence of categories* $\mathbf{FEt}(C) \to \mathbf{FEt}(X)$.

Proof. This follows (by [**SGA 1**, IX.6.8]) from the fact that each geometric fiber of $X \to C$ (a smooth 3-dimensional quadric or a cone over a smooth 2-dimensional quadric) is algebraically simply connected. $\square$

Proposition 8.6.10. *We have* $x \in X(\mathbf{A})^{\text{et,Br}}$.

Proof. Suppose that G is a finite étale group scheme over $\mathbb{Q}$, and $X' \to X$ is a G-torsor. We must show that one of the twists of $X' \to X$ has an adelic point not obstructed by the Brauer group. By Lemma 8.6.9, $X' \to X$ is the base extension of a G-torsor $C' \to C$. We may replace C' by a twist to

Unofficial version for incremental online use

assume that c lifts to some $c'' \in C'(\mathbb{Q})$. Let C'' be the irreducible component of C' containing c''. The fiber product $X'' := X \times_C C''$ fits in a diagram

$$\begin{tikzcd} X'' \arrow[r, hook] \arrow[d, "\pi''"'] & X' \arrow[r, "G\text{-torsor}"] \arrow[d, "\pi'"'] & X \arrow[r] \arrow[d, "\pi"'] & Y \arrow[d] \\ C'' \arrow[r, hook] & C' \arrow[r, "G\text{-torsor}"] & C \arrow[r, "f"] & \mathbb{P}^1. \end{tikzcd}$$

Since $C'' \to C$ is finite étale, C'' is smooth and projective; moreover, C'' is integral and has a $\mathbb{Q}$-point, so C'' is a nice curve. Similarly, X'' is smooth and projective, and $X'' \to C''$ has geometrically integral fibers (just like $Y \to \mathbb{P}^1$), so X'' is nice too.

We claim that x lifts to a point $x'' \in X''(\mathbf{A})$. For each finite prime p, let $x''_p = (x_p, c'') \in X''(\mathbb{Q}_p)$. Since U is algebraically simply connected, the inverse image of U in $C''(\mathbb{R})$ is a disjoint union of copies of U; let U'' be the copy containing c'', let $c''_{\mathbb{R}} \in U''$ be the point mapping to $c_{\mathbb{R}} \in U$, and let $x''_{\mathbb{R}} = (x_{\mathbb{R}}, c''_{\mathbb{R}}) \in X''(\mathbb{R})$. Thus we have $x'' \in X''(\mathbf{A})$ mapping to $x \in X(\mathbf{A})$.

The same proof as for Proposition 8.6.8 shows that $x'' \in X''(\mathbf{A})^{\mathrm{Br}}$, so $X'(\mathbf{A})^{\mathrm{Br}}$ is nonempty. This argument applies to all finite étale torsors over X, so $X(\mathbf{A})^{\mathrm{et,Br}}$ is nonempty. $\square$

This completes the proof of Theorem 8.6.5.

8.6.3. Hypersurfaces and complete intersections.

(Reference: [**PV04**])

Definition 8.6.11. A scheme-theoretic intersection $X = H_1 \cap \cdots \cap H_r$ of hypersurfaces $H_i \subset \mathbb{P}^n$ is called a **complete intersection** if $\dim X = n - r$.

In particular, any hypersurface in $\mathbb{P}^n$ is a complete intersection.

Theorem 8.6.12. *Let k be a number field. If X is a smooth complete intersection in some $\mathbb{P}^n_k$ and $\dim X \geq 3$, then the descent obstruction and Brauer–Manin obstruction for X are vacuous; that is,*

$$X(\mathbf{A})^{\text{descent}} = X(\mathbf{A})^{\mathrm{Br}} = X(\mathbf{A}).$$

Sketch of proof. By Theorem 8.5.4, it suffices to prove $X(\mathbf{A})^{\mathrm{et,Br}} = X(\mathbf{A})$. This follows immediately from the following two claims:

(i) The variety $X_{\overline{k}}$ is algebraically simply connected (Definition 3.5.45).

(ii) The homomorphism $\operatorname{Br} k \to \operatorname{Br} X$ is an isomorphism.

Part (i) follows from the weak Lefschetz theorem, which says that the homomorphism of fundamental groups $\pi_1(X(\mathbb{C}), x) \to \pi_1(\mathbb{P}^n(\mathbb{C}), x)$ is an isomorphism (here an embedding $\overline{k} \hookrightarrow \mathbb{C}$ is chosen and $x \in X(\mathbb{C})$) [**Mil63**, Theorem 7.4]. For the proof of (ii), see [**PV04**, Proposition A.1]. $\square$

Unofficial version for internal online use

Heuristics suggest that most smooth hypersurfaces $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$ of degree $d > n+1 = \dim X + 2$ have no rational points. On the other hand, a positive fraction of such hypersurfaces have $\mathbb{Q}_p$-points for all $p \leq \infty$ [**PV04**, Theorem 3.6]. Thus one expects many counterexamples to the local-global principle among such hypersurfaces. But there is no smooth hypersurface of dimension ≥ 3 for which the local-global principle has been *proved* to fail! The reason we are unable to prove anything in this setting is that our only available tools, the descent and Brauer–Manin obstructions, give no information.

We need some new obstructions!

Remark 8.6.13. The Brauer–Manin obstruction does yield counterexamples to the local-global principle for some *2-dimensional* hypersurfaces, such as some cubic surfaces; see Section 9.4.9.

Remark 8.6.14. There are some *conditional* counterexamples among hypersurfaces of higher dimension. For instance, Lang's conjecture [**Lan74**, (1.3)] that $V(\mathbb{Q})$ is finite for every nice hyperbolic $\mathbb{Q}$-variety V implies the existence of nice hypersurfaces in $\mathbb{P}^4$ that violate the local-global principle; see [**SW95**, **Poo01**]. (A smooth variety V over a subfield of $\mathbb{C}$ is **(Brody) hyperbolic** if every holomorphic map $\mathbb{C} \to V(\mathbb{C})$ is constant.)

Exercises

8.1. Prove Proposition 8.1.8, Corollary 8.1.9, and Corollary 8.1.10.

8.2. Let k be a global field. Let X be a proper k-variety such that $X(\mathbf{A}) \neq \emptyset$. Let $A \in \operatorname{Br} X$. Suppose that there exists a place w such that the evaluation map $X(k_w) \to \operatorname{Br} k_w$ given by A is not constant. Prove that weak approximation for X fails.

8.3. (Brauer–Manin obstruction for a degree 4 del Pezzo surface) Let X be the smooth surface defined by

$$uv = x^2 - 5y^2,$$
$$(u+v)(u+2v) = x^2 - 5z^2$$

in $\mathbb{P}^4_{\mathbb{Q}}$. (This example is from [**BSD75**, §4].) Let $K = \mathbf{k}(X)$.

(a) Prove that $X(\mathbf{A}) \neq \emptyset$. (*Suggestion*: Let Y be the smooth genus 1 curve obtained by intersecting X with the hyperplane $x = 0$. Spread out Y to a smooth proper scheme over $\mathbb{Z}[S^{-1}]$ for some finite set of places S. For $p \notin S$, use the Hasse–Weil bound or Lang's theorem on H^1 over finite fields to show that Y has an $\mathbb{F}_p$-point, and deduce that Y has a $\mathbb{Q}_p$-point.)

Unofficial version for individual online use

(b) Let A be the class of the quaternion algebra $\left(5, \frac{u+v}{u}\right)$ in $\operatorname{Br} K$. Find other representations of A to show that $A \in \operatorname{Br} X$. (*Hint*: Why does it suffice to find representations on open subsets that cover the codimension 1 points of X?)

(c) Prove that if $P = (u : v : x : y : z) \in X(\mathbb{Q}_p)$ for some $p \leq \infty$, then

$$\operatorname{inv}_p A(P) = \begin{cases} 0 & \text{if } p \neq 5, \\ 1/2 & \text{if } p = 5. \end{cases}$$

(*Hint*: If $5 \in \mathbb{Q}_p^{\times 2}$, what can be said about the image of A in $\operatorname{Br} X_{\mathbb{Q}_p}$?)

(d) Deduce that $X(\mathbf{A})^{\mathrm{Br}} = \emptyset$, so $X(\mathbb{Q}) = \emptyset$.

8.4. Let S be a finite set of places of a number field k, containing all the archimedean places. Let $\mathcal{O}_{k,S}$ be the ring of S-integers. Let $\mathcal{G}$ be a finite étale group scheme over $\mathcal{O}_{k,S}$. Prove that $\mathrm{H}^1(\mathcal{O}_{k,S}, \mathcal{G})$ is finite.

8.5. (Integral descent) Let $\mathcal{O}_{k,S}$ and $\mathcal{G}$ be as above. Let X be a finite-type separated $\mathcal{O}_{k,S}$-scheme, and let $Z \to X$ be a $\mathcal{G}$-torsor. For each $\tau \in \mathrm{H}^1(\mathcal{O}_{k,S}, \mathcal{G})$, define a twisted torsor $f^\tau \colon Z^\tau \to X$ such that

$$X(\mathcal{O}_{k,S}) = \coprod_{\tau \in \mathrm{H}^1(\mathcal{O}_{k,S}, \mathcal{G})} f^\tau(Z^\tau(\mathcal{O}_{k,S})).$$

8.6. Let $\mathcal{O}_{k,S}$ be as above. Let $\mathcal{U}$ be an "affine curve of genus 1 over $\mathcal{O}_{k,S}$", by which we mean a smooth, separated, finite-type $\mathcal{O}_{k,S}$-scheme whose generic fiber is an affine open subset U of a nice k-curve E of genus 1. Show that Faltings's theorem implies that $\mathcal{U}(\mathcal{O}_{k,S})$ is finite. (*Hints*: Show that you may enlarge S and/or extend k as needed. Find a sequence of Galois coverings $U'' \to U' \to U$, where $U' = X' - F'$ with X' a nice genus 1 curve and $F' \subseteq X'$ a closed subscheme with $\#F(\bar{k}) \geq 4$, and U'' is an affine open subset of a ramified covering $X'' \to X'$ branched only over F'.)

8.7. Let k be a number field. Let X be a k-variety. Let G be a smooth affine algebraic group over k. Let $Z \xrightarrow{f} X$ be a G-torsor.

(a) Prove that for each place v, the set $f(Z(k_v))$ is open in $X(k_v)$. (*Hint*: Proposition 3.5.73(ii).)

(b) Prove that for each place v, the evaluation map

$$X(k_v) \to \mathrm{H}^1(k_v, G)$$

associated to f is continuous (for the v-adic topology on $X(k_v)$ and the discrete topology on $\mathrm{H}^1(k_v, G)$).

(c) Prove that for each place v, the set $f(Z(k_v))$ is closed in $X(k_v)$.

Unofficial version for incidental online use

(d) Use results from the proof of Theorem 6.5.13 to prove that

$$f(Z(\mathbf{A})) = X(\mathbf{A}) \cap \prod_v f(Z(k_v))$$

as subsets of $\prod_v X(k_v)$.

(e) Prove that $f(Z(\mathbf{A}))$ is closed in $X(\mathbf{A})$.

(f) Prove that for each $\tau \in \mathrm{H}^1(k, G)$,

$$\left\{ (x_v) \in X(\mathbf{A}) : x_v \text{ maps to } \tau_v \in \mathrm{H}^1(k_v, G) \text{ for all } v \right\} = f^\tau(Z^\tau(\mathbf{A})),$$

where τ_v denotes the image of τ in $\mathrm{H}^1(k_v, G)$.

(g) Prove that $X(\mathbf{A})^f = \bigcup_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(\mathbf{A}))$.

(h) Prove that if X is proper, then $X(\mathbf{A})^f$ is closed in $X(\mathbf{A})$.

Unofficial version for incidental online use

Unofficial version for incidental online use

Chapter 9

Surfaces

Curves can be divided into those of genus 0, those of genus 1, and those of genus > 1. In these three cases, the canonical sheaf ω_X is anti-ample, trivial ($\mathscr{O}_X$), and ample, respectively.

Similarly, one can classify higher-dimensional varieties according to how ample ω_X is. At one extreme lie the Fano varieties, for which $\omega_X^{\otimes(-1)}$ is ample; at the other lie the varieties of general type.

9.1. Kodaira dimension

(Reference: [**Iit82**, §10.5])

Let X be a nice variety over a field k. We will associate to X an element

$$\kappa = \kappa(X) \quad \in \quad \{-\infty, 0, 1, \ldots, \dim X\}$$

called the **Kodaira dimension of** X.

Let ω_X be the canonical sheaf.

Case 1: We have $\mathrm{H}^0(X, \omega_X^{\otimes m}) = 0$ *for all* $m \in \mathbb{Z}_{\geq 1}$. Then define $\kappa := -\infty$.

Case 2: We have $\mathrm{H}^0(X, \omega_X^{\otimes m}) \neq 0$ *for some* $m \in \mathbb{Z}_{\geq 1}$. If m is such that $\mathrm{H}^0(X, \omega_X^{\otimes m}) \neq 0$, then a choice of basis defines a rational map

$$\phi_m \colon X \dashrightarrow \mathbb{P}^{N(m)}$$

(defined on the open subscheme U_m of points at which the global sections generate $\omega_X^{\otimes m}$). In this case, let $\overline{\phi_m(X)}$ denote the Zariski closure of $\phi_m(U_m)$ in $\mathbb{P}^{N(m)}$. Then for $m > 1$ sufficiently large and divisible, $\overline{\phi_m(X)}$ is independent of m up to birational equivalence (cf. [**Iit82**, §10.1]), and we let κ be its dimension. In fact, in Case 2 the following definitions are equivalent:

Unofficial version for incidental online use

(i) $\kappa := \max_m \dim \overline{\phi_m(X)}$.

(ii) κ is the integer such that there exist $c_1, c_2 \in \mathbb{R}_{>0}$ such that

$$c_1 m^\kappa < \dim_k \mathrm{H}^0(X, \omega_X^{\otimes m}) < c_2 m^\kappa$$

for all $m > 0$ such that $\mathrm{H}^0(X, \omega_X^{\otimes m}) \neq 0$.

(iii) $\kappa := (\operatorname{tr\,deg}_k \operatorname{Frac} R) - 1$, where R is the **canonical ring**

$$\bigoplus_{m \geq 0} \mathrm{H}^0(X, \omega_X^{\otimes m}).$$

The equivalence of (i) and (ii) is [**Iit82**, Theorem 10.2]. The equivalence of (i) and (iii) follows since the function field of $\overline{\phi_m(X)}$ for sufficiently large and divisible m is the degree 0 homogeneous part of $\operatorname{Frac} R$ (and for other m it is smaller).

Proposition 9.1.1. *Let X be a nice curve of genus g. Then*

$$\begin{aligned} g = 0 \quad &\Longrightarrow \quad \kappa(X) = -\infty, \\ g = 1 \quad &\Longrightarrow \quad \kappa(X) = 0, \\ g \geq 2 \quad &\Longrightarrow \quad \kappa(X) = 1. \end{aligned}$$

Proof. We leave this as Exercise 9.1. $\square$

Proposition 9.1.2.

(a) *If X and Y are birationally equivalent nice k-varieties, then $\kappa(X) = \kappa(Y)$.*

(b) *If X is a nice k-variety and $L \supseteq k$ is a field extension, then $\kappa(X_L) = \kappa(X)$.*

Proof.

(a) The proof of [**Har77**, Theorem II.8.19] generalizes to prove that the birational map $X \dashrightarrow Y$ induces a natural isomorphism

$$\mathrm{H}^0(Y, \omega_Y^{\otimes m}) \to \mathrm{H}^0(X, \omega_X^{\otimes m})$$

for any $m \geq 0$, so these vector spaces have the same dimension.

(b) The formation of $\mathrm{H}^0(X, \omega_X^{\otimes m})$ commutes with field extension. $\square$

Definition 9.1.3. If X is a geometrically integral k-variety that is birational to a nice k-variety Y, define $\kappa(X) = \kappa(Y)$.

Proposition 9.1.2 shows that the definition is independent of the choice of Y. Resolution of singularities is known if $\operatorname{char} k = 0$, so then a Y exists and $\kappa(X)$ is automatically defined. (The paper [**Luo87**] contains a definition of $\kappa(X)$ that does not rely on resolution of singularities, and hence works in every characteristic.)

Unofficial version for incidental online use

Definition 9.1.4. If $\kappa(X) = \dim X$ (the maximum possible), then X is said to be of **general type**, or **pseudo-canonical**. For a nice variety of general type, one can show that for m sufficiently large, ϕ_m is birational onto its image [**Iit82**, §10.2a, §10.6b]. For instance, if X is a nice curve of general type, then the Riemann–Roch theorem shows that $m \geq 3$ suffices (more specifically, this follows from [**Har77**, Corollary IV.3.2(b)], since for $g \geq 2$, we have $3(2g-2) \geq 2g+1$). If X is a nice surface of general type, then $m \geq 5$ suffices [**Bom73**], [**Eke88**].

Example 9.1.5. Let X be a nice variety. If ω_X is ample, then X is of general type.

Warning 9.1.6. The converse need not hold. Suppose that Y is a nice surface of degree 5 in $\mathbb{P}^3_{\mathbb{C}}$, so $\omega_Y \simeq \mathscr{O}(1)$ by [**Har77**, Example II.8.20.3]. Let $X \to Y$ be the blowup of Y at a point $P \in Y(\mathbb{C})$. By the proof of Proposition 9.1.2, the rational map f_m determined by $\omega_X^{\otimes m}$ equals the composition

$$X \longrightarrow Y \xrightarrow{m\text{-uple}} \mathbb{P}^{N(m)}.$$

Thus X is of general type, but f_m is not a closed immersion for any $m \geq 1$, so ω_X is not ample.

9.2. Varieties that are close to being rational

(Reference: [**Kol96**])

9.2.1. Rational, stably rational, and unirational varieties.

Definition 9.2.1. Let X be an n-dimensional integral variety over an algebraically closed field k. Call X **rational** if it is birational to $\mathbb{P}^n$. Call X **stably rational** if there exists $m \in \mathbb{N}$ such that $X \times \mathbb{P}^m$ is rational. Call X **unirational** if there exists a dominant rational map $\mathbb{P}^N \dashrightarrow X$ for some $N \geq 0$.

Remark 9.2.2. Suppose that X is unirational, so there exists a dominant rational map $\phi\colon \mathbb{P}^N \dashrightarrow X$ for some $N \geq 0$. Then there exists also a dominant rational map $\mathbb{P}^n \dashrightarrow X$ with $n = \dim X$; in fact, one can show that there exists a rational map $\mathbb{P}^n \dashrightarrow \mathbb{P}^N$ such that the composition $\mathbb{P}^n \dashrightarrow \mathbb{P}^N \dashrightarrow X$ is dominant.

Example 9.2.3. Fix integers $0 \leq m \leq n$ and an n-dimensional k-vector space V. The **Grassmannian** $\mathrm{Gr}(m,n) = \mathrm{Gr}(m,V)$ is the moduli space of m-dimensional subspaces of V. It is birational to $\mathbb{P}_k^{m(n-m)}$ (even if k is not algebraically closed), since if we identify V with $k^m \times k^{n-m}$, then $\mathrm{Gr}(m,n)$ has a Zariski open subspace $U \simeq \mathbb{A}^{m(n-m)}$ parameterizing the graphs of linear maps $k^m \to k^{n-m}$.

Unofficial version for incidental online use

Example 9.2.4. Consider $\mathbb{P}\mathscr{E} \to \mathbb{P}^1$, where $\mathscr{E}$ is a rank 2 vector bundle on $\mathbb{P}^1$. By [**Har77**, Corollary V.2.14], $\mathscr{E} \simeq \mathscr{O}(m) \oplus \mathscr{O}(n)$ for some $m, n \in \mathbb{Z}$. Tensoring $\mathscr{E}$ with a line bundle does not change $\mathbb{P}\mathscr{E}$, so we may assume that $\mathscr{E} \simeq \mathscr{O} \oplus \mathscr{O}(n)$ for some $n \geq 0$; the corresponding $\mathbb{P}\mathscr{E}$ is called the **Hirzebruch surface** F_n. Since $\mathscr{E}$ is locally free of rank 2, there exists a dense open subscheme U of $\mathbb{P}^1$ such that the part of $\mathbb{P}\mathscr{E}$ above U is isomorphic to $\mathbb{P}^1 \times U$; thus F_n is a rational surface for each n.

Remark 9.2.5 (Rationality in a family)**.** In a family of varieties $\mathcal{X} \xrightarrow{f} B$, rationality of one fiber $\mathcal{X}_b := f^{-1}(b)$ does not imply rationality of the other fibers. In fact, there exists a smooth projective morphism $\mathcal{X} \to B$ of $\mathbb{C}$-varieties such that $\{b \in B(\mathbb{C}) : \mathcal{X}_b \text{ is rational}\}$ and $\{b \in B(\mathbb{C}) : \mathcal{X}_b \text{ is not rational}\}$ are both dense in $B(\mathbb{C})$ for the analytic topology; see [**HPT16**, Theorem 1.1]. In the example constructed, for $b \in B(\mathbb{C})$ outside a countable union of lower-dimensional closed subvarieties, the fiber $\mathcal{X}_b$ is not even *stably* rational.

Remark 9.2.5 is one of the reasons for introducing rational connectedness, which is weaker than rationality and stable rationality; see Theorem 9.2.18.

Proposition 9.2.6 (Cohomology of a rational surface)**.** *Let X be a nice rational surface over a separably closed field k. Then $\operatorname{Pic} X$ is a free finite-rank abelian group, and for any prime $\ell \neq \operatorname{char} k$,*

$$\begin{aligned}
\mathrm{H}^0_{\mathrm{et}}(X, \mathbb{Q}_\ell) &\simeq \mathbb{Q}_\ell, \\
\mathrm{H}^1_{\mathrm{et}}(X, \mathbb{Q}_\ell) &= 0, \\
\mathrm{H}^2_{\mathrm{et}}(X, \mathbb{Q}_\ell) &\simeq (\operatorname{Pic} X) \otimes \mathbb{Q}_\ell(-1), \\
\mathrm{H}^3_{\mathrm{et}}(X, \mathbb{Q}_\ell) &= 0, \\
\mathrm{H}^4_{\mathrm{et}}(X, \mathbb{Q}_\ell) &\simeq \mathbb{Q}_\ell(-2).
\end{aligned}$$

Sketch of proof. The middle isomorphism is induced by (7.6.2). The statements are true for $\mathbb{P}^2$, and one can show that their truth is unaffected by blowing up a point. $\square$

Remark 9.2.7. Here we explain a variant of unirationality. A dominant rational map $Y \dashrightarrow X$ is called **separably dominant** if $\mathbf{k}(Y)$ is a finite separable extension of $\mathbf{k}(X)$. Call an n-dimensional integral variety X **separably unirational** if there exists a separably dominant rational map $\mathbb{P}^n \dashrightarrow X$. In characteristic 0 there is no difference between unirational and separably unirational. But in characteristic p, the property of being separably unirational is better behaved in many regards.

Unofficial version for incidental online use

9.2.2. Ruled and uniruled varieties.

Definition 9.2.8. Let X be an n-dimensional integral variety over an algebraically closed field k. Call X **ruled** if it is birational to $Y \times \mathbb{P}^1$ for some integral k-variety Y. Call X **uniruled** if there exists a dominant rational map $Y \times \mathbb{P}^1 \dashrightarrow X$ for some integral k-variety Y of dimension $n-1$. (A point is not uniruled.)

Proposition 9.2.9. *If X is uniruled, there is a rational curve through a general point of X, i.e., there is a dense open subset $U \subset X$ such that for every $x \in U(k)$, there is a nonconstant rational map $\mathbb{P}^1 \dashrightarrow X$ whose image contains x. The converse holds if k is uncountable.*

Proof. Suppose that X is uniruled, say via $Y \times \mathbb{P}^1 \dashrightarrow X$. We may replace Y by the dense open set consisting of $y \in Y$ such that $\{y\} \times \mathbb{P}^1 \dashrightarrow X$ is defined and nonconstant. The image of the dominant rational map $Y \times \mathbb{P}^1 \dashrightarrow X$ contains a dense open subset U of X; this proves the first part.

Now let us prove the converse. Let $n = \dim X$. Replace X by a birationally equivalent variety to assume that X is projective. The theory of the Hilbert scheme shows that the nonconstant rational maps $\mathbb{P}^1 \dashrightarrow X$ fall into countably many algebraic families $B \times \mathbb{P}^1 \dashrightarrow X$. If any of these rational maps $B \times \mathbb{P}^1 \dashrightarrow X$ is dominant, then for a general linear $(n-1)$-dimensional section Y of a nonempty affine open subscheme of B, the rational map $Y \times \mathbb{P}^1 \dashrightarrow X$ is dominant, so X is uniruled. Otherwise, each rational map $B \times \mathbb{P}^1 \dashrightarrow X$ has image contained in a positive-codimensional subvariety of X. Since k is uncountable, the union of these images cannot cover the k-points of any dense open subset U of X. □

Remark 9.2.10. As in Remark 9.2.7, one can also define **separably uniruled**.

There is also a criterion for being separably uniruled in terms of the existence of a *single* rational curve satisfying a condition that guarantees that it moves in a family, as we now explain. Let X be a nice variety of dimension d over an algebraically closed field. Let $\mathscr{T}_X$ be the **tangent bundle** of X, defined as the $\mathscr{O}_X$-dual of the sheaf of 1-forms Ω_X; it is a rank d vector bundle. Given a rational curve $f \colon \mathbb{P}^1 \to X$, we obtain a rank d vector bundle $f^*\mathscr{T}_X$ on $\mathbb{P}^1$. Every vector bundle on $\mathbb{P}^1$ is a direct sum of line bundles, so $f^*\mathscr{T}_X \simeq \mathscr{O}(a_1) \oplus \cdots \oplus \mathscr{O}(a_d)$ for some $a_1, \ldots, a_d \in \mathbb{Z}$. Call the rational curve **free** if $a_i \geq 0$ for all i, and **very free** if $a_i \geq 1$ for all i.

Theorem 9.2.11. *Let X be a nice variety over an algebraically closed field. Then X is separably uniruled if and only if X contains a free rational curve.*

Proof. See [**Kol96**, Theorem IV.1.9]. □

Unofficial version for individual online use

9.2.3. Rationally connected varieties. Suppose that X is a nice variety over an algebraically closed field k. Roughly, X is called rationally connected if there is an algebraic family of rational curves such that for almost every pair of points (x, x'), there is a rational curve in the family joining them.

Let us make this precise. In this section, by a **rational curve** in X we mean a (possibly constant) rational map $f\colon \mathbb{P}^1 \dashrightarrow X$; by Proposition 3.6.5(b), it would be equivalent to require f to be a morphism. Say that two points $x, x' \in X(k)$ can be **joined by a rational curve** if there is a rational curve f such that $x, x' \in f(\mathbb{P}^1)$. An **algebraic family of rational curves**, parameterized by a base variety B, is a rational map $F\colon B \times \mathbb{P}^1 \dashrightarrow X$; this is a family in the sense that for (almost every) $b \in B(k)$, the restriction of F to $\{b\} \times \mathbb{P}^1$ defines a rational map $\mathbb{P}^1 \dashrightarrow X$. Given such a family, the pairs of points that it joins are the pairs of the form $(F(b,t), F(b,t'))$ for some $b \in B(k)$ and $t, t' \in \mathbb{P}^1(k)$.

Definition 9.2.12. The variety X is **rationally connected** if there is a variety B and a rational map $F\colon B \times \mathbb{P}^1 \dashrightarrow X$ such that the rational map

$$\begin{aligned} B \times \mathbb{P}^1 \times \mathbb{P}^1 &\dashrightarrow X \times X \\ (b, t, t') &\longmapsto (F(b,t), F(b,t')) \end{aligned}$$

is dominant.

Proposition 9.2.13. *If X is rationally connected, then any general pair of points can be joined by a rational curve; i.e., there is a dense open subset U of $X \times X$ such that any pair $(x, x') \in U(k)$ can be joined by a rational curve. The converse holds if k is uncountable.*

Proof. The proof is the same as that of Proposition 9.2.9. □

We define **separably rationally connected** by replacing "dominant" by "separably dominant" in the definition of rationally connected. Here is the analogue of Theorem 9.2.11.

Theorem 9.2.14. *Let X be a nice variety over an algebraically closed field. Then X is separably rationally connected if and only if X contains a very free rational curve.*

Proof. See [**Kol96**, Theorem IV.3.7]. □

Moreover, it turns out that if X is separably rationally connected, then *any* finite subset of $X(k)$ is contained in a very free rational curve.

Rational connectedness also has a topological implication:

Theorem 9.2.15. *If X is a rationally connected variety over $\mathbb{C}$, then the manifold $X(\mathbb{C})$ is simply connected.*

Unofficial version for incidental online use

Proof. See [**Cam91**, Theorem 3.5] or [**KMM92b**, 2.5.3]. □

9.2.4. Rationally chain connected varieties.

Definition 9.2.16. A variety X over an algebraically closed field k is **rationally chain connected** if there exists a variety B, a proper morphism $\mathcal{C} \to B$ whose fibers are connected unions of rational curves, and a rational map $\mathcal{C} \dashrightarrow X$ such that the induced rational map $\mathcal{C} \times_B \mathcal{C} \dashrightarrow X \times X$ is dominant.

If X is rationally chain connected, then a general pair (x, x') of points on X can be joined by a chain of rational curves, i.e., there exist points $x_0, \ldots, x_n$ with $x_0 = x$ and $x_n = x'$ such that for $i = 0, 1, \ldots, n-1$, the points x_i and x_{i+1} can be joined by a rational curve.

Although rational chain connectedness seems weaker than rational connectedness, the definitions turn out to be equivalent under mild hypotheses:

Theorem 9.2.17 ([**KMM92b**, (2.1)] and [**Kol96**, Theorem IV.3.10.3])**.** *A smooth variety X over a field of characteristic 0 is rationally chain connected if and only if it is rationally connected.*

Theorem 9.2.17 implies that rational connectedness behaves well in families:

Theorem 9.2.18 (Deformation invariance of rational connectedness [**KMM92b**, 2.4])**.** *Let k be an algebraically closed field of characteristic 0. Let S be a connected k-variety. Let $\pi \colon X \to S$ be a smooth proper morphism with geometrically integral fibers. If one fiber is rationally connected, then all fibers are rationally connected.*

Sketch of proof. One shows that

- the set of $s \in S$ such that the fiber $\pi^{-1}(s)$ has a very free rational curve is open; and
- the set of $s \in S$ such that the fiber $\pi^{-1}(s)$ is rationally chain connected is closed.

By Theorems 9.2.14 and 9.2.17, both sets equal the set of $s \in S$ such that $\pi^{-1}(s)$ is rationally connected. A nonempty open and closed subset of a connected space is the whole space. □

9.2.5. Fano varieties.

Definition 9.2.19. Let X be a nice variety over a field k, and let ω_X be its canonical sheaf. Call X **Fano** if $\omega_X^{\otimes(-1)}$ is ample.

Unofficial version for incidental online use

Example 9.2.20. If $X = \mathbb{P}^n$, then $\omega_X^{\otimes(-1)} \simeq \mathscr{O}(n+1)$ [**Har77**, Example II.8.20.1], so X is Fano.

Example 9.2.21. Let X be a nice curve. A line bundle $\mathscr{L}$ on X is ample if and only if $\deg \mathscr{L} > 0$; applying this to $\omega_X^{\otimes(-1)}$ shows that X is Fano if and only if $2 - 2g > 0$, which holds if and only if $g = 0$.

Example 9.2.22. A nice hypersurface of degree d in $\mathbb{P}^n$ is Fano if and only if $d \le n$.

Proposition 9.2.23. *Let $L \supseteq k$ be an extension of fields, and let X be a k-variety. Then X is Fano if and only X_L is Fano.*

Proof. The formation of ω_X commutes with base change, so the same is true of $\omega_X^{\otimes(-1)}$. Also, the property that a line bundle has global sections determining a closed immersion is unaffected by field extension, so ampleness is unaffected by field extension; see [**EGA IV**$_2$, 2.7.2] for a more general statement. $\square$

Let X be a Fano variety. Let $m = \dim X$. Let K be a canonical divisor on X. If $-K$ is very ample, then the complete linear system $|-K|$ embeds X as a subvariety of some $\mathbb{P}^n$, and the degree of this subvariety is the number of points (counted with multiplicity) resulting from cutting it with m general hyperplanes in $\mathbb{P}^n$; equivalently, this degree equals the self-intersection number $(-K)^m$ on X. In general, $-K$ is only ample, but some positive integer multiple of $-K$ is very ample, so again $(-K)^m$ is positive. We define the **degree** of X as $(-K)^m$.

Warning 9.2.24. The property of being Fano is not invariant under birational maps between nice varieties. See Remark 9.4.6.

9.2.6. Implications. Throughout this section, X is a nice variety of dimension $d \ge 1$ over $\mathbb{C}$. The following diagram summarizes the known implications

Unofficial version for incidental online use

between the properties we have been discussing:

$$
\begin{tikzcd}
 & \text{rational} \arrow[d, Rightarrow, "\neq"'] & \\
 & \text{stably rational} \arrow[d, Rightarrow, "\neq"'] & \\
 & \text{unirational} \arrow[d, Rightarrow] & \text{Fano} \arrow[dl, Rightarrow, "\neq"'] \\
\text{rationally chain connected} \arrow[r, Leftrightarrow] & \text{rationally connected} \arrow[r, Rightarrow] \arrow[d, Rightarrow, "\neq"'] & \mathrm{H}^0(X, \Omega_X^{\otimes m}) = 0 \ \forall m \geq 1 \\
 & \text{uniruled} \arrow[d, Rightarrow] & \\
 & \kappa = -\infty. &
\end{tikzcd}
$$

The symbol $\neq$ means that the properties are not equivalent, i.e., that there is a known counterexample to the converse of the implication.

Some remarks:

- Unirational varieties of dimension 1 are rational. Separably unirational varieties of dimension 2 are rational. In higher dimensions, unirational does not imply rational, even over $\mathbb{C}$. In fact, there are several invariants that can be used to prove nonrationality:
  - *Intermediate Jacobian*: Every smooth cubic 3-fold X in $\mathbb{P}^4$ is unirational, but Clemens and Griffiths proved that X is never rational. They proved that the intermediate Jacobian $J^3(Y)$ of a rational 3-fold Y is a product of Jacobians of nice curves, but $J^3(X)$ does not have this form [**CG72**, (0.12)]. Beauville, Colliot-Thélène, Sansuc, and Swinnerton-Dyer constructed a nice 3-fold X that is stably rational but not rational [**BCTSSD85**]; their nonrationality proof again relied on the intermediate Jacobian.
  - *Birational automorphism group*: Some (and maybe all) smooth quartic 3-folds X in $\mathbb{P}^4$ are unirational [**Seg60**, V.19], but Iskovskikh and Manin proved that such X are never rational [**IM71**]. In fact, they showed that $\operatorname{Bir} X$ is isomorphic to $\operatorname{Aut} X$, which is finite [**MM63**, Theorem 2], while $\operatorname{Bir} \mathbb{P}^3$ is enormous.
  - *Torsion in* $\mathrm{H}^3(X, \mathbb{Z})$: Artin and Mumford gave the example of a double cover X of $\mathbb{P}^3$ branched along a quartic surface [**AM72**, §2]. They showed that X is not rational by showing that $\mathrm{H}^3(X, \mathbb{Z})_{\mathrm{tors}}$ is a birational invariant of 3-folds that distinguishes X from $\mathbb{P}^3$ [**AM72**, Proposition 1]. In fact, for the same reason, X is not even

Unofficial version for incidental online use

stably rational. The group $\mathrm{H}^3(X, \mathbb{Z})_{\mathrm{tors}}$ can also be interpreted as the unramified cohomology group $\mathrm{H}^2_{\mathrm{nr}}(X, \mathbb{Q}/\mathbb{Z})$.

- *Higher unramified cohomology*: Colliot-Thélène and Ojanguren constructed a nice 6-fold X such that the unramified cohomology group $\mathrm{H}^3_{\mathrm{nr}}(X, \mathbb{Q}/\mathbb{Z})$ is nonzero even though $\mathrm{H}^2_{\mathrm{nr}}(X, \mathbb{Q}/\mathbb{Z}) = 0$; the former implies that X is not stably rational [**CTO89**]. For rationally connected varieties, the group $\mathrm{H}^3_{\mathrm{nr}}(X, \mathbb{Q}/\mathbb{Z})$ also measures the failure of the integral Hodge conjecture [**CTV12**, Théorème 1.1].

- The theorem that Fano varieties in characteristic 0 are rationally connected was proved independently in [**Cam92**, Corollaire 3.2] and [**KMM92a**, Theorem 0.1].
- It is expected that there exist Fano varieties (and hence rationally connected varieties) that are not unirational. For instance, smooth hypersurfaces of degree n in $\mathbb{P}^n$ are Fano, but maybe for large n they are not unirational.
- It is easy to construct rationally connected varieties that are not Fano, or even rational varieties that are not Fano. See Remark 9.4.6, for example.
- Mumford conjectured that X is rationally connected *if and only if* $\mathrm{H}^0(X, \Omega_X^{\otimes m}) = 0$ for all $m \geq 1$ [**Kol96**, Conjecture IV.3.8.1]. This is known for $d \leq 3$ [**KMM92b**, Theorem 3.2]. (Here Ω_X is the sheaf of 1-forms, not the canonical sheaf, so $\Omega_X^{\otimes m}$ is a vector bundle of rank d^m.)
- If C is a curve of positive genus, then $C \times \mathbb{P}^1$ is uniruled, but not rationally connected, because any rational curve in $C \times \mathbb{P}^1$ maps to a point under the projection to C.
- It is conjectured that uniruled is equivalent to $\kappa = -\infty$.

Remark 9.2.25. It is not known whether there exists a single nice hypersurface of degree at least 4 that is rational.

9.2.7. Non-algebraically closed ground fields.

Definition 9.2.26. Let X be a nice variety over an arbitrary field k. Call X **rational**, **unirational**, **separably unirational**, **ruled**, **uniruled**, **separably uniruled**, **rationally connected**, **separably rationally connected**, or **rationally chain connected**, if $X_{\overline{k}}$ is.

If we want to say that the property truly holds over k, we use the prefix k-. For instance, X is k-**unirational** if there exists a dominant rational map $\mathbb{P}^N_k \dashrightarrow X$ for some $N \geq 0$.

Unofficial version for incidental online use

Conjecture 9.2.27 (Colliot-Thélène)**.** *Let X be a nice variety over a number field k. Suppose that X is rationally connected. Then the Brauer–Manin obstruction to the local-global principle is the only obstruction.*

See [**PV04**, Remark 3.3] for the history of Conjecture 9.2.27.

9.3. Classification of surfaces

9.3.1. Proper birational morphisms.

(References: [**Lic68**], [**Lip69**, §27], [**Mor82**, Chapter 2, Section 3])

9.3.1.1. *Terminology.* Throughout Section 9.3.1, we use the following terminology. A **regular surface** is a regular integral separated noetherian scheme X of dimension 2. A **curve** in X is an integral codimension 1 subscheme $C \subset X$ such that C is proper over some field k (the latter condition is automatic if X itself is proper over k). The properness assumption is there so that for any divisor D on X we may define $C.D := \deg_k \mathscr{O}_X(D)|_C$ (cf. [**Lic68**, I.§1]); since there may be more than one possibility for k given C, we write $(C.D)_k$ when necessary. Curves are called **skew** if they do not intersect. Call a curve C **contractible** if there is a proper birational morphism $f \colon X \to Y$ to another regular surface such that $f(C)$ is a closed point $P \in Y$ and f restricts to an isomorphism from $X - C$ to $Y - \{P\}$. (Some authors relax the regularity requirement on Y and allow Y to be only normal at P; see [**Lip69**, §27].) If C is contractible, then Y, P, and f are uniquely determined up to isomorphism: the key point is that normality forces $\mathscr{O}_{Y,P}$ to equal $\bigcap_{x \in C} \mathscr{O}_{X,x} \subseteq \mathbf{k}(X)$. Call a curve C a (-1)-**curve** if $C \simeq \mathbb{P}^1_L$ and $(C.C)_L = -1$ for some field L; then call $L = \mathrm{H}^0(C, \mathscr{O}_C)$ the **constant field** of C.

9.3.1.2. *Blowing up a regular surface at a closed point.* The blowup of a regular surface Y at a closed point P is another regular surface X with a proper birational morphism $X \to Y$ [**Lic68**, II.A.1.5]. In this case, the fiber above P is a contractible curve $C \subseteq X$ called the **exceptional divisor**. Moreover, C is a (-1)-curve with constant field $\mathbf{k}(P)$ [**Lic68**, Propositions II.A.2.9 and II.A.2.8].

9.3.1.3. *Factorization of birational maps.* Any finite composition of blowups as above is a birational morphism. Part (a) of the following is a converse.

Theorem 9.3.1 (Factorization of birational morphisms)**.** *Let $f \colon X \to Y$ be a proper birational morphism between regular surfaces.*

(a) *The morphism f factors as a sequence of blowups at closed points.*

(b) *If moreover X is smooth over a field k and f is a k-morphism, then*
   (i) *Y is smooth over k, and*
   (ii) *each point P blown up in* (a) *is such that $\mathbf{k}(P)/k$ is separable.*

Unofficial version for incidental online use

Proof.

(a) See [**Lic68**, Theorem 1.15].

(b) (This proof is loosely inspired by [**Coo88**].) By working our way down the sequence of blowups, it suffices to handle the case in which $X = \operatorname{Bl}_P Y$ for some regular surface Y and closed point $P \in Y$.

  (ii) Factor $[\mathbf{k}(P) : k]$ as si, where s is the separable degree and i is the inseparable degree. By Section 9.3.1.2, the exceptional divisor $C \subset X$ is isomorphic to $\mathbb{P}^1_{\mathbf{k}(P)}$ and satisfies

$$C.C = [\mathbf{k}(P) : k]\,(C.C)_{\mathbf{k}(P)} = -[\mathbf{k}(P) : k] = -si.$$

  On the other hand, since $\mathbf{k}(P) \otimes_k \overline{k}$ is a product of s local rings each of length i over itself, the pullback of C to a divisor on $X_{\overline{k}}$ equals $\sum_{j=1}^{s} iD_j$ for some skew integral divisors $D_j \subset X_{\overline{k}}$ conjugate to each other; thus $C.C = \sum_{j=1}^{s}(iD_j).(iD_j) = si^2 D_1.D_1$. So si^2 divides $-si$. Hence $i = 1$; i.e., $\mathbf{k}(P)/k$ is separable.

  (i) By Proposition 3.5.22(iii), Y is smooth at P. On the other hand, $Y - \{P\}$ is isomorphic to an open subscheme of the smooth scheme $\operatorname{Bl}_P Y$, so $Y - \{P\}$ is smooth. Hence Y is smooth. □

Theorem 9.3.2 (Factorization of birational maps)**.** *Let $\phi\colon X \dashrightarrow Y$ be a birational map between regular proper surfaces over a field k.*

(a) *There exists a regular surface Z with proper birational morphisms f and g forming a commutative diagram of rational maps*

$$\begin{tikzcd} & Z \arrow[dl, "f"'] \arrow[dr, "g"] & \\ X \arrow[rr, dashed, "\phi"] & & Y. \end{tikzcd}$$

(b) *The rational map ϕ factors into blowups at closed points and inverses of such blowups.*

Proof.

(a) This is a consequence of [**Lip69**, Theorem 26.1].

(b) Combine (a) with Theorem 9.3.1(a). □

9.3.1.4. *Criteria for contractibility.* One would like an *intrinsic* criterion for contractibility of a curve $C \subset X$, instead of a criterion involving an unspecified proper birational morphism to some unspecified Y. For smooth projective varieties X over an algebraically closed field, Castelnuovo gave the following criterion: C is contractible if and only if $C \simeq \mathbb{P}^1_k$ and $C.C = -1$ [**Har77**, Theorem V.5.7]. Here is the generalization to regular surfaces.

Unofficial version for individual online use

Theorem 9.3.3 (Criteria for contractibility)**.** *Let X be a regular surface that is proper over a noetherian ring A. For a curve $C \subset X$ mapping to a point in* $\operatorname{Spec} A$*, the following are equivalent.*

(i) *C is contractible.*

(ii) *There is a regular surface Y proper over A, a closed point $P \in Y$, and an A-isomorphism $X \simeq \operatorname{Bl}_P Y$ sending C to the exceptional divisor.*

(iii) *C is a (-1)-curve.*

If X is a nice surface over a field $A = k$, then additional equivalent criteria may be given (in these, K denotes a canonical divisor on X):

(iv) *$C.C < 0$ and $C.K < 0$.*

(v) *$C_{k_s} = \bigcup_{i=1}^n E_i$ for some $\mathfrak{G}_k$-orbit $\{E_1, \dots, E_n\}$ of skew (-1)-curves on X_{k_s} with constant field k_s. In this case, $C.C = -n$, $C.K = -n$, and C is geometrically reduced.*

Proof.

(i)⇒(ii): The proper birational morphism contracting C factors into blowup morphisms, by Theorem 9.3.1. Since C is integral, there can be only one blowup.

(ii)⇒(iii): This was mentioned already in Section 9.3.1.2.

(iii)⇒(i): (This is the difficult part.) The morphism $X \to \operatorname{Spec} A$ is projective ([**Lip69**, Corollary 27.2]), so this is a special case of [**Lip69**, Theorem 27.1].

From now on, X is a nice surface over a field k.

(ii)⇒(v): By Theorem 9.3.1, $X \simeq \operatorname{Bl}_P Y$ for some nice Y and closed point $P \in Y$ with $\mathbf{k}(P)/k$ separable. Then X_{k_s} is the blowup of Y_{k_s} along the subscheme P_{k_s}, which consists of a $\mathfrak{G}_k$-orbit in $Y(k_s)$, so C_{k_s} is as described. We can compute $C.C$ and $C.K$ after base extension to k_s: since $E_i.E_j = 0$ for $i \neq j$, all the quantities are the sum of the quantities for the individual E_i. We have $E_i.E_i = -1$ and $E_i.K = -1$ (see Exercise 9.4), so the results follow. Finally, $C_{\overline{k}}$ is a disjoint union of copies of $\mathbb{P}^1_{\overline{k}}$, so C is geometrically reduced.

(v)⇒(iv): We have $-n < 0$.

(iv)⇒(i): See the proof of [**Mor82**, Theorem 2.7]. □

Corollary 9.3.4. *Let X be a nice surface over a field k. Every (-1)-curve on $X_{\overline{k}}$ is definable over k_s, i.e., is the base extension of a (-1)-curve on X_{k_s} with constant field k_s.*

Proof. We may assume that k is separably closed. Let D be a (-1)-curve on $X_{\overline{k}}$. Let C be its image under $X_{\overline{k}} \to X_{k_s}$. As divisors on $X_{\overline{k}}$, we have

Unofficial version for incidental online use

$C_{\overline{k}} = qD$ for some $q \geq 1$. Thus $C.C < 0$ and $C.K < 0$. By (iv)⇒(v) in Theorem 9.3.3, C is a (-1)-curve with constant field k_s and C is geometrically reduced. Thus $C_{\overline{k}} = D$. □

For more general contractibility criteria, including the case of blowing down entire configurations of curves at once, see [**Art62**, Theorems 2.3, 2.7, and 2.9], [**Art66**, Corollary 7], and [**Lip69**, Theorem 27.1].

9.3.1.5. *Minimal surfaces.*

Definition 9.3.5. Let X be a regular surface. Call X **relatively minimal** if every proper birational morphism from X to another regular surface is an isomorphism. If in addition, every birational map from a regular surface Y to X is a morphism, call X **minimal**.

Proposition 9.3.6. *A regular surface X is relatively minimal if and only if it does not contain a curve C satisfying one of the equivalent conditions of Theorem 9.3.3. In particular, a nice surface X over a field k is relatively minimal if and only if X_{k_s} does not contain a $\mathfrak{G}_k$-orbit of skew (-1)-curves with constant field k_s.*

Corollary 9.3.7. *Relative minimality is unchanged by inseparable extension of the base field.*

Warning 9.3.8. Relative minimality can be lost under separable extension of the base field. It can happen that X_{k_s} contains (-1)-curves but that each such curve intersects one of its other Galois conjugates.

Theorem 9.3.9 (Existence of relatively minimal models)**.** *Let X be a nice surface over a field k. Then there exists a proper birational morphism from X to some relatively minimal surface.*

Proof. If not, then one could iteratively blow down orbits of (-1)-curves on X_{k_s} as in Theorem 9.3.3(v) forever. But then one could do the same over $\overline{k}$, which is impossible by the proof of [**Har77**, Theorem V.5.8]. □

Warning 9.3.10. There can exist more than one relatively minimal surface in a birational equivalence class, as the following example shows.

Example 9.3.11. The obvious isomorphism $\mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^2$ defines a birational map $\mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$ indeterminate only at $P := (\infty, \infty)$. The indeterminacy can be resolved by blowing up P on $\mathbb{P}^1 \times \mathbb{P}^1$ to produce a

Unofficial version for incidental online use

surface X fitting in a diagram

$$\begin{tikzcd} & X \arrow[dl] \arrow[ddr] & \\ \mathbb{P}^1 \times \mathbb{P}^1 \arrow[drr, dashed] & & \\ & & \mathbb{P}^2. \end{tikzcd}$$

More explicitly, the strict transforms of $\mathbb{P}^1 \times \{\infty\}$ and $\{\infty\} \times \mathbb{P}^1$ are skew (-1)-curves in X, and blowing them down produces $\mathbb{P}^2$. Both $\mathbb{P}^1 \times \mathbb{P}^1$ and $\mathbb{P}^2$ are relatively minimal, but not minimal.

On the other hand, we have the following.

Proposition 9.3.12 (Uniqueness of minimal models)**.** *If X_1 and X_2 are* minimal *regular surfaces in the same birational equivalence class, then they are isomorphic.*

Proof. The inverse rational maps $X_1 \dashrightarrow X_2$ and $X_2 \dashrightarrow X_1$ extend to morphisms whose composition in either order is the identity. □

9.3.1.6. *Fibered surfaces.* There is a variant of the theory of minimal surfaces in which everything is fibered over a noetherian scheme S. To obtain this variant, change "regular surface" to "regular surface equipped with a proper morphism to S", and change "proper birational morphism" to "proper birational S-morphism" everywhere; this also changes the notions of relatively minimal and minimal. Then in Theorem 9.3.3, consider only curves C that map to a closed point in S.

A key setting is the one in which S is the spectrum of a discrete valuation ring, or more generally an integral separated Dedekind scheme. If Z is a nice curve of genus $g \geq 1$ (or more generally, a regular proper integral curve of positive arithmetic genus) over the function field of such an S, then among regular surfaces proper over S with generic fiber Z, there exists a minimal one: this is a consequence of [**Lic68**, Theorem 4.4]. It is unique by Proposition 9.3.12, and is called the **minimal regular proper model** of Z. See also [**Chi86**].

9.3.2. Surfaces over algebraically closed fields.

(Reference: [**Mor82**, Chapter 2])

Definition 9.3.13. Let X be a nice variety over a field. Let D be a divisor on X. Then

Unofficial version for incidental online use

(i) D is **numerically equivalent to** 0 if $D.C = 0$ for all closed integral curves C on X.

(ii) D is **nef** (numerically effective) if $D.C \geq 0$ for all closed integral curves C on X.

The same terminology applies to the line bundle associated to D.

Theorem 9.3.14 (Minimal models of surfaces)**.** *Let k be an algebraically closed field. Let X be a relatively minimal nice surface over k, with canonical divisor K. Then exactly one of the following holds:*

(i) *X is rational or ruled (in which case $\kappa(X) = -\infty$), or*

(ii) *K is nef (in which case $\kappa(X) \in \{0, 1, 2\}$ and X is minimal).*

Proof. See [**Mor82**, Corollary 2.2 and Lemma 2.4]. □

A more refined classification is possible. For the rest of Section 9.3.2, we assume that k is algebraically closed and X is a relatively minimal nice surface over k. First, one can subdivide according to the Kodaira dimension $\kappa := \kappa(X)$:

9.3.2.1. $\kappa = -\infty$.

Rational surfaces. The only Hirzebruch surface F_n that contains a (-1)-curve is F_1, which is isomorphic to the blowup of $\mathbb{P}^2$ at a point. Therefore the rational surfaces

$$F_0, \mathbb{P}^2, F_2, F_3, \ldots$$

are all relatively minimal. One can show that every rational relatively minimal surface is isomorphic to one of these. We have $F_0 \simeq \mathbb{P}^1 \times \mathbb{P}^1$.

Ruled surfaces. Given a nice curve C and a rank 2 vector bundle $\mathscr{E}$ on C, the ruled surface $\mathbb{P}\mathscr{E} \to C$ is relatively minimal. Every ruled relatively minimal surface is isomorphic to one of these.

9.3.2.2. $\kappa = 0$. In this section, we assume that $\operatorname{char} k \neq 2$; see [**BM76**] for the full details in characteristic 2. The minimal surfaces of Kodaira dimension 0 are the **abelian surfaces** (2-dimensional abelian varieties), **K3 surfaces** (nice surfaces X with $\mathrm{H}^1(X, \mathscr{O}_X) = 0$ and $K = 0$), and quotients of these by a finite group scheme acting freely. A quotient so obtained that is not an abelian surface or a K3 surface is either

- a **bielliptic surface** (see Definition 8.6.2), or
- an **Enriques surface** (a quotient of a K3 surface by an étale group scheme of order 2).

Example 9.3.15. If G is a finite subgroup scheme of an abelian surface A acting by translation on A, then A/G is another abelian surface, with an isogeny $A \to A/G$.

Unofficial version for incidental online use

Example 9.3.16 (Bielliptic surface)**.** Let E_1 and E_2 be elliptic curves. Let $t \in E_1(k)$ be of order exactly 2. Let $G = \mathbb{Z}/2\mathbb{Z}$ act on $E_1 \times E_2$ so that the nontrivial element acts as $(x, y) \mapsto (x + t, -y)$ for some nontrivial $t \in E_2(k)$ of order 2. Let X be the quotient of $E_1 \times E_2$ by the action of G. Then X is a bielliptic surface. If X were an abelian surface, then the morphism $E_1 \times E_2 \to X$ would be a homomorphism up to translation, so its geometric fibers, the G-orbits in $(E_1 \times E_2)(\overline{k})$, would all be cosets of one subgroup, but they are not. If X were a K3 surface, it would be algebraically simply connected, but X has $E_1 \times E_2$ as a nontrivial connected finite étale cover.

9.3.2.3. $\kappa = 1$. All surfaces with $\kappa = 1$ are **elliptic surfaces**, surfaces fibered over a curve C such that all but finitely many fibers are of genus 1, except that if k is of characteristic 2 or 3, there are also **quasi-elliptic surfaces**, which are fibered into singular curves of arithmetic genus 1. But not all elliptic (or quasi-elliptic) surfaces X have $\kappa = 1$; in general all one can say is $\kappa \in \{-\infty, 0, 1\}$. If the base curve C is of genus at least 2, then $\kappa = 1$ is guaranteed, but if C has genus 0 or 1, then one needs to know more about X to determine κ.

9.3.2.4. $\kappa = 2$. These are, by definition, surfaces of general type. As a warmup, recall that *curves* of general type can be classified by their genus $g \in \{2, 3, \ldots\}$, and for each g, there is a quasi-projective variety M_g whose k-points correspond to the isomorphism classes of genus g curves. There is an analogue for surfaces, in which g is replaced by a *pair* of integers (e, K^2). Here e is the **topological Euler characteristic**, defined by

$$e := \sum_{i=0}^{4} (-1)^i \dim \mathrm{H}^i_{\mathrm{Betti}}(X, \mathbb{Q})$$

if $k = \mathbb{C}$, or by

$$e := \sum_{i=0}^{4} (-1)^i \dim \mathrm{H}^i_{\mathrm{et}}(X, \mathbb{Q}_\ell)$$

if k is an arbitrary algebraically closed field, where ℓ is a prime chosen so that $\ell \neq \operatorname{char} k$. And K^2 is the self-intersection of a canonical divisor. It is not known what the range of possibilities for (e, K^2) is, but for fixed (e, K^2), the general type minimal surfaces over $\mathbb{C}$ are parameterized by a coarse moduli space that is a quasi-projective variety **[Gie77]**.

Definition 9.3.17. Let k be an algebraically closed field. A nice k-variety X of arbitrary dimension is called a **minimal model** if K is nef. When X is a surface, this notion coincides with the notion of minimal surface given in Definition 9.3.5, because of Theorem 9.3.14 and the multiple examples of relatively minimal rational and ruled surfaces.

9.3.3. Surfaces over arbitrary fields.

Unofficial version for incidental online use

(Reference: [**Mor82**, Chapter 2, Section 3])

Definition 9.3.18. Let X be a nice surface over a field k. The group $\operatorname{Num} X$ is the quotient of $\operatorname{Pic} X$ by the subgroup of classes of line bundles numerically equivalent to 0. We have $\operatorname{Num} X \simeq \mathbb{Z}^\rho$ for some $\rho \geq 1$ called the **Picard number** of X.

Warning 9.3.19. The Picard number is unchanged by inseparable extension of the base field, but it can grow under separable extension. For example, let $X = \operatorname{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{P}^1$. Then $X_{\mathbb{C}} \simeq \mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}$, so $\operatorname{Pic} X_{\mathbb{C}} \simeq \mathbb{Z}^2$, but complex conjugation interchanges the coordinates, so by Exercise 6.10b, $\operatorname{Pic} X$ is isomorphic to the diagonal copy of $\mathbb{Z}$ in $\mathbb{Z}^2$. Thus $\rho(X) = 1$ and $\rho(X_{\mathbb{C}}) = 2$.

The following builds on the work of many people, including Castelnuovo, Enriques, Manin, Iskovskikh, and Mori.

Theorem 9.3.20. *Let k be a field. Let X be a nice k-surface, and let K be a canonical divisor. Then* at least one *of the following properties holds:*

(i) *X is not relatively minimal (see Proposition 9.3.6).*

(ii) *$\rho = 1$ and $-K$ is ample.*

(iii) *$\rho = 2$ and X is a conic bundle over a nice k-curve Y such that for every $y \in Y$, the fiber X_y is isomorphic to an irreducible and geometrically reduced $\mathbf{k}(y)$-curve of degree 2 in $\mathbb{P}^2_{\mathbf{k}(y)}$ (i.e., each* geometric *fiber is either a smooth conic or a union of two intersecting lines defined over a separable quadratic extension, each a Galois conjugate of the other).*

(iv) *K is nef.*

Moreover, these four classes of varieties are pairwise disjoint, except that some surfaces satisfy both (i) *and* (iii)*.*

Proof. See [**Mor82**, Theorem 2.7]. For the classification of surfaces satisfying both (i) and (iii), see [**Isk79**, Theorem 4]. □

Corollary 9.3.21.

(a) *A rational surface over k is birational (over k) to either a del Pezzo surface (see Section 9.4) or a conic bundle over a conic.*

(b) *A ruled surface over k is birational to a conic bundle over a nice k-curve.*

Remark 9.3.22. The arithmetic of del Pezzo surfaces will be discussed in detail in Section 9.4. For the arithmetic of conic bundles, see [**Sko01**, Chapter 7].

Corollary 9.3.23. *Let k be a separably closed field.*

(a) *The relatively minimal rational surfaces over k are $\mathbb{P}^2$ and the Hirzebruch surfaces F_n for $n \in \{0\} \cup \{2, 3, \ldots\}$.*

Unofficial version for incremental online use

(b) *The relatively minimal ruled surfaces over k with base of positive genus are the surfaces $\mathbb{P}\mathscr{E} \to Y$, where Y is a nice k-curve of positive genus and $\mathscr{E}$ is a rank 2 vector bundle on Y.*

Proof. In Theorem 9.3.20, we are in case (ii) or (iii). If (ii), then $X_{\overline{k}} \simeq \mathbb{P}^2_{\overline{k}}$, so $X \simeq \mathbb{P}^2$ by Remark 4.5.9.

If (iii), then the conic bundle X corresponds to an element of

$$\mathrm{H}^1(Y, \mathrm{PGL}_2) \hookrightarrow \mathrm{H}^2(Y, \mathbb{G}_m) = \operatorname{Br} Y,$$

but the latter is trivial by Theorem 6.9.7. Thus $X \simeq \mathbb{P}\mathscr{E}$ for some rank 2 vector bundle $\mathscr{E}$ on Y. Finally, if Y itself is a conic, then $Y \simeq \mathbb{P}^1$ (Remark 4.5.9 again), and the classification of vector bundles on $\mathbb{P}^1$ shows that $\mathscr{E} \simeq \mathscr{O} \oplus \mathscr{O}(n)$ for some $n \geq 0$. Finally, $\mathbb{P}\mathscr{E}$ is relatively minimal if and only if $(\mathbb{P}\mathscr{E})_{\overline{k}}$ is relatively minimal, which holds if and only $n \neq 1$. $\square$

Proposition 9.3.24 ([**Wei56**]). *Let k be a finite field $\mathbb{F}_q$. Let X be a nice rational surface over k. Then*

$$\#X(k) = q^2 + (\operatorname{tr} \operatorname{Frob}_q \mid \operatorname{Pic} X_{\overline{k}})q + 1,$$

and X has a k-point.

Proof. Apply Proposition 9.2.6 to $X_{\overline{k}}$ and then use the Lefschetz trace formula (7.5.18) to obtain the formula. Since $\operatorname{tr} \operatorname{Frob}_q \mid \operatorname{Pic} X_{\overline{k}} \in \mathbb{Z}$, we obtain $\#X(k) \equiv 1 \pmod{q}$, so $X(k) \neq \emptyset$. $\square$

Remark 9.3.25. As mentioned in (3) in Section 1.2.4, the final conclusion of Proposition 9.3.24 generalizes to rationally chain connected nice varieties [**Esn03**, Corollary 1.3].

9.4. Del Pezzo surfaces

(Reference: [**Kol96**, III.3])

Recall from Section 9.2.5 that a Fano variety is a nice variety for which $-K$ (an anticanonical divisor) is ample.

Definition 9.4.1. A **del Pezzo surface** is a (nice) Fano variety of dimension 2.

Let X be a del Pezzo surface. According to the general definition for Fano varieties in Section 9.2.5, the degree of X is the positive integer $d := (-K).(-K) = K.K$. It then turns out that $\dim \mathrm{H}^0(X, -K) = d + 1$ [**Kol96**, Corollary III.2.3.5.2], and that $-K$ is very ample when $d \geq 3$ [**Kol96**, Proposition III.3.4.3]. Thus, if $d \geq 3$, then $|-K|$ embeds X as a degree d surface in $\mathbb{P}^d$.

Unofficial version for incidental online use

9.4.1. Del Pezzo surfaces over a separably closed field.

Lemma 9.4.2. *Let k be a separably closed field. Let X be a del Pezzo surface over k. If C is a closed integral curve on X with $C.C < 0$, then C is a (-1)-curve with constant field k.*

Proof. Since $-K$ is ample, $C.(-K) > 0$. Theorem 9.3.3(iv)⇒(v) implies that C is a (-1)-curve with constant field k. □

Definition 9.4.3. Let $0 \le r \le 8$. Points $P_1, \ldots, P_r \in \mathbb{P}^2(k)$ are in **general position** if they are distinct and *none* of the following hold:

(i) Three of the P_i lie on a line.
(ii) Six of the P_i lie on a conic.
(iii) Eight of the P_i lie on a singular cubic, with one of these eight points at the singularity.

Theorem 9.4.4 (Classification of del Pezzo surfaces)**.** *Let k be a separably closed field. Let X be a del Pezzo surface over k. Then exactly one of the following holds:*

- *$X \simeq \mathbb{P}^1 \times \mathbb{P}^1$; then* $\deg X = 8$.
- *There exists r with $0 \le r \le 8$ such that X is the blowup of $\mathbb{P}^2$ at r k-points in general position; then* $\deg X = 9 - r \in \{1, 2, \ldots, 9\}$.

Proof. Let $X \to Y$ be a proper birational morphism to a relatively minimal surface Y. By Corollary 9.3.23, $Y \simeq \mathbb{P}^2$ or $Y \simeq F_n$ for some $n \in \{0\} \cup \mathbb{Z}_{\ge 2}$. A section of $F_n \to \mathbb{P}^1$ has self-intersection $-n$ [**Har77**, Proposition V.2.9], and its strict transform in X would have self-intersection at least as negative, which contradicts Lemma 9.4.2 if $n \ge 2$. Thus $Y \simeq \mathbb{P}^2$ or $Y \simeq \mathbb{P}^1 \times \mathbb{P}^1$. By Theorem 9.3.1(b), X is obtained from Y by iteratively blowing up k-points. The blowup of $\mathbb{P}^1 \times \mathbb{P}^1$ at a k-point is isomorphic to the blowup of $\mathbb{P}^2$ at two k-points (Example 9.3.11), so we need only consider blowups of $\mathbb{P}^2$. If we ever blow up a point on an exceptional curve from a previous blowup, the strict transform C of that exceptional curve in X would satisfy $C.C < -1$, contradicting Lemma 9.4.2. Thus X is the blowup of $\mathbb{P}^2$ at a finite subset $\{P_1, \ldots, P_r\}$ of $X(k)$. Since $-K$ is ample, $0 < (-K).(-K) = K.K = 9 - r$ (the last equality follows from [**Har77**, Proposition V.3.3]), so $r \le 8$. If three of the P_i were on a line, the strict transform C of that line would satisfy $C.C \le 1 - 3 \le -2$, contradicting Lemma 9.4.2. The other restrictions on the P_i are similarly derived; see [**Dem80**, Théorème 1(i)⇔(iii)]. □

Remark 9.4.5. If X is as in Theorem 9.4.4, then $\operatorname{Pic} X \simeq \mathbb{Z}^{10-d}$: this is true when X is $\mathbb{P}^2$ or $\mathbb{P}^1 \times \mathbb{P}^1$, and blowing up a k-point adds a new factor of $\mathbb{Z}$ [**Har77**, Proposition V.3.2]. One can also describe the canonical class and

Unofficial version for incidental online use

the intersection pairing on $\operatorname{Pic} X$ explicitly with respect to a suitable basis [**Man86**, Theorem 23.8].

Remark 9.4.6. If $r \geq 9$ and X is the blowup of $\mathbb{P}^2$ at any r points, then $K.K = 9 - r \leq 0$, so X cannot be a del Pezzo surface. This shows that the property of being a del Pezzo surface is not invariant under birational maps.

Proposition 9.4.7 (Exceptional curves on a del Pezzo surface)**.** *Let k be a separably closed field. Let $X \to \mathbb{P}^2$ be the blowup of points $x_1, \ldots, x_r$ in general position, where $0 \leq r \leq 8$. Then the exceptional curves are the fibers above the x_i together with the strict transforms of the following curves in $\mathbb{P}^2$:*

(i) *a line through* 2 *of the x_i;*

(ii) *a conic through* 5 *of the x_i;*

(iii) *a cubic passing through* 7 *of the x_i, such that one of them is a double point* (*on the cubic*)*;*

(iv) *a quartic passing through* 8 *of the x_i, such that three of them are double points;*

(v) *a quintic passing through* 8 *of the x_i, such that six of them are double points; and*

(vi) *a sextic passing through* 8 *of the x_i, such that seven of them are double points and one of them is a triple point.*

Proof. See [**Man86**, Theorem 26.2]. $\square$

9.4.2. Del Pezzo surfaces over an arbitrary field. The proof of the following will be scattered over the next few subsections within Section 9.4.

Theorem 9.4.8. *Let k be a field. Let X be a del Pezzo surface over k of degree $d \geq 5$.*

(i) *If $d = 7$ or* 5*, then X has a k-point.*

(ii) *If $\dim k \leq 1$, then X has a k-point.*

(iii) *If X has a k-point, then X is birational to $\mathbb{P}^2_k$.*

(iv) *If X has a k-point and k is infinite, then $X(k)$ is Zariski dense in X.*

(v) *The homomorphism $\operatorname{Br} k \to \operatorname{Br} X$ is surjective.*

(vi) *If k is a global field, then X satisfies the local-global principle.*

(vii) *If k is a global field, then X satisfies weak approximation.*

Part (iii) implies (iv). To prove (v), list all finite groups G acting on $\mathbb{Z}^{10-d}$ that could be the image of the $\mathfrak{G}_k$-action on $\operatorname{Pic} X_{k_s}$ respecting the intersection pairing, check that $\mathrm{H}^1(\mathfrak{G}_k, \operatorname{Pic} X_{k_s}) = 0$ in each case, and apply Corollaries 6.7.8 and 6.9.11. Parts (vi) and (iii) imply (vii).

Unofficial version for incidental online use

Remark 9.4.9. In the case where k is finite, Proposition 9.3.24 proves (ii) even without the restriction $d \geq 5$.

Remark 9.4.10. When $d \leq 4$, most parts of Theorem 9.4.8 can fail. Part (i) holds for $d = 1$ but can fail for $d = 2, 3, 4$. Part (ii) can fail for $d = 2, 3, 4$ [**CTM04**]. The birational invariant $\mathrm{H}^1(\mathfrak{G}_k, \operatorname{Pic} X_{k_s})$ (see Exercise 9.6) is 0 for $\mathbb{P}^2_k$, but it can be nonzero for a degree d del Pezzo surface over a global field if $d \leq 4$; thus (iii) can fail for each $d \leq 4$. For such an example, Corollaries 6.7.8 and 6.9.11 shows that $\operatorname{Br} k \to \operatorname{Br} X$ will fail to be surjective; that is, (v) fails. This means that there is potentially a Brauer–Manin obstruction to the local-global principle and/or weak approximation, and in fact part (vi) can fail for $d = 2, 3, 4$ and part (vii) can fail for $d = 1, 2, 3, 4$, as will be discussed below.

Remark 9.4.11 (Unirationality of del Pezzo surfaces)**.** It may be that every del Pezzo surface over k with a k-point is *k-unirational*. This has already been proved for all $d \geq 3$ [**Seg43**; **Seg51**; **Man86**, Theorems 29.4 and 30.1; **Kol02**, Theorem 1.1; **Pie12**, Proposition 5.19; **Kne15**, Theorem 2.1], and also under additional hypotheses for $d = 2$ and $d = 1$ [**Man86**, Theorems 29.4; **STVA14**, Theorems 1.1 and 3.2; **FvL16**, Theorem 1.1; **KM17**, Corollary 36]. For each surface for which this holds, part (iv) of Theorem 9.4.8 holds too.

9.4.3. Degree 9. Then $X_{k_s} \simeq \mathbb{P}^2_{k_s}$, so X is a Severi–Brauer surface. In particular:

- If X has a k-point, then $X \simeq \mathbb{P}^2_k$ (Proposition 4.5.10).
- If $\dim k \leq 1$, then $X \simeq \mathbb{P}^2_k$.
- If k is a global field, then X satisfies the local-global principle (Theorem 4.5.11).

9.4.4. Degree 8.

Proposition 9.4.12. *Let X be a degree 8 del Pezzo surface over a field k. Then exactly one of the following holds:*

(1) *There is a degree 2 étale extension $L \supseteq k$ and a nice conic C over L such that X is isomorphic to the restriction of scalars $\operatorname{Res}_{L/k} C$. (In the split case $L = k \times k$, this means simply that X is a product of two nice conics over k.)*

(2) *X is the blowup of $\mathbb{P}^2_k$ at a k-point.*

Proof. By Theorem 9.4.4, either $X_{k_s} \simeq (\mathbb{P}^1 \times \mathbb{P}^1)_{k_s}$ or X_{k_s} is the blowup of $\mathbb{P}^2_{k_s}$ at a k_s-point.

Unofficial version for incidental online use

(1) Suppose that $X_{k_s} \simeq (\mathbb{P}^1 \times \mathbb{P}^1)_{k_s}$; i.e., X is a twist of $\mathbb{P}^1 \times \mathbb{P}^1$. To understand the twists, we need to compute $\operatorname{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_{k_s})$. First, $\operatorname{Aut} \mathbb{P}^1_{k_s} \simeq \mathrm{PGL}_2(k_s)$ (see [**Har77**, Example II.7.1.1]). Let $A \leq \operatorname{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_{k_s})$ be the subgroup generated by the action of $\mathrm{PGL}_2(k_s)$ on each factor and the involution that interchanges the two factors. Let S and I be the kernel and image of the homomorphism

$$\operatorname{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_{k_s}) \to \operatorname{Aut}(\operatorname{Pic}(\mathbb{P}^1 \times \mathbb{P}^1)_{k_s})$$

describing the action of automorphisms on the Picard group, which is $\mathbb{Z} \times \mathbb{Z}$ (see [**Har77**, Example II.6.6.1 and Corollary II.6.16]). We have a commutative diagram

(9.4.13)

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{PGL}_2(k_s) \times \mathrm{PGL}_2(k_s) \arrow[r, hook] \arrow[d] & A \arrow[r] \arrow[d] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & S \arrow[r] & \operatorname{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_{k_s}) \arrow[r] & I \arrow[r] & 1 \end{tikzcd}$$

with exact rows. Any automorphism in S induces linear automorphisms of the spaces of global sections of $\mathscr{O}(1,0)$ and $\mathscr{O}(0,1)$, and hence is given by an element of $\mathrm{PGL}_2(k_s) \times \mathrm{PGL}_2(k_s)$. In other words, the left vertical homomorphism is an isomorphism. On the other hand, an automorphism of $(\mathbb{P}^1 \times \mathbb{P}^1)_{k_s}$ acts on the Picard group $\mathbb{Z} \times \mathbb{Z}$ so as to preserve the ample cone, which is the first quadrant, so it can only be the identity or the coordinate-interchanging involution of $\mathbb{Z} \times \mathbb{Z}$. In other words, the right vertical homomorphism is an isomorphism. Thus the middle vertical homomorphism is an isomorphism too.

Taking cohomology of either of the now-identified rows of (9.4.13) yields a map of pointed sets

$$\mathrm{H}^1(k, \operatorname{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_{k_s}) \longrightarrow \mathrm{H}^1(k, \mathbb{Z}/2\mathbb{Z}).$$

An element of the latter corresponds to a degree 2 étale extension $L \supseteq k$, and its preimage in $\mathrm{H}^1(k, \operatorname{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_{k_s}))$ is in bijection with

$$\mathrm{H}^1(k, \text{the } L/k\text{-twist of } \mathrm{PGL}_2 \times \mathrm{PGL}_2) \simeq \mathrm{H}^1(L, \mathrm{PGL}_2),$$

the isomorphism arising from a nonabelian analogue of Shapiro's lemma. The latter set $\mathrm{H}^1(L, \mathrm{PGL}_2)$ parameterizes twists of $\mathbb{P}^1$ over L, i.e., conics over L. Thus twists of $\mathbb{P}^1 \times \mathbb{P}^1$ are parameterized by pairs (L, C) where L is a degree 2 étale extension of k and C is a nice conic over L. By writing out explicit 1-cocycles, one can verify that the twist corresponding to (L, C) is the restriction of scalars $\operatorname{Res}_{L/k} C$.

(2) There is a unique exceptional curve on X_{k_s}. It must be Galois invariant, so it descends to a genus 0 curve E over k. Blow down E to get a morphism $X \to Y$, where Y is a Severi–Brauer surface over k. The

Unofficial version for incidental online use

image of E is a k-point on Y, so $Y \simeq \mathbb{P}^2_k$. Thus X is the blowup of $\mathbb{P}^2_k$ at a k-point. $\square$

Corollary 9.4.14. *If* $\dim k \le 1$*, then any degree* 8 *del Pezzo surface* X *over* k *has a* k*-point.*

Proof. It suffices to consider case (1) of Proposition 9.4.12. Since $\dim k \le 1$, we have $\operatorname{Br} L = 0$. Since C is a 1-dimensional Severi–Brauer variety over L, it has an L-point. Finally, $X(k) = C(L)$. $\square$

Corollary 9.4.15. *Let* X *be a degree* 8 *del Pezzo surface over a field* k*. If* X *has a* k*-point, then* X *is birational to* $\mathbb{P}^2_k$*.*

Proof. In case (2) of Proposition 9.4.12, X is a blowup of $\mathbb{P}^2_k$, and hence birational to $\mathbb{P}^2_k$. In case (1), X has the form $\operatorname{Res}_{L/k} C$; if X has a k-point, then C has an L-point, so $C \simeq \mathbb{P}^1_L$, which is birational to $\mathbb{A}^1_L$, so X is birational to $\operatorname{Res}_{L/k} \mathbb{A}^1_L \simeq \mathbb{A}^2_k$, which is birational to $\mathbb{P}^2_k$. $\square$

Corollary 9.4.16. *A degree* 8 *del Pezzo surface over a global field* k *satisfies the local-global principle.*

Proof. If $X = \operatorname{Res}_{L/k} C$, apply the local-global principle to C over L. If X is the blowup of $\mathbb{P}^2_k$ at a k-point, then X has a k-point already. $\square$

9.4.5. Degree 7.

Proposition 9.4.17. *A degree* 7 *del Pezzo surface* X *is* $\mathbb{P}^2_k$ *blown up at either two* k*-points or at a closed point whose residue field is separable of degree* 2 *over* k*.*

Proof. There are three exceptional curves on X_{k_s}, arranged in a chain, say E_1, E_2, E_3 in order. The middle one E_2 is Galois-stable, so E_2 descends to a nice genus 0 curve over k. Blowing down E_2 yields a nice surface Y with a k-point. Blowing down E_1 and E_3 together instead yields a Severi–Brauer variety Z over k. Since Z is birational to Y, it has a k-point too, so $Z \simeq \mathbb{P}^2_k$. The image of $E_1 \cup E_3$ in $Z \simeq \mathbb{P}^2_k$ is what must be blown up to recover X. $\square$

9.4.6. Degree 6.

Lemma 9.4.18. *Let* X *be a degree* 6 *del Pezzo surface over a field* k*. If there exist separable extensions* K *and* L *with* $[K : k] = 2$ *and* $[L : k] = 3$ *such that* X *has a* K*-point and an* L*-point, then* X *has a* k*-point.*

Proof. Consider the anticanonical embedding $X \subseteq \mathbb{P}^6$. If the K-point or L-point is defined over k, we are done. Otherwise the conjugates of the

Unofficial version for incidental online use

two points give five geometric points on X. If these five points are sufficiently generic on X, then the 4-dimensional linear subspace of $\mathbb{P}^6$ passing through them intersects X in a 0-cycle of degree 6, of which five points are accounted for, and the remaining point is $\mathfrak{G}_k$-stable, hence a k-point. One can remove the genericity hypothesis by invoking the Lang–Nishimura theorem (Theorem 3.6.11): the construction above defines a rational map $\operatorname{Sym}^2 X \times \operatorname{Sym}^3 X \dashrightarrow X$, and the hypothesis supplies a k-point on the smooth source, so the target has a k-point. $\square$

There are six exceptional curves on X_{k_s}, forming a hexagon. Label them $E_1, \ldots, E_6$ in order around the hexagon.

Proposition 9.4.19. *Let X be a degree 6 del Pezzo surface over a field k. If either $\dim k \leq 1$, or k is a global field and $X(\mathbf{A}) \neq \emptyset$, then X has a k-point.*

Proof. (This is based on [**CT72**].) Since the action of $\mathfrak{G}_k$ on $\{E_1, \ldots, E_6\}$ respects intersections, it preserves the partition $\{\{E_1, E_3, E_5\}, \{E_2, E_4, E_6\}\}$. The stabilizer in $\mathfrak{G}_k$ of $\{E_1, E_3, E_5\}$ is G_K for some separable extension K of degree 1 or 2. Blowing down E_1, E_3, E_5 simultaneously on X_K yields a degree 9 del Pezzo surface Y. If $\dim k \leq 1$, then $\operatorname{Br} K = 0$, so $Y \simeq \mathbb{P}^2_K$, so Y has a K-point. If k is a global field and $X(\mathbf{A}) \neq \emptyset$, then $X(\mathbf{A}_K) \neq \emptyset$, so $Y(\mathbf{A}_K) \neq \emptyset$, so $Y \simeq \mathbb{P}^2_K$ by Theorem 4.5.11 (the local-global principle for Severi–Brauer varieties). In either case, Y has a K-point, and X is birational to Y, so X has a K-point.

The same argument using the partition $\{\{E_1, E_4\}, \{E_2, E_5\}, \{E_3, E_6\}\}$ shows that X has an L-point for some separable extension L of degree 1 or 3. If either K or L has degree 1, then X has a k-point already. Otherwise Lemma 9.4.18 shows that X has a k-point. $\square$

Sketch of alternative proof. Let $U = X - \bigcup_{i=1}^{6} E_i$. Then U_{k_s} is $\mathbb{P}^2_{k_s}$ with three lines deleted; in other words $U_{k_s} \simeq \mathbb{G}_m^2$. One can prove that in general, if U is a variety over a field k and $U_{k_s} \simeq \mathbb{G}_m^n$ for some $n \in \mathbb{N}$, then U is a torsor under a torus T. If $\dim k \leq 1$, then Theorem 5.12.19(b) shows that U has a k-point. Now suppose that k is a global field and $X(\mathbf{A}) \neq \emptyset$. For every v, Proposition 3.5.75 shows that $X(k_v)$ is Zariski dense in X, so U has a k_v-point. By Theorem 5.12.32, U has a k-point. Hence X has a k-point. $\square$

Proposition 9.4.20. *Let X be a degree 6 del Pezzo surface over a field k. If X has a k-point, then X is birational to $\mathbb{P}^2_k$.*

Proof. Let $x \in X(k)$.

Case 1: The point x lies on a unique exceptional curve E_i. Then E_i is defined over k and may be blown down, so we reduce to the case of a degree 7 del Pezzo surface.

Unofficial version for media online use

Case 2: The point x lies on the intersection of two exceptional curves. Suppose that $x \in E_1 \cap E_2$. Then $E_3 \cup E_6$ is $\mathfrak{G}_k$-stable. Blowing down E_3 and E_6 simultaneously, we reduce to the case of a degree 8 del Pezzo surface.

Case 3: The point x does not lie on any exceptional curve. Make the variety *more* complicated by blowing up x! This yields a degree 5 del Pezzo surface Y. Let D be the exceptional divisor for this blowup. Let P be the dual graph of the ten exceptional curves, so P has one vertex for each exceptional curve, and one edge for each intersecting pair of exceptional curves. Then P turns out to be the Petersen graph; this shows that there are three exceptional curves on Y meeting D, and they are disjoint. Blowing them down let us reduce to the case of a degree 8 del Pezzo surface. $\square$

9.4.7. Degree 5. Recall the fine moduli space $M_{0,5}$ of Example 2.3.9.

Lemma 9.4.21. *Let $\mathcal{X}$ be the blowup of $\mathbb{P}^2$ at the points $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, and $(1:1:1)$. Then there is an open immersion $M_{0,5} \hookrightarrow \mathcal{X}$, and the S_5-action on $M_{0,5}$ extends to an S_5-action on $\mathcal{X}$. Moreover, $S_5 \to \operatorname{Aut}\mathcal{X}$ is an isomorphism.*

Proof. Let $\mathcal{X}'$ be the complement in $\mathcal{X}$ of the ten exceptional curves, so $\mathcal{X}'$ is the complement in $\mathbb{P}^2$ of the $\binom{4}{2}$ lines through the four blown-up points. Then $\mathcal{X}'$ and $M_{0,5}$ are the same open subvariety of $\mathbb{A}^2$! By symmetry, the transposition $(0,1,\infty,x,y) \mapsto (0,1,\infty,y,x)$ of $M_{0,5}$ extends to an automorphism of $\mathcal{X}$. A calculation shows that the 5-cycle

$$(0,1,\infty,x,y) \longmapsto (y,0,1,\infty,x) \sim \left(0,1,\infty,\frac{1}{y},\frac{x-y}{y(x-1)}\right)$$

also extends. These generate S_5, so S_5 acts faithfully on $\mathcal{X}$. The dual graph of the set of the exceptional curves is the Petersen graph P. We have

$$S_5 \hookrightarrow \operatorname{Aut}\mathcal{X} \to \operatorname{Aut} P \simeq S_5. \tag{9.4.22}$$

The homomorphism $\operatorname{Aut}\mathcal{X} \to \operatorname{Aut} P$ is injective since an automorphism preserving each of the ten exceptional curves would act on the blowdown $\mathbb{P}^2$ and would fix the four blown-up points, forcing it to be the identity. Thus all the homomorphisms in (9.4.22) are isomorphisms. $\square$

Remark 9.4.23. One can show that $\mathcal{X} \supset \mathcal{X}'$ is isomorphic to the compactification $\overline{M}_{0,5} \supset M_{0,5}$ of Example 2.3.12. This explains why the S_5-action on $M_{0,5}$ extends to $\mathcal{X}$.

Lemma 9.4.24. *Every degree 5 del Pezzo surface over a field k is dominated by the Grassmannian $\operatorname{Gr}(2,5)$.*

Proof. Let $\mathcal{X}$ be the degree 5 del Pezzo surface in Lemma 9.4.21. The group S_5 acts on k^5 by permuting the coordinates, so it acts on the Grassmannian

Unofficial version for incidental online use

$\mathrm{Gr}(2,5)$ defined in Example 9.2.3. Given a general point $[W] \in \mathrm{Gr}(2,5)$, so W is a 2-dimensional subspace of k^5, the intersections of W with the five coordinate hyperplanes are five distinct lines in W, and projectivizing yields a point of $M_{0,5}$. This defines the first of the two S_5-equivariant rational maps

$$\mathrm{Gr}(2,5) \dashrightarrow M_{0,5} \hookrightarrow \mathcal{X}, \tag{9.4.25}$$

and the second map is the open immersion of Lemma 9.4.21. The first map is dominant since given five distinct points in $\mathbb{P}^1$, or equivalently five distinct lines in a 2-dimensional space W, one can choose linear functionals $\lambda_1, \ldots, \lambda_5 \colon W \to k$ cutting out these lines, and the image of the linear map $(\lambda_1, \ldots, \lambda_5) \colon W \to k^5$ represents a preimage in $\mathrm{Gr}(2,5)$.

We now twist. Over a *separably closed* field, there is only one degree 5 del Pezzo surface; see Exercise 9.8. Thus, over k, any other one is a twist X of $\mathcal{X}$ by a cocycle ξ representing a class in $\mathrm{H}^1(k, \operatorname{Aut} \mathcal{X}_{k_s}) = \mathrm{H}^1(k, S_5)$. Twist k^5 and (9.4.25) by ξ to obtain a degree 5 étale k-algebra L and

$$\mathrm{Gr}(2,L) \dashrightarrow M_{0,5}^{(L)} \hookrightarrow X, \tag{9.4.26}$$

where $M_{0,5}^{(L)}$ is as in Example 2.3.11. In $\mathrm{Gr}(2,L)$, the space L is just another 5-dimensional vector space, so $\mathrm{Gr}(2,L) \simeq \mathrm{Gr}(2,5)$. Thus $\mathrm{Gr}(2,5)$ dominates X. $\square$

Remark 9.4.27. Let X be a degree 5 del Pezzo surface. Let $X' \subset X$ be the complement of the ten exceptional curves. The proof of Lemma 9.4.24 shows that $X' \subset X$ is isomorphic to $M_{0,5}^{(L)} \subset \overline{M}_{0,5}^{(L)}$ for some degree 5 étale k-algebra L, where $\overline{M}_{0,5}^{(L)}$ is as in 2.3.12.

Corollary 9.4.28. *Every degree 5 del Pezzo surface has a k-point.*

Proof. Combine Lemma 9.4.24 with the Lang–Nishimura theorem (Theorem 3.6.11). $\square$

The literature contains several different proofs of Corollary 9.4.28; see [**Enr97**] (not quite complete), [**SD72**], [**SB92**], [**Sko93**], [**Kol96**, Exercise III.3.13], and [**Has09**, Exercise 3.1.4]. The proof we gave is closest to that in [**Sko93**].

Lemma 9.4.24 implies that a degree 5 del Pezzo surface X over k is k-unirational, but even more is true: X is *k-rational*—this was first proved by Manin [**Man66**, Theorem 3.15] (at least for perfect k), assuming Enriques's claim that $X(k) \neq \emptyset$).

Theorem 9.4.29. *Every degree 5 del Pezzo surface over a field k is birational to $\mathbb{P}^2_k$.*

Unofficial version for media online use

Proof. Let X be the del Pezzo surface. Let $X' \subset X$ be the complement of the exceptional curves in X.

First suppose that X' has a k-point x. Then the blowup of X at x is a degree 4 del Pezzo surface Y. There are 16 exceptional curves on Y (over k_s): the strict transforms of the ten exceptional curves on X, the preimage of x, and five more. Moreover, those last five curves are skew, as can be checked over $\overline{k}$: if Y is the blowup of $\mathbb{P}^2$ at points $x_1, \ldots, x_5$ in general position, and X is the blowup of $\mathbb{P}^2$ at $x_1, \ldots, x_4$, then the five curves are the strict transforms of the conic through $x_1, \ldots, x_5$ and of the four lines connecting each of $x_1, \ldots, x_4$ to x_5. Blowing down this $\mathfrak{G}_k$-stable set of five skew lines on Y yields a degree 9 del Pezzo surface Z with a k-point, so $Z \simeq \mathbb{P}^2_k$.

Now suppose that X' has no k-points. The pair $X' \subset X$ is isomorphic to $M_{0,5}^{(L)} \subset \overline{M}_{0,5}^{(L)}$ for some degree 5 étale k-algebra L. Then $M_{0,5}^{(L)}$ has no k-point, so there is no closed immersion $\operatorname{Spec} L \hookrightarrow \mathbb{P}^1_k$. Counting the closed points on $\mathbb{P}^1_k$ with each residue field shows this is possible only in these cases:

(i) $L = k^5$ with $k = \mathbb{F}_2$ or $k = \mathbb{F}_3$; or

(ii) $L = \mathbb{F}_2 \times \mathbb{F}_4 \times \mathbb{F}_4$ with $k = \mathbb{F}_2$.

In case (i), X is the blowup of $\mathbb{P}^2_k$ at four k-points, so X is birational to $\mathbb{P}^2_k$. In case (ii), $L \simeq L_3 \times L_2$ for étale algebras L_3 of degree 3 and L_2 of degree 2. Fix one closed immersion $\iota\colon \operatorname{Spec} L_3 \to \mathbb{P}^1_k$. Then each $(\operatorname{Aut} \mathbb{P}^1)$-orbit of closed immersions $\operatorname{Spec} L \to \mathbb{P}^1_k$ contains a unique representative whose restriction to $\operatorname{Spec} L_3$ is ι, so X' is isomorphic to the space of closed immersions $\operatorname{Spec} L_2 \to U := \mathbb{P}^1 - \iota(\operatorname{Spec} L_3)$. Thus we have birational equivalences

$$X \sim X' \sim \operatorname{Res}_{L_2/k} U \sim \operatorname{Res}_{L_2/k} \mathbb{A}^1_k \simeq \mathbb{A}^2_k \sim \mathbb{P}^2_k. \qquad \square$$

9.4.8. Degree 4. These X are smooth intersections of two quadrics in $\mathbb{P}^4$ [**Kol96**, Theorem III.3.5.4]. If k is a global field, then the local-global principle can fail (Exercise 8.3), and weak approximation can fail even if X has a k-point [**CTS77**, III, Exemple (a)].

9.4.9. Degree 3. These are nice cubic surfaces in $\mathbb{P}^3$ [**Kol96**, Theorem III.3.5.3]. Mordell [**Mor49**] conjectured that nice cubic surfaces over $\mathbb{Q}$ satisfy the local-global principle, but this turned out to be false [**SD62**, §2]. Selmer [**Sel53**] proved that diagonal cubic surfaces $ax^3+by^3+cz^3+dw^3=0$ in $\mathbb{P}^3_{\mathbb{Q}}$ for nonzero integers a, b, c, d *satisfy* the local-global principle if $ab = cd$ or $|abcd| \le 500$, but later Cassels and Guy [**CG66**] discovered that the surface

$$5x^3 + 9y^3 + 10z^3 + 12w^3 = 0$$

over $\mathbb{Q}$ violates the local-global principle. Also, weak approximation can fail even if X is minimal and has a rational point [**SD62**, §3] (we ask for

Unofficial version for incidental online use

X to be minimal since otherwise one could simply blow up a k-point on a degree 4 counterexample to weak approximation). See [**CTKS87**] for many more counterexamples.

9.4.10. Degree 2. The anticanonical map is a degree 2 morphism $X \to \mathbb{P}^2$ ramified along a nice curve of degree 4 in $\mathbb{P}^2$ [**Kol96**, Theorem III.3.5.2]. In other words, X is of degree 4 in a weighted projective space $\mathbb{P}(1,1,1,2)$. If k is a global field, then X need not satisfy the local-global principle: Kresch and Tschinkel [**KT04**] give many counterexamples, including the surface over $\mathbb{Q}$ defined by the weighted homogeneous equation

$$w^2 = -6x^4 - 3y^4 + 2z^4.$$

Colliot-Thélène observed that one can obtain a counterexample also by replacing z^2 by z^4 in Iskovskikh's surface of Section 8.2.5; this results in the surface

$$y^2 = -z^4 + (3w^2 - x^2)(x^2 - 2w^2)$$

over $\mathbb{Q}$.

Weak approximation can fail too, even if X is minimal and has a k-point [**KT04**].

Remark 9.4.30. So far, every time a del Pezzo surface has been found to violate the local-global principle, the violation has been explained by the Brauer–Manin obstruction, as predicted by Conjecture 9.2.27.

9.4.11. Degree 1. Then X is of degree 6 in a weighted projective space $\mathbb{P}(1,1,2,3)$ [**Kol96**, Theorem III.3.5.1]. The common zero locus of any basis s_1, s_2 of the 2-dimensional space $\mathrm{H}^0(X, -K)$ is independent of the choice of basis. This locus consists of a single degree 1 point, since $(-K).(-K) = 1$. In other words, the intersection of any two distinct divisors in $|-K|$ is a canonical k-point! Thus $X(k) \neq \emptyset$.

In particular, the local-global principle holds trivially. On the other hand, there can be a Brauer–Manin obstruction to weak approximation, even if X is minimal [**VA08**, Proposition 7.1].

9.4.12. Summary. The results on the arithmetic of del Pezzo surfaces are summarized in the following table, whose entries answer the following questions about a del Pezzo surface of specified degree over a field k:

- **k-point:** Must the surface have a k-point?
- **k-rational†:** *If the surface has a k-point*, must it be birational to $\mathbb{P}^2_k$?
- **k-unirational†:** *If the surface has a k-point*, must it be dominated by $\mathbb{P}^2_k$?

Unofficial version for incidental online use

- **local-global:** If k is a global field, must the surface satisfy the local-global principle?
- **weak appr.:** If k is a global field, must the surface satisfy weak approximation?

Degree	k-point	k-rational†	k-unirational†	local-global	weak appr.
9	NO	YES	YES	YES	YES
8	NO	YES	YES	YES	YES
7	YES	YES	YES	YES	YES
6	NO	YES	YES	YES	YES
5	YES	YES	YES	YES	YES
4	NO	NO	YES	NO	NO
3	NO	NO	YES	NO	NO
2	NO	NO	?	NO	NO
1	YES	NO	?	YES	NO

The daggers † warn that those columns presume the existence of a k-point.

9.5. Rational points on varieties of general type

9.5.1. Curves of genus > 1 over number fields.

(References: [**HS00**], [**BG06**])

Let X be a nice curve over a field K. In Section 2.6.4.2, we stated the following result, conjectured by Mordell in 1922 (for $K = \mathbb{Q}$) [**Mor22**] and proved by Faltings in 1983.

Theorem 9.5.1 ([**Fal83**]). *Let X be a nice curve of genus > 1 over a number field K. Then $X(K)$ is finite.*

We will not give a proof, since the known proofs are very complicated. Faltings's proof uses an idea of Parshin to reduce the problem to proving a conjecture of Shafarevich that for a fixed number field K, a fixed finite set of places S of K, and a fixed $d \geq 0$, there are at most finitely many isomorphism classes of d-dimensional abelian varieties over K with good reduction outside S [**Fal83**]. Vojta [**Voj91**] gave a different proof of Theorem 9.5.1, based on diophantine approximation, and later Bombieri [**Bom90**] gave a more elementary version of Vojta's proof; Bombieri's proof is presented also in [**HS00**].

Remark 9.5.2. All known proofs of Theorem 2.6.8 are ineffective. In other words, it is not known whether there exists a Turing machine that takes as input a number field K and equations for a nice K-curve X of genus > 1, and outputs the list of K-points on X. See [**Poo02**] for more about this problem.

Unofficial version for incidental online use

9.5.2. Curves of genus > 1 over function fields.

(References: [**Sam66**, **Vol97**])

The analogue of Theorem 9.5.1 over global function fields can fail because of Frobenius morphisms, as the following two examples show.

Example 9.5.3. Let X_0 be a nice curve of genus > 1 over a finite field $\mathbb{F}_q$. Let $K = \mathbf{k}(X_0)$. Let $X = (X_0)_K$. By Proposition 3.6.5(b), $X(K) = \operatorname{Hom}_{\mathbb{F}_q}(X_0, X_0)$, which is infinite since it contains the q^n-power Frobenius morphism for every $n \geq 0$.

Example 9.5.4. Let q be an odd prime power, and let $K = \mathbb{F}_q(t)$. Let $f \in \mathbb{F}_q[x]$ be a separable polynomial of degree ≥ 5. Let X be the nice K-curve birational to $f(t)y^2 = f(x)$, so X has genus > 1. Then for every $n \geq 0$, we have $(t^{q^n}, f(t)^{(q^n-1)/2}) \in X(K)$, so $X(K)$ is infinite.

This example can be explained using the nice K-curve Y birational to the affine curve $y^2 = f(x)$: Under the isomorphism $X_{K(f(t)^{1/2})} \to Y_{K(f(t)^{1/2})}$ sending (x, y) to $(x, f(t)^{1/2}y)$, the points above correspond to $(t^{q^n}, f(t)^{q^n/2})$, which are as constructed in Example 9.5.3.

If we consider function fields over *infinite* constant fields, then the analogue of Theorem 9.5.1 can fail even in characteristic 0:

Example 9.5.5. Let $K = \mathbb{C}(t)$. Let X_0 be a curve over $\mathbb{C}$. Let $X = (X_0)_K$. Then $X(K)$ is infinite since it contains $X_0(\mathbb{C})$.

Nevertheless, there are positive results. To state them, we introduce a few definitions.

Definition 9.5.6. A **function field with field of constants** k is $K := \mathbf{k}(V)$, where V is an integral k-variety and k is algebraically closed in K.

Remark 9.5.7. By Proposition 2.2.22(i), the requirement that k be algebraically closed in K is automatically satisfied if V is geometrically integral.

Definition 9.5.8. Let K be a function field with field of constants k. Let X be a K-variety.

(i) Call X **constant** or **split** if $X = Y_K$ for some k-variety Y.

(ii) Call X **isotrivial** if there exists a finite extension $K' \supset K$ such that $X_{K'}$ is constant (with respect to the constant field of K').

Example 9.5.9. The curves in Examples 9.5.3 and 9.5.5 are constant. The curve in Example 9.5.4 is isotrivial but not constant.

Theorem 9.5.10. *Let K be a function field with field of constants k. Let X be a regular, projective, geometrically integral K-curve of genus > 1 such*

Unofficial version for incidental online use

that $X(K)$ is infinite. If $\operatorname{char} k = 0$*, then X is constant. If* $\operatorname{char} k = p$*, then X is isotrivial. Moreover, X is nice, so $g(X_{\overline{K}}) = g(X)$.*

Proof. By induction on $\operatorname{tr}\deg(K/k)$, we may reduce to the case in which $\operatorname{tr}\deg(K/k) = 1$. For $\operatorname{char} k = 0$, the first complete proof appeared in [**Gra65**] (see also [**Man63**], which was corrected in [**Col90**]). For $\operatorname{char} k = p$, we may assume that k is algebraically closed; then [**Sam66**, Théorème 4] proves the result when $g(X_{\overline{K}}) > 1$, and in particular when $g(X_{\overline{K}}) = g(X)$ since we assumed $g(X) > 1$. If $g(X_{\overline{K}}) < g(X)$, then $X(K)$ is finite by [**Vol91**, Theorem 3]. Finally, by Theorem 2.5.1, the curve X is nice if and only if $g(X_{\overline{K}}) = g(X)$. $\square$

See [**Miw69**] for more detailed results.

9.5.3. Higher-dimensional varieties.

(Reference: [**Lan91**])

Conjecture 9.5.11 (Bombieri, Lang independently)**.** *Let k be a number field. Let X be a geometrically integral k-variety of general type such that* $\dim X > 0$*. Then $X(k)$ is not Zariski dense in X.*

There are various stronger forms proposed by Lang, discussed in [**Lan91**, I,§3]. Here is one of them:

Conjecture 9.5.12 (Lang)**.** *Let k be a number field. Let X be a geometrically integral k-variety of general type such that* $\dim X > 0$*. Then there exists a closed subvariety $S \subsetneq X$ such that $(X - S)(L)$ is finite for all finite extensions $L \supseteq k$.*

In fact, Lang predicts what S should be [**Lan91**, I,§3].

Faltings simplified and generalized Vojta's methods to prove that Conjectures 9.5.11 and 9.5.12 are true when X is a subvariety of an abelian variety [**Fal91**].

Exercises

9.1. Use the Riemann–Roch theorem to prove Proposition 9.1.1.

9.2. Given a field k, describe all nice k-varieties that are simultaneously Fano and of general type.

9.3. Let X be a nice surface over a field k. Let $C \subset X$ be a curve. Show that C is a (-1)-curve with constant field k on X if and only if $C_{\overline{k}}$ is a (-1)-curve on $X_{\overline{k}}$.

Unofficial version for incidental online use

9.4. Let X be a nice surface over a field k. Let K be a canonical divisor on X. Let $C \subset X$ be a curve. Without using Theorem 9.3.3, show that C is a (-1)-curve on X with constant field k if and only if $C.C = -1$ and $C.K = -1$.

9.5. Let X be a nice surface over an algebraically closed field k. For a coherent sheaf $\mathscr{F}$ on X and for any $i \geq 0$, define $h^i(\mathscr{F}) := \dim_k \mathrm{H}^i(X, \mathscr{F})$ and the **Euler characteristic** $\chi(\mathscr{F}) := \sum_{i \geq 0} (-1)^i h^i(\mathscr{F})$. Let $C \subset X$ be a curve. Without using Theorem 9.3.3, show that C is a (-1)-curve if and only if $\chi(\mathscr{O}_C) > 0$ and $C.C = -h^0(\mathscr{O}_C)$.

9.6. Let X be a nice surface over a field k. Let P be a closed point of X. Let $L = \mathbf{k}(P)$; suppose that L is separable over k. Let Y be the blowup of X at P. Let $\mathbb{Z}[\mathfrak{G}_k/\mathfrak{G}_L]$ be the permutation module associated to $L \supseteq k$.

(a) Prove that $\operatorname{Pic} Y_{k_s} \simeq \operatorname{Pic} X_{k_s} \oplus \mathbb{Z}[\mathfrak{G}_k/\mathfrak{G}_L]$.

(b) Prove that the natural homomorphism

$$\mathrm{H}^1(\mathfrak{G}_k, \operatorname{Pic} X_{k_s}) \longrightarrow \mathrm{H}^1(\mathfrak{G}_k, \operatorname{Pic} Y_{k_s})$$

is an isomorphism.

(c) Deduce that $\mathrm{H}^1(\mathfrak{G}_k, \operatorname{Pic} X_{k_s})$ is a birational invariant of a nice surface X over a perfect field k.

9.7. Let $X \subseteq \mathbb{P}^n_k$ be a degree 3 hypersurface over a field k for some $n \geq 2$.

(a) Let L be a degree 2 separable field extension of k. Prove that if X has an L-point, then X has a k-point.

(b) Do the same without the separability hypothesis.

(Cassels and Swinnerton-Dyer conjectured that the same holds for an extension L of k of any degree d not divisible by 3, but this is unknown even in the case $\dim X = 2$, $k = \mathbb{Q}$, $d = 4$; see **[Cor76]**.)

9.8. Let k be a field.

(a) Prove that for $0 \leq r \leq 4$, the group $\mathrm{PGL}_3(k) = \operatorname{Aut} \mathbb{P}^2_k$ acts transitively on the set of r-tuples of points in $\mathbb{P}^2(k)$ in general position.

(b) Fix a separably closed field k. For $5 \leq d \leq 9$, determine the number of isomorphism types of degree d del Pezzo surfaces over k.

9.9. Let k be a finite field. Prove that there are exactly seven isomorphism types of degree 5 del Pezzo surfaces over k.

Unofficial version for incidental online use

Unofficial version for incidental online use

Appendix A

Universes

(Reference: [**SGA** $4_{\mathbf{I}}$, I.Appendice])

The plan is to assume the existence of a very large set, called a universe, such that almost all the constructions we need can be carried out within it. Those constructions that cannot be carried out within it can be carried out in a larger universe.

According to [**SGA** $4_{\mathbf{I}}$, I.Appendice], the theory of universes comes from "the secret papers of N. Bourbaki". According to [**SGA 1**, VI, §1], the details will be given in a book in preparation by Chevalley and Gabriel to appear in the year 3000.

A.1. Definition of universe

Everything is a set. In particular, elements of a set are themselves sets. Given a set x, let $\mathcal{P}(x)$ be the set of all subsets of x.

Definition A.1.1 ([**SGA** $4_{\mathbf{I}}$, I.Appendice, Définition 1])**.** A **universe** is a set $\mathcal{U}$ satisfying the following conditions:

(U.I) If $y \in \mathcal{U}$ and $x \in y$, then $x \in \mathcal{U}$.

(U.II) If $x, y \in \mathcal{U}$, then $\{x, y\} \in \mathcal{U}$.

(U.III) If $x \in \mathcal{U}$, then $\mathcal{P}(x) \in \mathcal{U}$.

(U.IV) If $I \in \mathcal{U}$, and $(x_i)_{i \in I}$ is a collection of elements of $\mathcal{U}$, then the union $\bigcup_{i \in I} x_i$ is an element of $\mathcal{U}$.

A universe $\mathcal{U}$ is not a "set of all sets". In particular, a universe cannot be a member of itself; see Exercise A.2.

Unofficial version for incidental online use

A.2. The universe axiom

To the usual ZFC axioms of set theory (the Zermelo-Frenkel axioms with the axiom of choice), one adds the **universe axiom** [**SGA** $4_{\mathbf{I}}$, I.Appendice.§4]:[1]

Every set is an element of some universe.

Suppose that ZFC is consistent. Then it turns out that the *negation* of the universe axiom is consistent with ZFC: given a model of ZFC, one can build another model of ZFC in which the universe axiom *fails*. But it is not known whether the universe axiom itself is consistent with ZFC.

The universe axiom is so convenient that we are going to assume it despite its uncertain status relative to ZFC.

Remark A.2.1. The original proof of Fermat's last theorem made use of constructions relying on the universe axiom! But the proof can probably be redone without this axiom; see Section A.5.

A.3. Strongly inaccessible cardinals

Definition A.3.1. A cardinal κ is **strongly inaccessible** if the following two conditions hold:

(1) For every $\lambda < \kappa$, we have $2^\lambda < \kappa$.

(2) Whenever $(\lambda_i)_{i \in I}$ is a family of cardinals indexed by a set I such that $\#I < \kappa$ and $\lambda_i < \kappa$ for every $i \in I$, we have $\sum_{i \in I} \lambda_i < \kappa$.

The two smallest strongly inaccessible cardinals are 0 and $\aleph_0$. By (1), any other strongly inaccessible cardinal κ must be larger than all of

$$\begin{aligned} \beth_0 &:= \aleph_0 \\ \beth_1 &:= 2^{\aleph_0} \\ \beth_2 &:= 2^{2^{\aleph_0}} \\ &\vdots \end{aligned}$$

By (2), κ must also be larger than the supremum $\beth_\omega$ of all these. Transfinite induction continues this sequence of cardinals by defining $\beth_\alpha$ for any ordinal α. Then κ must be larger than $\beth_{\omega^\omega}$, $\beth_{\omega^{\omega^\omega}}$, ..., and even $\beth_{\omega_1}$, where ω_1 is the first uncountable ordinal. Identify each cardinal with the first ordinal of

[1] In [**SGA** $4_{\mathbf{I}}$, I.Appendice.§4] one finds an additional axiom (UB) that is present only because Bourbaki's axioms for set theory are different from the usual ZFC axioms. Bourbaki's set theory includes a global choice operator τ: for any 1-variable predicate $P(x)$, the expression $\tau_x P(x)$ represents an element y such that $P(y)$ is true, if such a y exists. Axiom (UB) says that for any 1-variable predicate $P(x)$ and any universe $\mathcal{U}$, if there exists $y \in \mathcal{U}$ such that $P(y)$ is true, then $\tau_x P(x)$ is an element of $\mathcal{U}$. So axiom (UB) says that the elements produced by the global choice operator lie in a given universe whenever possible.

Unofficial version for incidental online use

its cardinality. Then $\omega_1 \leq 2^{\aleph_0} = \beth_1$, so $\beth_{\omega_1} \leq \beth_{\beth_1}$. But κ is also larger than $\beth_{\beth_{\omega_1}}$, $\beth_{\beth_{\beth_{\omega_1}}}$, and so on.

Theorem A.3.2. *Within ZFC, the universe axiom is equivalent to the following "large cardinal axiom":*

> *For every cardinal, there is a strictly larger strongly inaccessible cardinal.*

Proof. One direction is easy, because if $\mathcal{U}$ is a universe, then the cardinal $\sup\{\#x : x \in \mathcal{U}\}$ is strongly inaccessible. For the other direction, see [**SGA** $4_{\mathbf{I}}$, I.Appendice.§5], which constructs a universe from a strongly inaccessible cardinal. □

A.4. Universes and categories

We now assume that an uncountable universe $\mathcal{U}$ has been fixed.

Recall that everything is a set. For instance, an ordered pair (x, y) is $\{x, \{y\}\}$. A group is a 4-tuple (G, m, i, e) such that various conditions hold. Even a scheme can be described as a set.

Definition A.4.1. A **small category** is a category in which the collection of objects is a set (instead of a class).

We want all our categories to be small categories. Thus for example, **Sets** will denote not the category of all sets, but the category of *sets that are elements of* $\mathcal{U}$. Similarly, **Groups** will be the category of groups that are elements of $\mathcal{U}$, and so on.

For categories such as these two, the set of objects is a subset of $\mathcal{U}$ having the same cardinality as $\mathcal{U}$, which implies that the set of objects cannot be an *element* of $\mathcal{U}$. This creates a minor problem: the collection of all functors $\mathbf{Schemes}^{\mathrm{opp}} \to \mathbf{Sets}$, say, is a set of cardinality *larger than that of* $\mathcal{U}$! The category of such functors is still a small category, but it lives in a larger universe $\mathcal{U}'$.

A.5. Avoiding universes

Suppose that we want to prove theorems that are not conditional on the universe axiom. Then we cannot define the category **Schemes** as the set of schemes that are elements of a particular universe $\mathcal{U}$. Instead we choose *a* category of schemes that is closed under various operations, and work within that category [**SP**, Tag 020S, Tag 03XB]. Ideally, we should then show that our choice did not matter for our particular objects of study; see [**SP**, Tag 00VY] for an example of this.

Unofficial version for incidental online use

Exercises

A.1. Classify all finite universes.

A.2. Let $\mathcal{U}$ be a universe. Prove that $\mathcal{U} \notin \mathcal{U}$.

A.3. Let $P_0 = \emptyset$. For $n \in \mathbb{N}$, inductively define $P_{n+1} := \mathcal{P}(P_n)$. Let $\mathcal{U} = \bigcup_{n \in \mathbb{N}} P_n$. Prove that $\mathcal{U}$ is a universe.

Unofficial version for incidental online use

Appendix B

Other kinds of fields

Unofficial version for incidental online use

In Section 1.1, we introduced some of the most important fields for number theory, namely local and global fields. Here we discuss some other fields that arise in nature.

B.1. Higher-dimensional local fields

Higher-dimensional local fields are defined recursively as follows. A 0-**dimensional local field** is a finite field. For $n \geq 1$, an n-**dimensional local field** is a field complete with respect to a discrete valuation whose residue field is an $(n-1)$-dimensional local field. Local class field theory can be generalized to these fields, and there is also a generalization of global class field theory to finitely generated fields [**Kat79**], [**Kat80**], [**Kat82**], [**KS86**]. These generalizations involve K-theory.

Example B.1.1. The field $\mathbb{Q}_p((t))$ is a 2-dimensional local field.

Warning B.1.2. An n-dimensional local field for $n \neq 1$ is not a local field in the sense of Section 1.1.2. In the rest of this book, we use the term "local field" as in Section 1.1.2.

B.2. Formally real and real closed fields

(Reference: [**Jac89**, Chapter 11])

Definition B.2.1. A field k is **formally real** if it satisfies one of the following equivalent conditions:

(i) k admits a total ordering compatible with the addition and multiplication.

(ii) -1 is not a sum of squares in k.

The implication (ii)$\Rightarrow$(i) is not obvious. Its proof uses Zorn's lemma to find a maximal subgroup P of $k^\times$ that is closed under addition and contains $k^{\times 2}$ but not -1. Then P turns out to be the set of positive elements for an ordering on k. See [**Jac89**, Theorem 11.1] for details.

Definition B.2.2. A field k is **real closed** if it satisfies one of the following equivalent conditions:

(i) $-1 \notin k^{\times 2}$, and $k(\sqrt{-1})$ is algebraically closed.

(ii) $1 < [\overline{k} : k] < \infty$.

(iii) k is an ordered field such that every positive element has a square root and every odd degree polynomial in $k[x]$ has a zero.

(iv) k is a formally real field with no nontrivial formally real algebraic extension.

The equivalence of these conditions is not obvious. For the proof, see [**Jac89**, Theorems 11.2, 11.3, and 11.14]. The entire theory is due to Artin and Schreier.

The field $\mathbb{Q}$ is formally real but not real closed. The field $\mathbb{R}$ is real closed, as is the subfield of real numbers that are algebraic over $\mathbb{Q}$. Every formally real field has an algebraic extension that is real closed.

B.3. Henselian fields

(Reference: [**Ray70a**] or [**BLR90**, §2.3])

Complete discrete valuation rings are not the only rings satisfying Hensel's lemma.

Definition B.3.1. Let R be a local ring, and let k be its residue field. The ring R is called **henselian** if one of the following equivalent conditions holds:

(1) Every finite R-algebra is a product of local rings.

(2) Hensel's lemma for lifting roots: If $f \in R[x]$ is a monic polynomial whose reduction $\bar{f} \in k[x]$ has a simple zero $\bar{a} \in k$, then there exists a zero $a \in R$ of f reducing to $\bar{a}$.

(3) Hensel's lemma for lifting factorizations: If $f \in R[x]$ is a monic polynomial, any factorization of its reduction $\bar{f} = \bar{g}\bar{h}$ into relatively prime monic polynomials $\bar{g}, \bar{h} \in k[x]$ lifts to a factorization $f = gh$ into monic polynomials $g, h \in R[x]$.

(For the equivalence, see [**Ray70a**, I.§1.5 and VII.§3.3].)

Unofficial version for incidental online use

Definition B.3.2. A valued field is **henselian** if its valuation subring is henselian.

Example B.3.3. Let $k = \mathbb{Q}_p \cap \overline{\mathbb{Q}}$, i.e., the set of elements of $\mathbb{Q}_p$ that are algebraic over $\mathbb{Q}$. Restrict the p-adic valuation on $\mathbb{Q}_p$ to a valuation on k. Then k is a noncomplete henselian field. This field acts in many ways like $\mathbb{Q}_p$, but is algebraic over $\mathbb{Q}$, which can be an advantage.

Definition B.3.4. A henselian ring (or its fraction field) is called **strictly henselian** if its residue field is separably closed.

Example B.3.5. The maximal unramified extension k^{unr} of a discretely valued field k is strictly henselian (cf. [**Ray70a**, X.§2]) but usually not complete. For example, if k is a nonarchimedean local field, then k^{unr} is not complete.

Given a commutative local ring R, its **henselization** R^h is a henselian local ring with the following universal property: every homomorphism from R to a henselian local ring factors through R^h. Such a ring R^h exists: it can be constructed as the direct limit of R' as R' ranges over étale local R-algebras having the same residue field as R [**Ray70a**, VIII, Théorème 1].

If F is a valued field and R is its valuation ring, then one can define the henselization of F by $F^h := \operatorname{Frac}(R^h)$. The field k in Example B.3.3 is the henselization of $\mathbb{Q}$ with its p-adic valuation. One can also define the **strict henselization**. See [**Ray70a**, Chapitre VIII] or [**BLR90**, §2.3, Definitions 6 and 6′] for details.

B.4. Hilbertian fields

(References: [**Ser97**, Chapter 9] and [**FJ08**, Chapters 12, 13, and 16])

Given the polynomial

$$f(t, x) := (t + 5)x^2 + (2t - 3)x + (t^2 - 9) \in \mathbb{Q}[t, x]$$

and the number 4, we can specialize f by evaluating each coefficient at $t = 4$; the result is

$$f(4, x) = 9x^2 + 5x + 7 \in \mathbb{Q}[x].$$

The simplest version of the Hilbert irreducibility theorem states that for every irreducible polynomial $f(t, x) \in \mathbb{Q}[t, x]$, there are infinitely many $a \in \mathbb{Q}$ such that the specialized polynomial $f(a, x) \in \mathbb{Q}[x]$ is irreducible. The definition of hilbertian field is modeled after this property. (For other equivalent definitions, see [**Ser97**, Chapter 9] and [**FJ08**, §12.1].)

Definition B.4.1. A field k is **hilbertian** if for every finite list of irreducible two-variable polynomials $f_1, \ldots, f_n \in k[t, x]$ with each f_i separable in x,

Unofficial version for incidental online use

there are infinitely many $a \in k$ such that the one-variable polynomials $f_1(a, x), \dots, f_n(a, x) \in k[x]$ are simultaneously irreducible.

Global fields are hilbertian [**FJ08**, 13.4.2]. If K is a finitely generated transcendental extension of *any* field k, then K is hilbertian [**FJ08**, 13.4.2]. Finite fields, local fields, and separably closed fields are not hilbertian, as will be shown in the exercises.

B.5. Pseudo-algebraically closed fields

(Reference: [**FJ08**, Chapter 11])

These are studied in model theory.

Definition B.5.1. A field k is **pseudo-algebraically closed** (PAC) if every geometrically integral variety over k has a k-point. (See Section 2.2 for the definition of "geometrically integral variety" and Section 2.3.2 for the definition of "k-point".)

Remark B.5.2. Bertini theorems show that every geometrically integral variety of positive dimension over k contains a geometrically integral curve, so Definition B.5.1 is unchanged if we replace "variety" by "curve". (Here "curve" means "variety of dimension 1".)

The following are examples of PAC fields:

- separably closed fields;
- infinite algebraic extensions of finite fields;
- nonprincipal ultraproducts of distinct finite fields (that is, $\left(\prod_{i=1}^{\infty} k_i\right)/\mathfrak{m}$ where the k_i are finite fields of distinct orders, and $\mathfrak{m}$ is a nonprincipal maximal ideal of the ring $\prod_{i=1}^{\infty} k_i$.)

Question B.5.3 ([**FJ08**, 11.5.9(a)])**.** Is the maximal solvable extension of $\mathbb{Q}$ a PAC field?

Exercises

B.1. Let k be a local field. Let n be a positive integer such that $\operatorname{char} k \nmid n$. Prove that $k^\times/k^{\times n}$ is finite.

B.2. Prove that finite fields are not hilbertian.

B.3. Prove that separably closed fields are not hilbertian.

B.4. Prove that local fields are not hilbertian.

Unofficial version for incidental online use

Appendix C

Properties under base extension

Unofficial version for incidental online use

C.1. Morphisms

Let *blah* be a property of morphisms of schemes. We can ask the following questions:

Definition: Where in EGA (or elsewhere) is blah defined?

Composition: Is a composition of two blah morphisms blah?

Base extension: Let $f\colon X \to S$ be a morphism of schemes, and let $f'\colon X' \to S'$ be its base extension by a morphism $S' \to S$. If f is blah, must f' be blah?

fpqc descent: Let $f\colon X \to S$ be a morphism of schemes, and let $f'\colon X' \to S'$ be its base extension by an *fpqc* morphism $S' \to S$. If f' is blah, must f be blah?

Spreading out: Does blah spread out in the sense of Theorem 3.2.1(iv)?

Answers are given in Table 1 on pp. 302–303. If a reference is given, the answer is "YES". In some cases, if the answer is obvious or it follows easily from other entries, we write "YES" or "NO" instead of giving a reference. If you see a superscript (such as [4]), then please read the corresponding caveat below:

1. Our definitions of fppf and fpqc are less restrictive than the standard ones suggested by the acronyms; see Section 3.4.
2. In the fpqc column, the EGA references assume that the base extension is by a faithfully flat and quasi-compact morphism. This implies descent for

our more general notion of fpqc morphism, by Lemma C.1.1 below, provided that we know that blah is **local on the base** (in the Zariski topology), i.e., that for any morphism $f\colon X \to S$ and any Zariski open covering $\{S_i\}$ of S, the morphism f is blah if and only if $f|_{f^{-1}S_i}\colon f^{-1}S_i \to S_i$ is blah for all i. Conversely, if blah satisfies fpqc descent and is stable under base extension by open immersions, then blah is local on the base.

Lemma C.1.1 below says roughly that the "open covering" given by an fpqc morphism can be "refined" to another fpqc morphism consisting of a faithfully flat quasi-compact morphism followed by a Zariski open covering morphism.

3. In the rows labelled "geom. connected", "geom. integral", "geom. irreducible", and "geom. reduced", we are considering a morphism of finite presentation whose fibers have the specified property. The first and third properties for morphisms are called connected and irreducible in [**EGA IV**$_2$, 4.5.5].

4. The morphisms
$$\operatorname{Spec} k[x, x^{-1}] \amalg \operatorname{Spec} k[x]/(x) \longrightarrow \operatorname{Spec} k[x] \longrightarrow \operatorname{Spec} k$$
have geometrically integral fibers, but the unique fiber of the composition is not even connected. On the other hand, see [**EGA IV**$_2$, 4.5.7] for some positive results.

5. The morphisms
$$\operatorname{Spec} k[x]/(x^2) \longrightarrow \operatorname{Spec} k[x] \longrightarrow \operatorname{Spec} k$$
have geometrically reduced (and even geometrically integral) fibers, but their composition does not.

6. The property of being an immersion satisfies fppf descent, but it is not known whether it satisfies fpqc descent.

7. A composition of projective morphisms $X \to Y \to Z$ is projective *if Z is quasi-compact or the topological space underlying Z is noetherian.*

8. A composition of quasi-projective morphisms $X \to Y \to Z$ is quasi-projective *if Z is quasi-compact.*

9. Projective and quasi-projective do not satisfy fpqc descent, because they are not even local on the base in the Zariski topology; see [**Har77**, Exercise II.7.13] for a counterexample.

10. To generalize the spreading out properties for projective and quasi-projective morphisms beyond Theorem 3.2.1 to the setting of more general limits, one should work over a quasi-separated base.

11. To generalize the spreading out properties for étale, faithfully flat, flat, fppf, smooth, and G-unramified morphisms beyond Theorem 3.2.1 to

Unofficial version for incidental online use

the setting of more general limits, one should work over a quasi-compact base.

12. What is called G-unramified here is called unramified in [**EGA IV**$_4$, 17.3.1]. See Warning 3.5.32.

Lemma C.1.1. *Any fpqc morphism of schemes $f\colon X \to Y$ fits into a commutative diagram*

$$\begin{tikzcd}
X'' \arrow[dd, dotted, "\substack{\text{faithfully flat}\\ \text{quasi-compact}}"'] \arrow[dr, dotted, "\text{open immersion}"] & & \\
& X' \arrow[dl, dotted] \arrow[dr, dotted, "\text{Zariski open covering}"] & \\
Y' \arrow[dr, dotted, "\text{Zariski open covering}"'] & & X \arrow[dl, "f"] \\
& Y &
\end{tikzcd}$$

in which $Y' \to Y$ and $X' \to X$ are Zariski open covering morphisms, $X'' \to X'$ is an open immersion, and $X'' \to Y'$ is faithfully flat and quasi-compact. (*In particular, $X'' \to Y$ is fpqc.*)

Proof. Let $\{Y_i\}$ be an affine open cover of Y. Let $Y' = \coprod Y_i$, and let $X' = \coprod f^{-1}Y_i$. By definition of fpqc, for each i there is a quasi-compact open subscheme U_i of $f^{-1}Y_i$ with $f(U_i) = Y_i$. Let X'' be the open subscheme $\coprod U_i$ of X'. Then $X'' \to Y'$ is faithfully flat and quasi-compact, because each morphism $f|_{U_i}\colon U_i \to Y_i$ is so. $\square$

(Please contact the author if you can fill in some of the blanks in Table 1.)

Unofficial version for incidental online use

Table 1: Properties of morphisms

blah	Definition	Composition	Base extension	fpqc descent[2]	Spreading out
affine	[**EGA II**, 1.6.1]	[**EGA II**, 1.6.2(ii)]	[**EGA II**, 1.6.2(iii)]	[**EGA IV**$_2$, 2.7.1(xiii)]	[**EGA IV**$_3$, 8.10.5(viii)]
bijective		YES	NO	[**EGA IV**$_2$, 2.6.1(iv)]	NO
closed	[**EGA I**, 2.2.6]	[**EGA I**, 2.2.7(i)]	NO	[**EGA IV**$_2$, 2.6.2(ii)]	
closed immersion	[**EGA I**, 4.2.1]	[**EGA I**, 4.2.5]	[**EGA I**, 4.3.2]	[**EGA IV**$_2$, 2.7.1(xii)]	[**EGA IV**$_3$, 8.10.5(iv)]
dominant	[**EGA I**, 2.2.6]	[**EGA I**, 2.2.7(i)]	NO		
étale	[**EGA IV**$_4$, 17.3.1]	[**EGA IV**$_4$, 17.3.3(ii)]	[**EGA IV**$_4$, 17.3.3(ii)]	[**EGA IV**$_4$, 17.7.3(ii)]	[**EGA IV**$_4$, 17.7.8(ii)][11]
faithfully flat	[**EGA I**, **0**:6.7.8]	YES	YES	YES	YES[11]
finite	[**EGA II**, 6.1.1]	[**EGA II**, 6.1.5(ii)]	[**EGA II**, 6.1.5(iii)]	[**EGA IV**$_2$, 2.7.1(xv)]	[**EGA IV**$_3$, 8.10.5(x)]
finite presentation	[**EGA IV**$_1$, 1.6.1]	[**EGA IV**$_1$, 1.6.2(ii)]	[**EGA IV**$_1$, 1.6.2(iii)]	[**EGA IV**$_2$, 2.7.1(vi)]	
finite type	[**EGA I**, 6.3.1]	[**EGA I**, 6.3.4(ii)]	[**EGA I**, 6.3.4(iv)]	[**EGA IV**$_2$, 2.7.1(v)]	
flat	[**EGA I**, **0**:6.7.1]	[**EGA IV**$_2$, 2.1.6]	[**EGA IV**$_2$, 2.1.4]	[**EGA IV**$_2$, 2.2.11(iv)]	[**EGA IV**$_3$, 11.2.6(ii)][11]
formally étale	[**EGA IV**$_4$, 17.1.1]	[**EGA IV**$_4$, 17.1.3(ii)]	[**EGA IV**$_4$, 17.1.3(iii)]		
formally smooth	[**EGA IV**$_4$, 17.1.1]	[**EGA IV**$_4$, 17.1.3(ii)]	[**EGA IV**$_4$, 17.1.3(iii)]	[**SP**, Tag 06CS]	
formally unram.	[**EGA IV**$_4$, 17.1.1]	[**EGA IV**$_4$, 17.1.3(ii)]	[**EGA IV**$_4$, 17.1.3(iii)]		
fppf[1]	Definition 3.4.1	YES	YES	YES	YES[11]
fpqc[1]	[**Vis05**, 2.34]	[**Vis05**, 2.35(i)]	[**Vis05**, 2.35(v)]		
geom. connected[3]	[**EGA IV**$_2$, 4.5.5]	NO[4]	[**EGA IV**$_2$, 4.5.6(ii)]	[**EGA IV**$_2$, 4.5.6(ii)]	[**EGA IV**$_3$, 9.7.7(ii)]
geom. integral[3]	[**EGA IV**$_2$, 4.6.2]	NO[4,5]	[**EGA IV**$_2$, 4.6.5(i)]	[**EGA IV**$_2$, 4.6.5(i)]	[**EGA IV**$_3$, 9.7.7(iv)]
geom. irreducible[3]	[**EGA IV**$_2$, 4.5.5]	NO[4]	[**EGA IV**$_2$, 4.5.6(ii)]	[**EGA IV**$_2$, 4.5.6(ii)]	[**EGA IV**$_3$, 9.7.7(i)]
geom. reduced[3]	[**EGA IV**$_2$, 4.6.2]	NO[5]	[**EGA IV**$_2$, 4.6.5(i)]	[**EGA IV**$_2$, 4.6.5(i)]	[**EGA IV**$_3$, 9.7.7(iii)]
homeomorphism		YES	NO	[**EGA IV**$_2$, 2.6.2(iv)]	
immersion	[**EGA I**, 4.2.1]	[**EGA I**, 4.2.5]	[**EGA I**, 4.3.2]	[**SP**, Tag 02YM][6]	[**EGA IV**$_3$, 8.10.5(iii)]
injective	[**EGA I**, 3.5.11]	YES	NO	[**EGA IV**$_2$, 2.6.1(ii)]	NO
isomorphism	[**EGA I**, 2.2.2]	YES	YES	[**EGA IV**$_2$, 2.7.1(viii)]	[**EGA IV**$_3$, 8.10.5(i)]
loc. immersion	[**EGA I**, 4.5.1]	[**EGA I**, 4.5.5(i)]	[**EGA I**, 4.5.5(iii)]		

Unofficial version for incidental online use

Table 1: Properties of morphisms (continued)

blah	Definition	Composition	Base extension	fpqc descent[2]	Spreading out
loc. isomorphism	[**EGA I**, 4.5.2]	[**EGA I**, 4.5.5(i)]	[**EGA I**, 4.5.5(iii)]		
loc. of finite pres.	[**EGA IV**$_1$, 1.4.2]	[**EGA IV**$_1$, 1.4.2(ii)]	[**EGA IV**$_1$, 1.4.2(iii)]	[**EGA IV**$_2$, 2.7.1(iv)]	
loc. of finite type	[**EGA I**, 6.6.2]	[**EGA I**, 6.6.6(ii)]	[**EGA I**, 6.6.6(iii)]	[**EGA IV**$_2$, 2.7.1(iii)]	
monomorphism	[**EGA I**, **0**:4.1.1]	YES	YES	[**EGA IV**$_2$, 2.7.1(ix)]	[**EGA IV**$_3$, 8.10.5(ii)]
open	[**EGA I**, 2.2.6]	[**EGA I**, 2.2.7(i)]	NO	[**EGA IV**$_2$, 2.6.2(i)]	
open immersion	[**EGA I**, 4.2.1]	[**EGA I**, 4.2.5]	[**EGA I**, 4.3.2]	[**EGA IV**$_2$, 2.7.1(x)]	[**EGA IV**$_3$, 8.10.5(iii)]
projective	[**EGA II**, 5.5.2]	[**EGA II**, 5.5.5(ii)][7]	[**EGA II**, 5.5.5(iii)]	NO[9]	[**EGA IV**$_3$, 8.10.5(xiii)][10]
proper	[**EGA II**, 5.4.1]	[**EGA II**, 5.4.2(ii)]	[**EGA II**, 5.4.2(iii)]	[**EGA IV**$_2$, 2.7.1(vii)]	[**EGA IV**$_3$, 8.10.5(xii)]
quasi-affine	[**EGA II**, 5.1.1]	[**EGA II**, 5.1.10(ii)]	[**EGA II**, 5.1.10(iii)]	[**EGA IV**$_2$, 2.7.1(xiv)]	[**EGA IV**$_3$, 8.10.5(ix)]
quasi-compact	[**EGA I**, 6.6.1]	[**EGA I**, 6.6.4(ii)]	[**EGA I**, 6.6.4(iii)]	[**EGA IV**$_2$, 2.6.4(v)]	
quasi-finite	[**EGA II**, 6.2.3]	[**EGA II**, 6.2.4(ii)]	[**EGA II**, 6.2.4(iii)]	[**EGA IV**$_2$, 2.7.1(xvi)]	[**EGA IV**$_3$, 8.10.5(xi)]
quasi-projective	[**EGA II**, 5.3.1]	[**EGA II**, 5.3.4(ii)][8]	[**EGA II**, 5.3.4(iii)]	NO[9]	[**EGA IV**$_3$, 8.10.5(xiv)][10]
quasi-separated	[**EGA IV**$_1$, 1.2.1]	[**EGA IV**$_1$, 1.2.2(ii)]	[**EGA IV**$_1$, 1.2.2(iii)]	[**EGA IV**$_2$, 2.7.1(ii)]	
radicial	[**EGA I**, 3.5.4]	[**EGA I**, 3.5.6(i)]	[**EGA I**, 3.5.7(ii)]	[**EGA IV**$_2$, 2.6.1(v)]	[**EGA IV**$_3$, 8.10.5(vii)]
sch.-th. dominant	[**EGA IV**$_3$, 11.10.2]	YES	NO	[**EGA IV**$_3$, 11.10.5(i)]	
separated	[**EGA I**, 5.4.1]	[**EGA I**, 5.5.1(ii)]	[**EGA I**, 5.5.1(iv)]	[**EGA IV**$_2$, 2.7.1(i)]	[**EGA IV**$_3$, 8.10.5(v)]
smooth	[**EGA IV**$_4$, 17.3.1]	[**EGA IV**$_4$, 17.3.3(ii)]	[**EGA IV**$_4$, 17.3.3(iii)]	[**EGA IV**$_4$, 17.7.3(ii)]	[**EGA IV**$_4$, 17.7.8(ii)][11]
surjective	[**EGA I**, 2.2.6]	[**EGA I**, 2.2.7(i)]	[**EGA I**, 3.5.2(ii)]	[**EGA IV**$_2$, 2.6.1(i)]	[**EGA IV**$_3$, 8.10.5(vi)]
univ. bicontinuous	[**EGA IV**$_2$, 2.4.2]	[**EGA IV**$_2$, 2.4.3(ii)]	[**EGA IV**$_2$, 2.4.3(iii)]		
univ. closed	[**EGA II**, 5.4.9]	[**EGA IV**$_2$, 2.4.3(ii)]	[**EGA IV**$_2$, 2.4.3(iii)]	[**EGA IV**$_2$, 2.6.4(ii)]	
univ. homeom.	[**EGA IV**$_2$, 2.4.2]	[**EGA IV**$_2$, 2.4.3(ii)]	[**EGA IV**$_2$, 2.4.3(iii)]	[**EGA IV**$_2$, 2.6.4(iv)]	
univ. open	[**EGA IV**$_2$, 2.4.2]	[**EGA IV**$_2$, 2.4.3(ii)]	[**EGA IV**$_2$, 2.4.3(iii)]	[**EGA IV**$_2$, 2.6.4(i)]	
unramified	[**SP**, Tag 02G4]	[**SP**, Tag 02G9]	[**SP**, Tag 02GA]	[**SP**, Tag 02VM]	
G-unramified[12]	[**EGA IV**$_4$, 17.3.1]	[**EGA IV**$_4$, 17.3.3(ii)]	[**EGA IV**$_4$, 17.3.3(iii)]	[**EGA IV**$_4$, 17.7.3(ii)]	[**EGA IV**$_4$, 17.7.8(ii)][11]

Unofficial version for incidental online use

C.2. Varieties

Table 2. Properties of varieties

blah	Definition	Base extension	Descent
connected	[**EGA I**, 2.1.8]	NO	YES
loc. integral	[**EGA I**, 2.1.8]	NO	YES
integral	[**EGA I**, 2.1.8]	NO	YES
irreducible	[**EGA I**, 2.1.8]	NO	YES
reduced	[**EGA I**, **0**:4.1.4]	NO	YES
regular	[**EGA I**, **0**:4.1.4]	NO	[**EGA IV**$_2$, 6.5.2(i)]

Each YES in the "Descent" column denotes the easy fact that if X is a k-variety and $L \supseteq k$ is a field extension such that the L-variety X_L has the property, then X has the property too.

C.3. Algebraic groups

Let *blah* be a property of an algebraic group G over a field k. We can ask the following questions:

Base extension: If G is blah and $L \supseteq k$ is a field extension, must G_L be blah?

Subgroup: If G is blah, must every closed subgroup scheme of G be blah?

Quotient: If G is blah and $H \leq G$ is a closed normal subgroup scheme, must G/H be blah?

Extension: If $1 \to A \to B \to C \to 1$ is an exact sequence of algebraic groups and A and C are blah, must B be blah?

Descent: If $L \supseteq k$ is a field extension and G_L is blah, must G be blah?

Answers are given in Table 3; we omit the answers for "Descent" since they are "YES" for every property listed. If a reference is given, the answer is "YES". In some cases, if the answer is obvious or it follows easily from other entries, we write "YES" or "NO" instead of giving a reference. If you see a superscript (such as ^{4}), please read the corresponding comment below:

1. The answer is "YES" if the extension B is commutative or C is connected. But in general the answer is "NO": if $\operatorname{char} k \neq 2$, then the group G in Exercise 5.1 is an extension of groups of multiplicative type, but G itself is not of multiplicative type.
2. Let $k = \mathbb{F}_p(t)$ and $L = \mathbb{F}_p(t^{1/p})$. If G is the subgroup $x^p - ty^p = 0$ in $\mathbb{G}_a^2$ over k, then G is reduced, but G_L is not.
3. If G is as in comment 2, then $G \times G$ is not reduced.

Unofficial version for incidental online use

4. The conjugation action of PGL_2 on the space M_2 of 2×2 matrices gives an injective homomorphism $\mathrm{PGL}_2 \to \mathrm{GL}_4$ whose image is contained in SL_4 (because PGL_2 is simple).
5. For any $n \geq 2$, the group SL_n is simply connected, but its quotient $\mathrm{PGL}_n \simeq \mathrm{SL}_n / \mu_n$ is not.

The answers are the same for fppf group schemes over a field, and in this setting, one can add a row for "finite type" with all answers being YES.

Unofficial version for incidental online use

Table 3: Properties of algebraic groups

blah	Base extension	Subgroup	Quotient	Extension
abelian variety	YES	YES if geom. int.	YES	YES
adjoint	YES	NO	YES	YES
affine	[**EGA II**, 1.6.2(iii)]	YES	[**SGA** $3_{\mathbf{I}}$, $\mathrm{VI_B}$ 11.7]	Proposition 5.2.7(b)
connected = geom. connected	YES	NO	YES	YES
finite	[**EGA II**, 6.1.5(iii)]	YES	[**SGA** $3_{\mathbf{I}}$, $\mathrm{VI_B}$ 9.2(xii)]	Proposition 5.2.7(b)
(finite) étale = unramified	[**EGA IV**$_4$, 17.3.3(ii)]	YES	[**SGA** $3_{\mathbf{I}}$, $\mathrm{VI_B}$ 9.2(xii)]	Proposition 5.2.7(b)
multiplicative type	YES	[**SGA** $3_{\mathbf{II}}$, IX 8.1]	[**SGA** $3_{\mathbf{II}}$, IX 8.1]	NO[1]
proper	[**EGA II**, 5.4.2(iii)]	YES	YES	Proposition 5.2.7(b)
reduced	NO[2]	NO	[**SGA** $3_{\mathbf{I}}$, $\mathrm{VI_B}$ 9.2(ix)]	NO[3]
reductive	YES	NO	YES	YES
semisimple	YES	NO	YES	YES
solvable	YES	YES	YES	YES
simply connected	YES	NO[4]	NO[5]	
smooth = geom. reduced	[**EGA IV**$_4$, 17.3.3(iii)]	NO	[**SGA** $3_{\mathbf{I}}$, $\mathrm{VI_B}$ 9.2(xii)]	Proposition 5.2.7(b)
torus	YES	YES if geom. int.	YES	YES[1]
unipotent	YES	YES	YES	YES

Unofficial version for incidental online use

Bibliography

[Ahl78] Lars V. Ahlfors, *Complex analysis*: *An introduction to the theory of analytic functions of one complex variable*, 3rd ed., International Series in Pure and Applied Mathematics, McGraw-Hill Book Co., New York, 1978. MR510197 (80c:30001) ↑207

[Ale85] Yismaw Alemu, *On zeros of forms over local fields*, Acta Arith. **45** (1985), no. 2, 163–171. MR797260 (86i:11017) ↑7

[Ami55] S. A. Amitsur, *Generic splitting fields of central simple algebras*, Ann. of Math. (2) **62** (1955), 8–43. MR0070624 (17,9d) ↑109

[Ana73] Sivaramakrishna Anantharaman, *Schémas en groupes, espaces homogènes et espaces algébriques sur une base de dimension 1*, Sur les Groupes Algébriques, Bull. Soc. Math. France Mém, vol. 33, Soc. Math. France, Paris, 1973, pp. 5–79 (French). MR0335524 (49 #305) ↑182

[AK81] G. I. Arkhipov and A. A. Karatsuba, *Local representation of zero by a form*, Izv. Akad. Nauk SSSR Ser. Mat. **45** (1981), no. 5, 948–961, 1198 (Russian). MR637611 (83e:10028) ↑7

[AT67] E. Artin and J. Tate, *Class field theory*, W. A. Benjamin, Inc., New York-Amsterdam, 1967. MR0223335 (36 #6383) ↑26

[Art62] Michael Artin, *Some numerical criteria for contractability of curves on algebraic surfaces*, Amer. J. Math. **84** (1962), 485–496. MR0146182 (26 #3704) ↑270

[Art66] Michael Artin, *On isolated rational singularities of surfaces*, Amer. J. Math. **88** (1966), 129–136. MR0199191 (33 #7340) ↑270

[Art71] M. Artin, *On the joins of Hensel rings*, Advances in Math. **7** (1971), 282–296. MR0289501 (44 #6690) ↑178

[Art74] M. Artin, *Algebraic construction of Brieskorn's resolutions*, J. Algebra **29** (1974), 330–348. MR0354665 ↑88

[Art86a] M. Artin, *Néron models*, Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 213–230. MR861977 ↑143

[Art86b] M. Artin, *Lipman's proof of resolution of singularities for surfaces*, Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 267–287. MR861980 ↑35, 88

[AM72] M. Artin and D. Mumford, *Some elementary examples of unirational varieties which are not rational*, Proc. London Math. Soc. (3) **25** (1972), 75–95. MR0321934 (48 #299) ↑265

Unofficial version for incidental online use

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.–London–Don Mills, Ont., 1969. MR0242802 (39 #4129) ↑75

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 94–115. MR0219512 (36 #2593) ↑v, 22, 29

[AG60] Maurice Auslander and Oscar Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409. MR0121392 (22 #12130) ↑188

[Ax64] James Ax, *Zeroes of polynomials over finite fields*, Amer. J. Math. **86** (1964), 255–261. MR0160775 (28 #3986) ↑6

[Ax65] James Ax, *A field of cohomological dimension* 1 *which is not* C_1, Bull. Amer. Math. Soc. **71** (1965), 717. MR0199177 (33 #7326) ↑24

[AK65] James Ax and Simon Kochen, *Diophantine problems over local fields. I*, Amer. J. Math. **87** (1965), 605–630. MR0184930 (32 #2401) ↑7

[Azu51] Gorô Azumaya, *On maximally central algebras*, Nagoya Math. J. **2** (1951), 119–150. MR0040287 (12,669g) ↑198

[Bau92] Werner Bauer, *On the conjecture of Birch and Swinnerton-Dyer for abelian varieties over function fields in characteristic* $p > 0$, Invent. Math. **108** (1992), no. 2, 263–287, DOI 10.1007/BF02100606. MR1161093 ↑221

[BCTSSD85] Arnaud Beauville, Jean-Louis Colliot-Thélène, Jean-Jacques Sansuc, and Peter Swinnerton-Dyer, *Variétés stablement rationnelles non rationnelles*, Ann. of Math. (2) **121** (1985), no. 2, 283–318, DOI 10.2307/1971174 (French). MR786350 (86m:14009) ↑109, 265

[Ber05] Inta Bertuccioni, *Brauer groups and cohomology*, Arch. Math. (Basel) **84** (2005), no. 5, 406–411. MR2139543 (2005m:14029) ↑192

[BS15] Bhargav Bhatt and Peter Scholze, *The pro-étale topology for schemes*, Astérisque **369** (2015), 99–201 (English, with English and French summaries). MR3379634 ↑212

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108. MR0179168 (31 #3419) ↑146

[BSD75] B. J. Birch and H. P. F. Swinnerton-Dyer, *The Hasse problem for rational surfaces*, J. Reine Angew. Math. **274/275** (1975), 164–174. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III. MR0429913 (55 #2922) ↑253

[Bom73] E. Bombieri, *Canonical models of surfaces of general type*, Inst. Hautes Études Sci. Publ. Math. **42** (1973), 171–219. MR0318163 (47 #6710) ↑259

[Bom90] Enrico Bombieri, *The Mordell conjecture revisited*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **17** (1990), no. 4, 615–640. MR1093712 (92a:11072) ↑286

[BG06] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR2216774 ↑286

[BM76] E. Bombieri and D. Mumford, *Enriques' classification of surfaces in char. p. III*, Invent. Math. **35** (1976), 197–232. MR0491720 (58 #10922b) ↑272

[Bor91] Armand Borel, *Linear algebraic groups*, 2nd ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991. MR1102012 (92d:20001) ↑121

[BP90] Armand Borel and Gopal Prasad, *Addendum to: "Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups" [Inst. Hautes Études Sci. Publ. Math.* ***69*** *(1989), 119–171; MR1019963 (91c:22021)]*, Inst. Hautes Études Sci. Publ. Math. **71** (1990), 173–177. MR1079647 ↑159

[BS64] A. Borel and J.-P. Serre, *Théorèmes de finitude en cohomologie galoisienne*, Comment. Math. Helv. **39** (1964), 111–164 (French). MR0181643 ↑157, 159

Unofficial version for incidental online use

[Bor88] M. V. Borovoĭ, *Galois cohomology of real reductive groups and real forms of simple Lie algebras*, Funktsional. Anal. i Prilozhen. **22** (1988), no. 2, 63–64, DOI 10.1007/BF01077606 (Russian); English transl., Funct. Anal. Appl. **22** (1988), no. 2, 135–136. MR947609 ↑158

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge [Results in Mathematics and Related Areas. 3rd Series.] A Series of Modern Surveys in Mathematics, vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034) ↑64, 67, 69, 71, 73, 74, 75, 76, 79, 82, 84, 89, 97, 100, 101, 103, 110, 111, 112, 139, 143, 144, 149, 151, 183, 296, 297

[Bou12] N. Bourbaki, *Éléments de mathématique. Algèbre. Chapitre 8. Modules et anneaux semi-simples*, Springer, Berlin, 2012 (French). Second revised edition of the 1958 edition [MR0098114]. MR3027127 ↑16

[Bri09] Michel Brion, *Anti-affine algebraic groups*, J. Algebra **321** (2009), no. 3, 934–952, DOI 10.1016/j.jalgebra.2008.09.034. MR2488561 (2009j:14059) ↑149

[BT87] F. Bruhat and J. Tits, *Groupes algébriques sur un corps local. Chapitre III. Compléments et applications à la cohomologie galoisienne*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **34** (1987), no. 3, 671–698 (French). MR927605 (89b:20099) ↑157

[Cam91] F. Campana, *On twistor spaces of the class $\mathscr{C}$*, J. Differential Geom. **33** (1991), no. 2, 541–549. MR1094468 (92g:32059) ↑263

[Cam92] F. Campana, *Connexité rationnelle des variétés de Fano*, Ann. Sci. École Norm. Sup. (4) **25** (1992), no. 5, 539–545 (French). MR1191735 (93k:14050) ↑266

[Cam04] Frédéric Campana, *Orbifolds, special varieties and classification theory*, Ann. Inst. Fourier (Grenoble) **54** (2004), no. 3, 499–630 (English, with English and French summaries). MR2097416 (2006c:14013) ↑51

[Cao17] Yang Cao, *Sous-groupe de Brauer invariant et obstruction de descente itérée*, April 24, 2017. Preprint, `arXiv:1704.05425v2`. ↑248

[Cas67] J. W. S. Cassels, *Global fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 42–84. MR0222054 ↑v, 2

[Cas86] J. W. S. Cassels, *Local fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986. MR861410 (87i:11172) ↑223

[CG66] J. W. S. Cassels and M. J. T. Guy, *On the Hasse principle for cubic surfaces*, Mathematika **13** (1966), 111–120. MR0211966 ↑284

[Čes15] Kęstutis Česnavičius, *Poitou–Tate without restrictions on the order*, Math. Res. Lett. **22** (2015), no. 6, 1621–1666, DOI 10.4310/MRL.2015.v22.n6.a5. MR3507254 ↑228, 229

[Che36] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 73–75. ↑6

[Che54] C. Chevalley, *On algebraic group varieties*, J. Math. Soc. Japan **6** (1954), 303–324. MR0067122 (16,672g) ↑131

[CW30] C. Chevalley and A. Weil, *Un théorème d'arithmétique sur les courbes algébriques*, Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris **195** (1930), 570–572. ↑227

[Chi86] T. Chinburg, *Minimal models for curves over Dedekind rings*, Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 309–326. MR861982 ↑271

[Cho57] Wei-Liang Chow, *On the projective embedding of homogeneous varieties*, Algebraic Geometry and Topology. A Symposium in Honor of S. Lefschetz, Princeton University Press, Princeton, NJ, 1957, pp. 122–128. MR0084851 (18,936c) ↑125

[CG72] C. Herbert Clemens and Phillip A. Griffiths, *The intermediate Jacobian of the cubic threefold*, Ann. of Math. (2) **95** (1972), 281–356. MR0302652 (46 #1796) ↑265

Unofficial version for individual online use

[Col90] Robert F. Coleman, *Manin's proof of the Mordell conjecture over function fields*, Enseign. Math. (2) **36** (1990), no. 3-4, 393–427. MR1096426 ↑288

[CT72] Jean-Louis Colliot-Thélène, *Surfaces de Del Pezzo de degré* 6, C. R. Acad. Sci. Paris Sér. A-B **275** (1972), A109–A111 (French). MR0302653 (46 #1797) ↑281

[CT90] Jean-Louis Colliot-Thélène, *Surfaces rationnelles fibrées en coniques de degré* 4, Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math., vol. 91, Birkhäuser Boston, Boston, MA, 1990, pp. 43–55 (French). MR1104699 ↑235

[CT92] Jean-Louis Colliot-Thélène, *L'arithmétique des variétés rationnelles*, Ann. Fac. Sci. Toulouse Math. (6) **1** (1992), no. 3, 295–336 (French, with English and French summaries). MR1225663 ↑235

[CT98] J.-L. Colliot-Thélène, *The Hasse principle in a pencil of algebraic varieties*, Number Theory (Tiruchirapalli, 1996), Contemp. Math., vol. 210, Amer. Math. Soc., Providence, RI, 1998, pp. 19–39. MR1478483 (98g:11075) ↑235

[CTKS87] Jean-Louis Colliot-Thélène, Dimitri Kanevsky, and Jean-Jacques Sansuc, *Arithmétique des surfaces cubiques diagonales*, Diophantine Approximation and Transcendence Theory (Bonn, 1985), Lecture Notes in Math., vol. 1290, Springer, Berlin, 1987, pp. 1–108, DOI 10.1007/BFb0078705 (French). MR927558 ↑285

[CTM04] Jean-Louis Colliot-Thélène and David A. Madore, *Surfaces de del Pezzo sans point rationnel sur un corps de dimension cohomologique un*, J. Inst. Math. Jussieu **3** (2004), no. 1, 1–16, DOI 10.1017/S1474748004000015 (French, with English and French summaries). MR2036596 ↑278

[CTO89] Jean-Louis Colliot-Thélène and Manuel Ojanguren, *Variétés unirationnelles non rationnelles: au-delà de l'exemple d'Artin et Mumford*, Invent. Math. **97** (1989), no. 1, 141–158, DOI 10.1007/BF01850658 (French). MR999316 (90m:14012) ↑266

[CTPS16] Jean-Louis Colliot-Thélène, Ambrus Pál, and Alexei N. Skorobogatov, *Pathologies of the Brauer–Manin obstruction*, Math. Z. **282** (2016), no. 3-4, 799–817, DOI 10.1007/s00209-015-1565-x. MR3473644 ↑235, 249

[CTS77] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc, *La descente sur une variété rationnelle définie sur un corps de nombres*, C. R. Acad. Sci. Paris Sér. A-B **284** (1977), no. 19, A1215–A1218 (French, with English summary). MR0447250 ↑227, 284

[CTS80] J.-L. Colliot-Thélène and J.-J. Sansuc, *La descente sur les variétés rationnelles*, Journées de Géométrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Angers, 1979, Sijthoff & Noordhoff, Alphen aan den Rijn, 1980, pp. 223–237 (French). MR605344 (82d:14016) ↑227

[CTS87] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc, *La descente sur les variétés rationnelles. II*, Duke Math. J. **54** (1987), no. 2, 375–492, DOI 10.1215/S0012-7094-87-05420-2 (French). MR899402 (89f:11082) ↑227

[CTSSD87a] Jean-Louis Colliot-Thélène, Jean-Jacques Sansuc, and Peter Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces. I*, J. Reine Angew. Math. **373** (1987), 37–107. MR870307 (88m:11045a) ↑235

[CTSSD87b] Jean-Louis Colliot-Thélène, Jean-Jacques Sansuc, and Peter Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces. II*, J. Reine Angew. Math. **374** (1987), 72–168. MR876222 (88m:11045b) ↑235

[CTSD94] Jean-Louis Colliot-Thélène and Peter Swinnerton-Dyer, *Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties*, J. Reine Angew. Math. **453** (1994), 49–112, DOI 10.1515/crll.1994.453.49. MR1285781 ↑235

[CTV12] Jean-Louis Colliot-Thélène and Claire Voisin, *Cohomologie non ramifiée et conjecture de Hodge entière*, Duke Math. J. **161** (2012), no. 5, 735–801, DOI 10.1215/00127094-1548389 (French, with English and French summaries). MR2904092 ↑266

Unofficial version for incidental online use

[Con02] Brian Conrad, *A modern proof of Chevalley's theorem on algebraic groups*, J. Ramanujan Math. Soc. **17** (2002), no. 1, 1–18. MR1906417 (2003f:20078) ↑125

[Con08] Brian Conrad, *Several approaches to non-Archimedean geometry*, p-adic geometry, Univ. Lecture Ser., vol. 45, Amer. Math. Soc., Providence, RI, 2008, pp. 9–63, DOI 10.1090/ulect/045/02. MR2482345 ↑49

[Con12a] Brian Conrad, *Weil and Grothendieck approaches to adelic points*, Enseign. Math. (2) **58** (2012), no. 1-2, 61–97, DOI 10.4171/LEM/58-1-3. MR2985010 ↑49

[Con12b] Brian Conrad, *Finiteness theorems for algebraic groups over function fields*, Compos. Math. **148** (2012), no. 2, 555–639, DOI 10.1112/S0010437X11005665. MR2904198 ↑159

[Con15] Brian Conrad, *Minimal models for elliptic curves*, November 21, 2015. Preprint, available at `http://math.stanford.edu/~conrad/papers/minimalmodel.pdf` . ↑144, 145

[CGP10] Brian Conrad, Ofer Gabber, and Gopal Prasad, *Pseudo-reductive groups*, New Mathematical Monographs, vol. 17, Cambridge University Press, Cambridge, 2010. MR2723571 (2011k:20093) ↑135, 148, 158, 162

[Coo88] Kevin R. Coombes, *Every rational surface is separably split*, Comment. Math. Helv. **63** (1988), no. 2, 305–311, DOI 10.1007/BF02566770. MR948785 (89d:14055) ↑268

[Cor76] D. F. Coray, *Algebraic points on cubic hypersurfaces*, Acta Arith. **30** (1976), no. 3, 267–296. MR0429731 ↑289

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR1628193 (99e:11068) ↑237, 249

[dJ96] A. J. de Jong, *Smoothness, semi-stability and alterations*, Inst. Hautes Études Sci. Publ. Math. **83** (1996), 51–93. MR1423020 (98e:14011) ↑35

[dJ05] A. J. de Jong, *A result of Gabber*, August 9, 2005. Preprint, `http://www.math.columbia.edu/~dejong/papers/2-gabber.pdf` . ↑191

[Del71] Pierre Deligne, *Théorie de Hodge. II*, Inst. Hautes Études Sci. Publ. Math. **40** (1971), 5–57 (French). MR0498551 (58 #16653a) ↑161

[Del74] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307 (French). MR0340258 (49 #5013) ↑210, 215, 217

[Del80] Pierre Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252 (French). MR601520 (83c:14017) ↑217, 223

[DM69] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109. MR0262240 (41 #6850) ↑40

[Dem09] Cyril Demarche, *Obstruction de descente et obstruction de Brauer–Manin étale*, Algebra Number Theory **3** (2009), no. 2, 237–254 (French, with English and French summaries). MR2491944 ↑246, 247

[Dem80] M. Demazure, *Surfaces de Del Pezzo II. — Éclater n points dans* $\mathbb{P}^2$, Séminaire sur les Singularités des Surfaces (Michel Demazure, Henry Charles Pinkham, and Bernard Teissier, eds.), Lecture Notes in Mathematics, vol. 777, Springer, Berlin, 1980. ↑276

[DG70] Michel Demazure and Pierre Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, Éditeur, Paris, 1970 (French). Avec un appendice *Corps de classes local* par Michiel Hazewinkel. MR0302656 (46 #1800) ↑149

[Dem50] V. B. Demyanov, *On cubic forms in discretely normed fields*, Doklady Akad. Nauk SSSR (N.S.) **74** (1950), 889–891 (Russian). MR0037836 (12,315d) ↑7

[Die75] J. Dieudonné, *On the history of the Weil conjectures*, Math. Intelligencer **10** (1975). Reprinted in pp. ix-xviii of E. Freitag and R. Kiehl, *Étale cohomology and the Weil conjectures*, Springer-Verlag, 1988. ↑210

Unofficial version for individual online use

[Dwo60] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. MR0140494 (25 #3914) ↑210

[EHKV01] Dan Edidin, Brendan Hassett, Andrew Kresch, and Angelo Vistoli, *Brauer groups and quotient stacks*, Amer. J. Math. **123** (2001), no. 4, 761–777. MR1844577 (2002f:14002) ↑192

[EGA I] A. Grothendieck, *Éléments de géométrie algébrique. I. Le langage des schémas*, Inst. Hautes Études Sci. Publ. Math. **4** (1960). MR0217083 (36 #177a) ↑55, 84, 90, 302, 303, 304

[EGA II] A. Grothendieck, *Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes*, Inst. Hautes Études Sci. Publ. Math. **8** (1961). MR0217084 (36 #177b) ↑100, 101, 302, 303, 306

[EGA IV_1] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I*, Inst. Hautes Études Sci. Publ. Math. **20** (1964) (French). MR0173675 (30 #3885) ↑55, 56, 57, 65, 302, 303

[EGA IV_2] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II*, Inst. Hautes Études Sci. Publ. Math. **24** (1965) (French). MR0199181 (33 #7330) ↑36, 43, 65, 66, 73, 264, 300, 302, 303, 304

[EGA IV_3] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Inst. Hautes Études Sci. Publ. Math. **28** (1966). MR0217086 (36 #178) ↑42, 46, 57, 59, 80, 302, 303

[EGA IV_4] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math. **32** (1967) (French). MR0238860 (39 #220) ↑74, 82, 83, 90, 301, 302, 303, 306

[Eis95] David Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995. MR1322960 (97a:13001) ↑67, 71

[Eis03] Kirsten Eisenträger, *Hilbert's tenth problem for algebraic function fields of characteristic 2*, Pacific J. Math. **210** (2003), no. 2, 261–281. MR1988534 (2004d:12014) ↑50

[Eke88] Torsten Ekedahl, *Canonical models of surfaces of general type in positive characteristic*, Inst. Hautes Études Sci. Publ. Math. **67** (1988), 97–144. MR972344 (89k:14069) ↑259

[EJ06] Andreas-Stephan Elsenhans and Jörg Jahnel, *The Diophantine equation $x^4 + 2y^4 = z^4 + 4w^4$*, Math. Comp. **75** (2006), no. 254, 935–940 (electronic). MR2197001 (2007e:11143) ↑51

[Enr97] Federigo Enriques, *Sulle irrazionalità da cui può farsi dipendere la risoluzione d'un' equazione algebrica $f(xyz) = 0$ con funzioni razionali di due parametri*, Math. Ann. **49** (1897), no. 1, 1–23, DOI 10.1007/BF01445357 (Italian). MR1510950 ↑283

[Esn03] Hélène Esnault, *Varieties over a finite field with trivial Chow group of 0-cycles have a rational point*, Invent. Math. **151** (2003), no. 1, 187–191, DOI 10.1007/s00222-002-0261-8. MR1943746 (2004e:14015) ↑6, 275

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366 (German). English translation: Finiteness theorems for abelian varieties over number fields, 9–27 in *Arithmetic Geometry (Storrs, Conn., 1984)*, Springer, New York, 1986. Erratum in: Invent. Math. **75** (1984), 381. MR718935 (85g:11026a) ↑50, 286

[Fal91] Gerd Faltings, *Diophantine approximation on abelian varieties*, Ann. of Math. (2) **133** (1991), no. 3, 549–576. MR1109353 (93d:11066) ↑288

[FvL16] Dino Festi and Ronald van Luijk, *Unirationality of del Pezzo surfaces of degree 2 over finite fields*, Bull. Lond. Math. Soc. **48** (2016), no. 1, 135–140, DOI 10.1112/blms/bdv085. MR3455757 ↑278

Unofficial version for individual online use

[Fly00] E. Victor Flynn, *Coverings of curves of genus 2*, Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 65–84. MR1850599 (2002f:11074) ↑236

[FK88] Eberhard Freitag and Reinhardt Kiehl, *Étale cohomology and the Weil conjecture*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge [Results in Mathematics and Related Areas. 3rd Series.] A Series of Modern Surveys in Mathematics, vol. 13, Springer-Verlag, Berlin, 1988. Translated from the German by Betty S. Waterhouse and William C. Waterhouse; With an historical introduction by J. A. Dieudonné. MR926276 (89f:14017) ↑165, 205

[FJ08] Michael D. Fried and Moshe Jarden, *Field arithmetic*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge [Results in Mathematics and Related Areas. 3rd Series.] A Series of Modern Surveys in Mathematics, vol. 11, Springer-Verlag, Berlin, 2008. Revised by Jarden. MR2445111 (2009j:12007) ↑8, 35, 297, 298

[Frö67] A. Fröhlich, *Local fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 1–41. MR0236145 ↑v, 1

[Fuj02] Kazuhiro Fujiwara, *A proof of the absolute purity conjecture (after Gabber)*, Algebraic Geometry 2000, Azumino (Hotaka), Adv. Stud. Pure Math., vol. 36, Math. Soc. Japan, Tokyo, 2002, pp. 153–183. MR1971516 (2004d:14015) ↑197

[Ful98] William Fulton, *Intersection theory*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge [Results in Mathematics and Related Areas. 3rd Series.] A Series of Modern Surveys in Mathematics, vol. 2, Springer-Verlag, Berlin, 1998. MR1644323 (99d:14003) ↑218

[Gab01] O. Gabber, *On space filling curves and Albanese varieties*, Geom. Funct. Anal. **11** (2001), no. 6, 1192–1200. MR1878318 (2003g:14034) ↑222

[Gie77] D. Gieseker, *Global moduli for surfaces of general type*, Invent. Math. **43** (1977), no. 3, 233–282. MR0498596 (58 #16687) ↑273

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR2266528 (2007k:16033) ↑16, 17, 18, 21, 27, 109, 196

[Gra65] Hans Grauert, *Mordells Vermutung über rationale Punkte auf algebraischen Kurven und Funktionenkörper*, Inst. Hautes Études Sci. Publ. Math. **25** (1965), 131–149 (German). MR0222087 (36 #5139) ↑288

[Gre66] Marvin J. Greenberg, *Rational points in Henselian discrete valuation rings*, Inst. Hautes Études Sci. Publ. Math. **31** (1966), 59–64. MR0207700 (34 #7515) ↑7

[Gre69] Marvin J. Greenberg, *Lectures on forms in many variables*, W. A. Benjamin, Inc., New York–Amsterdam, 1969. MR0241358 (39 #2698) ↑3, 7

[Gro62] Alexander Grothendieck, *Fondements de la géométrie algébrique. [Extraits du Séminaire Bourbaki, 1957–1962.]*, Secrétariat mathématique, Paris, 1962 (French). MR0146040 (26 #3566) ↑123

[Gro68a] Alexander Grothendieck, *Formule de Lefschetz et rationalité des fonctions L [see 1608788]*, Dix Exposés sur la Cohomologie des Schémas, Adv. Stud. Pure Math., vol. 3, North-Holland, Amsterdam, 1968, pp. 31–45 (French). MR3202554 ↑217

[Gro68b] Alexander Grothendieck, *Le groupe de Brauer. I. Algèbres d'Azumaya et interprétations diverses*, Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam, 1968, pp. 46–66 (French). MR0244269 (39 #5586a) ↑186, 189, 191

[Gro68c] Alexander Grothendieck, *Le groupe de Brauer. II. Théorie cohomologique*, Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam, 1968, pp. 67–87 (French). MR0244270 (39 #5586b) ↑186, 188, 191

[Gro68d] Alexander Grothendieck, *Le groupe de Brauer. III. Exemples et compléments*, Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam, 1968, pp. 88–188 (French). MR0244271 (39 #5586c) ↑186, 187, 196, 197, 198, 199, 221, 222

Unofficial version for incidental online use

[Gro95a] Alexander Grothendieck, *Technique de descente et théorèmes d'existence en géométrie algébrique. I. Généralités. Descente par morphismes fidèlement plats*, Séminaire Bourbaki, Vol. 5, Exp. No. 190, Soc. Math. France, Paris, 1995, pp. 299–327 (French). MR1603475 ↑97, 100, 101

[Gro95b] Alexander Grothendieck, *Technique de descente et théorèmes d'existence en géométrie algébrique. VI. Les schémas de Picard: propriétés générales*, Séminaire Bourbaki, Vol. 7, Mai 1962, Exp. No. 236, Soc. Math. France, Paris, 1995, pp. 221–243 (French). MR1611207 ↑141, 142

[Har94] David Harari, *Méthode des fibrations et obstruction de Manin*, Duke Math. J. **75** (1994), no. 1, 221–260, DOI 10.1215/S0012-7094-94-07507-8 (French). MR1284820 ↑235

[Har97] David Harari, *Flèches de spécialisations en cohomologie étale et applications arithmétiques*, Bull. Soc. Math. France **125** (1997), no. 2, 143–166 (French, with English and French summaries). MR1478028 ↑235

[Har00] D. Harari, *Weak approximation and non-abelian fundamental groups*, Ann. Sci. École Norm. Sup. (4) **33** (2000), no. 4, 467–484, DOI 10.1016/S0012-9593(00)00118-X (English, with English and French summaries). MR1832820 ↑81

[Har02] David Harari, *Groupes algébriques et points rationnels*, Math. Ann. **322** (2002), no. 4, 811–826 (French, with English and French summaries). MR1905103 (2003e:14038) ↑247

[Har04] David Harari, *Weak approximation on algebraic varieties*, Arithmetic of Higher-Dimensional Algebraic Varieties (Palo Alto, CA, 2002), Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, pp. 43–60. MR2029861 (2004k:11101) ↑52

[HS02] David Harari and Alexei N. Skorobogatov, *Non-abelian cohomology and rational points*, Compositio Math. **130** (2002), no. 3, 241–273. MR1887115 (2003b:11056) ↑227, 249

[Har67] Günter Harder, *Halbeinfache Gruppenschemata über Dedekindringen*, Invent. Math. **4** (1967), 165–191 (German). MR0225785 ↑150

[Har75] G. Harder, *Über die Galoiskohomologie halbeinfacher algebraischer Gruppen. III*, J. Reine Angew. Math. **274/275** (1975), 125–138 (German). Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III. MR0382469 ↑159

[HW16] Yonatan Harpaz and Olivier Wittenberg, *On the fibration method for zero-cycles and rational points*, Ann. of Math. (2) **183** (2016), no. 1, 229–295, DOI 10.4007/annals.2016.183.1.5. MR3432584 ↑235

[HM98] Joe Harris and Ian Morrison, *Moduli of curves*, Graduate Texts in Mathematics, vol. 187, Springer-Verlag, New York, 1998. MR1631825 ↑41

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116) ↑v, vii, 4, 31, 32, 33, 34, 41, 42, 46, 47, 48, 49, 54, 55, 63, 64, 65, 66, 67, 69, 71, 73, 89, 91, 97, 166, 170, 173, 174, 177, 201, 205, 258, 259, 260, 264, 268, 270, 276, 279, 300

[Has24] Helmut Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. **153** (1924), 113–130, DOI 10.1515/crll.1924.153.113 (German). MR1581027 ↑7

[Has09] Brendan Hassett, *Rational surfaces over nonclosed fields*, Arithmetic Geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, RI, 2009, pp. 155–209. MR2498061 ↑283

[HPT16] Brendan Hassett, Alena Pirutka, and Yuri Tschinkel, *Stable rationality of quadric surface bundles over surfaces*, March 30, 2016. Preprint, `arXiv:1603.09262v1`. ↑260

[Hig51] Graham Higman, *A finitely generated infinite simple group*, J. London Math. Soc. **26** (1951), 61–64. MR0038348 (12,390c) ↑78

Unofficial version for incidental online use

[HS00] Marc Hindry and Joseph H. Silverman, *Diophantine geometry: an introduction*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. MR1745599 (2001e:11058) ↑286

[Hir64] Heisuke Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II*, Ann. of Math. (2) 79 (1964), 109–203; ibid. (2) **79** (1964), 205–326. MR0199184 (33 #7333) ↑35

[Igu55] Jun-ichi Igusa, *On some problems in abstract algebraic geometry*, Proc. Nat. Acad. Sci. U. S. A. **41** (1955), 964–967. MR0074085 ↑142

[Iit82] Shigeru Iitaka, *Algebraic geometry: an introduction to birational geometry of algebraic varieties*, Graduate Texts in Mathematics, vol. 76, Springer-Verlag, New York, 1982. MR637060 (84j:14001) ↑257, 258, 259

[Isk71] V. A. Iskovskikh, *A counterexample to the Hasse principle for systems of two quadratic forms in five variables*, Mat. Zametki **10** (1971), 253–257 (Russian). MR0286743 (44 #3952) ↑232

[Isk79] V. A. Iskovskih, *Minimal models of rational surfaces over arbitrary fields*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 1, 19–43, 237 (Russian); English transl., Math. USSR-Izv. **14** (1980), no. 1, 17–39. MR525940 (80m:14021) ↑274

[IM71] V. A. Iskovskih and Ju. I. Manin, *Three-dimensional quartics and counterexamples to the Lüroth problem*, Mat. Sb. (N.S.) **86(128)** (1971), 140–166 (Russian). MR0291172 (45 #266) ↑265

[Jac89] Nathan Jacobson, *Basic algebra. II*, 2nd ed., W. H. Freeman and Company, New York, 1989. MR1009787 (90m:00007) ↑295, 296

[KMT74] Tatsuji Kambayashi, Masayoshi Miyanishi, and Mitsuhiro Takeuchi, *Unipotent algebraic groups*, Lecture Notes in Mathematics, vol. 414, Springer-Verlag, Berlin, 1974. MR0376696 (51 #12871) ↑127

[Kat79] Kazuya Kato, *A generalization of local class field theory by using K-groups. I*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **26** (1979), no. 2, 303–376. MR550688 (81b:12016) ↑295

[Kat80] Kazuya Kato, *A generalization of local class field theory by using K-groups. II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **27** (1980), no. 3, 603–683. MR603953 (83g:12020a) ↑295

[Kat82] Kazuya Kato, *A generalization of local class field theory by using K-groups. III*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **29** (1982), no. 1, 31–43. MR657870 (83g:12020b) ↑295

[KS86] Kazuya Kato and Shuji Saito, *Global class field theory of arithmetic schemes*, Applications of Algebraic K-theory to Algebraic Geometry and Number Theory, Part I, II (Boulder, Colo., 1983), Contemp. Math., vol. 55, Amer. Math. Soc., Providence, RI, 1986, pp. 255–331. MR862639 (88c:11041) ↑295

[KT03] Kazuya Kato and Fabien Trihan, *On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$*, Invent. Math. **153** (2003), no. 3, 537–592, DOI 10.1007/s00222-003-0299-2. MR2000469 (2004h:11058) ↑221, 222

[Kat76] Nicholas M. Katz, *An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields*, Mathematical Developments Arising from Hilbert Problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), Amer. Math. Soc., Providence, RI, 1976, pp. 275–305. MR0424822 (54 #12780) ↑217

[Kat01] Nicholas M. Katz, *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. **7** (2001), no. 1, 29–44. Dedicated to Professor Chao Ko on the occasion of his 90th birthday. MR1803934 (2002d:14028) ↑223

[Kle05] Steven L. Kleiman, *The Picard scheme*, Fundamental Algebraic Geometry, Math. Surveys Monogr., vol. 123, Amer. Math. Soc., Providence, RI, 2005, pp. 235–321. MR2223410 ↑139, 141, 142

Unofficial version for incidental online use

[Kne15] Amanda Knecht, *Degree of unirationality for del Pezzo surfaces over finite fields*, J. Théor. Nombres Bordeaux **27** (2015), no. 1, 171–182 (English, with English and French summaries). MR3346968 ↑278

[Kne65a] Martin Kneser, *Galois-Kohomologie halbeinfacher algebraischer Gruppen über $\mathfrak{p}$-adischen Körpern. I*, Math. Z. **88** (1965), 40–47 (German). MR0174559 (30 #4760) ↑157

[Kne65b] Martin Kneser, *Galois-Kohomologie halbeinfacher algebraischer Gruppen über $\mathfrak{p}$-adischen Körpern. II*, Math. Z. **89** (1965), 250–272 (German). MR0188219 (32 #5658) ↑157

[Kne66] Martin Kneser, *Strong approximation*, Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), Amer. Math. Soc., Providence, RI, 1966, pp. 187–196. MR0213361 ↑150

[Kne67] M. Kneser, *Semi-simple algebraic groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 250–265. MR0217077 (36 #171) ↑132, 146

[Knu83] Finn F. Knudsen, *The projectivity of the moduli space of stable curves. III. The line bundles on $M_{g,n}$, and a proof of the projectivity of $\overline{M}_{g,n}$ in characteristic* 0, Math. Scand. **52** (1983), no. 2, 200–212. MR702954 ↑41

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR754003 (86c:11086) ↑226

[Kol96] János Kollár, *Rational curves on algebraic varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge [Results in Mathematics and Related Areas. 3rd Series.] A Series of Modern Surveys in Mathematics, vol. 32, Springer-Verlag, Berlin, 1996. MR1440180 (98c:14001) ↑259, 261, 262, 263, 266, 275, 283, 284, 285

[Kol02] János Kollár, *Unirationality of cubic hypersurfaces*, J. Inst. Math. Jussieu **1** (2002), no. 3, 467–476, DOI 10.1017/S1474748002000117. MR1956057 ↑278

[Kol07a] János Kollár, *A conjecture of Ax and degenerations of Fano varieties*, Israel J. Math. **162** (2007), 235–251, DOI 10.1007/s11856-007-0097-4. MR2365862 (2008j:14017) ↑8

[Kol07b] János Kollár, *Lectures on resolution of singularities*, Ann. of Math. Stud., vol. 166, Princeton University Press, Princeton, NJ, 2007. MR2289519 (2008f:14026) ↑35

[Kol16] János Kollár, *Severi–Brauer varieties: a geometric treatment*, June 14, 2016. Preprint, `arXiv:1606.04368v1`. ↑106

[KM17] János Kollár and Massimiliano Mella, *Quadratic families of elliptic curves and unirationality of degree 1 conic bundles*, Amer. J. Math. **139** (2017), no. 4, 915–936. ↑278

[KMM92a] János Kollár, Yoichi Miyaoka, and Shigefumi Mori, *Rational connectedness and boundedness of Fano manifolds*, J. Differential Geom. **36** (1992), no. 3, 765–779. MR1189503 (94g:14021) ↑266

[KMM92b] János Kollár, Yoichi Miyaoka, and Shigefumi Mori, *Rationally connected varieties*, J. Algebraic Geom. **1** (1992), no. 3, 429–448. MR1158625 (93i:14014) ↑263, 266

[Koy03] Yoshihiro Koya, *On a duality of Galois cohomology and the strict cohomological dimension of higher local fields*, JP J. Algebra Number Theory Appl. **3** (2003), no. 2, 289–299. MR1999167 (2004g:11107) ↑15

[KT04] Andrew Kresch and Yuri Tschinkel, *On the arithmetic of del Pezzo surfaces of degree 2*, Proc. London Math. Soc. (3) **89** (2004), no. 3, 545–569, DOI 10.1112/S002461150401490X. MR2107007 ↑285

[KT08] Andrew Kresch and Yuri Tschinkel, *Effectivity of Brauer–Manin obstructions*, Adv. Math. **218** (2008), no. 1, 1–27, DOI 10.1016/j.aim.2007.11.017. MR2409407 (2009e:14038) ↑236

Unofficial version for incidental online use

[KT11] Andrew Kresch and Yuri Tschinkel, *Effectivity of Brauer–Manin obstructions on surfaces*, Adv. Math. **226** (2011), no. 5, 4131–4144, DOI 10.1016/j.aim.2010.11.012. MR2770443 (2012e:14047) ↑236

[Lan52] Serge Lang, *On quasi algebraic closure*, Ann. of Math. (2) **55** (1952), 373–390. MR0046388 (13,726d) ↑3, 7

[Lan54] Serge Lang, *Some applications of the local uniformization theorem*, Amer. J. Math. **76** (1954), 362–374. MR0062722 (16,7a) ↑92

[Lan56] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR0086367 (19,174a) ↑156, 162

[Lan74] Serge Lang, *Higher dimensional diophantine problems*, Bull. Amer. Math. Soc. **80** (1974), 779–787. MR0360464 (50 #12914) ↑253

[Lan91] Serge Lang, *Number theory. III*, Encyclopaedia of Mathematical Sciences, vol. 60, Springer-Verlag, Berlin, 1991. Diophantine geometry. MR1112552 (93a:11048) ↑288

[Lan94] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR1282723 (95f:11085) ↑v, 86

[LW54] Serge Lang and André Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827. MR0065218 (16,398d) ↑222, 223

[LMB00] Gérard Laumon and Laurent Moret-Bailly, *Champs algébriques*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge [Results in Mathematics and Related Areas. 3rd Series.] A Series of Modern Surveys in Mathematics, vol. 39, Springer-Verlag, Berlin, 2000 (French). MR1771927 (2001f:14006) ↑39, 182

[Lew52] D. J. Lewis, *Cubic homogeneous polynomials over p-adic number fields*, Ann. of Math. (2) **56** (1952), 473–478. MR0049947 (14,251g) ↑7

[Lia14] Yongqi Liang, *Principe local-global pour les zéro-cycles sur certaines fibrations au-dessus de l'espace projectif*, Bull. Soc. Math. France **142** (2014), no. 2, 269–301 (French, with English and French summaries). MR3269347 ↑235

[Lic68] Stephen Lichtenbaum, *Curves over discrete valuation rings*, Amer. J. Math. **90** (1968), 380–405. MR0230724 (37 #6284) ↑267, 268, 271

[Lip69] Joseph Lipman, *Rational singularities, with applications to algebraic surfaces and unique factorization*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 195–279. MR0276239 (43 #1986) ↑267, 268, 269, 270

[Lip78] Joseph Lipman, *Desingularization of two-dimensional schemes*, Ann. Math. (2) **107** (1978), no. 1, 151–207. MR0491722 (58 #10924) ↑35

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné; Oxford Science Publications. MR1917232 (2003g:14001) ↑46, 47, 48, 144

[LLR05] Qing Liu, Dino Lorenzini, and Michel Raynaud, *On the Brauer group of a surface*, Invent. Math. **159** (2005), no. 3, 673–676. MR2125738 ↑221

[LT16] Qing Liu and Jilong Tong, *Néron models of algebraic curves*, Trans. Amer. Math. Soc. **368** (2016), no. 10, 7019–7043, DOI 10.1090/tran/6642. MR3471084 ↑89

[Luo87] Zhao Hua Luo, *Kodaira dimension of algebraic function fields*, Amer. J. Math. **109** (1987), no. 4, 669–693. MR900035 (88i:14029) ↑258

[Man63] Yu. I. Manin, *Rational points on algebraic curves over function fields*, Izv. Akad. Nauk SSSR Ser. Mat. **27** (1963), 1395–1440 (Russian); English transl., Transl. Amer. Math. Soc., Ser. 2 **50** (1966), no. 2, 189–234. MR0157971 (28 #1199) ↑288

[Man66] Ju. I. Manin, *Rational surfaces over perfect fields*, Inst. Hautes Études Sci. Publ. Math. **30** (1966), 55–113 (Russian, with English summary). MR0225780 ↑283

[Man71] Y. I. Manin, *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, 1971, pp. 401–411. MR0427322 (55 #356) ↑227

Unofficial version for noncommercial online use

[Man86] Yu. I. Manin, *Cubic forms: algebra, geometry, arithmetic*, 2nd ed., North-Holland Mathematical Library, vol. 4, North-Holland Publishing Co., Amsterdam, 1986. Translated from the Russian by M. Hazewinkel. MR833513 (87d:11037) ↑277, 278

[Mar77] G. A. Margulis, *Cobounded subgroups in algebraic groups over local fields*, Funkcional. Anal. i Priložen. **11** (1977), no. 2, 45–57, 95 (Russian). MR0442107 ↑150

[Mat15] Yuya Matsumoto, *Good reduction criterion for K3 surfaces*, Math. Z. **279** (2015), no. 1-2, 241–266, DOI 10.1007/s00209-014-1365-8. MR3299851 ↑87, 88

[Mat80] Hideyuki Matsumura, *Commutative algebra*, 2nd ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980. MR575344 (82i:13003) ↑35, 84

[MM63] Hideyuki Matsumura and Paul Monsky, *On the automorphisms of hypersurfaces*, J. Math. Kyoto Univ. **3** (1963/1964), 347–361. MR29#5819 ↑265

[Maz92] Barry Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45. MR1181085 (93j:14020) ↑51

[MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit Methods in Number Theory: Rational Points and Diophantine Equations, Panoramas et Synthèses, vol. 36, Société Mathématique de France, Paris, 2012, pp. 99–117. ↑238

[Mil72] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190. MR0330174 (48 #8512) ↑111

[Mil75] J. S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), no. 3, 517–533. MR0414558 ↑221

[Mil80] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, NJ, 1980. MR559531 (81j:14002) ↑165, 175, 178, 182, 186, 192, 198, 199, 214

[Mil81] J. S. Milne, *Comparison of the Brauer group with the Tate-Šafarevič group*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 735–743 (1982). MR656050 ↑221

[Mil86a] J. S. Milne, *Abelian varieties*, Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR861974 ↑143

[Mil86b] J. S. Milne, *Jacobian varieties*, Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212. MR861976 ↑139

[Mil13] J. S. Milne, *Class field theory (v4.02)*, March 23, 2013. Available at `http://www.jmilne.org/math/` . ↑v

[Mil63] J. Milnor, *Morse theory*, Ann. of Math. Stud., vol. 51, Princeton University Press, Princeton, NJ, 1963. Based on lecture notes by M. Spivak and R. Wells. MR0163331 (29 #634) ↑252

[Min89] Kh. P. Minchev, *Strong approximation for varieties over an algebraic number field*, Dokl. Akad. Nauk BSSR **33** (1989), no. 1, 5–8, 92 (Russian, with English summary). MR984929 ↑243, 244

[Miw69] Megumu Miwa, *On Mordell's conjecture for the curve over function field with arbitrary constant field*, J. Math. Soc. Japan **21** (1969), 229–233. MR0241423 ↑288

[Moo08] Gregory H. Moore, *The emergence of open sets, closed sets, and limit points in analysis and topology*, Historia Math. **35** (2008), no. 3, 220–241, DOI 10.1016/j.hm.2008.01.001 (English, with English and German summaries). MR2455202 (2010d:01006) ↑167

[Mor22] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Phil. Soc. **21** (1922), 179–192. ↑286

[Mor49] L. J. Mordell, *Rational points on cubic surfaces*, Publ. Math. Debrecen **1** (1949), 1–6. MR0030982 ↑284

Unofficial version for incidental online use

[Mor82] Shigefumi Mori, *Threefolds whose canonical bundles are not numerically effective*, Ann. of Math. (2) **116** (1982), no. 1, 133–176, DOI 10.2307/2007050. MR662120 (84e:14032) ↑267, 269, 271, 272, 274

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970. MR0282985 (44 #219) ↑138, 139

[Mum77] David Mumford, *Stability of projective varieties*, Enseignement Math. (2) **23** (1977), no. 1-2, 39–110. MR0450272 ↑41

[MO15] David Mumford and Tadao Oda, *Algebraic geometry. II*, Texts and Readings in Mathematics, vol. 73, Hindustan Book Agency, New Delhi, 2015. MR3443857 ↑67

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; With a foreword by G. Harder. MR1697859 (2000m:11104) ↑v

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026 ↑15, 196

[Nis55] Hajime Nishimura, *Some remarks on rational points*, Mem. Coll. Sci. Univ. Kyoto. Ser. A. Math. **29** (1955), 189–192. MR0095851 (20 #2349) ↑92

[Nis79] E. A. Nisnevič, *A properness theorem for Galois cohomology over function fields*, Dokl. Akad. Nauk BSSR **23** (1979), no. 12, 1065–1068, 1148 (Russian, with English summary). MR562141 ↑159

[Oes84] Joseph Oesterlé, *Nombres de Tamagawa et groupes unipotents en caractéristique p*, Invent. Math. **78** (1984), no. 1, 13–88, DOI 10.1007/BF01388714 (French). MR762353 ↑159

[Ols16] Martin C. Olsson, *Algebraic spaces and stacks*, American Mathematical Institute Colloquium Publications, vol. 62, Amer. Math. Soc., Providence, 2016. ↑39

[OVV07] D. Orlov, A. Vishik, and V. Voevodsky, *An exact sequence for $K_*^M/2$ with applications to quadratic forms*, Ann. of Math. (2) **165** (2007), no. 1, 1–13. MR2276765 (2008c:19001) ↑24

[Pey02] Emmanuel Peyre, *Points de hauteur bornée et géométrie des variétés (d'après Y. Manin et al.)*, Astérisque **282** (2002), ix, 323–344 (French, with French summary). Séminaire Bourbaki, Vol. 2000/2001, Exp. No. 891. MR1975184 (2004b:11094) ↑51

[Pfi95] Albrecht Pfister, *Quadratic forms with applications to algebraic geometry and topology*, London Mathematical Society Lecture Note Series, vol. 217, Cambridge University Press, Cambridge, 1995. MR1366652 (97c:11046) ↑3, 7

[Phe91] Thanases Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math. **103** (1991), no. 1, 1–8. MR1079837 (92e:11145) ↑50

[Pie12] Marta Pieropan, *On the unirationality of Del Pezzo surfaces over an arbitrary field*, July 5, 2012. Master's thesis, Concordia University and Université Paris-Sud 11. ↑278

[Pla69] V. P. Platonov, *The problem of strong approximation and the Kneser-Tits hypothesis for algebraic groups*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 1211–1219 (Russian). MR0258839 ↑150

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen. MR1278263 (95b:11039) ↑121, 138, 149, 150, 159

Unofficial version for incidental online use

[Poo01] Bjorn Poonen, *The Hasse principle for complete intersections in projective space*, Rational Points on Algebraic Varieties, 2001, pp. 307–311. MR1875178 (2002j:14028) ↑253

[Poo02] Bjorn Poonen, *Computing rational points on curves*, Number Theory for the Millennium, III (Urbana, IL, 2000), 2002, pp. 149–172. MR1956273 (2003k:11105) ↑286

[Poo06] Bjorn Poonen, *Heuristics for the Brauer–Manin obstruction for curves*, Experiment. Math. **15** (2006), no. 4, 415–420. MR2293593 (2008d:11062) ↑236

[Poo08] Bjorn Poonen, *Undecidability in number theory*, Notices Amer. Math. Soc. **55** (2008), no. 3, 344–350. MR2382821 ↑50

[Poo10] Bjorn Poonen, *Insufficiency of the Brauer–Manin obstruction applied to étale covers*, Ann. of Math. (2) **171** (2010), no. 3, 2157–2169, DOI 10.4007/annals.2010.171.2157. MR2680407 (2011g:14061) ↑246, 249

[Poo14] Bjorn Poonen, *Why all rings should have a* 1, April 1, 2014. Preprint, `arXiv:1404.0135v1`. ↑x

[PV04] Bjorn Poonen and José Felipe Voloch, *Random Diophantine equations*, Arithmetic of Higher-Dimensional Algebraic Varieties (Palo Alto, CA, 2002), 2004, pp. 175–184. With appendices by Jean-Louis Colliot-Thélène and Nicholas M. Katz. MR2029869 ↑252, 253, 267

[Pra77] Gopal Prasad, *Strong approximation for semi-simple groups over function fields*, Ann. of Math. (2) **105** (1977), no. 3, 553–572. MR0444571 ↑150

[RV99] Dinakar Ramakrishnan and Robert J. Valenza, *Fourier analysis on number fields*, Graduate Texts in Mathematics, vol. 186, Springer-Verlag, New York, 1999. MR1680912 (2000d:11002) ↑1, 2

[Rap14] Andrei S. Rapinchuk, *Strong approximation for algebraic groups*, Thin Groups and Superstrong Approximation, Math. Sci. Res. Inst. Publ., vol. 61, Cambridge Univ. Press, Cambridge, 2014, pp. 269–298. MR3220894 ↑149

[Ray70a] Michel Raynaud, *Anneaux locaux henséliens*, Lecture Notes in Mathematics, vol. 169, Springer-Verlag, Berlin, 1970 (French). MR0277519 (43 #3252) ↑67, 74, 76, 79, 296, 297

[Ray70b] Michel Raynaud, *Faisceaux amples sur les schémas en groupes et les espaces homogènes*, Lecture Notes in Mathematics, vol. 119, Springer-Verlag, Berlin, 1970 (French). MR0260758 (41 #5381) ↑182

[RY00] Zinovy Reichstein and Boris Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056, DOI 10.4153/CJM-2000-043-5. With an appendix by János Kollár and Endre Szabó. MR1782331 (2001k:14088) ↑96

[Roq64] Peter Roquette, *Isomorphisms of generic splitting fields of simple algebras*, J. Reine Angew. Math. **214/215** (1964), 207–226. MR0166215 (29 #3492) ↑109

[Roq02] Peter Roquette, *The Riemann hypothesis in characteristic p, its origin and development. I. The formation of the zeta-functions of Artin and of F. K. Schmidt*, Mitt. Math. Ges. Hamburg **21** (2002), no. 2, 79–157. Hamburger Beiträge zur Geschichte der Mathematik. MR1973592 (2004i:11136) ↑210

[Roq04] Peter Roquette, *The Riemann hypothesis in characteristic p, its origin and development. II. The first steps by Davenport and Hasse*, Mitt. Math. Ges. Hamburg **23** (2004), no. 2, 5–74. MR2107374 (2006f:11103) ↑210

[Roq06] Peter Roquette, *The Riemann hypothesis in characteristic p, its origin and development. III. The elliptic case*, Mitt. Math. Ges. Hamburg **25** (2006), 103–176. MR2309232 (2008d:11097) ↑210

[Rus70] Peter Russell, *Forms of the affine line and its additive group*, Pacific J. Math. **32** (1970), 527–539. MR0265367 (42 #277) ↑127

Unofficial version for incidental online use

[Sal90] P. Salberger, *Some new Hasse principles for conic bundle surfaces*, Séminaire de Théorie des Nombres, Paris 1987–88, Progr. Math., vol. 81, Birkhäuser Boston, Boston, MA, 1990, pp. 283–305. MR1042775 ↑235

[SS91] P. Salberger and A. N. Skorobogatov, *Weak approximation for surfaces defined by two quadratic forms*, Duke Math. J. **63** (1991), no. 2, 517–536, DOI 10.1215/S0012-7094-91-06322-2. MR1115119 ↑235

[STVA14] Cecília Salgado, Damiano Testa, and Anthony Várilly-Alvarado, *On the unirationality of del Pezzo surfaces of degree 2*, J. Lond. Math. Soc. (2) **90** (2014), no. 1, 121–139, DOI 10.1112/jlms/jdu014. MR3245139 ↑278

[Sal85] David J. Saltman, *The Brauer group and the center of generic matrices*, J. Algebra **97** (1985), no. 1, 53–67, DOI 10.1016/0021-8693(85)90073-0. MR812169 (87a:13005) ↑200

[Sam66] Pierre Samuel, *Compléments à un article de Hans Grauert sur la conjecture de Mordell*, Inst. Hautes Études Sci. Publ. Math. **29** (1966), 55–62 (French). MR0204430 (34 #4272) ↑287, 288

[San81] J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, J. Reine Angew. Math. **327** (1981), 12–80, DOI 10.1515/crll.1981.327.12 (French). MR631309 ↑149, 150

[SW95] Peter Sarnak and Lan Wang, *Some hypersurfaces in* $\mathbf{P}^4$ *and the Hasse-principle*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 3, 319–322 (English, with English and French summaries). MR1346134 (96j:14014) ↑253

[Sch31] Friedrich Karl Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math. Z. **33** (1931), no. 1, 1–32, DOI 10.1007/BF01174341 (German). MR1545199 ↑157

[Sch82] Peter Schneider, *Zur Vermutung von Birch und Swinnerton-Dyer über globalen Funktionenkörpern*, Math. Ann. **260** (1982), no. 4, 495–510, DOI 10.1007/BF01457028 (German). MR670197 ↑221

[Seg43] B. Segre, *A note on arithmetical properties of cubic surfaces*, J. London Math. Soc **18** (1943), 24–31. MR0009471 ↑278

[Seg51] Beniamino Segre, *On the rational solutions of homogeneous cubic equations in four variables*, Math. Notae **11** (1951), 1–68. MR0046064 ↑278

[Seg60] Beniamino Segre, *Variazione continua ed omotopia in geometria algebrica*, Ann. Mat. Pura Appl. (4) **50** (1960), 149–186 (Italian). MR0121698 (22 #12432) ↑265

[Sel53] Ernst S. Selmer, *Sufficient congruence conditions for the existence of rational points on certain cubic surfaces*, Math. Scand. **1** (1953), 113–119. MR0057908 ↑284

[Ser55] Jean-Pierre Serre, *Géométrie algébrique et géométrie analytique*, Ann. Inst. Fourier, Grenoble **6** (1955), 1–42 (French). MR0082175 (18,511a) ↑48, 49, 166

[Ser58] Jean-Pierre Serre, *Sur la topologie des variétés algébriques en caractéristique p*, Symposium internacional de topología algebraica [International symposium on algebraic topology], Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958, pp. 24–53 (French). MR0098097 ↑142

[Ser60] Jean-Pierre Serre, *Morphismes universels et variétés d'Albanese*, Séminaire Claude Chevalley, tome 4, 1958/1959, 1960, pp. Exposé 10 (French). ↑140, 141

[Ser65] Jean-Pierre Serre, *Zeta and L functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 82–92. MR0194396 (33 #2606) ↑207

[Ser67] J.-P. Serre, *Local class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 128–161. MR0220701 ↑25

Unofficial version for internal online use

[Ser73] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973. Translated from the French; Graduate Texts in Mathematics, No. 7. MR0344216 (49 #8956) ↑251

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg. MR554237 (82e:12016) ↑1, 12, 20, 80, 112, 128

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre. MR1757192 (2000m:11049) ↑145, 185, 238, 297

[Ser02] Jean-Pierre Serre, *Galois cohomology*, Corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author. MR1867431 (2002i:12004) ↑12, 14, 15, 24, 27, 105, 157, 158, 162

[SGA 1] Alexander Grothendieck, *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3, Société Mathématique de France, Paris, 2003 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1960–61. [Geometric Algebra Seminar of Bois-Marie 1960-61]; Directed by A. Grothendieck. With two papers by M. Raynaud. Updated and annotated reprint of the 1971 original [Lecture Notes in Math., vol. 224, Springer, Berlin]. MR2017446 (2004g:14017) ↑8, 49, 78, 79, 80, 239, 251, 291

[SGA 3_{I}] Philippe Gille and Patrick Polo (eds.), *Schémas en groupes (SGA 3). Tome I. Propriétés générales des schémas en groupes*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 7, Société Mathématique de France, Paris, 2011 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1962–64. [Algebraic Geometry Seminar of Bois-Marie 1962–64]; A seminar directed by M. Demazure and A. Grothendieck with the collaboration of M. Artin, J.-E. Bertin, P. Gabriel, M. Raynaud and J.-P. Serre; Revised and annotated edition of the 1970 French original. MR2867621 ↑43, 122, 123, 124, 125, 133, 306

[SGA 3_{II}] *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*, Séminaire de Géométrie Algébrique du Bois-Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, vol. 152, Springer-Verlag, Berlin, 1962/1964 (French). MR0274459 (43 #223b) ↑124, 128, 132, 306

[SGA 3_{III}] Philippe Gille and Patrick Polo (eds.), *Schémas en groupes (SGA 3). Tome III. Structure des schémas en groupes réductifs*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 8, Société Mathématique de France, Paris, 2011 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1962–64. [Algebraic Geometry Seminar of Bois-Marie 1962–64]; A seminar directed by M. Demazure and A. Grothendieck with the collaboration of M. Artin, J.-E. Bertin, P. Gabriel, M. Raynaud and J.-P. Serre; Revised and annotated edition of the 1970 French original. MR2867622 ↑134, 135, 198

[SGA 4_{I}] *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos*, Lecture Notes in Mathematics, vol. 269, Springer-Verlag, Berlin, 1972 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4); Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat. MR0354652 (50 #7130) ↑168, 291, 292, 293

[SGA 4_{II}] *Théorie des topos et cohomologie étale des schémas. Tome 2*, Lecture Notes in Mathematics, vol. 270, Springer-Verlag, Berlin, 1972 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4); Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat. MR0354653 (50 #7131) ↑175

[SGA 4_{III}] *Théorie des topos et cohomologie étale des schémas. Tome 3*, Lecture Notes in Mathematics, vol. 305, Springer-Verlag, Berlin, 1973 (French). Séminaire de Géométrie

Unofficial version for individual online use

Algébrique du Bois-Marie 1963–1964 (SGA 4); Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat. MR0354654 (50 #7132) ↑214, 217

[SGA $4\frac{1}{2}$] P. Deligne, *Cohomologie étale*, Lecture Notes in Mathematics, vol. 569, Springer-Verlag, Berlin, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$; Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier. MR0463174 (57 #3132) ↑165, 214, 219, 220

[SGA 5] *Cohomologie l-adique et fonctions L*, Lecture Notes in Mathematics, vol. 589, Springer-Verlag, Berlin-New York, 1977 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1965–1966 (SGA 5); Edité par Luc Illusie. MR0491704 (58 #10907) ↑93, 94

[Sha72] Stephen S. Shatz, *Profinite groups, arithmetic, and geometry*, Ann. of Math. Stud., vol. 67, Princeton University Press, Princeton, NJ, 1972. MR0347778 (50 #279) ↑3, 178, 192

[SB92] N. I. Shepherd-Barron, *The rationality of quintic Del Pezzo surfaces—a short proof*, Bull. London Math. Soc. **24** (1992), no. 3, 249–250, DOI 10.1112/blms/24.3.249. MR1157259 ↑283

[Shl92] Alexandra Shlapentokh, *Hilbert's tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic*, Trans. Amer. Math. Soc. **333** (1992), no. 1, 275–298. MR1091233 (92m:11144) ↑50

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original. MR95m:11054 ↑241

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005) ↑144

[Sim11] Carlos Simpson, *Local systems on proper algebraic V-manifolds*, Pure Appl. Math. Q. **7** (2011), no. 4, Special Issue: In memory of Eckart Viehweg, 1675–1759, DOI 10.4310/PAMQ.2011.v7.n4.a27. MR2918179 ↑78

[Sko93] Alexei N. Skorobogatov, *On a theorem of Enriques-Swinnerton-Dyer*, Ann. Fac. Sci. Toulouse Math. (6) **2** (1993), no. 3, 429–440 (English, with English and French summaries). MR1260765 ↑283

[Sko99] Alexei N. Skorobogatov, *Beyond the Manin obstruction*, Invent. Math. **135** (1999), no. 2, 399–424. MR1666779 (2000c:14022) ↑248

[Sko01] Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001. MR1845760 (2002d:14032) ↑ix, 151, 182, 229, 232, 239, 245, 274

[Sko09] Alexei Skorobogatov, *Descent obstruction is equivalent to étale Brauer–Manin obstruction*, Math. Ann. **344** (2009), no. 3, 501–510. MR2501300 ↑246, 247

[Spr98] T. A. Springer, *Linear algebraic groups*, 2nd ed., Progress in Mathematics, vol. 9, Birkhäuser Boston Inc., Boston, MA, 1998. MR1642713 (99h:20075) ↑121, 127, 129

[SP] The Stacks Project authors, *Stacks Project*, 2015. Available at `http://stacks.math.columbia.edu` . ↑74, 98, 99, 101, 168, 169, 182, 293, 302, 303

[Ste65] Robert Steinberg, *Regular elements of semisimple algebraic groups*, Inst. Hautes Études Sci. Publ. Math. **25** (1965), 49–80. MR0180554 (31 #4788) ↑157

[Sto07] Michael Stoll, *Finite descent obstructions and rational points on curves*, Algebra Number Theory **1** (2007), no. 4, 349–391. MR2368954 (2008i:11086) ↑247

[SD62] H. P. F. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika **9** (1962), 54–56. MR0139989 ↑284

[SD67] H. P. F. Swinnerton-Dyer, *An application of computing to class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 280–291. MR0219514 ↑146

Unofficial version for incidental online use

[SD72] H. P. F. Swinnerton-Dyer, *Rational points on del Pezzo surfaces of degree* 5, Algebraic geometry, Oslo 1970 (Proc. Fifth Nordic Summer School in Math.), Wolters-Noordhoff, Groningen, 1972, pp. 287–290. MR0376684 ↑283

[Sza09] Tamás Szamuely, *Galois groups and fundamental groups*, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, Cambridge, 2009. MR2548205 (2011b:14064) ↑76

[Tam94] Günter Tamme, *Introduction to étale cohomology*, Universitext, Springer-Verlag, Berlin, 1994. Translated from the German by Manfred Kolster. MR1317816 (95k:14033) ↑165

[Tat52] John Tate, *Genus change in inseparable extensions of function fields*, Proc. Amer. Math. Soc. **3** (1952), 400–406. MR0047631 (13,905b) ↑47, 48

[Tat63] John Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295. MR0175892 ↑145

[Tat65] John T. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 93–110. MR0225778 (37 #1371) ↑207

[Tat67] J. T. Tate, *Global class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 162–203. MR0220697 ↑26

[Tat94] John Tate, *Conjectures on algebraic cycles in l-adic cohomology*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 71–83. MR1265523 (95a:14010) ↑207, 220

[Tat95a] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Exp. No. 306, Soc. Math. France, Paris, 1995, pp. 415–440. MR1610977 ↑145, 146, 221

[Tat95b] J. Tate, *WC-groups over $\mathfrak{p}$-adic fields*, Séminaire Bourbaki, Vol. 4, Exp. No. 156, Soc. Math. France, Paris, 1995, pp. 265–277. MR1610926 ↑158

[Ter66] Guy Terjanian, *Un contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris Sér. A-B **262** (1966), A612 (French). MR0197450 (33 #5615) ↑7

[Tol93] Domingo Toledo, *Projective varieties with non-residually finite fundamental group*, Inst. Hautes Études Sci. Publ. Math. **77** (1993), 103–119. MR1249171 ↑78

[Tre91] S. L. Tregub, *Birational equivalence of Brauer-Severi manifolds*, Uspekhi Mat. Nauk **46** (1991), no. 6(282), 217–218 (Russian); English transl., Russian Math. Surveys **46** (1991), no. 6, 229. MR1164209 (93d:14035) ↑109

[VA08] Anthony Várilly-Alvarado, *Weak approximation on del Pezzo surfaces of degree* 1, Adv. Math. **219** (2008), no. 6, 2123–2145, DOI 10.1016/j.aim.2008.08.007. MR2456278 ↑285

[Vid94] Carlos R. Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc. **120** (1994), no. 1, 249–253. MR1159179 (94b:11122) ↑50

[Vis05] Angelo Vistoli, *Grothendieck topologies, fibered categories and descent theory*, Fundamental algebraic geometry, Math. Surveys Monogr., vol. 123, Amer. Math. Soc., Providence, RI, 2005, pp. 1–104. MR2223406 ↑38, 66, 115, 167, 302

[Voj91] Paul Vojta, *Siegel's theorem in the compact case*, Ann. of Math. (2) **133** (1991), no. 3, 509–548. MR1109352 (93d:11065) ↑286

[Vol91] J. F. Voloch, *A Diophantine problem on algebraic curves over function fields of positive characteristic*, Bull. Soc. Math. France **119** (1991), no. 1, 121–126 (English, with French summary). MR1101942 ↑150, 288

[Vol97] José Felipe Voloch, *Diophantine geometry in characteristic p: a survey*, Arithmetic Geometry (Cortona, 1994), Sympos. Math., XXXVII, Cambridge Univ. Press, Cambridge, 1997, pp. 260–278. MR1472501 ↑287

Unofficial version for incidental online use

[Vos65] V. E. Voskresenskiĭ, *On two-dimensional algebraic tori*, Izv. Akad. Nauk SSSR Ser. Mat. **29** (1965), 239–244 (Russian). MR0172881 (30 #3097) ↑159

[Vos67] V. E. Voskresenskiĭ, *On two-dimensional algebraic tori. II*, Izv. Akad. Nauk SSSR Ser. Mat. **31** (1967), 711–716 (Russian). MR0214597 (35 #5446) ↑131

[War36] E. Warning, *Bermerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 73–75. ↑6

[Wat75] William C. Waterhouse, *Basically bounded functors and flat sheaves*, Pacific J. Math. **57** (1975), no. 2, 597–610. MR0396578 ↑173

[Wat79] William C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979. MR547117 (82e:14003) ↑115

[Wei94] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR1269324 (95f:18001) ↑192

[Wei48a] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann & Cie., Paris, 1948 (French). MR0027151 (10,262c) ↑210

[Wei48b] André Weil, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg **8** (1946), Hermann & Cie., Paris, 1948 (French). MR0029522 ↑143

[Wei49] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. MR0029393 (10,592e) ↑209, 210

[Wei56] André Weil, *Abstract versus classical algebraic geometry*, Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, vol. III, Erven P. Noordhoff N.V., Groningen; North-Holland Publishing Co., Amsterdam, 1956, pp. 550–558. MR0092196 ↑275

[Wit08] Olivier Wittenberg, *On Albanese torsors and the elementary obstruction*, Math. Ann. **340** (2008), no. 4, 805–838, DOI 10.1007/s00208-007-0170-7. MR2372739 (2008m:14022) ↑141, 153

[Wit10] Olivier Wittenberg, *La connexité rationnelle en arithmétique*, Variétés rationnellement connexes: aspects géométriques et arithmétiques, Panor. Synthèses, vol. 31, Soc. Math. France, Paris, 2010, pp. 61–114 (French, with English and French summaries). MR2931860 ↑6, 140, 141

Unofficial version for incidental online use

Unofficial version for incidental online use

Index

Unofficial version for individual online use

Unofficial version for individual online use

Unofficial version for incidental online use

Unofficial version for incidental online use

Unofficial version for incidental online use

Unofficial version for internal online use

Unofficial version for internal online use

Unofficial version for incidental online use