Geometry and Arithmetic of Surfaces

Draft, 3rd January 2021

Martin Bright
Damiano Testa
Ronald van Luijk

Contents

1

Introduction

Proper introduction goes here.

Motivation

Why should a number theorist be interested in algebraic geometry? In this course we hope to answer this question, by showing essentially geometric reasons why certain Diophantine equations fail to have solutions. But we will begin by placing the study of Diophantine equations into the context of algebraic geometry, to see how techniques from many different realms of mathematics can be useful in their study.

Suppose that we are interested in studying the integer or rational solutions to a polynomial equation $f \in \mathbf{Z}[X_0, X_1, \ldots, X_n]$. We assume f to be homogeneous, so that the sets of integer and rational solutions coincide: more precisely, any rational solution may be turned into an integer one by clearing denominators. We wish to define a geometric object X as

$$\text{“ } X = \{f = 0\} \subset \mathbf{P}^n \text{ ”}, \tag{1.1}$$

so that X is the zero-set of the polynomial f in projective space. This is, as it stands, not a definition at all. What we really mean is, for example,

$$X(\mathbf{Q}) = \{(X_0 : \cdots : X_n) \in \mathbf{P}^n(\mathbf{Q}) \mid f(X_0, \ldots, X_n) = 0\} \tag{1.2}$$

where $\mathbf{P}^n(\mathbf{Q})$ is the set of $(n+1)$-tuples of rational numbers, modulo multiplying them all through by a common factor. Given that f has integer coefficients, we can take any $(n+1)$-tuple of elements of any ring R and substitute it into f, and so define $X(R)$ in exactly the same way, replacing $\mathbf{Q}$ by R in the definition (1.2) above. In this way we can consider the sets $X(\mathbf{R})$, $X(\mathbf{C})$, $X(\mathbf{F}_p)$ and

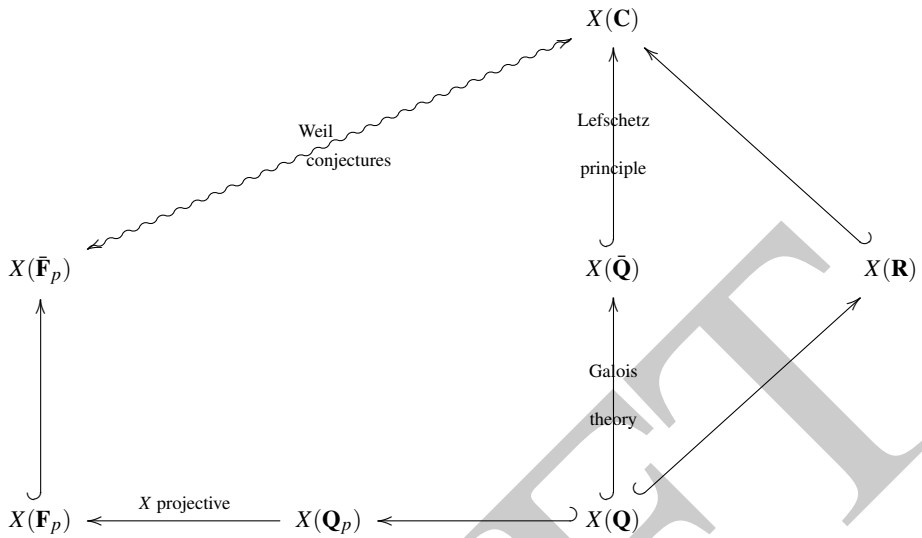


Figure 1.1 Some of the sets of points associated to a Diophantine equation

so on. There are obvious maps between some of these sets: for example, $\mathbf{Q}$ is contained in $\mathbf{R}$ and so $X(\mathbf{Q})$ is contained in $X(\mathbf{R})$.

In Figure 1.1, several of these point sets are shown. The one which really interests us is $X(\mathbf{Q})$, the set of rational solutions to our polynomial equation. Unfortunately, this is also the point set we know least about. The object of studying the algebraic geometry of X is to use techniques available over the various fields other than $\mathbf{Q}$ to deduce facts about $X(\mathbf{Q})$.

- On $X(\mathbf{R})$ we can use real analysis. For example, if X is smooth then $X(\mathbf{R})$ is a real manifold. In particular, it is easy to check whether $X(\mathbf{R})$ is empty – and if $X(\mathbf{R})$ is empty then $X(\mathbf{Q})$ is certainly empty too!
- On $X(\mathbf{C})$ we have all the tools available to study complex analytic varieties. For example, $X(\mathbf{C})$ has cohomology groups which give much information about its geometry, and these come with Hodge decompositions.
- It may not be obvious that much can be said about $X(\bar{\mathbf{Q}})$. However, a general idea known as the *Lefschetz principle* says that any (first-order) algebraic fact which can be proved about $X(\mathbf{C})$, whether or not the proof uses methods outside algebra, also applies to $X(\bar{\mathbf{Q}})$ and indeed to $X(K)$ where K is any algebraically closed field of characteristic zero. In particular, in this course we will use the fact that the Picard groups of X over $\bar{\mathbf{Q}}$ and over $\mathbf{C}$ are the

same, and will often identify them. [No they're not. Néron–Severi groups maybe.]

- Given that X is defined over $\mathbf{Q}$, many objects associated to X over $\bar{\mathbf{Q}}$ come equipped with an action of the Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. In particular, the point set $X(\bar{\mathbf{Q}})$ and the Picard group $\mathrm{Pic}(X_{\bar{\mathbf{Q}}})$ have Galois actions, and we can use Galois theory to deduce results about the corresponding objects over $\mathbf{Q}$.
- In the same way that $X(\mathbf{Q})$ embeds into $X(\mathbf{R})$, it also embeds into $X(\mathbf{Q}_p)$ for any prime p. Again, $X(\mathbf{Q}_p)$ can be studied by analytic methods, and in particular it is straightforward to decide whether $X(\mathbf{Q}_p)$ is empty for any given p.
- Given that X is a projective variety, any point in $X(\mathbf{Q}_p)$ can be represented as $(x_0 : \cdots : x_n)$ where the x_i all lie in $\mathbf{Z}_p$ and are not all divisible by p. This point then has a well-defined reduction modulo p, and so we get a map from $X(\mathbf{Q}_p)$ to $X(\mathbf{F}_p)$. Often, the study of $X(\mathbf{Q}_p)$ actually comes down to the study of $X(\mathbf{F}_p)$, especially when p is a prime of good reduction for X. Varieties over finite fields have many advantages – in particular, they have only finitely many points which can easily be listed!
- Finally, a rather more deep and complicated link exists between the geometry of $X(\bar{\mathbf{F}}_p)$ and that of $X(\mathbf{C})$, given by the Weil conjectures. We will not discuss this link at all in this course, but mention it as a powerful example of the application of algebraic geometry to arithmetic.

Remark 1.0.1. The mapping $R \mapsto X(R)$ is actually a functor from the category of commutative rings to the category of sets. This functor is the *functor of points* of the scheme X defined by (1.1). This way of looking at schemes can be very profitable: see (Eisenbud and Harris, 2000, Chapter VI) for an explanation.

Prerequisites

Cite good references for background material on algebraic geometry. Need to know about varieties over fields which aren't algebraically closed, but we avoid schemes. Occasionally mention sheaves but knowledge of them isn't vital.

Overview

Something about the structure of the course, with reference to the diagram above.

2

The Hasse principle

In this chapter we introduce the notion of "local-global" techniques in the study of Diophantine equations: studying solutions of an equation over a global field k (such as a number field) by looking at the solutions over the various local fields which are the completions of k.

1: Do we want the details of Hensel's Lemma etc. in this chapter, or do we want to have it as more of an introduction and to put the details later?

2.1 Local solubility

In this book we are concerned with studying rational solutions to polynomial equations and, in particular, the question of whether a given set of polynomial equations has any rational solutions at all. If a polynomial equation defined over the rational numbers has no rational solutions, it can sometimes be very easy to prove this, as the following examples demonstrate.

Example 2.1.1. The conic $x^2+y^2+z^2=0 \subset \mathbf{P}^2_{\mathbf{Q}}$ has no rational points, because it has no real points: the only solution to this equation in real numbers is $x=y=z=0$.

Example 2.1.2. The conic $x^2+y^2=3z^2 \subset \mathbf{P}^2_{\mathbf{Q}}$ has no rational points. For suppose that (x,y,z) were a solution. After multiplying them all by an appropriate constant, we could assume that x,y,z were coprime integers. Then x^2,y^2,z^2 would each be congruent to 0 or 1 $\pmod 4$; looking at the equation shows that they would all have to be $0 \pmod 4$, and therefore x,y,z would all be even, contradicting the assumption that they were coprime.

In both of these examples, we have proved that $X(\mathbf{Q})=\emptyset$ by showing that $X(\mathbf{Q}_v)=\emptyset$ for some place v. In the first case it was $v=\infty$, the real place. In the second case we showed that $X(\mathbf{Z}/4\mathbf{Z})$ was empty, but we would like to think of this as showing the non-existence of solutions over $\mathbf{Q}_2$.

For any variety X over a number field k, the condition that X have points over every completion k_v of k is clearly a necessary condition for X to have rational points over k. In order for such a condition to be useful in determining whether a given variety has rational points, we would like to have some procedure for determining when it holds. The first task in this section will be to show that deciding whether X has points in every completion of k can be achieved by a finite procedure.

Throughout this section, k will denote a number field. We begin by looking at a single non-Archimedean completion k_v, where the indispensable tool is Hensel's Lemma. This comes in several guises; we will begin with the one-variable case. Two comprehensive resources for the various versions of Hensel's Lemma are Bourbaki (1998, Chapitre 3, §4) and Greenberg (1969, Chapter 5). We will denote the ring of integers of k_v by $\mathfrak{o}_v$, and let π be a uniformiser in $\mathfrak{o}_v$.

2: Do we want to phrase these in terms of local fields, or is it OK to have them for completions of number fields?

3: Do we prefer stating these using absolute values, valuations or modular arithmetic?

Theorem 2.1.3 (Hensel's Lemma)**.** *Let $f \in \mathfrak{o}_v[X]$ be a polynomial, and suppose that $x_0 \in \mathfrak{o}_v$ satisfies*

$$|f(x_0)|_v < (|f'(x_0)|_v)^2.$$

Then there exists a unique $x \in \mathfrak{o}_v$ satisfying $|x - x_0|_v < |f'(x_0)|_v/|f(x_0)|_v$ and $f(x) = 0$.

Proof See Cassels (1986, Chapter 4, Lemma 3.1). □

Exercise 2.1.4. Show that an element $a \in \mathbf{Z}_2^\times$ is a square if and only if the equation $X^2 - a$ has a solution modulo 8.

A straightforward corollary to the one-variable form of Hensel's Lemma is the following sufficient condition for the existence of a k_v-point on a projective hypersurface. Recall that a vector in $\mathfrak{o}_v^n$ is *primitive* if its entries do not all lie in the maximal ideal of $\mathfrak{o}_v$.

Corollary 2.1.5. *Let $F \in \mathfrak{o}_v[X_0, \ldots, X_n]$ be a homogeneous polynomial in n variables. Suppose that $\mathbf{x_0} \in \mathfrak{o}_v^n \smallsetminus \{\mathbf{0}\}$ is primitive and satisfies*

$$|F(\mathbf{x_0})|_v < (|(\partial F/\partial X_j)(\mathbf{x_0})|_v)^2$$

for some j. Then there exists a non-zero $\mathbf{x} \in \mathfrak{o}_v^n$ satisfying $F(\mathbf{x}) = 0$.

Proof Write $\mathbf{x_0} = (a_0, \ldots, a_n)$, set $X_i = a_i$ for $i \neq j$, and apply Theorem 2.1.3 to the resulting polynomial in one variable X_j. □

For varieties defined by more than one polynomial, we need a more general version of Hensel's Lemma. A reasonably straightforward generalisation of the proof to matrices yields the following theorem.

Theorem 2.1.6. *Let $f_1,\dots,f_r \in \mathfrak{o}_v[x_1,\dots,x_n]$ be polynomials, with $r \le n$, and denote by $\mathbf{J}$ the Jacobian matrix $\partial(f_1,\dots,f_r)/\partial(x_1,\dots,x_n)$. Given $\mathbf{x_0} \in \mathfrak{o}_v^n$, suppose that there is an $r \times r$ submatrix of $\mathbf{J}(\mathbf{x_0})$ of determinant e satisfying*

$$\max_i\{|f_i(\mathbf{x_0})|_v\} < |e^2|.$$

Then there exists $\mathbf{x} \in \mathfrak{o}_v^n$ satisfying $\max_i\{|\mathbf{x}_i - (\mathbf{x_0})_i|_v\} < |e|$ and, for all i, $f_i(\mathbf{x}) = 0$.

Proof See Greenberg (1969, 5.21). □

A version of Theorem 2.1.6 with weaker hypotheses is given by Fisher (1997).

Armed with Hensel's Lemma, we can now show that it is indeed a finite procedure to decide whether a smooth variety has points over k_v. The most straightforward case is when the variety is a complete intersection in affine space.

Proposition 2.1.7. *Let $f_1,\dots,f_r \in \mathfrak{o}_v[x_1,\dots,x_n]$ be polynomials defining a variety $V \subset \mathbf{A}^n_{k_v}$ that is smooth of dimension $n-r$, and such that $f_1,\dots,f_r$ generate the ideal $I(V,k_v)$. Then there is a finite procedure to decide whether there exists $\mathbf{x} \in \mathfrak{o}_v^n$ satisfying $f_i(\mathbf{x}) = 0$ for all i.*

Proof Let π be a uniformiser in $\mathfrak{o}_v$. The algorithm proceeds as follows. Start with $m = 1$, and list all the solutions to $f_1 = \cdots = f_r = 0$ in $(\mathfrak{o}_v/(\pi^m))^n$. If there are none, then the equations are not soluble in $\mathfrak{o}_v$. If there is such a solution that, in addition, satisfies the condition of Theorem 2.1.6, then there exists a solution over $\mathfrak{o}_v$. Otherwise, increase m and repeat.

It remains to show that this procedure terminates. Every solution modulo π^{m+1} is obtained by lifting a solution modulo π^m. If the procedure were not to terminate, then it would instead construct (by lifting to $\mathfrak{o}_v$) an infinite sequence $\mathbf{x_1}, \mathbf{x_2}, \dots \in \mathfrak{o}_v^n$ satisfying, for all m,

(i) $\mathbf{x_{m+1}} \equiv \mathbf{x_m} \pmod{\pi^m}$;
(ii) for all i, $|f_i(\mathbf{x_m})|_v < |\pi|_v^m$;
(iii) for every $r \times r$ submatrix $\mathbf{M}$ of $\mathbf{J}(\mathbf{x_m})$, we have $|\det \mathbf{M}|_v < |\pi|_v^{m/2}$.

These vectors form a Cauchy sequence in $\mathfrak{o}_v^n$, which therefore converges to some $\mathbf{x} \in \mathfrak{o}_v^n$. By continuity, we have $f_1(\mathbf{x}) = \cdots = f_r(\mathbf{x}) = 0$, and the rank of $\mathbf{J}(\mathbf{x})$ is strictly less that r. By the Jacobian criterion, this contradicts the assumption that V is smooth of dimension $n-r$. □

To extend the proof to smooth varieties that are not complete intersections,

we use the fact that a smooth variety admits an affine cover by complete intersections. As we will show, this follows from the Jacobian criterion for smoothness.

Proposition 2.1.8. *Let $X \subset \mathbf{A}^n_{k_v}$ be a smooth affine variety, and let $f_1, \dots, f_r \in \mathfrak{o}_v[x_1, \dots, x_n]$ be generators for the ideal of X. Then there is a finite procedure to determine whether there exists $\mathbf{x} \in \mathfrak{o}_v^n$ satisfying $f_i(\mathbf{x}) = 0$ for all i.*

Proof This proof is closely related to that of Néron (1964, Proposition 20). Let d be the dimension of X. Let $\mathbf{J}$ be the Jacobian matrix $\partial(f_1, \dots, f_r)/\partial(x_1, \dots, x_n)$. For every subset $S \subset [1, r]$ of size $n-d$, we consider the algebraic set V_S defined by the set of polynomials $\mathscr{F}_S = \{f_i : i \in S\}$, and the corresponding Jacobian matrix $\mathbf{J}_S$ obtained by taking the corresponding rows of $\mathbf{J}$. Each V_S contains X, so we have $\dim V_S \geq d$. Every $(n-d) \times (n-d)$ minor of $\mathbf{J}$ is also a minor of one of the $\mathbf{J}_S$; the Jacobian criterion for smoothness then shows that every point of X is also a smooth point of dimension d on some V_S. Let $\mathscr{S}$ denote the set of S occurring in this way.

For $S \in \mathscr{S}$, the fact that X and V_S have a smooth point of dimension d in common means that the variety X is an irreducible component of V_S. Let V'_S be the union of the remaining components. Extend $\mathscr{F}_S$ to a set of generators $\mathscr{F}_S \cup \mathscr{G}_S$ for the ideal $I(V'_S, k_v)$; then, for every point $x \in X \smallsetminus (X \cap V'_S)$, we have $g(x) \neq 0$ for some $g \in \mathscr{G}_S$. Taking the union $\mathscr{G} = \bigcup_{S \in \mathscr{S}} \mathscr{G}_S$, we see that the sets $X \smallsetminus \{g = 0\}$, for $g \in \mathscr{G}$, form a finite affine open cover of X.

We can scale the $g \in \mathscr{G}$ to have coefficients in $\mathfrak{o}_v$. Because at least one $g \in \mathscr{G}$ is non-zero at each point of X, the Nullstellensatz gives

$$(f_1, \dots, f_r, \mathscr{G}) = (1) \subset k_v[x_1, \dots, x_n]. \tag{2.1}$$

Working instead over $\mathfrak{o}_v$, the ideal generated by all these polynomials is not necessarily the unit ideal, but writing 1 in terms of the generators and clearing denominators shows that it must at least contain a constant:

$$\pi^s \in (f_1, \dots, f_r, \mathscr{G}) \subset \mathfrak{o}_v[x_1, \dots, x_n] \quad \text{for some } s \geq 0. \tag{2.2}$$

We deduce the following consequence: if $\mathbf{x} \in \mathfrak{o}_v^n$ is such that $f_i(\mathbf{x}) = 0$ for all $i = 1 \dots, r$, then there exists $g \in \mathscr{G}$ such that $\pi^{s+1} \nmid g(\mathbf{x})$. Indeed, (2.2) gives

$$\sum_{i=1}^{r} a_i f_i + \sum_{g \in \mathscr{G}} b_g g = \pi^s$$

for suitable $a_i, b_g \in \mathfrak{o}_v[x_1, \dots, x_n]$; evaluating at $\mathbf{x}$ shows that the $g(\mathbf{x})$ cannot all be divisible by π^{s+1}.

For any $S \in \mathscr{S}$ and any $g \in \mathscr{G}_S$, the equations

$$f_i(x_1, \dots, x_n) = 0 \quad \text{for all } i \in S; \quad x_{n+1} g(x_1, \dots, x_n) = \pi^s \tag{2.3}$$

in $n+1$ variables define a variety $Y_{S,g} \subset \mathbf{A}^{n+1}_{k_v}$ that is isomorphic to $X \smallsetminus \{g=0\}$, and is therefore a smooth complete intersection of dimension d. Moreover, the solutions over $\mathfrak{o}_v$ to the equations (2.3) are in bijection with the $\mathbf{x} \in \mathfrak{o}_v^n$ satisfying $f_i(\mathbf{x}) = 0$ for all $i = 1, \ldots, r$, and $\pi^{s+1} \nmid g(\mathbf{x})$. So every solution $\mathbf{x}$ to the original equations corresponds to a solution in $\mathfrak{o}_v$ to one of the finitely many sets of equations (2.3); and the existence of such solutions can be decided by Proposition 2.1.7. □

Corollary 2.1.9. *Let $X \subset \mathbf{P}^n_{k_v}$ be a smooth projective variety. Then there is a finite procedure to determine whether $X(k_v)$ is empty.*

Proof We can scale the defining equations for X so that they have coefficients in $\mathfrak{o}_v$. Any k_v-point on X may be scaled to give a primitive $\mathfrak{o}_v$-point, which then corresponds to an $\mathfrak{o}_v$-point on one of the standard affine pieces of X. These may be tested for solubility by Proposition 2.1.8. □

We end this section by giving one of the most useful versions of Hensel's Lemma, which will play an important role in the following section.

Proposition 2.1.10. *Let $X \subset \mathbf{A}^n_{k_v}$ be an affine variety of dimension d, and let $f_1, \ldots, f_r \in \mathfrak{o}_v[x_1, \ldots, x_n]$ be generators for the ideal of X. Denote by $\mathbf{F}$ the residue field of $\mathfrak{o}_v$. Let $\tilde{X} \subset \mathbf{A}^n_{\mathbf{F}}$ be the reduction of X (see Definition 3.6.3) and suppose that the reductions $\tilde{f}_1, \ldots, \tilde{f}_r \in \mathbf{F}[x_1, \ldots, x_n]$ generate the ideal $I(\tilde{X}, \mathbf{F})$. Suppose that $\tilde{\mathbf{x}} \in \tilde{X}(\mathbf{F})$ is a point at which $\tilde{X}$ is smooth of dimension d. Then there exists $\mathbf{x} \in \mathfrak{o}_v^n$ that lies in $X(k_v)$ and lifts $\tilde{\mathbf{x}}$.*

Proof We prove the case $d = n - r$, that is, when X is a complete intersection. This case is a direct application of Theorem 2.1.6. Let $\mathbf{x_0} \in \mathfrak{o}_v^n$ be any lift of $\tilde{\mathbf{x}}$. The assumption that $\tilde{X}$ is smooth of dimension $n-r$ at $\tilde{\mathbf{x}}$ means that there is an $r \times r$ submatrix of the Jacobian matrix $\mathbf{J}(\mathbf{x_0})$ which reduces to an invertible matrix over $\mathbf{F}$, and so has determinant in $\mathfrak{o}_v^\times$. So the theorem applies and gives $\mathbf{x} \in \mathfrak{o}_v^n$ congruent to $\mathbf{x_0}$ modulo v, and satisfying $f_i(\mathbf{x}) = 0$ for all i.

In general, we reduce to the case of a complete intersection; what follows is a sketch of the argument. Let $\mathbf{J}$ be the Jacobian matrix $\partial(f_1, \ldots, f_r)/\partial(x_1, \ldots, x_n)$. The hypotheses show that there is a $(n-d) \times (n-d)$ submatrix of $\mathbf{J}(\tilde{\mathbf{x}})$ having non-zero determinant in $\mathbf{F}$; after renumbering, we may assume that the top-left $(n-d) \times (n-d)$ submatrix has this property. Denote by R the polynomial ring $\mathfrak{o}_v[x_1, \ldots, x_n]$. Let I be the ideal $I(X, k_v) \cap R$, which by assumption is generated by $f_1, \ldots, f_r$, and let $I' \subset I$ be the ideal in R generated by $f_1, \ldots, f_{n-d}$. The kernel of evaluation at the point $\tilde{\mathbf{x}}$ is a maximal ideal of R whose images in R/I and R/I' we will denote $\mathfrak{m}$ and $\mathfrak{m}'$ respectively. Now the Jacobian criterion shows that the local rings $(R/I)_{\mathfrak{m}}$ and $(R/I')_{\mathfrak{m}'}$ are both regular, hence

integral domains, and both of dimension $d+1$. Therefore the quotient map $(R/I')_{\mathfrak{m}'} \to (R/I)_{\mathfrak{m}}$ is an isomorphism, showing that image of the ideal I in the ring $(R/I')_{\mathfrak{m}'}$ is the zero ideal. Since I is finitely generated, it follows that there exists $g \in (R/I') \smallsetminus \mathfrak{m}'$ satisfying $gI = 0$ in R/I'. In geometric terms, we have found $g \in R$ satisfying $g(\tilde{\mathbf{x}}) \neq 0$ and such that the open subset of $Z(\{f_1,\dots,f_{n-d}\},k)$ defined by $g \neq 0$ is an open subset of X. This open subset is isomorphic to the affine complete intersection $Y \subset \mathbf{A}_k^{n+1}$ defined by the equations $f_1(x_1,\dots,x_n) = \cdots = f_{n-d}(x_1,\dots,x_n) = 0$ and $x_{n+1}g(x_1,\dots,x_n) = 1$. Applying the proposition to Y now gives the result. □

To complete this section on testing local solubility, we must also address Archimedean places. Solubility of a variety over the complex numbers $\mathbf{C}$ is determined by the Nullstellensatz: the affine variety defined by a set of polynomials is empty if and only if the polynomials generate the unit ideal. Over $\mathbf{R}$, there is an extensive theory of algorithmic algebraic geometry, and we quote the following result.

Theorem 2.1.11. *Let k be a number field and let $f_1,\dots,f_r \in k[x_1,\dots,x_n]$ be polynomials defining a variety $X \subset \mathbf{A}_k^n$. Let v be a real place of k. There is a finite procedure to determine whether $X(k_v)$ is empty.*

Proof See Basu et al. (2006, Theorem 13.13). □

2.2 Everywhere local solubility

So far we have been studying how to tell whether a variety has points over a single completion k_v of a number field k. However, for the local-global principle to be useful, we would like to be able to tell whether a given variety over k has points in *all* completions of k.

Definition 2.2.1. Let k be a number field. The ring of *adèles* of k is the restricted direct product $\mathbf{A}_k = \prod' k_v$ with respect to the rings of integers of the k_v. This is the subring of the direct product $\prod_v k_v$ consisting of those elements (x_v) such that x_v is an integer at all but finitely many places v. The set of *adelic points* of a variety X over k is the set $X(\mathbf{A}_k)$ of points of X with coordinates in the adèles of k.

Remark 2.2.2. The notation $X(\mathbf{A}_k)$ makes sense: since $\mathbf{A}_k$ is a k-algebra, a polynomial in $k[x_1,\dots,x_n]$ can be evaluated at an n-tuple of elements of $\mathbf{A}_k$, so one can ask for the set of those n-tuples for which the evaluation is zero. It is easy to check that $X(\mathbf{A}_k)$ can be identified with those elements of the direct

product $(P_v) \in \prod_v X(k_v)$ such that P_v has coordinates which are integers in k_v, for all but finitely many places v.

If X is projective, then we have the equality $X(\mathbf{A}_k) = \prod_v X(k_v)$. This is because any point of projective space over k_v can be written with coordinates which are integers in k_v.

Using this notation and assuming that X is projective, we see that $X(\mathbf{A}_k)$ is non-empty precisely when all of the $X(k_v)$ are non-empty, that is, when X is everywhere locally soluble.

The key to showing that checking everywhere local solubility is a finite process is to show that, for almost all places, there is nothing to do. This follows from three important facts: given a smooth variety X over k, its reduction at almost all places is also smooth; a smooth variety over a finite field has points over that field whenever the field is large enough; and smooth points over the residue field lift to points over the completion (Proposition 2.1.10). Let us address the first of these facts.

Lemma 2.2.3. *Let k be a number field with ring of integers $\mathfrak{o}$. Let $X \subset \mathbf{P}^n_k$ be a smooth, projective variety of dimension d and let $f_1, \dots, f_r \in \mathfrak{o}[X_0, \dots, X_n]$ be polynomials generating the ideal $I(X,k)$. Then, for all primes $\mathfrak{p}$ of $\mathfrak{o}$ outside a finite computable set, the variety over $\mathbf{F}_\mathfrak{p} = \mathfrak{o}/\mathfrak{p}$ defined by the reductions of $f_1, \dots, f_r$ modulo $\mathfrak{p}$ is also smooth of dimension d.*

Proof Let X have dimension d, and let $\mathscr{D} \subset \mathfrak{o}[X_0, \dots, X_n]$ be the set of all $(n-d) \times (n-d)$ minors of the Jacobian matrix $\partial(f_1, \dots, f_r)/\partial(X_0, \dots, X_n)$. The assumption that X is smooth implies, by the projective Jacobian criterion, that $f_1, \dots, f_r$ together with all $D \in \mathscr{D}$ have no common zeros. By the Nullstellensatz, this means that the ideal they generate in $k[X_0, \dots, X_n]$ is the whole ring, and so one can compute polynomials $a_1, \dots, a_r$ and $(b_D)_{D \in \mathscr{D}}$, all in $k[X_0, \dots, X_n]$, satisfying

$$a_1 f_1 + \cdots + a_r f_r + \sum_{D \in \mathscr{D}} b_D D = 1.$$

Clearing denominators gives an expression

$$a'_1 f_1 + \cdots + a'_r f_r + \sum_{D \in \mathscr{D}} b'_D D = N \tag{2.4}$$

where $N \in \mathfrak{o}$ is an integer, and $a'_i = N a_i$ and $b'_D = N b_D$ all lie in $\mathfrak{o}[X_0, \dots, X_n]$. Now let $\mathfrak{p}$ be a prime of $\mathfrak{o}$ not dividing N. Reducing (2.4) modulo $\mathfrak{p}$ gives an identity

$$\tilde{a}'_1 \tilde{f}_1 + \cdots + \tilde{a}'_r \tilde{f}_r + \sum_{D \in \mathscr{D}} \tilde{b}'_D \tilde{D} = \tilde{N}$$

where $\tilde{N} \neq 0$ lies in $\mathbf{F}_\mathfrak{p}$. Therefore $\tilde{f}_1, \ldots, \tilde{f}_r$ and $\{\tilde{D} \colon D \in \mathscr{D}\}$ have no common zeros in $\mathbf{P}^n_{\mathbf{F}_\mathfrak{p}}$. Thus the variety $V(\tilde{f}_1, \ldots, \tilde{f}_r) \subset \mathbf{P}^n_{\mathbf{F}_\mathfrak{p}}$, which is known to have dimension d by Lemma 3.6.8, satisfies the projective Jacobian criterion, so is smooth of dimension d. □

The next step is to show that, given a fixed variety X over a number field k, we have $X(k_\mathfrak{p}) \neq \emptyset$ for all sufficiently large primes $\mathfrak{p}$ at which the reduction of X is smooth. Given Proposition 2.1.10, it is sufficient to find a point on the reduction, and so we are led to the question of determining whether a variety over a finite field has any points. An elementary, but often useful, result in this direction is the following.

Theorem 2.2.4 (Chevalley, Warning)**.** *Let* $\mathbf{F}$ *be a finite field of characteristic* p*, and let* $f_1, \ldots, f_r \in \mathbf{F}[x_1, \ldots, x_n]$ *be polynomials. If* $\sum_i \deg f_i < n$*, then*

$$\#\{\mathbf{x} \in \mathbf{F}^n \mid f_1(\mathbf{x}) = \cdots = f_r(\mathbf{x}) = 0\}$$

is divisible by p*. In particular, if the* f_i *are non-constant homogeneous polynomials, then they have a non-trivial common zero.*

Proof See Serre (1973, Chapter I, §2, Theorem 3). □

For more general results, we turn to the study of the number of points of a variety over a finite field, the subject of many deep results in arithmetic geometry. Our first such result is the Hasse–Weil bound for the number of points of a smooth curve over a finite field, proved by Hasse for elliptic curves and by Weil (1948, p. 70, Corollaire 3) for curves of any genus.

Theorem 2.2.5 (Hasse, Weil)**.** *Let* C *be a smooth projective curve of genus* g *over a finite field* $\mathbf{F}$ *of order* q*. Then the number of points of* C *satisfies*

$$|\#C(\mathbf{F}) - (q+1)| \leq 2g\sqrt{q}.$$

Using this result inductively, Lang and Weil (1954) were able to prove a similar statement about higher-dimensional varieties, as follows.

Theorem 2.2.6 (Lang, Weil)**.** *There exists a constant* $A(n,d,r)$ *depending only on* n, d, r *such that, for any finite field* $\mathbf{F}$ *of order* q *and any projective variety* $V \subset \mathbf{P}^n_\mathbf{F}$ *of dimension* r *and degree* d*, we have*

$$|\#V(\mathbf{F}) - q^r| \leq (d-1)(d-2)q^{r-\frac{1}{2}} + A(n,d,r)q^{r-1}.$$

A more sophisticated approach comes from the Weil conjectures, one of the crowning achievements of 20th-century mathematics. What follows is an extremely brief summary of how the proof of the Weil conjectures through étale cohomology can be applied to bound the number of points on a variety

over a finite field. See Milne (1980) or Freitag and Kiehl (1988) for a thorough treatment.

Let X_0 be a smooth, projective, geometrically irreducible variety of dimension d over a finite field $\mathbf{F}$ of q elements. Let ℓ be any prime not dividing q and let $\bar{X}_0$ denote the base change of X_0 to an algebraic closure of $\mathbf{F}$. The ℓ-adic cohomology groups $\mathrm{H}^i(\bar{X}_0, \mathbf{Q}_\ell)$ were defined, using étale cohomology, by Grothendieck and others; they are finite-dimensional vector spaces over $\mathbf{Q}_\ell$, and zero for $i > 2d$. It can be shown that the number of points of $X_0(\mathbf{F})$ is given by the Lefschetz trace formula:

$$\#X_0(\mathbf{F}) = \sum_{i \geq 0} (-1)^i \operatorname{Tr}(F^* \colon \mathrm{H}^i(\bar{X}_0, \mathbf{Q}_\ell) \to \mathrm{H}^i(\bar{X}_0, \mathbf{Q}_\ell)),$$

where $F^* \colon \mathrm{H}^i(\bar{X}_0, \mathbf{Q}_\ell) \to \mathrm{H}^i(\bar{X}_0, \mathbf{Q}_\ell)$ is the endomorphism on $\mathrm{H}^i(\bar{X}_0, \mathbf{Q}_\ell)$ induced by the q-power Frobenius morphism on $\bar{X}_0$. Deligne (1974) proved that the eigenvalues of F^* acting on $\mathrm{H}^i(\bar{X}_0, \mathbf{Q}_\ell)$ are algebraic integers, all of whose conjugates have complex absolute value $q^{i/2}$. Since the trace of an endomorphism is simply the sum of the eigenvalues, this gives bounds on the traces of Frobenius in terms of the dimensions of the groups $\mathrm{H}^i(\bar{X}_0, \mathbf{Q}_\ell)$. That X_0 is geometrically irreducible implies that $\mathrm{H}^{2d}(\bar{X}_0, \mathbf{Q}_\ell)$ and $\mathrm{H}^0(\bar{X}_0, \mathbf{Q}_\ell)$ both have dimension 1, giving

$$|\#X_0(\mathbf{F}) - (q^d + 1)| \leq \sum_{i=1}^{2d-1} q^{i/2} \dim \mathrm{H}^i(\bar{X}_0, \mathbf{Q}_\ell). \tag{2.5}$$

If X_0 is the reduction of some variety X over a number field, then the dimension of $\mathrm{H}^i(\bar{X}_0, \mathbf{Q}_\ell)$ is the same as the dimension of the complex cohomology group $\mathrm{H}^i(X(\mathbf{C}), \mathbf{C})$, that is, the ith Betti number $b_i(X(\mathbf{C}))$. We shall see in Chapter 9 how to compute the Betti numbers of some surfaces, in particular hypersurfaces in $\mathbf{P}^3$.

Putting this all together, we get the following statement.

Proposition 2.2.7. *Let k be a number field, and let $X \subset \mathbf{P}^n_k$ be a smooth, geometrically irreducible variety, given as the zero-set of a finite number of homogeneous polynomials. Suppose that the Betti numbers $b_i(X(\mathbf{C}))$ are known. Then there is a finite procedure to determine whether $X(\mathbf{A}_k)$ is empty.*

Proof If the given polynomials do not already generate the ideal $I(X,k)$, then there is an algorithm to compute new ones that do: see Cox et al. (2015, Section 4.2). Clearing denominators gives a set of generators with integer coefficients. So assume that $f_1, \ldots, f_r \in \mathfrak{o}[X_0, \ldots, X_n]$ generate $I(X,k)$. We further assume that $I(X,k)$ is not the unit ideal, since otherwise $X(\mathbf{A}_k)$ is certainly empty.

Using Lemma 2.2.3, we can find a finite set S of primes of k outside which the variety defined by $f_1, \dots, f_r$ is smooth. The inequality (2.5) gives a bound M such that, for all finite places $\mathfrak{p}$ of k outside S and satisfying $\#(\mathfrak{o}/\mathfrak{p}) > M$, the equations $f_1 = \cdots = f_r = 0$ have a smooth solution in $\mathfrak{o}/\mathfrak{p}$ and so, by Proposition 2.1.10, $X(k_\mathfrak{p})$ is non-empty. At the remaining finite number of finite places, Corollary 2.1.9 shows that checking solubility of X is a finite procedure. Solubility at any complex places is automatic. Solubility at real places can be checked by Theorem 2.1.11. □

2.3 The Hasse principle

We have seen that, for a smooth projective variety X over a number field k, checking whether $X(\mathbf{A}_k)$ is non-empty is a finite process. For some families of varieties, this is enough to determine whether $X(k)$ is non-empty. The most famous example is the following theorem of Hasse and Minkowski, covering the case of quadratic forms.

Theorem 2.3.1 (Hasse, Minkowski)**.** *Let k be a number field, and let $X \subset \mathbf{P}^n_k$ be defined by one quadratic form. If $X(\mathbf{A}_k)$ is non-empty, then $X(k)$ is non-empty.*

Proof See Serre (1973, Chapter 4, §3, Theorem 8). □

Because of this theorem, we say that quadratic forms satisfy the *Hasse principle*. We now define this principle more generally.

Definition 2.3.2. Let X be a variety over a number field k. We say that X *satisfies the Hasse principle* or that the *Hasse principle holds for* X if the implication

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

holds. If this implication does not hold, then we say that X is a *counterexample to the Hasse principle*.

In other words, a variety X is a counterexample to the Hasse principle if X has a point over every completion of k, but no point over k. If X is projective, then X satisfies the Hasse principle if and only if the implication $X(\mathbf{A}_k) \neq \emptyset \Rightarrow X(k) \neq \emptyset$ holds.

It is usually more useful to talk not about whether an individual variety satisfies the Hasse principle, but rather whether a whole family of varieties satisfy the Hasse principle. For example, the Hasse–Minkowski theorem states that all

quadrics satisfy the Hasse principle. In addition to quadrics, some other families of varieties are also known to satisfy the Hasse principle: for example, Severi–Brauer varieties (Châtelet, 1944); del Pezzo surfaces of degree at least 5 (due to various authors; see Várilly-Alvarado, 2013, Theorem 2.1); and varieties that are principal homogeneous spaces under simply connected algebraic groups (Kneser, Harder, Chernousov; see Platonov and Rapinchuk, 1994, Theorem 6.4 and Theorem 6.6).

4: Does this last one need any more adjectives?

Not all varieties satisfy the Hasse principle: here is an example, discovered independently by Lind (1940) and Reichardt (1942).

Example 2.3.3. The curve of genus 1 defined by the equation

$$2Y^2 = X^4 - 17Z^4 \tag{2.6}$$

is a counterexample to the Hasse principle over $\mathbf{Q}$. In other words, this equation has solutions over $\mathbf{Q}_v$ for each place v, but has no rational solution.

Remark 2.3.4. The equation (2.6) is not homogeneous, so does not define a projective variety. There are two ways round this: either give the variable Y weight 2, so that the equation defines a smooth variety in a weighted projective space; or take one affine piece, say by setting Z equal to 1, form the projective closure of this affine curve, and then blow up to resolve the resulting singular point at infinity. The two procedures lead to isomorphic smooth, projective curves (since they have the same function field), of genus 1. To prove nonexistence of rational solutions, none of this matters, since it is immediately clear that any rational solution must have all of X, Y, Z nonzero.

Proof Clearly there are real solutions. There are also solutions in $\mathbf{Q}_p$ for all $p \geq 3$ where the equation (2.6) has smooth reduction modulo p, since the Hasse bound (Theorem 2.2.5) says that any smooth curve of genus 1 over $\mathbf{F}_p$ has at least $p + 1 - 2\sqrt{p} > 0$ points, and any of these lifts by Hensel's Lemma to a point over $\mathbf{Q}_p$. It only remains to check the finitely many primes of bad reduction (which are 2 and 17), and in each case a point is easily found.

We now show that there can be no rational solution to (2.6). If there were, then without loss of generality we could write it as (X, Y, Z) with X, Y, Z integers and X, Z coprime. What primes may divide Y? If $q > 2$ is prime and $q \mid Y$, then reducing modulo q gives $X^4 \equiv 17Z^4 \pmod{q}$ and so 17 is a square modulo q. By quadratic reciprocity, this means that q is a square modulo 17.

Since 2 and -1 are also squares modulo 17, we deduce that Y is a product of squares modulo 17 and thus Y is a square modulo 17. We can therefore write $Y \equiv Y_0^2 \pmod{17}$. Substituting into (2.6), we get $2Y_0^4 \equiv X^4 \pmod{17}$

and hence that 2 is a fourth power modulo 17. But this is not true, and so there can be no rational solution. □

Most of the arguments in this proof are entirely local arguments: they involve making deductions about $X(\mathbf{Q}_v)$ for various places v. But there is one step which is not local, and that is the use of quadratic reciprocity. The theorem of quadratic reciprocity gives a link between behaviour at one prime and behaviour at another prime, and thus shows that the possible locations of our hypothetical rational solution in the various $X(\mathbf{Q}_v)$ are not independent of each other. We will see this technique repeated in the following examples.

Example 2.3.5 (Birch and Swinnerton-Dyer, 1975)**.** The surface X defined by the equations

$$\begin{cases} uv = x^2 - 5y^2 \\ (u+v)(u+2v) = x^2 - 5z^2 \end{cases}$$

in $\mathbf{P}^4_{\mathbf{Q}}$ with coordinates u,v,x,y,z is a counterexample to the Hasse principle.

Proof We begin by showing that X has points everywhere locally. To do this, note that the points $[u:v:x:y:z] = [1:1:1:0:\sqrt{-1}]$, $[10:-10:5:5:\sqrt{5}]$ and $[5:0:0:0:\sqrt{-5}]$ all lie on X, and that, for any place $v \neq 2$, at least one of them is defined over $\mathbf{Q}_v$. As for $\mathbf{Q}_2$, the point $[-25:5:0:5:2\sqrt{-15}]$ lies in $X(\mathbf{Q}_2)$.

To show that X has no rational points, we begin by supposing that there exists a rational solution $[u:v:x:y:z]$, where we may assume that u,v are coprime integers (but the other coordinates need not be integers). Observe also that $(x,y) \neq (0,0)$.

Firstly we look at $X(\mathbf{Q}_5)$. The 5-adic valuations of x^2 and $5y^2$ are different, since one is even and the other is odd. Therefore both x and y are 5-adic integers, since otherwise uv would not be a 5-adic integer. Now suppose that 5 divided uv; then 5 would divide x, and therefore 5 would divide $(u+v)(u+2v)$. But 5 can divide at most one of u,v, so we have a contradiction and deduce that 5 divides neither u nor v. Similarly, 5 divides neither $(u+v)$ nor $(u+2v)$.

Now we use quadratic reciprocity, in the following guise: if an integer n can be written as $n = x^2 - 5y^2$ for rational numbers x and y, then every prime $p \equiv \pm 2 \pmod 5$ divides n to an even power (see Lemma 16.2.7 below). We deduce that uv (and hence u and v individually) are only divisible by such primes to even powers, and therefore that u and v are both congruent to $\pm 1 \pmod 5$. Similarly, both $(u+v)$ and $(u+2v)$ are congruent to $\pm 1 \pmod 5$. But these statements cannot all be true, and we conclude that no rational solution exists. □

The following lemma completes the proof.

Lemma 2.3.6. *Let n be an integer, and suppose that there exist rational numbers x, y satisfying $n = x^2 - 5y^2$. If p is a prime congruent to $\pm 2 \pmod 5$, then $v_p(n)$ is even.*

Proof Let d be a common multiple of the denominators of x and y. Multiplying through by d^2, which does not change the parity of $v_p(n)$ for any prime p, we may assume that x and y are integers. If now e is the highest common factor of x and y, then dividing by e^2 reduces to the case when x and y are coprime. We will show that, if p is a prime satisfying $p \equiv \pm 2 \pmod 5$, then p does not divide n.

Suppose that $p \neq 5$ is an odd prime dividing n. Reducing the equation modulo p gives $x^2 - 5y^2 \equiv 0 \pmod p$. Since x and y are coprime, they are not both divisible by p, and so neither is. We get $5 \equiv (x/y)^2 \pmod p$, so 5 is a quadratic residue modulo p and reciprocity shows $p \equiv \pm 1 \pmod 5$. □

The surface X in Example 2.3.5 is a del Pezzo surface of degree 4. We shall study del Pezzo surfaces in general in Chapter 7.

So far we have used the inclusion of the set of k-rational points of X into the set of adelic points of X to prove the non-existence of k-rational points. In fact, even if X has k-rational points, we may be interested in understanding how accurately the set of rational points of X is approximated by the set of adelic points of X, rather than just deciding whether it is empty. For instance, we can further ask whether X satisfies weak approximation.

Definition 2.3.7. A variety X over a number field k satisfies *weak approximation* if $X(k)$ is dense in $\prod_{v \in \Omega_k} X(k_v)$, with the product topology. Equivalently, given any open subsets $U_v \subset X(k_v)$ for finitely many places v of k, there exists a point in $X(k)$ lying in each U_v under the embedding $X(k) \subset X(k_v)$.

We conclude with one further example which, though not a counterexample to the Hasse principle, is a counterexample to weak approximation.

Example 2.3.8 (Swinnerton-Dyer (1962))**.** The singular cubic surface S defined by the equation

$$T(X^2 + Y^2) = (4Z - 7T)(Z^2 - 2T^2) \tag{2.7}$$

in $\mathbf{P}^3_{\mathbf{Q}}$ with homogeneous coordinates X, Y, Z, T has real locus with two connected components. Rational points of S are dense in one component; the other contains no rational points.

5: Read the original article!

Proof To see the two connected components of the real locus, we look at the affine piece $T \neq 0$, given by the equation

$$x^2 + y^2 = (4z-7)(z^2-2) \tag{2.8}$$

in $\mathbf{A}^3_{\mathbf{Q}}$ with coordinates $x = \frac{X}{T}, y = \frac{Y}{T}, z = \frac{Z}{T}$. This is the surface of revolution about the z-axis of the elliptic curve

$$u^2 = (4z-7)(z^2-2). \tag{2.9}$$

The right-hand side of this equation is positive only for $|z| \leq \sqrt{2}$ and $z \geq 7/4$; these two ranges for z determine the two connected components of the curve, and hence two connected components of the surface (2.8).

Firstly, we will show that rational points are dense in the component $z \geq 7/4$. The point $(x_0, y_0, z_0) = (1,1,2)$ lies in the surface. Consider the circle given by the intersection of the surface with the plane $z = z_0$. This is a plane conic with a rational point, and so has an isomorphism (given by projection away from the rational point) to $\mathbf{P}^1_{\mathbf{Q}}$. On $\mathbf{P}^1_{\mathbf{Q}}$ rational points are dense in the real points; we deduce that the same is true for the circle.

On the other hand, we can produce many more points to which this argument can be applied. The intersection of our surface with the plane $\{x = y\}$ is the elliptic curve $2v^2 = (4z-7)(z^2-2)$, and our point corresponds to the point $(1,2)$ on this curve. That point lies in the same real component as the point at infinity, which is the identity element for the addition law on the elliptic curve. It turns out that our point has infinite order, and so its multiples are dense in that real component of the curve. We thus get a set of points of the affine surface (2.8) with z-coordinates dense in $\{z \geq 7/4\}$, and so a dense set of rational points on that connected component of the surface.

Secondly, we must prove that there are no rational solutions $[X : Y : Z : T]$ with $|Z/T| \leq \sqrt{2}$. We may assume that Z, T are coprime integers and that $T > 0$. Multiplying the original equation (2.7) through by T gives

$$T(7T - 4Z)(2T^2 - Z^2) = (TX)^2 + (TY)^2 \tag{2.10}$$

and, on this component, each of the left-hand terms T, $7T - 4Z$ and $2T^2 - Z^2$ is non-negative.

Quadratic reciprocity again appears in this proof in the guise of a well-known classical fact about quadratic forms: if n is a positive integer which can be written as $n = a^2 + b^2$, with $a, b \in \mathbf{Q}$, then any prime congruent to 3 (mod 4) must divide n to an even power. Applying this to (2.10) shows that, if $p \equiv 3 \pmod 4$, then the power of p dividing the left-hand side must be even. We claim that, in fact, the power of p dividing each of T, $7T - 4Z$ and

$2T^2 - Z^2$ must be even. To prove this, we look at their possible common factors and show that no such p can divide more than one of them.

- Since T and Z are coprime, we have $(T, 7T - 4Z) = (T, 4)$ so the only prime dividing both T and $7T - 4Z$ can be 2.
- $(T, 2T^2 - Z^2) = (T, Z^2) = 1$ so no prime can divide both T and $2T^2 - Z^2$.
- Suppose that $p \equiv 3 \pmod 4$ divides $(7T - 4Z, 2T^2 - Z^2)$. Then p also divides $(7T + 4Z)(7T - 4Z) - 16(2T^2 - Z^2) = 17T^2$ and, since $p \neq 17$, then p must divide T, which we have already seen is impossible.

Therefore none of T, $7T - 4Z$, $2T^2 - Z^2$ is congruent to $3 \pmod 4$. Since Z and T are coprime, if T were even, then Z would have to be odd, and therefore $2T^2 - Z^2 \equiv 3 \pmod 4$; whereas, if T were odd, then T would have to be congruent to $1 \pmod 4$ and therefore $7T - 4Z \equiv 3 \pmod 4$, giving a contradiction in either case. So there can be no rational solutions to (2.10), so none to (2.7) with $T \neq 0$ and $|Z/T| \leq \sqrt{2}$. □

3

Geometrical background

3.1 Affine varieties

6: Should we mention that we are following Hartshorne/Silverman/....

For any field ℓ and any non-negative integer n, we let $\mathbf{A}^n(\ell)$ be the set ℓ^n.

Let k be a field and let n be a non-negative integer; denote by R the polynomial ring $k[x_1,\ldots,x_n]$. Let ℓ be an extension of k. For any element $P = (\xi_1,\ldots,\xi_n) \in \mathbf{A}^n(\ell)$ and any $f \in R$, we define the evaluation $f(P) \in \ell$ by $f(P) = f(\xi_1,\ldots,\xi_n)$. Let $S \subset R$ be a subset; we define the *zero set* $Z(S,\ell) \subset \mathbf{A}^n(\ell)$ to be the set of all common zeros with coordinates in the field ℓ of the polynomials in S:

$$Z(S,\ell) = \{P \in \mathbf{A}^n(\ell) \mid \forall f \in S,\ f(P) = 0\}.$$

Example 3.1.1. Take $k = \mathbf{Q}$ and $\ell = \mathbf{R}$, and suppose that S consists of the single polynomial $x^2 + y^2 - 1 \in \mathbf{Q}[x,y]$. Then $Z(S,\mathbf{R})$ is the unit circle in $\mathbf{R}^2$.

Example 3.1.2. If the set S consists of only the zero polynomial, then we have $Z(S,\ell) = \mathbf{A}^n(\ell)$. Similarly, we have $Z(\{1\},\ell) = \emptyset$.

If $S \subset R$ is a set of polynomials, I the ideal generated by S, and $\sqrt{I}$ the radical of I, then the three sets $Z(S,\ell)$, $Z(I,\ell)$ and $Z(\sqrt{I},\ell)$ coincide. By Hilbert's Basis Theorem (see Atiyah and Macdonald, 1969, Corollary 7.6), the ideal I of R is generated by a finite set S'; the previous sentence implies $Z(S,\ell) = Z(S',\ell)$.

Definition 3.1.3. Let Z be a subset of $\mathbf{A}^n(\ell)$. We say that Z *can be defined over* k if there exists a subset $S \subset R$ such that $Z = Z(S,\ell)$.

Whenever $k \subset k' \subset \ell$ are field extensions and Z is a subset of $\mathbf{A}^n(\ell)$ that can be defined over k, then Z can also be defined over k'.

Lemma 3.1.4. *Let J be an index set, and let $(I_j)_{j\in J}$ be a collection of ideals*

of R. Then we have

$$Z\Big(\sum_{j\in J} I_j, \ell\Big) = \bigcap_{j\in J} Z(I_j, \ell)$$

and, if J is finite,

$$Z\Big(\prod_{j\in J} I_j, \ell\Big) = \bigcup_{j\in J} Z(I_j, \ell).$$

Proof See Exercise 3.1. □

Proposition 3.1.5. *There is a topology on* $\mathbf{A}^n(\ell)$ *of which the closed sets are exactly the sets* $Z \subset \mathbf{A}^n(\ell)$ *that can be defined over k.*

Proof This follows from Example 3.1.2 and Lemma 3.1.4. □

Definition 3.1.6. The *k-Zariski topology* on $\mathbf{A}^n(\ell)$ is the topology of Proposition 3.1.5.

Lemma 3.1.7. (i) *Let* $k \subset k' \subset \ell$ *be field extensions. The* k'*-Zariski topology on* $\mathbf{A}^n(\ell)$ *is a refinement of the k-Zariski topology on* $\mathbf{A}^n(\ell)$.

(ii) *Let* $k \subset \ell \subset \ell'$ *be field extensions. The k-Zariski topology on* $\mathbf{A}^n(\ell)$ *is the restriction of the k-Zariski topology on* $\mathbf{A}^n(\ell')$.

Proof See Exercise 3.2. □

Let $\bar{k}$ denote a fixed algebraic closure of the field k, and let $G_k = \mathrm{Aut}(\bar{k}/k)$ be the group of field automorphisms of $\bar{k}$ that restrict to the identity on k.

Definition 3.1.8. An *affine algebraic set V over k* is a subset of $\mathbf{A}^n(\bar{k})$, for some n, that can be defined over k, together with the field k itself. We call the field k the *base field* of V. The *Zariski topology* on V is the topology induced by the k-Zariski topology on $\mathbf{A}^n(\bar{k})$. A *quasi-affine algebraic set over k* is an open subset of an affine algebraic set over k, together with the field k as base field, and with the induced topology.

Remark 3.1.9. (i) In cases where we need to make a distinction between an affine algebraic set V over k and its underlying set of points in $\mathbf{A}^n(\bar{k})$, we will refer to the latter as $V(\bar{k})$.

(ii) Note that G_k acts on $V(\bar{k})$ (see Remark 3.5.4).

(iii) By Lemma 3.1.4, the intersections and the finite unions of affine algebraic sets over k are again affine algebraic sets over k.

Definition 3.1.10. Let n be a non-negative integer. *Affine n-space* $\mathbf{A}^n_k$ *over k* is the set $\mathbf{A}^n(\bar{k})$, with k as the base field.

7: we actually have an n already from the very beginning...

d: Should this be a topological space instead? Same comment for projective space.

8: Should we then also redefine algebraic sets to be topological spaces?

Definition 3.1.11. For any subset $S \subset R$, we denote by $V_k(S)$ the affine algebraic set over k with underlying set of points $Z(S,\bar{k})$. If $f_1,\dots,f_r \in R$ are polynomials, then $V_k(f_1,\dots,f_r)$ means $V_k(\{f_1,\dots,f_r\})$.

Recall that a topological space is called *irreducible* if it is nonempty and cannot be expressed as the union of two proper closed subsets. Irreducible topological spaces have the property that every nonempty open subset is dense and irreducible.

9: I guess nonemptiness follows...

Definition 3.1.12. A subset Z of $\mathbf{A}^n(\ell)$ is *irreducible over k* if Z is irreducible in the k-Zariski topology.

Definition 3.1.13. An *affine variety over k* is an affine algebraic set over k that is irreducible over k. A *quasi-affine variety over k* is a quasi-affine algebraic set over k that is irreducible over k.

10: Some people (Gille–Szamuely) require geometrically reduced. We don't.

To any subset Z of $\mathbf{A}^n(\ell)$ we associate the set $I(Z,k)$ of polynomials in R vanishing on Z:

$$I(Z,k) = \{f \in R \mid \forall P \in Z,\ f(P) = 0\}.$$

The set $I(Z,k)$ is an ideal in R, and in fact a radical ideal. If V is an affine algebraic set over k, then we write $I(V) = I(V(\bar{k}),k)$.

Example 3.1.14. If Z is the unit circle in $\mathbf{R}^2$, we obtain $I(Z,\mathbf{Q}) = (x^2+y^2-1) \subset \mathbf{Q}[x,y]$. In this case, the ideal $I(Z,\mathbf{R})$ of $\mathbf{R}[x,y]$ is generated by the ideal $I(Z,\mathbf{Q})$. This need not be the case in general: for example, let Z be the subset $\{\sqrt{12}\} \subset \mathbf{A}^1(\mathbf{R})$. Then $I(Z,\mathbf{R})$ is the ideal of $\mathbf{R}[x]$ generated by $x-\sqrt{12}$, but $I(Z,\mathbf{Q})$ is generated by x^2-12. More extremely, the ideal $I(\{\pi\},\mathbf{R})$ in $\mathbf{R}[x]$ is generated by the polynomial $x-\pi$, while $I(\{\pi\},\mathbf{Q})$ is the zero ideal in $\mathbf{Q}[x]$, because π is transcendental.

Remark 3.1.15. Let k' be a subfield of ℓ containing k and set $R' = k'[x_1,\dots,x_n]$. Let Z be a subset of $\mathbf{A}^n(\ell)$. Then the ideals $I(Z,k)$ and $I(Z,k')$ of R and R', respectively, satisfy

$$I(Z,k) = I(Z,k') \cap R.$$

Lemma 3.1.16. *Let ℓ be a field extension of the field k and let n be a non-negative integer. Let S,T be subsets of R and let Z,W be subsets of $\mathbf{A}^n(\ell)$. Let $\overline{Z} \subset \mathbf{A}^n(\ell)$ be the closure of Z in the k-Zariski topology. The operations $Z(\,\cdot\,,\ell)$ and $I(\,\cdot\,,k)$ satisfy the following properties:*

11: n already exists, and is determined by R.

12: Also useful (for algebraic statistics): for $Z \subset \mathbf{A}^n(k)$, the k-closure of Z in $\mathbf{A}^n(k)$ is the intersection of $\mathbf{A}^n(k)$ with the k-closure of Z in $\mathbf{A}^n(\ell)$, and this last set is also the ℓ-closure of Z in $\mathbf{A}^n(\ell)$. Stronger: ideal over ℓ is generated by ideal over k. Similar statement for sets that start off being defined over k, or does that already follow from what's here?

(i) *if $S \subset T$, then $Z(S,\ell) \supset Z(T,\ell)$;*
(ii) *if $Z \subset W$, then $I(Z,k) \supset I(W,k)$;*

(iii) $I(Z \cup W, k) = I(Z,k) \cap I(W,k)$;
(iv) $\overline{Z} = Z(I(Z,k),\ell)$;
(v) $\sqrt{(S)} \subset I(Z(S,\ell),k)$;
(vi) $Z(S,\ell) = Z(I(Z(S,\ell),k),\ell)$;
(vii) $I(Z,k) = I(Z(I(Z,k),\ell),k)$.

Proof See Exercise 3.3. □

Using Lemma 3.1.16(iv), we can reinterpret Example 3.1.14 to show that the $\mathbf{Q}$-Zariski closure of $\{\sqrt{12}\} \subset \mathbf{A}^1(\mathbf{R})$ is $\{\pm\sqrt{12}\}$, and that the $\mathbf{Q}$-Zariski closure of $\{\pi\} \subset \mathbf{A}^1(\mathbf{R})$ is the whole of $\mathbf{A}^1(\mathbf{R})$.

The inclusion of Lemma 3.1.16(v) may be strict: if S consists of the single polynomial $x^2+y^2+1 \in \mathbf{Q}[x,y]$, then we have $\sqrt{(S)} = (S)$, while $Z(S,\mathbf{R})$ is empty and so $I(Z(I,\mathbf{R}),\mathbf{Q})$ is the whole of $\mathbf{Q}[x,y]$. However, over an algebraically closed field, the zero set of an ideal does determine the ideal itself, at least up to taking the radical. A precise statement is given by Hilbert's Nullstellensatz.

Theorem 3.1.17 (Hilbert's Nullstellensatz)**.** *Let Ω be an algebraically closed field, let n be a non-negative integer, and let $I \subset \Omega[x_1,\ldots,x_n]$ be an ideal. Then the ideal $I(Z(I,\Omega),\Omega)$ is the radical of I.*

Proof See Atiyah and Macdonald (1969, p. 85, Exercise 14). □

Corollary 3.1.18. *Suppose that ℓ is an algebraically closed field containing the field k. Let I be an ideal in $k[x_1,\ldots,x_n]$. Then $I(Z(I,\ell),k)$ is the radical of I.*

Proof Write $R = k[x_1,\ldots,x_n]$ and $R_\ell = \ell[x_1,\ldots,x_n]$. Denote by I_ℓ the ideal in R_ℓ generated by I. We have $Z(I,\ell) = Z(I_\ell,\ell)$, and so the Nullstellensatz gives $I(Z(I,\ell),\ell) = \sqrt{I_\ell}$. We obtain

13: *R* already exists! Or shouldn't it??

$$I(Z(I,\ell),k) = I(Z(I,\ell),\ell) \cap R = \sqrt{I_\ell} \cap R.$$

To finish the proof, it suffices to show that the ideal $\sqrt{I_\ell} \cap R$ is the radical of I. Clearly, there is an inclusion $\sqrt{I} \subset \sqrt{I_\ell} \cap R$. Let g be an element of the ideal $\sqrt{I_\ell} \cap R$, and let r be a positive integer such that g^r lies in I_ℓ; we will show that g^r lies in I. Write $g^r = \sum_{i=i}^{s} h_i f_i$ where $h_1,\ldots,h_s$ are in R_ℓ and $f_1,\ldots,f_s$ are in I. Choose a basis $(\alpha_1,\ldots,\alpha_t)$ for a k-vector space W containing the coefficients of the polynomials $h_1,\ldots,h_s$ where, without loss of generality, we assume $\alpha_1 = 1$. The set of all polynomials in R_ℓ having coefficients in W is a free R-module, isomorphic to $R \otimes_k W$, with $(\alpha_1,\ldots,\alpha_t)$ as a basis. Write each

polynomial $h_1,\dots,h_s$ in the form $h_i = \sum_{j=1}^{t} h_{ij}\alpha_j$ where h_{ij} is in R. Thus the equality

$$g^r\alpha_1 = g^r = \sum_{i=1}^{s} h_i f_i = \sum_{i=1}^{s}\sum_{j=1}^{t} h_{ij} f_i \alpha_j = \sum_j \sum_i h_{ij} f_i \alpha_j$$

holds, and comparing the coefficient of α_1 with respect to the basis $(\alpha_1,\dots,\alpha_t)$ shows that g^r equals $\sum_i h_{i1} f_i \in I$, completing the proof. □

Corollary 3.1.19. *Let n be a non-negative integer. The operations $Z(\,\cdot\,,\bar{k})$ and $I(\,\cdot\,,k)$ determine an inclusion-reversing bijection between affine algebraic sets over k in $\mathbf{A}^n_k$ and radical ideals in $k[x_1,\dots,x_n]$. Under this bijection, the affine algebraic varieties correspond to the prime ideals.*

Proof Corollary 3.1.18 to the Nullstellensatz immediately shows that the two operations are mutually inverse. The last statement is Exercise **??**. □

14: Add exercise?

Example 3.1.20. Affine n-space $\mathbf{A}^n_k$ over k is irreducible, as it corresponds to the zero ideal, which is prime.

Example 3.1.21. Let f be an irreducible polynomial in $k[x_1,\dots,x_n]$. The affine algebraic set $V_k(f)$ is irreducible. See Exercise 3.4.

Definition 3.1.22. Let V be an affine algebraic set over k. For any field extension ℓ of k, the set of *ℓ-points* of V is $V(\ell) = Z(I(V),\ell)$. For affine algebraic sets $W \subset V$ over k and $U = V \smallsetminus W$, we set $U(\ell) = V(\ell) \smallsetminus W(\ell)$.

15: Do we want/need to define the Zariski topology on $V(\ell)$?

By Lemma 3.1.16(vi), the notation introduced in this definition is consistent with the previous usage $V(\bar{k})$.

16: slightly confusing, as you have to apply Corollary 3.1.18 with $\ell = \bar{k}$. If $V = Z(I,\bar{k})$, then the k-closure of V in $\mathbf{A}^n_k$ is $Z(I(V,k),\ell) = Z(\sqrt{I},\ell) = V(\ell)$

Remark 3.1.23. Let V be an affine algebraic set over k. A consequence of Corollary 3.1.18 is that the set $V(\bar{k})$ of $\bar{k}$-points of V is k-Zariski dense in the set $V(\ell)$ of ℓ-points, whenever ℓ contains $\bar{k}$. For example, the $\bar{\mathbf{Q}}$-points of any affine algebraic set are $\mathbf{Q}$-Zariski dense in the complex points.

Definition 3.1.24. Let $V \subset \mathbf{A}^n_k$ be an affine algebraic set over k. The *coordinate ring* of V is the quotient ring $A(V) = k[x_1,\dots,x_n]/I(V)$.

Remark 3.1.25. An affine algebraic set V over k is irreducible if and only if $A(V)$ is an integral domain.

Remark 3.1.26. Consider the elements of $k[x_1,\dots,x_n]$ as functions from $\mathbf{A}^n(\bar{k})$ to $\bar{k}$. Restricting these functions to $V(\bar{k})$ gives a ring homomorphism φ from $k[x_1,\dots,x_n]$ to the ring of functions from $V(\bar{k})$ to $\bar{k}$. By definition, $I(V)$ is the kernel of φ; so $A(V)$ may be identified with the image of φ.

Let $V \subset \mathbf{A}_k^n$ be an affine algebraic set. By Corollary 3.1.19, the closed subsets of V correspond with the radical ideals of $k[x_1,\dots,x_n]$ that contain $I(V,k)$, that is, with the radical ideals of the coordinate ring $A(V)$. For any ideal $J \subset A(V)$, its pull back $\tilde{J} \subset k[x_1,\dots,x_n]$, and any field extension ℓ of k, we also write $Z(J,\ell)$ for $Z(\tilde{J},\ell)$. If a subset $S \subset A(V)$ generates J, then any set $\tilde{S} \subset k[x_1,\dots,x_n]$ of lifts of S, together with $I(V,k)$, generates $\tilde{J}$, so we have

$$Z(J,\ell) = V \cap Z(\tilde{S},\ell) = \{P \in V(\ell) : \forall f \in S, f(P) = 0\}.$$

We also write $Z(S,\ell)$ for this. For any element $f \in A(V)$, we define the quasi-affine algebraic set $D(f) = V - Z(f,\bar{k})$ over k.

Proposition 3.1.27. *Let V be an affine algebraic set over k. The collection $\{D(f) : f \in A(V)\}$ of open subsets is a basis of the k-Zariski topology on V.*

17: Do we want/need this more generally for $V(\ell)$ for any extension ℓ of k?

Proof Let $U \subset V$ be an open subset and $P \in U(\bar{k})$ a point. Set $Z = V - U$. Then there is an element $\tilde{g} \in I(Z,k)$ with $\tilde{g}(P) \neq 0$. Let g denote its image in $A(V)$. Then we have $Z \subset Z(g,\bar{k}) \not\ni P$, so $D(g)$ is an open neighbourhood of P in U. □

Definition 3.1.28. Let X be a topological space. A *minimal closed subset* of X is a non-empty closed subset $Z \subset X$ that is minimal among all non-empty closed subsets of X.

Note that minimal closed subsets are irreducible.

Remark 3.1.29. Let V be an affine algebraic set over k. The bijection of Corollary 3.1.19, composed with the quotient map $k[x_1,\dots,x_n] \to A(V)$, induces an inclusion-reversing bijection between the closed subsets of V and the radical ideals of $A(V)$. The irreducible closed subsets correspond to prime ideals. The minimal closed subsets correspond to the maximal ideals of $A(V)$.

Example 3.1.30. The points of $\mathbf{A}_k^n(k)$ are minimal closed subsets of $\mathbf{A}_k^n$: the point $(\xi_1,\dots,\xi_n)$ equals $V_k(x_1-\xi_1,\dots,x_n-\xi_n)$. However, a minimal closed subset need not consist of a single point. For example, the algebraic set $V_{\mathbf{Q}}(x^2-12) = \{\pm\sqrt{12}\} \subset \mathbf{A}_{\mathbf{Q}}^1(\bar{\mathbf{Q}})$ is a minimal closed subset of $\mathbf{A}_{\mathbf{Q}}^1$.

It is a purely topological fact that any minimal closed subset is the closure of any of its points. The following proposition shows that, in the Zariski topology, every point is contained in such a subset.

Proposition 3.1.31. *Let V be an affine algebraic set over k. For each point $P \in V$, the closure of P in V is a minimal closed subset of V, corresponding to the maximal ideal of $A(V)$ consisting of all functions $f \in A(V)$ that vanish at P. Furthermore, all maximal ideals arise in this way.*

Proof By Remark 3.1.29, the irreducible closed subset $\overline{\{P\}}$ corresponds to a prime ideal $\mathfrak{p}$ of $A(V)$, namely the image under the map $k[x_1,\dots,x_n] \to A(V)$ of the ideal $I(\overline{\{P\}},k) = I(\{P\},k)$ in $k[x_1,\dots,x_n]$. Through the identification of Remark 3.1.26, the ideal $\mathfrak{p}$ is the kernel of the evaluation map $A(V) \to \bar{k}$ that sends $f \in A(V)$ to $f(P) \in \bar{k}$. The image of this ring homomorphism is a subring of $\bar{k}$ that contains k, so it is a field. Therefore, the kernel $\mathfrak{p}$ is maximal, so $\overline{\{P\}}$ is a minimal non-empty closed subset. The last statement of the proposition follows from the fact that each minimal closed subset is the closure of any of its points. □

In fact, we shall see in Proposition 3.5.5 that the closure of a point $P \in V$ is the orbit of P under the group $G_k = \mathrm{Aut}(\bar{k}/k)$ of automorphisms of $\bar{k}$ that restrict to the identity on k.

Definition 3.1.32. Let X be a topological space. Then the *dimension* of X, denoted $\dim X$, is the supremum of all the integers n for which there is a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X. The *dimension* of a quasi-affine algebraic set over k is its dimension as a topological space.

18: What is an open subset of V? Does it come with a ground field?

We will see in Proposition 3.5.2 that the dimension of a quasi-affine algebraic set does not depend on the base field.

Remark 3.1.33. Any topological space without irreducible subsets, in particular the empty affine algebraic set over k, does not admit such chains. As the supremum of the empty set of integers is $-\infty$, the dimension of such spaces is $-\infty$.

19: are there more such spaces?

By Remark 3.1.29, the closed subsets of an affine algebraic set V correspond to the radical ideals in the coordinate ring $A(V)$. Since $A(V)$ is noetherian, the topological space $V(\bar{k})$ is also noetherian, which means that it satisfies the descending chain condition on closed subsets. This implies the following proposition.

Proposition 3.1.34. *Every quasi-affine algebraic set V over k can be expressed uniquely as a finite union of quasi-affine varieties over k, each closed in V, none of which is contained in another.*

20: In fact, this is also true for zero sets in ℓ^n with the k-Zariski topology. For $k = \ell = \mathbf{R}$ this helps the algebraic statisticians.

Proof This follows from Proposition I.1.5 of Hartshorne (1977) and the fact that an open subspace of a noetherian topological space is also noetherian. □

21: last statement is not there; proof needed?

Definition 3.1.35. Let V be a quasi-affine algebraic set over k. The *irreducible components* of V are the quasi-affine varieties appearing in Proposition 3.1.34.

Exercise 3.1.36. Let V be a non-empty quasi-affine algebraic set. Show that

the dimension of V is the maximum of the dimensions of its irreducible components.

Recall that the *Krull dimension* of a commutative ring A is the supremum of all the integers n for which there is a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ of distinct prime ideals of A.

Proposition 3.1.37. *Let V be an affine variety over k. The following three quantities are equal:*

(i) *the dimension of V;*
(ii) *the Krull dimension of the coordinate ring $A(V)$;*
(iii) *the transcendence degree over k of the fraction field of $A(V)$.*

22: purposely not used the function field, which we may want to define differently

Furthermore, each maximal chain of distinct irreducible closed subsets of V has length $\dim V$.

Proof By Remark 3.1.29, the irreducible closed subsets of V correspond with the prime ideals in the coordinate ring $A(V)$. This implies the equality of the first two quantities. The rest of the proposition is Theorem 13.A of Eisenbud (1995). □

Exercise 3.1.38. Show that the dimension of affine n-space $\mathbf{A}^n_k$ over k is equal to n.

23: better not to have exercises mid text?

The following two exercises collect some topological facts that we will use to prove Proposition 3.1.41.

Exercise 3.1.39. Let X be a topological space and suppose that for each point $x \in X$, the closure of x in X is a minimal closed subset of X. Let $U \subset X$ be an open subset.

(i) Let $Z \subset X$ be a subset satisfying $Z \cap U \neq \emptyset$. Then the following statements are equivalent:
   (a) Z is a minimal closed subset of U;
   (b) Z is a minimal closed subset of X;
   (c) there is a $P \in Z \cap U$ such that Z is the closure of P in U;
   (d) there is a $P \in Z$ such that Z is the closure of P in X;
   (e) Z is non-empty and, for all $P \in Z \cap U$, the closure of P in U is Z;
   (f) Z is non-empty and, for all $P \in Z$, the closure of P in X is Z.

(ii) Every closed subset of U is the disjoint union of minimal closed subsets of U.

(iii) Let $Z \subset U$ be a closed subset of U. Then Z is minimal among all non-empty closed subsets of U if and only if Z is minimal among all irreducible closed subsets of U.

Exercise 3.1.40. Let X be a topological space containing a non-empty open subset U.

(i) For every chain

$$Z_0 \subset Z_1 \subset \cdots \subset Z_n$$

of distinct irreducible closed subsets of U, the closures

$$\overline{Z}_0 \subset \overline{Z}_1 \subset \cdots \subset \overline{Z}_n$$

form a chain of distinct irreducible closed subsets of X.

(ii) Suppose that for every minimal irreducible closed subset of U, the closure in X is a minimal irreducible closed subset of X. Then, if the first chain in (i) is maximal, so is the second.

(iii) Suppose furthermore that all maximal chains of distinct irreducible closed subsets of X have the same length, and that U contains an irreducible closed subset. Then we have $\dim U = \dim X$.

24: what's a non-empty topology without irreducible closed subsets? (See a couple of checks back)

Proposition 3.1.41. *Let V be an affine variety over k and $U \subset V$ a nonempty open subset. Then* $\dim U = \dim V$.

Proof By Proposition 3.1.31, the variety V satisfies the hypotheses on X of Exercise 3.1.39. That exercise and Proposition 3.1.37 together imply the hypotheses of Exercise 3.1.40, which yields $\dim U = \dim V$. □

25: Make prop'n again?

Exercise 3.1.42. Let V be a quasi-affine algebraic subset of $\mathbf{A}^n_k$. Show $\dim V \leq n$.

Definition 3.1.43. Let $V \subset \mathbf{A}^n_k$ be a quasi-affine algebraic set over k of dimension d, and suppose that the ideal $I(V) \subset k[x_1, \ldots, x_n]$ is generated by polynomials $f_1, \ldots, f_r$. Let $P \in V(\bar{k})$ be a point. We say that V is *smooth* at P if the Jacobian matrix $((\partial f_i/\partial x_j)(P))$ has rank $n-d$. If V is not smooth at P, then V is *singular* at P. The quasi-affine variety V is *smooth* if it is smooth at every point in $V(\bar{k})$.

Smoothness is equivalent to the non-vanishing of certain minors of the Jacobian matrix, so it is an open condition. In particular, if a quasi-affine variety V is smooth at a point P, then V is smooth on a dense open set containing P. Note that in order to verify smoothness, we take generators $f_1, \ldots, f_r$ of the ideal $I(V)$ of V; there exist varieties V for which this is not equivalent to taking $f_1, \ldots, f_r$ such that V is the zero set of the ideal generated by $f_1, \ldots, f_r$.

26: Give example, or make that an exercise.

Example 3.1.44. Let L be the line $V_{\mathbf{Q}}(x,y)$ in $\mathbf{A}^3_{\mathbf{Q}}$. The ideal $I(L,\mathbf{Q})$ is generated by x and y, so the coordinate ring $A(L)$ is isomorphic to $\mathbf{Q}[z]$, the fraction field of which has transcendence degree 1, so L is 1-dimensional. The Jacobian matrix at any point is the 2×3 matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

which has rank 2. Therefore L is smooth.

Example 3.1.45. Let C be the affine variety $V_{\mathbf{Q}}(y^2-x^3)\subset \mathbf{A}^2_{\mathbf{Q}}$. The homomorphism $A(C)\to \mathbf{Q}[t]$ given by $x\mapsto t^2$ and $y\mapsto t^3$ induces an isomorphism $\kappa(C)\to\mathbf{Q}(t)$, and so the dimension of C is 1. The ideal $I(C,\mathbf{Q})$ is generated by y^2-x^3; the Jacobian matrix is the 1×2 matrix $\begin{pmatrix}-3x^2 & 2y\end{pmatrix}$. The rank of this matrix is 1 at all points other than $(0,0)$. Since $(0,0)$ lies in C, it follows that the only singular point of C is $(0,0)$.

27: Example with singular points over extensions?

Example 3.1.46. Let k be the field $\mathbf{F}_3(t)$, and let V be the affine variety $V_k(x^3-t)\subset \mathbf{A}^1_k$. The ideal $I(V,k)$ is generated by the polynomial x^3-t. The Jacobian matrix at the unique point of V is the 1×1 matrix (0), and so V is not smooth, even though $V(k)$ is empty. On the other hand, consider the field extension $\mathbf{F}_3(t)\subset \mathbf{F}_3(s)=\ell$ such that $t=s^3$. Let V' denote the affine variety over ℓ defined by the same polynomial $x^3-t=(x-s)^3$. Then $I(V',\ell)$ is generated by the polynomial $x-s$, and V' is smooth.

28: Use k' instead of ℓ?

29: worth using the same example much earlier to point out the difference with Silverman's terminology of "being defined over" which does not correspond to our definition in case k is not perfect.

30: Also add result that over perfect fields the two notions coincide. Better yet: If ℓ is a separable field extension of k and $Z=\overline{Z}^k$, then $I(Z,\ell)=I(Z,k)R_\ell$. This is EGA-IV Corollary 4.6.4 (page 68).

3.2 Projective varieties

The approach we followed in Section 3.1 carries over with no difficulty to projective varieties. We maintain the setup of the previous section: we let $k\subset\ell$ be an extension of fields and we denote by $\bar{k}$ an algebraic closure of k. Let n be a non-negative integer. The multiplicative group $\ell^\times$ acts freely on the set $\mathbf{A}^{n+1}(\ell)\smallsetminus\{0\}$ by $\lambda\cdot(\xi_0,\dots,\xi_n)\mapsto(\lambda\xi_0,\dots,\lambda\xi_n)$; we define the set $\mathbf{P}^n(\ell)$ of ℓ-points of projective space to be the quotient of $\mathbf{A}^{n+1}(\ell)\smallsetminus\{0\}$ by the action of $\ell^\times$.

Let i be an element of $\{0,\dots,n\}$ and let $U_i(\ell)\subset\mathbf{P}^n(\ell)$ be the subset consisting of all points whose i-th coordinate is non-zero. There is an obvious injection $j_i\colon \mathbf{A}^n(\ell)\hookrightarrow\mathbf{P}^n(\ell)$ given by

$$j_i(\xi_1,\dots,\xi_n)=[\xi_1,\dots,\xi_i,1,\xi_{i+1},\dots,\xi_n];$$

the image of j_i is $U_i(\ell)$. We call $U_i(\ell)$ the i-th *standard affine patch* of $\mathbf{P}^n(\ell)$.

31: notation projective points not introduced yet. I'd prefer $(\xi_1:\dots:\xi_i:1:\xi_{i+1}:\dots:\xi_n)$, or some other dots...

32: "affine patch" even though this is only about sets of points? I.e., no base field.

Denote by R the polynomial ring $k[X_0,\dots,X_n]$ in $n+1$ variables over k. If $F \in R$ is a *homogeneous* polynomial and P is in $\mathbf{A}^{n+1}(\ell)$, then $F(P)$ vanishes if and only if $F(\lambda \cdot P)$ vanishes for all $\lambda \in \ell^\times$. Thus, a homogeneous polynomial has a well-defined vanishing set in $\mathbf{P}^n(\ell)$, and the condition that a homogeneous polynomial vanish at a point applies to elements of $\mathbf{P}^n(\ell)$.

Let $S \subset R$ be a subset consisting of homogeneous polynomials; we define the *zero set* $Z(S,\ell) \subset \mathbf{P}^n(\ell)$ to be the set of all common zeros with coordinates in the field ℓ of the polynomials in S:

33: mention it will always be clear from the context whether $Z(S,\ell)$ lives in $\mathbf{A}^{n+1}$ or $\mathbf{P}^n$? Same for $V_k(S)$ later.

$$Z(S,\ell) = \{P \in \mathbf{P}^n(\ell) \mid \forall F \in S,\, F(P) = 0\}.$$

Recall that every polynomial f in R can be written uniquely as a sum of homogeneous polynomials of different degrees, called the *homogeneous parts* of f. If $S \subset R$ is any subset, not necessarily consisting of homogeneous polynomials, we define the *zero set* $Z(S,\ell) \subset \mathbf{P}^n(\ell)$ to be the set of all common zeros with coordinates in the field ℓ of the homogeneous parts of all the polynomials in S.

34: ever useful?

Given any subset Z of $\mathbf{P}^n(\ell)$, we can consider the inverse image of Z under the quotient map $\mathbf{A}^{n+1}(\ell) \smallsetminus \{0\} \to \mathbf{P}^n(\ell)$. This inverse image, together with the point 0 if Z is non-empty, is called the *affine cone* over Z. If Z is the zero set in $\mathbf{P}^n(\ell)$ by a set of homogeneous polynomials, then the affine cone over Z is the zero set in $\mathbf{A}^{n+1}(\ell)$ of the same set of polynomials. Note that for this statement to be true, it is essential that we defined the affine cone over the empty set to be empty. Many statements about Z can be interpreted as statements about the affine cone over Z, and therefore can be studied using results on affine schemes.

35: Mention some specific properties (irreducibility...)? Or does this come later?

Definition 3.2.1. An ideal $I \subset R$ is *homogeneous* if it can be generated by homogeneous polynomials. The *irrelevant ideal* is the homogeneous ideal generated by $X_0,\dots,X_n$; it consists of all polynomials with no constant term.

The reason for the name "irrelevant ideal" is that the zero set of the irrelevant ideal in $\mathbf{P}^n(\bar{k})$ is empty.

Exercise 3.2.2. Show that, if I is a homogeneous ideal in R, then a polynomial f lies in I if and only if each of the homogeneous parts of f lies in I. Moreover, this property characterises homogeneous ideals.

Definition 3.2.3. Let Z be a subset of $\mathbf{P}^n(\ell)$. We say that Z *can be defined over* k if there exists a subset $S \subset R$ of homogeneous polynomials such that $Z = Z(S,\ell)$.

In the same way as in the affine case, the zero sets of sets of homogeneous polynomials form the closed sets of the *k-Zariski topology* on $\mathbf{P}^n(\ell)$.

Definition 3.2.4. A *projective algebraic set V over k* is a subset of $\mathbf{P}^n(\bar{k})$, for some n, that can be defined over k, together with the field k itself. We call the field k the *base field* of V. The *Zariski topology* on V is the topology induced by the k-Zariski topology on $\mathbf{P}^n(\bar{k})$. A *quasi-projective algebraic set over k* is an open subset of a projective algebraic set over k, together with the field k as base field, and with the induced topology.

Definition 3.2.5. Let n be a non-negative integer. *Projective n-space* $\mathbf{P}^n_k$ *over* k is the set $\mathbf{P}^n(\bar{k})$, with k as the base field.

36: we already had an n.

Definition 3.2.6. For any subset $S \subset R$ of (homogeneous) polynomials, we denote by $V_k(S)$ the projective algebraic set over k with underlying set of points $Z(S,\bar{k})$. If $F_1,\ldots,F_r \in R$ are homogeneous polynomials, then $V_k(F_1,\ldots,F_r)$ means $V_k(\{F_1,\ldots,F_r\})$.

37: for clarity, add "$\subset \mathbf{P}^n_k$" and/or "$\subset \mathbf{P}^n(\bar{k})$"?

As in the affine case, a subset of $\mathbf{P}^n(\ell)$ is said to be *irreducible over k* if it is irreducible in the k-Zariski topology.

Definition 3.2.7. A *projective variety over k* is a projective algebraic set over k that is irreducible over k. A *quasi-projective variety over k* a quasi-projective algebraic set over k that is irreducible over k.

Example 3.2.8. For $i \in \{0,\ldots,n\}$ the i-th standard affine patch U_i of $\mathbf{P}^n_k$ is the quasi-projective variety over k defined by $X_i \neq 0$.

38: is this a definition? Before we only had sets of points.

To any subset Z of $\mathbf{P}^n(\ell)$ we associate the homogeneous radical ideal $I(Z,k)$ of polynomials in R vanishing on Z. This is the same as the ideal of polynomials vanishing on the affine cone over Z. If V is a projective algebraic set over k, then we write $I(V) = I(V(\bar{k}),k)$, where $V(\bar{k})$, as before, denotes the underlying set of points of V.

Analogously to the affine case, we want to establish a correspondence between projective algebraic sets and homogeneous radical ideals. Note, though, that both the irrelevant ideal and the whole ring $k[X_0,\ldots,X_n]$ are homogeneous radical ideals with empty vanishing set. Combined with the following exercise, the Projective Nullstellensatz shows that this is the only exception.

39: exception to what?

Exercise 3.2.9. Show that the irrelevant ideal and the whole ring $k[X_0,\ldots,X_n]$ are the *only* homogeneous radical ideals with empty vanishing set.

Theorem 3.2.10 (Projective Nullstellensatz)**.** *Suppose that ℓ is an algebraically closed field containing the field k. Let I be a homogeneous ideal in $k[X_0,\ldots,X_n]$ such that $Z(I,\ell) \subset \mathbf{P}^n(\ell)$ is non-empty. Then $I(Z(I,\ell),k)$ is the radical of I.*

Proof Let $C(I)$ denote the zero set in $\mathbf{A}^{n+1}(\ell)$ of the ideal I; the set $C(I) \smallsetminus \{0\}$ coincides with the inverse image of $Z(I,\ell) \subset \mathbf{P}^n(\ell)$ under the projection map $\mathbf{A}^{n+1}(\ell) \smallsetminus \{0\} \to \mathbf{P}^n(\ell)$. Since $Z(I,\ell)$ is non-empty, it follows that $C(I)$ is the affine cone over $Z(I,\ell)$, and hence that $I(C(I),k)$ is the same ideal as $I(Z(I,\ell),k)$. Applying Corollary 3.1.18 to I gives the result. □

40: we already have an n

Corollary 3.2.11. *Let n be a non-negative integer. The operations $Z(\,\cdot\,,\bar{k})$ and $I(\,\cdot\,,k)$ determine a bijection between projective algebraic sets over k in $\mathbf{P}^n_k$ and homogeneous radical ideals in $k[X_0,\dots,X_n]$ different from the irrelevant ideal. Under this bijection, the projective algebraic varieties correspond to the prime ideals.*

Definition 3.2.12. Let V be a projective algebraic set over k. For any field extension ℓ of k, the set of *ℓ-points* of V is $V(\ell) = Z(I(V),\ell)$. For projective algebraic sets $W \subset V$ over k and $U = V \smallsetminus W$, we set $U(\ell) = V(\ell) \smallsetminus W(\ell)$.

41: Notations $\mathbf{P}^n(\bar{k})$ and $U_i(\bar{k})$ consistent...

Definition 3.2.13. Let $V \subset \mathbf{P}^n_k$ be a projective algebraic set over k. The *homogeneous coordinate ring* of V is the quotient ring $\Gamma(V) = k[X_0,\dots,X_n]/I(V)$. The ring $\Gamma(V)$ has a grading induced by the natural grading on $k[X_0,\dots,X_n]$ and homogeneous elements of $\Gamma(V)$ are called *forms* on V.

42: why Γ?

43: From this line to the next seems old

In contrast to the affine case, elements of the homogeneous coordinate ring of a projective algebraic set do not give well-defined functions on that set.

Let V be a projective algebraic set over k. An element of $\Gamma(V)$ determines a function on the affine cone over V, but this function does not induce a function on $V(\bar{k})$ unless it is constant. However, a ratio of two forms of the same degree does indeed induce a function on the open subset of $V(\bar{k})$ where the denominator is non-zero.

Definition 3.2.14. Let $V \subset \mathbf{P}^n_k$ be a projective variety over k. The *function field* $\kappa(V)$ of V is the degree zero part of the field of fractions of the coordinate ring $\Gamma(V)$. Elements of $\kappa(V)$ are called *rational functions* on V.

Remark 3.2.15. By definition, an element of $\kappa(V)$ is represented by a quotient of two forms of the same degree in $\Gamma(V)$. Equivalently, an element of $\kappa(V)$ may be represented by a quotient of two homogeneous polynomials in $k[X_0,\dots,X_n]$ of the same degree; two such quotients F/G and F'/G' represent the same element of $\kappa(V)$ if and only if $FG' - F'G$ lies in $I(V)$.

Definition 3.2.16. A rational function $h \in \kappa(V)$ is *regular* at a point P of V if h admits a representation F/G, with $F,G \in \Gamma(V)$ forms of the same degree, such that $G(P) \neq 0$.

Definition 3.2.17. Let $V \subset \mathbf{P}^n_k$ be a projective variety over k, and let $Z \subset V$ be a

closed irreducible subset. The *local ring* of Z in V, denoted $\mathscr{O}_{V,Z}$, is the subring of $\kappa(V)$ consisting of those rational functions which are regular at some point of Z (or, equivalently, on a dense open subset of Z).

44: Do we also want the local ring of Z in a quasi-rpojective or quasi-affine variety V?

We want to consider affine varieties as quasi-projective varieties and for this reason we recall some standard properties of the inclusions j_i of the standard affine patches of $\mathbf{P}^n_k$. If $f \in k[x_1,\dots,x_n]$ is a polynomial of degree d, then the i-th homogenisation of f is the homogeneous polynomial $F^i(X_0,\dots,X_n)$ defined by

$$F^i(X_0,\dots,X_n) = X_i^d\, f\Big(\frac{X_0}{X_i},\dots,\frac{X_{i-1}}{X_i},\frac{X_{i+1}}{X_i},\dots,\frac{X_n}{X_i}\Big).$$

Conversely, if $F \in k[X_0,\dots,X_n]$ is a homogeneous polynomial, then the i-th dehomogenisation of F is the polynomial $f^i \in k[x_1,\dots,x_n]$ defined by

45: mention homogenisation of dehomogenisation of F is not necessarily F?

$$f^i(x_1,\dots,x_n) = F(x_1,\dots,x_{i-1},1,x_i,\dots,x_n).$$

46: confusing notation! "F^i is determined by f and f^i by F!!!!!!

(i) If $f_1,\dots,f_r$ are polynomials in $k[x_1,\dots,x_n]$, then the image under j_i of $V_k(f_1,\dots,f_r) \subset \mathbf{A}^n_k$ is $U_i \cap V_k(F^i_1,\dots,F^i_r)$.

47: for clarity, add "in $\mathbf{P}^n_k$"?

(ii) If $f \in k[x_1,\dots,x_n]$ is a regular function on $\mathbf{A}^n_k$, then for each point $P \in A^n_k(\ell)$ the equality $f(P) = F^i(j_i(P))$ holds in ℓ.

48: What does this mean? We can't evaluate F^i at $j_i(P)$...

(iii) If $F_1,\dots,F_r$ are homogeneous polynomials in $k[X_0,\dots,X_n]$, then the inverse image under j_i of $V_k(F_1,\dots,F_r) \subset \mathbf{P}^n_k$ is $V_k(f^i_1,\dots,f^i_r)$.

(iv) If $F,G \in k[X_0,\dots,X_n]$ are forms on $\mathbf{P}^n_k$ of the same degree then, for each point $P \in U_i(\ell)$ such that $G(P) \neq 0$, the equality

$$\frac{F(P)}{G(P)} = \frac{f^i(j_i{}^{-1}(P))}{g^i(j_i{}^{-1}(P))}$$

holds in ℓ.

49: and g^i is nonzero at $j_i^{-1}(P)$ and f^i/g^i is regular at P.

50: that

(v) If $X \subset \mathbf{P}^n_k$ is a projective variety which meets U_i, then the correspondence of (iv) determines an isomorphism from $\kappa(X)$ to the function field of the affine variety $j_i{}^{-1}(X)$.

(vi) Let $X \subset \mathbf{P}^n_k$ be a projective variety, and let Z be an irreducible closed subset of X which meets U_i. Then the isomorphism of (v) identifies the local ring of Z in X with the local ring of $j_i{}^{-1}(Z)$ in the affine variety $j_i{}^{-1}(X)$.

Exercise 3.2.18. For $i \in \{0,\dots,n\}$, show that the inclusion $j_i\colon \mathbf{A}^n(\ell) \hookrightarrow \mathbf{P}^n(\ell)$ is a homeomorphism onto its image $U_i(\ell)$, which is open in $\mathbf{P}^n(\ell)$.

In the next section we introduce morphisms and isomorphisms of varieties. Using these notions we will be able to say that the affine variety A_k^n and the quasi-projective varieties $U_0, \ldots, U_n$ are all isomorphic.

51: Dimension

3.3 Regular functions and morphisms

We start by defining the notion of regular functions on affine and projective algebraic sets separately.

If V is an affine algebraic set in $\mathbf{A}_k^n$, then, as we have already seen, an element of the polynomial ring $k[x_1, \ldots, x_n]$ defines a function $V(\bar{k}) \to \bar{k}$. More generally, if f, g are two elements of $k[x_1, \ldots, x_n]$, then we can define the function $P \mapsto f(P)/g(P)$ on the open subset of V where g does not vanish. With this in mind, we define a regular function to be one which is locally given by a ratio of polynomials.

Definition 3.3.1. Let V be a quasi-affine algebraic set in $\mathbf{A}_k^n$. A function $f\colon V \to \bar{k}$ is *regular* at a point $P \in V(\bar{k})$ if there are polynomials $g, h \in k[x_1, \ldots, x_n]$ and an open neighbourhood U of P inside V such that h does not vanish anywhere on U and we have $f(Q) = g(Q)/h(Q)$ for all $Q \in U(\bar{k})$. The function f is *regular* on V if f is regular at every point of V.

52: Put in an example

If V is a projective algebraic set in $\mathbf{P}_k^n$, then an element of $k[X_0, \ldots, X_n]$ determines a function on the affine cone over V, but this function does not induce a function on $V(\bar{k})$ unless it is constant. However, a ratio of two forms g, h of the same degree does induce a function on the open subset U of $V(\bar{k})$ where h does not vanish. Indeed, for any point $Q \in U(\bar{k})$, the ratio $g(\tilde{Q})/h(\tilde{Q})$ is the same among all lifts $\tilde{Q}$ of Q to the affine cone $\mathbf{A}_k^{n+1}$ over $\mathbf{P}_k^n$. We denote this ratio by $(g/h)(Q)$.

Definition 3.3.2. Let V be a quasi-projective algebraic set in $\mathbf{P}_k^n$. A function $f\colon V \to \bar{k}$ is *regular* at a point $P \in V(\bar{k})$ if there are homogeneous polynomials $g, h \in k[X_0, \ldots, X_n]$ of the same degree, and an open neighbourhood U of P inside V such that h does not vanish anywhere on U and we have $f(Q) = (g/h)(Q)$ for all $Q \in U(\bar{k})$. The function f is *regular* on V if f is regular at every point of V.

53: Put in an example

Definition 3.3.3. An *algebraic set* over k is a quasi-affine or quasi-projective algebraic set over k. A *variety* over k is a quasi-affine or quasi-projective variety over k.

In other words, a variety is an irreducible algebraic set. We will often view an open subset of an algebraic set over k as an algebraic set over k, by implicitly attaching the base field k.

The regular functions on an algebraic set V form a subring of the ring $\mathrm{Map}(V(\bar{k}),\bar{k})$ of all maps $V(\bar{k}) \to \bar{k}$. We denote this subring by $\mathscr{O}(V)$.

Remark 3.3.4. As the regular functions are locally quotients of polynomials over k, they can in fact be evaluated at any point of V over a field extension of k. We obtain a natural homomorphism $\mathscr{O}(V) \to \mathrm{Map}(V(\ell),\ell)$ for any field extension ℓ of k.

Lemma 3.3.5. *Let V be an algebraic set over k. If we endow $\bar{k}$ with the k-Zariski topology on $\mathbf{A}^1_k(\bar{k})$, then every regular function $f\colon V(\bar{k}) \to \bar{k}$ is continuous.*

Proof Suppose that V is a quasi-affine algebraic set contained in $\mathbf{A}^n_k$. Then the (easy) proof is exactly the same as that of Lemma I.3.1 of Hartshorne (1977), which does not use the fact that V is irreducible, nor that k is algebraically closed. The proof for the case that V is quasi-projective is similar, and left to the reader. □

Lemma 3.3.6. *Let V be an algebraic set over k and let U be a dense open subset of V. Then the natural restriction map $\mathscr{O}(V) \to \mathscr{O}(U)$ is injective.*

Proof Suppose $f,g \in \mathscr{O}(V)$ agree on U. Then the regular function $h = f - g$ vanishes on U, so by Lemma 3.3.5 it vanishes on the closure of U, which equals V because U is dense in V. Hence, f and g agree on V. □

Recall from Remark 3.1.26 that for any affine algebraic set $V \subset \mathbf{A}^n_k$, the natural map $\varphi\colon k[x_1,\ldots,x_n] \to \mathrm{Map}(V(\bar{k}),\bar{k})$ induces an injection $A(V) \to \mathrm{Map}(V(\bar{k}),\bar{k})$. Clearly the function induced by a polynomial is regular, that is, the image of φ is contained in $\mathscr{O}(V)$. Proposition 3.3.7 states that the image is in fact equal to $\mathscr{O}(V)$. Although this proposition is generalised by Proposition 3.3.20, which does not require V to be irreducible, we include it here because its independent proof includes an elegant and useful argument.

Proposition 3.3.7. *Let V be an affine variety. The injection $A(V) \to \mathscr{O}(V)$ is an isomorphism.*

Proof It suffices to prove that the image of φ contains $\mathscr{O}(V)$. Let $f \in \mathscr{O}(V)$ be a regular function. For every point $P \in V(\bar{k})$, there are an open neighbourhood U_P of P and polynomials g_P, h_P such that $f = g_P/h_P$ on U_P. If P,Q are two points, then g_P/h_P and g_Q/h_Q agree on the intersection $U_P \cap U_Q$. Therefore the polynomial $q = g_P h_Q - g_Q h_P$ vanishes on $U_P \cap U_Q$, which is dense in V; so

q lies in $I(V,k)$. It follows that g_P/h_P and g_Q/h_Q define the same element α of the field of fractions $K = \mathrm{Frac}\,A(V)$. Therefore, for all P, the ratio f_P/g_P equals α in K. For each P, since $h_P(P)$ is non-zero, α is contained in the localisation $A(V)_{\mathfrak{m}_P}$, where $\mathfrak{m}_P = I(P,k)$ is the maximal ideal of $A(V)$ corresponding to the closure of P (see Proposition 3.1.31). Thus α lies in $A(V)_{\mathfrak{m}}$ for any maximal ideal $\mathfrak{m}$. Since every integral domain is equal to the intersection, inside its field of fractions, of its localisations at all maximal ideals, the element α lies in $A(V)$. It is easily verified that $\varphi(\alpha)$ is f. □

54: Find reference.

Having defined regular functions, we will now define a morphism between algebraic sets simply as a function that transforms regular functions into regular functions. This definition has the advantage of being elegant and useful, but is not very explicit. Afterwards, we shall give an explicit description of a morphism of algebraic sets.

55: pulls back instead of transforms?

Definition 3.3.8. Let V and W be algebraic sets over k. A *morphism* from W to V is a continuous function $\varphi\colon W \to V$ such that, for every open set $U \subset V$ and every regular function $f \in \mathscr{O}(U)$, the pull-back $(f \circ \varphi)\colon \varphi^{-1}(U) \to \bar{k}$ is a regular function on the algebraic set $\varphi^{-1}(U)$ over k. An *isomorphism* is a morphism admitting an inverse that is also a morphism.

56: Check V versus $V(\bar{k})$ everywhere

Proposition 3.3.9. *Let V be a quasi-affine algebraic set in $\mathbf{A}^n_k$ and W an algebraic set over k. Then a function $\varphi\colon W \to V$ is a morphism if and only if there exist regular functions $f_1, \ldots, f_n \in \mathscr{O}(W)$ such that φ is given by*

$$Q \mapsto (f_1(Q), f_2(Q), \ldots, f_n(Q)).$$

57: Or give a proof!

Proof Exercise. □

Morphisms into projective space do not admit as simple a description as morphisms into affine space, but at least we can say what they look like locally.

Proposition 3.3.10. *Let V be a quasi-projective algebraic set in $\mathbf{P}^n_k$ and W an algebraic set over k. A function $\varphi\colon W \to V$ is a morphism if and only if, for every point $P \in W$, there exist a neighbourhood U of P and regular functions $f_0, \ldots, f_n \in \mathscr{O}(U)$ such that φ is given on U by*

$$Q \mapsto (f_0(Q) : \cdots : f_n(Q)).$$

58: Is this going to add more than Proposition 3.3.12? Yes, I think so [Ronald]

Proof Exercise. □

Exercise 3.3.11. Let V and W be algebraic sets over k and let $\varphi\colon W \to V$ be a function. Show that the following statements are equivalent:

(i) the function φ is a morphism;

(ii) for every open subset $U \subset V$, the inverse image $\varphi^{-1}(U)$ is an open subset of W and the restriction of φ is a morphism $\varphi^{-1}(U) \to U$;
(iii) there exists a cover $\mathscr{U}$ of V by open subsets such that, for all $U \in \mathscr{U}$, the inverse image $\varphi^{-1}(U)$ is an open subset of W and the restriction of φ is a morphism $\varphi^{-1}(U) \to U$.

Proposition 3.3.12. *Let V be a quasi-projective algebraic set in $\mathbf{P}^n_k$ and W an algebraic set over k. A function $\varphi\colon W \to V$ is a morphism if and only if, for each $i \in \{0,\dots,n\}$, the inverse image $\varphi^{-1}(U_i \cap V)$, where U_i is the i-th standard affine patch of $\mathbf{P}^n_k$, is open in W and there exist regular functions $f_{i,0},\dots,f_{i,i-1},f_{i,i+1},\dots,f_{i,n} \in \mathscr{O}(\varphi^{-1}(U_i \cap V))$ such that the restriction of φ to $\varphi^{-1}(U_i \cap V)$ is given by*

$$Q \mapsto (f_{i,0}(Q) : \cdots : f_{i,i-1}(Q) : 1 : f_{i,i+1}(Q) : \cdots : f_{i,n}(Q)).$$

Proof Exercise. □ 59: This should come after the isomorphism $\mathbf{A}^n \to U_i$.

Let V be an affine variety over k, and let α be an element of the field of fractions of the coordinate ring $A(V)$, which is an integral domain. In general, α does not define a function of the whole of V but, writing $\alpha = g/h$ with $g,h \in A(V)$, we see that α does define a regular function on the open set U where h is non-zero. However, the representation of α as a fraction is not necessarily unique. A different representation $\alpha = g'/h'$ defines a regular function on a potentially different open set U', and the two functions agree on the intersection $U \cap U'$. By Lemma 3.3.6, each function is determined by its restriction to $U \cap U'$, and so we would like to consider the two functions as "the same" in some sense. This motivates the following definition.

Definition 3.3.13. Let V be a variety over k. A *rational function* on V is an equivalence class of pairs (U,f) consisting of a non-empty open set $U \subset V$ and a regular function $f \in \mathscr{O}(U)$, where two pairs (U,f) and (U',f') are equivalent if the restrictions of f and f' to $U \cap U'$ agree. A rational function on V is *regular* on an open subset U of V if it is represented by (U,f) for some $f \in \mathscr{O}(U)$.

As any finite number of non-empty open subsets of a variety intersect in a dense open subset, we indeed have an equivalence in Definition 3.3.13 by Lemma 3.3.6: three regular functions $f \in \mathscr{O}(U)$, $f' \in \mathscr{O}(U')$, and $f'' \in \mathscr{O}(U'')$ agree on the non-empty intersection $U \cap U' \cap U''$ if and only if every two of them agree on the appropriate intersections of two of the three open subsets.

If f is a regular function on an open subset U of a variety, then, by abuse of notation, we often denote the rational function represented by (U,f) by f as well. Obviously, this rational function is regular on U.

The rational functions on a variety V clearly form a ring. In fact they form a field: if (U, f) is a pair representing a rational function with f not identically zero, then there is a non-empty open subset $U' \subset U$ on which f is never zero and so the pair $(U', 1/f)$ defines a rational function that is a multiplicative inverse of the original one.

Definition 3.3.14. Let V be a variety over k. The field of rational functions on V is called the *function field* of V and denoted $\kappa(V)$.

If V is an affine variety, then the motivation before Definition 3.3.13 describes a homomorphism $\mathrm{Frac}(A(V)) \to \kappa(V)$. We will see that this is an isomorphism in Proposition 3.3.20.

Suppose $\alpha \in \kappa(V)$ is a rational function that is regular on the open subsets U and U' of V. Then there are regular functions $f \in \mathscr{O}(U)$ and $f' \in \mathscr{O}(U')$ such that the pairs (U, f) and (U', f') represent α. There is a common extension $U \cup U' \to \bar{k}$ of f and f', which is again a regular function, so α is also regular on the union $U \cup U'$. It follows that there is a unique maximal open subset of V on which α is regular.

In a similar way, we define the local ring at a point of an algebraic set to consist of equivalence classes of regular functions defined on an open neighbourhood of that point. In fact, as any two open neighbourhoods of P intersect in an open neighbourhood of P, we need not require that V be irreducible. More generally, we now define the local ring at any irreducible subset.

Definition 3.3.15. Let V be an algebraic set over k let $Z \subset V$ be an irreducible subset. The *local ring* $\mathscr{O}_{V,Z}$ is the ring of equivalence classes of pairs (U, f) consisting of an open subset U of V satisfying $Z \cap U \neq \emptyset$ and a regular function $f \in \mathscr{O}(U)$, where two pairs (U, f) and (U', f') are equivalent if there exists an open subset $U'' \subset U \cap U'$ with $Z \cap U'' \neq \emptyset$ on which f and f' agree.

We leave it to the reader to verify, using Lemma 3.3.6, that we do indeed have an equivalence relation in Definition 3.3.15. When V is clear from the context, we often write $\mathscr{O}_Z$ instead of $\mathscr{O}_{V,Z}$. It follows from the continuity of regular functions that the local ring at an irreducible subset Z of V is the same as the local ring at the closure $\overline{Z}$.

Remark 3.3.16. Note that if $Z = P$ is a point, then the open subsets U of V with $Z \cap U \neq \emptyset$ are merely the open neighbourhoods of P. If, moreover, V is a variety, then it follows from Lemma 3.3.6 that the equivalence relation in Definition 3.3.15 coincides with the one used to define the local ring in Hartshorne (1977, Section I.3), which requires the functions f and f' to agree on the whole of $U \cap U'$. If V is not irreducible, then this last description does not define an equivalence relation.

Example 3.3.17. Suppose V is a variety over k. Then V is irreducible itself, and the local ring $\mathscr{O}_{V,V}$ coincides with the function field $\kappa(V)$.

For any algebraic set V, an open subset U, an irreducible subset Z, and a point $P \in U \cap Z$, the natural maps

$$\mathscr{O}_{U,P} \to \mathscr{O}_{V,P} \qquad \text{and} \qquad \mathscr{O}_{U,U\cap Z} \to \mathscr{O}_{V,Z}$$

are isomorphisms. Furthermore, there are natural k-algebra homomorphisms

60: The first follows from the second. Leave it out?

$$\mathscr{O}(V) \to \mathscr{O}(U) \to \mathscr{O}_{V,P} \to \mathscr{O}_{V,Z},$$

where the first map is the restriction map, the second sends $f \in \mathscr{O}(U)$ to the class of (U, f) in $\mathscr{O}_{V,P}$, and the third sends the class of (U, f) in $\mathscr{O}_{V,P}$ to its class in $\mathscr{O}_{V,Z}$. Moreover, if V is a variety, then there is also a natural map

$$\mathscr{O}_{V,Z} \to \kappa(V),$$

sending the class of (U, f) in $\mathscr{O}_{V,Z}$ to its class in $\kappa(V)$.

Definition 3.3.18. Let $\varphi\colon W \to V$ be a morphism of algebraic sets. We say that φ is dominant if its image is dense in V.

Proposition 3.3.19. *Let $\varphi\colon W \to V$ be a morphism of algebraic sets. Let U be an open subset of V and Z an irreducible subset of W. Suppose $P \in \varphi^{-1}(U) \cap Z$ is a point. The pull-back $f \mapsto f \circ \varphi$ of regular functions induces various k-algebra homomorphisms, all denoted by φ^*, making the diagram*

$$\begin{array}{ccccccc}
\mathscr{O}(V) & \longrightarrow & \mathscr{O}(U) & \longrightarrow & \mathscr{O}_{V,\varphi(P)} & \longrightarrow & \mathscr{O}_{V,\varphi(Z)} \\
\downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*} \\
\mathscr{O}(W) & \longrightarrow & \mathscr{O}(\varphi^{-1}(U)) & \longrightarrow & \mathscr{O}_{W,P} & \longrightarrow & \mathscr{O}_{W,Z}
\end{array}$$

commute. If V and W are varieties and φ is dominant, then the pull-back also induces a k-algebra homomorphism $\varphi^*\colon \kappa(V) \to \kappa(W)$ making the diagram

$$\begin{array}{ccc}
\mathscr{O}_{V,\varphi(Z)} & \longrightarrow & \kappa(V) \\
\downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*} \\
\mathscr{O}_{W,Z} & \longrightarrow & \kappa(W)
\end{array}$$

commute. Furthermore, if φ is an isomorphism, then all the induced maps are isomorphisms as well.

Proof This all follows easily from the definition of morphisms. For the second statement, we use the fact that φ is dominant to conclude that for every non-empty open subset U of V, the open subset $f^{-1}(U)$ of W is non-empty.

The final statement follows from comparing the first two statements applied to both $\varphi \circ \varphi^{-1}$ and id_V, as well as comparing the statements applied to both $\varphi^{-1} \circ \varphi$ and id_W. □

61: Insert a proposition that express $I(\varphi^{-1}(Z))$ in terms of $I(Z)$. And the other way around? What about components and the relation between their coordinate rings and those of the big ones?

If V is affine, then we can relate the various rings above to the coordinate ring of V. For any commutative ring A with a prime ideal $\mathfrak{p}$ and an element $f \notin \mathfrak{p}$, we let A_f denote the localisation of A with respect to the multiplicative set $\{f^i : i \geq 0\}$, and we let $A_\mathfrak{p}$ denote the localisation of A with respect to the set $A - \mathfrak{p}$. If A is an integral domain, then the natural A-algebra homomorphisms $A \to A_f \to A_\mathfrak{p} \to \mathrm{Frac}(A)$ are all injective.

62: Refer to some results about localisations in the appendix?

Let V be an affine algebraic set. For any $g, h \in A(V)$ and $D(h) = V - Z(h, \bar{k})$, there is a regular function on $D(h)$, denoted g/h, that sends $Q \in D(h)(\bar{k})$ to $g(Q)/h(Q)$. Since $D(h)$ equals $D(h^n)$ for any $n > 0$, this induces a natural homomorphism $A(V)_h \to \mathscr{O}(D(h))$ of k-algebras. In Proposition 3.3.20 we will see that this map is an isomorphism, which justifies the notation g/h for the regular function on $D(h)$. For any irreducible closed subset Z of V corresponding to a prime ideal $\mathfrak{p}$ of $A(V)$, we have $Z \cap D(h) \neq \emptyset$ if and only if $h \notin \mathfrak{p}$ (this follows from Corollary 3.1.18 to the Nullstellensatz), so we also obtain a natural homomorphism $A(V)_\mathfrak{p} \to \mathscr{O}_{V,Z}$ sending $g/h \in A(V)_\mathfrak{p}$ to $(D(h), g/h)$. If V is an affine variety, then we get the k-algebra homomorphism $\mathrm{Frac}(A(V)) \to \kappa(V)$ we have seen before.

Proposition 3.3.20. *Let V be an affine algebraic set in $\mathbf{A}^n_k$, let $Z \subset V$ be an irreducible closed subset, and let $\mathfrak{p} \subset A(V)$ be the prime ideal associated to Z. Let $f \in A(V)$ be an element, and set $D(f) = V - Z(f, \bar{k})$. Let $P \in D(f) \cap Z$ be a point, and let $\mathfrak{m} \subset A(V)$ be the maximal ideal associated to the closure of P in V. Then the maps described above are isomorphisms of k-algebras making the diagram*

$$\begin{array}{ccccccc}
A(V) & \longrightarrow & A(V)_f & \longrightarrow & A(V)_\mathfrak{m} & \longrightarrow & A(V)_\mathfrak{p} \\
\downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong \\
\mathscr{O}(V) & \longrightarrow & \mathscr{O}(D(f)) & \longrightarrow & \mathscr{O}_{V,P} & \longrightarrow & \mathscr{O}_{V,Z}
\end{array}$$

commute. If V is an affine variety, then the map $\mathrm{Frac}(A(V)) \to \kappa(V)$ is an isomorphism of k-algebras that makes the diagram

$$\begin{array}{ccc}
A(V)_\mathfrak{p} & \longrightarrow & \mathrm{Frac}(A(V)) \\
\downarrow\cong & & \downarrow\cong \\
\mathscr{O}_{V,Z} & \longrightarrow & \kappa(V)
\end{array}$$

commute.

Proof The special case that V is irreducible is easier to prove. In fact, Proposition 3.3.7 does the hardest part of this easy case. For the general case, we follow the proof of Proposition II.2.2 of Hartshorne (1977). It is clear that the diagram commutes, so it suffices to verify that all vertical maps are isomorphisms.

We start with the map $A(V)_{\mathfrak{p}} \to \mathscr{O}_{V,Z}$. To prove injectivity, let $g,h,g',h' \in A(V)$ be elements with with $h,h' \notin \mathfrak{p}$, and let U be the open subset where h and h' both do not vanish. Assume that the regular maps on U given by $Q \mapsto g(Q)/h(Q)$ and $Q \mapsto g'(Q)/h'(Q)$ agree on some open subset $U' \subset U$ with $Z \cap U' \neq \emptyset$. After shrinking U' if necessary, we may assume that U' is one of the basis opens of Remark **??**, so $U' = D(q)$ for some $q \in A(V)$. Then $q(gh' - g'h) \in A(V)$ vanishes on V, which implies $q(gh' - g'h) = 0$ in $A(V)$. This means that in the local ring $A(V)_{\mathfrak{p}}$, we have $g/h = g'/h'$ as well, which proves injectivity. For surjectivity, let $U \subset V$ be an open subset with $Z \cap U \neq \emptyset$ and $\rho \in \mathscr{O}(U)$ an element. Then locally around a point in $Z \cap U$ the regular function ρ is given by $Q \mapsto g(Q)/h(Q)$ for some $g,h \in A(V)$; the element $g/h \in A(V)_{\mathfrak{p}}$ maps to the class represented by (U,ρ), which shows surjectivity. We conclude that the map $A(V)_{\mathfrak{p}} \to \mathscr{O}_{V,Z}$ is indeed an isomorphism.

The map $A(V)_{\mathfrak{m}} \to \mathscr{O}_{V,P}$ being an isomorphism is the special case with $Z = P$. If V is irreducible, that is, it is an affine variety, then the map $\mathrm{Frac}(A(V)) \to \kappa(V)$ being an isomorphism is the special case with $Z = V$.

63: if it's a special case anyway, should it not be in the proposition???

We continue with the map $A(V)_f \to \mathscr{O}(D(f))$. The proof of injectivity is similar to before. Indeed, if the regular functions on $D(f)$ given by $Q \mapsto g(Q)/f^m(Q)$ and $Q \mapsto h(Q)/f^n(Q)$ for some $g,h \in A(V)$ and integers $m,n \geq 0$ agree on $D(f)$, then $f(gf^n - hf^m)$ vanishes on V, so $f(gf^n - hf^m) = 0$ in $A(V)$ and thus $g/f^m = h/f^n$ in $A(V)_f$. For surjectivity, let $\rho \in \mathscr{O}(D(f))$ be a regular function on $D(f)$. Then there exists a cover $\mathscr{U}$ of $D(f)$ by open subsets such that for each $U \in \mathscr{U}$, there are elements $g_U, h_U \in A(V)$ with h_U not vanishing anywhere on U, such that $\rho(Q) = g_U(Q)/h_U(Q)$ for all $Q \in U(\bar{k})$. After shrinking U if necessary, we may assume that U is one of the basis opens of Remark **??**, so $U = D(q_U)$ for some $q_U \in A(V)$. We claim that we may assume $h_U = q_U$ for all $U \in \mathscr{U}$. Indeed, from the fact that h_U does not vanish on $D(q_U)$, we find $Z(h_U,\bar{k}) \subset Z(q_U,\bar{k})$, so by Corollary 3.1.18 to the Nullstellensatz, we have $q_U \in \sqrt{(h_U)}$. Hence, there exist an integer $n \geq 1$ and an element $s_U \in A(V)$ such that $q_U^n = s_U h_U$. If we set $h'_u = q'_U = q_U^n$ and $g'_U = s_U g_U$, then for $Q \in U = D(q_U) = D(h'_U)$ we have

$$\frac{g_U(Q)}{h_U(Q)} = \frac{(s_U g_U)(Q)}{(s_U h_U)(Q)} = \frac{g'_U(Q)}{h'_U(Q)}.$$

Hence, we may replace g_U, h_U, q_U by g'_U, h'_U, q'_U, which proves the claim.

For any subset $\mathscr{S} \subset \mathscr{U}$ we have

$$Z(f,\bar{k}) = V - D(f) \subset V - \bigcup \mathscr{S} = \bigcap_{U \in \mathscr{S}} (V-U) = Z\big(\{h_U : U \in \mathscr{S}\},\bar{k}\big). \quad (3.1)$$

By Corollary 3.1.18 to the Nullstellensatz, the inclusion in (3.1) is an equality if and only if there exist an integer $n \geq 1$ and elements $r_U \in A(V)$ for $U \in \mathscr{S}$, all but finitely many equal to 0, such that

$$f^n = \sum_{U \in \mathscr{S}} r_U h_U.$$

Since we have equality for $\mathscr{S} = \mathscr{U}$, there are a finite subset $\mathscr{U}' \subset \mathscr{U}$, an integer $n \geq 1$, and elements $r_U \in A(V)$ for $U \in \mathscr{U}'$ such that $f^n = \sum_{U \in \mathscr{U}'} r_U h_U$. Applying the above to $\mathscr{S} = \mathscr{U}'$, we conclude that $\mathscr{U}'$ also covers $D(f)$. After replacing $\mathscr{U}$ by $\mathscr{U}'$, the cover $\mathscr{U}$ is finite.

Now, for each $U, W \in \mathscr{U}$ and each point $Q \in U \cap W = D(h_U) \cap D(h_W) = D(h_U h_W)$ we have $g_U(Q)/h_U(Q) = g_W(Q)/h_W(Q)$, so $h_U h_W(g_U h_W - g_W h_U)$ vanishes on V. It follows that we have $h_U h_W(g_U h_W - g_W h_U) = 0$ in $A(V)$, or, equivalently, $h_W^2(h_U g_U) - h_U^2(h_W g_W)$. After replacing h_U and g_U by h_U^2 and $h_U g_U$, respectively, and similarly for all elements of $\mathscr{U}$, we still have $\rho(Q) = g_U(Q)/h_U(Q)$ for all $Q \in U(\bar{k})$, and we have have $g_U h_W = g_W h_U$ in $A(V)$ for all $U, W \in \mathscr{U}$.

Let $n \geq 1$ and r_U, for $U \in \mathscr{U}$, be such that $f^n = \sum_{U \in \mathscr{U}} r_U h_U$, and set $g = \sum_{U \in \mathscr{U}} r_U g_U$. Then for each $W \in \mathscr{U}$, we have

$$h_W g = \sum_{U \in \mathscr{U}} r_U g_U h_W = \sum_{U \in \mathscr{U}} r_U h_U g_W = f^n g_W,$$

so $\rho(Q) = g_W(Q)/h_W(Q) = g(Q)/f^n(Q)$ for all $Q \in W$. It follows that the map $A(V)_f \to \mathscr{O}(D(f))$ sends g/f^n to ρ, so the map is surjective, and therefore an isomorphism.

The last fact that $A(V) \to \mathscr{O}(V)$ is an isomorphism is the special case that $f = 1$. □

64: Add similar statement for projective varieties

65: Add something like Prop. I.3.5 of Hartshorne (1977).

66: From this line to the next seems old

3.4 Rational maps and morphisms

Let X be a projective algebraic set over k and let n be a non-negative integer.

Definition 3.4.1. Let F be an $(n+1)$-tuple of forms of the same degree in $\Gamma(X)$. The $(n+1)$-tuple F is *regular* at a point P of X if the forms in F do not all vanish identically at P.

67: $P \in X(\bar{k})$ or $X(\ell)$ for some ℓ? And regular on $U \subset X$ means regular at each $P \in U(\bar{k})$?

If $F = (F_0, \dots, F_n)$ is regular at P, then $F(P) = [F_0(P), \dots, F_n(P)]$ determines a well-defined point in $\mathbf{P}^n_k$. If $P \in X(\ell)$ is an ℓ-point of X, then $F(P)$ is also an ℓ-point of $\mathbf{P}^n_k$.

68: leave out "also"

Definition 3.4.2. Let V be a dense open subset of X. Two $(n+1)$-tuples of forms F and G in $\Gamma(X)$ are defined to be equivalent if there is a dense open set $U \subset V$ on which both F and G are regular, and their values on U coincide. A *rational map* $\varphi\colon V \dashrightarrow \mathbf{P}^n_k$ is an equivalence class of such $(n+1)$-tuples in $\Gamma(X)$.

69: why distinguish V and X?

70: What's a value? I guess in $\mathbf{P}^n_k$ of course, but perhaps better to make precise.

71: also make more intuitive: say beforehand we get a map $U \to \mathbf{P}^n_k$ for some open U and mention this can be extended by taking an equivalent $(n+1)$-tuple, thus giving the following definition.

The $(n+1)$-tuples $(F_0, \dots, F_n)$ and $(G_0, \dots, G_n)$ represent the same rational map on V if and only if there is a dense open set U of V on which both F and G are regular and such that, for all $i, j \in \{0, \dots, n\}$, the form $F_iG_j - F_jG_i$ vanishes on all the $\bar{k}$-points of U, and hence on X by continuity. By the Nullstellensatz, this happens if and only if all the forms $F_iG_j - F_jG_i$ are zero in $k[X_0, \dots, X_n]$.

72: uhh, in $\Gamma(X)$?

Definition 3.4.3. Let $U \subset V$ be dense open subsets of the projective algebraic set X over k. A rational map $\varphi\colon V \dashrightarrow \mathbf{P}^n_k$ is *regular* at a point $P \in U$ if there is an $(n+1)$-tuple representing φ that is regular at P. A *morphism* $U \to \mathbf{P}^n_k$ is a rational map that is regular at every point of U.

73: would be nice if a morphism was actually a map...

If U, Y are open subsets of projective algebraic sets over k, with $Y \subset \mathbf{P}^n_k$, then a *morphism* $U \to Y$ is a morphism $U \to \mathbf{P}^n_k$ the image of which is contained in Y. As is usual, an *isomorphism* between two open subsets U, Y of projective algebraic sets is a morphism $U \to Y$ admitting an inverse which is also a morphism.

74: inverse **that**

Definition 3.4.4. A rational map $\varphi\colon X \dashrightarrow Y$ of varieties over k is *dominant* if the image of any representative of φ is dense in Y.

75: An inverse how? morphisms are not maps as currently defined...

76: what's a variety? I've only seen (quasi-)affine and (quasi-)projective varieties. So here it could be either? But rational maps are only defined on quasi-projective varieties. Are we implicitly identifying (quasi-)affine varieties with quasi-projective varieties? Does the identification not matter???

If $\varphi\colon X \to Y$ is a dominant rational map of varieties, then any rational function on Y is defined on a dense open subset of the image of ϕ, and therefore induces a rational function on X. In this way, φ induces an injective field homomorphism $\kappa(Y) \to \kappa(X)$.

77: every field homomorphism is injective.

Definition 3.4.5. A dominant rational map $\varphi\colon X \to Y$ of varieties is *birational* if it admits a rational inverse, that is, if there is a dominant rational map $\psi\colon Y \to X$ such that $\psi \circ \varphi$ represents the same rational map as the identity map on X, and similarly $\varphi \circ \psi$ represents the identity map on Y. In this case, we also say that the varieties X and Y are *birational*.

78: word "dominant" redundant?

79: the **same rational map as** the identity

Example 3.4.6. Let $C \subset \mathbf{P}^2_{\mathbf{Q}}$ be the variety defined by the equation $X^2 + Y^2 = Z^2$. The point $P_0 = [1, 0, 1]$ is in $C(\mathbf{Q})$. We show that projection from the point P_0 to the Y-axis induces a morphism $C \to \mathbf{P}^1_{\mathbf{Q}}$. Let $P = [x, y, z] \neq P_0$ be a point

on C; the equation of the line L through P_0 and P is $yX+(z-x)Y-yZ=0$. The line L meets the Y-axis $X=0$ at the point $[0,y,z-x]$ and we obtain a rational map

80: mention composition with the isomorphism between Y-axis and $\mathbf{P}^1$.

$$\pi\colon C \dashrightarrow \mathbf{P}^1_{\mathbf{Q}}, \qquad [x,y,z] \mapsto [y,z-x],$$

corresponding to the pair of forms $(Y,Z-X)$. The rational map π is regular at all points on C except possibly for the points whose coordinates satisfy $y=z-x=0$, that is, the point P_0. Nevertheless, the map π is regular also at the point P_0 since it is also represented by the pair $(X+Z,Y)$. Indeed, the identity $Y^2-(Z-X)(X+Z)=0$ holds in $\Gamma(C)$. Therefore, the rational map π is a morphism.

d: Include the example of projection away from a point in $\mathbf{P}^n$ to show that not always rational maps extend and to introduce blow ups of a point in $\mathbf{P}^n$ for birational invariance of Brauer groups.

Exercise 3.4.7. Show that the morphism π of Example 3.4.6 is an isomorphism by computing an inverse. As a consequence, we obtain a parametrisation of all the $\mathbf{Q}$-points of C.

81: Any line is isomorphic to $\mathbf{P}^1_k$; any conic with a point is also isomorphic to line!!!

Recall that we have defined a homeomorphisms $j_0,\dots,j_n$ from affine space $\mathbf{A}^n_k$ to the standard affine patches $U_0,\dots,U_n$ in $\mathbf{P}^n_k$. This allows us to identify the affine variety $\mathbf{A}^n_k$ with each of the quasi-projective varieties $U_0,\dots,U_n \subset \mathbf{P}^n_k$ (see also Exercise 3.2.18). Using these identifications we extend our definition of rational maps and morphisms to include maps to and from open subsets of affine algebraic sets.

Exercise 3.4.8. Show that a rational map from an affine or projective variety X over k to affine space $\mathbf{A}^n_k$ is given by an n-tuple of elements of the function field $\kappa(X)$.

82: more generally to an affine variety $Y \subset \mathbf{A}^n$?

Definition 3.4.9. A *variety* is a quasi-affine or quasi-projective variety. A variety is *affine* if it is isomorphic to an affine variety.

83: this was already used before

84: are we making a distinction between affine varieties and varieties that are affine??? maybe something like "We also say a variety is affine if it is merely isomorphic to an affine variety"

Example 3.4.10. Let $\pi\colon \mathbf{A}^2_k \to \mathbf{A}^1_k$ be the projection morphism $(x,y)\mapsto x$ and let $\phi\colon \mathbf{A}^1_k \dashrightarrow \mathbf{A}^2_k$ be the rational map $t \mapsto (t,t^{-1})$. The restrictions of π and ϕ to $V_k(xy-1)$ and $\mathbf{A}^1_k \smallsetminus \{0\}$, respectively, are mutually inverse morphisms. We deduce that the quasi-affine variety $\mathbf{A}^1_k \smallsetminus \{0\}$ is affine.

Exercise 3.4.11. Let f be a polynomial in $k[x_1,\dots,x_n]$ and let $U_f \subset \mathbf{A}^n_k$ denote the open subset defined by $f \neq 0$. Show that the quasi-affine variety U_f is affine. Deduce that, if X is an affine subvariety of $\mathbf{A}^n_k$, then the quasi-affine variety $X \cap U_f$ is also affine.

Exercise 3.4.12. Let X,Y be isomorphic affine varieties over k; show that the coordinate rings of X and Y are isomorphic. Show that regular functions on X correspond to morphisms $X \to \mathbf{A}^1_k$.

Definition 3.4.13. Let X be an open subset of a projective algebraic set over k and let P be a point of X. The point P is *smooth* on X if there is an open set $U \subset X$ containing P such that U is isomorphic to a quasi-affine variety U' and the point P corresponds to a smooth point of U'. We say that X is *smooth* if every point of X is smooth.

Theorem 3.4.14. *Let X be an open subset of a projective algebraic set over k. The following are equivalent:*

(i) *X is smooth;*
(ii) *there is a cover of X by smooth open quasi-affine varieties;*
(iii) *every open subset of X is smooth;*
(iv) *the affine cone over X is smooth away from the cone vertex.*

Proof See Exercise **??**. □

85: Add reference, if moved back into actually used text

Example 3.4.15 (The Cayley cubic surface)**.** Let $S \subset \mathbf{P}^3_{\mathbf{Q}}$ be the surface defined by the cubic equation

$$X_0X_1X_2 + X_0X_1X_3 + X_0X_2X_3 + X_1X_2X_3 = 0.$$

We compute the singular points of S using Theorem 3.4.14(iv). The Jacobian matrix of the given polynomial for the affine cone over S is the 1×4 matrix with entries

$$X_1X_2 + X_1X_3 + X_2X_3 \qquad X_0X_2 + X_0X_3 + X_2X_3$$
$$X_0X_1 + X_0X_3 + X_1X_3 \qquad X_0X_1 + X_0X_2 + X_1X_2.$$

The singular points of the affine cone over S are defined by the vanishing of these polynomials together with the defining equation of S. An explicit computation shows that the solutions to this system consists exactly of the quadruples with three vanishing entries. We deduce that the only singular points of S are the four points $[0,0,0,1], [0,0,1,0], [0,1,0,0], [1,0,0,0]$.

86: zero entries. A constant can not vanish...

87: technically, this does not follow from 3.4.14, as it does not state how singular points of X relate to the singular locus of the cone over X.

3.5 Change of base field

Recall that k is any field, $\bar{k}$ an algebraic closure of k, and $G_k = \mathrm{Aut}(\bar{k}/k)$. Let $\ell \supset k$ be a field extension and denote by $\bar{\ell}$ a fixed algebraic closure of ℓ.

Definition 3.5.1. Let $\ell \supset k$ be a field extension and let X be a projective algebraic set over k. The *base change* of X to ℓ is the projective algebraic set X_ℓ over ℓ consisting of the set $X(\bar{\ell})$, with ℓ as base field. If U is an open subset of

d: Add the statement that rational maps from regular varieties extend in codimension one; point out that birational morphisms induce an isomorphism with an open subset of the target whose complement has codimension at least two. Use this in invariance of Brauer groups under birational morphisms.

88: Should we talk about quasi-projective algebraic sets all the way and only define varieties after we defined morphisms?

X, then the *base change* of U to ℓ is the open subset $U(\bar{\ell})$ of X_ℓ, together with ℓ as base field.

Proposition 3.5.2. *Let X be a projective algebraic set over k; the dimension of the base change X_ℓ is the same as the dimension of X.*

89: why only for projective ones?

If X is a quasi-projective algebraic set over k, we denote by $\bar{X}$ the base change of X to $\bar{k}$.

90: Why not just for any algebraic variety?

Definition 3.5.3. Let $\mathscr{P}$ be a property of open subsets of projective algebraic sets over k and let X be an open subset of a projective algebraic set over k. The property $\mathscr{P}$ *holds geometrically* for X if $\mathscr{P}$ holds for $\bar{X}$.

91: Add definition of nice: smooth, projective, geometrically irreducible (geometrically reduced is implied by smooth); Also talk about finite extensions of ground field inside function field (Poonen, Prop. 2.2.19-2.2.20), and fact that on a nice variety, the ring of regular functions is just the ground field (see answer Zulip question Material week 6)

Thus, for example, X is *geometrically irreducible* if $\bar{X}$ is irreducible. For example, the affine variety $Z(x^2-12,\bar{\mathbf{Q}}) \subset \mathbf{A}^1_{\mathbf{Q}}$ is irreducible over $\mathbf{Q}$, but not geometrically irreducible.

If the characteristic of k is zero, then first-order properties hold geometrically if and only if they hold for the base change to any algebraically closed field containing k. This statement goes under the name of the Lefschetz principle, although in this form it is Tarski's result on quantifier elimination. As a consequence, for our purposes it is usually equivalent to check a property over $\bar{k}$ or over any algebraically closed field containing k. In particular, for varieties over $\mathbf{Q}$, we can typically check geometric properties over $\mathbf{C}$ instead of over $\bar{\mathbf{Q}}$, if we want.

92: From this line to the next seems old

irreducible components

inseparable extensions/smoothness, generators of radicals, comment about schemey base extension

properties that are stable under base change

being non-empty, being empty, reducibility, being rational (to be defined), being isomorphic to a fixed variety over k, having a dominant map to another thing, being affine, being projective (and their negations), being closed/open,

Is smoothness preserved under base change? (non-smoothness is not...) Is regularity?

3.5.1 Finite extensions and Galois actions

Remark 3.5.4. The group $\mathrm{Aut}(\ell/k)$ of automorphisms of ℓ that restrict to the identity on k acts coordinatewise on $\mathbf{A}^n(\ell)$. It also acts on $R_\ell = \ell[x_1,\ldots,x_n]$ by acting on the coefficients. For any $f \in R_\ell$ and $P \in \mathbf{A}^n(\ell)$ we have $(\sigma f)(\sigma P) = \sigma(f(P))$, so for any subset $S \subset R_\ell$ we have $P \in Z(S,\ell)$ if and only if $\sigma P \in Z(\sigma S,\ell)$.

Proposition 3.5.5. *Let V be an affine algebraic set over k and let $Z \subset V(\bar{k})$ be*

a set that is closed in the $\bar{k}$-Zariski topology. Then the closure of Z in V (in the k-Zariski topology) equals $\bigcup_{\sigma\in G_k}\sigma(Z)$.

Proof Let n be the integer for which V is a subset of $\mathbf{A}^n_k$. Since V is closed in $\mathbf{A}^n_k$, the closure of Z in V equals the closure in $\mathbf{A}^n_k$, so it suffices to prove the case $V=\mathbf{A}^n_k$. Let $\overline{Z}$ denote the closure of Z in the k-Zariski topology. By Remark 3.5.4, each $\sigma(Z)$ is contained in $\overline{Z}$, so it suffices to show that the complement of the union $\bigcup_{\sigma\in G_k}\sigma(Z)$ is contained in the complement of $\overline{Z}$.

Suppose $Q\in\mathbf{A}^n_k(\bar{k})$ is a point with $Q\notin\sigma(Z)$ for all $\sigma\in G_k$. Equivalently, $\sigma^{-1}Q\notin Z$ for all $\sigma\in G_k$. Since Q is defined over a finite extension of k, the set

$$S=\{\sigma^{-1}Q\,:\,\sigma\in G_k\}$$

is finite. Let $J\subset\bar{k}[x_1,\ldots,x_n]$ be an ideal with $Z=Z(J,\bar{k})$, which is a vector space over $\bar{k}$. For each point $R\in S$, we let A_R denote the subspace of J consisting of those functions that vanish at R. From $R\notin Z$, we conclude that A_R is a proper subspace of J. Since $\bar{k}$ is infinite, the vector space J is not the union of finitely many proper subspaces, so there exists a polynomial $f\in J$ with $f(R)\neq 0$ for all $R\in S$. This is essentially an easy application of the Prime Avoidance Theorem (Eisenbud, 1995, Section 3.2). We obtain $(\sigma f)(Q)=\sigma(f(\sigma^{-1}Q))\neq 0$ for all $\sigma\in G_k$.

Let $k'\subset\bar{k}$ be a finite normal extension of k containing all coefficients of f, and let k'_{s} denote the separable closure of k inside k'. Then k'_{s} is a finite Galois extension of k. Set $q=[k':k'_{\mathrm{s}}]$. Then we have $f^q\in k'_{\mathrm{s}}[x_1,\ldots,x_n]$, and we define

$$F=\prod_{\tau\in\mathrm{Gal}(k'_{\mathrm{s}}/k)}\tau(f^q).$$

Since F is invariant under $\mathrm{Gal}(k'_{\mathrm{s}}/k)$, its coefficients are contained in k. Because each $\tau\in\mathrm{Gal}(k'_{\mathrm{s}}/k)$ extends to an automorphism of $\bar{k}$, we have $(\tau f^q)(Q)\neq 0$ for all $\tau\in\mathrm{Gal}(k'_{\mathrm{s}}/k)$, so $F(Q)\neq 0$. As f divides F, the polynomial F vanishes on Z and hence on $\overline{Z}$, so Q does not lie in $\overline{Z}$. □

Corollary 3.5.6. *Let V be an affine algebraic set over k. Then the minimal closed subsets of V are exactly the orbits of G_k acting on $V(\bar{k})$.*

Proof A non-empty closed subset is a minimal closed subset if and only if it is the closure of any of its points, so this follows from Proposition 3.5.5. □

3.6 Reduction modulo a prime

Let k be a number field, and let X be an affine or projective variety over k. We would like to say what it means to reduce the variety X modulo a prime ideal $\mathfrak{p}$ of k. This is a rather subtle problem: if X is considered only up to isomorphism of varieties, then there is no well-defined "reduction" of X. However, if X is given a fixed embedding into affine or projective space, then we can indeed give a meaning to reduction modulo $\mathfrak{p}$.

93: R was a polynomial ring earlier!!!!

To put ourselves in a slightly more general context, for the remainder of this section, k will denote an arbitrary field; R will be a discrete valuation ring with field of fractions k and maximal ideal $\mathfrak{p}$; and $\mathbf{F}$ will be the residue field $R/\mathfrak{p}$. For example, if k is a number field and $\mathfrak{p}$ a prime ideal of the ring of integers of k, then we can take $R \subset k$ to be the subring of elements having non-negative valuation at $\mathfrak{p}$. If a is an element of R, then $\tilde{a}$ will denote its image in $\mathbf{F}$.

94: really semi-colons?

Before thinking about varieties, we consider points. The situation differs for affine and projective space. If $P \in \mathbf{A}^n(k)$ is a point with coordinates $(a_1, \ldots, a_n)$, then it only makes sense to reduce P modulo $\mathfrak{p}$ if all the coordinates actually lie in R; in that case, the point $\tilde{P} = (\tilde{a}_1, \ldots, \tilde{a}_n) \in \mathbf{A}^n(\mathbf{F})$ is what we will call the "reduction of P" modulo $\mathfrak{p}$. So reduction modulo $\mathfrak{p}$ is only defined on the subset $\mathbf{A}^n(R) \subset \mathbf{A}^n(k)$ consisting of points having coordinates in R. On the other hand, in projective space, every point can be reduced modulo $\mathfrak{p}$, as follows. Let $P \in \mathbf{P}^n(k)$ be a point with projective coordinates $(a_0 : \cdots : a_n)$. By multiplying through by an appropriate power of a uniformising element, we can ensure that all of $a_0, \ldots, a_n$ lie in R, and not all of them lie in $\mathfrak{p}$. Then reducing modulo $\mathfrak{p}$ gives a well-defined point $\tilde{P} = (\tilde{a}_0 : \cdots : \tilde{a}_n) \in \mathbf{P}^n(\mathbf{F})$. In this way we obtain a reduction map $\mathbf{P}^n(k) \to \mathbf{P}^n(\mathbf{F})$. (Scheme enthusiasts can see this as an example of the "valuative criterion of properness": every k-point of $\mathbf{P}^n$ extends to an R-point.)

Similarly, we can reduce points over extension fields. Suppose that $R \subset S$ is an extension of discrete valuation rings, and write ℓ for the field of fractions of S and $\mathbf{F}'$ for the residue field. As above, we obtain reduction maps $\mathbf{A}^n(S) \to \mathbf{A}^n(\mathbf{F}')$ and $\mathbf{P}^n(\ell) \to \mathbf{P}^n(\mathbf{F}')$. Beware, however, that these reduction maps do not depend only on ℓ, but also on the chosen extension of the valuation from k to ℓ corresponding to the valuation ring S. In particular, there is no natural map $\mathbf{P}^n(\bar{k}) \to \mathbf{P}^n(\bar{\mathbf{F}})$; rather, there is one such map for each way of extending the valuation to $\bar{k}$.

Now consider varieties. An affine or projective variety is a set of points defined by some algebraic equations. To define the "reduction" of the variety modulo $\mathfrak{p}$, there are two obvious choices: either reduce the points modulo $\mathfrak{p}$, or reduce the equations modulo $\mathfrak{p}$. It turns out that these give the same result.

However, we need to be a little careful when using defining equations, as shows by the following examples.

Example 3.6.1. Let $X \subset \mathbf{A}^1_{\mathbf{Q}}$ be the point with coordinate 1. Let us try to find the reduction of X modulo 5.

- One possible defining polynomial for X is the polynomial $x-1 \in \mathbf{Q}[x]$. Reducing this polynomial modulo 5 gives $x-1 \in \mathbf{F}_5[x]$, defining the variety consisting of the single point with coordinate 1 in $\mathbf{A}^1_{\mathbf{F}_5}$.
- An alternative defining polynomial for X is the polynomial $5x-5 \in \mathbf{Q}[x]$. Reducing this modulo 5 gives $0 \in \mathbf{F}_5[x]$, which vanishes on the whole of $\mathbf{A}^1_{\mathbf{F}_5}$.
- A third possible defining polynomial for X is $(x-1)/5$. Since the coefficients of this polynomial have negative valuation at 5, we don't even know how to reduce this polynomial modulo 5.

It is clear that, in this example, the first choice of defining polynomial is the "right" one to use for defining the reduction of X modulo 5. Because the ideal $I(X,\mathbf{Q})$ is principal, all choices for a defining polynomial are related by multiplying by an element of $\mathbf{Q}$. For varieties defined by more than one polynomial, the situation is more complicated, as illustrated by the following example.

Example 3.6.2. Let $X \subset \mathbf{A}^2_{\mathbf{Q}}$ be the point $(0,0)$. Let us try to find the reduction of X modulo 5.

- One possible set of defining polynomials is $\{x,y\} \subset \mathbf{Q}[x,y]$. Reducing these modulo 5 gives $\{x,y\} \subset \mathbf{F}_5[x,y]$, defining the single point $(0,0) \in \mathbf{A}^2_{\mathbf{F}_5}$.
- Another set of defining polynomials is $\{x,x+5y\} \subset \mathbf{Q}[x,y]$. Reducing either of these polynomials modulo 5 gives $x \in \mathbf{F}_5[x,y]$, so the vanishing set of their reductions is the whole y-axis in $\mathbf{A}^2_{\mathbf{F}_5}$.

Again, the first pair of defining polynomials gives the "right" answer. However, if we were handed the second pair of defining polynomials, then we would have to do a little work to turn them into a set of polynomials giving the "right" answer.

For the purposes of defining the reduction of a variety, we can simply use *all* the possible defining polynomials at once, giving rise to the following definition.

Definition 3.6.3. Let $X \subset \mathbf{A}^n_k$ be an algebraic set with ideal $I(X,k) \subset k[x_1,\ldots,x_n]$. Define the ideal $\tilde{I} \subset \mathbf{F}[x_1,\ldots,x_n]$ to be the image of $I(X,k) \cap R[x_1,\ldots,x_n]$ under

the natural map $R[x_1,\dots,x_n] \to \mathbf{F}[x_1,\dots,x_n]$. The *reduction of X modulo* $\mathfrak{p}$ is the algebraic set $\tilde{X} \subset \mathbf{A}^n_{\mathbf{F}}$ defined by the ideal $\tilde{I}$.

Similarly, if $X \subset \mathbf{P}^n_k$ is an algebraic set with ideal $I(X,k) \subset k[x_0,\dots,x_n]$, then the *reduction of X modulo* $\mathfrak{p}$ is the algebraic set $\tilde{X} \subset \mathbf{P}^n_{\mathbf{F}}$ defined by the ideal that is the image of $I(X,k) \cap R[x_0,\dots,x_n]$ under the natural map $R[x_0,\dots,x_n] \to \mathbf{F}[x_0,\dots,x_n]$.

In other words, $\tilde{X}$ is the common zero set of the reductions modulo $\mathfrak{p}$ of all polynomials vanishing on X and having coefficients in R. (In scheme-theoretic terms, $\tilde{X}$ is the special fibre of the closure of X in $\mathbf{A}^n_R$ or $\mathbf{P}^n_R$.) This definition is not immediately useful for computation: given a finite set of defining polynomials for X, it does not tell us how to compute a finite set of defining polynomials for $\tilde{X}$.

Lemma 3.6.4. *Let $f_1,\dots,f_r \in R[x_1,\dots,x_n]$ be polynomials, and let I and J be the ideals generated by $f_1,\dots,f_r$ in the rings $k[x_1,\dots,x_n]$ and $R[x_1,\dots,x_n]$ respectively. Let $\pi \in R$ be a generator for the prime ideal $\mathfrak{p}$. Then the ideal $I \cap R[x_1,\dots,x_n]$ is equal to the* saturation

$$(J:\pi^\infty) = \{f \in R[x_1,\dots,x_n] \mid \textit{there exists an integer } s \geq 0 \textit{ such that } \pi^s f \in J\}.$$

Proof Suppose first that f lies in $(J:\pi^\infty)$. Then, for a suitable $s \geq 0$, we have $\pi^s f = \sum_i a_i f_i$ for some $a_1,\dots,a_r \in R[x_1,\dots,x_n]$; dividing through by π^s shows that f lies in I, as claimed. On the other hand, suppose that $f \in R[x_1,\dots,x_n]$ lies in I; then we can write $f = \sum_i b_i f_i$ for some $b_1,\dots,b_r \in k[x_1,\dots,x_n]$, and clearing denominators shows that $\pi^s f$ lies in J for some $s \geq 0$. □

Given $f_1,\dots,f_r$ as in the lemma, there is an algorithm to compute generators for the saturation $(J:\pi^\infty)$. This gives a way to compute defining polynomials for $\tilde{X}$, given defining polynomials for X.

95: (see ?)

Remark 3.6.5. The case when X is a hypersurface, defined by a single polynomial f, is particularly simple. After multiplying by a suitable power of π, we can ensure that the coefficients of f all lie in R, but do not all lie in $\mathfrak{p}$; then $\tilde{X}$ is defined by the reduction of f modulo $\mathfrak{p}$.

There is another trap for the unwary, illustrated by the following example.

Example 3.6.6. Consider the variety $X \subset \mathbf{A}^1_{\mathbf{Q}}$ consisting of the two points $\{0,5\}$. A generator for the ideal $I(X,\mathbf{Q})$ is the polynomial $f = x(x-5)$. Let us try to find the reduction of X modulo 5. The polynomial f has integer coefficients, not all divisible by 5, and so the reduction $\tilde{X}$ is defined by $\tilde{f} = x^2 \in \mathbf{F}_5[x]$ and consists of the single point $0 \in \mathbf{A}^1(\mathbf{F}_5)$. However, $\tilde{f}$ does not generate the ideal $I(\tilde{X},\mathbf{F}_5) = (x)$. The reason is not that f was a poor choice of generator: it is that the ideal $\tilde{I}$ in Definition 3.6.3 is not radical.

This is an example in which working with varieties has genuine disadvantages compared to working with schemes. As a scheme, the reduction of X modulo 5 is not reduced; but, as a variety, our reduction $\tilde{X}$ is a perfectly respectable smooth variety over $\mathbf{F}_5$, consisting of a single point. When dealing with reductions of varieties, we will usually want to require that this phenomenon does not happen: explicitly, that there is a set of generators for $I(X,k)$ whose reductions generate $I(\tilde{X},\mathbf{F})$.

We now look at the relationship between reducing the points of a variety modulo a prime, and reducing the defining equations. If $X \subset \mathbf{A}^n_k$ is an affine variety, and $P \in X(k)$ is a point having coordinates in R, then it is easy to check that the reduction $\tilde{P} \in \mathbf{A}^n(\mathbf{F})$, as defined above, lies in $\tilde{X}(\mathbf{F})$. A similar remark holds for projective varieties: if $X \subset \mathbf{P}^n_k$ is a projective variety, we obtain a reduction map $X(k) \to \tilde{X}(\mathbf{F})$.

The algebraic set $\tilde{X}$ is defined by its points over an algebraic closure $\bar{\mathbf{F}}$ of $\mathbf{F}$. Reducing points of $X(k)$ is only ever going to produce points of $\tilde{X}(\mathbf{F})$, which by themselves are usually not enough to characterise $\tilde{X}$. However, the following lemma says that the $\bar{\mathbf{F}}$-points of $\tilde{X}$ are precisely those points obtained by reducing $\bar{k}$-points of X.

Lemma 3.6.7. *Let X be an affine or projective variety over k, and let $\tilde{X}$ be the reduction of X modulo $\mathfrak{p}$. Let $\mathbf{F}'$ be a finite extension of $\mathbf{F}$ contained in a fixed algebraic closure $\bar{\mathbf{F}}$, and let $\tilde{P} \in \tilde{X}(\mathbf{F}')$ be a point. Then there exist a finite extension ℓ/k; a discrete valuation on ℓ, extending that on k, with residue field $\mathbf{F}'$; and a point $P \in X(\ell)$ reducing to $\tilde{P}$.*

96: Why contained in a fixed $\bar{\mathbf{F}}'$? Also, really semi-colons?

Proof Exercise □

97: Prove this ourselves!

We conclude by showing that, for projective varieties, reducing modulo $\mathfrak{p}$ preserves the dimension.

Lemma 3.6.8. *Let $X \subset \mathbf{P}^n_k$ be a projective variety, and let $\tilde{X} \subset \mathbf{P}^n_{\mathbf{F}}$ be the reduction of X modulo $\mathfrak{p}$. Then $\tilde{X}$ has the same dimension as X.*

Proof We will make use of the Hilbert polynomial (see Hartshorne, 1977, Chapter I, Theorem 7.5). Let $J \subset R[x_0,\ldots,x_n]$ be the ideal $R[x_0,\ldots,x_n] \cap I(X,k)$. This is a homogeneous ideal not containing any non-zero element of R. Denote by $\tilde{J}$ the image of J in $\mathbf{F}[x_0,\ldots,x_n]$. The ideal $\tilde{J}$ cuts out, by definition, the algebraic set $\tilde{X}$, and so the Nullstellensatz gives $I(\tilde{X},\mathbf{F}) = \sqrt{\tilde{J}}$. The quotient by J satisfies

$$(R[x_0,\ldots,x_n]/J) \otimes_R k \cong \Gamma(X)$$
$$(R[x_0,\ldots,x_n]/J) \otimes_R \mathbf{F} \cong \mathbf{F}[x_0,\ldots,x_n]/\tilde{J}.$$

These are all graded rings, and the above isomorphisms respect the gradings. Each graded piece of $R[x_0,\dots,x_n]/J$ is a finitely generated, torsion-free R-module, and is therefore free; so the corresponding graded pieces of $\Gamma(X)$ and $\mathbf{F}[x_0,\dots,x_n]/\tilde{J}$, which are obtained by taking the tensor product of the same free R-module with k and $\mathbf{F}$ respectively, have the same dimension. Therefore $\Gamma(X)$ and $\mathbf{F}[x_0,\dots,x_n]/\tilde{J}$ have the same Hilbert polynomial and hence the same dimension. The ring $\Gamma(\tilde{X})$ is the quotient of $\mathbf{F}[x_0,\dots,x_n]/\tilde{J}$ by its nilradical, so has the same dimension (the quotient map induces a bijection between the sets of prime ideals of the two rings). Therefore X and $\tilde{X}$ have the same dimension. □

Remark 3.6.9. The corresponding result for affine varieties does not hold. For example, the variety $X \subset \mathbf{A}^1_{\mathbf{Q}}$ defined by $5x = 1$ gives the empty variety when reduced modulo 5. However, it turns out that this is the only thing that can go wrong: as long as the reduction $\tilde{X}$ is non-empty, then it (and indeed each of its components) has the same dimension as X. See Stacks Project (2015, Tag 00QK).

98: From this line to the next seems old

This chapter will contain a summary of what we assume in the way of geometry. In particular, we should include facts about varieties over non-algebraically closed base fields, which are often tricky to track down in the standard textbooks.

- Varieties à la Silverman. A variety comes equipped with a base field.
- Coordinate rings of affine varieties; function fields; local rings.
- Base change. Think about points over fields, especially reducing points modulo primes.
- Irreducibility; geometrically irreducible iff base field is algebraically closed in function field.
- Galois actions on points, subvarieties, function fields etc.
- Divisors, local rings, effects of base change and completion. Residue field at a point.

Exercises

3.1 Prove Lemma 3.1.4.

3.2 Prove Lemma 3.1.7.

3.3 Prove Lemma 3.1.16.

3.4 Show that, if $f \in k[x_1,\dots,x_n]$ is irreducible, then the affine algebraic set $V_k(f)$ is irreducible.

3.5 Show that if X is any topological space and $Y \subset X$ is an irreducible subspace, then the closure $\overline{Y}$ is also irreducible.

4

The Picard group

Given a set of polynomial equations defined over $\mathbf{Q}$, we aim to study their rational solutions by considering the geometry of the variety X which they define. One geometric invariant which has a great effect on the arithmetic is the Picard group of X, and we will devote some time to the general definition of the Picard group and to understanding its structure for some specific surfaces.

4.1 Definition of the Picard group

One way to see the construction of the Picard group is to try to mimic the construction of the homology groups of a manifold. In that case, we form a free group of "cycles" and take the quotient by a subgroup of "boundaries". In the case of algebraic varieties, it is reasonable to replace the cycles by algebraic subvarieties. However, there is nothing immediately obvious to replace the boundaries, since a subvariety does not have a boundary. Many ways have been devised to solve this problem in arbitrary codimension, but in codimension one there is one which is particularly straightforward to define.

In what follows, X will be a *smooth* irreducible variety over a field k. While the definitions will be valid for any field k, it may be easier at a first reading to imagine k algebraically closed.

Definition 4.1.1. A *prime divisor* on a smooth variety X over a field k is an irreducible closed subvariety $Z \subset X$ of codimension one, also defined over k. A *divisor* is a finite formal linear combination $D = \sum_i n_i Z_i$, $n_i \in \mathbf{Z}$, of prime divisors. The group of divisors on X, which is the free abelian group on the prime divisors, is denoted $\operatorname{Div} X$.

Remark 4.1.2. A prime divisor is not required to be nonsingular.

Remark 4.1.3. If X is a variety over a field k which is not algebraically closed, then a prime divisor does not have to be geometrically irreducible. For example, the 0-dimensional variety $\{\sqrt{2}, -\sqrt{2}\} \subset \mathbf{A}^1_{\mathbf{Q}}$, defined by the polynomial $x^2 - 2$, is irreducible as a variety over $\mathbf{Q}$, and is therefore a prime divisor on $\mathbf{A}^1_{\mathbf{Q}}$.

d: Make sure that "geometrically ..." is defined.

Definition 4.1.4. A divisor D is *effective* if it is a non-negative linear combination of prime divisors, i.e. if D can be written as $D_1 + \cdots + D_r$, with $D_1, \ldots, D_r$ prime divisors.

Definition 4.1.5. The *support* of a divisor D, written $\operatorname{supp} D$, is the closed subset of X defined as follows: write $D = \sum_i n_i Z_i$ with the n_i non-zero integers and the Z_i distinct prime divisors; then $\operatorname{supp} D = \bigcup_i Z_i$.

The idea is that a divisor looks, at least locally, like the set of zeros and poles of a rational function. Let us make this precise. For any prime divisor Z on X, the local ring $\mathscr{O}_{X,Z}$ is regular (see **??**) and one-dimensional (because Z has codimension one in X, and the prime ideals of $\mathscr{O}_{X,Z}$ correspond to subvarieties of X containing Z.). It is therefore a discrete valuation ring, so there is an associated valuation $v_Z \colon \kappa(X)^\times \to \mathbf{Z}$. Given a rational function $f \in \kappa(X)^\times$, we call the integer $v_Z(f)$ the *valuation* or the *order* of f along Z. Using valuations we can associate to any non-zero rational function on X a divisor, which encapsulates all the infomation about the zeros and poles of f.

Definition 4.1.6. Let $f \in \kappa(X)^\times$ be a rational function on X. We define the *divisor of* f to be

$$\operatorname{div} f = (f) = \sum_Z v_Z(f) Z$$

where the sum is taken over all prime divisors $Z \subset X$.

Remark 4.1.7. This sum is finite – that is, $v_Z(f) = 0$ for all but finitely many prime divisors Z. To see this, suppose that X is embedded in projective space $\mathbf{P}^N$. By definition, we can write f as a quotient of two polynomials not vanishing on X; they are each zero only on a closed subset of codimension one in X, which is therefore the union of finitely many prime divisors.

Proposition 4.1.8. *Let X be a smooth variety and let f and g be non-zero rational functions on X.*

(i) *If the divisor (f) is effective, then f is a regular function on X, that is, $f \in \mathscr{O}(X)$.*
(ii) *If the divisor (f) is 0, then f is an invertible regular function on X, that is, $f \in \mathscr{O}(X)^\times$.*

(iii) *If X is projective and the divisor (f) is 0, then f is constant.*

(iv) *If X is projective and the divisors (f) and (g) coincide, then there is a constant $a \in k^\times$ such that $f = ag$.*

Proof We first prove (i). Since being regular is a local condition, we may check it on an affine neighbourhood of each point of X; so assume that X is affine. Then we can identify $\mathscr{O}(X)$ with the coordinate ring $A(X)$, and every divisor $D \subset X$ corresponds to the prime ideal $I(D) \subset A(X)$ of height one. (Recall that the *height* of a prime ideal $\mathfrak{p}$ in a ring R is the maximal n for which there exists a chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$ of prime ideals in R. By the correspondence between between prime ideals and subvarieties, the height of a prime ideal is equal to the codimension of the corresponding subvariety.) Since X is a variety, $A(X)$ is a Noetherian integral domain; moreover, since X is smooth, $A(X)$ is regular and, in particular, normal. The assumption that f is effective means precisely that f lies in $\mathscr{O}_{X,D}$ for all divisors D of X. The result then follows from Hartshorne (1977, Proposition 6.3A) which states that, for a normal Noetherian domain A, we have $A = \cap_{\mathfrak{p}} A_{\mathfrak{p}}$, where the intersection is over all prime ideals of height one and takes place inside the field of fractions of A.

99: Give a reference for this.

For (ii), apply (i) to both f and f^{-1}. Statement (iii) follows from the fact that the only regular functions on a projective variety are constant (Chapter I, Theorem 3.4(a) Hartshorne, 1977, see). Statement (iv) follows by applying (iii) to the quotient f/g. □

Definition 4.1.9. A divisor of the form (f) for some $f \in \kappa(X)^\times$ is called a *principal divisor*. The subgroup of $\operatorname{Div} X$ consisting of the principal divisors is denoted by $\operatorname{Princ} X$.

Definition 4.1.10. Two divisors $D, D' \in \operatorname{Div} X$ are *linearly equivalent*, written $D \sim D'$, if their difference $D - D'$ is principal.

Example 4.1.11. Suppose that D and D' are two linearly equivalent, non-zero, effective divisors, whose supports have no component in common. Then, by definition, there is a function $f \in \kappa(X)^\times$ such that $(f) = D - D'$. Now the function f defines a rational map from X to $\mathbf{P}^1_k$, such that $f^{-1}(0) = D$ and $f^{-1}(\infty) = D'$. The other fibres of this rational map are all effective divisors which are also linearly equivalent to D, so give a "family" of effective divisors "moving" from D to D'.

d: Try to say something about analogy with homology?

We can now define the Picard group of a smooth variety.

Definition 4.1.12. Let X be a smooth variety. The *Picard group* of X is the

quotient group

$$\operatorname{Pic} X = \frac{\operatorname{Div} X}{\operatorname{Princ} X}.$$

Example 4.1.13. $\operatorname{Pic} \mathbf{A}^n = 0$ for any $n \geq 0$. To prove this, we must show that any irreducible subvariety of codimension one in $\mathbf{A}^n$ may be defined by a single polynomial. This reduces to the algebraic fact that, in a unique factorisation domain, any prime ideal of height one is principal. For a proof, see Eisenbud (1995, Corollary 10.6).

The same reasoning as in Example 4.1.13 allows us to prove some useful local results about divisors.

Proposition 4.1.14. *Let X be a smooth variety, let P be a point of X and let D be a divisor on X. Then D is* locally principal *at P: there exist a non-empty open neighbourhood $U \subset X$ of P and a function $f \in \kappa(X)^\times$ such that $D = (f)$, as divisors on U.*

Proof It is sufficient to prove the statement for prime divisors D, for then it follows for general divisors just by taking products of the relevant functions. If P does not lie in $\operatorname{supp} D$, then the statement is trivial: we may take $f = 1$.

Suppose that P does lie in $\operatorname{supp} D$. After replacing X by an affine neighbourhood of P, we may assume that X is affine, with coordinate ring $A(X)$. Since D has codimension one in X, the associated ideal $I(D) \subset A(X)$ has height one. By Proposition 3.3.20, the local ring $\mathscr{O}_{X,P}$ can be identified with the localisation of $A(X)$ at the maximal ideal $I(P)$. The natural bijection between ideals of $\mathscr{O}_{X,P}$ and ideals of $A(X)$ contained in $I(P)$ (see **?**) shows that the ideal $I(D)\mathscr{O}_{X,P}$ has height one. More generally, this shows that prime ideals of height one in $\mathscr{O}_{X,P}$ correspond to prime divisors of X passing through P.

Since X is smooth, $\mathscr{O}_{X,P}$ is regular (see **??**), and every regular local ring is a unique factorisation domain (**?**). Therefore $I(D)\mathscr{O}_{X,P}$ is principal by Eisenbud (1995, Corollary 10.6); let $f \in \mathscr{O}_{X,P}$ be a generator. Then f also generates $I(D)\mathscr{O}_{X,D}$, so we have $v_D(f) = 1$. Moreover, f is not contained in any other height-one prime ideal of $\mathscr{O}_{X,P}$ since otherwise that ideal would contain $I(D)\mathscr{O}_{X,P}$, contradicting that it also has height one. In other words, f does not vanish on any prime divisors passing through P apart from D. Now take U to be an open neighbourhood of P on which f is regular, and not containing any prime divisor apart from D at which f has a zero or a pole. □

100: Read this through and add references

Locally principal divisors are known as *Cartier divisors*. Proposition 4.1.14 states that, on a smooth variety, every divisor is Cartier. The following is a useful consequence.

Corollary 4.1.15. *Let D be a divisor on a smooth variety X and let P be a point of X. Then D is linearly equivalent to a divisor D' with $P \notin \operatorname{supp} D'$.*

Proof Indeed, Proposition 4.1.14 gives a non-empty open neighbourhood U of P and a function $f \in \kappa(X)$ such that (f) and D have the same restriction to U. Therefore $D' = D - (f)$ is a divisor linearly equivalent to D and with support avoiding U and hence P. □

Of course, the divisor D' in Corollary 4.1.15 need not be effective, even if D is effective.

As a consequence of Proposition 4.1.14, we can define the inverse image of a divisor under a morphism. Let $\phi\colon Y \to X$ be a morphism of varieties, and let D be a divisor on Y. Suppose that the image of ϕ is not contained in the support of D. Then we can define $\phi^*(D) \in \operatorname{Div} Y$ by pulling back functions that locally define D, as follows. By Proposition 4.1.14, there exist an open cover $\{U_i\}$ of X and functions $f_i \in \kappa(X)$ such that, for all i, the restriction of D to U_i coincides with the divisor (f_i). Moreover, for all pairs i, j, the divisors (f_i) and (f_j) coincide on $U_i \cap U_j$ (since they both coincide with D), so Proposition 4.1.8 shows $f_i/f_j \in \mathscr{O}(U_i \cap U_j)^\times$. (In Hartshorne (1977, Section II.6), a Cartier divisor is defined to be given by such a collection $\{U_i, f_i\}$.)

The assumption that $\phi(Y)$ is not contained in the support of D means that each f_i lies in $\mathscr{O}^\times_{X,\phi(Y)}$, so by Proposition 3.3.19 we can pull f_i back to $\phi^* f_i \in \kappa(Y)$. We obtain an open cover $\{V_i = \phi^{-1}(U_i)\}$ of Y and $f_i \in \kappa(Y)$ satisfying $f_i/f_j \in \mathscr{O}(V_i \cap V_j)^\times$ for all i, j. These data define a divisor on Y: for every prime divisor $Z \subset Y$, define $n_Z \in \mathbf{Z}$ by choosing i such that V_i meets Z, and setting $n_Z = v_Z(f_i)$. The condition $f_i/f_j \in \mathscr{O}(V_i \cap V_j)^\times$ shows that n_Z does not depend on the choice of i. Now define $\phi^*(D) = \sum n_Z Z$, the sum being over all prime divisors Z on Y.

Remark 4.1.16. It is easy to check that pulling back divisors respects linear equivalence: if D_1 and D_2 are linearly equivalent divisors on X, then $\phi^*(D_1)$ and $\phi^*(D_2)$ are linearly equivalent on Y. This allows us to define a homomorphism $\phi^*\colon \operatorname{Pic} X \to \operatorname{Pic} Y$ as follows: if $\phi(Y)$ is not contained in $\operatorname{supp} D$, then define $\phi^*[D] = [\phi^* D]$; otherwise, choose and point in $\phi(Y)$ and use Corollary 4.1.15 to replace D by a linearly equivalent divisor avoiding P, whose support therefore does not contain $\phi(Y)$.

An important case of this definition is when Y is a closed subvariety of X. In this case, when we talk about the *intersection* with Y of a divisor D on X, or the *restriction* of D to Y, we means its pullback $\phi^*(D)$ under the inclusion morphism of $\phi\colon Y \to X$.

Example 4.1.17. Any plane in $\mathbf{P}^3$ is a divisor on $\mathbf{P}^3$. Given a surface $X \subset \mathbf{P}^3$,

a *plane section* is a divisor on X obtained as the restriction of a plane not containing X. Any two planes in $\mathbf{P}^3$ are linearly equivalent divisors: if Π_1 and Π_2 are planes in $\mathbf{P}^3$ defined by linear forms l_1 and l_2 respectively, then the rational function l_1/l_2 has divisor $\Pi_1 - \Pi_2$. It follows that any two plane sections of X are also linearly equivalent.

More generally, let $X \subseteq \mathbf{P}^n$ be any projective variety. For the same reason, any two hyperplane sections of X are linearly equivalent. We will often talk of "the" hyperplane section to mean the class in $\operatorname{Pic} X$ of a hyperplane section.

Remark 4.1.18. Bertini's Theorem (Hartshorne, 1977, Chapter II, Theorem 8.18) shows that, if X is smooth and k algebraically closed, then almost all hyperplane sections of X are nonsingular. Generalisations of this result can give many consequences of the form "Any divisor D is equivalent to a difference $A - B$ with A, B effective and *special*", where *special* can mean, for example: smooth; avoiding a given finite set of points; transverse to a given finite set of subvarieties; and so on.

d: "Algebraically closed" can be replaced by "infinite": do we care?

Exercise 4.1.19. Let Z be a prime divisor in a smooth variety X, and let U denote the complement $X \smallsetminus Z$. Show that the sequence

$$\mathbf{Z} \to \operatorname{Pic} X \to \operatorname{Pic} U \to 0,$$

where the first map is $1 \mapsto Z$ and the second $D \mapsto D \cap U$, is exact.

Exercise 4.1.20. Use the result of Exercise 4.1.19 to show that $\operatorname{Pic} \mathbf{P}^n \cong \mathbf{Z}$, for any positive integer n.

On a smooth curve, a divisor is a formal sum of zero-dimensional subvarieties, and it is straightforward to define the degree of a divisor.

Definition 4.1.21. Let X be a smooth curve over a field k, and let Z be a prime divisor on X. The residue field $\kappa(Z)$ is a finite extension of k, and we define the *degree* of Z to be $\deg(Z) = [\kappa(Z) : k]$. For a general divisor $D = \sum_i n_i Z_i$ on X, we define $\deg(D) = \sum_i n_i \deg(Z_i)$.

If k is algebraically closed, then we have $\deg(Z_i) = 1$ for all i, so the formula reduces to $\deg(D) = \sum_i n_i$.

Example 4.1.22. Take $X = \mathbf{A}^1_{\mathbf{Q}}$. For the prime divisor $Z_1 = \{0\}$, we have $\kappa(Z_1) = \mathbf{Q}$ and so $\deg(Z_1) = 1$. For the prime divisor $Z_2 = \{\sqrt{2}, -\sqrt{2}\}$ of Remark 4.1.3, we have $\kappa(Z_2) = \mathbf{Q}(\sqrt{2})$ and so $\deg(Z_2) = 2$.

Proposition 4.1.23. *Let X be a smooth, projective curve over a field k. For any function $f \in \kappa(X)$, the divisor (f) has degree zero. Thus there is a well-defined degree map* $\deg\colon \operatorname{Pic} X \to \mathbf{Z}$.

Proof See Hartshorne (1977, II, Corollary 6.10) and either observe that the proof there works over arbitrary fields, or use Exercise 4.2.3 below to pass to an algebraic closure of k. □

Remark 4.1.24. We have been assuming throughout that X is a smooth variety. For a general (not necessarily smooth) variety X, various terms that we have been using refer to slightly different things. Definition 4.1.1 defines a *Weil divisor*, and a Weil divisor is not necessarily locally principal. As long as the local ring at every Weil divisor is a DVR (which is, for example, the case if X is normal), then we can define the divisor of a rational function, and so define linear equivalence of Weil divisors. This gives a group called the *Weil divisor class group*. The Picard group, on the other hand, is in general defined as the group of isomorphism classes of line bundles on X. For an irreducible normal variety, the Picard group is isomorphic to the group of Cartier divisors modulo linear equivalence. This is equal to the Weil divisor class group if X is locally factorial and, in particular, if X is smooth. For a thorough treatment of these ideas, see Section II.6 of Hartshorne (1977).

4.2 Change of base field

Let X be a smooth, geometrically irreducible variety over a field k, and let ℓ/k be a field extension. The relationship between $\operatorname{Pic} X$ and $\operatorname{Pic} X_\ell$ is subtle; in this section we gather some results about it. In the case of a Galois extension, we will be able to prove some of these results using cohomology in Chapter 14.

By definition, we have

$$\operatorname{Pic} X = \frac{\operatorname{Div} X}{\operatorname{Princ} X} = \frac{\text{Divisors on } X \text{ defined over } k}{\text{Divisors of functions defined over } k}$$

and

$$\operatorname{Pic} X_\ell = \frac{\operatorname{Div} X_\ell}{\operatorname{Princ} X_\ell} = \frac{\text{Divisors on } X \text{ defined over } \ell}{\text{Divisors of functions defined over } \ell}.$$

Given a prime divisor Z on X, we can obtain a divisor on X_ℓ as follows. The base change Z_ℓ is a closed subset of codimension 1 in X_ℓ, so decomposes as a finite union of irreducible components that are prime divisors: $Z_\ell = \bigcup_i Z_i$. Now let $t \in \mathscr{O}_{X,Z}$ be a uniformising element, and define $D_Z = \sum_i v_{Z_i}(t) Z_i$. The map sending each Z to the corresponding D_Z extends to a homomorphism from $\operatorname{Div} X$ to $\operatorname{Div} X_\ell$, which is injective since Z is uniquely determined as the Zariski closure over k of each Z_i. This allows us to consider $\operatorname{Div} X$ as a subgroup of $\operatorname{Div} X_\ell$.

Example 4.2.1. Take $X = \mathbf{A}^1_{\mathbf{Q}}$ and let Z be the prime divisor $\{\sqrt{2}, -\sqrt{2}\}$ of Remark 4.1.3. Take $\ell = \mathbf{Q}(\sqrt{2})$. The base change Z_ℓ decomposes into $Z_1 = \{\sqrt{2}\}$ and $Z_2 = \{\sqrt{2}\}$. The function $t = x^2 - 2$ is a uniformising element in $\mathscr{O}_{X,Z}$. On X_ℓ we have $v_{Z_1}(t) = v_{Z_2}(t) = 1$, and so the image of Z in $\operatorname{Div} X_\ell$ is $Z_1 + Z_2$.

Remark 4.2.2. If ℓ/k is separable, then we have $v_{Z_i}(t) = 1$ for all i; we prove the important case, when ℓ/k is a finite separable extension. Write $\ell \cong k[x]/(f)$ and $K = \kappa(Z)$. By **?**, the ring $\mathscr{O}_{X,Z} \otimes_k \ell$ is isomorphic to the product of the rings $\mathscr{O}_{X_\ell,Z_i}$. Consider the ring

$$K[x]/(f) = K \otimes_k \ell = \mathscr{O}_{X,Z}/(t) \otimes_k \ell = \prod_i \mathscr{O}_{X_\ell,Z_i}/(t).$$

The polynomial f is separable over k, hence also over K; so this ring is a product of field extensions of K. In particular, this means that t is a uniformising element in each $\mathscr{O}_{X_\ell,Z_i}$.

Exercise 4.2.3. If X is a curve, show that the map $\operatorname{Div} X \to \operatorname{Div} X_\ell$ preserves degree.

Exercise 4.2.4. Show that the map on divisor groups defined above is compatible with the natural map on function fields, that is, the diagram

$$\begin{array}{ccc} \kappa(X) & \xrightarrow{\text{div}} & \operatorname{Div} X \\ \downarrow & & \downarrow \\ \kappa(X_\ell) & \xrightarrow{\text{div}} & \operatorname{Div} X_\ell \end{array}$$

commutes.

It follows that there is an induced homomorphism $\operatorname{Pic} X \to \operatorname{Pic} X_\ell$.

Suppose that ℓ/k is a (possibly infinite) Galois extension. The Galois group $G = \operatorname{Gal}(\ell/k)$ acts on $\operatorname{Div} X_\ell$ and compatibly on $\kappa(X_\ell)$, inducing an action on $\operatorname{Pic} X_\ell$. The image of i lies in the Galois-fixed subgroup $(\operatorname{Pic} X_\ell)^G$.

Theorem 4.2.5. *Let ℓ/k be a Galois extension of fields, write $G = \operatorname{Gal}(\ell/k)$, and let X be a variety defined over k. Let $i\colon \operatorname{Pic} X \to \operatorname{Pic} X_\ell$ be the natural homomorphism defined above.*

(i) $\operatorname{Div} X = (\operatorname{Div} X_\ell)^G$, *that is, a divisor on X_ℓ is defined over k if and only if it is fixed by the Galois action.*
(ii) *If X is a projective variety, then i is injective.*
(iii) *If $X(k)$ is non-empty then i gives an surjection from* $\operatorname{Pic} X$ *to* $(\operatorname{Pic} X_\ell)^G$.

(iv) *More generally, if k is a number field and X has points everywhere locally, that is, $X(k_v) \neq \emptyset$ for all places v of k, then again $i\colon \operatorname{Pic} X \to (\operatorname{Pic} X_\ell)^G$ is an surjection.*

Proof (i) A divisor in $\operatorname{Div} X_\ell$ is fixed by G if and only if the coefficient of each prime divisor W is equal to the coefficients of all its conjugates σW, for $\sigma \in G$. Such a divisor can therefore be written as a sum

$$\sum_i n_i \Big(\sum_{\sigma \in G} \sigma W_i \Big)$$

for finitely many prime divisors W_i. By **??**, each closed subset $\bigcup_{\sigma\in G} \sigma W_i$ is defined over k and is therefore a prime divisor Z_i on X. Remark 4.2.2 shows that $\sum_{\sigma\in G} \sigma W_i$ is in fact the image of Z_i in $\operatorname{Div} X_\ell$, completing the proof.

(ii) This comes down to saying that if a divisor D is defined over k and is the divisor of a function defined over ℓ, then it is in fact the divisor of a function defined over k. This is an easy consequence of Hilbert's Theorem 90 (Proposition 14.7.13).

101: Do we want to add the proof, maybe as an exercise?

(iii) .

102: Find a reference or add a proof for the next two. Does this naturally fit in chapter 15?

□

Example 4.2.6. We give counterexamples to show that the various parts of the theorem can fail when the conditions are not satisfied.

If X is not projective, then (ii) does not necessarily hold. Take any quadratic extension $\ell/\mathbf{Q}$ and let X be $\mathbf{P}^1_{\mathbf{Q}}$ with a pair of points removed that are conjugate over ℓ. Then the removed points constitute a prime divisor on $\mathbf{P}^1_{\mathbf{Q}}$, and Exercise 4.1.19 shows $\operatorname{Pic} X \cong \mathbf{Z}/2\mathbf{Z}$. However, the same exercise shows that $\operatorname{Pic} X_\ell$ is trivial.

If X does not have points everywhere locally, then (iii) and (iv) do not have to hold. Let X be a conic curve in $\mathbf{P}^2_{\mathbf{Q}}$ with no rational points, such as the curve $\{x^2+y^2+z^2=0\}$. The curve X has many points over quadratic extensions, such as the point $P=[1:1:i]$ defined over $\ell=\mathbf{Q}(i)$. The base change X_ℓ is isomorphic to $\mathbf{P}^1_\ell$, and therefore P is linearly equivalent to its Galois conjugate – so the divisor class $[P]$ is fixed by $\operatorname{Gal}(\ell/\mathbf{Q})$. Since $[P]$ generates $\operatorname{Pic} X_\ell$, this means that $\operatorname{Gal}(\ell/\mathbf{Q})$ acts trivially on $\operatorname{Pic} X_\ell \cong \mathbf{Z}$. But there is no divisor of degree 1 on X, and in particular the class $[P]$ contains no divisor defined over $\mathbf{Q}$. The image of $\operatorname{Pic} X$ is of index 2 in $\operatorname{Pic} X_\ell$.

4.3 Intersection numbers

In this section, we let X be a smooth *surface* over a field k. Given two curves in X, they will generally intersect in a finite number of points. The number of points is called their intersection number, and it gives us a very useful bilinear form on the Picard group.

Definition 4.3.1. Let C_1 and C_2 be two curves on X, and let P be a point over the algebraic closure $\bar{k}$ lying in both C_1 and C_2. We say that C_1 and C_2 *intersect transversely* at P if, in the local ring $\mathcal{O}_{X,P}$, there are functions f_1, f_2 which generate the unique maximal ideal and are such that $(f_1) = C_1$ and $(f_2) = C_2$ on a neighbourhood of P. We say that C_1 and C_2 *intersect transversely* if they intersect transversely at all points of intersection.

This definition corresponds to the intuitive notion that the curves are nonsingular at P and have distinct tangent directions.

Example 4.3.2. In $\mathbf{A}^2_{\mathbf{Q}}$, the two coordinate axes intersect transversely at the origin O. They are defined by $\{x = 0\}$ and $\{y = 0\}$, and the maximal ideal of functions vanishing at O is (x, y).

Example 4.3.3. Again in $\mathbf{A}^2_{\mathbf{Q}}$, consider the curves $\{x = 0\}$ and $\{y^2 = x^3\}$. They intersect at O, but the ideal generated by the functions x and $y^2 - x^3$ is (x, y^2) which is not the whole of the maximal ideal (x, y). Therefore the curves do not intersect transversely.

It follows easily from the definition that the intersection of two curves that intersect transversely consists of isolated points (in the Zariski topology). Since any variety is quasi-compact in the Zariski topology, the two curves intersect in only finitely many points.

103: We should state this somewhere

Definition 4.3.4. Let X be a smooth surface over a field k, and let D and D' be two prime divisors on X which intersect transversely. We define the *intersection number* of D and D' to be

$$D \cdot D' = \#(D \cap D')$$

where the cardinality of the intersection $D \cap D'$ is taken over the algebraic closure of k.

If X is projective, then it turns out that the intersection number respects linear equivalence of divisors, so gives a useful way of studying the Picard group. This fails if X is not projective: for example, the coordinate axes in $\mathbf{A}^2$ have intersection number 1 despite both being principal divisors.

Theorem 4.3.5. *Let X be a smooth projective surface. The intersection number extends uniquely to a symmetric bilinear pairing* $\operatorname{Div} X \times \operatorname{Div} X \to \mathbf{Z}$ *which respects linear equivalence, and hence to a symmetric bilinear pairing* $\operatorname{Pic} X \times \operatorname{Pic} X \to \mathbf{Z}$.

Proof See Hartshorne (1977, Chapter V, Theorem 1.1). □

Definition 4.3.6. Let X be a smooth surface and D a divisor on X. The *self-intersection number* of D is the intersection number $D^2 = D \cdot D$.

A curve never intersects itself transversely, but we can make sense of the self-intersection as a number of intersection points by intersecting D with a linearly equivalent divisor.

Example 4.3.7. Any two distinct lines in $\mathbf{P}^2$ intersect transversely in precisely one point, and therefore have intersection number 1. Moreover, any line is linearly equivalent to any other line. We deduce that the self-intersection number of a line in $\mathbf{P}^2$ is 1.

Example 4.3.8. Let $X \subset \mathbf{P}^n$ be a projective surface, and let H be a hyperplane section of X. Then H^2 is the *degree* of X, defined to be the number of points of intersection of X with any sufficiently general linear subspace of dimension $n-2$. To see this, use the fact that $H^2 = H_1 \cdot H_2$ where H_1 and H_2 are any two sufficiently general hyperplane sections of X.

Exercise 4.3.9. Suppose that X is a smooth hypersurface in $\mathbf{P}^3$ defined by a single equation of degree d. Show that the degree of X is equal to d.

Example 4.3.10. Let $X \subset \mathbf{P}^n$ be a projective surface, and let C be an irreducible curve on X. Then $H \cdot C$ is the *degree* of C, defined to be the number of points of intersection of C with a sufficiently general hyperplane.

Exercise 4.3.11. Let X be the projective quadric surface $xy = zw$, and let U be the open subset defined by $w \neq 0$.

(i) Show that U is isomorphic to $\mathbf{A}^2$, and deduce that $\operatorname{Pic} U = 0$.
(ii) Show that $X \setminus U$ consists of two straight lines. Using the exact sequence of Exercise 4.1.19, show that $\operatorname{Pic} X \cong \mathbf{Z}^2$, generated by the classes of these two straight lines.
(Hint: to show that the two lines are not equivalent, you may like to use intersection numbers.)

The intersection number defines a new equivalence relation on divisors on a surface.

Definition 4.3.12. Let X be a smooth surface. Two divisors D and D' on X are said to be *numerically equivalent* if $D \cdot E = D' \cdot E$ for all divisors E on X.

Given that intersection numbers respect linear equivalence, this gives an equivalence relation coarser than linear equivalence. The subgroup of classes in $\operatorname{Pic} X$ which are numerically equivalent to 0 is denoted by $\operatorname{Pic}^{\mathrm{n}} X$.

d: The symbol "$\operatorname{Pic}^{\mathrm{n}} X$" is only used again once in the following section: do we really want to define it?

4.4 Structure of the Picard group over C

When X is a smooth projective variety over the complex numbers **C**, one can use methods from the theory of analytic varieties to deduce results about the Picard group of X. Here we mention briefly some useful facts arising from this.

104: Do we want to state what's true over an arbitrary field?

There is an exact sequence of analytic sheaves on X known as the exponential sequence, which gives rise to an exact sequence of cohomology groups:

$$\mathrm{H}^1(X(\mathbf{C}), \mathbf{Z}) \to \mathrm{H}^1(X, \mathscr{O}_X) \to \operatorname{Pic} X \to \mathrm{H}^2(X(\mathbf{C}), \mathbf{Z}).$$

We state several interesting facts about this sequence.

- Since X is a smooth projective variety, $X(\mathbf{C})$ is a compact manifold. Its integral cohomology groups $\mathrm{H}^i(X(\mathbf{C}), \mathbf{Z})$ are therefore finitely generated abelian groups.
- The group $\mathrm{H}^1(X, \mathscr{O}_X)$ is a finite-dimensional complex vector space, and it turns out that $\mathrm{H}^1(X(\mathbf{C}), \mathbf{Z})$ is a lattice in this vector space. The image of $\mathrm{H}^1(X, \mathscr{O}_X)$ in $\operatorname{Pic} X$ is therefore a complex torus, and in fact is an Abelian variety. It is denoted $\operatorname{Pic}^0 X$, and lies inside the kernel $\operatorname{Pic}^{\mathrm{n}} X$ of the intersection pairing.
- The image of $\operatorname{Pic} X$ in $\mathrm{H}^2(X(\mathbf{C}), \mathbf{Z})$ is isomorphic to $\operatorname{Pic} X / \operatorname{Pic}^0 X$, and it is a finitely generated abelian group, called the *Néron–Severi group* of X.

For more background to these results, see Appendix B of Hartshorne (1977).

5

Differentials and the canonical divisor

In this chapter we define differentials on a variety, and study some of their basic properties. The main purpose for us will be to define the canonical divisor class, which is important for classifying varieties and for defining embeddings of abstract varieties into projective space. Knowing something about the canonical class will also allow us to apply the Riemann–Roch theorem, which is a vital tool for studying the curves which lie in a surface. The emphasis in this chapter will be on understanding differentials in an explicit way, so that we can do calculations with them.

105: MISSING: what happens under base change (Hartshorne II.8.3A)? Relation linear systems and rational maps; base points, removable base points

A standard and excellent reference for this material is Section II.8 of Hartshorne (1977).

5.1 Modules of differentials

Let A be a commutative ring (with identity) and B a commutative A-algebra. This means that there is a map $\iota\colon A \to B$, and we will often be careless in identifying elements of A with their image in B. In particular, if M is a B-module, then it is also an A-module, and we can write am instead of $\iota(a)m$ for $a \in A$ and $m \in M$.

Definition 5.1.1. An *A-derivation* of B into a B-module M is a map $d\colon B \to M$ such that:

(i) d is additive, i.e. $d(b+b') = d(b) + d(b')$ for all $b, b' \in B$;
(ii) d satisfies the Leibniz rule $d(bb') = bd(b') + b'd(b)$ for all $b, b' \in B$; and
(iii) $d(a) = 0$ for all $a \in A$.

It follows from properties (ii) and (iii) that d is an A-linear map: that is, $d(ab) = ad(b)$ for all $a \in A$ and $b \in B$.

106: (iii) equiv with A-linearity

Definition 5.1.2. The *module of relative differential forms* of B over A is a B-module $\Omega_{B/A}$, together with an A-derivation $d\colon B \to \Omega_{B/A}$, satisfying the following universal property: for any B-module M and for any A-derivation $d'\colon B \to M$, there exists a unique B-module homomorphism $f\colon \Omega_{B/A} \to M$ such that $d' = f \circ d$.

Exercise 5.1.3. Show that, if such an object exists, then it is unique up to unique isomorphism: that is, if two modules $\Omega_{B/A}$ and $\Omega'_{B/A}$ are both candidates satisfying the conditions of Definition 5.1.2, then there is a unique isomorphism between them. Hence we really can talk about "the" module $\Omega_{B/A}$.

If $\mathrm{Der}_A(B,M)$ denotes the set of all A-derivations from B into M, then the universal property of $\Omega_{B/A}$ gives a natural bijection $\mathrm{Der}_A(B,M) \leftrightarrow \mathrm{Hom}_B(\Omega_{B/A},M)$.

Proposition 5.1.4. *The module of relative differential forms $\Omega_{B/A}$ exists.*

Proof Let F be the free B-module generated by a set of formal symbols $\{db : b \in B\}$. Define a submodule R of F generated by the following:

(i) $d(b+b') - db - db'$ for all $b, b' \in B$;
(ii) $d(bb') - bdb' - b'db$ for all $b, b' \in B$;
(iii) da for all $a \in A$.

Now let $\Omega_{B/A}$ be the quotient F/R. Define $d\colon B \to \Omega_{B/A}$ by $b \mapsto db$; then, by construction, d is a derivation. If $d' : B \to M$ is a derivation of B into M, then define the homomorphism $f\colon \Omega_{B/A} \to M$ by $db \mapsto d'(b)$. This is well defined, since d' is a derivation, and satisfies $d' = f \circ d$. It is also unique: since the symbols db generate $\Omega_{B/A}$, any homomorphism $\Omega_{B/A} \to M$ is defined by where it sends the db, and so the requirement $f(db) = d'b$ fixes f. □

Exercise 5.1.5. Let $B = A[x_1, \ldots, x_n]$ be a polynomial ring over A. Show that $\Omega_{B/A}$ is the free B-module of rank n generated by the dx_i.

Proposition 5.1.6. *Let I be an ideal of B and set $C = B/I$. Then there is a natural exact sequence of C-modules*

$$I/I^2 \xrightarrow{f} \Omega_{B/A} \otimes_B C \xrightarrow{g} \Omega_{C/A} \to 0,$$

where f sends $b \in I$ to $db \otimes 1$, and g send $db \otimes c$ to $cd\bar{b}$, where $\bar{b}$ is the image of b in C.

Proof This proposition can be proved using more abstract methods, but we give an explicit proof.

Let us first check that f is well defined. The ideal I^2 is generated by elements of the form $b = xy$ with $x, y \in I$. Then $db = xdy + ydx$, and so

$$db \otimes 1 = x(dy \otimes 1) + y(dx \otimes 1) = dy \otimes \bar{x} + dx \otimes \bar{y} = 0.$$

Moreover, f is a C-linear map. If $b \in I$ and $c \in C$, lift c to an element $b' \in B$; then the action of c on I/I^2 takes b to the class of $b'b$. Now

$$d(b'b) \otimes 1 = (b'db + bdb') \otimes 1 = (db \otimes c) + (db' \otimes b) = c(db \otimes 1)$$

proving that f is indeed C-linear.

To show exactness, we will look explicitly at systems of generators and relations for the modules $\Omega_{B/A} \otimes_B C$ and $\Omega_{C/A}$, as described in the proof of Proposition 5.1.4. It is a general fact about tensor products that, if a B-module M is described by generators and relations, then $M \otimes_B C$ is described by the same generators, and the same relations but with coefficients pushed into C. So $\Omega_{B/A} \otimes_B C$ is the C-module generated by symbols db for all $b \in B$, where we identify db with $db \otimes 1$. The relations for additivity and for vanishing on A are unchanged from $\Omega_{B/A}$, but for the Leibniz rule we should take relations $d(bb') - \bar{b}db' - \bar{b}'db$, where $\bar{b}$ denotes the image of b in C.

107: Find reference

Now consider the module $\Omega_{C/A}$. This is generated by symbols dc for all $c \in C$, but (since $B \to C$ is surjective) we can equally well generate it by db for all $b \in B$, as long as we add relations $db - db'$ whenever $b - b' \in I$. Having done this, it makes no difference whether we take additivity relations $d(c + c') - dc - dc'$ for $c \in C$, or $d(b + b') - db - db'$ for all $b \in B$. A similar statement holds for the Leibniz rule relations.

To summarise, we have presentations for both $\Omega_{B/A} \otimes_B C$ and $\Omega_{C/A}$ as C-modules. They both have the same set of generators $\{db\}$, and their set of relations differ only in that $\Omega_{C/A}$ has the additional relations $db - db'$ whenever $b - b' \in I$; equivalently (using the additivity relation) the additional relations can be db for all $b \in I$. Therefore the natural map $\Omega_{B/A} \otimes C \to \Omega_{C/A}$ is surjective, and its kernel is precisely the submodule generated by the $db \otimes 1$ for all $b \in I$, as stated. □

Example 5.1.7. If $A = k$ is a field, $B = k[x, y]$, and $C = k[x, y]/(x^2 + y^2 - 1)$, then $\Omega_{C/A}$ is the C-module generated by dx and dy with relation $2xdx + 2ydy = 0$.

Example 5.1.8. If $A = k$ is a field, and $B = k[\varepsilon]/(\varepsilon^2)$, then $\Omega_{B/A}$ is the B-module generated by $d\varepsilon$ and the relation $2\varepsilon d\varepsilon = 0$.

There are many more interesting exact sequences describing for instance the behavior of modules of relative differential forms under tensor products, and

the relation of the modules $\Omega_{B/A}$, $\Omega_{C/A}$, $\Omega_{C/B}$ for any B-algebra C. For more information, see Hartshorne (1977, Section II.8). Here we will only present what we need for our purposes.

Proposition 5.1.9. *If B is an integral domain with fraction field K, then $\Omega_{K/A} \cong \Omega_{B/A} \otimes_B K$.*

108: Find a proof or a reference for this: Hartshorne, Prop. II.8.2A refers to Matsumura (localisation)

5.2 Differentials on varieties

For this section, let k be a field. If X is a smooth, irreducible variety over k, we will define the regular differentials on X as a subset of the vector space of differentials $\Omega_{\kappa(X)/k}$.

109: Weren't varieties always irreducible?

Definition 5.2.1. Let X be a smooth, irreducible variety over a field k. A differential $\omega \in \Omega_{\kappa(X)/k}$ is *regular* at a point $P \in X$ if there exists an affine open neighbourhood $U \subset X$ of P, with coordinate ring B, such that the B-submodule $\Omega_{B/k}$ of $\Omega_{\kappa(X)/k}$ contains ω.

110: Why is one a submodule of the other? Uses enough to be worth mentioning! Hartshorne II.8.15 says nonsingular implies Ω_X is locally free, and locally free implies flat, and $B \to K$ is injective if B is an integral domain, and Hartshorne II.8.2a... Counterexample with local ring of singular point on a curve?

Example 5.2.2. Consider $\mathbf{P}^1_k(x,y)$ with function field $k(t)$ for $t = x/y$, and set $\omega = dt$. Then the affine part $y \neq 0$ can be identified with $\mathbf{A}^1(t)$, which has coordinate ring $k[t]$. Since the $k[t]$-module $\Omega_{k[t]/k}$ is generated by dt, we find that ω is regular at every point of $\mathbf{A}^1$.

In the following definition, when we require an object to be regular at every point of a subset, we really mean *every* point, whatever field it may be defined over. It is certainly not enough to check the condition only for points of $X(k)$.

Definition 5.2.3. For every open subset $U \subset X$ let $\mathscr{O}_X(U)$ denote the subring of $\kappa(X)$ of functions that are regular at every point of U, and let $\Omega_X(U)$ denote the $\mathscr{O}_X(U)$-submodule of $\Omega_{\kappa(X)/k}$ consisting of differentials ω that are regular at every point of U.

111: X as in 5.2.1?

Remark 5.2.4. We have in fact just defined two sheaves: the structure sheaf $\mathscr{O}_X$ and the sheaf of differentials Ω_X on the variety X.

Proposition 5.2.5. *If U is an affine subvariety of X with coordinate ring B, then we have $\Omega_X(U) = \Omega_U(U) = \Omega_{B/k}$.*

Proof Since the function fields $\kappa(X)$ and $\kappa(U)$ are equal, this follows immediately from Definition 5.2.1. □

112: what about second equality? Definition only requires for **some** open affine.

Given a variety X over k, are there differentials on X which are regular

everywhere? The following example shows that this is not the case for the projective line.

Example 5.2.6. Consider $\mathbf{P}^1_k(x,y)$ with function field $K = k(t) = k(s)$ for $t = x/y$ and $s = t^{-1}$. It follows from Exercise 5.1.5 and Proposition 5.1.9 that $\Omega_{K/k}$ is the 1-dimensional vector space over K generated by dt (or, equally well, by ds). The regular differentials on $\mathbf{A}^1(t)$ are in the $k[t]$-module generated by dt, while those on $\mathbf{A}^1(s)$ are in the $k[s]$-module generated by $ds = d(t^{-1}) = -t^{-2}dt$. The intersection in $\Omega_{K/k}$ is 0, so $\Omega_{\mathbf{P}^1}(\mathbf{P}^1) = 0$, i.e., there are no nonzero differentials that are regular on $\mathbf{P}^1$.

Exercise 5.2.7. Consider the differential $\omega = dx/y$ on the affine curve C in $\mathbf{A}^2_k(x,y)$ given by $y^2 = f(x)$ for some polynomial f with no repeated roots. Show that ω is regular at every point of C. Show that this is consistent with Proposition 5.2.5. Show that if f has degree 3, then ω is in fact regular on the entire projective closure of C in $\mathbf{P}^2$.

Exercise 5.2.8 (*)**.** Show that if X is a hypersurface in $\mathbf{P}^n$ for $n \geq 3$, then $\Omega_X(X) = 0$.

Exercise 5.2.9 (*)**.** Show that if X is a complete intersection in $\mathbf{P}^n$ of dimension at least 2, then $\Omega_X(X) = 0$.

113: can I do these? define and/or say something about complete intersections

When studying the rational points on a variety X over a number field, it is often tempting to try to map X to another variety Y on which we can control the set of points more easily. Every rational point on X would then map to a rational point of Y, so all we would need to check is which rational points of Y lift to rational points on X, a process that is particularly easy when Y does not contain any rational points. Given X, the following proposition gives restrictions on Y (to the extend that it may show this approach is useless for X).

Proposition 5.2.10. *If $f\colon X \to Y$ is a surjective morphism of smooth irreducible varieties over a field k, and f is generically smooth (which is automatic in characteristic 0), then the induced map $f^*\colon \Omega_Y(Y) \to \Omega_X(X)$ is injective.*

Proof Since f is generically smooth, there is an open subset $U \subset X$ such that $f\colon U \to Y$ is smooth (cf. Hartshorne, 1977, Lemma III.10.5). This is equivalent to saying that for any point $x \in U$, and $y = f(x)$, the induced map $T_x \to T_y$ on Zariski tangent spaces is surjective, or equivalently, the map $\mathfrak{m}_y/\mathfrak{m}_y^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$ is injective, where $\mathfrak{m}_x$ and $\mathfrak{m}_y$ denote the maximal ideals of the local rings at x and y respectively (see Hartshorne, 1977, Proposition III.10.4). Now take any nonzero differential $\omega \in \Omega_Y(Y)$. Since $f(U)$ is dense in Y and ω can not vanish

on an open subset, there is a $y \in f(U)$ such that ω does not vanish at y. Take any $x \in U$ such that $f(x) = y$. Then by the above the map $\mathfrak{m}_y/\mathfrak{m}_y^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$ is injective. These k-vector spaces are the stalks at y and x of the sheaves Ω_Y and Ω_X respectively. Since ω does not vanish at y, its image in the stalk at y is nonzero, and by injectivity, so is its image in the stalk at x, and therefore the image of ω in $\Omega_X(X)$ is nonzero. □

114: Refer to Hartshorne II.8.7

115: Make this work for non-algebraically closed k. Can we do this without sheaves?

Corollary 5.2.11. *Let X be a smooth variety over a field k. If $\Omega_X(X) = 0$, and* $\operatorname{char} k = 0$*, then there is no surjective morphism from X to a nonsingular curve of positive genus or to an abelian variety of positive dimension.*

Proof Suppose $f\colon X \to Y$ is a surjective morphism for some Y. Since the characteristic is zero, the morphism f is generically smooth, so Proposition 5.2.10 tells us that $\Omega_Y(Y) = 0$. This prevents Y from being a curve of genus $g > 0$, or an abelian variety of dimension $g > 0$, both of which would satisfy $\dim_k \Omega_Y(Y) = g$. □

Exercise 5.2.9 and Corollary 5.2.11 show that if X is a complete intersection of dimension at least 2, then there is no hope for a morphism from X to a curve of positive genus or an abelian variety of positive dimension.

We finish this section with some results describing the dimension of $\Omega_{K/k}$ when K/k is a field extension.

Definition 5.2.12. Let K be a field extension of k. Then K is *separably generated* over k if there exists a transcendence basis $\{t_i\}$ for K/k such that K is a separable algebraic extension of $k(\{t_i\})$.

Proposition 5.2.13. *Let K be a finitely generated extension field of a field k. Then* $\dim_K \Omega_{K/k} \geq \operatorname{tr.deg.} K/k$*, with equality if and only if K is separably generated over k.*

Proof See [somewhere]. □

116: Find a reference

Corollary 5.2.14. *Let $K = \kappa(X)$ be the function field of a variety X over a* perfect *field k. Then* $\operatorname{tr.deg.} K/k = \dim X$*, and so $\Omega_{\kappa(X)/k}$ is a vector space of dimension* $\dim X$.

117: Find a reference

118: Is it trivial that k perfect and K/k fin. generated implies K/k separably generated?

119: The "Then" doesn't use perfectness yet, does it?

120: Maybe enough to assume the variety is geometrically reduced. Yes, I think so, according to Poonen 2.2.16 and 2.2.20. But what does that measn when all varieties are by definition reduced? Also equivalent to ideal over alg. closure being generated by ideal over k? See Cor. to Matsumura 27.E (Lemma 2) and 27.F (Lemma 3). Also equiv to ideal over k generating a radical ideal over $\bar{k}$?

121: Would indeed be better to replace perfect by function field being separably generated. Then also state lemma that this is implied by being smooth, even our definition of smooth.

5.3 Differential n-forms

So far, we have been studying differential 1-forms on a variety. It turns out that the differential n-forms also give very important invariants. In particular,

since the space of n-forms is one-dimensional, we can associate a divisor to an n-form, and all such divisors are linearly equivalent. The divisor class to which they belong is the canonical divisor class.

Let X be a smooth variety over a field k, of dimension n. By Corollary 5.2.14, the vector space $\Omega_{\kappa(X)/k}$ over $\kappa(X)$ has dimension n. Its nth exterior power $\bigwedge^n \Omega_{\kappa(X)/k}$ is therefore a 1-dimensional vector space over $\kappa(X)$; a generator is given by $dx_1 \wedge \cdots \wedge dx_n$, where $x_1, \ldots, x_n$ are any functions such that $dx_1, \ldots, dx_n$ generate $\Omega_{\kappa(X)/k}$.

Definition 5.3.1. Take an n-form $\omega \in \bigwedge^n \Omega_{\kappa(X)/k}$ and a point P on X. Let $t_1, \ldots, t_n$ be a set of local parameters at P. Then $dt_1, \ldots, dt_n$ generate $\Omega_{\kappa(X)/k}$, and so there is a unique $g \in \kappa(X)$ such that $\omega = g dt_1 \wedge \ldots \wedge dt_n$. We say that ω is *regular at* P if this g is regular at P.

It is straightforward to check that the set of n-forms which are regular at P forms a subgroup of $\Omega_{\kappa(X)/k}$. Moreover, if ω is regular at P, and $f \in \kappa(X)$ is a function which is regular at P, then $f\omega$ is clearly also regular at P.

Definition 5.3.2. For any open subset $U \subset X$, define an n-form $\omega \in \bigwedge^n \Omega_{\kappa(X)/k}$ to be *regular on* U if it is regular at each point of U. Let $\omega_X(U)$ denote the set of all such n-forms.

By our previous comments, $\omega_X(U)$ is a sub-$\mathcal{O}_X(U)$-module of $\bigwedge^n \Omega_{\kappa(X)/k}$.

Remark 5.3.3. Using sheaves, it is more natural to define the sheaf ω_X as the highest exterior power $\bigwedge^n \Omega_X$ of the sheaf of 1-forms on X.

122: No sheafification needed?

Definition 5.3.4. The *geometric genus* of a smooth variety X over k is $g(X) = \dim_k \omega_X(X)$.

Example 5.3.5. For a curve C we have $\Omega_C = \omega_C$, so we have already seen that $\omega_{\mathbf{P}^1}(\mathbf{P}^1) = 0$ and thus $g(\mathbf{P}^1) = 0$.

The fact that $\bigwedge^n \Omega_{\kappa(X)/k}$ is one-dimensional means that n-forms on X behave rather like rational functions. Recall that we can associate, to each rational function f, a divisor (f). We now show how to do the same for n-forms. Firstly, we define the order of vanishing of an n-form along a prime divisor.

Definition 5.3.6. Let X be a smooth variety over a field k, let Z be a prime divisor on X, and let P be a point of Z. Take a non-zero n-form $\omega \in \bigwedge^n \Omega_{\kappa(X)/k}$. Let $t_1, \ldots, t_n$ be a set of local parameters at P. Then there is a unique $g \in \kappa(X)$ such that $\omega = g dt_1 \wedge \ldots \wedge dt_n$. We define $v_Z(\omega) = v_Z(g)$.

Exercise 5.3.7. Show that this definition does not depend on the choice of the point P.

Now we can put these valuations together to obtain a divisor.

Definition 5.3.8. Let X be a smooth variety over a field k. To any non-zero n-form $\omega \in \bigwedge^n \Omega_{\kappa(X)/k}$ we associate the divisor

$$(\omega) = \sum_Z v_Z(\omega) Z \in \operatorname{Div} X,$$

where the summation is over all prime divisors of X.

123: Mention that this behaves well under base change, that is, canonical divisor of base change is base change of canonical divisor. Same for divisor associated to a function, which could be stated in chapter on Picard group. This is ingredient for base change of del Pezzo being del Pezzo.

Exercise 5.3.9. Show that the sum is finite – that is, $v_Z(\omega) = 0$ for all but finitely many prime divisors Z.

It is important to realise that the function g in Definition 5.3.6 really does depend on the point P, and so there is no reason to expect the divisor (ω) to be the divisor of any rational function.

For any two non-zero $\omega, \omega' \in \bigwedge^n \Omega_{\kappa(X)/k}$ there is a $g \in \kappa(X)$ such that $\omega = g\omega'$, so (ω) and (ω') are linearly equivalent.

Definition 5.3.10. The class in $\operatorname{Pic} X$ of any, and thus all, $(\omega) \in \bigwedge^n \Omega_{\kappa(X)/k}$ is called the *canonical divisor class* of X. The divisors in this class are called *canonical divisors*.

Exercise 5.3.11. Compute the divisor (dt) on $\mathbf{P}^1(x,y)$ with $t = x/y$.

Exercise 5.3.12. Let k be a field. Let $e \geq 2$ be an integer. The weighted projective space $\mathbf{P}_k(1,e,1)$ with coordinates X,Y,Z has two open affine subsets U_1 and U_2, given by $Z \neq 0$ and $X \neq 0$, respectively. Set $x = X/Z$ and $y = Y/Z^e$, so that U_1 is naturally isomorphic to $\mathbf{A}^2(x,y)$. Let $f \in k[x]$ be a separable polynomial of degree d, and let $C \subset U_1$ be the affine curve given by $y^2 = f(x)$. Let C' denote the projective closure of C in $\mathbf{P}(1,e,1)$.

(i) Show that if $d \leq 2e$, then C' is contained in $U_1 \cup U_2$.
(ii) Assume $e = 1$ and $d = 2$. Show that C' is smooth, and compute the divisor (dx/y) on C'.
(iii) Assume $e = 1$ and $d = 3$. Show that C' is smooth, and compute the divisor (dx/y) on C'. (Note that in this case C' is not contained in $U_1 \cup U_2$.)
(iv) Assume $e \geq 2$ and $d = 2e$. Show that C' is smooth, and compute the divisor (dx/y) on C'.
(v) Assume $e \geq 2$ and $d = 2e-1$. Show that C' is smooth, and compute the divisor (dx/y) on C'.

Exercise 5.3.13. Compute the divisor $(dt_1 \wedge \ldots \wedge dt_n)$ on $\mathbf{P}^n(x_0,x_1,\ldots,x_n)$ with $t_i = x_i/x_0$.

Exercise 5.3.14. Let X be a smooth hypersurface in $\mathbf{P}^n_k(x_0,\ldots,x_n)$ given by a homogeneous polynomial F of degree d, let L be any linear form in $k[x_0,\ldots,x_n]$ that does not vanish on X, and set

$$\omega = \frac{x_0^n L^{-n-1+d}}{\partial F/\partial x_n} dt_1 \wedge \ldots \wedge dt_{n-1}$$

124: Give hint? Choices of $i=0$ (used for dehomogenisation) and $j=n$ (which t_j to leave out); other choices give $\pm$ same differential! Check that nonvanishing of a partial derivative tells you which t_j is not necessary for generating maximal ideal. Actually, doesn't that mean the derivative should have been with respect to x_n??? Yes, indeed...

with $t_i = x_i/x_0$. After checking that all degrees work out to make ω a well-defined element of $\bigwedge^{n-1}\Omega_{\kappa(X)/k}$, show that we have $(\omega) = (-n-1+d)(H\cap X)$, where H is the hyperplane given by $L=0$.

Note that $\dim X = n-1$, and with the notation of the previous exercise, there exist $(n-1)$-forms that are regular everywhere if and only if $d \geq n+1$, while there are no regular 1-forms if $n > 2$. The following proposition is a generalization of the previous exercise.

Proposition 5.3.15. *Let $X \subset \mathbf{P}^n$ be a smooth complete intersection of dimension $n-t$, of which the ideal $I(X,k)$ is generated by the polynomials $F_1,\ldots,F_t$ of degrees $d_1,\ldots,d_t$ respectively. Then every canonical divisor on X is linearly equivalent to $(-n-1+\sum_{i=1}^t d_i)H$ where H is any hyperplane section of X.*

Proposition 5.3.15 follows from Hartshorne (1977, Proposition II.8.20); for a step-by-step approach, see Exercise II.8.4 there. Besides the sheaf-theoretic proof given there, the following exercises also lead to a (fairly heavily) computational proof.

For any t polynomials $f_1,\ldots,f_t \in k[x_1,\ldots,x_n]$, and any sequence $J=(j_l)_{l=1}^t$ with $1 \leq j_1 < \ldots < j_t \leq n$ we define $M_J = M_J(f_1,\ldots,f_t)$ to be the determinant of the matrix $A = (\partial f_i/\partial x_{j_l})_{i,l=1}^t$.

Exercise 5.3.16. Let $X \subset \mathbf{A}^n(x_1,\ldots,x_n)$ be a smooth complete intersection of dimension $n-t$, defined by the polynomials $f_1,\ldots,f_t \in k[x_1,\ldots,x_n]$. Let J be a sequence as above, and let I be the increasing sequence of the elements of $\{1,\ldots,n\}\smallsetminus J$. Then up to sign the differential $\omega_J = M_J^{-1} dx_{i_1}\wedge\ldots\wedge dx_{i_{n-t}}$ is independent of the choice of J.

Exercise 5.3.17. Use the notation as in the previous exercise, and assume P is a point on X. Then there is a particular sequence J as in that exercise such that $M_J(P) \neq 0$ and for the corresponding sequence I, the elements $x_i - x_i(P)$ with $i \in I$ form a set of local parameters at P. Conclude that $(\omega_J) = 0$ on $X \subset \mathbf{A}^n$.

125: combine some of these exercises? If so, change plural in announcement of these exercises

Exercise 5.3.18. Homogenize the previous exercises to find out the contribution to (ω) of the hyperplane at infinity of the projective closure of X. Check that your answer agrees with Proposition 5.3.15.

Exercise 5.3.19. Suppose X is a smooth complete intersection as in Proposition 5.3.15, and assume that X is a surface. Compute the self-intersection of a canonical divisor on X.

The following exercise gives another generalization of exercise 5.3.14.

Exercise 5.3.20. Let $\mathbf{P}(w_0, w_1, \ldots, w_n)$ be weighted projective n-space with coordinates $x_0, \ldots, x_n$ such that x_i has weight w_i, and assume $w_0 = 1$. Let X be a smooth hypersurface in $\mathbf{P}(w_0, w_1, \ldots, w_n)$ of (weighted) degree d. Set $D = X \cap H$ where H is the hyperplane given by $x_0 = 0$. Then any canonical divisor on X is linearly equivalent to $(d - \sum_i w_i)D$.

Exercise 5.3.21. Find an example of a variety X of dimension n for which the map $\bigwedge^n(\Omega_X(X)) \to \omega_X(X)$ is not surjective.

6

Linear systems and the Riemann–Roch Theorem

6.1 Equivalent effective divisors

Let X be a smooth variety over a field k, and let D be any divisor on X. We define the k-vector space

$$L(D) = \{ f \in \kappa(X)^\times \mid (f) + D \text{ is effective } \} \cup \{0\}. \tag{6.1}$$

Given a nonzero function $f \in L(D)$, the definition says that $D' = (f) + D$ is effective; but it is also linearly equivalent to D. Conversely, suppose that D' is an effective divisor on X linearly equivalent to D; then there is a function $f \in \kappa(X)^\times$ such that $D' = D + (f)$, and so $f \in L(D)$. So there is a correspondence

$$L(D) \smallsetminus \{0\} \longrightarrow \{\text{Effective divisors linearly equivalent to } D\}.$$

If X is projective, then Proposition 4.1.8 says that two functions f, f' give rise to the same divisor $(f) = (f')$ if and only if their quotient is constant. In that case there is a *bijective* correspondence

$$\frac{L(D) \smallsetminus \{0\}}{k^\times} \longleftrightarrow \{\text{Effective divisors linearly equivalent to } D\}. \tag{6.2}$$

If $L(D)$ is a finite-dimensional vector space, then the left-hand side of this correspondence can be thought of as the projective space $\mathbf{P}(L(D))$.

126: or the dual???

Definition 6.1.1. The set of divisors in (6.2), which we denote $|D|$, is called the *complete linear system* associated to the divisor class $[D]$.

Example 6.1.2. Let X be $\mathbf{P}^2_k$ with coordinates X_0, X_1, X_2 and take D to be the line $\{X_0 = 0\}$. Then

$$L(D) = \left\{ \frac{aX_0 + bX_1 + cX_2}{X_0} \mid a, b, c \in k \right\}.$$

Here $L(D)$ has dimension 3, and the effective divisors linearly equivalent to D

are all divisors defined by $aX_0 + bX_1 + cX_2 = 0$ for $a, b, c \in k$ – that is, they are the straight lines in $\mathbf{P}^2$. They are parametrised by a projective space of dimension 2, called the *dual* of $\mathbf{P}^2$.

In this example, the space $L(D)$ is finite-dimensional. However, this does not have to be true if X is not projective.

Example 6.1.3. Let X be $\mathbf{A}^1_k$ with coordinate t, and let D be the divisor $\{t = 0\}$. Then

$$L(D) = \{t^{-1}P(t) \mid P \in k[t]\}$$

which has infinite dimension. Intuitively, this can happen because $\mathbf{A}^1$ is "missing" the point at infinity, so the functions in $L(D)$ may have poles of arbitrary degree there.

Proposition 6.1.4. *Let X be a smooth projective variety, and let D be a divisor on X. Then $L(D)$ is finite-dimensional.*

Proof See Hartshorne (1977, Theorem II.5.19). □

Definition 6.1.5. Let X be a projective variety over a field k and let D be a divisor on X. Define $\ell(D) := \dim_k L(D)$ to be the dimension of the vector space (6.1).

Proposition 6.1.6. *Let X be a smooth projective surface over a field k, let D be a divisor on X and let H be a hyperplane section on X. Suppose that $D \cdot H < 0$. Then $\ell(D) = 0$.*

Proof If $\ell(D) \geq 1$, then there would be an effective divisor D' linearly equivalent to D, such that $D' \cdot H < 0$. Since any prime divisor Z satisfies $Z \cdot H = \deg Z > 0$, this is a contradiction. □

Example 6.1.7. Let C be a curve lying in a smooth projective surface X. If C is linearly equivalent to another curve C' which meets C transversely, then $C^2 = C \cdot C' \geq 0$. But a curve does not have to have positive self-intersection. For example, let X be a smooth cubic surface in $\mathbf{P}^3_{\mathbf{C}}$ and let C be one of the 27 straight lines lying on X. If there were any other effective divisor on X linearly equivalent to C, then $\ell(C) > 1$ and there would be a whole infinite family of effective divisors C' linearly equivalent to C. Since they would all satisfy $C' \cdot H = 1$, they would all be straight lines – yet there are only finitely many straight lines in X, so this cannot be true. In fact, as we shall see, $C^2 = -1$ for a straight line C lying in a smooth cubic surface.

Exercise 6.1.8. Show that, if $D' \sim D$, then the vector spaces $L(D')$ and $L(D)$ are isomorphic.

We conclude this section by looking at what happens to the space $L(D)$ under base change.

Proposition 6.1.9. *Let X be a smooth variety over a field k, let D be a divisor on X and let k'/k be a field extension. Denote by $D_{k'} \in \mathrm{Div}(X_{k'})$ the base change of D (see Section 4.2). Then the k'-vector space $L(D_{k'})$ has a basis consisting of functions contained in $\kappa(X)$. In particular, we have $\ell(D_{k'}) = \ell(D)$.*

Proof In the case that k'/k is Galois, this will be proved in Section 14.10. For the general case, see **?**. To deduce the last sentence, note that $L(D) = L(D_{k'}) \cap \kappa(X)$; so the k'-basis of $L(D_{k'})$ described is also a k-basis of $L(D)$. □

127: Find a reference for this

6.2 Rational maps to projective space

In this section, we show how divisor classes can give rise to rational maps into projective space. For more details about the subject of this section, see Hartshorne (1977, Section II.7).

Fix a divisor D on a variety X, and choose a basis $(f_1, \ldots, f_d)$ of $L(D)$, where $d = \ell(D)$. Then these functions may be used to define a rational map

$$\phi_D \colon X \dashrightarrow \mathbf{P}^{d-1}, \quad P \mapsto [f_1(P) : \cdots : f_d(P)].$$

This map is regular wherever the f_i are all defined and do not all vanish. It may be possible to clear denominators and so extend the domain of ϕ_D.

Remark 6.2.1. We have defined ϕ_D by choosing a basis for $L(D)$. Choosing a different basis gives a map which differs from ϕ_D by a linear automorphism of $\mathbf{P}^{d-1}$. So, in fact, ϕ_D is defined only up to automorphisms of $\mathbf{P}^{d-1}$. It is, however, possible to avoid this ambiguity by taking the domain of ϕ_D to be $\mathbf{P}(L(D))$, the projective space of dimension $\ell(D) - 1$ associated to the vector space $L(D)$.

128: Or its dual?

Suppose that D' is linearly equivalent to D, say $D' = D + (f)$. Then, given any basis $\{f_i\}$ for $L(D)$, we obtain a basis $\{f^{-1} f_i\}$ for $L(D')$. These bases define *the same* rational map, and so the map ϕ_D really depends only on the linear equivalence class of D. We will often speak of the rational map associated to a divisor *class*, rather than to an individual divisor.

Example 6.2.2. Let X be $\mathbf{P}^1_k$, with coordinates s, t, and let P be the point $s = 0$. Then a basis for $L(P)$ is given by $\{1, t/s\}$, and we obtain the rational map $\phi_P = [1 : t/s] = [s : t]$, the identity morphism.

Now consider the divisor $2P$. A basis for $L(2P)$ is given by $\{1, t/s, t^2/s^2\}$,

and the corresponding rational map is $\phi_{2P} = [s^2 : st : t^2]$, which embeds $\mathbf{P}^1$ as the conic curve $\{y^2 = xz\}$ in $\mathbf{P}^2$. Observe that any pair of points makes an effective divisor equivalent to $2P$, and these are precisely the divisors cut out by hyperplane sections under this embedding.

Similarly, we obtain $\phi_{3P} = [s^3 : s^2t : st^2 : t^3]$, embedding $\mathbf{P}^1$ as the *twisted cubic curve* in $\mathbf{P}^3$.

129: Example commented out, it was wrong, but could be added after 6.2.5 for normal complete intersections. Other fixes may be possible as well...

Remark 6.2.3. If the functions f_i do not span the whole of $L(D)$, we still obtain a rational map. For example, take $X = \mathbf{P}^1$ as in example 6.2.2 and $D = 3P$, but take the functions $\{1, t^2/s^2, t^3/s^3\}$. The corresponding map $[s^3 : st^2 : t^3]$ maps $\mathbf{P}^1$ to the cuspidal cubic curve $\{y^3 = xz^2\}$. But there is really nothing new here – this map can equally be obtained by embedding $\mathbf{P}^1$ as the twisted cubic in $\mathbf{P}^3$, and then projecting to $\mathbf{P}^2$ in an appropriate way.

Exercise 6.2.4. Let C be the curve in $\mathbf{P}^3(x,y,z,w)$ parametrized by $(u^4 : u^3t : ut^3 : t^4)$. Let H be the hyperplane given by $w = 0$ and let D be the pull-back of the divisor H under the inclusion of C in $\mathbf{P}^3$. Show that the functions $1, x/w, y/w, z/w$ do not generate $L(D)$. Find a divisor which is linearly equivalent to D, but is not a hyperplane section. (Hint: find an isomorphism from C to $\mathbf{P}^1$ and find what divisor D corresponds to on $\mathbf{P}^1$.)

The next proposition will be needed in an exercise. Note that any smooth variety is normal, and that a variety defined by a single equation (a hypersurface) is a complete intersection.

Proposition 6.2.5. *Let X be a projective variety that is a normal complete intersection in $\mathbf{P}^n$ and H a hyperplane in $\mathbf{P}^n$ that does not contain X. Then the map $L(mH) \to L(mH \cap X)$ is surjective for all $m \geq 0$.*

Proof See Hartshorne (1977, Exercise II.8.4(c)). □

Exercise 6.2.6. Use Proposition 6.2.5 to show that the geometric genus of a hypersurface in $\mathbf{P}^n$ of degree d equals $\binom{d-1}{n}$.

Example 6.2.7. Let $\omega_0, \ldots, \omega_r$ be a basis for the vector space of regular differentials on X. Since $\bigwedge^n \Omega_{k(X)/k}$, with $n = \dim X$, is 1-dimensional over $k(X)$, there are rational functions $g_0, g_1, \ldots, g_r$ such that $\omega_i = g_i\omega_0$. Note that $g_0 = 1$. We can define an associated rational map by $P \mapsto [g_0(P) : g_1(P) : \cdots : g_r(P)]$.

130: Fix arbitrary j instead of just 0.

Exercise 6.2.8. Show that the g_i in Example 6.2.7 are a basis for $L(D)$ with $D = (\omega_0)$.

131: well, not if we start at $i = 1$, as we did before....

6.3 Ample and very ample divisors

The hyperplane sections of a projective variety are very useful in studying its geometry. However, we have seen that a variety may admit many maps to projective spaces, and even many embeddings into projective spaces; so the idea of "hyperplane section" is not intrinsically defined. The notions of ample and very ample divisors are ones which embody some of the properties of hyperplane sections.

Definition 6.3.1. A divisor D on a projective variety X is *very ample* if a basis of $L(D)$ determines a morphism $X \to \mathbf{P}^n$ that is an isomorphism to a closed subvariety of $\mathbf{P}^n$.

132: Do we need "embedding" to be defeined precisely? Close dimmersiom? Isomorphism to a closed subvariety.

Exercise 6.3.2. Show that any divisor that is linearly equivalent to a very ample divisor, is in fact itself very ample.

Example 6.3.3. If X is embedded in $\mathbf{P}^n$, then any hyperplane section of X is a very ample divisor.

Conversely, every very ample divisor on X is of this form for some embedding $X \to \mathbf{P}^r$.

Definition 6.3.4. A divisor D on X is called ample if some positive multiple of D is very ample.

Example 6.3.5. Let C be a smooth curve. Then any divisor of positive degree is ample, by the Riemann–Roch Theorem for curves . However, a divisor of degree 1 is very ample if and only if C has genus 0.

133: find reference: HH IV.3.3

Example 6.3.6. Consider the cone X given by $x^2 + y^2 = z^2$ in $\mathbf{P}^3$. Show that any two lines on X through the vertex of X are linearly equivalent. Show that each of these lines is ample, but not very ample. (Ok, this is cheating, as we said X would always be smooth; later we will see del Pezzo surfaces, for some of which the anticanonical sheaf is ample, yet not very ample).

Exercise 6.3.7. Find all sequences $(d_1, \ldots, d_r)$ with $d_i \geq 2$ such that a canonical divisor on a smooth complete intersection X in $\mathbf{P}^{r+2}$ of hypersurfaces of degree $d_1, \ldots, d_r$ is not very ample. (Compare this to the next lecture.)

134: sort out this reference

6.4 Arithmetic genus and the adjunction formula

Any projective variety X has an integer invariant, written $p_a(X)$, called the *arithmetic genus* of X. This may be defined in several equivalent ways: for

example, in terms of the Euler characteristic of the structure sheaf of X by

$$p_a(X) = (-1)^{\dim X}(\chi(\mathscr{O}_X) - 1)$$

or using the Hilbert polynomial of X. See Hartshorne (1977, Chapter I, Exercise 7.2).

Proposition 6.4.1. *Let C be a smooth, projective curve. Then $p_a(C) = p_g(C)$, the geometric genus of C.*

Proof See Hartshorne (1977, Chapter IV, Proposition 1.1). □

Remark 6.4.2. If $k = \mathbf{C}$, then $C(\mathbf{C})$ is a Riemann surface with a well-defined topological genus. The topological genus is equal to the geometric genus.

135: Find a reference – Mumford?

Theorem 6.4.3 (Adjunction formula)**.** *Let C be a (possibly singular) curve in a smooth projective surface X. Let K be a canonical divisor on X. Then*

$$2p_a(C) - 2 = C \cdot (C + K).$$

Proof For non-singular curves, this is Hartshorne (1977, Chapter V, Proposition 1.5). The general case will follow easily from the Riemann–Roch Theorem. □

Remark 6.4.4. In particular, the adjunction formula shows that linearly equivalent effective divisors have the same arithmetic genus. Thus all curves of degree 3 in $\mathbf{P}^2$ have arithmetic genus 1, whether they are smooth or not. For example, the smooth cubic curve $y^2 = x(x-1)(x-2)$ has arithmetic genus 1, and indeed geometric genus 1. The nodal cubic $y^2 = x(x-1)^2$ and the cuspidal cubic $y^2 = x^3$ both also have arithmetic genus 1, although they are birational to $\mathbf{P}^1$ which has arithmetic and geometric genus 0.

Remark 6.4.5. The previous remark can be viewed as a special case of the following fact: arithmetic genus is constant in "continuously varying families" of projective varieties, by which we mean that it is locally constant on the fibres of a flat proper morphism. See Hartshorne (1977, Chapter III, Corollary 9.10) for further reading.

Exercise 6.4.6. Let C be a curve of degree d in $\mathbf{P}^2$. Show that $p_a(C) = (d-1)(d-2)/2$.

6.5 The Riemann–Roch Theorem

In many situations, it is very useful to know the number $\ell(D)$ associated to a divisor D, but so far we have no way of computing it in any but the simplest ex-

amples. The Riemann–Roch Theorem relates $\ell(D)$ to some intersection numbers. We will need one more definition.

Remark 6.5.1. There is another vector space which can be associated to a divisor D, the first sheaf cohomology group of X with values in $\mathscr{O}(D)$. We will rarely need to know anything about this vector space, other than that its dimension is (of course) non-negative. The reason we mention it at all is that it makes an appearance in the statement of the Riemann–Roch Theorem.

Definition 6.5.2. Let X be a smooth projective surface, and D a divisor on X. The *superabundance* of D, written $s(D)$, is defined by $s(D) = \dim \mathrm{H}^1(X, \mathscr{O}(D))$.

Theorem 6.5.3 (Riemann–Roch)**.** *Let X be a smooth, geometrically irreducible, projective surface over a field k. Let K be a canonical divisor on X, and let D be any divisor on X. Then*

$$\ell(D) - s(D) + \ell(K-D) = \tfrac{1}{2}D\cdot(D-K) + 1 + p_a(X).$$

Proof See Hartshorne (1977, Chapter V, Theorem 1.6). Although there the theorem is proved under the assumption that k is algebraically closed, all the quantities involved are preserved by moving from k to its algebraic closure: see Kollár et al. (2004, Exercise 3.34). □

Example 6.5.4. Let X be a smooth, geometrically irreducible, projective surface, let H be a hyperplane section of X, and let D be any divisor on X. Then, for n sufficiently large, $D+nH$ is equivalent to an effective divisor.

Proof Recall that $H^2 = \deg X > 0$ from Example 4.3.8. We deduce that

$$(K-(D+nH))\cdot H = K\cdot H - D\cdot H - n\deg X$$

is negative for n sufficiently large. Under that condition, applying the Riemann–Roch Theorem to $D+nH$ gives

$$\begin{aligned}\ell(D+nH) &\geq \tfrac{1}{2}(D+nH)\cdot(D+nH-K)+1+p_a(X)\\ &\geq \tfrac{1}{2}(n^2\deg X + n(2H\cdot D - H\cdot K) + D^2 - D\cdot K) + 1 + p_a(X)\end{aligned}$$

which is at least 1 for n sufficiently large, and therefore $D+nH$ is linearly equivalent to an effective divisor. □

136: deg D not defined, so changed it back to $H\cdot D$...

Remark 6.5.5. This can easily be generalised by replacing H with any ample divisor.

Exercise 6.5.6. Let X be a smooth, rational surface which can be embedded in $\mathbf{P}^n$ by its anticanonical divisor, i.e. such that $K_X = -H$ where H is a hyperplane section. Such a surface is a del Pezzo surface. In this case, $p_a(X) = 0$. For

example, X could be a cubic surface in $\mathbf{P}^3$ or the intersection of two quadrics in $\mathbf{P}^4$.

137: hmmm, we want "nice", so smooth, projective, geometrically integral, where the last thing means geometrically irreducible and something about ideal over $\bar{k}$ being generated by ideal over k for geometrically reduced. Or actually, that follows from smooth..., and geometrically connected would be fine, too. Put definition of "nice" in chapter on geometry!

(i) Let C be a smooth curve in X. Use the adjunction formula to show that $C^2 \geq -1$.

(ii) Conversely, let D be a divisor satisfying $D^2 \geq -1$ and $D.H > 0$. Use the Riemann–Roch Theorem to show that the linear equivalence class of D contains an effective divisor.

(iii) Let D be a divisor on X such that nD is principal for some positive integer n. Show that $D^2 = 0$. Using the Riemann–Roch theorem, deduce that $D \sim 0$ and therefore that $\mathrm{Pic}\, X$ is torsion-free.

7

Del Pezzo surfaces

[Martin: these three chapters could do with some re-organisation. I am putting this section on birational geometry here for now.]

Recall that a *birational map* $X \to Y$ of algebraic varieties is a dominant rational map $\phi\colon X \dashrightarrow Y$ that admits an inverse as a rational map, that is, there exists a dominant rational map $\psi\colon Y \dashrightarrow X$ such that $\psi \circ \phi = \mathrm{id}_X$ and $\phi \circ \psi = \mathrm{id}_Y$, where the compositions are given by composition of dominant rational maps. Equivalently, X and Y have isomorphic dense open subvarieties. A *birational morphism* is a birational map that is also a morphism. We say that two varieties X, Y are *birational* or *birationally equivalent* if there exists a birational map between them; this defines an equivalence relation on varieties.

Every dominant rational map between smooth, projective curves extends to a morphism; so two smooth, projective curves are birational if and only if they are isomorphic. In the case of curves, the relation of birational equivalence tells us nothing new. However, for higher-dimensional varieties, birational equivalence is strictly coarser than isomorphism, and classifying varieties up to birational equivalence is an important step towards classifying them up to isomorphism.

The most basic example of a birational morphism that is not an isomorphism is a blow-up. As we will see, in the case of surfaces all birational equivalences can be understood in terms of blow-ups.

7.1 Blowing up

In this section we review the definition and properties of blow-ups. Let X be a surface and let p be a point of X. Our aim is to define the *blow-up* of X at p, which is a smooth surface $\tilde{X} = \mathrm{Bl}_p X$ together with a morphism $\pi\colon \tilde{X} \to X$, such that

- the morphism π is an isomorphism outside $\pi^{-1}(p)$;
- the fibre $\pi^{-1}(p)$ is isomorphic to $\mathbf{P}^1$.

In particular, π is a birational morphism but not an isomorphism.

Before defining blow-ups more generally, we look at the example of blowing the affine plane $\mathbf{A}^2$ up at the origin. Almost all of the important features of blow-ups can be seen in this easily described example.

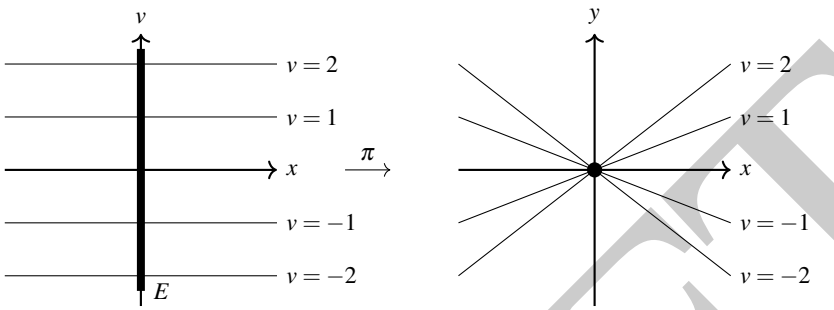
Example 7.1.1 (Blowing up $\mathbf{A}^2$)**.** Let k be any field and let $X = \mathbf{A}^2_k$ be the affine plane, with coordinates x, y. Let $\mathbf{P}^1_k$ be the projective line with coordinates u, v. The blow-up $\tilde{X}$ of X at the point $(0,0)$ can be described as the subvariety of $\mathbf{A}^2_k \times \mathbf{P}^1_k$ defined by the equation $xv = yu$, together with the morphism $\pi\colon \tilde{X} \to X$ given by $\pi((x,y),(u:v)) = (x,y)$. It is easily checked that $\tilde{X}$ is a smooth variety. If we think of $\mathbf{P}^1_k$ as parametrising the lines through $(0,0)$ in $\mathbf{A}^2_k$, then the equation $xv = yu$ simply specifies that the point (x,y) lies in the line defined by $(u:v)$, so we can think of $\tilde{X}$ as being described by this incidence relation. Alternatively, $\tilde{X}$ is the closure of the graph of the rational map $\mathbf{A}^2 \dashrightarrow \mathbf{P}^1$ given by projection away from the point $(0,0)$.

If $(a,b) \in \mathbf{A}^2$ is a point other than $(0,0)$, then $\pi^{-1}((a,b))$ consists of the single point $((a,b),(a:b))$. So π is an isomorphism outside $\pi^{-1}(0,0)$. On the other hand, $E = \pi^{-1}(0,0)$ consists of the whole fibre $(0,0) \times \mathbf{P}^1$, which is isomorphic to $\mathbf{P}^1$. E is called the *exceptional fibre* of the blow-up.

Let us look at the inverse images of some curves in $\mathbf{A}^2$. The x-axis L_1 is defined by the equation $y = 0$, so $\pi^{-1}(L_1)$ is cut out in $\mathbf{A}^2 \times \mathbf{P}^1$ by the equations $y = 0$ and $xv = 0$. This is the union of the set $\{x = y = 0\}$, which is the exceptional fibre E, and the set $\tilde{L}_1 = \{y = v = 0\}$, which consists of all points of the form $\{((a,0),(1:0))\}$ and is mapped isomorphically onto L_1 by π. We call $\tilde{L}_1$ the *strict transform* of L_1; another way to describe $\tilde{L}_1$ is that it is the closure in $\tilde{X}$ of $\pi^{-1}(L \setminus \{(0,0)\})$. The two components E and $\tilde{L}_1$ of $\pi^{-1}(L_1)$ meet in the point $((0,0),(1:0))$ of E. Similarly, the y-axis L_2 is defined by $x = 0$, and we find that $\pi^{-1}(L_2)$ consists of two components, E and $\tilde{L}_2$, meeting in the point $((0,0),(0:1))$. Here we see one important feature of blowing up: although the axes both pass through the point $(0,0)$, their strict transforms in $\tilde{X}$ are disjoint! By "replacing" the point $(0,0)$ with the projective line E, we have separated the two axes so that they no longer intersect. More generally, one can show the following, for any smooth irreducible curve $C \subset \mathbf{A}^2$ passing through $(0,0)$: the inverse image $\pi^{-1}(C)$ consists of E together with a curve $\tilde{C}$, the Zariski closure of $\pi^{-1}(C \setminus \{(0,0)\})$, that is mapped isomorphically to C by π, and $\tilde{C}$ meets E at the point corresponding to the tangent direction of C at $(0,0)$.

For many calculations, it easier to work with affine varieties, so we describe

the two affine patches of $\tilde{X}$ and how they map to $X = \mathbf{A}^2$. Consider the affine piece $\mathbf{A}^2 \times \mathbf{A}^1 \subset \mathbf{A}^2 \times \mathbf{P}^1$ given by $u \neq 0$; the intersection U of $\tilde{X}$ with this affine piece is defined by the equation $xv = y$. Projection to the coordinates (x, v) restricts to an isomorphism $U \to \mathbf{A}^2$, so the map $\pi\colon U \to X$ can be identified with the morphism $\mathbf{A}^2 \to \mathbf{A}^2$ defined by $(x, v) \mapsto (x, xv)$.



On each vertical line apart from $x = 0$, π acts as multiplication by a non-zero scalar (the x-coordinate of the line). However, the entire v-axis in the x, v-plane is "squashed" down to the point $(0, 0)$ in the x, y-plane. Note that, in this picture, the image of π does not contain any points of the y-axis apart from $(0, 0)$. Of course, the whole y-axis does lie in the image of π, but in the image under π of the other affine piece of $\tilde{X}$ that we cannot see in this picture.

In this affine piece, we can carry out some useful calculations. Again, let $L_1 \subset X$ be the x-axis. We have already seen that $\pi^{-1}(L_1)$ consists of the union of the x-axis $\tilde{L}_1$ and the v-axis E. Working in this affine piece, it is easy to see to compute the pull-back of L_1 as a divisor: $\pi^*(L_1) = (y) = (xv) = \tilde{L}_1 + E$. Moreover, we can see that $\tilde{L}_1$ and E meet transversely, allowing us to compute their intersection number: $\tilde{L}_1 \cdot E = 1$.

The other affine piece of $\tilde{X}$, described by $v \neq 0$, is similarly isomorphic to the u, y-plane. Following the various isomorphisms shows that $\tilde{X}$ is obtained by gluing two copies of $\mathbf{A}^2$, the first with coordinates (x, v) and the second with coordinates (u, y), using the mutually inverse isomorphisms

$$(x, v) = (uy, u^{-1}), \qquad (u, y) = (v^{-1}, xv)$$

defined on $\{u \neq 0\}$ and $\{v \neq 0\}$ respectively.

We conclude this long example with a calculation of the self-intersection number E^2. Remember that intersection numbers are invariant under linear equivalence on a projective variety, so we will need to blow up $\mathbf{P}^2$ instead of $\mathbf{A}^2$. Let Y be $\mathbf{P}^2_k$, and define $\pi\colon \tilde{Y} \to Y$ by blowing up one affine piece (which we identify with X) at its origin P and leaving the other two affine pieces unchanged. Let L be any line in Y not passing through P; then L is linearly

equivalent to the x-axis L_1 and $\pi^*(L)$ does not meet E. Since π^* respects linear equivalence, $\pi^*(L)$ is linearly equivalent to $\pi^*(L_1)$. Using the calculations above, we compute

$$0 = \pi^*(L)\cdot E = \pi^*(L_1)\cdot E = (\tilde{L}_1 + E)\cdot E = 1 + E^2,$$

showing $E^2 = -1$.

We will now define the blowing up of any variety X over a field k at any point $P \in X(k)$. It suffices to define the blow-up for X affine, since in general we can choose an affine piece U containing P and obtain the blow-up of X by gluing the blow-up of U to the remaining affine pieces of X. So assume that X is an affine variety in $\mathbf{A}^n_k$, and that P is the origin of $\mathbf{A}^n$ (which we can achieve by performing a translation defined over k).

Define the blow-up $\tilde{\mathbf{A}}^n$ of $\mathbf{A}^n$ at P to be the subvariety of $\mathbf{A}^n \times \mathbf{P}^{n-1}$ defined by the equations $x_i u_j = x_j u_i$, where $x_1, \ldots, x_n$ are the coordinates on $\mathbf{A}^n$, $u_1, \ldots, u_n$ are the coordinates on $\mathbf{P}^{n-1}$, and i, j run over all values from 1 to n. Let $\pi\colon \tilde{\mathbf{A}}^n \to \mathbf{A}^n$ be the natural projection, and let $E' \cong \mathbf{P}^{n-1}$ be $\pi^{-1}(P)$.

Definition 7.1.2. The *blow-up* of X at P, written $\mathrm{Bl}_P(X)$, is defined to be $\tilde{X}$, the strict transform of X, that is, the Zariski closure in $\tilde{\mathbf{A}}^n$ of $\pi^{-1}(X \smallsetminus \{P\})$, equipped with the morphism $\phi\colon \tilde{X} \to X$ that is the restriction of π. The subset $E = \phi^{-1}(P) = \tilde{X} \cap E'$ is the *exceptional fibre* of the blow-up.

In order to prove results about $\tilde{X}$, it is helpful to have a description of the affine pieces. As in Example 7.1.1, these are given by $u_i \neq 0$ for $i = 1, \ldots, n$. Since they all have similar descriptions, we take $i = 1$ for ease of notation. Let $U \subset \tilde{\mathbf{A}}^n$ be defined by $u_1 \neq 0$. The equations defining U within $\mathbf{A}^n \times \mathbf{A}^{n-1}$ are $x_1 u_j = x_j$ for $j \neq 1$, together with $x_i u_j = x_j u_i$ for $1, i, j$ distinct; but these follow from $x_1 u_j = x_j$. It follows that projection to the coordinates $x_1, u_2, \ldots, u_n$ defines an isomorphism $U \cong \mathbf{A}^n$, and we will use these coordinates on U from now on. The exceptional fibre E' is defined within U by $x_1 = 0$.

The first task is to find defining equations for $\tilde{X} \cap U$. Equations for the inverse image $\pi^{-1}(X) = \tilde{X} \cup E'$ are easily obtained by taking polynomials $f \in I(X) \subset k[x_1, \ldots, x_n]$ and substituting $x_j = x_1 u_j$ for $j = 2, \ldots, n$. Consider what the result looks like: every monomial of degree d appearing in f gives rise to a monomial consisting of x_1^d multiplied by a monomial of degree $\leq d$ in $u_2, \ldots, u_n$. We obtain

$$f(x_1, x_1 u_2, \ldots, x_1 u_n) = x_1^{d_f} \tilde{f} \tag{7.1}$$

for some $\tilde{f} \in k[x_1, u_2, \ldots, u_n]$ not divisible by x_1, with d_f being the minimal degree of a monomial in f. Note that $d_f \geq 1$, since $P = (0, \ldots, 0)$ lies in X.

Lemma 7.1.3. *The affine variety $\tilde{X} \cap U$ safisfies*

$$I(\tilde{X} \cap U) = \{\tilde{f} : f \in I(X)\},$$

where $\tilde{f}$ is defined as in (7.1)*.*

Proof The strict transform $\tilde{X}$ is irreducible, being the closure of the irreducible set $\pi^{-1}(X \setminus \{P\})$. Therefore $I(\tilde{X} \cap U) \subset k[x_1, u_2, \ldots, u_n]$ is a prime ideal. As calculated above, the polynomial $x_1^{d_f} \tilde{f}$ lies in $I(\tilde{X} \cap U)$, but $x_1^{d_f}$ does not, showing $\tilde{f} \in I(\tilde{X} \cap U)$.

Conversely, let $g \in I(\tilde{X} \cap U)$. The restriction of π to $U \setminus \{x_1 = 0\}$ is an isomorphism, and the corresponding isomorphism of coordinate rings is given by

$$\pi^* \colon k[x_1, x_1^{-1}, x_2, \ldots, x_n] \to k[x_1, x_1^{-1}, u_2, \ldots, u_n]$$

with $\pi^*(x_j) = x_1 u_j$ for $j \geq 2$. Under this isomorphism, the ideals generated by $I(X)$ on the left and $I(\tilde{X} \cap U)$ on the right correspond: this is the definition of $\tilde{X}$. Therefore we have $x_1^r g = \pi^*(f)$ for some $f \in I(X)$ and $r \geq 0$. Since $\pi^*(f) = x_1^{d_f} \tilde{f}$, it follows by unique factorisation that $g = \tilde{f}$. □

We now relate the geometry of the exceptional fibre $E = \pi^{-1}(P)$ to the local geometry of X at P. We first recall some definitions. For a polynomial $f \in k[x_1, \ldots, x_n]$, let $f = f^{(0)} + f^{(1)} + \ldots f^{(d)}$ be the decomposition of f into homogeneous polynomials, where $f^{(i)}$ is homogeneous of degree i. We define $m(f)$ to be the *initial term* of f, that is, $m(f) = f^{(i)}$ where i is the least non-negative integer such that $f^{(i)} \neq 0$. Note that f vanishes at $P = (0, 0, \ldots, 0)$ if and only if $f^{(0)} = 0$.

Definition 7.1.4. Let $X \subset \mathbf{A}^n$ be a variety containing the point $P = (0, 0, \ldots, 0)$. The (geometric) *tangent space* to X at P is the variety defined by the linear polynomials $\{f^{(1)} : f \in I(X)\}$. The *tangent cone* to X at P is the variety defined by the initial terms $\{m(f) : f \in I(X)\}$.

After a suitable translation, the same definition gives the tangent space and tangent cone at any other k-point of X. It is clear from the definitions that the tangent space is a linear subspace of $\mathbf{A}^n$ that contains the tangent cone; the following lemma described when they are equal.

Lemma 7.1.5. *Let $X \subset \mathbf{A}^n$ be a variety containing $P = (0, 0, \ldots, 0)$.*

(i) *Let $f_1, \ldots, f_m$ be generators for the ideal $I(X)$. The tangent space to X at P has dimension $n - r$, where r is the rank of the Jacobian matrix $(\partial(f_1, \ldots, f_m)/\partial(x_1, \ldots, x_n))(P)$. In particular, the dimension of the tangent space equals* $\dim X$ *if and only if X is smooth at P.*

(ii) *The tangent cone to X at P has dimension* $\dim X$.
(iii) *The tangent space and tangent cone to X at P coincide if and only if X is smooth at P.*

Proof To prove (i), note first that the linear polynomials $f_1^{(1)}, \ldots, f_m^{(1)}$ define the tangent space to X at P. Identifying linear forms with row vectors, the ith row of the Jacobian matrix is given by $f_i^{(1)}$, and so the tangent space is nothing other than the kernel of the Jacobian matrix. Its dimension is therefore $n-r$.

The proof of (ii) is more complicated, but the first step is straightforward and interesting in its own right. Namely, the local ring $\mathscr{O}_{X,P}$, with maximal ideal $\mathfrak{m}_P$, has an associated graded ring defined by $\mathrm{gr}(\mathscr{O}_{X,P}) = \bigoplus_i \mathfrak{m}_P^i/\mathfrak{m}_P^{i+1}$. Let I be the ideal defining the tangent cone, that is, the ideal generated by all $m(f)$ for $f \in I(X)$. Then it is easy to show that the natural homomorphism $k[x_1,\ldots,x_n]/I \to \mathrm{gr}(\mathscr{O}_{X,P})$ which sends each x_i to its class in $\mathrm{gr}(\mathscr{O}_{X,P})$ is an isomorphism. (In particular, this shows that the tangent cone is independent of the embedding of X in affine space.) To complete the proof, use the fact that the associated graded ring of a local ring has the same dimension as the local ring itself.

138: Find a reference for this: Atiyah–Macdonald?

Finally, (iii) follows from (i) and (ii): if X is not smooth at P, then the tangent space and the tangent cone have different dimensions, so are certainly not equal; of X is smooth at P, then the tangent cone is an algebraic set contained in the tangent space, which is irreducible and of the same dimension, so they are equal. □

The tangent cone is defined by homogeneous polynomials, so it is the affine cone over a variety in $\mathbf{P}^{n-1}$, called the *projectivised tangent cone*.

Proposition 7.1.6. *Let $\phi\colon \tilde{X} \to X$ be the blow-up in a point $P \in X(k)$. The exceptional divisor $E = \phi^{-1}(P)$ is naturally isomorphic to the projectivised tangent cone of X at P.*

Proof We may assume that X is a subvariety of $\mathbf{A}^n$ and $P = (0,0,\ldots,0)$ and use the notation as above. Let $\pi\colon \tilde{\mathbf{A}}^n \to \mathbf{A}^n$ be the blow-up at P, and let $E' \cong \mathbf{P}^{n-1}$ be $\pi^{-1}(P)$. We will show that $E = \tilde{X} \cap E'$ is defined in E' by the homogeneous polynomials $m(f)$ for $f \in I(X)$, which are precisely the polynomials defining the tangent cone. It suffices to do this on each standard affine piece of E', so we look at the affine piece $U \cong \mathbf{A}^{n-1}$ defined by $u_1 \neq 0$. Within U, the exceptional fibre $E' \cap U$ is defined by $x_1 = 0$.

By Lemma 7.1.3, the variety $\tilde{X} \cap U$ is defined by the polynomials $\tilde{f}$ for $f \in I(X)$, where $\tilde{f}$ is as in (7.1). To find equations for E, we substitute $x_1 = 0$ in these equations. Fix $f \in I(X)$ and consider what happens to each monomial of f. Any monomial of degree greater than d_f gives rise to a monomial in $\tilde{f}$

that is divisible by x_1, which therefore disappears when we substitute $x_1 = 0$. Any monomial of degree d_f survives but loses any power of x_1, equivalent to substituting $x_1 = 1$ in this monomial. We deduce that $E \cap U$ is defined by polynomials

$$\{m(f)(1, u_2, \ldots, u_n) : f \in I(X)\},$$

which are indeed the polynomials defining the corresponding affine piece of the projectivised tangent cone. □

Combining this proposition with Lemma 7.1.5 gives:

Corollary 7.1.7. *Let $X \subset \mathbf{A}^n$ be an affine variety of dimension d and let P be a smooth point of X. Then the exceptional fibre of the blow-up $\mathrm{Bl}_P(X) \to X$ is isomorphic to $\mathbf{P}^d$.*

strict transform of smooth curve through P meets E transversely, deduce $E^2 = -1$. Smoothness of $\tilde{X}$?

In this chapter we describe the geometry of an important class of surfaces, the del Pezzo surfaces. These are only a little more complicated than projective space, and yet their arithmetic is not completely understood. In particular, they can provide counterexamples to the Hasse principle, as we have seen in Chapter 2.

A good reference for the material in this chapter is Chapter 6 of Bjorn Poonen's notes (Poonen, 2008).

7.2 Definitions

Let k be any field and let $\bar{k}$ be an algebraic closure of k. Let X a smooth, projective, geometrically irreducible variety over k and let K_X be a canonical divisor on X.

Definition 7.2.1. The variety X is called *rational* if $X_{\bar{k}}$ is birationally equivalent to $\mathbf{P}^n_{\bar{k}}$ for some n.

Definition 7.2.2. The variety X is called a *Fano variety* if $-K_X$ is ample.

For instance, smooth hypersurfaces of degree at most n in $\mathbf{P}^n$ are examples of Fano varieties.

Definition 7.2.3. A *del Pezzo surface* is a Fano variety X of dimension 2. The *degree* of X is the self-intersection number $K_X \cdot K_X$.

Note that if $-K_X$ is very ample, then it determines an embedding of X into $\mathbf{P}^n$ for some n, under which $-K_X$ corresponds to a hyperplane section H. The

degree of this embedding is H^2 (see Example 4.3.8), which explains why the integer $(-K_X)^2$ is called the degree of a del Pezzo surface X.

Proposition 7.2.4. *If X is a rational surface, then X is k-birational to either a del Pezzo surface or a conic bundle over a conic.*

139: Find reference

Proposition 7.2.5. *The degree of a del Pezzo surface is positive.*

Proof Note that a very ample divisor H on any variety intersects every effective curve with positive intersection number, so in particular $H^2 > 0$. Therefore, if D is any ample divisor, so that, for some positive integer n, the divisor nD is very ample, then the inequality $0 < (nD)^2 = n^2D^2$ holds, and hence also $D^2 > 0$. The statement now follows from the fact that $-K_X$ is ample. □

7.3 Blowing up surfaces

A very important tool in birational geometry is the blow-up. In this section we review the definition and properties of blow-ups.

Let X be a surface and let p be a point of X. The *blow-up* of X at p is a smooth surface $\tilde{X} = \mathrm{Bl}_p X$, together with a morphism $\pi\colon \tilde{X} \to X$, such that

- the morphism π is an isomorphism outside $\pi^{-1}(p)$;
- the fibre $\pi^{-1}(p)$ is isomorphic to $\mathbf{P}^1$.

In particular, π is a birational morphism.

d: Make sure we define "birational".

The fibre $E = \pi^{-1}(p)$ is called the *exceptional divisor* of the blow-up. It can be thought of as a copy of the projectivised tangent space to X at p: there is one point of E for each tangent direction to X passing through E. Let C be a curve in X passing through p with multiplicity 1; then the closure of $\pi^{-1}(C \setminus p)$ is a curve in $\tilde{X}$, which intersects E in a unique point. Two curves in X passing through p will meet $E \subset \mathrm{Bl}_p(X)$ in the same point if and only if they have the same tangent direction at p.

d: ...and "multiplicity"!

Example 7.3.1. We will describe the affine plane $\mathbf{A}^2$ with coordinates x, y, blown up at the origin p. The variety $\tilde{X} = \mathrm{Bl}_p \mathbf{A}^2$ is not affine, and we describe it by gluing together two affine pieces.

One affine piece U is isomorphic to another copy of $\mathbf{A}^2$. Let u, v be the coordinates on U; then the morphism $\pi\colon U \to \mathbf{A}^2$ is given by $(x, y) = (u, uv)$. This is an isomorphism on the open set $\{u \neq 0\}$, and maps the whole affine line $\{u = 0\}$ to the point p. However, we cannot see quite the whole picture in this affine piece: the exceptional divisor is missing one point at infinity, and the

image of π is missing the y-axis. Notice how the lines $\{v = c\}$, which intersect the exceptional divisor in distinct points, are mapped to the lines $\{y = cx\}$, which go through the point p in different tangent directions.

The other affine piece U' looks identical: it is a copy of $\mathbf{A}^2$ with coordinates u', v', and the map $\pi' \colon U' \to \mathbf{A}^2$ is $(x,y) = (u'v', v')$. To obtain the variety $\tilde{X}$, we glue the two pieces U, U' together using the inverse pair of morphisms

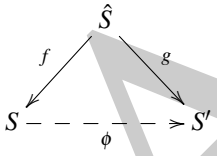
$$(u,v) = (u'v', \frac{1}{u'}), \qquad (u', v') = (\frac{1}{v}, uv)$$

which are defined on the open sets $\{u' \neq 0\}$ and $\{v \neq 0\}$ respectively. Under this gluing, the two affine lines $\{u = 0\} \subset U$ and $\{v' = 0\} \subset U'$, which are collapsed by π and π' respectively, glue to give a copy of $\mathbf{P}^1$, the exceptional divisor of the blow-up.

The central position of blow-ups in the birational geometry of surfaces is described by the following theorem.

140: Is a surface automatically projective?

Theorem 7.3.2. *Let $\phi \colon S \dashrightarrow S'$ be a birational map of surfaces. Then there is a surface $\hat{S}$ and a commutative diagram*



where the morphisms f, g are composites of blow-ups and isomorphisms.

d: This is also contained in (Hartshorne, 1977, Theorem V.5.5).

Proof For a proof stated over the complex numbers see Beauville (1996, Corollary II.12). □

Let C be an irreducible curve in X, and let $\pi \colon \tilde{X} \to X$ be the blow-up of X at a point p. If C passes through p, then there are different notions of the inverse image of C under π; it is clear what this should mean away from p (where π is an isomorphism), so we describe the difference near p. The inverse image of C under π as a divisor, written $\pi^* C$, is defined by taking a function f such that $(f) = C$ on some neighbourhood of p, pulling f back to $\tilde{X}$, and taking $\pi^* C = (\pi^* f)$. This divisor is called the *total transform* of C; it may contain the exceptional divisor with some multiplicity. On the other hand, we may also take the closure of $\pi^{-1}(C \setminus p)$; this is an irreducible curve in $\tilde{X}$, called the *strict transform* of C.

Proposition 7.3.3. *Suppose that C is a curve in X which has multiplicity m at p. Let C' denote the strict transform of C, and E the exceptional divisor. Then $\pi^* C = C' + mE$, and $C' \cdot E = m$.*

Proof See Hartshorne (1977, Proposition V.3.6). □

Proposition 7.3.4. *Suppose $\tilde{X} = \mathrm{Bl}_p(X)$ is the blow-up of a smooth surface X at a point p, with corresponding map $\pi\colon \tilde{X} \to X$. Let K_X and $K_{\tilde{X}}$ be canonical divisors on X and $\tilde{X}$ respectively, and let E denote the exceptional divisor on $\tilde{X}$ above p. Then E is isomorphic to $\mathbf{P}^1$, and $K_{\tilde{X}}$ is linearly equivalent to $\pi^* K_X + E$. Moreover, the map $\rho\colon \mathrm{Pic}X \oplus \mathbf{Z} \to \mathrm{Pic}\tilde{X}$ sending (D,n) to $\pi^* D + nE$ is an isomorphism. We have $E^2 = -1$, and for all $C, D \in \mathrm{Pic}X$ we have $(\pi^* C)\cdot(\pi^* D) = C \cdot D$ and $(\pi^* C)\cdot E = 0$. In particular, we have $K_{\tilde{X}} \cdot E = -1$.*

d: The isomorphism of E with $\mathbf{P}^1$ is a consequence of our definition of blow up.

Proof See Hartshorne (1977, Propositions V.3.1–3). □

Exercise 7.3.5. Suppose the setting of Proposition 7.3.4. Assume that you already know $E^2 = -1$. Prove that the map ρ is an isomorphism. (Hint: use that leaving out a closed subset of codimension 2 does not change the Picard group, while leaving out an irreducible closed subset of codimension 1 gives an exact sequence you have seen before.) Now also prove the rest of the theorem.

There is a partial converse to Proposition 7.3.4, which gives a criterion under which a curve can be blown *down*.

Theorem 7.3.6 (Castelnuovo's criterion)**.** *Let X be a smooth surface, and let E be a smooth curve in X such that $E^2 = -1$ and $E \simeq \mathbf{P}^1$. Then there exists a morphism $\pi\colon X \to Y$, with Y a smooth variety, such that π is an isomorphism away from E, and the image of E is a point in Y.*

Proof See Hartshorne (1977, Theorem V.5.7). □

Remark 7.3.7. In order to show that an integral curve E is isomorphic to $\mathbf{P}^1$, it suffices to show that the arithmetic genus of E is zero (see Hartshorne, 1977, Exercise IV.1.8(b)). We sometimes use this remark without mentioning it explicitly.

7.4 Del Pezzo surfaces as blow-ups

The following theorem describes how all del Pezzo surfaces, over the algebraic closure of the base field, become isomorphic to certain surfaces described simply using blow-ups.

Let r be an integer satisfying $0 \leq r \leq 8$ and let $p_1, \ldots, p_r$ be r distinct points in $\mathbf{P}^2$. We say that $p_1, \ldots, p_r$ are in *general position* if the following hold:

- no three of the points lie on a line,
- no six of the points lie on a conic,

- no eight of the points lie on a singular cubic, with one of these eight points at the singular point.

Theorem 7.4.1. *Suppose that k is algebraically closed and that X is a del Pezzo surface over k. Then X is isomorphic to either $\mathbf{P}^1 \times \mathbf{P}^1$, or to the blow-up of $\mathbf{P}^2$ in distinct points $p_1, \ldots, p_r$ in general position, where $0 \leq r \leq 8$. The degree of $\mathbf{P}^1 \times \mathbf{P}^1$ is 8. If X is the blow-up of $\mathbf{P}^2$ in r points, then its degree is $9-r$. Conversely, any blow-up of $\mathbf{P}^2$ in at most 8 points in general position is a del Pezzo surface.*

The full proof of Theorem 7.4.1 is not very deep, but too long to present here. Instead, we will break up the proof in parts. Assuming parts of the conclusion, we can prove the rest fairly easily. The following proposition therefore reclaims only part of the previous theorem.

Proposition 7.4.2. *Suppose that k is algebraically closed and that X is a del Pezzo surface over k. Then either X is isomorphic to $\mathbf{P}^1 \times \mathbf{P}^1$, or X is the blow-up of $\mathbf{P}^2$ in distinct points $p_1, \ldots, p_r$.*

141: Separably closed is good enough. See Tony's notes, though Bjorn's book might be better, as I think there was a problem with the reference [Coo] that Tony uses.

Proof See Manin (1986, Theorem 24.4). □

For the rest of this chapter, let X be a del Pezzo surface with canonical divisor K.

Corollary 7.4.3. *If the del Pezzo surface X is the blow-up of $\mathbf{P}^2$ in distinct points $p_1, \ldots, p_r$, then $r \leq 8$ and the degree of X equals $9-r$.*

Proof The canonical divisor $K_{\mathbf{P}^2}$ on $\mathbf{P}^2$ is linearly equivalent to $-3L$ where L is any line, so $K^2_{\mathbf{P}^2} = 9L^2 = 9$. Let $\pi\colon X \to \mathbf{P}^2$ be the blow-up of the points $p_1, \ldots, p_r$; for $i \in \{1, \ldots, r\}$, let E_i be the exceptional divisor lying above p_i. According to Proposition 7.3.4, we have $K_X \sim \pi^*(-3L) + \sum_i E_i$. Picking $L \subset \mathbf{P}^2$ to be a line which does not pass through any of the p_i, we have $(\pi^* L)^2 = L^2$ and $(\pi^* L) \cdot E_i = 0$ for all i. Similarly $E_i \cdot E_j = 0$ for $i \neq j$. Then

$$K_X^2 = (\pi^*(-3L))^2 + \sum_{i=1}^{r} E_i^2 = 9 - r.$$

From Proposition 7.2.5 we find $9 - r > 0$, so $r \leq 8$. □

Proposition 7.4.4. *If C is a closed integral curve on X, then $C^2 \geq -1$. Furthermore, equality implies $p_a(C) = 0$ and $K_X \cdot C = -1$.*

Proof The adjunction formula (Theorem 6.4.3) gives

$$C^2 + C \cdot K = 2p_a(C) - 2 \geq -2,$$

while $C \cdot K < 0$ since $-K$ is ample. □

If we have $C^2 = -1$, then, by Proposition 7.4.4, C satisfies the hypotheses of Castelnuovo's criterion (Theorem 7.3.6), and can therefore be blown down. We call C an *exceptional curve*.

Proposition 7.4.5. *Suppose Y is the blow-up of $\mathbf{P}^2$ in r distinct points, exactly s of which lie on the line L. Then the strict transform of L on Y has self-intersection $L^2 = 1 - s$.*

Proof Let $\pi\colon Y \to \mathbf{P}^2$ denote the blow-up. Let $E_1, \dots, E_s$ denote the exceptional curves above the s points on L. Let L' denote the strict transform of L on Y. Then, by Proposition 7.3.3, $\pi^* L = L' + \sum_{i=1}^{s} E_i$, so

$$1 = L^2 = (\pi^* L)^2 = (L' + \sum E_i)^2 = L'^2 + 2\sum L' \cdot E_i + \sum E_i^2.$$

Now $L \cdot E_i = 1$ and $E_i^2 = -1$ for each i. Therefore $L^2 = L'^2 + 2s - s$, so $L'^2 = 1 - s$. □

Corollary 7.4.6. *If the del Pezzo surface X is the blow-up of $\mathbf{P}^2$ in r points, then no three of these points are collinear.*

Proof This follows immediately from Propositions 7.4.5 and 7.4.4. □

Exercise 7.4.7. Show that if the del Pezzo surface X is the blow-up of $\mathbf{P}^2$ in r points, then no six of them lie on a conic.

Exercise 7.4.8. Show that if the del Pezzo surface X is the blow-up of $\mathbf{P}^2$ in 8 points, then they do not lie on a singular cubic that has its singular point at one of the 8 points.

The conditions of Corollary 7.4.6 and Exercises 7.4.7 and 7.4.8 together are summarized by saying that the r points must be in general position. Conversely, one can show that if $r \leq 6$ points on $\mathbf{P}^2$ are in general position, then the blow-up of $\mathbf{P}^2$ in those points is indeed a del Pezzo surface (see Manin, 1986, Theorem 24.5). For $r = 6$ we get the famous cubic surfaces in $\mathbf{P}^3$: see Hartshorne (1977, Section V.4). For $r = 7$ or $r = 8$, life gets significantly more complicated because then the anticanonical sheaf is no longer very ample, just ample (c.f. Manin, 1986, Remark 26.3). For a proof that even in this case, the converse mentioned in Theorem 7.4.1 is still true, see Demazure (1980, Theorem 1).

d: Those conditions are enough also for $r = 7$; should we mention it?

If X is the blow-up of $\mathbf{P}^2$ in $r \leq 8$ points, then Proposition 7.4.5 states that the strict transform of the line through any two of the points is an exceptional curve. The following exercise gives more exceptional curves.

Exercise 7.4.9. Suppose that X is the blow-up of $\mathbf{P}^2$ in $r \leq 8$ points $p_1, \dots, p_r$

in general position. Then the strict transform of each of the following curves in $\mathbf{P}^2$ are exceptional curves:

(i) a line containing 2 of the points;
(ii) a conic containing 5 of the points;
(iii) a cubic containing 7 of the points such that one of them is a double point (on that cubic);
(iv) a quartic containing 8 of the points such that three of them are double points;
(v) a quintic containing 8 of the points such that six of them are double points;
(vi) a sextic containing 8 of the points such that seven of them are double points and one is a triple point.

Remark 7.4.10. All the curves mentioned in Exercise 7.4.9 satisfy $(-K)\cdot C = 1$. If $-K$ is very ample, i.e., $r \leq 6$, then it determines an embedding into $\mathbf{P}^n$, and the image of all exceptional curves are lines: see Example 4.3.10. Together with the fibres above the points blown up, the curves described in Exercise 7.4.9 are in fact an exhaustive list of all exceptional curves on X (see Manin, 1986, Theorem 26.2). Proving this requires a better understanding of the Picard group of X, which we will work on next.

d: Should we say that the proof of this proposition follows at once from Proposition 7.3.4 and the fact that $\operatorname{Pic}\mathbf{P}^2 = \mathbf{Z}$?

Proposition 7.4.11. *Suppose X is the blow-up of $\mathbf{P}^2$ in $r \leq 8$ points $p_1, \ldots, p_r$ in general position. Let E_i denote the exceptional curve above p_i and let L denote the pull back of a line in $\mathbf{P}^2$. Then $\operatorname{Pic} X$ is generated by L and the E_i, with $-K_X \sim 3L - \sum E_i$. The intersection numbers are given by $L^2 = 1$, $L\cdot E_i = 0$, and $E_i \cdot E_j = -\delta_{ij}$.*

The intersection pairing turns the Picard group into a unimodular lattice of signature $(1,r)$. In particular this means that if we know a divisor up to numerical equivalence, then we know its divisor class. This will prove extremely useful in studying not only the geometry of the surface, but also the arithmetic. For instance, we get a representation of the absolute Galois group $\operatorname{Gal}(\bar{k}/k)$ into the automorphism group of this lattice. Better yet, since the canonical class $[K]$ is fixed under the Galois action, we get a representation into the automorphism group of the orthogonal complement of $[K]$, which is a root lattice.

d: Did we define this notation for divisor classes?

Proposition 7.4.12. *Suppose that C is an integral curve on X satisfying $C^2 = -1$. Then there is no other effective divisor D that is linearly equivalent to C.*

Proof Suppose that D is an effective divisor that is linearly equivalent to C. If D does not have C in its support, then D and C intersect in finitely many points, so $D\cdot C \geq 0$, which contradicts $D\cdot C = C^2 = -1$. We conclude that

D does have C in its support, so $D-C$ is an effective divisor that is linearly equivalent to 0, so $D-C=0$ and $D=C$. □

Proposition 7.4.12 is often phrased by saying that curves with negative selfintersection do not move.

We have already seen that, if C is an integral curve on X with $C^2=-1$, then we also have $(-K)\cdot C=1$, so by the adjunction formula $p_a(C)=0$ and so C is an exceptional curve. We now also define the notion of an exceptional divisor class, namely as a class D satisfying $D^2=-1$ and $K\cdot D=1$. Every exceptional curve represents an exceptional divisor class and Proposition 7.4.12 states that every exceptional divisor class contains at most one exceptional curve. In fact, a stronger statement is true.

Proposition 7.4.13. *Every exceptional divisor class contains exactly one exceptional curve.*

Proof Let D be any divisor in an exceptional divisor class. Note that for rational surfaces we have $\chi(\mathcal{O}_X)=1$. Therefore, the Riemann–Roch Theorem gives

142: Need a reference or proof for this.

$$\ell(D)-s(D)+\ell(K-D)=\frac{1}{2}D\cdot(D-K)+1+p_a(X)=1.$$

From $(-K)\cdot(K-D)=-K^2-1<0$ we see that no effective divisor is linearly equivalent to $K-D$, so $\ell(K-D)=0$. Hence $\ell(D)\geq 1$, which implies that there is indeed an effective divisor D' that is linearly equivalent to D. Since $(-K)$ intersects every irreducible curve in the support of D' positively, and $(-K)\cdot D'=1$, we see that D' is irreducible, and therefore an exceptional curve. By Proposition 7.4.12 it is the only exceptional curve in the class. □

Proposition 7.4.14. *Suppose that the del Pezzo surface X is the blow-up of $\mathbf{P}^2$ in $r\leq 8$ points $p_1,\ldots,p_r$ in general position. Then the fibres above the p_i and the curves in Exercise 7.4.9 are exactly all the exceptional curves on X.*

Proof By Proposition 7.4.13 it suffices to count the number of exceptional divisor classes in the Picard lattice. As every divisor class is uniquely represented by $D=aL-\sum_{i=1}^r b_iE_i$ for some a and b_i, we are counting the solutions to the equations $1=D\cdot(-K)=3a-\sum b_i$ and $-1=D^2=a^2-\sum b_i^2$. Setting $b_0=1$ for convenience, the first equation becomes $3a=\sum_{i=0}^r b_i$, under which the second becomes equivalent to $\sum_i(a-3b_i)^2=18$. This clearly gives finitely many solutions, all of which can be enumerated easily. □

Exercise 7.4.15. Determine the number of exceptional curves on a del Pezzo surface of degree d for each d (getting two possibilities for degree 8).

8

The Segre–Manin Theorem

8.1 Preliminary remarks

Let k be a field, $\bar{k}$ an algebraic closure of k and let X be a del Pezzo surface defined over k. Recall that X is a smooth projective surface defined over k whose anticanonical divisor is ample. Moreover, $\bar{X}$ is isomorphic to either $\mathbb{P}^1 \times \mathbb{P}^1$ or to the blow-up of $\mathbb{P}^2$ at $r \leq 8$ points in general position. In this lecture we focus on the structure of X in the case in which k is not necessarily algebraically closed. For our peace of mind, we shall assume that k is perfect. We use this assumption to deduce that an exceptional curve C on X, fixed by the action of the Galois group, is defined over k; *a priori*, we can only deduce that the divisor class of C is defined over a purely inseparable extension of k. It is a general fact that since $\mathrm{H}^1\big(X, \mathscr{O}_X\big) = (0)$, every divisor class on X defined over $\bar{k}$ is in fact defined over a separable closure of k.

The Segre–Manin Theorem addresses the question of k-unirationality of del Pezzo surfaces.

Definition 8.1.1. A variety X defined over a field k is k-unirational if there exists a rational variety Y defined over k and surjective morphism $Y \to X$ defined over k.

To check k-unirationality of X it suffices to assume that there is a dense open subset of X that is the image of an open subset of $\mathbf{P}_k^{\dim X}$.

d: Reference to Lang-Nishimura?

If X is smooth, projective and k-unirational, then it follows that X has a k-rational point. The Segre–Manin Theorem asserts that if a del Pezzo surface of degree at least two admits a k-rational point, then it is k-unirational (if the degree of X equals two, then the assumption is that the k-rational point is not contained in a special locus, see Theorem 8.2.1).

The strategy to prove the Segre–Manin Theorem consists in determining conditions on the action of the Galois group $\mathscr{G} := \mathrm{Gal}(\bar{k}/k)$, imposed by the

fact that $\mathscr{G}$ must permute the exceptional curves on X and preserve the intersection pairing. Note that the Galois group acts on the exceptional curves defined over $\bar{k}$; thus, whenever we talk about exceptional curves, we mean curves $E \subset \bar{X}$, isomorphic to $\mathbb{P}^1_{\bar{k}}$ such that $E^2 = -1$. Since there are only a finite number of exceptional curves on X (Proposition 7.4.14), there are only a finite number of possibilities for the action of the Galois group on the set of exceptional curves; we use this information in some cases to obtain more precise statements about the structure of X. The main ingredient is the following observation.

Lemma 8.1.2. *Let $\mathscr{C}$ be a finite set of disjoint exceptional curves on X and suppose that the action of $\mathscr{G}$ stabilizes $\mathscr{C}$. Then there is a morphism $X \to X'$ defined over k, which is an isomorphism on $X \setminus \mathscr{C}$ and which contracts each curve in $\mathscr{C}$ to a single point. The surface X' is again a del Pezzo surface.*

Proof The existence of the simultaneous contraction over the field k of all the exceptional curves in $\mathscr{C}$ is a consequence of Manin (1986, Theorem III.21.8). The fact that X' is a del Pezzo surface follows from Manin (1986, Corollary IV.24.5.2). □

Graphs of exceptional curves.

Let X be a del Pezzo surface defined over a field k. The Galois group acts in a natural way on the Picard group of $\bar{X}$ and it preserves the intersection pairing as well as the class of the canonical divisor K_X. The set $\mathscr{E}$ of divisor classes D in $\operatorname{Pic}\bar{X}$ such that $D^2 = K_X \cdot D = -1$ is therefore stable under the action of the Galois group. By Proposition 7.4.13, each element of $\mathscr{E}$ corresponds to a unique exceptional curve on $\bar{X}$; in this chapter, we frequently identify the divisor class in $\mathscr{E}$ with the corresponding exceptional curve on $\bar{X}$.

d: Refer to the appropriate chapter.

In the proof of the Segre–Manin Theorem we use an explicit analysis of the possible action of the Galois group on the set $\mathscr{E}$. To systematize the treatment, it is useful to introduce a graph encoding the exceptional curves and their intersection products.

Definition 8.1.3. The *graph of exceptional curves on X* is the (finite, loopless, undirected) graph G_X having the exceptional curves of $\bar{X}$ as vertices, and having $E_1 \cdot E_2$ edges between the vertices E_1 and E_2, where E_1 and E_2 are distinct exceptional curves.

Up to isomorphism, the graph G_X depends only on the degree of X (unless $\deg(X) = 8$). We prefer to maintain X in the notation since the action of the Galois group on G_X depends on X and the main reason for introducing G_X is

to analyze the various possibilities for this action on the exceptional curves on X.

The intersection number between exceptional curves E_1, E_2 satisfies

$$E_1 \cdot E_2 \in \{-1, 0, 1, 2, 3\},$$

the product being -1 if and only if $E_1 = E_2$. Moreover,

- if the degree of X is at least three (that is, $\bar{X}$ is not isomorphic to the blow-up of $\mathbb{P}^2$ at seven or eight points), then $E_1 \cdot E_2 \in \{-1, 0, 1\}$, and hence G_X is a graph without multiple edges;
- if the degree of X is two (that is, $\bar{X}$ is isomorphic to the blow-up of $\mathbb{P}^2$ at seven points), then $E_1 \cdot E_2 \in \{-1, 0, 1, 2\}$.

We shall mostly be interested in del Pezzo surfaces of degree at least three. Table **??** shows the graphs of the exceptional curves on $\bar{X}$, when $\bar{X}$ is isomorphic to the blow-up of $\mathbb{P}^2$ at one, two, three, four, or five points.

Exercise 8.1.4. Check that the graphs in Table **??** are correct and label the vertices by exceptional curves on $\bar{X}$ so that the number of edges between two distinct vertices equals the intersection number of the corresponding exceptional curves.

8.2 The Segre–Manin Theorem

A del Pezzo surface X defined over k need not have any k-rational point. If X is defined over a number field, then the Hasse principle (Definition 2.3.2) holds for del Pezzo surfaces of degree at least five. On the other hand, there are examples of del Pezzo surfaces of degree four, three, or two that violate the Hasse principle. Since a del Pezzo surface of degree one always has a k-rational point, the Hasse principle holds for such surfaces.

Thus it is sometimes possible to decide whether a del Pezzo surface X has or not a k-rational point checking for k_v-rational points for all valuations v (at least when k is a number field). Once we established that $X(k) \neq \emptyset$, we may be interested in understanding the structure of the set of k-rational points of X. This question is addressed by the Segre–Manin Theorem.

Theorem 8.2.1 (Segre–Manin)**.** *Let X be a del Pezzo surface of degree at least two defined over a field k and such that $X(k) \neq \emptyset$. If the degree of X is two, also assume that X contains a k-rational point not contained in four exceptional curves nor on the ramification divisor. Then X is k-unirational.*

We prove below some of the cases of the Segre–Manin Theorem; for a full proof see Manin (1986, Theorem IV.29.4), Kollár (2002, Theorem 1.1) and **?**, Corollary 18.

Sometimes the assumption $X(k) \neq \emptyset$ is automatically satisfied; this is the case if either $\bar{X} \simeq \mathrm{Bl}_p(\mathbf{P}^2_{\bar{k}})$, or $\deg X \in \{7,5,1\}$. Moreover, assuming that $X(k) \neq \emptyset$, it follows that X is k-rational if $\deg(X) \geq 5$. On the other hand, even when X is k-rational and X is a form of a blow-up of $\mathbb{P}^2_k$, it is not necessarily the case that X is the blow-up of $\mathbb{P}^2_k$ at a Galois invariant set of points.

Proof We prove the Segre–Manin Theorem one degree at a time, starting from degree nine and proceeding downwards.

Degree 9

In this case X becomes isomorphic to the projective plane after an extension of the base-field. It is possible that X has no k-rational points; if X does have k-rational points, then in fact X is k-isomorphic to $\mathbf{P}^2_k$. Here is an argument that requires the following two facts.

- If X is a form of $\mathbb{P}^2_k$, then there is a variety $X^\vee$ defined over k that is a form of $(\mathbb{P}^2_k)^\vee$, the dual projective plane of X, whose points correspond to lines in X; repeating this construction brings us back to X: $(X^\vee)^\vee$ is k-isomorphic to X.
- If X is a form of $\mathbb{P}^2_k$ having a *line* defined over k, then X is in fact isomorphic to $\mathbb{P}^2_k$ over k.

The first statement follows easily from a cohomological interpretation of forms of $\mathbb{P}^2$ over k: each form corresponds to a cohomology class, and the "dual" form corresponds to the opposite cohomology class. The second statement is a consequence of the fact that the linear system associated to a line induces a morphism to $\mathbb{P}^2_k$ and that this morphism is an isomorphism (see Example 6.1.2).

d: Add reference to appropriate lecture.

d: Reference to linear systems.

Thus we argue as follows. If X has a k-rational point p, then the set of all lines in $\bar{X}$ containing p is a subscheme of $X^\vee$ defined over k; it is clearly isomorphic to a line. Thus it follows that $X^\vee \simeq \mathbb{P}^2_k$, and in particular $X^\vee$ has a k-rational point. Applying the same reasoning to $X^\vee$ we deduce that $X \simeq (X^\vee)^\vee$ is k-isomorphic to $\mathbb{P}^2_k$.

Degree 8

There are two cases for the isomorphism class of X over the algebraic closure of k.

Case 1: $\bar{X} \simeq \mathrm{Bl}_p(\mathbb{P}^2_{\bar{k}})$.

In this case, $\bar{X}$ contains a unique exceptional curve E; the Galois group therefore fixes E and hence E is defined over k. Contracting E we obtain a form of $\mathbb{P}^2_k$ defined over k, together with a k-rational point, corresponding to the image of E. By the previous case we know that such a variety is isomorphic to $\mathbb{P}^2_k$ and therefore X is isomorphic over k to the blow-up of $\mathbb{P}^2_k$ at a k-rational point.

Case 2: $\bar{X} \simeq \mathbb{P}^1_{\bar{k}} \times \mathbb{P}^1_{\bar{k}}$.

The del Pezzo surface X need not have a k-rational point.

Exercise 8.2.2. Construct an example of a del Pezzo surface of degree eight defined over $\mathbb{Q}$, containing no rational points. (Hint: think about quadric surfaces in $\mathbb{P}^3_{\mathbb{Q}}$.)

We have $\mathrm{Pic}\,\bar{X} \simeq \mathbf{Z} \times \mathbf{Z}$ with intersection pairing defined by the standand hyperbolic lattice: if $(a,b) \in \mathbf{Z} \times \mathbf{Z}$ represents an element of $\mathrm{Pic}\,\bar{X}$, then $(a,b)^2 = 2ab$. Thus the divisor classes D such that $D^2 = 0$ are of the form $(n,0)$ or $(0,n)$, for some $n \in \mathbf{Z}$. Suppose that $X(k) \neq \emptyset$, and let p be a k-rational point; identify $p \in X$ with $(p_1,p_2) \in \mathbf{P}^1_k \times \mathbf{P}^1_k$ under an isomorphism $\bar{X} \simeq \mathbf{P}^1_{\bar{k}} \times \mathbf{P}^1_{\bar{k}}$ and note that although p is defined over k, the points $p_1, p_2 \in \mathbf{P}^1_{\bar{k}}$ need not be. The divisors on $\bar{X}$ corresponding to $L_1 := \{p_1\} \times \mathbb{P}^1_{\bar{k}}$ and $L_2 := \mathbb{P}^1_{\bar{k}} \times \{p_2\}$ satisfy $L_1^2 = L_2^2 = 0$ and $L_1 \cdot L_2 = 1$. We deduce that their classes form a basis for $\mathrm{Pic}\,\bar{X}$ and, since L_1 and L_2 are the unique divisors in their equivalence class containing p, it follows that the Galois group $\mathscr{G}$ stabilizes the set $\{L_1, L_2\}$. Thus the sum $L_1 + L_2$ is certainly invariant under $\mathscr{G}$. The morphism associated to the divisor $L_1 + L_2$ induces an isomorphism of X with a quadric surface Q in $\mathbb{P}^3_k$, containing the image of p as a k-rational point. Projecting Q away from p induces a birational map $X \simeq Q \dashrightarrow \mathbb{P}^2_k$ proving that X is k-rational and hence, in particular, k-unirational. Note that the splitting of X as a product of two product of $\mathbb{P}^1_k$ need not be defined over k. Whether the splitting occurs or not over k is equivalent to whether the divisors L_1 and L_2 are defined over the base field. Geometrically, the intersection of Q with the tangent plane to Q at p is the union of L_1 and L_2 and a degree two base extension of k may be required to make sure that L_1 and L_2 are defined.

Exercise 8.2.3. Let $X \subset \mathbf{P}^3_{\mathbf{Q}}$ be the quadric defined by

$$a_0X_0^2 + a_1X_1^2 + a_2X_2^2 + a_3X_3^2 = 0$$

where $a_0, a_1, a_2, a_3 \in \mathbf{Q}^*$. Suppose that $X(\mathbf{Q}) \neq \emptyset$. Show that there is an isomorphism $X \simeq \mathbf{P}^1_{\mathbf{Q}} \times \mathbf{P}^1_{\mathbf{Q}}$ defined over $\mathbf{Q}$ if and only if $a_0a_1a_2a_3$ is a square.

Find a form P of $\mathbf{P}^1_{\mathbf{Q}} \times \mathbf{P}^1_{\mathbf{Q}}$ with a rational point, such that P is not isomorphic to $\mathbf{P}^1_{\mathbf{Q}} \times \mathbf{P}^1_{\mathbf{Q}}$ over $\mathbf{Q}$. Determine a birational map of P to $\mathbf{P}^2_{\mathbf{Q}}$ defined over $\mathbf{Q}$.

Degree 7

In this case $\bar{X}$ is isomorphic to $\mathrm{Bl}_{p,q}(\mathbb{P}^2_{\bar{k}})$. Looking at the graph of exceptional curves on X, we immediately find that the Galois group stabilizes the "middle" vertex as well as the set containing the two "external" vertices (see Table **??**). We deduce that these two sets are defined over the base field and each consists of disjoint exceptional curves (one of the two trivially, since it contains a unique exceptional curve). Apply Lemma 8.1.2 to obtain a morphism $\pi\colon X \to X'$ contracting the pair of "external" curves whose image X' is a form of $\mathbb{P}^2$. The "middle" exceptional curve is also defined over k and its image under π in X' is a line, defined over k. This implies that X' is k-isomorphic to $\mathbf{P}^2_k$ being a form of $\mathbf{P}^2_k$ with a k-rational point. Therefore X is the blow-up of $\mathbf{P}^2_k$ at a pair of (possibly conjugate) points.

Exercise 8.2.4. Obtain the same result, considering the contraction of the "middle" exceptional curve. (Hint: the surface obtained by the contraction is a del Pezzo surface; what is its degree?)

Degree 6

In this case $\bar{X}$ is isomorphic to $\mathrm{Bl}_{p,q,r}(\mathbf{P}^2_{\bar{k}})$, with p, q, r not collinear. The automorphism group of the graph G_X acts transitively on the vertices (and on the edges): we should not expect to obtain many results without further assumptions. Indeed there are forms of $\mathrm{Bl}_{p,q,r}(\mathbf{P}^2_{\bar{k}})$ without k-rational points.

Suppose that X has a k-rational point p not contained in any exceptional curve. Blowing up p we obtain a del Pezzo surface of degree five, whose graph is the Petersen graph (Table **??**). The set $\mathscr{C}$ consisting of the three exceptional curves adjacent to the exceptional curve obtained by blowing up p is stable under the Galois group, and these three curves are disjoint (see Table **??**). Therefore contracting $\mathscr{C}$ we obtain a del Pezzo surface of degree eight, together with a rational point, and we conclude as above.

Exercise 8.2.5. Analyze the cases in which the k-rational point p lies on some exceptional curve.

All del Pezzo surfaces of degree at least six over an algebraically closed field are in fact also toric surfaces. It follows that for such surfaces the Hasse principle holds.

d: Reference? Also should we mention that they are defined over a number field in order for them to satisfy the Hasse principle?

Degree 5

In this case $\bar{X}$ is isomorphic to $\mathrm{Bl}_{p,q,r,s}(\mathbb{P}^2_{\bar{k}})$, with p,q,r,s not collinear in triples.

Exercise 8.2.6. Assume that $X(k) \neq \emptyset$. Show that X is birational to $\mathbb{P}^2_k$ over k.

It is a non-trivial result, stated by Enriques and proved by Swinnerton-Dyer, that del Pezzo surfaces of degree five always have a k-rational point (Enriques, 1897; Swinnerton-Dyer, 1972). It follows that del Pezzo surfaces of degree five are always k-rational and satisfy the Hasse principle.

All del Pezzo surfaces of degree at least five satisfy the Hasse principle (and in some cases always have a rational point); moreover, if they have a rational point, then they are automatically k-rational, not just k-unirational. Both properties fail for del Pezzo surfaces of degree four.

Degree 4

In this case $\bar{X}$ is isomorphic to $\mathrm{Bl}_{p,q,r,s,t}(\mathbb{P}^2_{\bar{k}})$, p,q,r,s,t not collinear in triples. All del Pezzo surfaces of degree four are isomorphic to complete intersection of two quadrics in $\mathbb{P}^4_k$. In Chapter 2 we saw an example of a del Pezzo surface S of degree four defined over $\mathbf{Q}$ that is a counter-example to the Hasse principle: the surface S has $\mathbf{Q}_v$-rational points for all valuations v of $\mathbf{Q}$, but it has no rational point.

d: Correct reference with same symbol.

Exercise 8.2.7. Show that the del Pezzo surface of degree four defined by

$$\begin{cases} 2x^2+y^2 = 2w^2+t^2 \\ 3x^2+2y^2 = w^2-z^2 \end{cases}$$

over $\mathbf{Q}$ contains no rational points.

The argument we use to prove the Segre–Manin Theorem in this case involves a bit more of geometric reasoning than the previous ones: here is a sketch. To simplify the proof we suppose that there is a point $p \in X(k)$ not lying on any exceptional curve. First recall that X is an intersection of two quadrics in $\mathbb{P}^4$ and that under this embedding in projective space, the exceptional curves are lines (Remark 7.4.10). Since the equations defining X have degree two, it follows that if a line ℓ in $\mathbf{P}^4$ intersects X in at least three distinct points, then it is in fact contained in X: all quadrics defining X vanish at all points of the line ℓ, since they vanish at three points on it. We deduce that every line in $\mathbf{P}^4$ through p intersects X in at most one more point, since by assumption p is not contained in any exceptional curve on X and hence no line through p is entirely contained in X. Thus projecting away from p determines an injective morphism $\pi\colon X \smallsetminus \{p\} \to \mathbf{P}^3_k$. We think of the projection π

as defined by choosing a hyperplane $\mathbf{P}^3_k \subset \mathbf{P}^4_k$ not containing the point p and associating to each point $q \in X \setminus \{p\}$ the intersection point of the line through p and q with the hyperplane $\mathbf{P}^3$. The closure of the image of π is a (smooth) surface X' in $\mathbf{P}^3_k$, defined over k since X and π are. To compute the degree of X', we choose a general line $L \subset \mathbf{P}^3$ and compute the number of intersection points of L with X' (Example 4.3.8). The inverse image under π of the line L is the intersection of $X \setminus \{p\}$ with the plane α_L containing L and p. Since the degree of X is four and L is general, we deduce that $\alpha_L \cap X$ contains four points, one of which if p. We conclude that $L \cap X'$ consists of three points and thus X' has degree three.

A more detailed analysis of the graph of the morphism π shows that it is an isomorphism of $X \setminus \{p\}$ with its image in X'. On the other hand, the complement of $\pi(X \setminus \{p\})$ is X' is a line $\ell \subset X'$: it follows that π is in fact the inverse of the blow-up of X at p and the line ℓ is the exceptional divisor of the blow up. Since p is defined over k, the line ℓ is defined over k and it is therefore k-isomorphic to $\mathbf{P}^1_k$.

Given any plane in $\mathbf{P}^3$ the intersection of the cubic surface X' with that plane is defined by an equation of degree three. If that plane passes through the line ℓ, then the line is certainly part of the intersection and so the residual intersection is defined by an equation of degree two. Generically this is a smooth conic though at five planes in the pencil it degenerates into a union of two lines. Moreover such a plane is tangent to the cubic surface X' at the intersection points of the conic and the line ℓ. Thus most points of ℓ determine a plane conic with a k-rational point, which is therefore k-isomorphic to $\mathbf{P}^1_k$; most conics appear twice in this family, once for each choice of point in the intersection of the conic with ℓ. It is now easy to prove that (most of) the isomorphisms between the conics residual to ℓ and $\mathbf{P}^1_k$ can in fact be chosen consistently to define a rational map $r\colon \ell \times \mathbf{P}^1_k \dashrightarrow X'$. The rational map r has degree two, since most conics are "accounted for" twice in the above argument. Thus X' is k-unirational, and hence X is also k-unirational. This concludes the proof of the Segre–Manin Theorem in this case.

For the remaining cases of del Pezzo surfaces of degree three and two we refer to Manin (1986, Theorem IV.29.4) and Kollár (2002, Theorem 1.1). □

9

Classification of surfaces

This chapter contains a brief introduction to the classification of curves and surfaces. We do not focus on the technical details, but only on the general features of the classification. The discussion is inspired by the Minimal Model Program, rather than the more classical notion of Kodaira dimension. While these two points of view agree very closely for curves, they differ on higher dimensional varieties. The content of this chapter is not needed in the rest of the book.

Let k be a field and let X be a smooth projective variety defined over k. The aim of the Minimal Model Program is to find a variety X_0, which reflects as much as possible the properties of the variety X, and which is as simple as possible. The variety X_0 is then called a *minimal model of* X. The criterion to decide whether a variety is simple enough to be called a minimal model is based on intersection properties of the canonical divisor with curves on X. In order to simplify the statements, we shall assume for this talk that the base field k is algebraically closed and that $\mathrm{char}(k) = 0$.

9.1 Minimal models of surfaces

We begin this section by outlining the general structure of the Minimal Model Program and then specialize to the case of surfaces. We start with a definition that is central to the discussion.

Definition 9.1.1. Let X be a smooth projective variety defined over an algebraically closed field k and let K_X be an anticanonical divisor on X. A *K-negative curve* is a curve $C \subset X$ such that $K_X \cdot C < 0$.

There are three main examples to keep in mind of K-negative curves that are relevant for the discussion below. First, let $\overline{X}$ be any smooth projective surface,

let $p \in \overline{X}$ be a point, and let $\pi\colon X \to \overline{X}$ be the blow-up of p. The exceptional divisor E of π satisfies $K_X \cdot E = -1$ (Proposition 7.3.4) and therefore E is a K-negative curve on X. Second, let B be a smooth projective curve, let $p \in B$ be a point, and let $X = B \times \mathbf{P}^1$. The divisor $C = \{p\} \times \mathbf{P}^1$ on X satisfies $C^2 = 0$ and hence by the adjunction formula (Theorem 6.4.3) we have $K_X \cdot C = -2$; we conclude that C is a K-negative curve. Third, a line in $\mathbf{P}^2$ is a K-negative curve.

d: We might include this as an excercise in the section on intersection numbers.

The guiding principle of the Minimal Model Program is that if a variety X contains K-negative curves, then it also contains certain special K-negative curves R called *extremal rays*. The three examples above are in fact examples of extremal rays. Associated to each extremal ray R there is a *contraction morphism* $c_R\colon X \to X'$ with the property that a curve C is contained in a fiber of c_R if and only if C is linearly equivalent to a multiple of R. Thus the variety X' contains "fewer" K-negative curves than X does. An important observation is that we do not (and cannot, in general) require X' to have the same dimension as X. Ideally, we can repeat this process starting from X': iterating this procedure, we obtain a sequence of contraction morphisms and varieties with fewer and fewer K-negative curves. The output of this construction should be a variety X_0 containing no K-negative curves at all, together with a sequence of contraction morphisms beginning with X and ending with X_0. On the variety X_0, the canonical divisor has the property that it intersects every curve on X_0 non-negatively.

The previous discussion leads us to the definition of a minimal model.

Definition 9.1.2. A smooth projective variety X is a minimal model if it contains no K-negative curve. Equivalently, if a canonical divisor K_X intersects every curve on X non-negatively.

There are several substantial technical difficulties when trying to implement the Minimal Model Program, mainly arising from the fact that the image of a contraction morphism need not be a *smooth* variety. It is possible to work around this issue in certain cases, but we shall not go into this.

d: Find a reference.

In the case in which X is itself a curve, then X contains (or rather *is*) a K-negative curve if and only if X is isomorphic to $\mathbf{P}^1$ (this follows at once from the fact that the degree of a canonical divisor on a smooth curve of genus g is $2g-2$ and a curve of genus zero is isomorphic to $\mathbf{P}^1$).

d: Add more details?

We now focus on the case of surfaces. There are three possibilities for the contraction of an extremal ray on a surface X:

(i) a blow-down of an exceptional curve;

(ii) a fibration $b\colon X \to B$, where B is a smooth projective curve and all the fibers of c are isomorphic to $\mathbf{P}^1$; and

(iii) the constant morphism of $\mathbf{P}^2$ to a point.

A surface not containing any exceptional curve is classically called *minimal*. A surface admitting a fibration as in (ii) is called a *ruled surface*. Note that with our definitions every surface that is a minimal model is also a minimal surface, but the converse does not hold. Indeed, $\mathbf{P}^2$ is a minimal surface, but not a minimal model; also a ruled surface is not a minimal model, but it is either minimal or isomorphic to $\mathrm{Bl}_p(\mathbf{P}^2)$. We summarize this discussion in the following theorem.

Theorem 9.1.3. *Suppose that X is a minimal surface that is not a minimal model; then either X is isomorphic to $\mathbf{P}^2$, or X is ruled.*

From the above results we conclude that if X is a smooth projective surface and there are K-negative curves on X, then there are also rational curves on X. Indeed, one of the starting points of the Minimal Model Program was the following remarkable implication: if the canonical divisor of X has negative intersection number with a curve $C \subset X$, then each point of C is contained in a rational curve. Varieties containing many rational curves have special properties; such varieties are not going to be minimal models.

In view of Theorem 9.1.3, we only have to classify the surfaces X that are minimal models. The next theorem lists all the minimal models of surfaces in increasing order of complexity, mentioning for each type the classical name of the corresponding surface. We note that if X is a surface that is a minimal model, then $(K_X)^2 \geq 0$. We give some further properties and some examples after the statement.

Theorem 9.1.4. *Let X be a smooth projective surface that is a minimal model.*

(i) *Suppose that $(K_X)^2 = 0$.*

- *If K_X is linearly equivalent to zero, then X is either an Abelian surface or a K3 surface.*
- *If K_X is numerically equivalent to zero, but not linearly equivalent to zero, then either X is an Enriques surface or X is a bielliptic surface.*
- *If K_X is not numerically equivalent to zero, then X is an elliptic surface.*

(ii) *Suppose that $(K_X)^2 > 0$. Then X is a surface of general type.*

An Abelian surface is a smooth projective variety together with the structure of an algebraic group. The group structure is commutative as a consequence of

the assumption that the variety is projective. Examples of Abelian surfaces include the Jacobians of genus two curves, as well as products of elliptic curves.

A K3 surface is a simply-connected surface with trivial canonical divisor. Examples of K3 surfaces include smooth quartic surfaces in $\mathbf{P}^3$, double covers of $\mathbf{P}^2$ branched above smooth plane sextics, (minimal resolutions of) quotients of Abelian surfaces by the inverse in the group law (in characteristic different from two).

d: Remember to mention that numerical equivalence classes coincide with all the remaining ones.

An Enriques surface is a quotient of a K3 surface by a fixed-point free involution. Examples of Enriques surfaces can be constructed as follows: let $\pi_1,\ldots,\pi_4$ be four planes in $\mathbf{P}^3$ with empty intersection and let S be a general sextic having the six lines contained in the pairwise intersections of the four planes $\pi_1,\ldots,\pi_4$ as double lines; the minimal resolution of the surface S is an Enriques surface.

A bielliptic surface is the quotient of a product $E\times F$ of two elliptic curves E and F by a finite group G of translations of E acting on F so that $F/G\simeq\mathbf{P}^1$. There are seven possibilities for the group G.

d: Elliptic surfaces?

An elliptic surface is a surface admitting a morphism to a curve, with genus one curves as general fibres. Not all such surfaces are elliptic surfaces: the only

d: Surfaces of general type?

9.2 The Hodge diamond

Let X be a smooth projective variety. For all integers $p,q\geq 0$, let $\Omega_X^p:=\bigwedge^p\Omega_X$ be the p-th exterior power of the sheaf of differential one-forms and let $h^{p,q}:=\dim \mathrm{H}^q\left(X,\Omega_X^p\right)$; the integers $h^{p,q}$ are called the *Hodge numbers*.

If X is defined over the complex numbers, then, for every integer k, the singular cohomology $\mathbb{C}$-vector spaces $\mathrm{H}^k\left(X,\mathbb{C}\right)$ admit a direct sum decomposition

$$\mathrm{H}^k\left(X,\mathbb{C}\right)=\bigoplus_{p+q=k}\mathrm{H}^q\left(X,\Omega_X^p\right)$$

called the *Hodge decomposition*. The Hodge numbers satisfy the identities

$$\begin{aligned} h^{p,q} &= h^{q,p},\\ h^{n-p,n-q} &= h^{p,q}, \end{aligned}$$

coming from the fact that $\mathrm{H}^q\left(X,\Omega_X^p\right)=\overline{\mathrm{H}^p\left(X,\Omega_X^q\right)}$ and from Poincaré duality, respectively. Moreover we also have the identity

$$e_{top}(X)=\sum_{p,q}(-1)^{p+q}h^{p,q}$$

where e_{top} is the topological Euler characteristic of the topological space associated to X, with the induced Euclidean topology.

Typically, the Hodge numbers are written in the following way:

$$\begin{array}{ccccccc} & & & h^{n,n} & & & \\ & & h^{n,n-1} & & h^{n-1,n} & & \\ & h^{n,n-2} & & h^{n-1,n-1} & & h^{n-2,n} & \\ & & \cdots & \cdots & \cdots & & \\ & & h^{1,0} & & h^{0,1} & & \\ & & & h^{0,0} & & & \end{array}$$

which takes the name *Hodge diamond*, for obvious reasons! We have $h^{0,0} = h^{n,n} = 1$. For a surface the Hodge diamond is

$$\begin{array}{ccccc} & & h^{2,2} & & \\ & h^{2,1} & & h^{1,2} & \\ h^{2,0} & & h^{1,1} & & h^{0,2} \\ & h^{1,0} & & h^{0,1} & \\ & & h^{0,0} & & \end{array}$$

where $\chi\big(X,\mathscr{O}_X\big) = h^{0,0} - h^{0,1} + h^{0,2} = 1 - h^{0,1} + h^{0,2}$ is the Euler characteristic of the structure sheaf, $p_a := h^{0,2} - h^{0,1}$ is the arithmetic genus, and $p_g := h^{2,0}$ is the geometric genus.

Smooth surfaces in $\mathbb{P}^3$

Let $X \subset \mathbb{P}^3$ be a smooth surface of degree d; we wish to determine the Hodge numbers of X. First, by an exercise of one of the previous lectures we know that $h^{1,0} = 0$ and hence $h^{0,1} = h^{2,1} = h^{1,2} = 0$; thus we have

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ h^{2,0} & & h^{1,1} & & h^{0,2} \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

To compute the remaining two Hodge numbers we are going to compute $\chi\big(X,\mathscr{O}_X\big)$ and $e_{top}(X)$.

The Euler characteristic $\chi\big(X,\mathscr{O}_X\big)$ is the evaluation at $n = 0$ of the Hilbert polynomial $\chi\big(X,\mathscr{O}_X(n)\big)$, which, for n large enough, coincides with the dimension of the degree n part of the graded ring $k[X_0,X_1,X_2,X_3]/(F)$, where

X_0, X_1, X_2, X_3 are homogeneous coordinates on $\mathbb{P}^3$ and F is a non-zero homogeneous polynomial of degree d, vanishing along X. The space of homogeneous polynomials of degree n in $\mathbb{P}^3$ has dimension $\binom{n+3}{3}$. The dimension of the space of polynomials of degree n vanishing along X has dimension $\binom{n+3-d}{3}$, since such polynomials are exactly the multiples of F. Thus the homogeneous part of degree n of $k[X_0, X_1, X_2, X_3]/(F)$ has dimension

$$\binom{n+3}{3} - \binom{n+3-d}{3} = \frac{1}{2}dn^2 + \frac{1}{2}(4d - d^2)n + \frac{1}{6}(d^3 - 6d^2 + 11d)$$

for $n \geq d$. Since the expression on the right of the last equation is a polynomial in n, it is the Hilbert polynomial of $X \subset \mathbb{P}^3$; evaluating at $n = 0$ and subtracting one we find $h^{0,2} = \binom{d-1}{3}$.

To compute the topological Euler characteristic of X, we shall follow two strategies: the first uses an identity called Noether's formula; the second uses Chern classes.

Noether's formula is the following identity:

$$\chi(X, \mathscr{O}_X) = \frac{1}{12}(K_X^2 + e_{top}(X)).$$

In our case K_X is linearly equivalent to $(d-4)H_X$, where H_X is the restriction of a plane to X. Since $H_X^2 = d$, we find $e_{top}(X) = 12\chi(X, \mathscr{O}_X) - d(d-4)^2$. This allows us to conclude that $h^{1,1} = \frac{d(2d^2-6d+7)}{3}$.

d: Use of adjunction formula.

d: Symbol H_X^2 and $d = d[point]$.

Alternatively, we use the sequences

$$0 \to \Omega_{\mathbb{P}^3} \to \mathscr{O}_{\mathbb{P}^3}(-1)^4 \to \mathscr{O}_{\mathbb{P}^3} \to 0,$$
$$0 \to \mathscr{O}_X(-d) \to \Omega_{\mathbb{P}^3}|_X \to \Omega_X \to 0,$$

the first one on $\mathbb{P}^3$, the second one on X. Both sequences were introduced in the previous lecture. The first is the Euler sequence. The second comes from the fact that any cotangent vector to $\mathbb{P}^3$ induces a cotangent vector to X; the kernel of this morphism is generated by the differential of the equation of X. Denote by H the hyperplane class in $\mathbb{P}^3$ and by H_X its restriction to X; taking total Chern classes, we find that

$$1 + c_1(\mathbb{P}^3) + c_2(\mathbb{P}^3) + c_3(\mathbb{P}^3) = (1-H)^4 = 1 - 4H + 6H^2 - 4H^3$$
$$1 + c_1(X) + c_2(X) = \frac{(1+c_1(\mathbb{P}^3)+c_2(\mathbb{P}^3)+c_3(\mathbb{P}^3))|_X}{(1-dH_X)} = (1 - 4H_X + 6H_X^2)(1 + dH_X + d^2H_X^2).$$

We have $c_2(X) = e_{top}(X)$, and, since X has degree d, also $H_X^2 = d[point]$; combining everything we conclude that

$$e_{top}(X) = d^3 - 4d^2 + 6d$$

and finally the Hodge diamond of X is

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ \binom{d-1}{3} & & \frac{d(2d^2-6d+7)}{3} & & \binom{d-1}{3} \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

Exercise 9.2.1. Compute the Hodge numbers of $\mathbb{P}^2$.

Exercise 9.2.2. Compute the Hodge numbers of smooth curves of degree d in $\mathbb{P}^2$.

Exercise 9.2.3. Compute the Hodge numbers of $C_1 \times C_2$, where C_1 and C_2 are smooth curves of genus g_1 and g_2 respectively.

Exercise 9.2.4 ($\star$)**.** Compute the Hodge numbers of smooth surfaces in $\mathbb{P}^4$ that are intersections of two hypersurfaces of degree d and e.

10

The Brauer group of a field

In this chapter we introduce the Brauer group of a field, defined to be the group of equivalence classes of central simple algebras over the field.

There are several clear and thorough references on Brauer groups: among them are Gille and Szamuely (2006); Bourbaki (2012); and Chapter IV of Milne (2008).

10.1 Hilbert symbols

Before defining the Brauer group of a general field, we introduce the Hilbert symbol. The Hilbert symbol is closely related to the Legendre symbol for quadratic residues, and it allows us to reformulate the counterexamples to the Hasse principle seen in Chapter 2 in a more uniform way. As we shall see later, this can be viewed as an explicit way of performing computations with quaternion algebras over number fields. Serre (1973, Chapter III) is an excellent reference when the field is the rational numbers, and everything can be made very explicit; see Milne (2008, Section III.4) for a thorough treatment of the general case.

Definition 10.1.1. Let k be a number field, let v be a place of k, and let a and b be two elements of $k_v^\times$. We define the *Hilbert symbol* $(a,b)_v$ of a and b at v to be

$$(a,b)_v = \begin{cases} 1 & \text{if the conic } ax^2+by^2=z^2 \text{ has a } k_v\text{-rational point;} \\ -1 & \text{otherwise.} \end{cases}$$

While this definition might appear rather *ad hoc*, the following results show that Hilbert symbols have many pleasant algebraic properties.

Proposition 10.1.2. *Let k be a number field and let v be a place of k. The Hilbert symbol has the following properties.*

(i) *Symmetry: for all $a,b \in k_v^\times$, $(a,b)_v = (b,a)_v$.*
(ii) *If either a or b is a square in k_v, then $(a,b)_v$ equals* 1.
(iii) *For all $a,b,c \in k_v^\times$, we have $(a,b)_v = (ac^2,b)_v$. That is, $(a,b)_v$ only depends on the class of a in $k_v^\times/(k_v^\times)^2$.*
(iv) *For all $a \in k_v^\times$, $(a,-a)_v = 1$.*
(v) *If $a \neq 0,1$, then $(a,1-a)_v = 1$.*

Proof These are all immediate from the definition of the Hilbert symbol. □

Proposition 10.1.3. *Let k be a number field, let v be a place of k and let $a,b \in k_v^\times$. The equality $(a,b)_v = 1$ holds if and only if a is a norm from $k_v(\sqrt{b})$.*

Remark 10.1.4. In some ways it would be more natural to use the algebra $k_v[t]/(t^2-b)$ instead of $k_v(\sqrt{b}$, whether or not b is a square. The distinction doesn't matter, though, since an element $a \in k_v$ is a norm from $k_v(\sqrt{b})$ if and only if it is a norm from $k_v[t]/(t^2-b)$. The only case where this needs to be checked is when b is a square, in which case both norm maps are easily seen to be surjective.

Proof of Proposition 10.1.3 In view of the above remark, we must prove: $(a,b)_v = 1$ is and only if a is a norm from $k_v[t]/(t^2-b)$. Suppose first that a is the norm of $\alpha+\beta t \in k_v[t]/(t^2-b)$. Then we have $a = \alpha^2 - b\beta^2$, and so $(x,y,z) = (1,\beta,\alpha)$ is a solution to $ax^2+by^2 = z^2$, showing that $(a,b)_v$ is 1.

Conversely, suppose that $x,y,z \in k_v$ satisfy $ax^2+by^2 = z^2$, with x,y,z not all zero. If x is non-zero, then we have $a = (z/x)^2 - b(y/x)^2$ and so a is the norm of $(z/x)+(y/x)t$. If x is zero, then y is non-zero and $b = (z/y)^2$ is a square, in which case the norm map $k_v[t]/(t^2-b) \to k_v$ is surjective. □

As a corollary, we can prove the easy part of the bilinearity of $(a,b)_v$.

Corollary 10.1.5. *Suppose that $a,b \in k_v^\times$ satisfy $(a,b)_v = 1$. Then, for all $c \in k_v^\times$, we have $(c,b)_v = (ac,b)_v$.*

Proof If a is a norm from $k_v(\sqrt{b})$, then c is a norm if and only if ac is a norm. □

There are simple explicit formulae to evaluate the Hilbert symbol for any completion of $\mathbf{Q}$.

Proposition 10.1.6. (i) *Let $a,b \in \mathbf{R}^\times$. Then*

$$(a,b)_\infty = \begin{cases} 1 & \text{if } a>0 \text{ or } b>0; \\ -1 & \text{if } a<0 \text{ and } b<0. \end{cases}$$

(ii) *Let p be an odd prime; let $a,b \in \mathbf{Q}_p^\times$, and write $a = p^\alpha u$ and $b = p^\beta v$ with $u,v \in \mathbf{Z}_p^\times$. Write $\varepsilon(p) = (p-1)/2$. Then*

$$(a,b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

In particular, $(u,v)_p = 1$ if $u,v \in \mathbf{Z}_p^\times$.

(iii) *Let $a,b \in \mathbf{Q}_2^\times$ and write $a = 2^\alpha u$ and $b = 2^\beta v$ with $u,v \in \mathbf{Z}_2^\times$. For $x \in \mathbf{Z}_2^\times$, write $\varepsilon(x) = (x-1)/2 \pmod 2$ and $\omega(x) = (x^2-1)/8 \pmod 2$. Then*

$$(a,b)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}.$$

Proof See Serre (1973, Chapter III, Theorem 1). □

We now describe some deeper properties of Hilbert symbols.

Proposition 10.1.7. *Let k be a number field.*

(i) *For each place v of k, the Hilbert symbol defines a non-degenerate symmetric bilinear form on the $\mathbf{F}_2$-vector space $k_v^\times/(k_v^\times)^2$.*

(ii) *For $a,b \in k^\times$, we have the* product formula

$$\prod_v (a,b)_v = 1$$

where the product is taken over all places of k.

Proof For direct proofs of these statements in the case $k = \mathbf{Q}$, using the description of Proposition 10.1.6, see Serre (1973, Chapter III, Theorems 2 and 3). In the general case, we outline how to deduce the statements from class field theory.

Statement (i), while it looks simple, rests on two highly non-trivial results of local class field theory for quadratic extensions. Given Corollary 10.1.5, to prove bilinearity of the Hilbert symbol it is enough to show $(ac,b) = 1$ whenever we have $(a,b) = -1$ and $(c,b) = -1$. By Proposition 10.1.3 it suffices to show that, whenever $b \in k_v^\times$ is non-square, the product of two non-norms from $k_v(\sqrt{b})$ is a norm. This follows from the existence of the local reciprocity map (Milne, 2008, Theorem I.1.1), which gives an isomorphism $k_v^\times/\mathrm{N}_{k_v(\sqrt{b})/k_v}(k_v(\sqrt{b})^\times) \to \mathrm{Gal}(k_v(\sqrt{b})/k_v)$.

To prove that the bilinear form defined by the Hilbert symbol is non-degenerate we must show that, if an element $a \in k_v^\times$ is not a square, then there exists $b \in k_v^\times$ satisfying $(a,b)_v = -1$. This follows from the Existence Theorem in local class field theory (Milne, 2008, Theorem I.1.4). Suppose that a is a non-square in $k_v^\times$. Let U be a complement in the $\mathbf{F}_2$-vector space $k_v^\times/(k_v^\times)^2$ to the subspace $\{1,a\}$ and let $\tilde{U}$ be the inverse image of U in $k^\times$. Then $\tilde{U} \subset k_v^\times$ is a subgroup

of index 2 in $k_v^\times$ not containing a. By the Existence Theorem, there exists a quadratic extension ℓ/k_v satisfying $\tilde{U} = \mathrm{N}_{\ell/k_v}(\ell^\times)$, and so a is not a norm from ℓ. We have $\ell = k_v(\sqrt{b})$ for some non-square $b \in k_v^\times$, and by Proposition 10.1.3 it follows that $(a,b)_v$ is -1.

Statement (ii), the product formula for the Hilbert symbol, is a consequence of the global reciprocity law of class field theory (Milne, 2008, Theorem V.5.3). Let a and b be elements of $k^\times$. If b is a square, then the formula is trivial; so assume that b is non-square. Let ℓ be the field $k(\sqrt{b})$. For each place v of k, the local symbol $(a,b)_v$ is identified (in the obvious way) with the image of a under the local reciprocity map $\theta_v \colon k_v^\times / \mathrm{N}_{\ell_w/k_v}(\ell_w^\times) \to \mathrm{Gal}(\ell_w/k_v)$, where w is a place of ℓ lying over v. Let $\mathbf{I}_k$ denote the group of idèles of k. The global reciprocity map $\theta \colon \mathbf{I}_k/\mathrm{N}_{\ell/k}\mathbf{I}_\ell \to \mathrm{Gal}(\ell/k)$ is the product of the local reciprocity maps and is trivial on $k^\times \subset \mathbf{I}_k$, giving $\prod_v (a,b)_v = 1$. □

The following long exercise shows how to formulate Example 2.3.5 in terms of norms and Hilbert symbols.

Exercise 10.1.8. Let X be a smooth, projective, geometrically irreducible variety over $\mathbf{Q}$. Let $f \in \kappa(X)^\times$ be a rational function on X, and suppose that there exists a quadratic extension $k = \mathbf{Q}(\sqrt{d})$ of $\mathbf{Q}$ such that the divisor (f) is a norm from k – that is, there is some divisor $D \in \mathrm{Div}\, X_k$ satisfying $(f) = \mathrm{N}_{k/\mathbf{Q}} D = D + \sigma(D)$, where σ is the generator of $\mathrm{Gal}(k/\mathbf{Q})$.

Let K be a field containing $\mathbf{Q}$; we aim to construct a function

$$\phi_K \colon X(K) \to K^\times / \mathrm{N}_{K(\sqrt{d})/K}(K(\sqrt{d})^\times)$$

associated to f.

Because X is geometrically irreducible, the base field k is algebraically closed in the function field $\kappa(X)$ **??**, and so the extension $\kappa(X_k)/\kappa(X)$ is a quadratic extension generated by a square root of d. To save on notation, we will write $\mathrm{N}_{k/\mathbf{Q}}$ not only for the norm map from k to $\mathbf{Q}$, but also for the norm map from $\kappa(X_k)$ to $\kappa(X)$.

(i) On the subset of $X(K)$ consisting of points at which f is regular and non-zero, define a function $\phi_{K,f}$ by setting $\phi_{K,f}(x)$ to be the class of $f(x)$ in $K^\times / \mathrm{N}_{K(\sqrt{d})/K}(K(\sqrt{d})^\times)$. Show that multiplying f by a norm does not affect the function $\phi_{K,f}$. In other words, if $g \in \kappa(X_k)^\times$ is a rational function on X_k, and f' is defined to be $\mathrm{N}_{k/\mathbf{Q}}(g) f$, show that the functions $\phi_{K,f}$ and $\phi_{K,f'}$ agree at the points where they are both defined.

(ii) Let P be a point in $X(K)$. Show that there exists a function $g \in \kappa(X_k)^\times$ such that $f' = \mathrm{N}_{k/\mathbf{Q}}(g) f$ has neither a zero nor a pole at P. Deduce that

various functions $\phi_{K,f'}$ patch together to produce a well-defined function ϕ_K as desired.

(iii) Taking $K = \mathbf{Q}_v$, we get a map which we can equally well write using the Hilbert symbol:

$$X(\mathbf{Q}_v) \to \{\pm 1\}, \qquad x \mapsto (d, \phi_{\mathbf{Q}_v}(x))_v.$$

Multiplying these maps, we get a map from the product of all the $X(\mathbf{Q}_v)$ to $\{\pm 1\}$ as follows:

$$\prod_v X(\mathbf{Q}_v) \to \{\pm 1\}, \qquad (x_v) \mapsto \prod_v (d, \phi_{\mathbf{Q}_v}(x_v))_v.$$

Show that the diagonal image of $X(\mathbf{Q})$ in $\prod_v X(\mathbf{Q}_v)$ must lie in the kernel of this map (i.e. the inverse image of 1).

(iv) Consider the surface described by Birch and Swinnerton-Dyer given in Example 2.3.5. Show the the divisor of the function $f = u/(u+v)$ is a norm from $\mathbf{Q}(\sqrt{5})$.

(v) Calculate the maps of (iii), and deduce that $X(\mathbf{Q})$ is empty.

10.2 Central simple algebras

d: Think about whether we want to add Severi-Brauer varieties.

The Brauer group of a field is an invariant that plays an important rôle in class field theory. It is also essential for defining the Brauer–Manin obstruction. The Brauer group consists of equivalence classes of central simple algebras, and we begin by studying these algebras.

An *algebra* over a field k is a vector space A over k endowed with a k-bilinear multiplication $A \times A \to A$ making A into a ring with identity 1_A. If A is non-zero, then the map $k \to A$ sending x to $x.1_A$ is an injective ring homomorphism with image contained in the centre of A. Note that we require the multiplication on A to be associative, but not necessarily commutative. If $\{a_\alpha\}_{\alpha \in I}$ is a basis of A, then to define the multiplication on A it is sufficient to define multiplication on the a_α, by specifying the *structure constants* $\{c_{\alpha\beta}^\gamma\}_{\alpha,\beta,\gamma \in I}$ satisfying $a_\alpha a_\beta = \sum_\gamma c_{\alpha\beta}^\gamma a_\gamma$. An algebra is a *division algebra* if every non-zero element has a multiplicative inverse.

143: Think about notation

Definition 10.2.1. Let k be a field and A an algebra over k. The algebra A is *central* if the centre of A is k. The algebra A is *simple* if it has exactly two two-sided ideals, namely $\{0\}$ and A itself. A *central simple algebra* over k is a finite-dimensional k-algebra that is both central and simple.

Note that a central simple algebra is, by definition, finite-dimensional in addition to being central and simple. Easy examples of central simple algebras are matrix algebras: for any field k and any natural number n, the k-algebra $\mathrm{M}_n(k)$ of $n \times n$ matrices with coefficients in k is a central simple algebra. More generally for any ring R, let $\mathrm{M}_n(R)$ denote the ring of $n \times n$ matrices over R.

Exercise 10.2.2. Let R be a ring, and let m, n be positive integers.

(i) Show that the R-algebras $\mathrm{M}_m(\mathrm{M}_n(R))$ and $\mathrm{M}_{mn}(R)$ are isomorphic.
(ii) Show that, if S is an R-algebra, then there is a natural isomorphism $\mathrm{M}_n(R) \otimes_R S \to \mathrm{M}_n(S)$.
(iii) If I is an ideal of R, let $\mathrm{M}_n(I)$ denote the subset of $\mathrm{M}_n(R)$ consisting of matrices with entries in I. Show that $I \leftrightarrow \mathrm{M}_n(I)$ is a bijection between the set of two-sided ideals of the ring R and the set of two-sided ideals of $\mathrm{M}_n(R)$.
(iv) Let Id denote the identity matrix in $\mathrm{M}_n(R)$. Show that the map $R \to \mathrm{M}_n(R)$ defined by $r \mapsto r\,\mathrm{Id}$ identifies the centre of R with the centre of $\mathrm{M}_n(R)$.
(v) Conclude that, if A is a central simple algebra over a field k, then $\mathrm{M}_n(A)$ is also a central simple algebra over k.

It is easy to see that every division algebra is simple, and so every finite-dimensional central division algebra over k is a central simple algebra over k. The matrix algebra $\mathrm{M}_n(k)$ is not a division algebra for $n \geq 2$, since it contains non-invertible matrices. A central simple algebra over k is called *split* if it is isomorphic to $\mathrm{M}_n(k)$ for some $n > 0$.

To see an example of a non-split central division algebra, take $k = \mathbf{R}$, and let $\mathbb{H}_{\mathbf{R}}$ be the $\mathbf{R}$-algebra of Hamilton quaternions: the underlying vector space of $\mathbb{H}_{\mathbf{R}}$ is $\mathbf{R}^4$ with basis $(1, i, j, ij)$, and multiplication is uniquely determined by

$$i^2 = -1, \quad j^2 = -1, \quad ji = -ij.$$

Note that the relation $(ij)^2 = -1$ is a consequence of the above.

Exercise 10.2.3. Show that $\mathbb{H}_{\mathbf{R}}$ is a division algebra over $\mathbf{R}$.

We did not use many properties of the field $\mathbf{R}$ in the preceding example: the fact that every element of $\mathbb{H}_{\mathbf{R}}$ has an inverse follows essentially from the fact that -1 is not a square in $\mathbf{R}$. This leads us to the more general definition of a quaternion algebra.

Definition 10.2.4. Let k be a field of characteristic different from 2 and let a, b be non-zero elements of k. Define the *quaternion algebra* $(a,b)_k$ to be

the k-algebra whose underlying vector space is k^4 with basis $(1,i,j,ij)$ and on which multiplication is uniquely determined by

$$i^2 = a, \quad j^2 = b, \quad ji = -ij.$$

As in the case of the algebra $\mathbb{H}_{\mathbf{R}}$, the relation $(ij)^2 = -ab$ follows from the definitions.

The notation for a quaternion algebra is very similar to that for a Hilbert symbol; we shall see (Exercise 10.4.4) that the two notions are closely related.

Exercise 10.2.5. Let k be a field of odd characteristic, and let a,b,c be elements of $k^\times$.

144: is zero odd? Check later uses as well?

(i) Prove that the quaternion algebra $(a,b)_k$ is a central simple algebra over k.
(ii) Prove that the three quaternion algebras $(a,b)_k$, $(b,a)_k$ and $(ac^2,b)_k$ are isomorphic.
(iii) Prove that the quaternion algebra $(a^2,b)_k$ is not a division algebra.
(iv) Suppose that a is not a square in k and let $\gamma \in k(\sqrt{a})^\times$. Prove that the algebras $(a,b)_k$ and $\left(a, b\mathrm{N}_{k(\sqrt{a})/k}(\gamma)\right)$ are isomorphic.

Example 10.2.6. Let A be the quaternion algebra $(-1,3)_{\mathbf{F}_7}$. We will show that this algebra is split by determining an explicit isomorphism $\rho : A \to \mathrm{M}_2(\mathbf{F}_7)$. It suffices to find two matrices $I,J \in \mathrm{M}_2(\mathbf{F}_7)$ satisfying the equations $I^2 = -\mathrm{Id}$, $J^2 = 3\mathrm{Id}$ and $IJ + JI = 0$, since the assignment $\rho(i) = I$ and $\rho(j) = J$ will then define a homomorphism of algebras; because A is simple, ρ is then injective and hence surjective by considering dimensions. The matrix

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

satisfies $I^2 = -\mathrm{Id}$; we try to find a compatible J of the form

$$J = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

The condition $IJ + JI = 0$ implies $a + d = 0$ and $b = c$. The condition $J^2 = 3\mathrm{Id}$ then becomes $(a^2 + b^2)\mathrm{Id} = 3\mathrm{Id}$. It therefore suffices to observe that $a = 1$, $b = 3$ satisfy the equation $a^2 + b^2 = 3$ to conclude.

Exercise 10.2.7. Let k be a field of odd characteristic.

(i) Show that, for any $a \in k^\times$, the quaternion algebra $(a,1)_k$ is split.
(ii) Deduce that, if $b \in k^\times$ is a norm from $k(\sqrt{a})$, then the algebra $(a,b)_k$ is split.

(iii) Deduce further that, for $a \neq 0, 1$, the algebra $(a, 1-a)_k$ is split.

A class of central simple algebras generalising the quaternion algebras is the class of cyclic algebras.

Definition 10.2.8. Let ℓ/k be a finite cyclic extension of fields of degree n. Given $b \in k^*$ and a generator σ of $\mathrm{Gal}(\ell/k)$, the *cyclic algebra* $(\ell/k, \sigma, b)$ is defined as follows: let $\ell[x]_\sigma$ denote the non-commutative "twisted polynomial ring", where $ax = x\sigma(a)$ for all $a \in \ell$; then $(\ell/k, \sigma, b)$ is the quotient of $\ell[x]_\sigma$ by the two-sided ideal $(x^n - b)$.

More explicitly, the k-algebra $(\ell/k, \sigma, b)$ is the vector space over ℓ with basis $1, x, x^2, \ldots, x^{n-1}$, and multiplication defined by

$$x^i x^j = \begin{cases} x^{i+j} & \text{if } i+j < n; \\ b x^{i+j-n} & \text{if } i+j \geq n; \end{cases}$$
$$ax = x\sigma(a) \quad \text{for all } a \in \ell.$$

Exercise 10.2.9. Verify that, when k has odd characteristic, $\ell = k(\sqrt{a})$ is a quadratic extension of k, and σ is the non-trivial element of $\mathrm{Gal}(\ell/k)$, the cyclic algebra $(\ell/k, \sigma, b)$ is isomorphic to the quaternion algebra $(a, b)_k$ defined above.

We shall see later **?**, using Galois cohomology, that the algebra $(\ell/k, \sigma, f)$ is split if and only if b is a norm for the extension ℓ/k, thus extending the case of quaternion algebras.

If k contains a primitive nth root of unity ζ, then Kummer theory shows that every cyclic extension ℓ/k of degree n is of the form $\ell = k(\sqrt[n]{a})$ for some $a \in k^\times$. Given $a, b \in k^\times$, we let $\sigma \in \mathrm{Gal}(k(\sqrt[n]{a})/k)$ be the automorphism that maps $\sqrt[n]{a} \mapsto \zeta \sqrt[n]{a}$, and define the cyclic algebra $(a, b)_{k,\zeta}$ by

$$(a, b)_{k,\zeta} = (k(\sqrt[n]{a})/k, \sigma, b).$$

We now turn to classifying central simple algebras over a field. An important step is the following theorem of Wedderburn, which reduces the problem to that of understanding division algebras.

Theorem 10.2.10 (Wedderburn)**.** *Let A be a central simple algebra over a field k. There are a division algebra D, unique up to isomorphism, and a positive integer n such that A is isomorphic to $\mathrm{M}_n(D)$.*

Proof See Gille and Szamuely (2006, Theorem 2.1.3). □

The division algebra D of Theorem 10.2.10 is necessarily finite-dimensional and central over k. For quaternion algebras, Wedderburn's theorem has a very

simple consequence: a quaternion algebra over a field k is either a division algebra or is isomorphic to $\mathrm{M}_2(k)$.

Next we examine tensor products of central simple algebras.

Lemma 10.2.11. *Let k be a field and let A and B be finite-dimensional simple algebras over k. If either A or B is central over k, then the tensor product $A \otimes_k B$ is simple.*

Proof See Milne (2008, Proposition IV.2.6). □

For a ring R, the symbol $Z(R)$ denotes the centre of R.

Lemma 10.2.12. *Let A and B be two finite-dimensional algebras over a field k. Then, inside $A \otimes_k B$, the equality $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$ holds.*

Proof This is a special case of Milne (2008, Proposition IV.2.3). □

Lemma 10.2.13. *Let A and B be central simple algebras over k. The k-algebra $A \otimes_k B$ is also a central simple algebra over k.*

Proof This follows immediately from Lemmas 10.2.11 and 10.2.12. □

Given any k-algebra A, we denote by A^{opp} the *opposite algebra* of A: A^{opp} is the k-algebra whose underlying vector space is the same as the vector space underlying A, and on which multiplication is defined by $a \cdot_{A^{\mathrm{opp}}} b = b \cdot_A a$, that is, multiplication in A^{opp} is multiplication in A in the opposite order. If A is a central simple algebra over k of dimension n, then A^{opp} is also a central simple algebra over k of dimension n.

We next give a characterisation of central simple algebras in terms of their endomorphism rings.

Proposition 10.2.14. *Let A be a non-zero algebra over k of finite dimension. Then A is a central simple algebra over k if and only if the homomorphism of k-algebras*

$$\begin{array}{rcl} \phi : A \otimes_k A^{\mathrm{opp}} & \longrightarrow & \mathrm{End}_k(A) \\ a \otimes b & \longmapsto & (x \mapsto axb) \end{array}$$

is an isomorphism.

145: Adjust displayed formula

Proof Suppose that A is a central simple algebra over k. By Lemma 10.2.13 the algebra $A \otimes_k A^{\mathrm{opp}}$ is also a central simple algebra. In particular, the homomorphism ϕ is either injective or zero. Since the identity element on the left maps to the identity element on the right, ϕ is injective. Comparing dimensions shows that ϕ is also surjective, hence an isomorphism.

In order to show that ϕ being an isomorphism implies that A is central,

suppose on the contrary that a is an element of the centre of A that does not lie in k. Then $a \otimes 1 - 1 \otimes a$ is a non-zero element of the kernel of ϕ, and so ϕ is not an isomorphism.

Finally, suppose that ϕ is an isomorphism, and let us show that A is simple. Let I be a two-sided ideal in A. Let n be the dimension of A over k, and let i be the dimension of I. Choosing a complementary subspace V to I, the tensor product $A \otimes A^{\mathrm{opp}}$ is the direct sum of the four subspaces $I \otimes_k I$, $I \otimes_k V$, $V \otimes_k I$ and $V \otimes_k V$. The first three of these are mapped by ϕ into the subspace $\mathrm{Hom}_k(A, I) \subset \mathrm{End}_k(A)$. Since ϕ is injective, looking at dimensions gives

$$i^2 + i(n-i) + (n-i)i \leq ni$$

and so we have either $i = 0$, or $2n - i \leq n$ and therefore $i = n$. Thus I is either the zero ideal or the whole of A, showing that A is simple. □

146: Bourbaki VIII, §14, Th. 1 has a possibly better proof.

We conclude this section with a discussion of the reduced norm. The determinant of a matrix is a tool that is useful in many ways, one of which is to characterise whether the matrix is invertible. On a general central simple algebra, the rôle of the determinant is played by the reduced norm, which we will now define.

Let A be a central simple algebra over a field k. The *norm* of an element $a \in A$, denoted $\mathrm{N}_{A/k}(a)$, is the determinant of the linear endomorphism $x \mapsto ax$ of A. (This is equal to the determinant of the endomorphism $x \mapsto xa$.) It is clear that, for all $a, b \in A$, we have $\mathrm{N}_{A/k}(ab) = \mathrm{N}_{A/k}(a)\mathrm{N}_{A/k}(b)$. It also follows easily from the definition that, if we fix a basis of A, then $\mathrm{N}_{A/k}(a)$ is a homogeneous polynomial of degree $\dim_k A$ in the coordinates of a, with coefficients in k.

Let us consider the case when $A = \mathrm{M}_n(k)$ is a matrix algebra. As a vector space, A is the direct sum of the n subspaces $E_1, \ldots, E_n$, where $E_i \cong k^n$ consists of those matrices whose entries outside the ith column are zero. Multiplication on the left by any matrix preserves this decomposition. For any matrix $m \in \mathrm{M}_n(k)$, the action of m on E_i is the same as its natural action on k^n, so we see $\mathrm{N}_{A/k}(m) = \big(\det(m)\big)^n$.

Definition 10.2.15. Let A be a central simple algebra over a field k, and fix an isomorphism $\phi : A \otimes_k k^{\mathrm{sep}} \to \mathrm{M}_n(k^{\mathrm{sep}})$ of k^{sep}-algebras. The *reduced norm* of an element $a \in A$ is defined to be $\mathrm{Nrd}_{A/k}(a) = \det(\phi(a \otimes 1))$.

Remark 10.2.16. (i) The definition of $\mathrm{Nrd}_{A/k}(a)$ does not depend on the choice of the isomorphism ϕ since, by Corollary 10.3.13, any two such isomorphisms are related by conjugation by an element of $\mathrm{M}_n(k^{\mathrm{sep}})$, which does not affect the determinant.

(ii) We have $\left(\mathrm{Nrd}_{A/k}(a)\right)^n = \mathrm{N}_{A/k}(a)$, where $n = \sqrt{\dim_k A}$. Indeed, the determinant of a linear transformation is unaffected by changing the base field, so this follows from the case of matrix algebras, described above.

(iii) It follows immediately from the definition that, for all $a, b \in A$, we have $\mathrm{Nrd}_{A/k}(ab) = \mathrm{Nrd}_{A/k}(a)\mathrm{Nrd}_{A/k}(b)$.

Like the determinant, the reduced norm is a homogeneous polynomial function on an algebra A:

Lemma 10.2.17. *Let A be a central simple algebra of dimension n^2 over a field k. Fix a basis $a_1, \ldots, a_{n^2}$ for A over k. There is a homogeneous polynomial F of degree n in $k[x_1, \ldots, x_{n^2}]$ such that, for all $\lambda_1, \ldots, \lambda_{n^2}$ in k, we have*

$$\mathrm{Nrd}_{A/k}(\lambda_1 a_1 + \cdots + \lambda_{n^2} a_{n^2}) = F(\lambda_1, \ldots, \lambda_{n^2}).$$

Proof Fix an isomorphism $\phi\colon A \otimes_k k^{\mathrm{sep}} \to \mathrm{M}_n(k^{\mathrm{sep}})$. Let $a = \sum_{i=1}^{n^2} \lambda_i a_i$ be an element of A. Since ϕ is a k^{sep}-linear map, the entries of the matrix $\phi(a \otimes 1)$ are linear polynomials in the λ_i, with coefficients in k^{sep}. Therefore the determinant $\mathrm{Nrd}_{A/k}(a) = \det(\phi(a \otimes 1))$ is given by $F(\lambda_1, \ldots, \lambda_{n^2})$, where F is a homogeneous polynomial of degree n with coefficients in k^{sep}. We must shows that F actually has coefficients in k.

The polynomial F^n has coefficients in k, since F^n is the polynomial expressing $\mathrm{N}_{A/k}(a)$ in terms of the coordinates λ_i. Let $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ be an automorphism, and let σF be the polynomial obtained by letting σ act on the coefficients of F; it satisfies $(\sigma F)(\mathbf{x}) = \sigma(F(\sigma^{-1}\mathbf{x}))$ for all $\mathbf{x} \in (k^{\mathrm{sep}})^{n^2}$. Then we have $(\sigma F)^n = \sigma(F^n) = F^n$, and therefore $\sigma F = \zeta F$ where ζ is an n-th root of unity in k^{sep}. To show $\zeta = 1$, it is enough to exhibit a vector $\mathbf{x} \in k^{n^2}$ such that $F(\mathbf{x})$ lies in k, since for such an $\mathbf{x}$ we have $\zeta F(\mathbf{x}) = (\sigma F)(\mathbf{x}) = F(\mathbf{x})$. But ϕ is an isomorphism of algebras, so we have $\mathrm{Nrd}(1_A) = \det(\phi(1)) = \det(\mathrm{Id}) = 1$. Writing $1_A = \sum_i \lambda_i a_i$ gives $F(\lambda_1, \ldots, \lambda_n) = 1$. Thus F is fixed by σ. This holds for all $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$, so F has coefficients in k. □

10.3 The Brauer group of a field

Definition 10.3.1. Let k be a field. Two central simple algebras A and B over k are *equivalent* if there are positive integers m and n such that $\mathrm{M}_m(A)$ and $\mathrm{M}_n(B)$ are isomorphic. This induces an equivalence relation on the set of isomorphism classes of central simple algebras over k, with transitivity following from Exercise 10.2.2(i). We denote the equivalence class of the central simple algebra A over k by $[A]$, and call it the *Brauer class* of A.

Wedderburn's Theorem shows that two central simple algebras are equivalent if and only if they are both matrix algebras over the same division algebra.

We are now in a position to define the Brauer group of the field k.

Definition 10.3.2. The *Brauer group* $\mathrm{Br}(k)$ of the field k is the abelian group whose elements are the equivalence classes of central simple algebras over k, with group operation $[A]\cdot[B] := [A \otimes_k B]$.

The Brauer group is indeed an abelian group. Associativity and commutativity come from standard properties of the tensor product. The identity in $\mathrm{Br}(k)$ is the class of the field k. By Proposition 10.2.14, the inverse of the class of a central simple algebra A is the class of A^{opp}, because $\mathrm{End}_k(A)$ is isomorphic to a matrix algebra over k.

Wedderburn's Theorem shows that each class in the Brauer group of a field contains a unique division algebra; the other algebras in that class are isomorphic to matrix algebras over that division algebra.

As an example of multiplication in the Brauer group, we look at the tensor product of two quaternion algebras. In general, there is no reason to expect the tensor product of two quaternion algebras to be equivalent to a third quaternion algebra, but we have the following bilinearity result.

Lemma 10.3.3. *Let k be a field of odd characteristic and let a,b,c be non-zero elements of k. Then there is an isomorphism*

$$(a,b)_k \otimes_k (a,c)_k \cong \mathrm{M}_2((a,bc)_k).$$

Proof This can be proved by exhibiting an explicit isomorphism: see Gille and Szamuely (2006, Lemma 1.5.2). □

In other words, the product of the classes $[(a,b)_k]$ and $[(a,c)_k]$ in $\mathrm{Br}k$ is the class $[(a,bc)_k]$. So the map from $k^\times \times k^\times$ to $\mathrm{Br}k$ that sends (a,b) to the class of the algebra $(a,b)_k$ is a bilinear map of abelian groups. (We have only proved linearity on one side, but it is also symmetric.) Combined with Exercise 10.2.5(ii), this also shows that the class of a quaternion algebra has order dividing 2 in the Brauer group.

Remark 10.3.4. Let k be any field. The second *Milnor K-group* of k, written $\mathrm{K}_2(k)$, is defined to be the quotient of the group $k^\times \otimes_{\mathbb{Z}} k^\times$ by the subgroup generated by all elements of the form $a \otimes (1-a)$ for $a \in k$ with $a \neq 0,1$. If k has odd characteristic then Lemma 10.3.3, together with Exercises 10.2.5(ii) and 10.2.7, shows that the map sending $a \otimes b$ to the class of $(a,b)_k$ induces a homomorphism $\mathrm{K}_2(k) \to \mathrm{Br}k[2]$. In fact, the induced homomorphism $\mathrm{K}_2(k)/2\mathrm{K}_2(k) \to \mathrm{Br}k[2]$ is an *isomorphism*, as was proved by Merkurjev (1981). This means that any class in $\mathrm{Br}k[2]$ is represented by a tensor product of quaternion algebras.

More generally, if k contains a primitive nth root of unity ζ, then there is a similar homomorphism $\mathrm{K}_2(k)/n\mathrm{K}_2(k) \to \mathrm{Br}\,k[n]$ defined by sending the class of $a \otimes b$ to the class of the cyclic algebra $(a,b)_{k,\zeta}$. That this is also an isomorphism is a celebrated theorem of Merkurjev and Suslin (1982).

Exercise 10.3.5. Prove that if k is algebraically closed, then $\mathrm{Br}(k)$ consists of the single element $[k]$. (Hint: it suffices to show that there are no non-trivial division algebras over k. If D is a division algebra over k, let d be an element of D and consider $k(d)$.)

In fact, a stronger statement is true.

Proposition 10.3.6 (Noether, Köthe)**.** *Let k be a separably closed field. The Brauer group* $\mathrm{Br}\,k$ *is trivial.*

Proof See Bourbaki (2012, §13, Proposition 3). □

Exercise 10.3.7. Find an explicit isomorphism between $\mathbb{H}_{\mathbf{R}} \otimes_{\mathbf{R}} \mathbf{C}$ and $\mathrm{M}_2(\mathbf{C})$.

We now look at the behaviour of central simple algebras under base extension.

Lemma 10.3.8. *Let ℓ/k be a field extension and A a finite-dimensional algebra over k. The algebra A is a central simple algebra over k if and only if $A \otimes_k \ell$ is a central simple algebra over ℓ.*

Proof Let $\phi : A \otimes_k A^{\mathrm{opp}} \to \mathrm{End}_k(A)$ be the homomorphism of Proposition 10.2.14. Let A_ℓ denote the base change $A \otimes_k \ell$. Using the natural isomorphisms

$$(A \otimes_k A^{\mathrm{opp}}) \otimes_k \ell \cong A_\ell \otimes_\ell A_\ell^{\mathrm{opp}} \quad \text{and} \quad \mathrm{End}_k(A) \otimes_k \ell \cong \mathrm{End}_\ell(A_\ell)$$

identifies the analogous homomorphism $\phi_\ell : A_\ell \otimes_\ell A_\ell^{\mathrm{opp}} \to \mathrm{End}_\ell(A_\ell)$ with the base change $\phi \otimes 1$. The linear map ϕ is an isomorphism if and only if its base change ϕ_ℓ is an isomorphism, so Proposition 10.2.14 gives the desired result. □

We call $A \otimes_k \ell$ the *extension* of A to ℓ. It is easy to check that extension to ℓ defines a group homomorphism $\mathrm{Br}(k) \to \mathrm{Br}(\ell)$, making Br into a functor from the category of fields to the category of abelian groups.

Define $\mathrm{Br}(\ell/k)$ to be the kernel of the extension map $\mathrm{Br}\,k \to \mathrm{Br}\,\ell$.

Proposition 10.3.9. *Let k be a field and let A be a finite-dimensional algebra over k. The algebra A is a central simple algebra over k if and only if there is a finite separable extension ℓ/k such that $A \otimes_k \ell$ is isomorphic to a matrix algebra.*

Proof Assume that there is such an extension ℓ. In particular, $A \otimes_k \ell$ is a central simple algebra, so Lemma 10.3.8 shows that A is a central simple algebra.

Conversely, suppose that A is a central simple algebra over k. Let k^{sep} be a separable closure of k. By Proposition 10.3.6, there is an isomorphism $\phi : A \otimes_k k^{\mathrm{sep}} \to \mathrm{M}_n(k^{\mathrm{sep}})$ for some positive integer n. Choose a basis $a_1, \ldots, a_r$ for A over k, and let ℓ be the subextension of k^{sep}/k generated by the entries of the matrices $\phi(a_1 \otimes 1), \ldots, \phi(a_r \otimes 1)$. Then the restriction of ϕ to $A \otimes_k \ell$ induces an isomorphism of $A \otimes_k \ell$ with $\mathrm{M}_n(\ell)$. □

A field ℓ as in the proposition is called a *splitting field* for A, and we say that A *splits* over ℓ.

The following two corollaries are immediate.

Corollary 10.3.10. *Let k be a field. The Brauer group* $\mathrm{Br}k$ *is the union of the groups* $\mathrm{Br}(\ell/k)$ *as ℓ runs over all finite separable extensions of k.* □

Corollary 10.3.11. *The dimension of a central simple algebra over k is a square.* □

Next we state the Skolem–Noether theorem, which has the consequence that all automorphisms of a central simple algebra are inner. We will need this later when we give the cohomological description of the Brauer group.

Theorem 10.3.12 (Skolem–Noether)**.** *Let k be a field, let A be a simple k-algebra, let B be a central simple k-algebra and let $f, g : A \to B$ be two homomorphisms. Then there exists an invertible element $b \in B$ such that $f(x) = bg(x)b^{-1}$ for all $x \in A$.*

Proof See Milne (2008, Theorem IV.2.10). □

Corollary 10.3.13. *Let A be a central simple algebra over a field k. Then every automorphism of A is inner, that is, given by conjugation by an element of A.*

Proof If $\phi : A \to A$ is an automorphism, then apply Theorem 10.3.12 with $f = \phi$ and $g = \mathrm{id}_A$. □

10.4 Brauer groups of some fields

In this section we describe the Brauer groups of several important fields, including the real numbers, the p-adic numbers and the rational numbers. We begin with the real numbers.

Theorem 10.4.1 (Frobenius)**.** *If A is a finite-dimensional division algebra over the real numbers $\mathbf{R}$, then A is isomorphic to either $\mathbf{R}$ itself, the field $\mathbf{C}$ of complex numbers, or the algebra $\mathbb{H}_{\mathbf{R}}$ of Hamilton quaternions.*

Proof See Bourbaki (2012, Section 19, Théorème 1). □

Corollary 10.4.2. *The Brauer group of $\mathbf{R}$ has order 2, generated by the class consisting of matrix algebras over the quaternion algebra $\mathbb{H}_{\mathbf{R}}$.*

We will be able to prove for ourselves that $\mathrm{Br}\,\mathbf{R}$ has order 2, without using Frobenius' theorem, after developing Galois cohomology in Chapter 14.

Next, we turn to local fields.

Theorem 10.4.3. *Let k be a number field and let v be a finite place of k. There is a canonical isomorphism* $\mathrm{inv}_v\colon \mathrm{Br}\,k_v \to \mathbf{Q}/\mathbf{Z}$.

Proof We will prove this in Section 15.2 using Galois cohomology. For a direct construction of inv_v, see Milne (2008, Section IV.4). □

The isomorphism inv_v in the preceding theorem is called the *Hasse invariant map* at v.

Exercise 10.4.4. Let v be a valuation of $\mathbf{Q}$. Show that the value of the invariant at v of the quaternion algebra $(a,b)_{\mathbf{Q}}$ is equal to the Hilbert symbol $(a,b)_v$ (under the unique group isomorphism between $\{1,-1\}$ and $\frac{1}{2}\mathbf{Z}/\mathbf{Z}$).

To state the following fundamental theorem, describing the Brauer group of a number field k, we also need to define invariant maps at infinite places. If v is a real place of k, then define $\mathrm{inv}_v\colon \mathrm{Br}\,k_v \to \mathbf{Q}/\mathbf{Z}$ to be the unique injective homomorphism mapping $\mathrm{Br}\,k_v \cong \mathrm{Br}\,\mathbf{R}$ to the subgroup $\{0, \frac{1}{2}\} \subset \mathbf{Q}/\mathbf{Z}$. If v is a complex place of k, then $\mathrm{Br}\,k_v$ is trivial and we define inv_v to be the zero map. Recall that Ω_k denotes the set of all places of a number field k. The following theorem is closely related to the reciprocity theorem of global class field theory, and generalises the product formula for the Hilbert symbol.

Theorem 10.4.5. *Let k be a number field. There is an exact sequence*

$$0 \to \mathrm{Br}\,k \to \bigoplus_{v\in\Omega_k} \mathrm{Br}\,k_v \xrightarrow{\sum_v \mathrm{inv}_v} \mathbf{Q}/\mathbf{Z} \to 0 \tag{10.1}$$

where the map $\mathrm{Br}\,k \to \bigoplus \mathrm{Br}\,k_v$ is the diagonal map induced by the inclusions of k into each completion k_v.

Proof For a proof using cohomology, see Milne (2008, VIII.4). □

The injectivity of the map $\mathrm{Br}\, k \to \bigoplus \mathrm{Br}\, k_v$ is the celebrated theorem of Albert and Brauer–Hasse–Noether; see Roquette (2005) for a historical discussion of this theorem and its proof.

The sequence (10.1) shows a very important property: the local invariants of a Brauer class satisfy a global relation. It is this compatibility condition which will form the basis of the Brauer–Manin obstruction.

We conclude this section by showing that a certain important class of fields, namely the quasi-algebraically closed fields, have trivial Brauer group. In particular, this proves that the Brauer group of a finite field is trivial.

Definition 10.4.6. A field k is said to be *quasi-algebraically closed*, or C_1, if every non-constant homogenous polynomial of degree d in n variables over k satisfying $n > d$ has a non-trivial zero in k^n.

Example 10.4.7. The Chevalley–Warning theorem (Theorem 2.2.4) shows that a finite field is C_1.

Theorem 10.4.8 (Tsen)**.** *Let K be the function field of a curve over an algebraically closed base field k. Then K is a C_1 field.*

Proof See Greenberg (1969, Theorem 3.6), Shatz (1972, Theorem IV.3.24) or Kollár (1996, Theorem IV.6.5). □

A property of C_1 fields that is important to us is that they have trivial Brauer group.

Theorem 10.4.9. *Let k be a C_1 field. Then* $\mathrm{Br}\, k$ *is trivial.*

Proof It is enough to show that no central simple algebra of dimension $n^2 > 1$ over k is a division algebra. Let A be such an algebra over k, and choose a basis $a_1, \ldots, a_{n^2}$ for A. By Lemma 10.2.17, we have

$$\mathrm{Nrd}_{A/k}(\lambda_1 a_1 + \cdots + \lambda_{n^2} a_{n^2}) = F(\lambda_1, \ldots, \lambda_{n^2}).$$

for some homogeneous $F \in k[x_1, \ldots, x_{n^2}]$ of degree n. Since k is C_1, the polynomial F admits a non-trivial zero. Therefore there is a non-zero element $a \in A$ satisfying $\mathrm{Nrd}_{A/k}(a) = 0$. By multiplicativity of the reduced norm, a cannot be invertible; thus A is not a division algebra. □

Corollary 10.4.10. (i) *If k is a finite field, then* $\mathrm{Br}\, k$ *is trivial.*
(ii) *If C is a curve over an algebraically closed field, then* $\mathrm{Br}\, \kappa(C)$ *is trivial.*

Proof These follow from Example 10.4.7 and Theorem 10.4.8, respectively. □

10.5 Motivation for the Brauer group of a variety

We conclude this chapter with a look at the Brauer group of the function field of a variety, which leads us to want to define the Brauer group of the variety. That will be the goal of the following two chapters.

Let X be a smooth, geometrically irreducibe, projective variety over a field k. The Brauer group of the field $\kappa(X)$ consists of equivalence classes of central simple algebras over $\kappa(X)$. Rather like evaluating an element of $\kappa(X)$ at a point of X, we can ask what it might mean to evaluate an element of $\mathrm{Br}\,\kappa(X)$ at a point of X.

Example 10.5.1. Take $X = \mathbf{A}^1_{\mathbf{Q}}$. The function field of X is $\kappa(X) = \mathbf{Q}(t)$. Consider the quaternion algebra $\mathscr{A} = (-1,t)_{\mathbf{Q}(t)}$. For any $a \in \mathbf{Q}$, we can try to evaluate $\mathscr{A}$ at the point defined by $t = a$, simply by substituting $t = a$ into the definition of $\mathscr{A}$. If a is non-zero, this gives us the quaternion algebra $(-1,a)_{\mathbf{Q}}$, which defines a class in $\mathrm{Br}\,\mathbf{Q}$. However, if a is zero, then we obtain an algebra $(-1,0)_{\mathbf{Q}}$ that is not a central simple algebra over $\mathbf{Q}$.

There is no need to restrict ourselves to $a \in \mathbf{Q}$. For any extension $K/\mathbf{Q}$ and any non-zero $a \in K$, we can evaluate $\mathscr{A}$ at $t = a$ to obtain an element of $\mathrm{Br}\,K$. So this kind of "evaluation" works for all points in the open set U defined by $t \neq 0$. In fact, it will turn out that the class of $\mathscr{A}$ in $\mathrm{Br}\,\kappa(X)$ lies in the subgroup $\mathrm{Br}\,U$.

Example 10.5.2. For a more complicated example, let X be the elliptic curve over $\mathbf{Q}$ defined by the Weierstrass equation

$$y^2 = (x-e_1)(x-e_2)(x-e_3)$$

and let $\mathscr{A}$ be the quaternion algebra $(3, x-e_1)_{\kappa(X)}$. Evaluating at any point of $X(\mathbf{Q})$ apart from $(e_1,0)$ gives a well-defined quaternion algebra over $\mathbf{Q}$, but it looks as if we cannot evaluate $\mathscr{A}$ at the point $(e_1,0)$. However, dividing $x-e_1$ by y^2 shows (as in Exercise 10.2.5(ii)) that $\mathscr{A}$ is isomorphic to the algebra $(3,((x-e_2)(x-e_3))^{-1})_{\kappa(X)}$. Here we can indeed substitute $(e_1,0)$ to get an algebra over $\mathbf{Q}$. So it seems that, just as with rational functions on varieties, it is sometimes possible to extend the domain of definition by writing the algebra in a different way. In fact, the algebra $\mathscr{A}$ lies in the subgroup $\mathrm{Br}\,X \subset \mathrm{Br}\,\kappa(X)$.

Following the analogy with rational functions, it is of course not surprising that not every rational function $f \in \kappa(X)$ can be evaluated at every point of X. If that were true, then a k-point of X would give a non-zero evaluation homomorphism $\kappa(X) \to k$, and there are no such homomorphisms. The way to understand this is to introduce the local ring at a point P of X. The local ring $\mathscr{O}_{X,P}$ is a subring of the function field $\kappa(X)$, and it admits an evaluation

homomorphism $\mathscr{O}_{X,P} \to \kappa(P)$. The functions lying in $\mathscr{O}_{X,P}$ are precisely those for which "evaluation at P" makes sense.

Exactly the same approach can be taken with Brauer groups. Rather than hoping for evaluation homomorphisms $\operatorname{Br}\kappa(X) \to \operatorname{Br}k$, we will define the Brauer group of the local ring $\mathscr{O}_{X,P}$ at a point P. This fits into a diagram

$$\operatorname{Br}\kappa(X) \leftarrow \operatorname{Br}\mathscr{O}_{X,P} \to \operatorname{Br}\kappa(P).$$

Thus any element of $\operatorname{Br}\kappa(X)$ lying in the image of $\operatorname{Br}\mathscr{O}_{X,P}$ can be evaluated at P to obtain an element of $\operatorname{Br}\kappa(P)$. In fact we shall see that, since X is smooth, the map $\operatorname{Br}\mathscr{O}_{X,P} \to \operatorname{Br}\kappa(X)$ is injective, and so we can consider $\operatorname{Br}\mathscr{O}_{X,P}$ as a subgroup of $\operatorname{Br}\kappa(X)$. It consists of those elements of $\operatorname{Br}\kappa(X)$ that "can be evaluated at P".

147: What does constant mean? If X is not geometrically reduced, then there could still be elements in an (inseparable) algebraic extension of the ground field; not if X is smooth of course, but that's not added here.

A geometrically irreducible projective variety admits no non-constant regular functions: there are no non-constant elements of $\kappa(X)$ that lie in $\mathscr{O}_{X,P}$ for all points P. For Brauer groups, however, this is more interesting: depending on the geometry of the variety, there can indeed be non-constant elements in $\operatorname{Br}\kappa(X)$ that lie in $\operatorname{Br}O_{X,P}$ for *all* points P of X. Such elements constitute the Brauer group of X.

In Chapter 11 we will start to make the above discussion precise by defining the Brauer group of a ring, and in particular the Brauer group of a local ring. In Chapter 12 we will use this to define the Brauer group of a variety.

11

The Brauer group of a ring

The definition of the Brauer group of a field can be generalised to apply to arbitrary commutative rings. We will need this, at least in the case of local rings, in order to define the Brauer group of a variety in the next chapter.

Central simple algebras over fields are examples of a more general class of algebras over commutative rings, called *Azumaya algebras*. Recall that a central simple algebra over a field is a finite-dimensional vector space, endowed with the structure of an algebra, and satisfying certain properties. If the base field is to be replaced by a commutative ring, then a natural generalisation is to replace vector spaces with projective modules, which are not necessarily free but are *locally* free. This gives a theory of Brauer groups closely matching that over fields. Similarly, over a field, we took the trivial class in the Brauer group to consist of matrix algebras. A matrix algebra over a field is the endomorphism algebra of a vector space, and so when we define the Brauer group of a ring we will take the trivial class to consist of the endomorphism rings of projective modules.

The study of Brauer groups of general commutative rings goes back to Auslander and Goldman (1960), building on the definition of "maximally central algebras" of Azumaya (1951). For a useful discussion of various equivalent definitions of Azumaya algebras and their history, see Bass (1967); DeMeyer and Ingraham (1971); Millar (2010).

11.1 Some commutative algebra

We begin by recalling some properties of localisation and of finitely generated projective modules. For any prime ideal $\mathfrak{p}$ of a commutative ring R and for any R-algebra M, let $M_{\mathfrak{p}}$ denote $M \otimes_R R_{\mathfrak{p}}$, let $k(\mathfrak{p})$ denote the field $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ and let $M(\mathfrak{p})$ denote $M \otimes_R k(\mathfrak{p})$.

Lemma 11.1.1. *Let R be a commutative ring, and let $f\colon M \to N$ be a homomorphism of R-modules. The following are equivalent:*

(i) *f is injective;*
(ii) *for every prime ideal $\mathfrak{p} \subset R$, the induced homomorphism $f_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective;*
(iii) *for every maximal ideal $\mathfrak{m} \subset R$, the induced homomorphism $f_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective.*

The same holds with 'injective' replaced by 'surjective'.

Proof See Atiyah and Macdonald (1969, Proposition 3.9). □

Let R be a commutative ring. The algebras that appear in the definition of the Brauer group of R will be finitely generated projective modules over R, and we now recall some properties of such modules. A good reference for this is Bourbaki (1998, Section II.5). If a module M over R is finitely generated and projective then, for every prime ideal $\mathfrak{p} \subset R$, the localisation $M_{\mathfrak{p}}$ is free over $R_{\mathfrak{p}}$, of finite rank (see Bourbaki, 1998, Section II.5.2, Théorème 1). This allows us to define the *rank* of a projective module M at a prime ideal $\mathfrak{p} \subset R$ (or, more succinctly, the $\mathfrak{p}$-rank of M) to be the rank of the free module $M_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$. (This is equal to the dimension of the vector space $M(\mathfrak{p})$ over the field $k(\mathfrak{p})$.) Since the localisation of a free module is again a free module of the same rank, it follows that, if $\mathfrak{p} \subset \mathfrak{q}$ are two prime ideals, then the $\mathfrak{q}$-rank of M is equal to the $\mathfrak{p}$-rank. In particular, if R is an integral domain, then every prime ideal contains the prime ideal 0, and so the $\mathfrak{p}$-rank of M is the same for every prime ideal $\mathfrak{p}$.

148: Mention localisation is exact?

Recall that an R-module M is called *faithful* if the natural map $R \to \mathrm{End}_R(M)$ is injective.

Lemma 11.1.2. *Let M be finitely generated projective module over a commutative ring R. The following are equivalent:*

(i) *M is a faithful R-module;*
(ii) *for every prime ideal $\mathfrak{p} \subset R$, the $\mathfrak{p}$-rank of M is non-zero;*
(iii) *for every maximal ideal $\mathfrak{m} \subset R$, the $\mathfrak{m}$-rank of M is non-zero.*

If R is an integral domain, then these are also equivalent to: M is non-zero.

Proof For a prime ideal $\mathfrak{p} \subset R$, the natural map $R_{\mathfrak{p}} \to \mathrm{End}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}})$ identifies $R_{\mathfrak{p}}$ with the scalar $n \times n$ matrices, where n is the $\mathfrak{p}$-rank of M. This map is injective if and only if n is non-zero. Now apply Lemma 11.1.1.

149: Illogical order of sentences?

If R is an integral domain, then the $\mathfrak{p}$-rank of M is the same at all prime ideals $\mathfrak{p}$, and is zero if and only if M is zero. □

For finitely generated projective modules, the following lemma makes a useful companion to Lemma 11.1.1.

Lemma 11.1.3. *Let R be a local ring with maximal ideal $\mathfrak{m}$, and let $f : M \to N$ be a homomorphism of free modules of finite rank over R. The following are equivalent:*

(i) *f is an isomorphism;*
(ii) *the induced homomorphism $M(\mathfrak{m}) \to N(\mathfrak{m})$ is an isomorphism.*

Proof The implication (i)⇒(ii) is immediate; let us prove (ii)⇒(i). By assumption the vector spaces $M(\mathfrak{m})$ and $N(\mathfrak{m})$ have equal dimension, so M and N have equal rank. The determinant of a square matrix representing f is nonzero modulo $\mathfrak{m}$, so is a unit in R; therefore the matrix is invertible and f is an isomorphism. □

We now examine the module of homomorphisms between two finitely generated projective modules.

Lemma 11.1.4. *Let M,N be finitely generated projective modules over a commutative ring R. Then the R-module $\mathrm{Hom}(M,N)$ is also finitely generated and projective.*

Proof By Bourbaki (1998, Section II.5.2, Théorème 1), there exist a finite number of elements $f_1,\dots,f_r \in R$ that generate R as an ideal, and such that, for every i, both localisations M_{f_i} and N_{f_i} are free of finite rank over R_{f_i}. Therefore the module $\mathrm{Hom}_R(M,N)_{f_i}$, which by Bourbaki (1998, Section II.2.7, Proposition 19) is isomorphic to $\mathrm{Hom}_{R_{f_i}}(M_{f_i},N_{f_i})$, is isomorphic to a module of matrices over R_{f_i} and in particular is free of finite rank. Applying Bourbaki (1998, Section II.5.2, Théorème 1) again shows that $\mathrm{Hom}(M,N)$ is finitely generated and projective over R. □

150: Easier to go through all localisations at prime/maximal ideals?

Lemma 11.1.5. *Let $R \to S$ be a homomorphism of commutative rings and let M,N be finitely generated projective R-modules. Then the natural homomorphism of S-modules*

$$\mathrm{Hom}_R(M,N) \otimes_R S \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S),$$

is an isomorphism.

151: comma?

Proof If S is a localisation of R, then the statement is a special case of Proposition 19 of Bourbaki (1998, Section II.2.7). We will use this to prove the general case by localisation.

Although both sides of the claimed isomorphism are S-modules, we can also consider them as R-modules, and the map as a homomorphism of R-modules.

By Lemma 11.1.1, to see that the homomorphism is an isomorphism, it is enough to check this locally on R. Let $\mathfrak{m} \subset R$ be a maximal ideal; then we have $M_\mathfrak{m} \cong R_\mathfrak{m}^m$ and $N_\mathfrak{m} \cong R_\mathfrak{m}^n$ for integers $m, n \geq 0$. It follows that there are isomorphisms

$$\mathrm{Hom}_R(M,N)_\mathfrak{m} \cong \mathrm{Hom}_{R_\mathfrak{m}}(M_\mathfrak{m}, N_\mathfrak{m}) \cong \mathrm{M}_{n\times m}(R_\mathfrak{m}).$$

Similarly, using that tensor products commute with localisation (Bourbaki, 1998, Section II.2.7, Proposition 18) we have

$$(M \otimes_R S)_\mathfrak{m} \cong (M_\mathfrak{m} \otimes_{R_\mathfrak{m}} S_\mathfrak{m}) \cong (S_\mathfrak{m})^m$$
$$(N \otimes_R S)_\mathfrak{m} \cong (N_\mathfrak{m} \otimes_{R_\mathfrak{m}} S_\mathfrak{m}) \cong (S_\mathfrak{m})^n$$
$$\mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)_\mathfrak{m} \cong \mathrm{Hom}_{S_\mathfrak{m}}((M \otimes_R S)_\mathfrak{m}, (N \otimes_R S)_\mathfrak{m}) \cong \mathrm{M}_{n\times m}(S_\mathfrak{m}).$$

Under these isomorphisms, the homomorphism

$$(\mathrm{Hom}_R(M,N) \otimes_R S)_\mathfrak{m} \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)_\mathfrak{m}$$

is identified with the natural base change map

$$\mathrm{M}_{n\times m}(R_\mathfrak{m}) \otimes_{R_\mathfrak{m}} S_\mathfrak{m} \to \mathrm{M}_{n\times m}(S_\mathfrak{m}),$$

which is easily seen to be an isomorphism. Applying Lemma 11.1.1 completes the proof. □

11.2 Definition of the Brauer group

An *algebra* over a commutative ring R is an R-module A endowed with an R-linear multiplication $A \times A \to A$, giving A the structure of a ring with identity 1_A. It follows that the map $R \to A$ sending r to $r.1_A$ is a ring homomorphism whose image is contained in the centre of A.

Lemma 11.2.1. *Let A be an algebra over a commutative ring R, and suppose that A is finitely generated and projective as an R-module. Then A is faithful if and only if the natural map $R \to A$ is injective.*

Proof The map $R \to \mathrm{End}_R A$ factors as $R \to A \to \mathrm{End}_R A$, where the second map sends a to the endomorphism $x \mapsto ax$. This second map is injective because it has the left inverse $f \mapsto f(1)$. Thus A is faithful if and only if $R \to A$ is injective. □

To generalise the notion of central simple algebra to an arbitrary commutative base ring, we use the characterisation of Proposition 10.2.14. For any algebra A over a commutative ring R, let ϕ_A be the homomorphism of R-algebras $A \otimes_R A^{\mathrm{opp}} \to \mathrm{End}_R A$ given by $\phi_A(a \otimes a')(x) = axa'$.

Definition 11.2.2. Let R be a commutative ring. An *Azumaya algebra over R* is an R-algebra that is finitely generated, faithful and projective as an R-module and for which ϕ_A is an isomorphism.

If R is a field, then Proposition 10.2.14 shows that an Azumaya algebra over R is a central simple algebra over R.

Let us see how ϕ_A behaves under base change. If S is a commutative R-algebra, there is the analogous homomorphism ϕ_{A_S} for the S-algebra $A_S = A \otimes_R S$; it is then easy to check that the diagram

$$\begin{array}{ccc} (A \otimes_R A^{\mathrm{opp}}) \otimes_R S & \xrightarrow{\phi_A \otimes \mathrm{id}_S} & (\mathrm{End}_R A) \otimes_R S \\ \downarrow & & \downarrow \\ A_S \otimes_S A_S^{\mathrm{opp}} & \xrightarrow{\phi_{A_S}} & \mathrm{End}_S A_S \end{array} \tag{11.1}$$

commutes, where the vertical maps are the isomorphisms of **??** and Lemma 11.1.5. This allows us to prove the following characterisation of Azumaya algebras.

Proposition 11.2.3. *Let R be a commutative ring and A an R-algebra that is finitely generated and projective as an R-module. The following conditions are equivalent.*

(i) *A is an Azumaya algebra over R.*
(ii) *For every prime ideal $\mathfrak{p}$ of R, the localisation $A_\mathfrak{p}$ is an Azumaya algebra over $R_\mathfrak{p}$.*
(iii) *For every prime ideal $\mathfrak{p}$ of R, the reduction $A(\mathfrak{p})$ is a central simple algebra over the field $k(\mathfrak{p})$.*
(iv) *For every maximal ideal $\mathfrak{m}$ of R, the localisation $A_\mathfrak{m}$ is an Azumaya algebra over $R_\mathfrak{m}$.*
(v) *For every maximal ideal $\mathfrak{m}$ of R, the reduction $A(\mathfrak{m})$ is a central simple algebra over the field $k(\mathfrak{m})$.*

Proof Lemma 11.1.1, together with the commutativity of (11.1), shows that the following are equivalent: ϕ_A is an isomorphism; $\phi_{A_\mathfrak{p}}$ is an isomorphism for all $\mathfrak{p}$; and $\phi_{A_\mathfrak{m}}$ is an isomorphism for all $\mathfrak{m}$. By Lemma 11.1.4, the ring $\mathrm{End}_R A$ is also a finitely generated, projective R-module, and so Lemma 11.1.3 shows that these are also equivalent to: $\phi_{A(\mathfrak{p})}$ is an isomorphism for all $\mathfrak{p}$; and $\phi_{A(\mathfrak{m})}$ is an isomorphism for all $\mathfrak{m}$.

Lemma 11.1.2 shows that the following are equivalent: A is faithful; $A_\mathfrak{p}$ is faithful for all $\mathfrak{p}$; $A(\mathfrak{p})$ is non-zero for all $\mathfrak{p}$; $A_\mathfrak{m}$ is faithful for all $\mathfrak{m}$; $A(\mathfrak{m})$ is non-zero for all $\mathfrak{m}$.

Combining these two statements proves the proposition. □

An easy consequence is that, for any faithful finitely generated projective R-module M, the R-algebra $A = \mathrm{End}_R(M)$ is an Azumaya algebra over R. Indeed, A is finitely generated and projective by Lemma 11.1.4; and, for every maximal ideal $\mathfrak{m}$ of R, the reduction $A(\mathfrak{m}) = \mathrm{End}_{k(\mathfrak{m})}(M(\mathfrak{m}))$ is a non-zero matrix algebra.

Remark 11.2.4. If R is an integral domain with field of fractions K then Proposition 11.2.3 shows that, for any Azumaya algebra A over R, the K-algebra $A \otimes_R K$ is a central simple algebra over K.

Definition 11.2.5. Let R be a commutative ring. Two Azumaya algebras A, B over R are *equivalent* if there are finitely generated faithful projective R-modules M, N such that the R-algebras $A \otimes_R \mathrm{End}_R(M)$ and $B \otimes_R \mathrm{End}_R(N)$ are isomorphic; we denote the equivalence class of A by $[A]$.

Since the tensor product of two central simple algebras is a central simple algebra (Lemma 10.2.13), it follows from Proposition 11.2.3 and the fact that forming tensor products commutes with base change that the tensor product of two Azumaya algebras is again an Azumaya algebra. Observe furthermore that, if A, A', B, B' are Azumaya algebras over a ring R such that A and A' are equivalent and B and B' are also equivalent, then the Azumaya algebras $A \otimes_R B$ and $A' \otimes_R B'$ are equivalent. It is now easy to check that the tensor product induces a group structure on the set of equivalence classes of Azumaya algebras over R. Under this operation, the identity is $[R]$, and the inverse of the class of an Azumaya algebra A over R is the class of A^{opp}.

Definition 11.2.6. Let R be a commutative ring. The *Brauer group* $\mathrm{Br}(R)$ of R is the group of equivalence classes of Azumaya algebras over R, with the operation induced by tensor product.

Over a field K, the Azumaya algebras over K are exactly the central simple algebras over K and the Brauer groups of Definitions 10.3.2 and 11.2.6 coincide.

Example 11.2.7. For any commutative ring R and positive integer n, the matrix algebra $\mathrm{M}_n(R)$ is an Azumaya algebra over R. The Brauer class of $\mathrm{M}_n(R)$ is the identity element of $\mathrm{Br}(R)$, since $\mathrm{M}_n(R)$ is isomorphic to $\mathrm{End}(R^n)$.

Remark 11.2.8. Let R be a commutative *local* ring, with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. In this case, a finitely generated R-module is projective if and only if it is free, and therefore the definition of an Azumaya algebra can be simplified: an Azumaya algebra A over R is an R-algebra that is finitely generated and free as an R-module and such that $A \otimes_R k$ is a central simple algebra

over k. Since the endomorphism algebra of a free R-module is isomorphic to a matrix algebra, two Azumaya algebras A, B over R are equivalent if and only if there are positive integers m, n such that the R-algebras

$$A \otimes_R \mathrm{M}_m(R) \cong \mathrm{M}_m(A) \quad \text{and} \quad B \otimes_R \mathrm{M}_n(R) \cong \mathrm{M}_n(B)$$

are isomorphic.

In their definition of the Brauer group of a commutative ring R, Auslander and Goldman (1960, p. 381) use central separable algebras. For a proof that these are the same as our Azumaya algebras see Bass (1967, Theorem 3.4.1) or DeMeyer and Ingraham (1971, Theorem II.3.4).

11.3 Properties and examples

We first consider the effect of base change on the Brauer group. Let $f\colon R \to S$ be a homomorphism of commutative rings.

Lemma 11.3.1. *Let A be an Azumaya algebra over R. Then $A \otimes_R S$ is an Azumaya algebra over S.*

Proof We first show that $A \otimes_R S$ is a faithful S-module. If $\mathfrak{q}$ is any prime ideal of S, then $\mathfrak{p} = f^{-1}\mathfrak{q}$ is a prime ideal of R. The canonical isomorphisms

$$(A \otimes_R S)_{\mathfrak{q}} \cong (A \otimes_R S) \otimes_S S_{\mathfrak{q}} \cong A \otimes_R S_{\mathfrak{q}} \cong (A \otimes_R R_{\mathfrak{p}}) \otimes_{R_{\mathfrak{p}}} S_{\mathfrak{q}}$$

(*cf.* Bourbaki, 1998, Section II.4.3, proof of Proposition 4) show that the $\mathfrak{q}$-rank of $A \otimes_R S$ is equal to the $\mathfrak{p}$-rank of A. By Lemma 11.1.2, it follows that $A \otimes_R S$ is faithful.

The homomorphism $\phi\colon A \otimes_R A^{\mathrm{opp}} \to \mathrm{End}_R A$ is surjective, and therefore its base change $\phi \otimes_R S$ is also surjective; the commutative diagram (11.1) then shows that $A \otimes_R S$ is an Azumaya algebra. □

152: why is surjectivity enough, and aren't we talking about isomorphisms?

It is straightforward to check that, if A and B are equivalent Azumaya algebras over R, then $A \otimes_R S$ and $B \otimes_R S$ are equivalent Azumaya algebras over S. We conclude that the ring homomorphism f induces a homomorphism

$$f_*\colon \mathrm{Br}(R) \longrightarrow \mathrm{Br}(S)$$

between the Brauer groups of R and S. If $g\colon S \to T$ is a second homomorphism of commutative rings, then the homomorphisms $g_* f_*$ and $(gf)_*$ coincide. Thus, Br defines a covariant functor from the category of commutative rings to the category of abelian groups.

We now generalize the notion of quaternion algebras over a field to what

we call Hamilton algebras over a commutative ring. While not all Hamilton algebras are Azumaya algebras, many of the examples that we will consider are of this form.

Definition 11.3.2. If a, b are elements of a commutative ring R, then the *Hamilton algebra* $(a,b)_R$ is the R-algebra freely generated by 1, i, j, ij as an R-module and with multiplication uniquely determined by

$$i^2 = a, \quad j^2 = b, \quad ji = -ij.$$

If $f\colon R \to S$ is a homomorphism of commutative rings and if a, b are elements of R, then the natural homomorphism

$$(a,b)_R \otimes_R S \to \big(f(a), f(b)\big)_S$$

is an isomorphism of algebras over S.

If k is a field of characteristic different from 2, and a, b are non-zero elements of k, then the Hamilton algebra $(a,b)_k$ over k is the quaternion algebra of Definition 10.2.4. We warn the reader that, in general, an Hamilton algebra need not be an Azumaya algebra, even in the case in which a and b are units in R, as some of the following examples show.

Example 11.3.3. Let A be the Hamilton algebra $(3,5)_{\mathbf{Z}}$ over $\mathbf{Z}$. The algebra $A \otimes \mathbf{Z}/3\mathbf{Z}$ is the Hamilton algebra $(0,-1)_{\mathbf{F}_3}$ over $\mathbf{F}_3$. This algebra is not simple, since the subspace spanned by i and ij is a two-sided ideal. It follows that A is not an Azumaya algebra over $\mathbf{Z}$. Of course, as we saw in Section 10.3, the Hamilton algebra $A \otimes \mathbf{Q} = (3,5)_{\mathbf{Q}}$ *is* a central simple algebra over $\mathbf{Q}$.

Example 11.3.4. Let A be the Hamilton algebra $(-1,-1)_{\mathbf{Z}}$ over $\mathbf{Z}$. The algebra $A \otimes \mathbf{Z}/2\mathbf{Z}$ is the Hamilton algebra $(1,1)_{\mathbf{F}_2}$ over $\mathbf{F}_2$. This algebra is not central, since it is commutative (as is any Hamilton algebra over a ring of characteristic 2). Therefore the Hamilton algebra A is not an Azumaya algebra over $\mathbf{Z}$.

153: Relate this to $\mathrm{Br}\,\mathbf{Z} = 0$.

Example 11.3.5. Let R be the ring $\mathbf{Q}[x, x^{-1}]$ and A the Hamilton algebra $(-1,x)_R$. For every maximal ideal $\mathfrak{m}$ of R, the image of x in the residue field $R/\mathfrak{m}$ is non-zero. Since the residue field has characteristic different from 2, the algebra $A \otimes R/\mathfrak{m}$ is a quaternion algebra and hence a central simple algebra over $R/\mathfrak{m}$. By Proposition 11.2.3 we deduce that A is an Azumaya algebra over R. We claim that the class of the Azumaya algebra A is not in the image of homomorphism $\iota_*\colon \mathrm{Br}(\mathbf{Q}) \to \mathrm{Br}(R)$ induced by the inclusion $\iota\colon \mathbf{Q} \to R$. Indeed, for any maximal ideal $\mathfrak{m}$ of R, the composition

$$\mathrm{Br}(\mathbf{Q}) \xrightarrow{\iota_*} \mathrm{Br}(R) \longrightarrow \mathrm{Br}(R/\mathfrak{m})$$

is induced by the inclusion $\mathbf{Q} \to R/\mathfrak{m}$. Therefore, if $R/\mathfrak{m}$ is isomorphic to $\mathbf{Q}$, then this composition is the identity. Let $\mathfrak{m}$ and $\mathfrak{n}$ be the ideals generated by $x-1$ and $x+1$, respectively. Since the image of A in $\mathrm{Br}(R/\mathfrak{m}) \cong \mathrm{Br}(\mathbf{Q})$ is the trivial class of $(-1,1)_{\mathbf{Q}}$, while its image in $\mathrm{Br}(R/\mathfrak{n}) \cong \mathrm{Br}(\mathbf{Q})$ is the non-trivial class of $(-1,-1)_{\mathbf{Q}}$, we conclude that the class of A in $\mathrm{Br}(R)$ is not in the image of ι_*. In the language of Chapter 12, we have just exhibited a non-constant class in $\mathrm{Br}(\mathbf{A}^1_{\mathbf{Q}} \smallsetminus \{0\})$.

Our next result is a "spreading out" result for Azumaya algebras.

154: Spreading out is 11.3.9, no? This is "being Azumaya is open", no?

Proposition 11.3.6. *Let R be a commutative ring and let A be an R-algebra that is finitely generated and projective as an R-module. Suppose that $\mathfrak{p}$ is a prime ideal of R such that $A \otimes k(\mathfrak{p})$ is a central simple algebra over $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. Then there is an element f in $R \smallsetminus \mathfrak{p}$ such that $A \otimes R[f^{-1}]$ is an Azumaya algebra over $R[f^{-1}]$.*

Proof Firstly, the corollary to Proposition 2 of Bourbaki (1998, Section II.5.1) shows that there exists $s \in R \smallsetminus \mathfrak{p}$ such that $A \otimes R[s^{-1}]$ is *free* over $R[s^{-1}]$. Using the isomorphism $R[s^{-1}][t^{-1}] \cong R[(st)^{-1}]$ and replacing R by $R[s^{-1}]$, we reduce to the case where A is free over R.

So now let A be an R-algebra that is finitely generated and free as an R-module, and suppose that $A(\mathfrak{p}) := A \otimes_R k(\mathfrak{p})$ is a central simple algebra over $k(\mathfrak{p})$. (In particular, this means that A has non-zero rank.) Denote by q the composite homomorphism $R \to R_{\mathfrak{p}} \to k(\mathfrak{p})$. Pick a basis for A as an R-module. This induces bases for $A \otimes_R A^{\mathrm{opp}}$ and $\mathrm{End}_R A$; let $\mathbf{M}$ be the $n^2 \times n^2$ matrix, with entries in R, representing the homomorphism ϕ. By Proposition 10.2.14, the homomorphism $A(\mathfrak{p}) \otimes_{k(\mathfrak{p})} A(\mathfrak{p})^{\mathrm{opp}} \to \mathrm{End}_{k(\mathfrak{p})} A(\mathfrak{p})$ is an isomorphism; by diagram (11.1), this homomorphism is just the base change of ϕ to $k(\mathfrak{p})$ and so is represented by a matrix obtained by simply applying q to all the entries of $\mathbf{M}$. It follows that $q(\det \mathbf{M})$ is non-zero and therefore that $\det \mathbf{M}$ does not lie in $\mathfrak{p}$. Set $f = \det \mathbf{M}$ and let S be $R[f^{-1}]$; then $\mathbf{M}$ has an inverse over the ring S, and so (again by diagram (11.1)) the map

$$A_S \otimes_S (A_S)^{\mathrm{opp}} \to \mathrm{End}_S A_S$$

is an isomorphism. Also, A_S is free of non-zero rank and hence faithful over S, meaning that A_S is an Azumaya algebra over S. □

Example 11.3.7. In Example 11.3.4 we saw that the Hamilton algebra $(-1,-1)_{\mathbf{Z}}$ is not an Azumaya algebra over $\mathbf{Z}$. However, it is true that $(-1,-1)_{\mathbf{Z}} \otimes \mathbf{Z}/p\mathbf{Z}$ is a central simple algebra over $\mathbf{F}_p$ for any odd prime p, and also that $(-1,-1)_{\mathbf{Z}} \otimes \mathbf{Q}$ is a central simple algebra over $\mathbf{Q}$. It follows that Propos-

ition 11.3.6 applies with $\mathfrak{p} = (p)$ for p odd, and also for $\mathfrak{p} = (0)$. In fact $(-1,-1)_{\mathbf{Z}} \otimes \mathbf{Z}[\frac{1}{2}]$ is an Azumaya algebra over $\mathbf{Z}[\frac{1}{2}]$.

Exercise 11.3.8. Taking $A = (-1,-1)_{\mathbf{Z}}$ as in the previous example, write down the 4×4 integer matrix representing the $\mathbf{Z}$-linear transformation $x \mapsto axa'$ on A for a, a' each taking the values $1, i, j, ij$. Put the entries of these 16 matrices as columns in a 16×16 matrix, which represents the linear transformation

$$A \otimes_{\mathbf{Z}} A^{\mathrm{opp}} \to \mathrm{End} A, \quad (a \otimes a') \mapsto (x \mapsto axa').$$

Verify that this 16×16 matrix has determinant 2^{16}.

Corollary 11.3.9. *Let R be an integral domain and let $\mathfrak{p}$ be a prime ideal in R. Let A' be an Azumaya algebra over the local ring $R_{\mathfrak{p}}$. Then there exist $f \in R \smallsetminus \mathfrak{p}$ and an Azumaya algebra A over $R[f^{-1}]$ satisfying $A \otimes_{R[f^{-1}]} R_{\mathfrak{p}} \cong A'$.*

Proof Because $R_{\mathfrak{p}}$ is local, A' is a free module over $R_{\mathfrak{p}}$. Let $x_1, \ldots, x_n$ be a basis for A', and define the corresponding *structure constants* $c_{\alpha\beta}^{\gamma} \in R_{\mathfrak{p}}$ by the formula $x_\alpha x_\beta = \sum_\gamma c_{\alpha\beta}^{\gamma} x_\gamma$. Take $g \in R \smallsetminus \mathfrak{p}$ to be such that $g c_{\alpha\beta}^{\gamma} \in R$ for all i, j, k; then all the $c_{\alpha\beta}^{\gamma}$ lie in the subring $R[g^{-1}] \subset R_{\mathfrak{p}}$. It follows that the $R[g^{-1}]$-submodule $B \subset A'$ generated by $x_1, \ldots, x_n$ is closed under multiplication, so it is an $R[g^{-1}]$-subalgebra of A'. Since $R[g^{-1}]$ injects into $R_{\mathfrak{p}}$, we see that $x_1, \ldots, x_n$ are linearly independent over $R[g^{-1}]$ and therefore B is free. By construction, B satisfies the hypotheses of Proposition 11.3.6. We obtain $h \in R[g^{-1}] \smallsetminus \mathfrak{p}[g^{-1}]$ such that $A = B \otimes_R R[g^{-1}][h^{-1}]$ is an Azumaya algebra over $R[g^{-1}][h^{-1}]$. Writing $h = h' g^{-r}$ with $h \in R$ and setting $f = gh'$, we have $R[g^{-1}][h^{-1}] = R[f^{-1}]$, and A is an $R[f^{-1}]$-algebra with the desired properties. □

155: Can we do this without the integral domain hypothesis?

The special case of Corollary 11.3.9 in which $\mathfrak{p}$ is the zero ideal is worth stating in its own right.

Corollary 11.3.10. *Let R be an integral domain with field of fractions K. Suppose that A' is a central simple algebra over K. Then there exist non-zero $f \in R$ and an Azumaya algebra A over $R[f^{-1}]$ satisfying $A \otimes K \cong A'$.*

Next, we examine Azumaya algebras over a complete local ring, beginning with an example.

Example 11.3.11. In Example 10.2.6 we showed that the quaternion algebra $A = (-1,3)_{\mathbf{F}_7}$ is isomorphic to a matrix algebra. Using Hensel's Lemma (Theorem 2.1.3) we now show that the Hamilton algebra $A' = (-1,3)_{\mathbf{Z}_7}$ is isomorphic to the matrix algebra $\mathrm{M}_2(\mathbf{Z}_7)$. Firstly, note that $A' \otimes_{\mathbf{Z}_7} \mathbf{F}_7$ and A are isomorphic (and in particular A' is an Azumaya algebra). Next, we find

matrices $I', J' \in \mathrm{M}_2(\mathbf{Z}_7)$ satisfying $(I')^2 = -\mathrm{Id}$, $(J')^2 = 3\mathrm{Id}$ and $I'J' + J'I' = 0$, as follows. Exactly as before, we set

$$I' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and try to solve for a, b, c, d. Again, the equation $I'J' + J'I' = 0$ translates to $a + d = 0$, $b = c$, and the equation $(J')^2 = 3\mathrm{Id}$ then becomes equivalent to the equation $a^2 + b^2 = 3$. We know that $a = 1$ and $b = 3$ is a solution modulo 7, and we can therefore set $a = 1$ and use Hensel's Lemma to solve the equation $1 + b^2 = 3$ in $\mathbf{Z}_7$, thereby finding J'. Hence, the matrices I', J' determine a homomorphism $\rho' \colon A' \to \mathrm{M}_2(\mathbf{Z}_7)$ of algebras over $\mathbf{Z}_7$, as in Example 10.2.6. To show that ρ' is an isomorphism, observe that it is a homomorphism of free $\mathbf{Z}_7$-modules that is an isomorphism modulo 7. Thus, ρ' is a $\mathbf{Z}_7$-linear map with invertible determinant, and therefore is an isomorphism.

The example we just discussed is a manifestation of a general fact: that the Brauer group of a complete local ring injects into the Brauer group of its residue field, which can be proved by an extension of the argument we just gave. The following proposition states that the map of Brauer groups is actually an isomorphism.

Proposition 11.3.12. *Let R be a complete, commutative local ring, with maximal ideal $\mathfrak{m}$. The natural map $\mathrm{Br}\, R \to \mathrm{Br}(R/\mathfrak{m})$ is an isomorphism.*

Proof See Auslander and Goldman (1960, Theorem 6.5). □

Corollary 11.3.13. *Let p be a prime, let k be a finite extension of $\mathbf{Q}_p$, and let R be the ring of integers in k. Then $\mathrm{Br}\, R$ is trivial.*

Proof The residue field of R is finite, and thus has trivial Brauer group by Corollary 10.4.10. □

Exercise 11.3.14. Show that the Brauer group of a finite ring is trivial. (Hint: Reduce to the local case and observe that a finite local ring is complete.) 156: also commutative?

We now state an important theorem, due to Auslander and Goldman, comparing the Brauer group of a regular integral domain to the Brauer group of its field of fractions. This result will be essential to our definition of the Brauer group of a variety in the next chapter.

Theorem 11.3.15. *If R is a regular integral domain with field of fractions K, then the natural homomorphism $\mathrm{Br}\, R \to \mathrm{Br}\, K$ is injective.*

Proof See Auslander and Goldman (1960, Theorem 7.2). □

When R is a regular integral domain, we will often think of the Brauer group of R as being a subgroup of the Brauer group of its fraction field.

Example 11.3.16. Auslander and Goldman also give an example showing that the assumption of regularity cannot be removed from Theorem 11.3.15. Indeed, set $R = \mathbf{R}[x,y]/(x^2+y^2)$ and let A be the Hamilton algebra $(-1,-1)_R$. Since $\mathbb{H}_{\mathbf{R}} = (-1,-1)_{\mathbf{R}}$ is an Azumaya algebra over $\mathbf{R}$ and A is isomorphic to $\mathbb{H}_{\mathbf{R}} \otimes R$, it follows that A is an Azumaya algebra over R. Denote by $\mathfrak{m}$ the maximal ideal (x,y) of R. The algebra $A \otimes R/\mathfrak{m}$ is isomorphic to $\mathbb{H}_{\mathbf{R}}$ and therefore represents the non-trivial element of $\mathrm{Br}(R/\mathfrak{m})$. We deduce that A represents a non-trivial element of $\mathrm{Br}\,R$. On the other hand, in the fraction field K of R the element x/y is a square root of -1 and therefore $A \otimes K$ is isomorphic to $\mathrm{M}_2(K)$. We conclude that the homomorphism $\mathrm{Br}\,R \to \mathrm{Br}\,K$ is not injective.

We finish with an algebraic statement which, while not essential to our treatment of the Brauer group, is closely related to the ideas of the following section. First, we prove a patching result for algebras and an extension result for projective modules.

157: Add reference

Lemma 11.3.17 (Patching)**.** *Let R be a ring, and let $f_1, f_2 \in R$ be two elements satisfying $R = Rf_1 + Rf_2$. Let A_1, A_2 be Azumaya algebras over R_{f_1} and R_{f_2} respectively, and suppose that $\phi\colon (A_2)_{f_1} \to (A_1)_{f_2}$ is an isomorphism of $R_{f_1 f_2}$-algebras. Then there exists an Azumaya algebra A over R such that A_{f_1} is isomorphic to A_1, and A_{f_2} is isomorphic to A_2.*

158: R commutative, I imagine?

Proof Consider both A_1 and A_2 as R-modules. The map $\psi\colon A_1 \times A_2 \to (A_1)_{f_2}$ given by $\psi(a_1,a_2) = a_1 - \phi(a_2)$ is an R-module homomorphism; define A to be its kernel. Thus A is the subset of $A_1 \times A_2$ consisting of pairs (a_1,a_2) satisfying $a_1 = \phi(a_2)$. Define multiplication on $A_1 \times A_2$ componentwise; the fact that ϕ is an isomorphism of algebras shows that A is closed under multiplication and so is an R-algebra. It is straightforward to check that A_{f_1} is isomorphic to A_1, and therefore $A_{\mathfrak{p}}$ is isomorphic to $(A_1)_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p}$ of R not containing f_1; similarly, $A_{\mathfrak{p}}$ is isomorphic to $(A_2)_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p}$ not containing f_2. By hypothesis, no prime ideal contains both f_1 and f_2. Since A_1 and A_2 are both Azumaya algebras, we deduce by Proposition 11.2.3 that A is an Azumaya algebra over R. □

159: Also need that 1 is in there, but it is.

Notice that, in the special case where A_1 and A_2 are submodules of the same algebra over R_{fg} and ϕ is the identity, we are just defining A to be the intersection of A_1 and A_2.

Exercise 11.3.18. Prove the following general patching statement. Let $f_1, \ldots, f_n$

be elements of R that generate R as an ideal, let $A_1,\dots,A_n$ be Azumaya algebras over $R_{f_1},\dots,R_{f_n}$ respectively, and suppose that there are isomorphisms $\phi_{ij}\colon (A_i)_{f_j} \to (A_j)_{f_i}$ for all i,j satisfying $\phi_{jk}\circ\phi_{ij} = \phi_{ik}$ (over $R_{f_if_jf_k}$) for all i,j,k. Then there is an Azumaya algebra A over R such that A_{f_i} is isomorphic to A_i for all i.

Lemma 11.3.19. *Let R be a regular integral Noetherian domain of Krull dimension d. Let S be a multiplicative subset of R and let M be a finitely generated projective $S^{-1}R$-module. If the rank of M is greater than d, then there is a finitely generated projective R-module $\tilde{M}$ such that $S^{-1}\tilde{M}$ and M are isomorphic.*

Proof Let $x_1,\dots,x_n$ be generators for M as an $S^{-1}R$-module and let N be the R-submodule of M spanned by $x_1,\dots,x_n$. By construction, N is finitely generated and $S^{-1}N$ is isomorphic to M; however, N is not necessarily projective. Since R is regular of finite Krull dimension, it follows by Auslander and Buchsbaum (1957, Corollary 4.8) that N admits a finite resolution

$$0 \to P_r \to \cdots \to P_0 \to N \to 0$$

by projective R-modules $P_0,\dots,P_r$. Moreover, since R is Noetherian, we may assume that $P_0,\dots,P_r$ are finitely generated: see Bass (1968, after Proposition 6.3). Localising the previous sequence at S we obtain a projective resolution of M which is therefore split and we deduce the isomorphism

$$M \oplus \bigoplus_{i \text{ odd}} S^{-1}P_i \cong \bigoplus_{i \text{ even}} S^{-1}P_i. \tag{11.2}$$

Since the R-modules $P_0,\dots,P_r$ are projective and finitely generated, if follows that there is a finitely generated projective R-module Q such that $Q \oplus \bigoplus_{i \text{ odd}} P_i$ is free; let q be its rank. Adding $S^{-1}Q$ to both sides of the isomorphism in (11.2) we find

$$M \oplus (S^{-1}R)^q \cong S^{-1}P',$$

where $P' \cong Q \oplus \bigoplus_{i \text{ even}} P_i$ is finitely generated and projective of rank greater than $d+q$. Using item (a) in Weibel (2013, Bass–Serre Cancellation Theorem I.2.3) we deduce that there is a projective R-module $\tilde{M}$ and an isomorphism $P' \cong \tilde{M} \oplus R^q$. Since the dimension of $S^{-1}R$ is at most the dimension of R, we can apply item (b) in the Bass–Serre Theorem to conclude that the $S^{-1}R$-modules M and $S^{-1}\tilde{M}$ are isomorphic and the proof is complete. □

Proposition 11.3.20. *Let R be a regular integral Noetherian domain of finite*

Krull dimension, with field of fractions K. Then there is an equality

$$\operatorname{Br} R = \bigcap_{\mathfrak{m}} \operatorname{Br} R_{\mathfrak{m}}$$

where the intersection is over all maximal ideals $\mathfrak{m}$ in R, and all Brauer groups are considered as subgroups of $\operatorname{Br} K$.

Proof We give a proof following Hoobler (1980).

Let α be a class in $\operatorname{Br} K$ lying in $\operatorname{Br} R_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R; we must show that α lies in $\operatorname{Br} R$. Define a set $S = \{f \in R \mid \alpha \in \operatorname{Br} R_f\}$. Corollary 11.3.9 shows that, for any maximal ideal $\mathfrak{m}$, there is an element f of $R \setminus \mathfrak{m}$ contained in S; thus S is not contained in any maximal ideal of R. The plan is to show that S is an ideal; then it will follow that S contains 1_R, and therefore that α lies in $\operatorname{Br} R$.

We first show that S is closed under multiplication by elements of R. If f is in S, and g is any element of R, then the inclusion $R_f \to K$ factors through R_{fg}, and so we have inclusions $\operatorname{Br} R_f \subseteq \operatorname{Br} R_{fg} \subset \operatorname{Br} K$ and fg lies in S.

Now let f and g be two elements of S; we must show that $f+g$ also lies in S. We reduce to the case in which $f+g$ is invertible by replacing R by R_{f+g}. By the definition of S, there are Azumaya algebras A_f over R_f and A_g over R_g, such that $A_f \otimes K$ and $A_g \otimes K$ both have class α in $\operatorname{Br} K$. Because $\operatorname{Br} R_{fg} \to \operatorname{Br} K$ is injective, it follows that $(A_f)_g$ and $(A_g)_f$ have the same class in $\operatorname{Br} R_{fg}$. Therefore there are finitely generated, projective modules P, Q over R_{fg}, of non-zero rank, and an isomorphism $(A_f)_g \otimes_{R_{fg}} \operatorname{End} P \cong (A_g)_f \otimes_{R_{fg}} \operatorname{End} Q$. Let V be a free R_{fg}-module of sufficiently large rank. From Lemma 11.3.19 we obtain a finitely generated, projective R_f-module $\tilde{P}$ and a finitely generated, projective R_g-module $\tilde{Q}$ such that $\tilde{P} \otimes_{R_f} R_{fg}$ and $P \otimes_{R_{fg}} V$ are isomorphic, and $\tilde{Q} \otimes_{R_g} R_{fg}$ and $Q \otimes_{R_{fg}} V$ are isomorphic. Thus we have an isomorphism

$$(A_f \otimes_{R_f} \operatorname{End} \tilde{P})_g \cong (A_g \otimes_{R_g} \operatorname{End} \tilde{Q})_f$$

of R_{fg}-algebras. To conclude, we apply Lemma 11.3.17 to the algebras $A_f \otimes_{R_f} \operatorname{End} \tilde{P}$ and $A_g \otimes_{R_g} \operatorname{End} \tilde{Q}$ obtaining an Azumaya algebra A over R whose class in $\operatorname{Br} K$ is α. □

12

The Brauer group of a variety

In this chapter we define and study the Brauer group of a smooth, geometrically irreducible variety. Following the motivation of Section 10.5, the Brauer group of a variety X will be the subgroup of $\mathrm{Br}\,\kappa(X)$ consisting of those elements that can be evaluated at all points of X.

Defining the Brauer group is straightforward, but computing the Brauer groups of specific varieties is a very different matter. Even the question of whether the Brauer group is finite is open for many classes of varieties. In this chapter we will give some results describing the Brauer groups of curves, affine and projective spaces. Later, in Chapter 15, we will see how to use Galois cohomology to compute the Brauer groups of other varieties, such as rational varieties.

12.1 Definition of the Brauer group

Let k be a field and $\bar{k}$ an algebraic closure of k. Recall that for a variety X over k and a point x in $X(\bar{k})$, we denote by $\mathscr{O}_{X,x}$ the local ring of X at x. If X is irreducible and x is a smooth point, then the ring $\mathscr{O}_{X,x}$ is a regular integral domain, so that by Theorem 11.3.15 the group $\mathrm{Br}\,\mathscr{O}_{X,x}$ can be viewed as a subgroup of $\mathrm{Br}\,\kappa(X)$. Elements of $\mathrm{Br}\,\kappa(X)$ lying in the image of $\mathrm{Br}\,\mathscr{O}_{X,x}$ are said to be *unramified* at x, and elements of $\mathrm{Br}\,\kappa(X)$ lying outside the image of $\mathrm{Br}\,\mathscr{O}_{X,x}$ are said to be *ramified* at x.

d: Martin and I think that this definition works equally well with separable closure.

160: Are points called x or P?

Definition 12.1.1. Let X be a smooth irreducible variety over k. The *Brauer group* $\mathrm{Br}\,X$ of X is the subgroup of $\mathrm{Br}\,\kappa(X)$ consisting of those elements that are unramified at all points of X, that is,

$$\mathrm{Br}\,X = \bigcap_{x\in X(\bar{k})} \mathrm{Br}\,\mathscr{O}_{X,x},$$

where the intersection is taken in the group $\mathrm{Br}\,\kappa(X)$.

Example 12.1.2. Let X be the non-singular del Pezzo surface of degree 4 of Example 2.3.5 defined by the equations

$$\begin{cases} uv = x^2 - 5y^2 \\ (u+v)(u+2v) = x^2 - 5z^2 \end{cases}$$

and let $\mathscr{A}$ be the quaternion algebra

$$\mathscr{A} = \left(5, \frac{u}{u+v}\right)$$

over $\kappa(X)$. We claim that the class of $\mathscr{A}$ in $\mathrm{Br}\,\kappa(X)$ lies in $\mathrm{Br}\,X$. To see this, first let P be a point of X where neither u nor $u+v$ vanishes. Then the Hamilton algebra over the local ring $\mathscr{O}_{X,P}$ defined by

$$\mathscr{A}_P = \left(5, \frac{u}{u+v}\right)_{\mathscr{O}_{X,P}}$$

is an Azumaya algebra, because its reduction modulo the maximal ideal of $\mathscr{O}_{X,P}$ is the central simple algebra $(5, u(P)/(u(P)+v(P)))_{k_P}$, where k_P is the residue field at P. Moreover, we have $\mathscr{A}_P \otimes_{\mathscr{O}_{X,P}} \kappa(X) = \mathscr{A}$, and so the class of $\mathscr{A}$ in $\mathrm{Br}\,\kappa(X)$ lies in the image of $\mathrm{Br}\,\mathscr{O}_{X,P}$.

To repeat the argument for points where either u or $u+v$ vanishes, we do some arithmetic in the function field $\kappa(X)$. Dividing both sides of the equation $uv = x^2 - 5y^2$ by v^2, we see that

$$\frac{u}{v} = \frac{x^2 - 5y^2}{v^2} = N_{\kappa(X)(\sqrt{5})/\kappa(X)}\left(\frac{x+\sqrt{5}y}{v}\right)$$

is a norm from $\kappa(X)(\sqrt{5})$, and so by Exercise 10.2.5(iv) the quaternion algebra $(5, v/(u+v))_{\kappa(X)}$ is isomorphic to $\mathscr{A}$. In a similar way, we get the following four quaternion algebras over $\kappa(X)$, all isomorphic:

$$\mathscr{A} = \left(5, \frac{u}{u+v}\right), \quad \left(5, \frac{v}{u+v}\right), \quad \left(5, \frac{u}{u+2v}\right), \quad \left(5, \frac{v}{u+2v}\right). \tag{12.1}$$

Repeating the argument above with these isomorphic algebras shows that the class of $\mathscr{A}$ in $\mathrm{Br}\,\kappa(X)$ lies in the image of $\mathrm{Br}\,\mathscr{O}_{X,P}$ for all points P of X, except possibly when $u(P)$ and $v(P)$ both vanish. That leaves only the four points $[0,0,\sqrt{5},\pm 1,\pm 1]$ where the class of $\mathscr{A}$ might be ramified.

To show that $\mathscr{A}$ is indeed unramified at these final four points, we produce yet another quaternion algebra isomorphic to $\mathscr{A}$. Let $f \in \kappa(X)$ and

$g \in \kappa(X)(\sqrt{5})$ be the functions

$$f = \frac{u}{u+v}, \qquad g = \frac{u+v+x-\sqrt{5}z}{u+x-\sqrt{5}y}.$$

Then we have

$$\begin{aligned} fN(g) &= \frac{u((u+v+x)^2-5z^2)}{(u+v)((u+x)^2-5y^2)} \\ &= \frac{u((u+v)^2+2x(u+v)+x^2-5z^2)}{(u+v)(u^2+2ux+x^2-5y^2)} \\ &= \frac{u((u+v)^2+2x(u+v)+(u+v)(u+2v))}{(u+v)(u^2+2ux+uv)} \\ &= \frac{2u+3v+2x}{u+v+2x}. \end{aligned}$$

Therefore $\mathscr{A}$ is isomorphic to the quaternion algebra

$$\left(5, \frac{2u+3v+2x}{u+v+2x}\right)_{\kappa(X)}$$

which by the argument above is unramified at the remaining four points of X.

The procedure followed in the example above may seem rather *ad hoc*. In Proposition 15.3.3, we shall see a general criterion for deciding when a cyclic algebra over the function field of a variety lies in the Brauer group of the variety. The calculation above may be viewed as an explicit form of the proof of that proposition.

Remark 12.1.3. To show that the class of an algebra $\mathscr{A} \in \mathrm{Br}\,\kappa(X)$ lies in $\mathrm{Br}X$, we need to find, for each point $x \in X$, an Azumaya algebra A_x over $\mathscr{O}_{X,x}$ such that $A_x \otimes_{\mathscr{O}_{X,x}} \kappa(X)$ is Brauer-equivalent to $\mathscr{A}$. In Example 12.1.2, we were able to do rather more than this: starting with a central simple algebra $\mathscr{A}$ over $\kappa(X)$, we found, for each $x \in X$, an $\mathscr{O}_{X,x}$-subalgebra A_x of $\mathscr{A}$ such that $A_x \otimes_{O_{X,x}} \kappa(X)$ was isomorphic to $\mathscr{A}$. In Auslander and Goldman (1960, proof of Proposition 7.4), the authors showed that this is always possible when X is smooth and of dimension at most two; the proof relies on the fact that, over a two-dimensional regular local ring, a maximal order in a central simple algebra is always projective. Auslander and Goldman comment that "It is not known at the present time whether the restriction on the dimension of R is actually necessary." More recently, Antieau and Williams (2014) have settled this question by showing that there is a smooth affine variety X over the complex numbers of dimension 6 and a division algebra in $\mathrm{Br}X$ admitting no maximal orders which are Azumaya algebras.

Remark 12.1.4. If X is a smooth irreducible *affine* variety over k with coordinate ring R, then the groups $\mathrm{Br}X$ and $\mathrm{Br}R$ coincide. Indeed, it is clear from the definition that the image of $\mathrm{Br}R$ in $\mathrm{Br}\,\kappa(X)$ lies in $\mathrm{Br}X$. To see that this inclusion is an equality, it suffices to apply Proposition 11.3.20. This is one reason that we assumed X to be smooth in Definition 12.1.1. In general, if X is not smooth, then the natural maps $\mathrm{Br}\,\mathscr{O}_{X,x} \to \mathrm{Br}\,\kappa(X)$ need not be injective (as seen in Example 11.3.16).

Let X be a smooth irreducible variety. If U is a non-empty open subvariety of X, then the function fields $\kappa(U)$ and $\kappa(X)$ can be identified, and so there is a natural inclusion $\mathrm{Br}X \subseteq \mathrm{Br}U$. If $\mathscr{U}$ is an open cover of X, then the equality

$$\mathrm{Br}X = \bigcap_{U\in\mathscr{U}} \mathrm{Br}U$$

follows immediately from Definition 12.1.1. If each $U \in \mathscr{U}$ is affine with coordinate ring R_U, then by Remark 12.1.4 we have

$$\mathrm{Br}X = \bigcap_{U\in\mathscr{U}} \mathrm{Br}R_U,$$

where, as before, the intersection takes place in $\mathrm{Br}\,\kappa(X)$.

We now define what it means to evaluate a Brauer class in $\mathrm{Br}X$ at a point of X. Let ℓ be a field containing k and let x be a point in $X(\ell)$. Then $\mathrm{Br}X$ is contained in the image of the natural injection $\mathrm{Br}\,\mathscr{O}_{X,x} \to \mathrm{Br}\,\kappa(X)$: if ℓ is a subfield of $\bar{k}$ then this follows immediately from the definition of $\mathrm{Br}X$, and otherwise by **??**. Evaluation at the point x defines a ring homomorphism $\mathscr{O}_{X,x} \to \ell$, inducing a group homomorphism $\mathrm{ev}_x\colon \mathrm{Br}\,\mathscr{O}_{X,x} \to \mathrm{Br}\,\ell$, which in turn restricts to a homomorphism

161: Need to describe local rings properly. Check how this fits with base change for Brauer groups.

$$\mathrm{ev}_x\colon \mathrm{Br}X \to \mathrm{Br}\,\ell.$$

If A is a class in $\mathrm{Br}X$ we sometimes denote $\mathrm{ev}_x(A)$ by $A(x)$. By Remark **??**, the evaluation map ev_x factors through $\mathrm{Br}\,\mathscr{O}_{X_\ell,x}$.

Example 12.1.5. In Example 12.1.2, we looked at the quaternion algebra $\mathscr{A} = (5, u/(u+v))$ on the variety X of Example 2.3.5. At any point P of $X(\ell)$ where neither u nor $u+v$ vanish, we saw that the algebra $(5, u/u+v)$ over $\mathscr{O}_{X,P}$ is an Azumaya algebra; evaluating at P gives the central simple algebra $(5, u(P)/(u(P)+v(P)))_\ell$.

The example above illustrates a general principle: given an explicit description of a central simple algebra $\mathscr{A}$ over $\kappa(X)$, and a point x of X, we can try to find $\mathscr{A}(x)$ by evaluating everything in sight at x; if we obtain a central simple

algebra, then it is $\mathscr{A}(x)$. Let formulate this principle into a precise lemma. Notice first that, for any finitely generated free module A with basis $\{e_1,\dots,e_n\}$ over a ring R, putting the structure of an R-algebra on A is the same as specifying the n^3 *structure constants* $c_{\alpha\beta}^{\gamma} \in R$ defined by $e_\alpha e_\beta = \sum_\gamma c_{\alpha\beta}^{\gamma} e_\gamma$.

Lemma 12.1.6. *Let X be a smooth variety over a field k, and let $\mathscr{A}$ be a central simple algebra over $\kappa(X)$. Fix a basis $\{e_1,\dots,e_n\}$ for $\mathscr{A}$ over $\kappa(X)$, and let $c_{\alpha\beta}^{\gamma} \in \kappa(X)$ be the corresponding structure constants. Let ℓ be an extension of k, and let $x \in X(\ell)$ be a point. Suppose that each $c_{\alpha\beta}^{\gamma}$ lies in $\mathscr{O}_{X,x}$. Let the ℓ-algebra B be the vector space ℓ^n endowed with the multiplicative structure defined by the structure constants $c_{\alpha\beta}^{\gamma}(x)$. If B is a central simple algebra, then the class of $\mathscr{A}$ in $\mathrm{Br}X$ is unramified at x, and $\mathscr{A}(x)$ is isomorphic to B.*

Proof Let A_x be the $\mathscr{O}_{X,x}$-submodule of $\mathscr{A}$ spanned by $\{e_1,\dots,e_n\}$. Since the e_i are linearly independent over $\kappa(X)$, they are also linearly independent over $\mathscr{O}_{X,x}$, so form a basis for A_x. The fact that all the $c_{\alpha\beta}^{\gamma}$ lie in $\mathscr{O}_{X,x}$ means that A_x is closed under multiplication and therefore is an $\mathscr{O}_{X,x}$-algebra. Let $\mathfrak{m}_x$ be the maximal ideal of $\mathscr{O}_{X,x}$; the evaluation map at x defines an isomorphism $\mathscr{O}_{X,x}/\mathfrak{m}_x \to \ell$. It follows easily from the definition of tensor product that there is an isomorphism $A_x \otimes_{\mathscr{O}_{X,x}} \ell \cong B$. If B is a central simple algebra, then Proposition 11.2.3 shows that A_x is an Azumaya algebra over $\mathscr{O}_{X,x}$. By construction, $A_x \otimes_{\mathscr{O}_{X,x}} \kappa(X)$ is isomorphic to $\mathscr{A}$, showing that the class of $\mathscr{A}$ is unramified at x, and $\mathscr{A}(x)$ is isomorphic to B by definition. □

Example 12.1.7. Let X be a smooth variety over a field of characteristic zero. Let $\mathscr{A}$ be the quaternion algebra (f,g) over $\kappa(X)$, defined by two non-zero functions $f,g \in \kappa(X)$. Taking the standard basis $\{1,i,j,ij\}$ for $\mathscr{A}$ gives 64 structure constants which are all either 0, ± 1, $\pm f$, $\pm g$ or $\pm fg$. For any point $x \in X(\ell)$ where both f and g are defined and non-zero, $\mathscr{A}$ is unramified at x and $\mathscr{A}(x)$ is the quaternion algebra $(f(x),g(x))$ over ℓ.

Proposition 12.1.8. *Let X be a smooth, geometrically irreducible variety over a field k, and let K/k be a field extension. Let $f\colon \mathrm{Br}\,\kappa(X) \to \mathrm{Br}\,\kappa(X_K)$ be the natural map. If a class $\alpha \in \mathrm{Br}\,\kappa(X)$ lies in $\mathrm{Br}X$, then its image $f(\alpha)$ lies in $\mathrm{Br}X_K$; thus f induces a homomorphism $\mathrm{Br}X \to \mathrm{Br}X_K$.*

Proof Given a point $x \in X_K(\bar{K})$ of X_K, let $Z \subseteq X_K$ be the closure of x in the k-Zariski topology on X_K. Since Z is non-empty, the Nullstellensatz shows that Z contains a point $y \in X(\bar{k})$. Under the inclusion $\kappa(X) \to \kappa(X_K)$, the image of

the local ring $\mathscr{O}_{X,y}$ is contained in $\mathscr{O}_{X_K,x}$; so we have a commutative diagram

$$\begin{array}{ccc} \operatorname{Br}\mathscr{O}_{X,y} & \longrightarrow & \operatorname{Br}\mathscr{O}_{X_K,x} \\ \downarrow & & \downarrow \\ \operatorname{Br}\kappa(X) & \xrightarrow{f} & \operatorname{Br}\kappa(X_K) \end{array}$$

If now α is a class of $\operatorname{Br}X$, then α lies in the image of $\operatorname{Br}\mathscr{O}_{X,y}$ and therefore $f(\alpha)$ lies in the image of $\operatorname{Br}\mathscr{O}_{X_K,x}$. This is true for all points x of X_K, so α lies in $\operatorname{Br}X_K$. □

162: Make sure this relates to what we say about local rings and base change.

We will now define some subgroups of the Brauer group of a variety which relate in different ways to the base field k.

Definition 12.1.9. Let X be a smooth, geometrically irreducible variety over a field k.

(i) The image of the natural map $\operatorname{Br}k \to \operatorname{Br}\kappa(X)$ lies in $\operatorname{Br}X$, and is denoted $\operatorname{Br}_0 X$. Classes in $\operatorname{Br}_0 X$ are called *constant* classes.
(ii) The kernel of the natural map $\operatorname{Br}X \to \operatorname{Br}X^{\mathrm{sep}}$ is denoted $\operatorname{Br}_1 X$. Classes in $\operatorname{Br}_1 X$ are called *algebraic* classes.
(iii) Classes in $\operatorname{Br}X$ which are not algebraic are called *transcendental* classes.

Of course, every element of $\operatorname{Br}\kappa(X)$ is split by some finite extension of $\kappa(X)$. An element is algebraic if it is split by an extension of $\kappa(X)$ induced by a separable extension of the base field k. Note that every constant class is algebraic, because every element of $\operatorname{Br}k$ is split by a finite separable extension of k. We have inclusions $\operatorname{Br}_0 X \subset \operatorname{Br}_1 X \subset \operatorname{Br}X$.

Example 12.1.10. The class of the algebra of Example 12.1.2 is algebraic, because that algebra splits if the base field is extended to $\mathbf{Q}(\sqrt{5})$.

Example 12.1.11. Let p be a prime and let k be the field $\mathbf{F}_p(t)$. We construct a class α in $\operatorname{Br}\mathbf{A}^1_k$ with the following properties:

- α is split by an inseparable extension of k;
- α is split by a separable extension of $\kappa(\mathbf{A}^1_k)$;
- α is not split by any separable extension of k.

Therefore, α does not lie in $\operatorname{Br}_1\mathbf{A}^1_k$.

Following Auslander and Goldman (1960, proof of Theorem 7.5), we define an algebra A over $\kappa(\mathbf{A}^1_k) = k(T)$ of dimension p^2 generated as a $k(T)$-algebra by two elements i, j satisfying the relations

$$i^p - i = T, \qquad j^p = t, \qquad ji = (i+1)j.$$

In other words, A is the cyclic algebra $(k(T)(i)/k(T),\sigma,t)$ (see Definition 10.2.8), where $k(T)(i)$ is the Artin–Schreier extension defined by $i^p - i = T$ and σ is the automorphism of $k(T)(i)/k(T)$ satisfying $\sigma(i) = i+1$. Then A is split by the inseparable extension $k(T)(j)/k(T)$ induced by $k\left(t^{\frac{1}{p}}\right)/k$, and it is split by the separable extension $k(T)(i)/k(T)$. The class α of A in $\mathrm{Br}\,k(T)$ is non-trivial, since an easy calculation shows that t is not a norm for the extension $k(T)(i)/k(T)$. The class of the algebra A lies in $\mathrm{Br}\,\mathbf{A}^1_k$ by Lemma 12.1.6, and it evaluates to the trivial class at the point $T = 0$, showing that the class of A is not in $\mathrm{Br}_0\,\mathbf{A}^1_k$. However, Auslander and Goldman show that $\mathrm{Br}_1\,\mathbf{A}^1_k$ is equal to $\mathrm{Br}_0\,\mathbf{A}^1_k$ and hence the class of A is not algebraic, that is, A is not split by any separable extension of k.

Exercise 12.1.12. Let X be a smooth, geometrically irreducible variety over a field k.

(i) Suppose that X has a k-point x. Show that the composition

$$\mathrm{Br}\,k \to \mathrm{Br}\,X \xrightarrow{\mathrm{ev}_x} \mathrm{Br}\,k$$

is the identity map. Deduce that, whenever $X(k)$ is non-empty, the natural map $\mathrm{Br}\,k \to \mathrm{Br}\,X$ is injective.

(ii) In the case in which k is a number field, draw the same conclusion under the assumption that X has points everywhere locally.

12.2 Properties of the Brauer group

We have said what it means for a Brauer class to be unramified at a point. Let us extend the definition and say what it means for a Brauer class to be unramified at any subvariety.

Definition 12.2.1. Let X be a smooth, geometrically irreducible variety over a field k, and let Z be a subvariety of X. A class $\alpha \in \mathrm{Br}\,\kappa(X)$ is *unramified* at Z if α lies in the image of the natural map $\mathrm{Br}\,\mathscr{O}_{X,Z} \to \mathrm{Br}\,\kappa(X)$.

Remark 12.2.2. (i) If Z is a point of X, then this definition agrees with our previous one.

163: Check our definitions of local ring for a point and for a subvariety work together.

(ii) Because X is smooth, the local ring $\mathscr{O}_{X,Z}$ is regular. By Theorem 11.3.15, the map $\mathrm{Br}\,\mathscr{O}_{X,Z} \to \mathrm{Br}\,\kappa(X)$ is injective.

(iii) Suppose that $Z \subset Y \subset X$ are subvarieties. Then we have an inclusion $\mathscr{O}_{X,Z} \subset \mathscr{O}_{X,Y}$ and therefore an inclusion $\mathrm{Br}\,\mathscr{O}_{X,Z} \subset \mathrm{Br}\,\mathscr{O}_{X,Y}$. In particular,

if a class is unramified at Z then it is unramified at Y. Since every subvariety contains a point of X, it follows that a class in $\mathrm{Br}X$ is unramified at all subvarieties.

We will now look at the behaviour of Brauer groups under morphisms of varieties.

Proposition 12.2.3. *Let $f: X \to Y$ be a morphism of smooth, geometrically irreducible varieties over a field k. Then there is an induced morphism $f^*: \mathrm{Br}Y \to \mathrm{Br}X$, making* Br *into a contravariant functor from the category of such varieties to the category of Abelian groups.*

Proof We follow Colliot-Thélène (1995). Let Z be the closure of the image of f, and let α be an element of $\mathrm{Br}Y$. Then α lies in $\mathrm{Br}\,\mathscr{O}_{Y,Z} \subset \mathrm{Br}\,\kappa(X)$. The residue field of the local ring $\mathscr{O}_{Y,Z}$ is the function field $\kappa(Z)$. Now $f: X \to Z$ is dominant, so induces a map of function fields $\kappa(Z) \to \kappa(X)$. We define $f^*(\alpha)$ to be the image of α under the homomorphism $\mathrm{Br}\,\mathscr{O}_{Y,Z} \to \mathrm{Br}\,\kappa(X)$ induced by the composite ring homomorphism $\mathscr{O}_{Y,Z} \to \kappa(Z) \to \kappa(X)$.

Let us show that $f^*(\alpha)$ lies in $\mathrm{Br}X$. Given any point x of X, we have a commutative diagram of rings

$$\begin{array}{ccccc} \mathscr{O}_{Y,f(x)} & \longrightarrow & \mathscr{O}_{Z,f(x)} & \longrightarrow & \mathscr{O}_{X,x} \\ \downarrow & & \downarrow & & \downarrow \\ \mathscr{O}_{Y,Z} & \longrightarrow & \kappa(Z) & \longrightarrow & \kappa(X) \end{array}$$

where the vertical maps are inclusions, and the horizontal maps come from the morphisms $X \to Z \to Y$. There is therefore a corresponding diagram of Brauer groups, with the vertical maps still being inclusions. The class α lies in $\mathrm{Br}\,\mathscr{O}_{Y,Z}$; by assumption, α is unramified on Y and so lies in $\mathrm{Br}\,\mathscr{O}_{Y,f(x)}$. By commutativity of the diagram, the class $f^*(\alpha) \in \mathrm{Br}\,\kappa(X)$ lies in $\mathrm{Br}\,\mathscr{O}_{X,x}$. Since this holds for any point x of X, we deduce that $f^*(\alpha)$ lies in $\mathrm{Br}X$.

Verifying that this construction makes Br into a contravariant functor is an easy exercise. □

Remark 12.2.4. In the case that f is the inclusion of an open subvariety X into Y, this definition of f^* is simply the inclusion $\mathrm{Br}Y \to \mathrm{Br}X$ given by regarding both as subgroups of $\mathrm{Br}\,\kappa(Y)$.

Let us now study the set of points at which a given Brauer class is unramified. The algebraic result of Corollary 11.3.9 can be interpreted geometrically as follows.

Proposition 12.2.5. *Let X be a smooth, geometrically irreducible variety over a field k, and let Z be a subvariety of X. Let α be a class in* $\mathrm{Br}\,\kappa(X)$ *that*

is unramified at Z. Then there is a dense affine open subset U of X, having non-empty intersection with Z, such that α lies in $\mathrm{Br}\,U$.

Proof Firstly, replacing X by any dense affine subset meeting Z, we may assume that X is affine. Let R be the coordinate ring of X, so that $\kappa(X)$ is the field of fractions of R. Denote by $\mathfrak{p}$ the prime ideal of R consisting of functions vanishing identically on Z; the local ring $\mathscr{O}_{X,Z}$ is then the localisation $R_{\mathfrak{p}}$.

By hypothesis, the class α lies in the image of $\mathrm{Br}\,\mathscr{O}_{X,Z}$ in $\mathrm{Br}\,\kappa(X)$. Let A' be a central simple algebra over $\mathscr{O}_{X,Z}$ representing the class α. By Corollary 11.3.9, there is a regular function $f \in R$, not vanishing identically on Z, and an Azumaya algebra A over $R[f^{-1}]$, satisfying $A \otimes R_{\mathfrak{p}} \cong A'$. Thus the class α lies in the image of the map $\mathrm{Br}\,R[f^{-1}] \to \mathrm{Br}\,\kappa(X)$. Now let U be the dense affine open subset of X defined by $f \neq 0$; by construction, U has non-empty intersection with Z. For any $x \in U$, we have inclusions $R[f^{-1}] \subset \mathscr{O}_{X,x} \subset \kappa(X)$; so the map $\mathrm{Br}\,R[f^{-1}] \to \mathrm{Br}\,\kappa(X)$ factors through $\mathrm{Br}\,\mathscr{O}_{X,x}$, showing that α lies in the image of $\mathrm{Br}\,\mathscr{O}_{X,x}$. Thus α is unramified at every point of U, that is, α lies in $\mathrm{Br}\,U$. □

Corollary 12.2.6. *If α is any class in* $\mathrm{Br}\,\kappa(X)$*, then there is a dense open subset $U \subset X$ such that α lies in* $\mathrm{Br}\,U$.

Proof This is simply Proposition 12.2.5 in the case when Z is the whole of X. □

Corollary 12.2.7. *Let α be any class in* $\mathrm{Br}\,\kappa(X)$*. Then the set of points of X at which α is unramified is open in X (in the Zariski topology).*

Proof Let V denote the set of points at which α is unramified. Proposition 12.2.5 shows that every point in V has an open neighbourhood contained in V, and therefore V is open. □

The closed subset of X consisting of those points where an element $\alpha \in \mathrm{Br}\,\kappa(X)$ is ramified is called the *ramification locus* of α. One of the deepest results in the theory of the Brauer group is the purity theorem, which we now state. Recall that a closed subset is said to be of pure codimension c if each of its irreducible components is of codimension c.

Theorem 12.2.8 (Purity Theorem)**.** *Let X be a smooth, geometrically irreducible variety over a field k. Suppose either that X has dimension at most* 2*, or that k has characteristic zero.*

(i) *Let α be a class in* $\mathrm{Br}\,\kappa(X)$*. Then the ramification locus of α is either empty, or of pure codimension* 1 *in X.*

(ii) *If Z is any closed subset of X of codimension at least 2, then* $\mathrm{Br}(X \smallsetminus Z)$ *coincides with* $\mathrm{Br}X$.

(iii) *There is an equality*

$$\mathrm{Br}X = \bigcap_{Z} \mathrm{Br}\,\mathscr{O}_{X,Z}$$

where Z runs over the prime divisors on X, and the intersection takes place in $\mathrm{Br}\,\kappa(X)$.

Proof A proof of this theorem is far beyond the scope of this book, but let us show that the statements are equivalent. (More precisely, we will show that if one of the three statements holds for all smooth, geometrically irreducible varieties over a particular field, then so do the other two.)

Assume (i), and suppose that α lies in $\mathrm{Br}(X \smallsetminus Z)$. Then the ramification locus of α is contained in Z, so cannot be of pure codimension 1; it is therefore empty. So α lies in $\mathrm{Br}X$, proving (i) $\Rightarrow$ (ii).

Now assume (ii), and suppose that α is a class lying in $\mathrm{Br}\,O_{X,Z}$ for all prime divisors Z. Then Proposition 12.2.5 shows that no Z is contained in the ramification locus of α. Therefore the ramification locus has codimension at least 2, so (ii) implies that α lies in $\mathrm{Br}X$, proving (ii) $\Rightarrow$ (iii).

Finally, assume (iii). Let α be an element of $\mathrm{Br}\,\kappa(X)$ and let U be the complement in X of the union of all components of the ramification locus that are of codimension 1 in X. Now, if Z is any prime divisor on U, then α is unramified at some point of Z and hence lies in $\mathrm{Br}\,\mathscr{O}_{U,Z}$. Applying (iii) to U, we see that α lies in $\mathrm{Br}U$. Thus the ramification locus of α contained only components of codimension 1, proving (iii) $\Rightarrow$ (i).

For the proof of the Purity Theorem, we refer to the literature. When X has dimension at most 2, Proposition 7.2 of Auslander and Goldman (1960) shows that (iii) holds, proving the theorem in that case. In the general case, we use the fact that $\mathrm{Br}X$ is isomorphic to the étale cohomology group $\mathrm{H}^2(X, \mathbb{G}_{\mathrm{m}})$; see Proposition 12.4.13 for a discussion of this. The statement corresponding to (ii) for $\mathrm{H}^2(X, \mathbb{G}_{\mathrm{m}})$ is a deep result in étale cohomology, proved by Grothendieck (1968, III, Section 6). □

Remark 12.2.9. In positive characteristic p, the Purity Theorem is not known to hold in general for varieties of dimension greater than 2. However, the Brauer group is torsion **??** and so splits as the direct sum of a p-primary part and a prime-to-p part. The Purity Theorem, and all the results below that depend on it, remain true for the prime-to-p part of the Brauer group.

Remark 12.2.10 (The unramified Brauer group). For any field K containing a base field k, we can consider the set S of all discrete valuation rings $A \subset K$

containing k and having fraction field K. For each such A, we have $\mathrm{Br}A \subset \mathrm{Br}K$, and so we define the *unramified Brauer group* of K/k to be

$$\mathrm{Br}_{\mathrm{nr}}(K/k) = \bigcap_{A \in S} \mathrm{Br}A$$

where the intersection takes place in $\mathrm{Br}K$. In particular, this may be applied to the function field of a smooth, geometrically irreducible variety X over k, giving us the unramified Brauer group $\mathrm{Br}_{\mathrm{nr}}(\kappa(X)/k)$. Let us compare this group, defined without any geometric information, to the Brauer group of X. Every prime divisor Z on X gives rise to a discrete valuation ring $O_{X,Z}$ that contains k and has fraction field $\kappa(X)$; so any element of $\mathrm{Br}_{\mathrm{nr}}(\kappa(X)/k)$ is unramified at every divisor of X, and the Purity Theorem shows that $\mathrm{Br}_{\mathrm{nr}}(\kappa(X)/k)$ is contained in $\mathrm{Br}X$. On the other hand, not all discrete valuations on $\kappa(X)$ arise from prime divisors on X. For example, a nonempty open subset of X has the same function field as X, but may have fewer prime divisors; and blowing up X in a point gives a new variety with the same function field, but with one extra prime divisor. However, if X is projective then it can be shown (using the valuative criterion of properness) that, for every discrete valuation ring A as above, there is a point x of X satisfying $\mathcal{O}_{X,x} \subset A \subset \kappa(X)$. Therefore any element of $\mathrm{Br}X$ is contained in $\mathrm{Br}A$. So, when X is projective, we have an identity $\mathrm{Br}X = \mathrm{Br}_{\mathrm{nr}}(\kappa(X)/k)$.

An important consequence of the Purity Theorem is that the Brauer group is a birational invariant of smooth, projective varieties. To show this, we first prove a lemma.

Lemma 12.2.11. *Let $f\colon X \to Y$ be a birational morphism between smooth, geometrically irreducible varieties over a field k. Suppose that $Z \subset Y$ is a closed subset of codimension at least two such that the restriction $X \setminus f^{-1}(Z) \to Y \setminus Z$ is an isomorphism. If Y satisfies the hypotheses of the Purity Theorem, then the induced map $f^*\colon \mathrm{Br}Y \to \mathrm{Br}X$ is an isomorphism.*

Proof We have a commutative diagram of Brauer groups as follows.

$$\begin{array}{ccc} \mathrm{Br}Y & \longrightarrow & \mathrm{Br}(Y \setminus Z) \\ {\scriptstyle f^*}\downarrow & & \downarrow \\ \mathrm{Br}X & \longrightarrow & \mathrm{Br}(X \setminus f^{-1}(Z)) \end{array}$$

The two horizontal arrows are inclusions; the top one is an equality, by the Purity Theorem. The right-hand vertical arrow is an isomorphism by assumption. Therefore the bottom arrow is an equality, and so f^* is an isomorphism. □

Remark 12.2.12. Even in the absence of the Purity Theorem, the same argument shows that the map $f^*\colon \operatorname{Br} Y \to \operatorname{Br} X$ is injective.

Corollary 12.2.13. *Let $\phi\colon X \dashrightarrow Y$ be a birational map of smooth, projective, geometrically irreducible surfaces over any field. Then the resulting isomorphism $\operatorname{Br}\kappa(Y) \cong \operatorname{Br}\kappa(X)$ induces an isomorphism $\operatorname{Br} Y \cong \operatorname{Br} X$.*

Proof By Theorem 7.3.2, we can factorise ϕ as $g \circ f^{-1}$, where $f\colon \tilde{X} \to X$ and $g\colon \tilde{X} \to Y$ are composites of blow-ups in points and isomorphisms. Because all the varieties concerned are surfaces, they satisfy the Purity Theorem. By Lemma 12.2.11, all the induced maps of Brauer groups are isomorphisms. □

Remark 12.2.14. One can prove in a similar way that the Brauer group is a birational invariant of smooth projective varieties of any dimension over a field of characteristic zero: see Grothendieck (1968, III, Section 7). Alternatively, this follows immediately from the identification of the Brauer group with the unramified Brauer group of the function field (see Remark 12.2.10), since the unramified Brauer group is clearly a birational invariant.

12.3 Examples

We are now in a position to compute the Brauer groups of some simple varieties.

Theorem 12.3.1. *Let k be an algebraically closed field, and let C be a smooth, geometrically irreducible curve over k. Then $\operatorname{Br} C$ is trivial.*

Proof Corollary 10.4.10(ii) shows that $\operatorname{Br}\kappa(C)$ is trivial, and so the subgroup $\operatorname{Br} C$ is also trivial. □

In positive characteristic, the question of how the Brauer group changes when passing from a separably closed field to its algebraic closure was studied by Grothendieck using flat cohomology. In particular, he proved the following:

Theorem 12.3.2 (Grothendieck)**.** *Let X be a projective variety over a separably closed field k, and denote by $\bar{X}$ the base change of X to an algebraic closure of k. Suppose that the Picard variety of X is smooth (for example, $\mathrm{H}^2(X, \mathscr{O}_X) = 0$ or $\mathrm{H}^1(X, \mathscr{O}_X) = 0$). Then the natural homomorphism $\operatorname{Br} X \to \operatorname{Br} \bar{X}$ is injective.*

Proof See Grothendieck (1968, Corollaire III.5.7). □

The hypothesis applies in particular to smooth, projective curves. Combining with Theorem 12.3.1, we obtain:

Corollary 12.3.3. *Let C be a smooth, geometrically irreducible, projective curve over a separably closed field. Then* $\mathrm{Br}C$ *is trivial.*

We next turn to computing the Brauer groups of affine and projective spaces.

Lemma 12.3.4. *Let k be any field. Then the only algebraic classes in* $\mathrm{Br}\mathbf{A}^1_k$ *are the constant classes, that is, the natural homomorphism* $\mathrm{Br}k \to \mathrm{Br}_1\mathbf{A}^1_k$ *is an isomorphism.*

Proof This is the first part of Theorem 7.5 of Auslander and Goldman (1960). □

Lemma 12.3.5. *Let k be a perfect field. Then the natural homomorphism* $\mathrm{Br}k \to \mathrm{Br}\mathbf{A}^1_k$ *is an isomorphism.*

Proof Because k is perfect, its separable closure is the same as its algebraic closure. Theorem 12.3.1 then shows that $\mathrm{Br}_1\mathbf{A}^1_k$ is equal to $\mathrm{Br}\mathbf{A}^1_k$, and so Lemma 12.3.4 gives the desired result. □

As we noted in Example 12.1.11, if k is not perfect then $\mathrm{Br}\mathbf{A}^1_k$ does contain non-constant elements.

Theorem 12.3.6. *Let k be a field of characteristic zero, and let n be a positive integer. Then the natural homomorphism* $\mathrm{Br}k \to \mathrm{Br}\mathbf{A}^n_k$ *is an isomorphism.*

Proof We proceed by induction, following Colliot-Thélène (1980, Proposition 1.3). The case $n = 1$ follows from Lemma 12.3.5. Assume $n > 1$ and regard $\mathbf{A}^n_k$ as $\mathbf{A}^{n-1}_k \times \mathbf{A}^1_k$ with coordinates $x_1, \ldots, x_{n-1}, t$. Let $\pi\colon \mathbf{A}^n_k \to \mathbf{A}^{n-1}_k$ be the projection onto the first $n-1$ coordinates, and let $\sigma\colon \mathbf{A}^{n-1}_k \to \mathbf{A}^n_k$ be the inclusion of the hyperplane $t = 0$. Thus $\pi \circ \sigma$ is the identity map on $\mathbf{A}^{n-1}_k$.

Let K be the function field of $\mathbf{A}^{n-1}_k$, and L the function field of $\mathbf{A}^n_k$; the map π^* identifies K with the subfield $k(x_1, \ldots, x_{n-1})$ of $L = k(x_1, \ldots, x_{n-1}, t)$. But L is also the function field of the affine line over K, and so we have the Brauer group $\mathrm{Br}\mathbf{A}^1_K$ contained in $\mathrm{Br}L$. We claim that $\mathrm{Br}\mathbf{A}^n_k$ is contained in $\mathrm{Br}\mathbf{A}^1_K$. To see this, note that to every point P of $\mathbf{A}^1_K$ is associated a subvariety of $\mathbf{A}^n_k$ (the scheme-theoretic closure of P), as follows: the point P is defined by a prime ideal in $K[t]$, and the intersection of that prime ideal with the subring $k[x_1, \ldots, x_{n-1}, t]$ is another prime ideal, which defines a subvariety Z of $\mathbf{A}^n_k$. It is straightforward to check that the local rings $\mathscr{O}_{\mathbf{A}^1_K, P}$ and $\mathscr{O}_{\mathbf{A}^n_k, Z}$, both subrings of L, coincide. Thus any element of $\mathrm{Br}L$ which is unramified at Z is also unramified at P, and so $\mathrm{Br}\mathbf{A}^n_k$ is contained in $\mathrm{Br}\mathbf{A}^1_K$. By Lemma 12.3.5, the homomorphism $\pi^*\colon \mathrm{Br}K \to \mathrm{Br}L$ maps $\mathrm{Br}K$ isomorphically to $\mathrm{Br}\mathbf{A}^1_K$; so $\mathrm{Br}\mathbf{A}^n_k$ is contained in the image of π^*.

Now let α be any class in $\mathrm{Br}\mathbf{A}^n_k$. As we have just seen, there is a class

$\beta \in \mathrm{Br}K$ satisfying $\alpha = \pi^*(\beta)$. But then we have $\sigma^*\alpha = \sigma^*\pi^*\beta = \beta$. By Proposition 12.2.3, β lies in $\mathrm{Br}\mathbf{A}_k^{n-1}$. Thus the map $\pi^*\colon \mathrm{Br}\mathbf{A}_k^{n-1} \to \mathrm{Br}\mathbf{A}_k^n$ is surjective.

The natural map $\mathrm{Br}k \to \mathrm{Br}\mathbf{A}_k^n$ factors as $\mathrm{Br}k \to \mathrm{Br}\mathbf{A}_k^{n-1} \xrightarrow{\pi^*} \mathrm{Br}\mathbf{A}_k^n$. By the inductive hypothesis, the left-hand component is an isomorphism. We have shown that the right-hand component is surjective. The whole composite map is injective, since $\mathbf{A}_k^n$ has a k-point; so it is an isomorphism. □

Corollary 12.3.7. *Let k be a field of characteristic zero, and let n be a positive integer. Then the natural homomorphism $\mathrm{Br}k \to \mathrm{Br}\mathbf{P}_k^n$ is an isomorphism.*

Proof Affine n-space $\mathbf{A}_k^n$ is an open subvariety of $\mathbf{P}_k^n$, so we have inclusions $\mathrm{Br}k \subseteq \mathrm{Br}\mathbf{P}_k^n \subseteq \mathrm{Br}\mathbf{A}_k^n$ inside $\mathrm{Br}\,\kappa(\mathbf{P}_k^n)$. By Theorem 12.3.6, all three groups coincide. □

The statement that $\mathrm{Br}k \to \mathrm{Br}\mathbf{P}_k^n$ is an isomorphism is true over any field, but in positive characteristic we cannot prove it in the same way as Corollary 12.3.7, for the simple reason that $\mathrm{Br}\mathbf{A}_k^n$ does contain non-constant elements. We describe an alternative approach by induction on n, again following Colliot-Thélène (1980, Proposition 1.3). Firstly, we prove the result for the projective line.

Lemma 12.3.8. *Let k be any field. Then the natural map $\mathrm{Br}k \to \mathrm{Br}\mathbf{P}_k^1$ is an isomorphism.*

Proof By Corollary 12.3.3, $\mathrm{Br}_1\mathbf{P}_k^1$ is equal to $\mathrm{Br}\mathbf{P}_k^1$. But $\mathrm{Br}_1\mathbf{P}_k^1$ is contained in $\mathrm{Br}_1\mathbf{A}_k^1$, which is the image of $\mathrm{Br}k$ by Lemma 12.3.4. □

Now we can apply Lemma 12.3.8 inductively in the same way as in the proof of Theorem 12.3.6 to prove the result for $\mathbf{P}^n$.

Theorem 12.3.9. *Let k be any field, and let n be a positive integer. Then the natural homomorphism $\mathrm{Br}k \to \mathrm{Br}\mathbf{P}_k^n$ is an isomorphism.*

Proof Suppose that n is greater than 1. Pick a point P of $\mathbf{P}_k^n$, and let $p\colon \mathbf{P}_k^n \dashrightarrow \mathbf{P}_k^{n-1}$ be the projection away from the point P. This rational map is not defined at P. However, p factors as $\mathbf{P}_k^n \xleftarrow{f} X \xrightarrow{\pi} \mathbf{P}_k^{n-1}$ where f is the blow-up of $\mathbf{P}^n$ at the point P and π is a morphism. By Remark 12.2.12, the induced map $f^*\colon \mathrm{Br}\mathbf{P}_k^n \to \mathrm{Br}X$ is injective, so it suffices to show that $\mathrm{Br}k \to \mathrm{Br}X$ is an isomorphism. This follows from Colliot-Thélène (1980, Proposition 1.3), as before; we sketch the details.

164: Make this an exercise earlier somewhere?

Notice that π is a morphism having fibres isomorphic to $\mathbf{P}_k^1$; and the inclusion σ of the exception divisor of the blow-up in X is a section of π. So we

are in a situation very much like that of Theorem 12.3.6. Letting K denote the function field of $\mathbf{P}^{n-1}_k$, we again have an identification of the function field L of X with the function field of $\mathbf{P}^1_K$. (Indeed, the function field of X is the same as that of $\mathbf{A}^n$, so the identification is the same as in the proof of Theorem 12.3.6.) Under this identification, $\mathrm{Br}X$ is contained in $\mathrm{Br}\mathbf{P}^1_K$; as before, this is true because every divisor on $\mathbf{P}^1_K$ can be identified with a divisor on X. By Lemma 12.3.8, the homomorphism $\pi^*\colon \mathrm{Br}K \to \mathrm{Br}L$ maps $\mathrm{Br}K$ isomorphically to $\mathrm{Br}\mathbf{P}^1_K$, and therefore $\mathrm{Br}X$ is contained in the image of π^*.

Finally, we use the section σ in the same way as in the proof of Theorem 12.3.6 to deduce that π^* maps $\mathrm{Br}\mathbf{P}^{n-1}_k$ isomorphically to $\mathrm{Br}X$. By induction, the natural homomorphism $\mathrm{Br}k \to \mathrm{Br}X$ is an isomorphism, and the result follows. □

Corollary 12.3.10. *Let k be any field, and let X be a smooth, projective, geometrically rational surface over k. Then there is an equality* $\mathrm{Br}_1 X = \mathrm{Br}X$.

Proof Let $\bar{k}$ be an algebraic closure of k, and k^{sep} the separable closure of k in $\bar{k}$. By assumption, the base change $\bar{X}$ of X to $\bar{k}$ is birational to $\mathbf{P}^2_{\bar{k}}$. By Corollary 12.2.13, there is an isomorphism $\mathrm{Br}\bar{X} \cong \mathrm{Br}\mathbf{P}^2_{\bar{k}}$. By Corollary 12.3.7, we have $\mathrm{Br}\mathbf{P}^2_{\bar{k}} \cong \mathrm{Br}\bar{k} = 0$. If k has characteristic zero, then this completes the proof.

If k has positive characteristic, we must work a little harder. We have $\mathrm{H}^1(X, \mathscr{O}_X) = 0$, since coherent sheaf cohomology groups respect base change and $\mathrm{H}^1(\bar{X}, \mathscr{O}_{\bar{X}})$ is trivial because $\bar{X}$ is rational. Therefore Theorem 12.3.2 applies, and we deduce that $\mathrm{Br}X^{\mathrm{sep}}$ is trivial. It follows that $\mathrm{Br}_1 X = \ker(\mathrm{Br}X \to \mathrm{Br}X^{\mathrm{sep}})$ is the whole of $\mathrm{Br}X$. □

We will see how to compute $\mathrm{Br}_1 X$ using Galois cohomology, in Chapter 15.

12.4 Other definitions of the Brauer group

165: This section maybe belongs later, at least after we've seen $\mathrm{Br} = \mathrm{H}^2$ for fields.

The definition of the Brauer group in Section 12.1 is convenient: by defining the Brauer group of a smooth, geometrically irreducible variety to be a subgroup of the Brauer group of its function field, we can apply all our knowledge of Brauer groups of fields to understand the Brauer group of a variety. In particular, our definition is useful for computations, as we will see in Chapter 15. However, the definition is also lacking in some respects: most notably, it does not generalise well to singular varieties, nor to those which are reducible. For deeper study of Brauer groups, it is important to be able to talk about the Brauer group of an arbitrary variety, or indeed an arbitrary scheme. In this section we

describe two more general notions of the Brauer group: one defined in terms of sheaves of Azumaya algebras, and the other using étale cohomology. For a smooth, geometrically irreducible, quasi-projective variety over a field, both these notions coincide with the definition of Section 12.1. The material of this section is not necessary for understanding any subsequent parts of this book.

In this section, we will freely use schemes, sheaves and étale cohomology. Most of the material in this section is covered in detail by Milne (1980) and by Grothendieck (1968). We reserve the notation $\mathrm{Br}X$ for the Brauer group as defined in Definition 12.1.1.

It often happens in algebraic geometry that classes of objects defined over a base ring may be extended without much work to classes of objects over an arbitrary scheme. This can be done to the definition of an Azumaya algebra, giving the notion of an Azumaya algebra over a scheme (or, indeed, over a ringed space). This definition was first made by Auslander (1966).

166: Sort out references in this section.

Proposition 12.4.1. *Let X be a scheme, and let $\mathscr{A}$ be a locally free sheaf of $\mathscr{O}_X$-algebras of finite presentation. The following are equivalent:*

(i) **A** *has non-zero rank everywhere, and the natural map*

$$\phi : \mathscr{A} \otimes_{\mathscr{O}_X} \mathscr{A}^{\mathrm{opp}} \to \mathscr{E}nd_{\mathscr{O}_X}\mathscr{A},$$

defined on an open set U by $(a \otimes a') \mapsto (x \mapsto axa')$, is an isomorphism;

(ii) *for every point $x \in X$, the stalk $\mathscr{A}_x$ is an Azumaya algebra over the local ring $\mathscr{O}_{X,x}$;*

(iii) *for every point $x \in X$, the fibre $\mathscr{A}_x \otimes_{\mathscr{O}_{X,x}} k_x$ is a central simple algebra over the residue field k_x;*

(iv) *there is an étale morphism $f : X' \to X$ such that $f^*\mathscr{A}$ is isomorphic to the matrix algebra $\mathrm{M}_n(\mathscr{O}_X)$, for some positive integer n.*

167: Do we want a sheafy matrix symbol?

Proof See Milne (1980, Chapter IV, Proposition 2.1). □

Definition 12.4.2. Let X be a scheme. An *Azumaya algebra* on X is a locally free, finitely presented sheaf of $\mathscr{O}_X$-algebras satisfying the equivalent properties of Proposition 12.4.1.

In the case that $X = \mathrm{Spec}\,R$ is an affine scheme, there is a standard equivalence between R-modules and sheaves of $\mathscr{O}_X$-modules. Proposition 11.2.3 shows that an R-algebra A is an Azumaya algebra (in the sense of Chapter 11) if and only if the corresponding sheaf $\tilde{A}$ is an Azumaya algebra on X.

We can also sheafify the definition of equivalence of Azumaya algebras.

Definition 12.4.3. Let X be a scheme. Two Azumaya algebras $\mathscr{A}, \mathscr{B}$ on X are

equivalent if there are locally free sheaves of $\mathscr{O}_X$-modules $\mathscr{E}, \mathscr{E}'$, everywhere of finite non-zero rank, such that $\mathscr{A} \otimes_{\mathscr{O}_X} \mathscr{E}nd\mathscr{E}$ is isomorphic to $\mathscr{B} \otimes_{\mathscr{O}_X} \mathscr{E}nd\mathscr{E}'$.

Again, this definition generalises that of Chapter 11 in the case that $X = \operatorname{Spec} R$ is affine.

Definition 12.4.4. Let X be a scheme. The *Azumaya Brauer group* of X, denoted $\mathrm{Br}_{\mathrm{Az}} X$, is the group of equivalence classes of Azumaya algebras over X, with the operation induced by tensor product.

In order to study the Azumaya Brauer group of a scheme, and in particular to show that it agrees with our Brauer group for smooth, geometrically irreducible varieties, we would like to relate it to some cohomology groups of X. From a formal point of view, this proceeds in exactly the same way as the identification of the Brauer group of a field with the second Galois cohomology group. Proposition 12.4.1(iv) shows that an Azumaya algebra of constant rank on X is a twisted form of the matrix algebra $\mathrm{M}_n(\mathscr{O}_X)$ for some n.

Proposition 12.4.5. *For any scheme X, there is a natural injection* $\mathrm{Br}_{\mathrm{Az}} X \to \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_{\mathrm{m}})$.

Sketch of proof See Milne (1980, Theorem 2.5) for the details. We sketch the argument in the case when Čech cohomology on $X_{\text{ét}}$ agrees with derived-functor cohomology, to point out the analogy with the proof of Theorem **??**.

Firstly, a sheafified version of the Skolem–Noether theorem (Theorem 10.3.12) shows that the automorphism sheaf of $\mathrm{M}_n(\mathscr{O}_X)$ is the sheaf associated to the group scheme PGL_n. Then standard Čech cohomology theory gives an injection from the set of isomorphism classes of Azumaya algebras of rank n^2 on X to the set $\mathrm{H}^1_{\text{ét}}(X, \mathrm{PGL}_n)$, which one can show is actually a bijection.

The exact sequence of sheaves on $X_{\text{ét}}$

$$0 \to \mathbb{G}_{\mathrm{m}} \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 0$$

gives rise to a long exact sequence in (non-abelian) cohomology, part of which is

$$\mathrm{H}^1_{\text{ét}}(X, \mathrm{GL}_n) \to \mathrm{H}^1_{\text{ét}}(X, \mathrm{PGL}_n) \to \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_{\mathrm{m}}).$$

The first group $\mathrm{H}^1_{\text{ét}}(X, \mathrm{GL}_n)$ parametrises isomorphism classes of locally free O_X-modules of rank n on X. A calculation shows that the homomorphism $\mathrm{H}^1_{\text{ét}}(X, \mathrm{GL}_n) \to \mathrm{H}^1_{\text{ét}}(X, \mathrm{PGL}_n)$ takes the class of a vector bundle $\mathscr{E}$ to the class of the endomorphism algebra $\mathscr{E}nd\mathscr{E}$. Thus the kernel of the map $\mathrm{H}^1_{\text{ét}}(X, \mathrm{PGL}_n) \to \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_{\mathrm{m}})$ consists of isomorphism classes of trivial Azumaya algebras, and

we obtain an embedding

$$\{\text{equivalence classes of Azumaya algebras of rank } n^2\} \to \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_{\mathrm{m}}).$$

It can then be shown that these maps for individual n together induce an injection $\mathrm{Br}_{\mathrm{Az}} X \to \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_{\mathrm{m}})$. □

Motivated by Proposition 12.4.5, we define a new variant of the Brauer group of a scheme.

Definition 12.4.6. Let X be a scheme. The *cohomological Brauer group* of X, denoted $\mathrm{Br}' X$, is the étale cohomology group $\mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_{\mathrm{m}})$.

Beware that some authors use $\mathrm{Br} X$ to denote the Azumaya Brauer group, and some use $\mathrm{Br} X$ to denote the cohomological Brauer group. Also, some authors use the name "cohomological Brauer group" and the notation $\mathrm{Br}' X$ or $\mathrm{Br} X$ to refer to the torsion subgroup of what we have called $\mathrm{Br}' X$.

In the case of a field K, the group $\mathrm{Br}'(K)$ is equal to the Galois cohomology group $\mathrm{H}^2(K, K^\times)$ and, as we saw in **??**, the injection $\mathrm{Br} K \to \mathrm{Br}' K$ is an isomorphism. It is a natural question to ask whether the equality $\mathrm{Br}_{\mathrm{Az}} = \mathrm{Br}'$ holds in more generality. Before turning to this question, we look at the relationship between $\mathrm{Br}' X$ and $\mathrm{Br}\, \kappa(X)$.

Proposition 12.4.7. *Let X be a regular integral Noetherian scheme. Then the natural map $\mathrm{Br}' X \to \mathrm{Br}'\, \kappa(X) = \mathrm{Br}\, \kappa(X)$ is injective.*

Proof We sketch the proof of Grothendieck (1968, Section II.1); see also Milne (1980, Chapter III, Example 2.22). Let $j\colon \operatorname{Spec} \kappa(X) \to X$ denote the inclusion of the generic point. The short exact sequence of sheaves on $X_{\text{ét}}$

$$0 \to \mathbb{G}_{\mathrm{m}} \to j_* \mathbb{G}_{\mathrm{m}} \to \mathscr{D}iv_X \to 0$$

defines the sheaf $\mathscr{D}iv_X$ of Cartier divisors on X. From it we deduce an exact sequence

$$0 \to \mathrm{H}^1_{\text{ét}}(X, \mathscr{D}iv_X) \to \mathrm{Br}' X \to \mathrm{H}^2_{\text{ét}}(X, j_* \mathbb{G}_{\mathrm{m}})$$

of cohomology groups. A calculation using Hilbert's Theorem 90 shows that $\mathrm{R}^1 j_* \mathbb{G}_{\mathrm{m}}$ vanishes. The Leray spectral sequence for j then shows that $\mathrm{H}^2_{\text{ét}}(X, j_* \mathbb{G}_{\mathrm{m}})$ injects into $\mathrm{Br}\, \kappa(X)$, and so we deduce that the kernel of the map $\mathrm{Br}' X \to \mathrm{Br}\, \kappa(X)$ is given by $\mathrm{H}^1_{\text{ét}}(X, \mathscr{D}iv_X)$. Because X is regular, the Cartier divisors on X are the same as the Weil divisors; thus there is an isomorphism of sheaves $\mathscr{D}iv_X \cong \bigoplus_D (\imath_D)_* \mathbf{Z}$, where $\imath_D\colon D \to X$ runs over the inclusions of all prime divisors on X. We deduce an isomorphism $\mathrm{H}^1_{\text{ét}}(X, \mathscr{D}iv_X) \cong \bigoplus_D \mathrm{H}^1_{\text{ét}}(D, \mathbf{Z})$, and an easy calculation show that the groups $\mathrm{H}^1_{\text{ét}}(D, \mathbf{Z})$ are trivial. Hence $\mathrm{Br}' X$ injects into $\mathrm{Br}\, \kappa(X)$. □

The proof of Proposition 12.4.7 also shows how to construct varieties X such that $\mathrm{Br}' X \to \mathrm{Br}\,\kappa(X)$ is *not* injective. For example, let X be an integral normal surface over an algebraically closed field. Developing the arguments of Grothendieck (1968, Section II.1), DeMeyer and Ford (1992) show that the kernel of the map $\mathrm{Br}' X \to \mathrm{Br}\,\kappa(X)$ is isomorphic to the cokernel of the natural map

$$\mathrm{Cl}(X) \to \bigoplus_P \mathrm{Cl}(\mathscr{O}^h_{X,P})$$

where Cl denotes the Weil divisor class group, P runs over the singular points of X, and $\mathscr{O}^h_{X,P}$ denotes the Henselisation of the local ring at P. Grothendieck refers to a construction of Mumford giving a variety for which this quotient is non-zero, and even non-torsion. Childs (1976) gives several explicit examples of this kind.

Example 12.4.8 (Childs, 1976, Theorem 5.1)**.** Let X be the affine variety over the complex numbers $\mathbf{C}$ defined by $z^2 = ux^2 + vy^2$, where u, v are polynomials in x, y not vanishing at $(0,0)$, and let P be the singular point $(0,0,0)$. Then $\mathrm{Cl}(\mathscr{O}^h_{X,P})$ has order 2; and $\mathrm{Cl}(X)$ has order 2 if and only if the equation $1 = u\alpha^2 + v\beta^2$ has a solution in the local ring $\mathscr{O}_{X,P}$, and has order 1 otherwise. Thus the kernel of $\mathrm{Br}' X \to \mathrm{Br}\,\kappa(X)$ has order 1 or 2, accordingly.

Example 12.4.9 (Childs, 1976, Theorem 6.1)**.** Let C be a smooth plane curve over the complex numbers $\mathbf{C}$ of genus greater than three. Let X be the affine cone over C. Then $\ker(\mathrm{Br}' X \to \mathrm{Br}\,\kappa(X))$ is a complex vector space of positive dimension.

For examples of singular del Pezzo surfaces X where $\ker(\mathrm{Br}' X \to \mathrm{Br}\,\kappa(X))$ is non-trivial, see Bright (2013).

Let us return to the question of when the Azumaya Brauer group $\mathrm{Br}_{\mathrm{Az}}$ coincides with the cohomological Brauer group Br'. One possible obstruction is given by the following lemma.

Lemma 12.4.10. *Let X be a scheme with finitely many connected components. The Azumaya Brauer group $\mathrm{Br}_{\mathrm{Az}}(X)$ is a torsion group.*

Proof The image of $\mathrm{H}^1_{\text{ét}}(X, \mathrm{PGL}_n)$ in $\mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_{\mathrm{m}})$ is killed by n (see Milne, 1980, Chapter IV, Proposition 2.7), and so any Azumaya algebra of rank n^2 corresponds to class of order dividing n in $\mathrm{Br}_{\mathrm{Az}} X$. The rank of a locally free $\mathscr{O}_X$-module is locally constant on X, so the lemma is true if X is connected. In the general case, the Azumaya Brauer group of X is the product of those of its connected components, and a product of finitely many torsion groups is again torsion. □

In particular, this shows that any scheme X such that $\mathrm{Br}'X$ is non-torsion (for example, the surfaces of Example 12.4.9) cannot possibly satisfy $\mathrm{Br}_{\mathrm{Az}}X = \mathrm{Br}'X$. However, the following theorem shows that, for quasi-projective varieties, this is the only obstruction.

Theorem 12.4.11. *Let X be a scheme admitting an ample invertible sheaf. Then the inclusion $\mathrm{Br}_{\mathrm{Az}}X \to \mathrm{Br}'X$ identifies $\mathrm{Br}_{\mathrm{Az}}X$ with the torsion subgroup of $\mathrm{Br}'X$.*

Proof This theorem is originally due to Gabber (unpublished). An alternative proof has been given by de Jong (n.d.). □

For a discussion of the proof of this theorem in the case that X is affine, or the union of two affine subschemes, see Hoobler (1982).

Finally, let us show that the definition of the Brauer group of a smooth, geometrically irreducible variety X over a field given in Definition 12.1.1 does indeed coincide with both $\mathrm{Br}_{\mathrm{Az}}X$ and $\mathrm{Br}'X$. As noted above, if X is affine then $\mathrm{Br}_{\mathrm{Az}}X$ coincides with our $\mathrm{Br}X$ almost by definition.

Lemma 12.4.12. *Let X be a regular integral scheme. Then $\mathrm{H}^p_{\mathrm{Zar}}(X, \mathscr{O}_X^\times)$ is trivial for all $p > 1$.*

Proof Let R_X be the sheaf of rational functions on X. We have the Weil-divisor exact sequence

$$0 \to \mathscr{O}_X^\times \to R_X^\times \to \bigoplus_{i_D\colon D \to X} (i_D)_*\mathbf{Z} \to 0$$

where the direct product is over all inclusions $i_D\colon D \to X$ of prime divisors on X. The sheaves $R_X^\times$ and $\bigoplus_D (i_D)_*\mathbf{Z}$ are both flasque, so this sequence is a flasque resolution of $\mathscr{O}_X^\times$ and can be used to compute its cohomology. Therefore $\mathrm{H}^p_{\mathrm{Zar}}(X, \mathscr{O}_X^\times)$ vanishes for $p > 1$. □

Proposition 12.4.13. *Let X be a smooth, geometrically irreducible variety over a field. If we identify $\mathrm{Br}'X = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_{\mathrm{m}})$ with its image in $\mathrm{Br}\,\kappa(X)$, then the Brauer group $\mathrm{Br}X$ of Definition 12.1.1 coincides with $\mathrm{Br}'X$.*

Proof Let $\mathscr{H}^i(\mathbb{G}_{\mathrm{m}})$ denote the Zariski sheaf on X associated to the presheaf defined by $U \mapsto \mathrm{H}^i_{\text{ét}}(U, \mathbb{G}_{\mathrm{m}})$. We claim that our $\mathrm{Br}X$ is naturally identified with $\mathrm{H}^0_{\mathrm{Zar}}(X, \mathscr{H}^2(\mathbb{G}_{\mathrm{m}}))$, as follows. The description of sheafification given by Hartshorne (1977, p. 64) shows that a section of $\mathrm{H}^0_{\mathrm{Zar}}(X, \mathscr{H}^2(\mathbb{G}_{\mathrm{m}}))$ is given by a locally compatible family of elements of the stalks $\mathrm{Br}'(\mathrm{Spec}\,\mathscr{O}_{X,x})$; given that these stalks all inject into $\mathrm{Br}\,\kappa(X)$, it follows that $\mathrm{H}^0_{\mathrm{Zar}}(X, \mathscr{H}^2(\mathbb{G}_{\mathrm{m}}))$ is identified with the intersection in $\mathrm{Br}\,\kappa(X)$ of the subgroups $\mathrm{Br}'(\mathrm{Spec}\,\mathscr{O}_{X,x})$. By Theorem 12.4.11 we have $\mathrm{Br}'(\mathrm{Spec}\,\mathscr{O}_{X,x}) = \mathrm{Br}_{\mathrm{Az}}(\mathrm{Spec}\,\mathscr{O}_{X,x}) = \mathrm{Br}\,\mathscr{O}_{X,x}$,

compatibly with the inclusions in $\mathrm{Br}\,\kappa(X)$, and so indeed the natural injection of $\mathrm{H}^0_{\mathrm{Zar}}(X, \mathscr{H}^2(\mathbb{G}_{\mathrm{m}}))$ into $\mathrm{Br}\,\kappa(X)$ identifies it with $\mathrm{Br}\,X$.

The sheaf $\mathscr{H}^i(\mathbb{G}_{\mathrm{m}})$ coincides with the higher direct image sheaf $\mathrm{R}^i f_* \mathbb{G}_{\mathrm{m}}$, where $f\colon X_{\text{ét}} \to X_{\mathrm{Zar}}$ is the natural map of sites. The Leray spectral sequence for f is

$$E_2^{pq} = \mathrm{H}^p_{\mathrm{Zar}}(X, \mathscr{H}^q(\mathbb{G}_{\mathrm{m}})) \Rightarrow \mathrm{H}^{p+q}_{\text{ét}}(X, \mathbb{G}_{\mathrm{m}}).$$

The sheaf $\mathscr{H}^1(\mathbb{G}_{\mathrm{m}})$ is the zero sheaf: if x is a closed point of X, then the stalk of $\mathscr{H}^1(\mathbb{G}_{\mathrm{m}})$ at x is the group $\mathrm{Pic}(\mathrm{Spec}\,\mathscr{O}_{X,x})$, which vanishes. Directly from the definition, $\mathscr{H}^0(\mathbb{G}_{\mathrm{m}})$ is the Zariski sheaf $\mathscr{O}_X^\times$, and so $\mathrm{H}^p_{\mathrm{Zar}}(X, \mathscr{H}^0(\mathbb{G}_{\mathrm{m}}))$ vanishes for $p > 1$ by Lemma 12.4.12. The spectral sequence therefore shows that the natural map $\mathrm{Br}' X \to \mathrm{H}^0_{\mathrm{Zar}}(X, \mathscr{H}^2(\mathbb{G}_{\mathrm{m}}))$ is an isomorphism, which by functoriality is compatible with the natural embeddings of both groups in $\mathrm{Br}\,\kappa(X)$. □

- Say something about Brauer groups over the complex numbers (using exponential sequence from Chapter 2?).
- Brauer groups of some varieties (e.g. finiteness of Brauer groups of K3 surfaces)

13

The Brauer–Manin obstruction

Manin (1971) realised that we can sometimes use an element of the Brauer group of a variety X to show that some adelic points on X cannot possibly be approximations to rational points; in extreme cases, this construction shows that X has no rational points. This obstruction to the existence of rational points is now known as the Brauer–Manin obstruction. It puts many counter-examples to the Hasse principle, such as those we saw in Chapter 2, into a general framework.

13.1 The obstruction

Throughout this section, let X be a smooth, projective, geometrically irreducible variety over a number field k.

Let ℓ be a field containing k. Recall that, given an element α of $\mathrm{Br}X$ and a point $P \in X(\ell)$, we can evaluate α at P to get a class $\alpha(P) \in \mathrm{Br}\,\ell$. In particular, for each place v of k, we can evaluate $\alpha \in \mathrm{Br}X$ at points of $X(k_v)$ to get classes in $\mathrm{Br}\,k_v$. We denote by α also the evaluation map $X(k_v) \to \mathrm{Br}\,k_v$ thus obtained. Composing with the local invariant map gives a *local evaluation map*

$$X(k_v) \xrightarrow{\alpha} \mathrm{Br}\,k_v \xrightarrow{\mathrm{inv}_v} \mathbf{Q}/\mathbf{Z} \tag{13.1}$$

for each place v. Before we can describe the Brauer–Manin obstruction, we need a finiteness result about these maps.

Proposition 13.1.1. *Let α be a class in $\mathrm{Br}X$. Then, for all but finitely many places $v \in \Omega_k$, we have $\alpha(P) = 0$ for all $P \in X(k_v)$.*

The proof of Proposition 13.1.1 is a classic "spreading out" type proof, similar to that of Lemma 2.2.3. In the language of schemes it can be made very brief (see Skorobogatov, 2001, p. 101) but we can also present the proof in a

more elementary way. We first prove it for integral points on an affine variety. Recall that, for an affine variety $Y \subset \mathbf{A}^n$ over a number field k, and a place v, the notation $Y(\mathfrak{o}_v)$ simply means the set of points of $Y(k_v)$ having coordinates that all lie in $\mathfrak{o}_v$.

Lemma 13.1.2. *Let k be a number field. Let $Y \subset \mathbf{A}^n_k$ be a smooth, geometrically irreducible variety over k, and let α be a class in $\operatorname{Br} Y$. Then, for all but finitely many places $v \in \Omega_k$, we have $\alpha(P) = 0$ for all $P \in Y(\mathfrak{o}_v)$.*

Proof Let $\mathfrak{o}_k$ be the ring of integers of k. Let I be the intersection of the ideal $I(X,k) \subset k[x_1,\dots,x_n]$ with the subring $\mathfrak{o}_k[x_1,\dots,x_n]$, and let R be the quotient ring $\mathfrak{o}_k[x_1,\dots,x_n]/I$. It is a subring of the coordinate ring $k[Y] = k[x_1,\dots,x_n]/I(X,k)$, and we have $k[Y] = k.R$. In particular, this shows that R is an integral domain. (In scheme-theoretic terms, $\operatorname{Spec} R$ is the Zariski closure of Y in $\mathbf{A}^n_{\mathfrak{o}_k}$.)

For every point $P \in Y(\bar{k})$, we have $\alpha \in \operatorname{Br} \mathscr{O}_{Y,P} \subset \operatorname{Br} \kappa(Y)$. If $\mathfrak{p} \subset R$ denotes the prime ideal that is the kernel of evaluation at P, then the local ring $\mathscr{O}_{Y,P}$ is also the localisation of R at $\mathfrak{p}$. Applying Corollary 11.3.9 shows that there exists $f_P \in R$ satisfying $f_P(P) \neq 0$, and such that α lies in the image of $\operatorname{Br} R[f_P^{-1}] \to \operatorname{Br} \mathscr{O}_{Y,P}$. Let $J \subset k[Y]$ be the ideal generated by all the f_P for $P \in Y(\bar{k})$. By the Nullstellensatz, J is the unit ideal. Thus we can write

$$a_{P_1} f_{P_1} + \cdots + a_{P_r} f_{P_r} = 1$$

where $P_1,\dots,P_r \in Y(\bar{k})$ are finitely many points, each a_{P_i} lies in $k[Y]$, and α lies in the image of $\operatorname{Br} R[f_{P_i}^{-1}]$ for all i. Clearing denominators gives

$$a'_{P_1} f_{P_1} + \cdots + a'_{P_r} f_{P_r} = N$$

with $a'_{P_i} \in R$ and $N \in \mathfrak{o}_k$. We claim that the conclusion follows for all finite places v satisfying $v(N) = 0$.

If v is a finite place with $v(N) = 0$, then let P lie in $Y(\mathfrak{o}_v)$. Substituting P into the above sum shows that some $f = f_{P_i}$ satisfies $v(f(P)) = 0$. Thus the image of f under the evaluation map $\mathrm{ev}_P \colon R \to \mathfrak{o}_v$ is invertible, and so the evaluation map factors through $R[f^{-1}]$. We obtain a commutative diagram

$$\begin{array}{ccc} \operatorname{Br} R[f^{-1}] & \longrightarrow & \operatorname{Br} \mathscr{O}_{Y,P} \\ \big\downarrow{\scriptstyle \mathrm{ev}_P} & & \big\downarrow{\scriptstyle \mathrm{ev}_P} \\ \operatorname{Br} \mathfrak{o}_v & \longrightarrow & \operatorname{Br} k_v. \end{array}$$

Because α lies in the image of $\operatorname{Br} R[f^{-1}]$ in $\operatorname{Br} \mathscr{O}_{Y,P}$, so $\alpha(P)$ lies in the image of $\operatorname{Br} \mathfrak{o}_v$ in $\operatorname{Br} k_v$. But $\operatorname{Br} \mathfrak{o}_v$ is trivial by Corollary 11.3.13. □

Proof of Proposition 13.1.1 Applying Lemma 13.1.2 to each of the standard affine pieces of X gives a finite set $S \subset \Omega_k$ such that, for $v \notin S$, the algebra α evaluates to zero on all $\mathfrak{o}_v$-points of all affine pieces. Since X is projective, every k_v-point of X can be scaled to give an $\mathfrak{o}_v$-point on one of the standard affine pieces of X. □

Remark 13.1.3. The condition that X be projective cannot be removed from Proposition 13.1.1. Indeed, Harari (1994, Théorème 2.1.1) has shown the following: if $U \subset X$ is a non-empty open subset of a smooth, projective, geometrically irreducible variety over a number field k, and $\alpha \in \mathrm{Br}U$ is a class which does not lie in $\mathrm{Br}X$, then there are infinitely many places v of k where the local evaluation map $U(k_v) \to \mathrm{Br}k_v$ associated to α is not zero.

Because X is projective, the set of adelic points $X(\mathbf{A}_k)$ of X is simply the direct product $\prod_v X(k_v)$. Fix a class $\alpha \in \mathrm{Br}X$. Adding together all the local maps (13.1), we obtain an adelic evaluation map

$$X(\mathbf{A}_k) \to \bigoplus_v \mathrm{Br}k_v \xrightarrow{\sum_v \mathrm{inv}_v} \mathbf{Q}/\mathbf{Z}. \tag{13.2}$$

For each place v of k, the set $X(k)$ is a subset of $X(k_v)$. Combining all the places, we obtain a diagonal embedding of $X(k)$ in the set $X(\mathbf{A}_k)$ of adelic points. The following observation is the key to the definition of the Brauer–Manin obstruction.

Proposition 13.1.4. *Let α be a class in $\mathrm{Br}X$. Then $X(k)$ lies in the kernel of the map* (13.2)*.*

Proof It is straightforward to check that the following diagram commutes:

$$\begin{array}{ccccc} X(k) & \longrightarrow & X(\mathbf{A}_k) & & \\ \alpha\downarrow & & \downarrow\alpha & & \\ \mathrm{Br}k & \longrightarrow & \bigoplus_v \mathrm{Br}k_v & \xrightarrow{\sum_v \mathrm{inv}_v} & \mathbf{Q}/\mathbf{Z} \end{array} \tag{13.3}$$

where the vertical arrows are evaluation of α at points, the top horizontal arrow is the inclusion of $X(k)$ in $X(\mathbf{A}_k)$, and the bottom line is the exact sequence (**??**). The composite map from $X(\mathbf{A}_k)$ to $\mathbf{Q}/\mathbf{Z}$ is the map of (13.2). Now suppose that $x \in X(k)$ is a point of X. Then we have $\sum_v \mathrm{inv}_v \alpha(x) = 0$ because $\alpha(x)$ lies in $\mathrm{Br}k$, and the bottom row of (13.3) is a complex. Hence the diagonal image of x in $X(\mathbf{A}_k)$ lies in the kernel of the adelic evaluation map, as claimed. □

With Proposition 13.1.4 in mind, we make the following definition.

Definition 13.1.5. Let α be a class in $\mathrm{Br}X$. Define

$$X(\mathbf{A}_k)^{\alpha} := \Big\{(P_v) \in X(\mathbf{A}_k) \;\Big|\; \sum_v \mathrm{inv}_v\, \alpha(P_v) = 0\Big\}.$$

If B is a subset of $\mathrm{Br}X$, similarly define

$$X(\mathbf{A}_k)^{B} := \Big\{(P_v) \in X(\mathbf{A}_k) \;\Big|\; \sum_v \mathrm{inv}_v\, \alpha(P_v) = 0 \text{ for all } \alpha \in B\Big\};$$

we use the notation $X(\mathbf{A}_k)^{\mathrm{Br}}$ for $X(\mathbf{A}_k)^{\mathrm{Br}X}$.

One way to look at this is as follows: the map (13.2) defines a pairing $X(\mathbf{A}_k) \times \mathrm{Br}X \to \mathbf{Q}/\mathbf{Z}$, and we have defined $X(\mathbf{A}_k)^B$ to be the subset of $X(\mathbf{A}_k)$ orthogonal to the set B under this pairing.

Proposition 13.1.4 states that $X(k)$ is contained in $X(\mathbf{A}_k)^B$ for any subset B of $\mathrm{Br}X$. In particular, if $X(\mathbf{A}_k)^B$ is empty, then $X(k)$ is also empty.

Definition 13.1.6. Let X be a smooth, projective, geometrically irreducible variety over a number field k. Let B be a subset of the Brauer group of X. If $X(\mathbf{A}_k)$ is not empty and $X(\mathbf{A}_k)^B$ is empty, then we say that there is a *Brauer–Manin obstruction to the Hasse principle* on X coming from B. If $X(\mathbf{A}_k)^B$ is strictly contained in $X(\mathbf{A}_k)$, we say that there is a *Brauer–Manin obstruction to weak approximation* on X coming from B. If B equals $\mathrm{Br}X$, we simply say that there is a Brauer–Manin obstruction to the Hasse principle or to weak approximation on X.

d: Recall the definition of weak approximation?

Notice that constant classes in $\mathrm{Br}X$ give no contribution to the obstruction.

Proposition 13.1.7. *If $\alpha \in \mathrm{Br}X$ lies in $\mathrm{Br}_0 X$, then the associated map* (13.2) *is zero.*

Proof This follows immediately from the exact sequence (**??**). □

It is a common abuse of notation to write $\mathrm{Br}X/\mathrm{Br}k$ for the quotient $\mathrm{Br}X/\mathrm{Br}_0 X$, even in the case in which the map $\mathrm{Br}k \to \mathrm{Br}X$ is not injective.

Remark 13.1.8. In view of Proposition 13.1.7, the pairing $X(\mathbf{A}_k) \times \mathrm{Br}X \to \mathbf{Q}/\mathbf{Z}$ is well defined when $\mathrm{Br}X$ is replaced by $\mathrm{Br}X/\mathrm{Br}k$. In many of the cases of interest, $\mathrm{Br}X/\mathrm{Br}k$ is a finite group, and it is possible to calculate $X(\mathbf{A}_k)^{\mathrm{Br}}$ explicitly.

In the next proposition we show that evaluation maps are continuous. In the proof we use the following constructions.

To every central simple algebra A over a field K, there is associated a variety V_A over K called a *Severi–Brauer variety*. This is a twisted form of projective space: if A has dimension n^2 over K, then, over a separable closure of K,

the variety V_A becomes isomorphic to $\mathbf{P}^{n-1}$. For details of the correspondence between central simple algebras and Severi–Brauer varieties, see Gille and Szamuely (2006, Chapter 5). For us, the most important property of the Severi–Brauer variety V_A is that $V_A(K)$ is non-empty if and only if A is isomorphic to a matrix algebra over K, that is, A represents the trivial class in $\mathrm{Br}\,K$.

Let Y be a smooth variety over a field K, and α a class in $\mathrm{Br}\,Y$. We can think of α as a family of elements of $\mathrm{Br}\,K$, parametrised by the points of Y; so it is not too much of a leap to think of the corresponding family of Severi–Brauer varieties parametrised by the points of Y. This idea turns out to be accurate, as described by Grothendieck (1968, Section I.8): it is possible to construct a *relative* Severi–Brauer variety T_α over K, equipped with a smooth morphism $T_\alpha \to Y$, such that the fibre $(T_\alpha)_P$ at a point $P \in Y(K)$ is a Severi–Brauer variety representing the Brauer class $\alpha(P)$. In particular, the fibre $(T_\alpha)_P$ has a K-point if and only if $\alpha(P)$ is trivial.

168: Find a better reference for this construction

We now analyse the local situation.

Proposition 13.1.9. *Let Y be a smooth variety over a local field K, and let α be a class in $\mathrm{Br}\,Y$. The evaluation map $\alpha\colon Y(K) \to \mathrm{Br}\,K$ is locally constant for the analytic topology on $Y(K)$.*

d: check that we call the topology on $Y(K)$ the analytic topology.

Proof We give a proof of this fact using the constructions sketched above.

We first show that, supposing $\alpha(P) = 0$ at a point $P \in Y(K)$, there is some neighbourhood U of P in the analytic topology on $Y(K)$ such that $\alpha(Q) = 0$ holds for all $Q \in U$. To see this, let $T_\alpha \to Y$ be the relative Severi–Brauer variety associated to α. By assumption, the class $\alpha(P)$ is trivial in $\mathrm{Br}\,K$; therefore the fibre $(T_\alpha)_P$ contains a K-point. Moreover, the morphism $f\colon T_\alpha \to Y$ is a smooth morphism of algebraic varieties, and hence the function $f_K\colon T_\alpha(K) \to Y(K)$ is a submersion of analytic manifolds over K. Thus, the Inverse Function Theorem (see Serre, 2006, Section II.III.10.2) shows that there is an analytic neighbourhood U of P over which f_K admits an analytic section; in particular, the fibres $(T_\alpha)_Q$, for $Q \in U$, all contain a K-point. Hence $\alpha(Q)$ is trivial for all $Q \in U$.

To conclude, let us suppose, instead of $\alpha(P) = 0$, that we have $\alpha(P) = \beta$ for some $\beta \in \mathrm{Br}\,K$. Considering β as an element of $\mathrm{Br}\,Y$ and applying the above argument to $\alpha - \beta$, we see that there is an analytic neighbourhood U of P in $Y(K)$ such that $\alpha(Q) = \beta$ holds for all $Q \in U$. In other words, the evaluation map $Y(K) \to \mathrm{Br}\,K$ is locally constant, proving the proposition. □

We return to the situation where X is a smooth, projective, geometrically irreducible variety over a number field k.

Corollary 13.1.10. *For each class α in* $\mathrm{Br}X$*, the adelic evaluation map* (13.2) *is continuous.*

Proof By Proposition 13.1.1, there is a finite set S of places of k such that the evaluation map $X(\mathbf{A}_k) \to \mathbf{Q}/\mathbf{Z}$ factors through the projection $\pi_S \colon X(\mathbf{A}_k) \to \prod_{v\in S} X(k_v)$. By definition of the adelic topology, the projection π_S is continuous and using Proposition 13.1.9 we conclude that the evaluation map is continuous. □

Corollary 13.1.11. *For each subset B of* $\mathrm{Br}X$*, the set $X(\mathbf{A}_k)^B$ is closed in $X(\mathbf{A}_k)$.*

Proof For each $\alpha \in B$, the set $X(\mathbf{A}_k)^\alpha$ is the inverse image of 0 under the adelic evaluation map, so is closed. Therefore $X(\mathbf{A}_k)^B$ is an intersection of closed sets, so is also closed. □

The reason that the definition of the Brauer–Manin obstruction is so useful is that the sets $X(\mathbf{A}_k)^\alpha$ are often explicitly computable; for certain classes of varieties, we can even compute the set $X(\mathbf{A}_k)^{\mathrm{Br}}$ effectively. We look at this problem in more detail in Section 15.4.

13.2 Examples

Example 13.2.1. Let X be the non-singular del Pezzo surface of degree 4 of Example 2.3.5 defined by the equations

$$\begin{cases} uv = x^2 - 5y^2 \\ (u+v)(u+2v) = x^2 - 5z^2 \end{cases}$$

and let $\mathscr{A}$ be the quaternion algebra

$$\mathscr{A} = \left(5, \frac{u}{u+v}\right)$$

over $\kappa(X)$. In Example 12.1.2, we saw that the class $\alpha \in \mathrm{Br}\,\kappa(X)$ of $\mathscr{A}$ lies in $\mathrm{Br}X$. Let us now show that there is a Brauer–Manin obstruction to the Hasse principle on X coming from α.

We will describe the map $X(\mathbf{Q}_v) \to \mathbf{Q}/\mathbf{Z}$, given by $P \mapsto \mathrm{inv}_v\,\alpha(P)$, separately for each place v. As noted in Example 12.1.7, it is often enough to evaluate the functions in the definition of $\mathscr{A}$ to compute the evaluation $\alpha(P)$.

At the real place ∞, notice that 5 is positive and hence a square in $\mathbf{R}$. Let $P = [u_0, v_0, x_0, y_0, z_0]$ in $X(\mathbf{R})$ be a point such that u_0 and v_0 are non-zero. Then $\alpha(P)$ is the class of the trivial algebra $(5, u_0/(u_0+v_0))_{\mathbf{R}}$ and

$\mathrm{inv}_\infty \alpha(P) = 0$. Since the map $P \mapsto \mathrm{inv}_\infty \alpha(P)$ is locally constant on $X(\mathbf{R})$ by Proposition 13.1.9, it follows that it is zero everywhere.

At a place corresponding to an odd prime p such that 5 is a square in $\mathbf{Q}_p$, the same argument works and shows that $\mathrm{inv}_p \alpha(P) = 0$ for all $P \in X(\mathbf{Q}_p)$.

Now suppose that $p \neq 5$ is an odd prime, such that 5 is not a square in $\mathbf{Q}_p$ and therefore not a square in $\mathbf{F}_p$ and let P be a point in $X(\mathbf{Q}_p)$. Choose coordinates $P = [u_0, v_0, x_0, y_0, z_0]$ such that u_0, v_0, x_0, y_0, z_0 all lie in $\mathbf{Z}_p$ and are not all divisible by p. Reducing the equations modulo p, we deduce that u_0 and v_0 can never be both divisible by p, since otherwise x_0/y_0 and x_0/z_0 would be square roots of 5 in $\mathbf{F}_p$. Similarly, p cannot divide both $u_0 + v_0$ and $u_0 + 2v_0$. It follows that, for each $P = [u, v, x, y, z] \in X(\mathbf{Q}_p)$, at least one of the expressions

$$\left(5, \frac{u}{u+v}\right), \quad \left(5, \frac{v}{u+v}\right), \quad \left(5, \frac{u}{u+2v}\right), \quad \left(5, \frac{v}{u+2v}\right)$$

is of the form $(5, b)$ with $b \in \mathbf{Z}_p^\times$, and therefore defines a quaternion algebra over $\mathbf{Q}_p$ whose class is $\alpha(P)$. By Proposition 10.1.6 the class $\alpha(P)$ is trivial in $\mathrm{Br}\,\mathbf{Q}_p$. We conclude that $\mathrm{inv}_p \alpha(P) = 0$ for all P in $X(\mathbf{Q}_p)$.

Next, we analyse the prime 2. Solving the equations defining X modulo 8 we find that u and v cannot both be even at a point of $X(\mathbf{Q}_2)$. (Note that working modulo 2 is not enough, since $(0, 0, 1, 1, 1) \in \mathbf{F}_2^5$ is a solution to the equations.) As before, for each $P \in X(\mathbf{Q}_2)$, one of u, v is odd, and similarly one of $(u+v), (u+2v)$ is odd. The formula of Proposition 10.1.6 shows that the Hilbert symbol $(5, b)_2$ is 1 whenever $b \in \mathbf{Z}_2$ is odd, so once again we conclude that $\mathrm{inv}_2 \alpha(P) = 0$ for all $P \in X(\mathbf{Q}_2)$.

Finally, we look at the prime 5. Let P be a point in $X(\mathbf{Q}_5)$. Choose coordinates $P = [u_0, v_0, x_0, y_0, z_0]$ such that u_0, v_0, x_0, y_0, z_0 all lie in $\mathbf{Z}_5$ and are not all divisible by 5. Reducing the coordinates of P modulo 5, we obtain a point $\bar{P}$ in $\mathbf{P}^4_{\mathbf{F}_5}$ satisfying the equations defining X. Let X_5 be the variety over $\mathbf{F}_5$ defined by the reduction modulo 5 of the equations defining X. The variety X_5 is the union of four planes, meeting in a common line; two of these planes are defined over $\mathbf{F}_5$ and the other two are quadratic and conjugate. The two defined over $\mathbf{F}_5$, which therefore contain all the points of $X_5(\mathbf{F}_5)$, are $\{u = v = x\}$ and $\{u = v = -x\}$. The line of intersection of these planes is $\{u = v = x = 0\}$, but no point of $X(\mathbf{Q}_5)$ reduces to a point on this line, as can be seen easily reducing the equations modulo 25. Therefore the point P in $X(\mathbf{Q}_5)$ satisfies $u_0 \equiv v_0 \equiv \pm x_0 \pmod 5$ with u_0, v_0, x_0 all being units in $\mathbf{Z}_5$. This means that $b = u_0/(u_0 + v_0)$ is congruent to 3 modulo 5, and the formula of Proposition 10.1.6 gives $(5, b)_5 = -1$. We deduce that $\mathrm{inv}_5 \alpha(P) = \frac{1}{2}$ for all $P \in X(\mathbf{Q}_5)$.

To summarise, let v be a place of $\mathbf{Q}$; we have proved that $\mathrm{inv}_v \alpha(P) = 0$

for all $P \in X(\mathbf{Q}_v)$ where $v \neq 5$, and that $\mathrm{inv}_5\,\alpha(P) = \frac{1}{2}$ for all $P \in X(\mathbf{Q}_5)$. It follows that

$$\sum_v \mathrm{inv}_v\,\alpha(P_v) = \tfrac{1}{2} \quad \text{for all } (P_v) \in X(\mathbf{A}_\mathbf{Q}).$$

So $X(\mathbf{A}_\mathbf{Q})^\alpha$ is empty, and therefore there is a Brauer–Manin obstruction to the Hasse principle on X.

We conclude by showing that the Brauer–Manin obstruction also explains the phenomenon of Example 2.3.8.

Example 13.2.2. Let S be the singular cubic surface of Example (2.3.8), defined in $\mathbf{P}^3_\mathbf{Q}$ by the equation

$$T(X^2+Y^2) = (4Z-7T)(Z^2-2T^2).$$

The two singular points of S are $(X:Y:Z:T) = (\pm i:1:0:0)$ where $i^2=-1$. Let U denote the complement in S of these two points. Any rational point of S must be contained in U, since neither of the singular points is rational.

Let $\mathscr{A}$ be the quaternion algebra over $\kappa(S)$ defined by

$$\mathscr{A} = \left(-1, \frac{4Z-7T}{T}\right).$$

Let us ignore for the moment that we have not defined $\mathrm{Br}\,S$. We will show that the class of $\mathscr{A}$ gives a Brauer–Manin obstruction to weak approximation that explains why one connected component of $S(\mathbf{R})$ contains no rational points. In doing so, we will show that the class of $\mathscr{A}$ lies in $\mathrm{Br}\,U$. In fact, our calculations are sufficient to show that the class of $\mathscr{A}$ lies in $\mathrm{Br}\,\tilde{S}$ where $\tilde{S}$ is any smooth projective variety birational to S.

As before, we start by finding alternative ways of writing the quaternion algebra $\mathscr{A}$. Firstly, looking at the defining equations of S we can see equalities

$$T(X^2+Y^2) + 2T^2(4Z-7T) = Z^2(4Z-7T)$$

and so

$$\frac{4Z-7T}{T} = \frac{X^2+Y^2+8ZT-14T^2}{Z^2}$$

as functions on S, immediately giving a new way of writing $\mathscr{A}$. Furthermore, since the denominator Z^2 is a square, we can replace it with any other square such as X^2, Y^2 or T^2 to get new quaternion algebras isomorphic to $\mathscr{A}$. Also, the defining equations give

$$\left(\frac{4Z-7T}{T}\right)\left(\frac{Z^2-2T^2}{T^2}\right) = \frac{X^2+Y^2}{T^2} = \mathrm{N}_{\kappa(S)(i)/\kappa(S)}\left(\frac{X+iY}{T}\right)$$

and so the algebra $(-1,(Z^2-2T^2)/T^2)$ is isomorphic to $\mathscr{A}$, and again the denominator here may be replaced by any square. In this way we find a set of isomorphic quaternion algebras over $\kappa(S)$:

$$\left(-1,\frac{4Z-7T}{T}\right),\quad \left(-1,\frac{X^2+Y^2+8ZT-14T^2}{(\text{square})}\right),\quad \left(-1,\frac{Z^2-2T^2}{(\text{square})}\right).$$

Let α be the common class in $\operatorname{Br}\kappa(S)$ of these algebras. At any point P of U, at least one of these expressions defines an Azumaya algebra over the local ring $\mathscr{O}_{S,P}$ and so can be used to evaluate the class α at P. Indeed, if Z^2-2T^2 vanishes at a point, then neither $4Z-7T$ nor T vanishes unless we have $Z=T=0$. In that case, the middle expression above defines an Azumaya algebra unless we also have $X^2+Y^2=0$, but the only points where that happens are the singular points, which are not in U.

We now analyse the invariant of α at each place separately. Let p be prime. If $p\equiv 1 \pmod 4$ then -1 is a square in $\mathbf{Q}_p$, and so $\operatorname{inv}_p\alpha(P)$ is 0 for all $P\in U(\mathbf{Q}_p)$.

If $p\equiv 3 \pmod 4$ then let P be a point of $U(\mathbf{Q}_p)$ and choose coordinates $P=[x,y,z,t]$ such that x,y,z,t lie in $\mathbf{Z}_p$ and are not all divisible by p. We argue as in the previous example: we prove that the local invariant is always zero by showing that at least one of $(4z-7t)/t, x^2+y^2+8zt-14t^2, z^2-2t^2$ is a p-adic unit. First we show that, if t is divisible by p, then $x^2+y^2+8zt-14t^2$ is a p-adic unit. Indeed, suppose that t is divisible by p; the equation of S shows that z is also divisible by p. Since $p\equiv 3 \pmod 4$, the value $x^2+y^2+8zt-14t^2$ could be divisible by p only if both x and y were divisible by p, contrary to our assumptions. We reduce to the case in which t is not divisible by p. Suppose that p divides both $4z-7t$ and z^2-2t^2; then p divides $16(z^2-2t^2)-(4z+7t)(4z-7t)=17t^2$. Since p does not divide t, it follows that p divides 17, but 17 is not congruent to 3 modulo 4. We conclude that p does not divides at most one of $4z-7t$ and z^2-2t^2, as we wanted to show.

We analyse what happens at 2. From the formula in Proposition 10.1.6(iii), we see that the Hilbert symbol $(-1,2^\beta v)_2$ takes the value 1 if $v\equiv 1 \pmod 4$, and takes the value -1 if $v\equiv 3 \pmod 4$. Let P be a point of $U(\mathbf{Q}_2)$ and choose coordinates $P=[x,y,z,t]$ such that x,y,z,t lie in $\mathbf{Z}_2$ and are not all even. If t is odd, then we have $(4z-7t)/t\equiv 1 \pmod 4$ and therefore $\alpha(P)$ is trivial. If t is even and z is odd, then we have $z^2-2t^2\equiv 1 \pmod 4$ and again $\alpha(P)$ is trivial. Lastly, if t and z are both even, then x,y are not both even, and therefore the value $x^2+y^2+8zt-14t^2$ is congruent to either 1 or 2 modulo 8, so that $\alpha(P)$ is trivial.

Finally, over $\mathbf{R}$, we see that $(4Z-7T)/T$ is non-negative on one component of $S(\mathbf{R})$, and strictly positive on a dense open subset of that compon-

ent, so $\mathrm{inv}_\infty \alpha = 0$ on that component. On the other component, however, $(4Z-7T)/T$ is strictly negative, and therefore $\mathrm{inv}_\infty \alpha = \frac{1}{2}$ on that component. We deduce that rational points can only be found in the component where $Z/T \geq \frac{7}{4}$, giving a Brauer–Manin obstruction to weak approximation on S.

In the example above, we worked with the open variety U obtained by removing the singular locus of a cubic surface S. It is a general fact that for every projective surface X there is a smooth projective surface X' and a morphism $X' \to X$ that is an isomorphism on the smooth locus of X. As a consequence, every smooth surface can be embedded as an open subset of a smooth projective surface. Note that, if the surface X is not smooth, then the smooth surface X' is not uniquely determined by the stated conditions, since it is always possible to replace X' by the blow-up at some point. Of course, all these surfaces X' are birational to one another.

d: Put this as a fact also in the blow up section, and maybe remove from here.

Going back to the surface S of Example 13.2.2, we worked on the open subset U, since we have not defined Brauer groups of singular varieties, and so we cannot talk about the Brauer group of S. At the same time, we were able to find an element α of $\mathrm{Br}\, U$ giving an obstruction to weak approximation. By an explicit computation, we discovered that the invariant map for the class α is trivial at almost all places: there is no reason to expect this on a non-projective variety. In fact, if S' is any smooth projective surface containing U, then the class α considered as a class in $\mathrm{Br}\, \kappa(S')$ does indeed lie in $\mathrm{Br}\, S'$. We can see this in different ways: we could explicitly construct an S' and check that the class α is unramified on S'; we could also use the result of Harari (1994) mentioned in Remark 13.1.3, since the local invariant maps of α are almost all zero. We can also formulate this conclusion as stating that the class α lies in the unramified Brauer group $\mathrm{Br}_{\mathrm{nr}}(\kappa(U)/k)$ (see Remark 12.2.10).

Exercise 13.2.3. Find a smooth projective surface S' (Exercise **??**) containing U and show explicitly that the class α lies in the Brauer group of S'.

d: Add ON MANIN'S CONJECTURE FOR A FAMILY OF CHÂTELET SURFACES?

14

Group cohomology

Much of this lecture comes from chapter 2 in Milne's notes on class field theory Milne (2008).

169: announce *i*'s

14.1 The problem

Let G be a group. A *G-module* is an *abelian* group M together with an action of G on M that respects the group structure, i.e., a homomorphism $G \to \operatorname{Aut} M$. A homomorphism $f\colon M \to N$ of G-modules is one that commutes with the actions of G. In other words, for every $\sigma \in G$ the diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ M & \xrightarrow[f]{} & N \end{array}$$

commutes. For any G-module M we write M^G for the largest subgroup of M on which G acts trivially. This group consists of all elements of M fixed by G and is called the group of G-invariants of M. Suppose that we have a short exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

of G-modules. Then clearly the map $f_*\colon A^G \to B^G$, which is the restriction of f, is also injective. Moreover, the sequence

$$0 \to A^G \xrightarrow{f_*} B^G \xrightarrow{g_*} C^G$$

is exact (since f is injective, an element $a \in A$ is fixed by G if and only if $f(a)$ is fixed). This means that "taking invariants is left exact." More precisely,

the functor from the category of G-modules to the category of abelian groups that sends each G-module M to its G-invariants M^G and each homomorphism $M \to N$ to its restriction $M^G \to N^G$ is a left-exact functor.

However, the map $g_*\colon B^G \to C^G$ may not be surjective. Group cohomology gives us information also about the cokernel of the map g_*. In our applications, the group G will almost always be a Galois group.

Example 14.1.1. Let C be the conic in $\mathbf{P}^2_{\mathbf{Q}}$ given by $x^2+y^2+z^2=0$. Then the natural sequence

$$0 \to \kappa(C_{\bar{\mathbf{Q}}})^*/\bar{\mathbf{Q}}^* \to \operatorname{Div} C_{\bar{\mathbf{Q}}} \to \operatorname{Pic} C_{\bar{\mathbf{Q}}} \to 0$$

is exact. Since any two points on a conic are linearly equivalent, the Galois group $G = \operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ acts trivially on $\operatorname{Pic} C_{\bar{\mathbf{Q}}}$, so $(\operatorname{Pic} C_{\bar{\mathbf{Q}}})^G = \operatorname{Pic} C_{\bar{\mathbf{Q}}} \cong \mathbf{Z}$. Note that C does not have any points over $\mathbf{Q}$, as it does not have any points over $\mathbf{R}$. We choose a divisor D_0 of degree 2 that is invariant under G (for instance the intersection points of C with a line defined over $\mathbf{Q}$, or an anticanonical divisor). We claim that $(\operatorname{Div} C_{\bar{\mathbf{Q}}})^G$ does not contain any divisors of odd degree; if it did, say $D \in (\operatorname{Div} C_{\bar{\mathbf{Q}}})^G$ and $\deg D = 2n+1$, then $D_1 = D - nD_0$ would be a divisor of degree 1 and by the Riemann–Roch Theorem for curves there would be an effective divisor of degree 1, i.e., a rational point, linearly equivalent to D_1. Therefore, the map $(\operatorname{Div} C_{\bar{\mathbf{Q}}})^G \to (\operatorname{Pic} C_{\bar{\mathbf{Q}}})^G \cong \mathbf{Z}$ has cokernel $\mathbf{Z}/2\mathbf{Z}$.

14.2 Explicit solution

Let G be a group. Use the conventions that $G^0 = \{1\}$ and $G^{-1} = \emptyset$.

Definition 14.2.1. For $i \geq -1$, let $C^i(G,M)$ denote the group of all functions (not necessarily homomorphisms) from G^i to M, called *i-cochains*. Let $d_i\colon C^i(G,M) \to C^{i+1}(G,M)$ be given by

$$\begin{aligned}(d_i\varphi)(g_1,\ldots,g_{i+1}) &= g_1\varphi(g_2,\ldots,g_{i+1}) + (-1)^{i+1}\varphi(g_1,\ldots,g_i) \\ &\quad + \sum_{j=1}^{i}(-1)^j\varphi(g_1,\ldots,g_jg_{j+1},\ldots,g_{i+1}).\end{aligned} \tag{14.1}$$

For $i \geq 0$, set $Z^i(G,M) = \ker(d_i)$ (the set of i-cocycles) and $B^i(G,M) = \operatorname{Im} d_{i-1}$ (the set of i-coboundaries).

In particular, because of our conventions, we have $C^0(G,M) = M$ and $C^{-1}(G,M) = 0$. It is easily checked that $d_i \circ d_{i-1} = 0$ for each $i \geq -1$, so we have an inclusion $B^i(G,M) \subset Z^i(G,M)$.

Definition 14.2.2. For each $i \geq 0$ we set $\mathrm{H}^i(G,M) = Z^i(G,M)/B^i(G,M)$.

Example 14.2.3. We have an equality $\mathrm{H}^0(G,M) = M^G$, so $i = 0$ gives nothing new.

Example 14.2.4. A 1-cocycle in $Z^1(G,M)$ is a function $\varphi\colon G \to M$ satisfying $\varphi(\sigma\tau) = \varphi(\sigma) + \sigma\varphi(\tau)$ for all $\sigma, \tau \in G$. A 1-coboundary is a function of the form $\sigma \mapsto \sigma m - m$ for some fixed $m \in M$.

Exercise 14.2.5. Show that if M is a G-module, and the action of G on M is trivial, then we have $\mathrm{H}^1(G,M) = \mathrm{Hom}(G,M)$.

Example 14.2.6. A 2-cocycle in $Z^2(G,M)$ is a function $\varphi\colon G \times G \to M$ satisfying

$$\rho\varphi(\sigma,\tau) = \varphi(\rho\sigma,\tau) - \varphi(\rho,\sigma\tau) + \varphi(\rho,\sigma)$$

for all $\rho, \sigma, \tau \in G$. A 2-coboundary is a function of the form $(\sigma,\tau) \mapsto \varphi(\sigma) + \sigma\varphi(\tau) - \varphi(\sigma\tau)$ for some fixed $\varphi \in C^1(G,M)$.

Suppose we have a short exact sequence

$$0 \to A \xrightarrow{\iota} B \to C \to 0$$

of G-modules. We define *connecting homomorphisms*

$$\delta_i\colon \mathrm{H}^i(G,C) \to \mathrm{H}^{i+1}(G,A)$$

follows. Let $\xi \in \mathrm{H}^i(G,C)$ be represented by the i-cocycle $\varphi\colon G^i \to C$ and lift φ to an i-cochain $\hat{\varphi}\colon G^i \to B$. Since $d_i(\varphi) = 0$, the $(i+1)$-cocycle $d_i(\hat{\varphi})\colon G^{i+1} \to B$ actually takes values in $\iota(A)$. The cocycle

$$(g_1,\ldots,g_{i+1}) \mapsto \iota^{-1}(d_i(\hat{\varphi})(g_1,\ldots,g_{i+1})) \tag{14.2}$$

represents the class $\delta_i(\xi)$.

Exercise 14.2.7. Show that $\delta_i(\xi)$ is independent of the choices of both the cocycle φ representing ξ, and its lift $\hat{\varphi}$. Also show that this description of δ_i does indeed define a homomorphism.

Proposition 14.2.8. *There is a natural long exact sequence*

$$\begin{aligned} 0 \to &\mathrm{H}^0(G,A) \to \mathrm{H}^0(G,B) \to \mathrm{H}^0(G,C) \xrightarrow{\delta_0} \\ &\mathrm{H}^1(G,A) \to \mathrm{H}^1(G,B) \to \mathrm{H}^1(G,C) \xrightarrow{\delta_1} \\ &\mathrm{H}^2(G,A) \to \mathrm{H}^2(G,B) \to \mathrm{H}^2(G,C) \xrightarrow{\delta_2} \\ &\cdots \end{aligned} \tag{14.3}$$

of abelian groups.

Proof See Milne (2008, II.1.9 and Proposition II.1.17). □

Our descriptions of the cohomology groups $\mathrm{H}^i(G,M)$ allow us to compute these groups explicitly, even though in particular examples this can be quite tedious. Fortunately, we have computers. For instance, MAGMA can often compute the groups that we will be interested in.

We endow the free abelian group $\mathbf{Z}[G]$ on the elements of G with a ring structure, defining the multiplication by

$$(\sum_g m_g g)(\sum_h n_h h) = \sum_{g,h} m_g n_h (gh).$$

The action of G on a G-module can be extended linearly to an action of the group ring $\mathbf{Z}[G]$. If we have any *abelian* group M, then giving M the structure of a G-module is equivalent to giving M the structure of a $\mathbf{Z}[G]$-module.

14.3 Abstract solution

The previous section gives an explicit description of cohomological groups. Homological algebra has a standard, more highbrow way of defining them. Although we will not use this point of view, it makes many proofs much simpler. In this section we present a short sketch of the idea.

Let Mod_G denote the abelian category of $\mathbf{Z}[G]$-modules and Ab the category of abelian groups. Then we have a functor from Mod_G to Ab that sends M to M^G. This functor, as we have seen, is left exact. One shows that Mod_G has enough so-called *injectives*, which is enough to conclude that there exist derived functors $\mathrm{H}^i(G,\,\cdot\,)$ for $i \geq 0$, such that $\mathrm{H}^0(G,M) = M^G$ for all $M \in \mathsf{Mod}_G$, and for each short exact sequence

$$0 \to A \to B \to C \to 0$$

of $\mathbf{Z}[G]$-modules, there are connecting homomorphisms $\delta_i \colon \mathrm{H}^i(G,C) \to \mathrm{H}^{i+1}(G,A)$ inducing a long exact sequence (14.3).

For details on how to compute the groups $\mathrm{H}^i(G,M)$ from taking an injective resolution of M, see for instance Milne (2008, Chapter II, "Definition of cohomology groups"). Note that $M^G = \mathrm{Hom}_G(\mathbf{Z},M)$, so instead of taking an injective resolution of M, we can also take a projective resolution of $\mathbf{Z}$, apply the functor $\mathrm{Hom}_G(\,\cdot\,,M)$, and then compute the cohomology of the resulting complex. Such a projective resolution can be constructed very explicitly and results in definition of cohomology groups as in the previous section. For details, see again Milne (2008, Chapter II).

If G is a topological group, then one could consider the full subcategory

of Mod_G of all $\mathbf{Z}[G]$-modules with continuous G-actions, with the discrete topology on the modules. We then obtain cohomology groups $\mathrm{H}^i_{\mathrm{cts}}(G,M)$ for each G-module M, also making up long exact sequences.

14.4 Group cohomology

170: different title?

Proposition 14.4.1. *Let G be a group and, for each j in a given index set J, let M_j be a G-module. Then for each $i \geq 0$ we have a natural isomorphism*

$$\mathrm{H}^i(G, \bigoplus_{s\in S} M_s) \to \bigoplus_{s\in S} \mathrm{H}^i(G, M_s).$$

Proof This follows immediately from the fact that we have a natural isomorphism

$$C^i(G, \bigoplus_{s\in S} M_s) \to \bigoplus_{s\in S} C^i(G, M_s)$$

for every $i \geq -1$. □

We now define some important maps on cohomology groups. For any subgroup H of a group G, the restrictions $C^i(G,M) \to C^i(H,M)$ induce *restriction homomorphisms*

$$\mathrm{Res}\colon \mathrm{H}^i(G,M) \to \mathrm{H}^i(H,M).$$

For any normal subgroup H of a group G, the natural maps $C^i(G/H, M^H) \to C^i(G,M)$ coming from composition with the quotient map $G \to G/H$ and the inclusion $M^H \to M$ induce the *inflation homomorphisms*

$$\mathrm{Infl}\colon \mathrm{H}^i(G/H, M^H) \to \mathrm{H}^i(G,M).$$

Proposition 14.4.2. *Let H be a normal subgroup of a group G, and let M be a G-module. Let $r > 0$ be an integer. If $\mathrm{H}^i(H,M) = 0$ for all $0 < i < r$, then the sequence*

$$0 \to \mathrm{H}^r(G/H, M^H) \xrightarrow{\mathrm{Infl}} \mathrm{H}^r(G,M) \xrightarrow{\mathrm{Res}} \mathrm{H}^r(H,M)$$

is exact.

171: Martin, reference, ok?

Proof See Milne (2008, Proposition II.1.34). □

In particular, Proposition 14.4.2 shows that we may identify $\mathrm{H}^r(G/H, M^H)$ with the cocycle classes in $\mathrm{H}^r(G,M)$ that lie in the kernel of the restriction map. Note moreover that the condition in that $\mathrm{H}^i(H,M) = 0$ for all $0 < i < r$ is automatically satisfied for $r = 1$.

For any subgroup H of a group G, we consider $\mathbf{Z}[G]$ as an H-module by

multiplication from the left, so $h(\sum_g n_g g) = \sum_g n_g(hg)$ for all $h \in H$. For any H-module M, we define the associated *induced module from H to G* to be the group

$$\mathrm{Ind}_H^G(M) = \mathrm{Hom}_{\mathbf{Z}[H]}(\mathbf{Z}[G], M)$$

of H-module homomorphisms; the group G acts on $\mathrm{Ind}_H^G(M)$ by

$$\sigma(\varphi)(x) = \varphi(x\sigma)$$

for all $\sigma \in G$, all $x \in \mathbf{Z}[G]$, and all $\varphi \in \mathrm{Ind}_H^G(M)$. In case H is the trivial subgroup of G, we abbreviate $\mathrm{Ind}_H^G(M)$ to $\mathrm{Ind}^G(M)$.

Proposition 14.4.3 (Shapiro's Lemma)**.** *Let H be a subgroup of a group G. For any H-module M, precomposition with the inclusion $H \subset G$ and post-composition with the map $\mathrm{Ind}_H^G(M) \to M$ given by $\varphi \mapsto \varphi(1)$ yields maps $C^i(G, \mathrm{Ind}_H^G(M)) \to C^i(H, M)$. These maps induce isomorphisms*

$$\mathrm{H}^i(G, \mathrm{Ind}_H^G(M)) \to \mathrm{H}^i(H, M).$$

Proof For each G-module M and each H-module N, we have natural isomorphisms

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \cong \mathrm{Hom}_H(M, N),$$

which shows that the functor $\mathrm{Ind}_H^G \colon \mathsf{Mod}_H \to \mathsf{Mod}_G$ is an adjoint of the functor $\mathsf{Mod}_G \to \mathsf{Mod}_H$ that sends M to itself, remembering only the H-module structure. Moreover, the functor Ind_H^G is exact and preserves injectives. This is enough to deduce the statement. For more details, see Milne (2008, Proposition 2.1.11). □

172: are all references to Milne (2008) independent of Milne's version???

Exercise 14.4.4. Prove Shapiro's Lemma for $i = 0$ directly by showing that every element in $(\mathrm{Ind}_H^G(M))^G$ is a constant map $g \mapsto m$ for some $m \in M^H$.

For a subgroup H of a group G and a G-module M, we can reinterpret each restriction map $\mathrm{Res} \colon \mathrm{H}^i(G, M) \to \mathrm{H}^i(H, M)$ as the composition of the isomorphism $\mathrm{H}^i(G, \mathrm{Ind}_H^G(M)) \to \mathrm{H}^i(H, M)$ from Shapiro's Lemma with the map $\mathrm{H}^i(G, M) \to \mathrm{H}^i(G, \mathrm{Ind}_H^G(M))$ that is induced by the map $m \mapsto (g \mapsto gm)$.

For any G-set X we can extend the action of G on X linearly to the free abelian group $\mathbf{Z}[X]$ on X, giving $\mathbf{Z}[X]$ the structure of a G-module.

Definition 14.4.5. A *permutation G-module* is a G-module M that is isomorphic to $\mathbf{Z}[X]$ for some G-set X.

In other words, a permutation G-module is a G-module M that is a free abelian group for which there exists a basis that is permuted by G. In particular,

we can apply this to the case that $X = G/H$ is the G-set of left-cosets of a subgroup H of G, on which G acts by $g'(gH) = (g'g)H$.

Exercise 14.4.6. Suppose G is a group and A is a G-set on which G acts transitively. Show that for any element $a \in A$ there is an isomorphism $G/G_a \to A$ of G-sets, where G_a is the stabilizer of a. Conclude that for each a there is an isomorphism $\mathbf{Z}[A] \to \mathbf{Z}[G/G_a]$ of G-modules.

Proposition 14.4.7. *Let H be a subgroup of a group G and let M be a G-module. Then there is a natural injective homomorphism*

$$\Psi\colon \mathbf{Z}[G/H] \otimes_{\mathbf{Z}} M \to \mathrm{Ind}_H^G(M)$$

of G-modules, where G acts on both factors of the tensor product, given by

$$\sum_C C \otimes m_C \mapsto (g \mapsto g m_{g^{-1}H}).$$

If H has finite index in G, then Φ is an isomorphism of G-modules, with the inverse given by

$$\varphi \mapsto \sum_{s \in S} sH \otimes s\varphi(s^{-}1),$$

where S is any set of representatives of the left cosets of H in G.

Proof It is easy to see that $\Psi(x)$ is $\mathbf{Z}[H]$-linear for every $x \in \mathbf{Z}[G/H]$, so Ψ is a well-defined map and easily seen to be a homomorphism of G-modules. Suppose $x, y \in \mathbf{Z}[G/H] \otimes_{\mathbf{Z}} M$ satisfy $\Psi(x) = \Psi(y)$ and write $x = \sum_C C \otimes m_C$ and $y = \sum_C C \otimes n_C$. For any coset C, choose an element $g \in G$ such that $g^{-1}H = C$. Then we have

$$g m_C = g m_{g^{-1}H} = \Psi(x)(g) = \Psi(y)(g) = g n_{g^{-1}H} = g n_C,$$

from which we deduce $m_C = n_C$. We conclude that $x = y$, so Ψ is injective. Assume H has finite index in G. Let $\Phi\colon \mathrm{Ind}_H^G(M) \to \mathbf{Z}[G/H] \otimes_{\mathbf{Z}} M$ be the map that is claimed to be the inverse of Ψ. One easily checks that Φ is independent of the choice of S, so it is well defined. We leave it as an exercise to check that the map is a homomorphism of G-modules and that Ψ and Φ are inverses of each other. □

Proposition 14.4.8. *Suppose G is a finite group and M a permutation G-module. Then the group $\mathrm{H}^1(G, M)$ is trivial.*

Proof Let A be a G-invariant basis for M. Then M is the direct sum, over all orbits C of A, of M_C, where M_C is the submodule of M generated by C. By Proposition 14.4.1 it suffices to show $\mathrm{H}^1(G, M_C) = 0$, so we have reduced

to the case that G acts transitively on A. Choose an element $a \in A$. By Exercise 14.4.6, the module M is isomorphic as a G-module to $\mathbf{Z}[G/G_a]$, where G_a is the stabilizer of a. Since G is finite, applying Proposition 14.4.7 to $H = G_a$ with G acting trivially on $\mathbf{Z}$, we find that $\mathbf{Z}[G/G_a] \cong \mathbf{Z}[G/G_a] \otimes \mathbf{Z}$ is isomorphic to the induced module $\mathrm{Ind}_{G_a}^G(\mathbf{Z})$. Therefore, by Shapiro's Lemma we have an isomorphism

173: G torsion should be enough? then use inflation restriction? how? G_a is not normal...

$$\mathrm{H}^1(G, \mathbf{Z}[G/G_a]) \cong \mathrm{H}^1(G, \mathrm{Ind}_{G_a}^G(\mathbf{Z})) \cong \mathrm{H}^1(G_a, \mathbf{Z}).$$

As the action of G_a on $\mathbf{Z}$ is trivial and G_a is torsion, while $\mathbf{Z}$ is torsion-free, we have $\mathrm{H}^1(G_a, \mathbf{Z}) \cong \mathrm{Hom}(G_a, \mathbf{Z}) = 0$. □

If H is a subgroup of G of finite index with a set S of coset representatives, and M is a G-module, then there is a natural map

$$\mathrm{Ind}_H^G(M) \to M, \qquad \varphi \mapsto \sum_{s \in S} s(\varphi(s^{-1})). \tag{14.4}$$

It is the composition of the inverse of Ψ of Proposition 14.4.7 with the map $\mathbf{Z}[G/H] \otimes M \to M$ that sends $C \otimes m$ to m. The map in (14.4) induces maps on cohomology, which composed with the isomorphisms of Shapiro's Lemma give the *corestriction maps*

$$\mathrm{Cor}\colon \mathrm{H}^i(H, M) \to \mathrm{H}^i(G, \mathrm{Ind}_H^G(M)) \to \mathrm{H}^i(G, M).$$

For $i = 0$ we can make this more concrete. By Exercise 14.4.4 we know that the isomorphism

$$M^H \cong \mathrm{H}^0(H, M) \to \mathrm{H}^0(G, \mathrm{Ind}_H^G(M)) \cong (\mathrm{Ind}_H^G(M))^G$$

of Shapiro's Lemma sends $x \in M^H$ to the constant function $g \mapsto x$. It follows that $\mathrm{Cor}\colon M^H \to M^G$ is given by $x \mapsto N_{G/H}(x)$, where $N_{G/H}(x) = \sum_{s \in S} sx$ is independent of the choice of S.

174: make $i = 0$ an exercise?

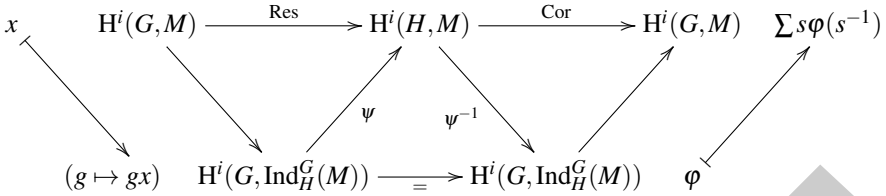
Proposition 14.4.9. *Let H be a subgroup of G of finite index n and let M be a G-module. Then the composition*

$$\mathrm{Cor} \circ \mathrm{Res}\colon \mathrm{H}^i(G, M) \to \mathrm{H}^i(G, M)$$

is multiplication by n.

Proof The restriction map Res is the composition of the map $\mathrm{H}^i(G, M) \to \mathrm{H}^i(G, \mathrm{Ind}_H^G(M))$ that is induced by the map $x \mapsto (g \mapsto gx)$ and the isomorphism

$\psi\colon \mathrm{H}^i(G,\mathrm{Ind}_H^G(M)) \to \mathrm{H}^i(H,M)$ from Shapiro's Lemma.



The corestriction map Cor is the composition of ψ^{-1} and the map $\mathrm{H}^i(G,\mathrm{Ind}_H^G(M)) \to \mathrm{H}^i(G,M)$ induced by $\varphi \mapsto \sum_{s\in S} s(\varphi(s^{-1}))$, where S is a set of coset representatives for G/H. Then the composition $\mathrm{Cor}\circ\mathrm{Res}$ is induced by the composition $M \to \mathrm{Ind}_H^G(M) \to M$ that is given by

$$x \mapsto (g \mapsto gx) \mapsto \sum_{s\in S} s(s^{-1}x) = \sum_s x = nx.$$

This proves the proposition. □

Proposition 14.4.10. *Suppose G is a finite group of order n. Then for all $i > 0$ the group $n\mathrm{H}^i(G,M)$ is trivial.*

Proof By Proposition 14.4.9, multiplication by n factors through $\mathrm{H}^i(\{1\},M) = 0$, cf. Milne (2008), Proposition II.1.31. □

Corollary 14.4.11. *If G is finite and M is finitely generated as an abelian group, then $\mathrm{H}^i(G,M)$ is finite.*

Proof The abelian groups $C^i(G,M)$ are finitely generated and therefore so are the groups $\mathrm{H}^i(G,M)$. By Proposition 14.4.10, the exponent of $\mathrm{H}^i(G,M)$ is a divisor of the order of G. The corollary follows immediately (cf. Milne, 2008, Corollary II.1.32). □

14.5 Cohomology of cyclic groups

We will see that when G is a cyclic group, we can compute the cohomology groups much more easily for (commutative) G-modules. Let G be a finite cyclic group of order n, say generated by σ. Much of what we will see depends on the choice of σ. Define the elements $\mathrm{N}, \Delta \in \mathbf{Z}[G]$ by

$$\mathrm{N} = \sum_{g\in G} g, \qquad \Delta = \sigma - 1.$$

For any G-module M we will also write N and Δ for the maps

$$m \mapsto \mathrm{N}m = \sum_{g \in G} gm \quad \text{and} \quad m \mapsto \Delta m = \sigma m - m$$

respectively. Let ${}_{\mathrm{N}}M$ and ${}_{\Delta}M$ denote the kernels of N and Δ, respectively. Note that ${}_{\Delta}M = M^G$.

Exercise 14.5.1. Show that a 1-cocycle $\varphi\colon G \to M$ is determined by the choice of $m = \varphi(\sigma)$. Show that the homomorphisms

$$s_1\colon M \to C^1(G,M), \quad (s_1(m))(\sigma^r) = \sum_{i=1}^{r} \sigma^i m$$
$$t_1\colon C^1(G,M) \to M, \quad t_1(\varphi) = \varphi(\sigma)$$

induce mutually inverse isomorphisms $\mathrm{H}^1(G,M) \rightleftharpoons {}_{\mathrm{N}}M/\Delta M$.

Exercise 14.5.2. Show that the homomorphisms

$$s_2\colon M \to C^2(G,M), \quad (s_2(m))(\sigma^i,\sigma^j) = \begin{cases} 0 & \text{if } i+j<n \\ m & \text{if } i+j \geq n \end{cases}$$
$$t_2\colon C^2(G,M) \to M, \quad t_2(\psi) = \sum_{i=0}^{n-1} \psi(\sigma^i,\sigma)$$

induce mutually inverse isomorphisms $\mathrm{H}^2(G,M) \rightleftharpoons M^G/\mathrm{N}M$.

These two isomorphisms are special cases of a more general construction, which we sketch for completeness. As referred to in Section 14.3, there are many ways of computing cohomology groups: any projective resolution of the G-module $\mathbf{Z}$ gives rise to a complex whose homology groups are isomorphic to $\mathrm{H}^i(G,M)$. As described by Milne (2008, Section II.1), the "standard" projective resolution of $\mathbf{Z}$ gives rise to the complex

$$C^0(G,M) \xrightarrow{d_0} C^1(G,M) \xrightarrow{d_1} C^2(G,M) \xrightarrow{d_2} C^3(G,M) \xrightarrow{d_3} \cdots$$

giving the calculation of $\mathrm{H}^i(G,M)$ in terms of cochains. On the other hand, when G is cyclic there is a more straightforward projective resolution of $\mathbf{Z}$ which gives rise to the complex

$$M \xrightarrow{\mathrm{N}} M \xrightarrow{\Delta} M \xrightarrow{\mathrm{N}} M \xrightarrow{\Delta} \cdots.$$

It follows from the fact that both resolutions of $\mathbf{Z}$ are projective that there are

homomorphisms s_i, t_i for $i \geq 1$, making the following diagram commute:

$$\begin{array}{ccccccccccc}
C^0(G,M) & \xrightarrow{d_0} & C^1(G,M) & \xrightarrow{d_1} & C^2(G,M) & \xrightarrow{d_2} & C^3(G,M) & \xrightarrow{d_3} & \cdots. \\
\| & & \uparrow s_1 \downarrow t_1 & & \uparrow s_2 \downarrow t_2 & & \uparrow s_3 \downarrow t_3 & & \\
M & \xrightarrow{\Delta} & M & \xrightarrow{\mathrm{N}} & M & \xrightarrow{\Delta} & M & \xrightarrow{\mathrm{N}} & \cdots
\end{array}$$

From here, it is a simple diagram-chase to verify that s_i, t_i induce mutually inverse isomorphisms between the homology groups of the two complexes. The reader can check that the homomorphisms defined in Exercises 14.5.1 and 14.5.2 do indeed make the diagram commute. Although we have only described the isomorphisms explicitly for $i = 1, 2$, they exist for all $i > 0$: for odd $i > 0$ there is an isomorphism $\mathrm{H}^i(G,M) \cong {}_{\mathrm{N}}M/\Delta M$ and for even $i > 0$ there is an isomorphism $\mathrm{H}^i(G,M) \cong {}_{\Delta}M/\mathrm{N}M$.

The maps s_i, t_i arose from comparing two projective resolutions of $\mathbf{Z}$ as a G-module, which did not depend on the module M. It follows that they enjoy many functorial properties, some of which we state in the following proposition.

Proposition 14.5.3. *Let G be a cyclic group with a fixed generator σ, and define* N *and* Δ *as above.*

(i) *Let $f\colon A \to B$ be a homomorphism of G-modules. Then the induced maps on cohomology make the following diagrams commute:*

$$\begin{array}{ccc}
\mathrm{H}^i(G,A) & \xrightarrow{f} & \mathrm{H}^i(G,B) \\
\cong \downarrow & & \downarrow \cong \quad \textit{for } i > 0 \textit{ odd;} \\
{}_{\mathrm{N}}A/\Delta A & \xrightarrow{f} & {}_{\mathrm{N}}B/\Delta B \\
\mathrm{H}^i(G,A) & \xrightarrow{f} & \mathrm{H}^i(G,B) \\
\cong \downarrow & & \downarrow \cong \quad \textit{for } i > 0 \textit{ even.} \\
A^G/\mathrm{N}A & \xrightarrow{f} & B^G/\mathrm{N}B
\end{array}$$

(ii) *Let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. Define a homomorphism*

$$\mathrm{N}_*\colon {}_{\mathrm{N}}C/\Delta C \longrightarrow A^G/\mathrm{N}A$$

as follows: given $c \in {}_{\mathrm{N}}C$, choose any lift $b \in B$ of c, and define $\mathrm{N}_*(c)$ to be $\mathrm{N}(b)$. This is well defined, and for any odd $i > 0$ the following diagram

commutes:

$$\begin{array}{ccc} \mathrm{H}^i(G,C) & \xrightarrow{\delta_i} & \mathrm{H}^{i+1}(G,A) \\ \cong\downarrow & & \downarrow\cong \\ {}_{\mathrm{N}}C/\Delta C & \xrightarrow{\mathrm{N}_*} & A^G/\mathrm{N}A \end{array} .$$

(iii) *Let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. Define a homomorphism*

$$\Delta_* : C^G/\mathrm{N}C \longrightarrow {}_{\mathrm{N}}A/\Delta A$$

as follows: given $c \in C^G$, choose any lift $b \in B$ of c, and define $\Delta_*(c)$ to be $\Delta(b) = \sigma b - b$. This is well defined, and for any even $i > 0$ the following diagram commutes:

$$\begin{array}{ccc} \mathrm{H}^i(G,C) & \xrightarrow{\delta_i} & \mathrm{H}^{i+1}(G,A) \\ \cong\downarrow & & \downarrow\cong \\ C^G/\mathrm{N}C & \xrightarrow{\Delta_*} & {}_{\mathrm{N}}A/\Delta A \end{array} .$$

Proof These are all straightforward exercises in diagram chasing. Those involving H^1 and H^2, which are the cases we will be using later, can also be checked using the explicit formulae of Exercises 14.5.1 and 14.5.2. □

Proposition 14.5.4. *Suppose that*

$$1 \to A \to B \to C \to 1$$

is an exact sequence of G-modules, where we view the map $A \to B$ as an injection. Then there is a long exact sequence

$$\begin{array}{ccccccc} 1 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G \\ & & & & & & \downarrow \\ & & & & {}_N A/\Delta A & \longrightarrow & {}_N B/\Delta B \longrightarrow {}_N C/\Delta C \\ & & & & \uparrow & & \downarrow \\ & & & & {}_\Delta C/NC & \longleftarrow & {}_\Delta B/NB \longleftarrow {}_\Delta A/NA \end{array}$$

of groups, where the left vertical arrows send c to Δb for any lift $b \in B$ of c, and the right vertical arrow sends c to Nb for any lift $b \in B$ of c.

Proof This is left as an exercise to the reader. □

Indeed, the long exact sequence of Proposition 14.5.4 is isomorphic to the usual long exact sequence of cohomology.

14.6 Noncommutative group cohomology

When A is a non-abelian group, but G still acts on A in the sense that there is a homomorphism $G \to \mathrm{Aut}A$, then some of the above still goes through. We say that A is a noncommutative G-module. Assume we are in that situation.

Definition 14.6.1. A 1-*cocycle* from G to A is a map $\varphi\colon G \to A$ that satisfies $\varphi(\sigma\tau) = \varphi(\sigma)\sigma(\varphi(\tau))$ for all $\sigma, \tau \in G$. Two 1-cocycles φ, ψ from G to A are called *cohomologous* if there exists an $a \in A$ such that for all $\sigma \in G$ we have $\psi(\sigma) = a^{-1}\varphi(\sigma)\sigma(a)$.

Definition 14.6.2. Let $\mathrm{H}^1(G,A)$ denote the pointed set of classes of cohomologous 1-cocycles, with the specified point being the class of the trivial cocycle φ satisfying $\varphi(g) = 1$ for all $g \in G$.

If M is abelian, then the notion of 1-cocycle is the same as before and two 1-cocycles are cohomologous if and only if they differ by a 1-coboundary; the new pointed set $\mathrm{H}^1(G,M)$ is therefore the underlying set of the group $\mathrm{H}^1(G,M)$ as defined before, together with the identity as specified point. Recall that a sequence

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

of pointed sets is called exact if $\mathrm{Im}\, f = g^{-1}(t)$, where t is the distinguished element of Z.

175: add connecting homs

Proposition 14.6.3. *Suppose that*

$$1 \to A \xrightarrow{\iota} B \to C \to 1$$

is an exact sequence of noncommutative G-modules. Then there is an exact sequence

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} \mathrm{H}^1(G,A) \to \mathrm{H}^1(G,B) \to \mathrm{H}^1(G,C)$$

of pointed sets, where δ sends $c \in C^G$ to the class of the 1-cocycle $G \to A$ given by $g \mapsto \iota^{-1}(b^{-1}g(b))$ for any lift $b \in B$ of c.

If, furthermore, $\iota(A)$ is in the centre of B, then there is a well-defined map $\Delta\colon \mathrm{H}^1(G,C) \to \mathrm{H}^2(G,A)$ of pointed sets sending the class of a 1-cocycle $\varphi\colon G \to C$ to the 2-cocycle

$$G^2 \to A, \qquad (g,h) \mapsto \iota^{-1}\big(\hat{\varphi}(g)g(\hat{\varphi}(h))(\hat{\varphi}(gh))^{-1}\big),$$

where $\hat{\varphi}\colon G \to B$ is any lift of φ. In this case the extended sequence

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} \mathrm{H}^1(G,A) \to \mathrm{H}^1(G,B) \to \mathrm{H}^1(G,C) \to \mathrm{H}^2(G,A)$$

of pointed sets is exact as well.

Proof See Serre (1968), Appendix to Chapter VII. □

As in the abelian case, given a normal subgroup H of G and a noncommutative G-module M, we can associate to every 1-cocycle $\varphi\colon G/H \to M^H$ a 1-cocycle $G \to M,\ g \mapsto \varphi(gH)$. This induces an inflation map

$$\mathrm{Infl}\colon \mathrm{H}^1(G/H, M^H) \to \mathrm{H}^1(G, M).$$

Exercise 14.6.4. Suppose G is a finite group. Suppose R is a ring on which G acts, and consider $M = R^*$ as a (possibly noncommutative) G-module. Suppose $\varphi\colon G \to M$ is a 1-cocycle. Take any $x \in R$ and set $a = \sum_{g\in G} \varphi(g) \cdot gx$. Show that we have an equality $\varphi(h) \cdot ha = a$ for all $h \in G$. Conclude that if a is invertible, then φ is cohomologous to 1.

Remark: This is a useful method to show that φ is cohomologous to 1 (or, equivalently in the abelian case, write φ as a 1-coboundary). If R has "enough units" then one can indeed choose x so that a is invertible. Sometimes it is possible to show this strategy works for any 1-cocycle so that we have $\mathrm{H}^1(G, M) = \{1\}$.

14.7 Galois cohomology

Let l/k be a Galois extension of fields with Galois group $G = \mathrm{Gal}(l/k)$, not necessarily finite. Let M be a (possibly noncommutative) G-module. For each finite extension k' of k that is contained in l we define

$$G_{k'} = \{g \in G \mid gx = x \text{ for all } x \in k'\}.$$

Clearly, $G_{k'}$ is normal.

For any normal subgroups H, H' of G with $H \subset H'$, the normal subgroup H'/H of G/H has quotient isomorphic to G/H', so we get inflation maps $\mathrm{H}^i(G/H', M^{H'}) \to \mathrm{H}^i(G/H, M^H)$. For a third normal subgroup H'' of G with $H' \subset H''$ we also get inflation maps $\mathrm{H}^i(G/H'', M^{H''}) \to \mathrm{H}^i(G/H', M^{H'})$. The compositions

$$\mathrm{H}^i(G/H'', M^{H''}) \to \mathrm{H}^i(G/H', M^{H'}) \to \mathrm{H}^i(G/H, M^H)$$

are the inflation maps $\mathrm{H}^i(G/H'', M^{H''}) \to \mathrm{H}^i(G/H, M^H)$. This means we have a system of compatible maps, of which we can consider those involving subgroups of finite index. For any integer $i \geq 0$ (with $i = 1$ if M is noncommutative) we define the *Galois cohomological* groups or pointed sets $\mathrm{H}^i(l/k, M)$ to

be the direct limit

$$\mathrm{H}^i(l/k,M) = \varinjlim \mathrm{H}^i(G/H, M^H),$$

where the direct limit runs over all finite-index normal subgroups H of G. Note that if G is finite, then $\mathrm{H}^i(l/k,M) = \mathrm{H}^i(G,M)$, so equivalently, we have

$$\mathrm{H}^i(l/k,M) = \varinjlim \mathrm{H}^i(k'/k, M^{\mathrm{Gal}(l/k')}),$$

where the direct limit runs over all finite field extensions k'/k. If l is a separable closure of k, then we also write $\mathrm{H}^i(k,M)$ for $\mathrm{H}^i(l/k,M)$. This notation is justified, as different separable closures l and l' give canonically isomorphic $\mathrm{H}^i(l/k,M)$ and $\mathrm{H}^i(l'/k,M)$ (see **?**, Section II.1.1)

Definition 14.7.1. Let M be a G-module. We say that the G-action on M is *continuous* if the equality

$$M = \bigcup_{k'} M^{\mathrm{Gal}(l/k')}$$

holds, where k' ranges over all finite Galois extensions of k that are contained in l.

Remark 14.7.2. To call the property above continuous would be perverse if there was no reason to do so. The group G is the inverse limit of the finite quotients G/H, where H runs over all finite-index normal subgroups H of G. In other words, it is the inverse limit of the groups $\mathrm{Gal}(k'/k)$, where k' runs over all finite Galois extensions of k that are contained in l. Taking the discrete topology on these finite groups, we endow G naturally with the smallest topology for which all quotient maps become continuous.

, the pro-finite topology, see (**?**, Section I.1) and (Milne, 2008, Section II.4). The open subgroups are exactly the groups fixing a finite subextension of k inside l. The action of G on M is continuous if and only if the stabilizer subgroups of each element of M is open. This is equivalent with saying that for every $m \in M$ there is a finite extension k' of k such that $\mathrm{Gal}(l/k')$ fixes m.

Remark 14.7.3. We warn the reader that if l is an infinite extension of k, then $\mathrm{H}^i(l/k,M)$ is not necessarily isomorphic to $\mathrm{H}^i(G,M)$, even when the action is continuous.

Assume that this is indeed the case, i.e., that we have

$$M = \bigcup_{k'} M^{\mathrm{Gal}(l/k')},$$

where k' ranges over all finite Galois extensions, so that G acts continuously on M. Then $\mathrm{H}^i(l/k,M)$ is isomorphic to $\mathrm{H}_{\mathrm{cts}}(G,M)$, where $\mathrm{H}^i_{\mathrm{cts}}(G,M)$ is as

defined at the end of Section 14.3. In particular, when M is commutative, this means that $\mathrm{H}^i(l/k,M)$ is isomorphic to the group of continuous i-cocycles modulo the coboundaries of continuous i-cochains. If M is noncommutative, then $\mathrm{H}^1(l/k,M)$ is the set of equivalence classes of continuous cocycles.

For the rest of this section we assume that every G-modules M satisfies

$$M = \bigcup_{k'} M^{\mathrm{Gal}(l/k')},$$

i.e., every element of M has a finite-index stabilizer in G, or, equivalently, that the action of G on M is continuous.

The groups $\mathrm{H}^i(l/k,M)$ are completely analogous to the usual cohomology groups $\mathrm{H}^i(G,M)$, and, as mentioned before, in fact equal when G is finite. In particular they form a functor from the category of discrete G-modules with continuous G-action to the category Ab of abelian groups and for $i=1$ a functor from the category of noncommutative G-modules with continuous G-action to the categories of pointed sets. Through the direct limits, inflation maps, restriction maps, and corestrictions maps are defined.

Almost all previous results about the functors $\mathrm{H}^i(G,\,\cdot\,)$ hold for the functors $\mathrm{H}^i(l/k,\,\cdot\,)$ as well, most of them without changes. For completeness, we cite the most important ones here in terms of Galois cohomology. These statements can be proved either by using the fact that taking direct limits commutes with taking cohomology (see Milne, 2008, Lemma II.4.1), or by redoing everything we did before in the category of discrete G-modules with continuous G-actions. For details we refer to (Milne, 2008, Section II.4) and (**?**, Section I.2).

Proposition 14.7.4. *Let M be a (not necessarily commutative) G-module. Then we have $\mathrm{H}^0(l/k,M) = M^G$. If the action of G on M is trivial, then $\mathrm{H}^1(l/k,M)$ equals the group or pointed set $\mathrm{Hom}_{cts}(G,M)$ of continuous homomorphisms from G to M.*

Example 14.7.5. Let k be any field, and consider the abelian group $\mathbf{Z}$ with trivial action of $\mathrm{Gal}(\bar{k}/k)$. For any finite extension ℓ/k, we have

$$\mathrm{H}^1(\ell/k,\mathbf{Z}) = \mathrm{Hom}(\mathrm{Gal}(\ell/k),\mathbf{Z}) = 0$$

as there are no non-constant homomorphisms from a finite group to $\mathbf{Z}$. Taking limits, it follows that

$$\mathrm{H}^1(k,\mathbf{Z}) = \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\bar{k}/k),\mathbf{Z}) = 0.$$

On the other hand, it is quite possible that $\mathrm{Hom}(\mathrm{Gal}(\bar{k}/k),\mathbf{Z})$, the set of *not*

necessarily continuous homomorphisms from the absolute Galois group of k to $\mathbf{Z}$, is non-trivial. For example, ...

176: Find an example!

Proposition 14.7.6. *Let*

$$0 \to A \to B \to C \to 0$$

be a short exact sequence of G-modules. Then there exist connecting homomorphisms $\delta_i \colon \mathrm{H}^i(G,C) \to \mathrm{H}^{i+1}(G,A)$ *inducing a long exact sequence*

$$\begin{aligned} 0 \to & A^G \to B^G \to C^G \xrightarrow{\delta_0} \\ & \mathrm{H}^1(G,A) \to \mathrm{H}^1(G,B) \to \mathrm{H}^1(G,C) \xrightarrow{\delta_1} \\ & \mathrm{H}^2(G,A) \to \mathrm{H}^2(G,B) \to \mathrm{H}^2(G,C) \xrightarrow{\delta_2} \\ & \dots \end{aligned} \tag{14.5}$$

□

Proposition 14.7.7. *For each j in a given index set J, let M_j be a G-module. Then for each i we have a natural isomorphism*

$$\mathrm{H}^i(l/k, \bigoplus_{j\in J} M_j) \to \bigoplus_{j\in J} \mathrm{H}^i(l/k, M_j).$$

□

If k'/k is a finite extension, then $H = \mathrm{Gal}(\bar{k}/k')$ is of finite index in $G = \mathrm{Gal}(\bar{k}/k)$. For an H-module M, we can therefore define the induced module $\mathrm{Ind}_H^G(M)$. To simplify notation, in this situation we will write $\mathrm{Ind}_{k'/k} M$ for $\mathrm{Ind}_H^G M$.

Exercise 14.7.8. Let X be a smooth variety over a field k. In this exercise we look at the structure of $\mathrm{Div}\,\bar{X}$ as a Galois module.

(i) Let Z be a prime divisor on X. Over $\bar{k}$, Z may split into several irreducible components; call them Z_i $(i = 1, \dots, n)$. Define $\mathrm{Div}_Z \bar{X}$ to be the subgroup of $\mathrm{Div}\,\bar{X}$ generated by the Z_i; that is, $\mathrm{Div}_Z \bar{X} = \bigoplus_{i=1}^n \mathbf{Z} Z_i$. Show that, as Galois modules,

$$\mathrm{Div}\,\bar{X} = \bigoplus_Z \mathrm{Div}_Z \bar{X}$$

where the sum is over all prime divisors Z on X.

(ii) Let G denote $\mathrm{Gal}(\bar{k}/k)$. Fix a prime divisor Z on X; as above, let Z_1 be one chosen irreducible component of Z over $\bar{k}$, and let $H \subset G$ be the subgroup fixing Z_1. By **??**, the fixed field k' of H is the minimal subfield of $\bar{k}$ over which Z_1 is defined. Using Exercise 14.4.6 and Proposition 14.4.7, show

that $\mathrm{Div}_Z X$ is an induced module: $\mathrm{Div}_Z X \cong \mathrm{Ind}_{k'/k} \mathbf{Z}$, where $\mathbf{Z}$ carries the trivial action of $H = \mathrm{Gal}(\bar{k}/k')$.

(iii) Deduce that $\mathrm{H}^1(k, \mathrm{Div}\,\bar{X})$ is trivial, and that there is an isomorphism $\mathrm{H}^2(k, \mathrm{Div}\,\bar{X}) \cong \mathrm{H}^2(k', \mathbf{Z})$.

Proposition 14.7.9. *Let k' be a Galois extension of k that is contained in l, and let M be a G-module. Let $r > 0$ be an integer. If $\mathrm{H}^i(l/k', M) = 0$ for all $0 < i < r$, then the sequence*

177: need k'/k to be finite?

$$0 \to \mathrm{H}^r(k'/k, M^{\mathrm{Gal}(l/k')}) \xrightarrow{\mathrm{Infl}} \mathrm{H}^r(l/k, M) \xrightarrow{\mathrm{Res}} \mathrm{H}^r(l/k', M)$$

is exact. □

Proposition 14.7.10. *Let k' be a field extension of k of degree n that is contained in l. Let M be a G-module. Then the composition*

178: need reference to k' in notation of Res and Cor?

$$\mathrm{Cor} \circ \mathrm{Res} \colon \mathrm{H}^i(l/k, M) \to \mathrm{H}^i(l/k, M)$$

is multiplication by n. □

Proposition 14.7.11. *Suppose that*

$$1 \to A \xrightarrow{\iota} B \to C \to 1$$

is an exact sequence of noncommutative G-modules. Then there is an exact sequence

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} \mathrm{H}^1(l/k, A) \to \mathrm{H}^1(l/k, B) \to \mathrm{H}^1(l/k, C)$$

of pointed sets. If, furthermore, $\iota(A)$ is in the centre of B, then there is a well-defined map $\Delta \colon \mathrm{H}^1(l/k, C) \to \mathrm{H}^2(l/k, A)$ of pointed sets In this case the extended sequence

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} \mathrm{H}^1(l/k, A) \to \mathrm{H}^1(l/k, B) \to \mathrm{H}^1(l/k, C) \to \mathrm{H}^2(l/k, A)$$

of pointed sets is exact as well. □

Proposition 14.7.12. *Suppose that M a permutation G-module. Then the group $\mathrm{H}^1(l/k, M)$ is trivial.* □

179: is this ok?

The following two propositions are often referred to as Hilbert 90. They can be proved using the strategy presented at the beginning of this section.

Proposition 14.7.13. *We have $\mathrm{H}^1(l/k, l^*) = 0$.*

Proof For finite extensions, see Milne (2008), Prop. II.1.22. For infinite extensions it then follows immediately as well, as we have $(l^*)^{\mathrm{Gal}(l/k')} = k'^*$ for any subfield k' of l containing k. □

Proposition 14.7.14. *If k^{sep} denotes a separable closure of k, then we have $\mathrm{H}^1(k, \mathrm{GL}_n(k^{\mathrm{sep}})) = 0$ for any positive integer n.*

180: find proof (also for general l instead of k^{sep}?)

Exercise 14.7.15. Suppose k is a perfect field and μ_n is the group of all n-th roots of unity in k^{sep}. Show that there is a natural isomorphism $k^*/(k^*)^n \to \mathrm{H}^1(k, \mu_n)$.

Proposition 14.7.16. *When k is a number field, we have $\mathrm{H}^3(k, \bar{k}^*) = 0$.*

181: find proof

Instead of the multiplicative group, one can also consider the additive group.

Proposition 14.7.17. *We have $\mathrm{H}^i(l/k, l) = 0$ for any $i > 0$.*

Proof For finite extensions, see Milne (2008), Prop. II.1.24. For infinite extensions it then follows immediately as well. □

14.8 Twists

Let k be a field and let l be an extension of k. To start vaguely, an l/k-twist of a fixed object X over k is an object A over k such that the base extensions X_l and A_l to l are isomorphic. Here an object over k could be anything for which this idea makes sense, such as an elliptic curve over k, a variety over k, a k-algebra, a k-vector space, or a central simple algebra over k.

We continue more precisely. Let *object* denote one of the notions elliptic curve, variety, algebra, vector space, central simple algebra, or scheme. For any field K, let $\mathscr{C}_K$ denote the category of objects over K; for any field extension L of K, let the base extension functor $\mathscr{C}_K \to \mathscr{C}_L$ be denoted by $X \mapsto X_L$.

Definition 14.8.1.

14.9 Brauer groups

Finally the reason why we care about all of this. It turns out that the Brauer group defined earlier can in fact be expressed as a galois cohomology group.

Let A be a central simple algebra over a perfect field k with algebraic closure $\bar{k}$. Write $G = \mathrm{Gal}(\bar{k}/k)$. Then over the algebraic closure there is an isomorphism

$$\varphi \colon M_r(\bar{k}) \to A \otimes_k \bar{k}.$$

We get a 1-cocycle $\xi \in \mathrm{H}^1(G, \mathrm{Aut}_{\bar{k}\text{-algebras}}(M_r(\bar{k}))$ by setting $\xi(\sigma) = \varphi^{-1}({}^{\sigma}\varphi)$.

Since every automorphism of a matrix algebra is inner, we get $\mathrm{Aut}_{\bar{k}\text{-algebras}}(M_r(\bar{k})) \cong \mathrm{PGL}_r(\bar{k})$, so $\xi \in \mathrm{H}^1(G, \mathrm{PGL}_r(\bar{k}))$. From the exact sequence

$$1 \to \bar{k}^* \to \mathrm{GL}_r(\bar{k}) \to \mathrm{PGL}_r(\bar{k}) \to 1$$

we get a map $\mathrm{H}^1(G, \mathrm{PGL}_r(\bar{k})) \to \mathrm{H}^2(G, \bar{k}^*)$, so we can map ξ to $\mathrm{H}^2(G, \bar{k}^*)$.

Proposition 14.9.1. *The map taking the central simple algebra A to the image of ξ in $\mathrm{H}^2(G, \bar{k}^*)$ induces an isomorphism $\mathrm{Br}\, k \to \mathrm{H}^2(G, \bar{k}^*)$.*

Proof See Serre (1968), X, §5, or Poonen (2008), Thm. 1.5.3. □

Exercise 14.9.2 (*)**.** Prove that any r^2-dimensional central simple algebra gives rise to an element of the Brauer group killed by r.

The above relates the Brauer group of a field to a Galois cohomological group. For a scheme X we have the following.

Proposition 14.9.3. *Let X be a regular, integral, quasi-compact scheme. Then there is an injection $\mathrm{Br}\, X \to \mathrm{Br}\, k(X)$.*

Proof See Milne (1980), III.2.22. □

Proposition 14.9.4. *long exact sequence containing ... ????*

14.10 Galois descent and divisor classes

In this section we study two problems of algebraic geometry where Galois cohomology arises in a very natural way. If K/k is a finite Galois extension, the two problems are:

- given a subvariety X of $\mathbf{P}^n_K$ which is fixed by the Galois action, to find defining equations for X with coefficients in k;
- given a variety X defined over k and a divisor class in $\mathrm{Pic}\, X$ fixed by the Galois action, to find (if possible) a divisor defined over k representing that class.

Both problems come down to understanding Galois actions on finite-dimensional vector spaces over K, so we begin by describing some results in that area. A good reference is Gille and Szamuely (2006, Section 2.3).

The first important observation is that a vector space over K does not automatically come equipped with a Galois action; rather, there are many possible Galois actions. The vector space K^n, of course, does have a canonical Galois

action, given by acting on each coordinate separately. Now, given a finite-dimensional vector space W over K, choosing a basis for W is the same as fixing an isomorphism $K^n \to W$, and so induces a Galois action. Explicitly, let $w_1, \dots, w_n$ be a basis for W; then the induced Galois action is

$$\sigma(a_1 w_1 + \cdots + a_n w_n) = \sigma(a_1) w_1 + \cdots + \sigma(a_n) w_n \qquad \text{for any } \sigma \in \mathrm{Gal}(K/k).$$

We will call this Galois action the *coordinate action* induced by the basis.

Definition 14.10.1. Let K/k be a Galois extension of fields, and let W be a vector space over K. An action of $\mathrm{Gal}(K/k)$ on W is *semi-linear* if

$$\sigma(aw) = \sigma(a)\sigma(w) \text{ for all } a \in K \text{ and } w \in W.$$

In particular, the coordinate action induced by any basis of K is semi-linear.

Another feature of the coordinate action associated to a basis $w_1, \dots, w_n$ of W is that the subset of W fixed by the coordinate action is precisely the k-span of $w_1, \dots, w_n$. So the same vectors form a K-basis for W, and a k-basis for $W^{\mathrm{Gal}(K/k)}$. This observation may be expressed in different ways.

Lemma 14.10.2. *Let K/k be a finite extension; let W be a vector space over K of dimension n, and V a sub-k-vector space of W. The following are equivalent:*

(i) *any k-basis of V is also a K-basis of W;*
(ii) *V is of dimension n over k, and spans W as a K-vector space;*
(iii) *the k-linear map $\phi\colon V \otimes_k K \to W$ defined by $\phi(v \otimes a) = av$ is an isomorphism.*

Proof (i)⇒(ii) is easy. To show (ii)⇒(i), let $v_1, \dots, v_n$ be a k-basis for V. By assumption, any $w \in W$ can be expressed as a K-linear combination of elements of V, which can themselves be expressed as k-linear combinations of $v_1, \dots, v_n$. So $v_1, \dots, v_n$ span W as a K-vector space; since there are n of them, they form a basis.

To prove (ii)⇔(iii), let w be any element of W. For all $a_1, \dots, a_r$ in K and all $v_1, \dots, v_r$ in V we have $a_1 v_1 + \cdots + a_r v_r = \phi(v_1 \otimes a_1 + \cdots + v_r \otimes a_r)$; so the K-span of V coincides with the image of ϕ. We deduce that V spans W if and only if ϕ is surjective. On the other hand, there are equalities

$$\dim_k(V \otimes_k K) = [K : k] \dim_k V \quad \text{and} \quad \dim_k W = [K : k]n,$$

so $\dim_k V$ is n if and only if the two vector spaces in (iii) have the same dimension over k. Since a surjective linear map of finite-dimensional vector spaces is an isomorphism if and only if the spaces have the same dimension, we deduce the equivalence (ii)⇔(iii). □

The main result in this section is that any semi-linear action of $\mathrm{Gal}(K/k)$ on W arises as above from some choice of basis.

Lemma 14.10.3 (Speiser)**.** *Let K/k be a finite Galois extension, and let W be a vector space over K equipped with a semi-linear action of* $\mathrm{Gal}(K/k)$*. Then the natural map $W^{\mathrm{Gal}(K/k)} \otimes_k K \to W$ is an isomorphism.*

Proof See Gille and Szamuely (2006, Lemma 2.3.8). □

Corollary 14.10.4. *Under the hypotheses of Lemma 14.10.3, let $v_1, \dots, v_n$ be a k-basis for $W^{\mathrm{Gal}(K/k)}$. Then $v_1, \dots, v_n$ also form a K-basis for W, and the Galois action on W is the coordinate action induced by this basis.*

Proof By Lemma 14.10.2, the vectors $v_1, \dots, v_n$ do indeed form a K-basis for W; so any $w \in W$ can be written as $w = a_1 v_1 + \cdots + a_n v_n$ for some $a_i \in K$. By semi-linearity of the action, we have

$$\sigma(w) = \sigma(a_1)\sigma(v_1) + \cdots + \sigma(a_n)\sigma(v_n) = \sigma(a_1)v_1 + \cdots + \sigma(a_n)v_n$$

for any $\sigma \in \mathrm{Gal}(K/k)$; that is, the Galois action is the coordinate action. □

As an application, we prove Proposition 6.1.9 in the case that k'/k is Galois.

Partial proof of Proposition 6.1.9 Suppose that k'/k is Galois. Since $D_{k'}$ is fixed by the action of $\mathrm{Gal}(k'/k)$, the natural semi-linear action of $\mathrm{Gal}(k'/k)$ on $\kappa(X_{k'})$ fixes $L(D_{k'})$ and so restricts to a semi-linear action on $L(D_{k'})$. By Lemma 14.10.3, any k-basis for $L(D_{k'})^{\mathrm{Gal}(k'/k)}$ is also a k'-basis for $L(D_{k'})$. □

182: Need to do the first problem.

Now let us turn to our second problem. Let X be a smooth, geometrically irreducible variety over a field k, let K/k be a finite Galois extension with Galois group G, and let $\alpha \in (\mathrm{Pic}\, X_K)^G$ be a divisor class fixed by the Galois action. We wish to determine whether there is a Galois-fixed divisor in the class α and, if there is, to find one.

The class α will be represented by a divisor $D \in \mathrm{Div}\, X_K$. For what follows, it will be helpful to assume that D is effective. We may do that, since it is certainly possible to find a Galois-fixed divisor E such that $D+E$ is effective; for example, we could take E to be the norm of the sum of the negative components of D. Then the class of $D+E$ contains a Galois-fixed divisor if and only if the class of D does.

The condition that α be fixed by the Galois action means that $\sigma D \sim D$ for all $\sigma \in G$. In other words, for each $\sigma \in G$, there exists a function f_σ such that $(f_\sigma) = \sigma D - D$. We can regard the collection of functions (f_σ) as a 1-cochain with values in $\kappa(X_K)^\times$; this cochain is not too far from being a 1-cocycle,

as may be seen by computing the coboundary $\phi(\sigma,\tau) = f_\sigma \sigma(f_\tau)/f_{\sigma\tau}$. The divisor of $\phi(\sigma,\tau)$ is

$$(\sigma D - D) + \sigma(\tau D - D) - (\sigma\tau D - D) = 0$$

and therefore, since X is projective, $\phi(\sigma,\tau)$ takes values in $K^\times$. Moreover, since ϕ is the coboundary of a cochain, we automatically have that ϕ is a 2-cocycle. (The possibly confusing thing here is that ϕ is a cocycle regardless of whether we view ϕ as taking values in $\kappa(X_K)^\times$ or in $K^\times$. On the other hand, whether ϕ is a coboundary very much depends on the group: by construction, ϕ is the coboundary of a cochain with values in $\kappa(X_K)^\times$, but it is quite possible that ϕ is not the coboundary of a cochain with values in $K^\times$.)

The functions f_σ are each defined only up to a constant multiple. Replacing each f_σ by a constant multiple will change ϕ by the coboundary of a 1-cochain with values in $K^\times$, and so it is the *class* of ϕ in $\mathrm{H}^2(K/k,K^\times)$ which is important.

183: What happens to ϕ if we replace D by an equivalent divisor?

Proposition 14.10.5. *Let K/k be a finite Galois extension. Let X be a smooth, geometrically irreducible, projective variety over k, and let D be a divisor on X_K whose class in* $\mathrm{Pic}\, X_K$ *is fixed by the natural Galois action. Let $(f_\sigma)_{\sigma\in G}$ be any functions satisfying $(f_\sigma) = \sigma D - D$, and define $\phi(\sigma,\tau) = f_\sigma \sigma(f_\tau)/f_{\sigma\tau}$. Then there is a Galois-fixed divisor equivalent to D if and only if ϕ is the coboundary of a 1-cochain with values in $K^\times$, that is, if and only if the class of ϕ in $\mathrm{H}^2(K/k,K^\times)$ is trivial.*

Proof Suppose first that ϕ is a coboundary; we will construct a Galois-fixed divisor equivalent to D. Let $\psi \in C^1(G,K^\times)$ be a 1-cochain such that $\delta\psi = \phi$, and define functions $g_\sigma = f_\sigma/\psi(\sigma)$. Then, by construction, the collection g_σ forms a 1-cocycle with values in $\kappa(X_K)^\times$.

Let $L(D)$ be the vector space over K defined in (6.1); this vector space (modulo constants) can be identified with the set of effective divisors equivalent to D, by sending the function $f \in L(D)$ to the divisor $(f) + D$. Because D is effective, the vector space $L(D)$ is non-zero. We define a *twisted action* of G on $L(D)$ by $(\sigma, f) \mapsto g_\sigma \sigma(f)$. It is easy to check that this is indeed a group action: firstly, if $f \in L(D)$ then $g_\sigma\sigma(f)$ also lies in $L(D)$; and, secondly, the action of $\sigma\tau$ is the same as the action of τ followed by the action of σ, which is a consequence of the fact that the g_σ form a cocycle. Moreover, this action is semi-linear. It is easily verified that, for any $f \in L(D)$ fixed by the twisted action, the divisor $(f) + D$ is a Galois-fixed divisor equivalent to D; in other words, the subset of $L(D)$ fixed by our twisted Galois action corresponds to those effective divisors, linearly equivalent to D, which are Galois-fixed in the usual sense. Now Lemma 14.10.3 shows that the subset of $L(D)$ fixed by the

twisted action is of dimension $\ell(D)$ over k, and in particular contains a non-zero element f; so $(f)+D$ is a Galois-fixed divisor linearly equivalent to D, as desired.

Conversely, suppose that there is a Galois-fixed divisor E linearly equivalent to D. Then there is a function $f \in \kappa(X_K)^\times$ such that $(f) = D - E$. As remarked above, choosing different functions f_σ only changes ϕ by a coboundary. In this case, we can choose $f_\sigma = \sigma f / f$, leading to $\phi(\sigma,\tau) = 1$ for all $\sigma,\tau \in G$. Since this ϕ is a coboundary (of the 1-cocycle which is also identically 1), it follows that the ϕ corresponding to any choice of f_σ is also a coboundary. □

184: Maybe say something about the cyclic case?

- Mention that if L/k is cyclic, then there is a sequence

$$k^\times / N(L^\times) \cong \hat{\mathrm{H}}^0(L/k, L^\times) \cong \hat{\mathrm{H}}^2(L/k, L^\times) = \ker(\mathrm{Br}\, k \to \mathrm{Br}\, L)$$

  that sends a to the cyclic algebra $\pm(L,\sigma,a)$ where the second isomorphism depends on the choice of the generator σ of $\mathrm{Gal}(L/k)$.
- Check example with discrete vs profinite topology.
- Map GL_n-torsors to $\mathbf{P}GL_n$-torsors via End (where appropriate).
- Brauer groups of $\mathbf{R}$ and $\mathbf{Q}_p$.
- If $k \subset K$, define $\mathrm{H}^2(k, k^\times) \to \mathrm{H}^2(K, K^\times)$ and show that it agrees with the map $\mathrm{Br}\, k \to \mathrm{Br}\, K$, $A \mapsto A \otimes K$.
- $\mathrm{H}^3(k, \bar{k}^\times) = 0$ for a number field k.

15

The Brauer group and cohomology

In this chapter we look at how the techniques of Galois cohomology can be used to find explicit elements of the Brauer group of a variety.

185: [Mention references, examples.]

We begin by relating the Brauer group to some Galois cohomology groups. In particular, we define a *residue map* which allows us to describe the Brauer group of a discrete valuation ring as a subgroup of the Brauer group of its field of fractions. Using the residue map, we obtain a complete description of the Brauer group of a local field. We also use the residue maps to give a description, in terms of Galois cohomology, of the *algebraic* part of the Brauer group of a variety. For more information on the transcendental part of the Brauer group, it would be necessary to use the more general techniques of étale cohomology, which will not be discussed in this book.

15.1 Residue maps

Let X be a smooth, irreducible variety over a field k of characteristic 0. The Brauer group of X is the subgroup of the Brauer group of the function field X consisting of those elements which are unramified at all points of X; as a consequence of the Purity Theorem we saw, in Theorem 12.2.8, that $\mathrm{Br}X$ is also the subgroup of $\mathrm{Br}\,\kappa(X)$ consisting of those elements unramified at all *divisors* on X. Let us now give a cohomological description of what it means for an element of $\mathrm{Br}\,\kappa(X)$ to be unramified at a divisor.

15.1.1 The group $\mathrm{H}^2(G,\mathbf{Z})$

186: Probably move this to the cohomology chapter

For any finite group G, the second cohomology group $\mathrm{H}^2(G,\mathbf{Z})$ is naturally isomorphic to the character group $\mathrm{Hom}(G,\mathbf{Q}/\mathbf{Z})$; in this section, we will prove this, and explicitly describe the isomorphism in terms of cocycles.

Fix a finite group G. Consider the exact sequence of G-modules with trivial action

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0. \tag{15.1}$$

For any positive integer n, the multiplication-by-n map $\mathbf{Q} \xrightarrow{\times n} \mathbf{Q}$ is an isomorphism. It follows that, for any finite group G of order dividing n acting trivially on $\mathbf{Q}$, the induced map on cohomology groups

$$\mathrm{H}^i(G,\mathbf{Q}) \xrightarrow{\times n} \mathrm{H}^i(G,\mathbf{Q})$$

is an isomorphism for any $i > 0$; combining this with Proposition 14.4.10, we deduce that it is also the zero map, and so $\mathrm{H}^i(G,\mathbf{Q}) = 0$ for all $i > 0$. It therefore follows from the exact sequence (15.1) that there are isomorphisms $\delta_i \colon \mathrm{H}^i(G,\mathbf{Q}/\mathbf{Z}) \to \mathrm{H}^{i+1}(G,\mathbf{Z})$ for all $i \geq 1$. Taking $i = 1$, we obtain the following proposition.

Proposition 15.1.1. *Let G be a finite group, acting trivially on the G-module $\mathbf{Z}$. Then there is an isomorphism*

$$\mathrm{Hom}(G,\mathbf{Q}/\mathbf{Z}) \cong \mathrm{H}^2(G,\mathbf{Z}).$$

Proof This follows from the above discussion, together with the fact, proved in Exercise 14.2.5, that $\mathrm{H}^1(G,\mathbf{Q}/\mathbf{Z})$ can be identified with $\mathrm{Hom}(G,\mathbf{Q}/\mathbf{Z})$. □

Let us give an explicit description of this isomorphism. Fix a finite group G and a homomorphism $\alpha \colon G \to \mathbf{Q}/\mathbf{Z}$, which we consider as a 1-cocycle. By the description (14.2) of the connecting homomorphism $\delta \colon \mathrm{H}^1(G,\mathbf{Q}/\mathbf{Z}) \to \mathrm{H}^2(G,\mathbf{Z})$, we compute $\delta\alpha$ by first lifting α to a function $\hat{\alpha} \colon G \to \mathbf{Q}$, which is in general not a homomorphism, and then setting

$$\delta\alpha(g_1,g_2) = g_1\hat{\alpha}(g_2) + \hat{\alpha}(g_1) - \hat{\alpha}(g_1g_2).$$

Since α was a homomorphism, it is easy to see that $\delta\alpha$ takes values in $\mathbf{Z}$. As the action of G is trivial, the equation above simplifies to

$$\delta\alpha(g_1,g_2) = \hat{\alpha}(g_2) + \hat{\alpha}(g_1) - \hat{\alpha}(g_1g_2). \tag{15.2}$$

As a particular case of this calculation, we deduce the following result.

Proposition 15.1.2. *Let G be a cyclic group of order n, and fix a generator g of G. Then the function $\phi \colon G^2 \to \mathbf{Z}$ defined by*

$$\phi(g^i,g^j) = \begin{cases} 0 & \text{if } i+j < n; \\ 1 & \text{if } i+j \geq n; \end{cases}$$

is a 2-cocycle, the class of which generates $\mathrm{H}^2(G,\mathbf{Z})$.

Proof The group $\mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$ is cyclic, generated by the homomorphism $\alpha\colon G \to \mathbf{Q}/\mathbf{Z}$ defined by $\alpha(g) = 1/n$. It follows from Proposition 15.1.1 that $\mathrm{H}^2(G, \mathbf{Z})$ is also cyclic of order n; all that remains is to prove that the class of ϕ is a generator. A lift of α to $\mathbf{Q}$ is the map $\hat{\alpha}\colon G \to \mathbf{Q}$ such that $\hat{\alpha}(g^i) = i/n$ when $0 \leq i < n$. Applying the formula (15.2) and setting $\phi := \delta\alpha$ then gives the result. □

For now, let R be a *complete* discrete valuation ring with field of fractions K and residue field k, which we suppose to be perfect. (In particular, this is true if k is finite, or if k has characteristic zero.) In this context, we can define a *residue map*, which is a homomorphism from $\mathrm{Br}\, K$ to $\mathrm{H}^1(k, \mathbf{Q}/\mathbf{Z})$. Later, we will apply this to the discrete valuation associated to a divisor D on a smooth variety X. The residue map at D carries information about how an algebra over the function field of X ramifies along D; in particular, we will see that the unramified algebras, those in the Brauer group of X, are precisely those having trivial residue along every divisor. We follow the treatment given by Colliot-Thélène and Swinnerton-Dyer (1994).

Proposition 15.1.3. *Let R be a complete discrete valuation ring with field of fractions K and perfect residue field k. Let A be a central simple algebra over K. Then there is a finite, unramified extension of K which splits A.*

Proof Several different proofs are available in the literature. A direct proof is given by Serre (1968, XII.2) of the following more specific fact: that A contains a maximal subfield which is unramified over K. □

Note that, when k is perfect, an unramified extension L/K is necessarily separable: this can be seen by looking at the trace form on L.

Remark 15.1.4. In Lemma 3.4 of Auslander and Brumer (1968), it is shown that Proposition 15.1.3 holds without the assumption that R is complete, though in that case the unramified splitting field is not necessarily contained in A.

Let A be a central simple algebra over K. By Proposition 15.1.3, there is a finite, unramified extension L/K over which A splits. Taking the normal closure, we may assume that L/K is Galois, so that the class of A defines a cohomology class in $\mathrm{H}^2(L/K, L^\times) \subset \mathrm{H}^2(K, \bar{K}^\times)$. Let $v_L\colon L^\times \to \mathbf{Z}$ be the valuation on L; as this map respects the Galois action, there is an induced map on cohomology

$$\mathrm{H}^2(L/K, L^\times) \longrightarrow \mathrm{H}^2(L/K, \mathbf{Z}).$$

Next, Proposition 15.1.1 gives an isomorphism

$$\delta\colon \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbf{Q}/\mathbf{Z}) = \mathrm{H}^1(L/K, \mathbf{Q}/\mathbf{Z}) \to \mathrm{H}^2(L/K, \mathbf{Z}).$$

Finally, since L/K is unramified, there is a natural isomorphism of Galois groups $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k)$, where ℓ is the residue field of L. Putting these various maps together as follows, we obtain the residue map.

Definition 15.1.5. Let R be a complete discrete valuation ring with field of fractions K and perfect residue field k, and let L be a finite, unramified, Galois extension of K with residue field ℓ. The *residue map* $\partial_{R,L}\colon \mathrm{Br}(L/K) \to \mathrm{H}^1(\ell/k, \mathbf{Q}/\mathbf{Z})$ is the composition

$$\mathrm{Br}(L/K) \cong \mathrm{H}^2(L/K, L^\times) \xrightarrow{v_L} \mathrm{H}^2(L/K, \mathbf{Z}) \xrightarrow{\delta^{-1}} \mathrm{H}^1(L/K, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\sim} \mathrm{H}^1(\ell/k, \mathbf{Q}/\mathbf{Z})$$

where v_L and δ are as above.

Exercise 15.1.6. Let n denote the degree $[L:K]$, and let π be a uniformising element in K. Show that the homomorphism $\mathrm{H}^1(\ell/k, \mathbf{Q}/\mathbf{Z}) \to \mathrm{H}^2(L/K, L^\times)$ defined by $\chi \mapsto \pi \cup \delta\chi$ is a right inverse to $\partial_{R,L}$.

If L' is another finite, unramified, Galois extension of K containing L, with residue field ℓ', then $v_{L'}$ restricts to v_L on L, and it follows that the diagram

$$\begin{array}{ccc} \mathrm{H}^2(L'/K, (L')^\times) & \xrightarrow{\partial_{R,L'}} & \mathrm{H}^1(\ell'/k, \mathbf{Q}/\mathbf{Z}) \\ \mathrm{Infl}\uparrow & & \mathrm{Infl}\uparrow \\ \mathrm{H}^2(L/K, L^\times) & \xrightarrow{\partial_{R,L}} & \mathrm{H}^1(\ell/k, \mathbf{Q}/\mathbf{Z}) \end{array}$$

commutes. As L ranges through all finite, unramified extensions of K, so ℓ ranges through all finite extensions of k; taking the limit, the residue maps $\partial_{R,L}$ therefore induce a map from $\mathrm{Br}\, K$ to $\mathrm{H}^1(k, \mathbf{Q}/\mathbf{Z})$.

187: Do we need to justify this more?

Definition 15.1.7. Let R be a complete discrete valuation ring, with field of fractions K and perfect residue field k. The *residue map* associated to R is the group homomorphism

$$\partial_R\colon \mathrm{Br}\, K \longrightarrow \mathrm{H}^1(k, \mathbf{Q}/\mathbf{Z})$$

which is the limit of the residue maps $\partial_{R,L}$ as L varies over all finite, unramified extensions of K.

More explicitly, suppose that R and K are as in Definition 15.1.7, and that we are given a central simple algebra A over K. By Proposition 15.1.3, there is a finite, unramified extension of K that splits A. Taking the normal closure, let L/K be a finite, unramified, Galois extension splitting A, and let ℓ be the residue field of L; then $\partial_R(A)$ is the image of $\partial_{R,L}(A)$ under the (injective) inflation homomorphism $\mathrm{H}^1(\ell/k, \mathbf{Q}/\mathbf{Z}) \to \mathrm{H}^1(k, \mathbf{Q}/\mathbf{Z})$.

Example 15.1.8. Take R to be $\mathbf{Q}[[t]]$, the ring of formal power series in the variable t with coefficients in $\mathbf{Q}$, so that K is $\mathbf{Q}((t))$, the corresponding field of formal Laurent series. Consider the quaternion algebra $A = (2,t)_K$. There are two obvious field extensions of K contained in A: the field $L = K(\sqrt{2}) = \mathbf{Q}(\sqrt{2})((t))$; and the field $L' = K(\sqrt{t}) = \mathbf{Q}((s))$, where $s^2 = t$. (There are also many other quadratic extensions of K contained in A, but these two are sufficient for this example.) Of these field extensions, the second is ramified: a uniformising element in L' is s, and by the relation $t = s^2$ we see that $v_{L'}(t) = 2$. On the other hand, L is unramified over K, as t is a uniformising element in L and so $v_L(t) = 1$. We may therefore use the extension L/K to compute the residue of A.

Let G be the Galois group of L/K, which is cyclic of order 2, and let g be the generator of G. By Proposition **??**, the class in $\mathrm{H}^2(G, L^\times)$ corresponding to A is represented by the cocycle $\psi\colon G^2 \to L^\times$ defined by

$$\psi(\mathrm{id},\mathrm{id}) = \psi(\mathrm{id},g) = \psi(g,\mathrm{id}) = 1, \quad \psi(g,g) = t.$$

Applying v_L to this cocycle gives a 2-cocycle with values in $\mathbf{Z}$:

$$\phi(\mathrm{id},\mathrm{id}) = \phi(\mathrm{id},g) = \phi(g,\mathrm{id}) = 0, \quad \phi(g,g) = 1.$$

According to Proposition 15.1.2, this corresponds under the isomorphism δ to the homomorphism $\alpha\colon G \to \mathbf{Q}/\mathbf{Z}$ defined by $\alpha(g) = \frac{1}{2}$. Now the inflation map $\mathrm{Infl}\colon \mathrm{H}^1(L/K, \mathbf{Q}/\mathbf{Z}) \to \mathrm{H}^1(K, \mathbf{Q}/\mathbf{Z})$ is simply pulling back homomorphisms $G \to \mathbf{Q}/\mathbf{Z}$ to homomorphisms $\mathrm{Gal}(\bar{K}/K) \to \mathbf{Q}/\mathbf{Z}$. We finally obtain $\partial_R(A) = \tilde{\alpha} \in \mathrm{H}^1(K, \mathbf{Q}/\mathbf{Z})$, where

$$\tilde{\alpha}(\sigma) = \begin{cases} 0 & \text{if } \sigma(s) = s; \\ \frac{1}{2} & \text{if } \sigma(s) = -s. \end{cases}$$

We may also define the residue map when R is not complete, as follows.

Definition 15.1.9. Let R be any discrete valuation ring, with field of fractions K and perfect residue field k. Denote by $\widehat{R}$ the completion of R, and by $\widehat{K}$ the completion of K. The *residue map* associated to R is the composite

$$\mathrm{Br}\, K \to \mathrm{Br}\, \widehat{K} \xrightarrow{\partial_{\widehat{R}}} \mathrm{H}^1(k, \mathbf{Q}/\mathbf{Z}).$$

The importance of the residue map is in the following statement, which says that the classes in $\mathrm{Br}\, K$ coming from Azumaya algebras over R are precisely those with zero residue.

Theorem 15.1.10. *Let R be a discrete valuation ring with field of fractions K*

and perfect residue field k. Then there is a short exact sequence

$$0 \to \mathrm{Br}\, R \to \mathrm{Br}\, K \xrightarrow{\partial_R} \mathrm{H}^1(k, \mathbf{Q}/\mathbf{Z}) \to 0.$$

Proof This is Theorem 3.3 of Auslander and Brumer (1968), and we sketch their proof. Firstly, every central simple algebra over K is split by a finite, unramified Galois extension, so it is enough to prove the corresponding statement for finite extensions. Let L/K be an unramified extension and denote by $U(L)$ the group of units in the valuation ring of L. By definition there is a short exact sequence

$$0 \to U(L) \to L^\times \xrightarrow{v_L} \mathbf{Z} \to 0 \tag{15.3}$$

that is split by sending $1 \in \mathbf{Z}$ to a uniformiser in $K^\times \subset L^\times$. It is shown by Auslander and Goldman (1960, Theorem A.15) that the subgroup of $\mathrm{Br}\, R$ split by L can be identified with the cohomology group $\mathrm{H}^2(L/K, U(L))$. The result now follows from the long exact cohomology sequence associated to (15.3). □

When combined with Theorem 12.2.8, this result allows us to state a cohomological version of the Purity Theorem.

Theorem 15.1.11 (Purity Theorem, second form)**.** *Let X be a smooth, irreducible variety over a field of characteristic zero. For each prime divisor Z on X, let ∂_Z denote the residue map $\partial_{\mathscr{O}_{X,Z}}\colon \mathrm{Br}\, \kappa(X) \to \mathrm{H}^1(\kappa(Z), \mathbf{Q}/\mathbf{Z})$ associated to the discrete valuation ring $\mathscr{O}_{X,Z}$. Then there is an exact sequence*

$$0 \to \mathrm{Br}\, X \to \mathrm{Br}\, \kappa(X) \xrightarrow{\oplus_Z \partial_Z} \bigoplus_Z \mathrm{H}^1(\kappa(Z), \mathbf{Q}/\mathbf{Z})$$

where the sum is taken over all prime divisors Z on X.

Proof The main part of the theorem, the exactness, comes directly from combining Theorem 12.2.8 with Theorem 15.1.10. But we must first show that any class in $\mathrm{Br}\, \kappa(X)$ has non-zero residue at only finitely many prime divisors Z.

Let α be a class in $\mathrm{Br}\, \kappa(X)$. By Corollary 12.2.6, there is a dense affine open subset $U \subset X$ such that α lies in $\mathrm{Br}\, U$. Now let Z be any prime divisor on X meeting U; then α is unramified at Z, and so Theorem 15.1.10 gives $\partial_Z(\alpha) = 0$. Thus α can have non-zero residue only at prime divisors not meeting U, of which there are finitely many. So the image of $\oplus_Z \partial_Z$ does indeed lie in the direct sum of the $\mathrm{H}^1(\kappa(Z), \mathbf{Q}/\mathbf{Z})$. Now Theorem 15.1.10 shows that any class in the kernel of $\oplus_Z \partial_Z$ lies in the intersection $\bigcap_Z \mathrm{Br}\, \mathscr{O}_{X,Z} \subset \mathrm{Br}\, \kappa(X)$, which by Theorem 12.2.8 is equal to $\mathrm{Br}\, X$. □

15.2 The Brauer group of a local field

The discussion of residue maps in the previous section, and Theorem 15.1.10, allow us to calculate the structure of the Brauer group of a local field.

Theorem 15.2.1. *Let p be prime, and let K be a finite extension of $\mathbf{Q}_p$. Then there is a canonical isomorphism $\mathrm{Br}\,K \to \mathbf{Q}/\mathbf{Z}$.*

Proof Let R denote the ring of integers of K, and k the residue field, which is finite. Theorem 15.1.10 tells us that there is an exact sequence

$$0 \to \mathrm{Br}\,R \to \mathrm{Br}\,K \xrightarrow{\partial} \mathrm{H}^1(k, \mathbf{Q}/\mathbf{Z}) \to 0.$$

Now $\mathrm{Br}\,R$ is trivial by Corollary **??**, and so ∂ is an isomorphism. To complete the proof, we must give a canonical isomorphism between $\mathrm{H}^1(k, \mathbf{Q}/\mathbf{Z})$ and $\mathbf{Q}/\mathbf{Z}$. The key to this is that, for each finite extension ℓ/k, there is a canonical generator for $\mathrm{Gal}(\ell/k)$, namely the Frobenius automorphism F_ℓ. If ℓ/k is an extension of degree n, we define an injective homomorphism ϕ_ℓ from $\mathrm{H}^1(\ell/k, \mathbf{Q}/\mathbf{Z}) = \mathrm{Hom}(\mathrm{Gal}(\ell/k), \mathbf{Q}/\mathbf{Z})$ to $\mathbf{Q}/\mathbf{Z}$ by defining $\phi_\ell(\alpha) = \alpha(F_\ell)$. It is straightforward to check that these homomorphisms fit together, in the sense that, for any extension ℓ'/ℓ, the map $\phi_{\ell'}$ restricts to ϕ_ℓ on $\mathrm{Hom}(\mathrm{Gal}(\ell/k), \mathbf{Q}/\mathbf{Z}) \subseteq \mathrm{Hom}(\mathrm{Gal}(\ell'/k), \mathbf{Q}/\mathbf{Z})$. The various homomorphisms ϕ_ℓ therefore define an injective homomorphism $\mathrm{H}^1(k, \mathbf{Q}/\mathbf{Z}) \to \mathbf{Q}/\mathbf{Z}$; it is surjective as well, since the image contains elements of every order. □

Definition 15.2.2. Let p be prime, and let K be a finite extension of $\mathbf{Q}_p$. The canonical isomorphism of Theorem 15.2.1 is called the *invariant map* and is denoted

$$\mathrm{inv}_K \colon \mathrm{Br}\,K \longrightarrow \mathbf{Q}/\mathbf{Z}.$$

In order to extend this definition to all completions of a number field, we also define

$$\mathrm{inv}_{\mathbf{R}} \colon \mathrm{Br}\,\mathbf{R} \to \mathbf{Q}/\mathbf{Z} \quad \text{and} \quad \mathrm{inv}_{\mathbf{C}} \colon \mathrm{Br}\,\mathbf{C} \to \mathbf{Q}/\mathbf{Z}$$

to be the unique injective homomorphism in each case (sending $\mathrm{Br}\,\mathbf{R}$ to $\{0, 1/2\}$ and $\mathrm{Br}\,\mathbf{C}$ to $\{0\}$). Now let k be a number field; for each place v of k, we denote by inv_v the composition

$$\mathrm{inv}_v \colon \mathrm{Br}\,k \to \mathrm{Br}\,k_v \xrightarrow{\mathrm{inv}_{k_v}} \mathbf{Q}/\mathbf{Z}.$$

188: Decide how this all fits in with Chapter 10.

Exercise 15.2.3. For any $x \in \mathbf{Q}/\mathbf{Z}$, find an explicit cyclic algebra A over $\mathbf{Q}_p$ with $\mathrm{inv}_{\mathbf{Q}_p}(A) = x$. Deduce that every class in $\mathrm{Br}\,\mathbf{Q}_p$ is represented by a cyclic algebra.

15.3 The algebraic Brauer group

Throughout this section, let X denote a smooth, geometrically irreducible variety over a field k. Recall from Section **??** that the *algebraic* part of the Brauer group of X, denoted $\mathrm{Br}_1 X$, consists of those classes in $\mathrm{Br}X$ which are split by a finite extension of the base field k. More precisely, a finite extension ℓ/k induces a finite extension of function fields $\kappa(X_\ell)/\kappa(X)$; a class $\alpha \in \mathrm{Br}X$ lies in $\mathrm{Br}_1 X$ if it is split by such an extension.

As X is geometrically irreducible, the two fields ℓ and $\kappa(X)$ are linearly disjoint extensions of k. It follows that there is a canonical isomorphism

$$\mathrm{Gal}(\kappa(X_\ell)/\kappa(X)) \cong \mathrm{Gal}(\ell/k).$$

Using this isomorphism, we will write $\mathrm{H}^2(\ell/k, \kappa(X_\ell)^\times)$ as slightly less cumbersome notation for the subgroup

$$\mathrm{H}^2(\kappa(X_\ell)/\kappa(X), \kappa(X_\ell)^\times) \subset \mathrm{H}^2(\kappa(X), \overline{\kappa(X)}^\times) = \mathrm{Br}\,\kappa(X).$$

The definition of $\mathrm{Br}_1 X$ as consisting of those classes in $\mathrm{Br}\,\kappa(X)$ which are both unramified and split by a finite extension of k means that, taking the limit over finite extensions ℓ/k, we can identify

$$\mathrm{Br}_1 X = \mathrm{H}^2(k, \kappa(\bar{X})^\times) \cap \mathrm{Br}X,$$

the intersection taking place inside $\mathrm{Br}\,\kappa(X)$.

To arrive at a computationally useful description of $\mathrm{Br}_1 X$, we first re-interpret the residue map at a prime divisor of X. The following proposition can be thought of as saying that the natural homomorphism $\mathrm{H}^2(k, \kappa(\bar{X})^\times) \to \mathrm{H}^2(k, \mathrm{Div}\,\bar{X})$ "is" the restriction of all the residue maps to $\mathrm{Br}_1 X$.

Proposition 15.3.1. *There is an injective homomorphism*

$$\phi : \mathrm{H}^2(k, \mathrm{Div}\,\bar{X}) \longrightarrow \bigoplus_Z \mathrm{H}^1(\kappa(Z), \mathbf{Q}/\mathbf{Z}),$$

where the sum is over all prime divisors Z on X, such that the diagram

$$\begin{array}{ccc} \mathrm{Br}\,\kappa(X) & \xrightarrow{\oplus_Z \partial_Z} & \bigoplus_Z \mathrm{H}^1(\kappa(Z), \mathbf{Q}/\mathbf{Z}) \\ \uparrow & & \uparrow \phi \\ \mathrm{H}^2(k, \kappa(\bar{X})^\times) & \xrightarrow{\mathrm{div}} & \mathrm{H}^2(k, \mathrm{Div}\,\bar{X}) \end{array}$$

commutes.

Proof As described in Exercise 14.7.8, the Galois module $\mathrm{Div}\,\bar{X}$ splits as a

direct sum of Galois modules $\mathrm{Div}_Z \bar{X}$, where Z runs over the prime divisors on X. We will define injective homomorphisms

$$\phi_Z \colon \mathrm{H}^2(k, \mathrm{Div}_Z \bar{X}) \to \mathrm{H}^1(\kappa(Z), \mathbf{Q}/\mathbf{Z})$$

and then take $\phi = \oplus_Z \phi_Z$.

Fix a prime divisor Z on X. Over $\bar{k}$, Z may decompose into several irreducible components Z_i; let k'/k be the minimal field of definition of one component Z_1. By **??**, k' can be taken to be the algebraic closure of k within $\kappa(Z)$. It was shown in Exercise 14.7.8 that the Galois module $\mathrm{Div}_Z \bar{X}$ is isomorphic to the induced module $\mathrm{Ind}_{k'/k} \mathbf{Z}$, and therefore Shapiro's Lemma (Proposition 14.4.3) gives an isomorphism $\mathrm{H}^2(k, \mathrm{Div}_Z \bar{X}) \cong \mathrm{H}^2(k', \mathbf{Z})$. Let

$$j \colon \mathrm{Gal}(\overline{\kappa(Z)}/\kappa(Z)) \to \mathrm{Gal}(\bar{k}/k')$$

be the homomorphism defined by restricting an automorphism of $\overline{\kappa(Z)}$ to $\bar{k}$. We define ϕ_Z to be the composite

$$\mathrm{H}^2(k, \mathrm{Div}_Z \bar{X}) \cong \mathrm{H}^2(k', \mathbf{Z}) \cong \mathrm{H}^1(k', \mathbf{Q}/\mathbf{Z}) \xrightarrow{j^*} \mathrm{H}^1(\kappa(Z), \mathbf{Q}/\mathbf{Z})$$

As k' is algebraically closed in $\kappa(Z)$, the homomorphism j is surjective; therefore j^*, and hence ϕ_Z, is injective.

We must now show that the diagram does indeed commute. This follows in a messy but straightforward way from the definitions. Recall the definition of the residue map ∂_Z as the composite homomorphism

$$\mathrm{Br}\,\kappa(X) \to \mathrm{Br}\,\widehat{\kappa(X)} \to \mathrm{H}^1(\kappa(Z), \mathbf{Q}/\mathbf{Z})$$

where $\widehat{\kappa(X)}$ is the completion of $\kappa(X)$ with respect to the discrete valuation defined by Z. We are given a class in $\mathrm{Br}\,\kappa(X)$ which is split by the finite extension $\kappa(X_\ell)/\kappa(X)$; since this extension (like every extension coming from an extension of the base field) is unramified above Z, we can use it to compute the residue. (The point of passing to the completion when defining the residue map was to guarantee the existence of an unramified splitting field; here we are in the happy position of having an unramified splitting field even before passing to the completion.) For brevity, write $K = \kappa(X)$ and $L = \kappa(X_\ell)$. After possibly enlarging ℓ, we may assume that ℓ/k is Galois, and that the divisors Z_i are all defined over ℓ (and in particular that k' is contained in ℓ). Now the residue map on $\mathrm{H}^2(L/K, L^\times)$ was defined to be the composition

$$\mathrm{H}^2(L/K, L^\times) \xrightarrow{c} \mathrm{H}^2(\widehat{L}/\widehat{K}, \widehat{L}^\times) \xrightarrow{v_1} \mathrm{H}^2(\widehat{L}/\widehat{K}, \mathbf{Z}) \xrightarrow{\mathrm{Infl} \circ \delta^{-1}} \mathrm{H}^1(\kappa(Z), \mathbf{Q}/\mathbf{Z}).$$

Here $\widehat{L}$ is the completion of L under a chosen extension of the valuation v_Z; we will choose the valuation associated to the divisor Z_1 on X_ℓ, which we

denote by v_1. The map c is as described in **??**. Now $\mathrm{Gal}(L/K)$ can be identified with $\mathrm{Gal}(\ell/k)$, and $\mathrm{Gal}(\widehat{L}/\widehat{K})$ can be identified with a subgroup, the decomposition group associated to the chosen valuation, which as we saw above is $H = \mathrm{Gal}(\ell/k')$. The map c is then restriction from $\mathrm{Gal}(\ell/k)$ to $\mathrm{Gal}(\ell/k')$ followed by the map induced by the inclusion $L^\times \subset \widehat{L}^\times$. The composition $L^\times \to \widehat{L}^\times \xrightarrow{v_1} \mathbf{Z}$ is just the valuation v_1 restricted to $L^\times$. Putting all this together, we are reduced to showing that the following diagram commutes:

$$\begin{array}{ccccc} \mathrm{H}^2(\ell/k, L^\times) & \xrightarrow{v_1 \circ \mathrm{Res}} & \mathrm{H}^2(\ell/k', \mathbf{Z}) & \xrightarrow{\mathrm{Infl} \circ \delta^{-1}} & \mathrm{H}^1(\kappa(Z), \mathbf{Q}/\mathbf{Z}) \\ \Big\downarrow{\scriptstyle \mathrm{div}} & & \Big\uparrow & & \\ \mathrm{H}^2(\ell/k, \mathrm{Div}_Z \bar{X}) & \longrightarrow & \mathrm{H}^2(\ell/k, \mathrm{Ind}_{k'/k} \mathbf{Z}) & & \end{array}.$$

The "top route" on this diagram is our original definition of the residue map, and the "bottom route" is the one used to construct our map ϕ. That the diagram does indeed commute is easily checked on cocycles. Explicitly, let us start with a cocycle $(\sigma, \tau) \mapsto f_{\sigma\tau}$ lying in $\mathrm{H}^2(\ell/k, L^\times)$. Denote by $v_{Z_1}, \ldots, v_{Z_n}$ the valuations on $L^\times$ associated to the divisors $Z_1, \ldots, Z_n$. Our chosen cocycle, along the "bottom route", then maps to:

$$(\sigma, \tau) \mapsto (v_{Z_1}(f_{\sigma\tau}), \ldots, v_{Z_n}(f_{\sigma\tau})) \in \mathrm{H}^2(\ell/k, \mathrm{Div}_Z \bar{X})$$
$$(\sigma, \tau) \mapsto (g \mapsto g v_{g^{-1}Z}(f_{\sigma\tau})) \in \mathrm{H}^2(\ell/k, \mathrm{Ind}_{k'/k} \mathbf{Z})$$

by Exercise 14.7.8 and Proposition 14.4.7; and to

$$(\sigma, \tau) \mapsto v_1(f_{\sigma\tau}) \in \mathrm{H}^2(\ell/k', \mathbf{Z})$$

by the proof of Shapiro's Lemma (Proposition 14.4.3). This is precisely what we get by following the "top" route. □

Corollary 15.3.2. *There is an exact sequence*

$$0 \to \mathrm{Br}_1 X \to \mathrm{H}^2(k, \kappa(\bar{X})^\times) \xrightarrow{\mathrm{div}} \mathrm{H}^2(k, \mathrm{Div}\, \bar{X}).$$

Proof As discussed above, $\mathrm{Br}_1 X$ consists of those elements of $\mathrm{Br}\, \kappa(X)$ which are unramified, and lie in the subgroup identified with $\mathrm{H}^2(k, \kappa(\bar{X}))$. The Purity Theorem (Theorem 15.1.11) shows that being unramified is equivalent to having trivial residue at each prime divisor; and Proposition 15.3.1 shows that this is equivalent to being in the kernel of $\mathrm{H}^2(k, \kappa(\bar{X})) \to \mathrm{H}^2(k, \mathrm{Div}\, \bar{X})$. □

189: Do we want to characterise these classes as ones which can be evaluated anywhere?

It is often useful to specialise Corollary 15.3.2 to the case of cyclic algebras, as follows.

Proposition 15.3.3. *Let X be a smooth, geometrically integral variety over a field k, ℓ/k a finite cyclic extension, σ a generator of* $\mathrm{Gal}(\ell/k)$ *and $f \in \kappa(X)^\times$. The cyclic algebra $(\ell/k, \sigma, f)$ is in the image of the natural map* $\mathrm{Br}(X) \to \mathrm{Br}(\kappa(X))$ *if and only if $(f) = N_{\ell/k}(D)$, for some $D \in \mathrm{Div}(X_\ell)$. If k is a number field and $X(k_v) \neq \emptyset$ for all valuations v of k, then $(\ell/k, f)$ comes from* $\mathrm{Br}(k)$ *if and only if we can take D to be principal.*

Proof 190: Take proof from Martin's thesis □

This description of $\mathrm{Br}_1 X$ as a subgroup of $\mathrm{H}^2(k, \kappa(\bar{X})^\times)$ allows us, with the help of a little more diagram-chasing, to describe a systematic way of producing elements of $\mathrm{Br}_1 X$ in certain situations. Recall that there is a natural map $\mathrm{Br}\, k \to \mathrm{Br}\, \kappa(X)$, the image of which lies in $\mathrm{Br}_1 X$. In view of Remark 13.1.8, if we are interested in calculating the Brauer–Manin obstruction associated to $\mathrm{Br}_1 X$, it suffices to find elements of $\mathrm{Br}_1 X$ which generate the quotient $\mathrm{Br}_1 X / \mathrm{Br}\, k$.

Proposition 15.3.4. *Let X be a smooth, geometrically irreducible, projective variety over a number field k. Then there is an isomorphism*

$$r\colon \mathrm{H}^1(k, \mathrm{Pic}\, \bar{X}) \longrightarrow \mathrm{Br}_1 X / \mathrm{Br}\, k.$$

Proof We construct the isomorphism as the composition of two homomorphisms.

Step 1. Consider the short exact sequence of Galois modules

$$0 \to \mathrm{Princ}\, \bar{X} \to \mathrm{Div}\, \bar{X} \to \mathrm{Pic}\, \bar{X} \to 0$$

which defines $\mathrm{Pic}\, \bar{X}$. Given that $\mathrm{H}^1(k, \mathrm{Div}\, \bar{X}) = 0$ (from Exercise 14.7.8), the associated long exact sequence in cohomology gives an isomorphism

$$\alpha\colon \mathrm{H}^1(k, \mathrm{Pic}\, \bar{X}) \xrightarrow{\sim} \ker\big(\mathrm{H}^2(k, \mathrm{Princ}\, \bar{X}) \to \mathrm{H}^2(k, \mathrm{Div}\, \bar{X})\big).$$

Step 2. By Proposition 4.1.8, the only functions on $\bar{X}$ with trivial divisor are the constant functions. It follows that there is a short exact sequence

$$0 \to \bar{k}^\times \to \kappa(\bar{X})^\times \xrightarrow{\mathrm{div}} \mathrm{Princ}\, \bar{X} \to 0.$$

Part of the associated long exact sequence in cohomology is

$$\mathrm{Br}\, k = \mathrm{H}^2(k, \bar{k}^\times) \to \mathrm{H}^2(k, \kappa(\bar{X})^\times) \xrightarrow{\beta} \mathrm{H}^2(k, \mathrm{Princ}\, \bar{X}) \to \mathrm{H}^3(k, \bar{k}^\times).$$

Step 3. We claim that restricting β to $\mathrm{Br}_1 X$ gives an isomorphism

$$\beta\colon \mathrm{Br}_1 X/\mathrm{Br}\, k \longrightarrow \ker\left(\mathrm{H}^2(k,\mathrm{Princ}\,\bar{X}) \to \mathrm{H}^2(k,\mathrm{Div}\,\bar{X})\right).$$

Consider the composition of homomorphisms $\kappa(\bar{X})^\times \xrightarrow{\mathrm{div}} \mathrm{Princ}\,\bar{X} \xrightarrow{i} \mathrm{Div}\,\bar{X}$, the second homomorphism being the inclusion map. These give rise to homomorphisms

$$\mathrm{H}^2(k,\kappa(\bar{X})^\times) \xrightarrow{\beta} \mathrm{H}^2(k,\mathrm{Princ}\,\bar{X}) \xrightarrow{i_*} \mathrm{H}^2(k,\mathrm{Div}\,\bar{X})$$

to which we can apply the kernel-cokernel exact sequence (**??**). We obtain an exact sequence

$$0 \to \ker\beta \to \ker(i_*\circ\beta) \xrightarrow{\beta} \ker i_* \to \mathrm{coker}\,\beta,$$

which translates into

$$\mathrm{Br}\, k \to \mathrm{Br}_1 X \xrightarrow{\beta} \ker\left(\mathrm{H}^2(k,\mathrm{Princ}\,\bar{X}) \to \mathrm{H}^2(k,\mathrm{Div}\,\bar{X})\right) \to \mathrm{H}^3(k,\bar{k}^\times).$$

(We have removed the left-hand 0 because $\ker\beta$ is the *image* of $\mathrm{Br}\, k$ in $\mathrm{H}^2(k,\kappa(\bar{X})^\times)$, rather than $\mathrm{Br}\, k$ itself.) As k is a number field, we have $\mathrm{H}^3(k,\bar{k}^\times) = 0$ by **??**. Therefore β does give the claimed isomorphism.

Step 4. Define $r := \beta^{-1}\circ\alpha$ to obtain the required isomorphism. □

As we shall describe in more detail in the following section, it is not only the statement of this proposition that is useful, but also the explicit nature of its proof. By following the steps of the proof, we can turn an explicitly given cocycle in $\mathrm{H}^1(k,\mathrm{Pic}\,\bar{X})$ into an explicit central simple algebra over $\kappa(X)$.

15.4 Computing the algebraic Brauer group

In this section, we apply the understanding of the algebraic Brauer group gained in the previous section to writing down explicit elements of $\mathrm{Br}_1 X$, for suitable varieties X. Other presentations of this material can be found in Kresch and Tschinkel (2008) and Bright and Swinnerton-Dyer (2004).

What exactly is the goal? Let k be a number field and X a smooth, projective, geometrically irreducible variety over k. An element of the algebraic Brauer group is a central simple algebra over $\kappa(X)$ split by a finite extension ℓ/k. Using the explicit correspondence between central simple algebras and 2-cocycles, to "write down" such a central simple algebra it is enough to write down a 2-cocycle representing a class in $\mathrm{H}^2(\ell/k,\kappa(X_\ell)^\times)$. This is a concrete,

finite amount of information: writing $G = \mathrm{Gal}(\ell/k)$, a 2-cocycle specifies an element of $\kappa(X_\ell)^\times$ for each pair (σ, τ) of elements of the finite group G.

When can we expect to write down "the whole" algebraic Brauer group? Again, suppose that X is a smooth, geometrically irreducible variety over a number field k. Then $\mathrm{Br}_1 X$ is infinite, since it contains at least the classes of all the constant algebras; even if $\mathrm{Br}\, k \to \mathrm{Br}_1 X$ is not injective, the kernel is finite and so the image is still very large. On the other hand, constant algebras do not contribute to the Brauer–Manin obstruction, so we are really interested in the quotient $\mathrm{Br}_1 X/\mathrm{Br}\, k$. This does stand some chance of being finite. As we have seen in Proposition 15.3.4, the quotient $\mathrm{Br}_1 X/\mathrm{Br}\, k$ is isomorphic to $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$; the structure of this group depends on the structure of $\mathrm{Pic}\,\bar{X}$, which is a geometric property of the variety $\bar{X}$.

If X is a smooth, projective, geometrically irreducible curve over a number field, then there are two possibilities: either X has genus zero, in which case $\mathrm{Pic}\,\bar{X}$ is isomorphic to $\mathbf{Z}$ with trivial Galois action, and $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$ is trivial; or X has genus at least 1, in which case $\mathrm{Pic}\,\bar{X}$ contains the Abelian variety $\mathrm{Pic}^0 \bar{X}$. In the latter case, $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$ contains much deep information about the arithmetic of X, and in particular contains the Tate–Shafarevich group of the Jacobian of X; this is notoriously difficult to understand even in individual examples, so we should not expect to be able to do anything about computing it in general.

On the other hand, surfaces behave very differently. We have seen in this book several examples of surfaces, in particular del Pezzo surfaces and K3 surfaces, which have *finitely generated* Picard group. Galois cohomology with values in a finitely generated abelian group is something we can successfully compute with.

Proposition 15.4.1. *Let X be a smooth, projective, geometrically irreducible variety over a number field k, and suppose that $\mathrm{Pic}\,\bar{X}$ is free and finitely generated. Then $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$, and therefore $\mathrm{Br}_1 X/\mathrm{Br}\, k$, are finite.*

Proof Let $Z_1, \ldots, Z_n$ be divisors on $\bar{X}$ whose classes freely generate $\mathrm{Pic}\,\bar{X}$. Each divisor Z_i is defined by a finite number of polynomial equations, each of which has finitely many coefficients; there is therefore a finite extension K/k containing all these coefficients, so that every Z_i is defined over K. It follows that $\mathrm{Gal}(\bar{k}/K)$ fixes each Z_i and so acts trivially on $\mathrm{Pic}\,\bar{X}$. We can identify $\mathrm{Pic}\,\bar{X}$ with $\mathrm{Pic}\, X_K$. Therefore we have

$$\mathrm{H}^1(K, \mathrm{Pic}\,\bar{X}) = \mathrm{Hom}(\mathrm{Gal}(\bar{k}/K), \mathrm{Pic}\,\bar{X}) = 0$$

by Example 14.7.5. The inflation-restriction sequence now gives

$$0 \to \mathrm{H}^1(K/k, \mathrm{Pic}\,\bar{X}) \to \mathrm{H}^1(k, \mathrm{Pic}\,\bar{X}) \to \mathrm{H}^1(K, \mathrm{Pic}\,\bar{X})$$

and so an isomorphism $\mathrm{H}^1(K/k, \mathrm{Pic}\,\bar{X}) \cong \mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$. This group is finite by Proposition 14.4.11. By Proposition 15.3.4, $\mathrm{Br}_1 X / \mathrm{Br}\, k$ is finite as well. □

Computing $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$

Let X be a variety satisfying the conditions of Proposition 15.4.1. Then not only is $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$ finite, but we can compute it, in the following sense. Suppose that we are given equations for X and equations for finitely many divisors $Z_1, \ldots, Z_n$ on $\bar{X}$, the classes of which freely generate $\mathrm{Pic}\,\bar{X}$. Suppose further that we already know a finite extension K/k over which all the Z_i are defined, together with $G = \mathrm{Gal}(K/k)$ and its action on the Z_i. Then there is an algorithm which computes the structure of $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$ as a finite group, and also explicit 1-cocycles representing classes which generate the group. (What is an explicit 1-cocycle in this context? It is a collection $\{D_\sigma : \sigma \in G\}$, where each D_σ is a class in $\mathrm{Pic}\,\bar{X}$, represented as a finite integer linear combination of the classes of the Z_i.) There is nothing mysterious about this calculation. The groups of cochains $C^i(G, \mathrm{Pic}\,\bar{X})$ are finitely generated $\mathbf{Z}$-modules, and the coboundary maps between them are linear maps represented by integer matrices, which can be written down. Computing the cohomology groups is therefore a matter of integer linear algebra, for which algorithms are known. (In practice there may well be more efficient ways of computing cohomology groups, but at least we can see that it is a finite calculation.)

As a slight extension of this, we do not necessarily require that the Z_i generate $\mathrm{Pic}\,\bar{X}$ *freely*; it is enough to have a finite set of divisors which generate $\mathrm{Pic}\,\bar{X}$. We will need to know the relations between their classes, that is, the kernel of the map $\oplus_i Z_i \to \mathrm{Pic}\,\bar{X}$. Under the hypothesis that $\mathrm{Pic}\,\bar{X}$ is free, numerical equivalence of divisors is the same as linear equivalence, and so this kernel can be deduced from the intersection numbers of the Z_i. 191: Reference for this?

Shrinking the field extension

Keeping the notation of the previous section, suppose that we have been given the variety X, the divisors Z_i which generate $\mathrm{Pic}\,\bar{X}$, the field K over which the Z_i are all defined, and the Galois group $\mathrm{Gal}(K/k)$; we have now computed $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$. The proof of Proposition 15.3.4 shows how to turn a class in $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$ into a central simple algebra over $\kappa(X)$ representing the corresponding class in $\mathrm{Br}_1 X$. At the moment any class in $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$ is represented

by a cocycle lying in $\mathrm{H}^1(K/k, \mathrm{Pic}\,\bar{X})$. However, the extension K/k may well be quite large, making calculations in cohomology (and in particular the procedure in the proof of Proposition 15.3.4) prohibitively lengthy. By definition we have

$$\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X}) = \varinjlim \mathrm{H}^1(\ell/k, (\mathrm{Pic}\,\bar{X})^{\mathrm{Gal}(\bar{k}/\ell)})$$

where ℓ runs over all finite extensions of k, the maps being the inflation maps. Therefore any class in $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$ arises by inflation from a class in some $\mathrm{H}^1(\ell/k, (\mathrm{Pic}\,\bar{X})^{\mathrm{Gal}(\bar{k}/\ell)})$. We have already shown that this is true with $\ell = K$, but for what follows it will be useful to be able to take $[\ell : k]$ as small as possible.

This can be accomplished as follows. We already have $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X}) \cong \mathrm{H}^1(G, \mathrm{Pic}\,\bar{X})$ where $G = \mathrm{Gal}(K/k)$. Fix a cocycle ϕ representing a class in $\mathrm{H}^1(G, \mathrm{Pic}\,\bar{X})$. Let G' be a normal subgroup of G. By the same procedure as before, we can compute $\mathrm{H}^1(G/G', (\mathrm{Pic}\,\bar{X})^{G'})$ and the inflation map

$$\mathrm{H}^1(G/G', (\mathrm{Pic}\,\bar{X})^{G'}) \xrightarrow{\mathrm{Infl}} H^1(G, \mathrm{Pic}\,\bar{X})$$

Trying all subgroups G', we can find the largest G' such that ϕ lies in the image of the inflation map, and therefore (setting $\ell = K^{G'}$) the smallest extension ℓ/k such that the class of ϕ arises by inflation from $\mathrm{H}^1(\ell/k, (\mathrm{Pic}\,\bar{X})^{\mathrm{Gal}(\bar{k}/\ell)}$.

There remains one problem. In what follows, we will show how to convert an explicit cocycle in $\mathrm{H}^1(\ell/k, \mathrm{Pic}\,X_\ell)$ into a central simple algebra in $\mathrm{Br}_1 X$. However, instead of a cocycle with values in $\mathrm{Pic}\,X_\ell$, we have in our hands at this stage a cocycle with values in $(\mathrm{Pic}\,\bar{X})^{\mathrm{Gal}(\bar{k}/\ell)}$, or in other words a cocycle with values in $(\mathrm{Pic}\,X_K)^{G'}$. In detail, an element of $(\mathrm{Pic}\,X_K)^{G'}$ is represented a divisor (in fact, a linear combination of the divisors Z_i which we started with) which is linearly equivalent to each of its conjugates under the action of G'. Assuming that X has points everywhere locally, the method described in Section **??** shows how to find an equivalent divisor defined over ℓ, that is, to make effective the isomorphism $(\mathrm{Pic}\,X_K)^{G'} \cong \mathrm{Pic}\,X_\ell$.

After following this procedure, we now have: a description of the group $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$; and, for each class c in that group, a finite extension ℓ/k and an explicit cocycle in $\mathrm{H}^1(\ell/k, \mathrm{Pic}\,X_\ell)$ representing the class c.

From $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$ to $\mathrm{Br}_1 X$

Suppose now that we are given a finite Galois extension ℓ/k, with known Galois group H, and an explicit 1-cocycle $\phi : H \to \mathrm{Pic}\,X_\ell$ representing a class in $\mathrm{H}^1(H, \mathrm{Pic}\,X_\ell)$. We assume that, for each $\sigma \in H$, $\phi(\sigma)$ is specified as a

divisor on X_ℓ, the class of which is $\phi(\sigma)$. The recipe of Proposition 15.3.4 consists of the following steps.

Step 1. Compute the image of ϕ under the connecting homomorphism $\alpha\colon \mathrm{H}^1(H, \mathrm{Pic}\, X_\ell) \to \mathrm{H}^2(H, \mathrm{Princ}\, X_\ell)$. This is a straightforward application of the definition. Firstly, we lift ϕ to a map $H \to \mathrm{Div}\, X_\ell$; this amounts to doing nothing, since each $\phi(\sigma)$ was already given as a divisor. Secondly, we define a 2-chain $\psi = \alpha(\phi)$ by

$$\psi(\sigma,\tau) = \phi(\sigma) + \sigma\phi(\tau) - \phi(\sigma\tau).$$

Then ψ is actually a 2-cocycle taking values in $\mathrm{Princ}\, X_\ell$.

Step 2. Try to lift ψ under the homomorphism $\beta\colon \mathrm{H}^2(H, \kappa(X_\ell)^\times) \to \mathrm{H}^2(H, \mathrm{Princ}\, X_\ell)$. There are potential problems here, since we must make use of the triviality of $\mathrm{H}^3(k, \bar{k}^\times)$. The process is as follows. Firstly, for each pair (σ,τ) of elements of H, find a rational function $f_{\sigma,\tau} \in \kappa(X_\ell)$ such that $(f_{\sigma,\tau}) = \psi(\sigma,\tau)$. (This is possible since $\psi(\sigma,\tau)$ is a principal divisor, by construction.[1]) Now the map $\eta\colon (\sigma,\tau) \mapsto f_{\sigma,\tau}$ is a 2-cochain with values in $\kappa(X_\ell)^\times$, but it has no reason to be a cocycle. Indeed, the $f_{\sigma,\tau}$ are each unique only up to a constant multiple, and we have no canonical way of choosing them. To see how far η is from being a cocycle, we look at the coboundary $\xi = \partial\eta$, which is a 3-cocycle taking values in $\ell^\times$. The fact that $\mathrm{H}^3(k, \bar{k}^\times)$ is trivial unfortunately does not imply that ξ is a coboundary, because $\mathrm{H}^3(\ell/k, \ell^\times)$ might not be trivial. What is true is that there is some finite extension ℓ'/ℓ such that the class of ξ maps to zero in $\mathrm{H}^3(\ell'/k, \ell'^\times)$ under the inflation map. Indeed, there is an effective algorithm to find such an ℓ', and to compute a 2-cochain $\zeta \in C^2(\mathrm{Gal}(\ell'/k), \ell'^\times)$ such that $\partial\zeta = \mathrm{Infl}(\xi)$: see Kresch and Tschinkel (2008, Proposition 6.3). Replacing ℓ by ℓ' and η by η/ζ, we reach the stage where η is indeed a 2-cocycle with values in $\kappa(X_\ell)^\times$. By the proof of Proposition 15.3.4, η represents the class of our desired algebra in $\mathrm{Br}_1 X$.

Remark 15.4.2. If X has a rational point over k, then enlarging ℓ to ℓ' will never be necessary. The reason is that a rational point $P \in X(k)$ gives a way of choosing the $f_{\sigma,\tau}$ correctly in the first place: assuming that P does not lie on the support of any of the divisors appearing in ψ, scale such that $f_{\sigma,\tau}(P)$ is 1.

[1] The curious reader may wonder how to find a rational function corresponding to a principal divisor. Essentially the algorithm works as follows. We work in projective space. Given a divisor known to be principal, write it as $D^+ - D^-$ with D^+, D^- effective. For some sufficiently large positive integer d, there is a form g of degree d which vanishes on D^-; but g will also vanish elsewhere, say on another divisor E. Now, if d was chosen sufficiently large, there will be another form f, also of degree d, vanishing precisely on D^+ and E; the function f/g then satisfies $(f/g) = D^+ - D^-$. For more details, see Kresch and Tschinkel (2008, Proposition 7.3).

Then η is automatically a cocycle. (Even if P does lie on one of the divisors, the implication still holds: see Skorobogatov (2001, Theorem 2.3.4(b)) and the proof at the bottom of p. 27 there.) Turning this around, this means that if ξ is not already a coboundary in $\mathrm{H}^3(\ell/k,\ell^\times)$, then X has no rational points over k. If the goal of computing the Brauer group was to try to find an obstruction to the existence of rational points on X, then there is no need to continue.

The case of a cyclic extension

An important special case of the calculation described in the preceding section is when the extension ℓ/k is cyclic. Recall from Section 14.5 that, for a finite cyclic group G acting on a module M, there are isomorphisms

$$\mathrm{H}^1(G,M) \cong {}_{\mathrm{N}}M/\Delta M \quad \text{and} \quad \mathrm{H}^2(G,M) \cong M^G/\mathrm{N}M.$$

It is important to keep in mind that these isomorphisms are not canonical, but depend on the choice of a generator of G.

We keep the notation of the preceding section: X is a smooth, geometrically irreducible variety over a number field k, and ℓ/k is a finite extension. Now suppose that $\mathrm{Gal}(\ell/k)$ is cyclic, and fix a generator σ of $\mathrm{Gal}(\ell/k)$. We have the isomorphism

$$\mathrm{H}^1(\ell/k,\mathrm{Pic}\,X_\ell) \cong {}_{\mathrm{N}}(\mathrm{Pic}\,X_\ell)/\Delta\mathrm{Pic}\,X_\ell.$$

By Proposition 15.3.4, every element of ${}_{\mathrm{N}}(\mathrm{Pic}\,X_\ell)/\Delta\mathrm{Pic}\,X_\ell$ gives rise to a class in $\mathrm{Br}_1 X/\mathrm{Br}k$; we would like to describe this class without going through the H^1s and H^2s of the procedure described previously.

Proposition 15.4.3. *Let $D \in \mathrm{Div}\,X_\ell$ be a divisor representing a class in ${}_{\mathrm{N}}(\mathrm{Pic}\,X_\ell)/\Delta\mathrm{Pic}\,X_\ell$. The divisor $\mathrm{N}D \in \mathrm{Div}\,X$ is principal; let $f \in \kappa(X)^\times$ be such that $(f) = \mathrm{N}D$. Then the image of the class of D under the sequence of maps*

$${}_{\mathrm{N}}(\mathrm{Pic}\,X_\ell)/\Delta\mathrm{Pic}\,X_\ell \cong \mathrm{H}^1(\ell/k,\mathrm{Pic}\,X_\ell) \xrightarrow{\mathrm{Infl}} \mathrm{H}^1(k,\mathrm{Pic}\,\bar{X}) \xrightarrow{r} \mathrm{Br}_1 X/\mathrm{Br}k$$

is the class of the cyclic algebra $(\kappa(X_\ell)/\kappa(X),\sigma,f)$.

Proof By the various functorial properties described in Proposition 14.5.3,

the following diagram commutes:

$$\begin{array}{ccccc}
\mathrm{H}^1(k,\mathrm{Pic}\,\bar{X}) & \xrightarrow{\alpha} & \mathrm{H}^2(k,\mathrm{Princ}\,\bar{X}) & \xleftarrow{\beta} & \mathrm{H}^2(k,\kappa(\bar{X})^\times) \\
{\scriptstyle\mathrm{Infl}}\uparrow & & {\scriptstyle\mathrm{Infl}}\uparrow & & {\scriptstyle\mathrm{Infl}}\uparrow \\
\mathrm{H}^1(\ell/k,\mathrm{Pic}\,X_\ell) & \longrightarrow & \mathrm{H}^2(\ell/k,\mathrm{Princ}\,X_\ell) & \longleftarrow & \mathrm{H}^2(\ell/k,\kappa(X_\ell)^\times)\cdot \\
\cong\downarrow & & \cong\downarrow & & \cong\downarrow \\
{}_{\mathrm{N}}\mathrm{Pic}\,X_\ell/\Delta\mathrm{Pic}\,X_\ell & \xrightarrow{\mathrm{N}_*} & \mathrm{Princ}\,X/\mathrm{N}(\mathrm{Princ}\,X_\ell) & \xleftarrow{\mathrm{div}} & \kappa(X)^\times/\mathrm{N}\kappa(X_\ell)^\times
\end{array}$$

The map $\beta^{-1}\circ\alpha$ of the top row was the definition of the isomorphism r of Proposition 15.3.4, and so the sequence of maps described in the statement of the proposition takes us up the left-hand column of the diagram and across the top row. On the other hand, going along the bottom row of the diagram takes our divisor D to the class of f in $\kappa(X)^\times/N\kappa(X_\ell)^\times$, and then **??** shows that going up the right-hand column maps the class of f to the class of the cyclic algebra $(\kappa(X_\ell)/\kappa(X),\sigma,f)$, as claimed. □

To summarise, the procedures described in this section allow us to do the following. Suppose that we are given a smooth, projective, geometrically irreducible variety X over a number field k, together with a finite Galois extension K/k and divisors $Z_1,\dots,Z_n$, defined over K, the classes of which generate $\mathrm{Pic}\,\bar{X}$, which we suppose to be free. Suppose that we know $\mathrm{Gal}(K/k)$ and its action on the Z_i. Then we can compute the abstract structure of $\mathrm{Br}_1X/\mathrm{Br}\,k$; and, for each class in $\mathrm{Br}_1X/\mathrm{Br}\,k$, we can find a minimal finite extension ℓ/k contained in K and an explicit 2-cocycle in $\mathrm{H}^2(\ell/k,\kappa(X_\ell)^\times)$ representing that class. If ℓ/k is cyclic, we can instead realise the cohomology class as the class of an explicit cyclic algebra.

16

A worked example

16.1 Introduction

In this chapter, we describe in detail how to compute the algebraic Brauer–Manin obstruction on a particular surface. The surface will be the diagonal quartic surface

$$X\colon \{X_0^4 + X_1^4 = 6X_2^4 + 12X_3^4\} \subset \mathbf{P}^3_{\mathbf{Q}}. \tag{16.1}$$

This surface is not a del Pezzo surface, but a K3 surface. It is geometrically slightly more complicated than the rational surfaces which have been our primary concern so far. However, it has many features which make it particularly amenable to computations.

- The surface X contains 48 obvious straight lines, and the classes of these straight lines generate the Picard group of X.
- The Galois action on the 48 lines is relatively easy to determine, and thus so is the Galois action on the Picard group.
- As we will see, the Azumaya algebras in $\mathrm{Br}_1 X$ are quaternion algebras, making it straightforward to find their invariants at the local points of X.
- Anything else?

Our computation will prove the following statement.

Theorem 16.1.1. *The surface X defined in* (16.1) *is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction.*

The example described in this section sometimes involves larger calculations than it would be comfortable to solve by hand. For these we will assume the use of a computer algebra system, and will state the results without justification. However, we aim to give sufficient detail that a sufficiently dedicated reader could check them.

16.2 Local solubility

To be a counterexample to the Hasse principle, X certainly must have points in each completion of $\mathbf{Q}$. For the real number this is clear – to be completely explicit, note that $[\sqrt[4]{17} : 1 : 1 : 1] \in X(\mathbf{R})$. For the p-adic completions of $\mathbf{Q}$, we will prove local solubility in a more general context, to give an idea of the methods which can be used. So, in this section, we let X be a general diagonal quartic surface defined by

$$X = \{a_0X_0^4 + a_1X_1^4 + a_2X_2^4 + a_3X_3^4\} \subset \mathbf{P}^3_{\mathbf{Q}}. \tag{16.2}$$

The indispensable tool in showing that varieties have points in p-adic fields is Hensel's Lemma. We state here a version in several variables.

d: Consider moving it before, say Chapter 1, possibly in the one-variable case.

Lemma 16.2.1 (Hensel)**.** *Let $f(X_0,\dots,X_n)$ be a polynomial in $n+1$ variables with integer coefficients. Fix a prime p, and suppose that there exist integers (x_i) and $0 \le j \le n$ such that $0 \le 2k < m$, where*

$$k = v_p\left(\frac{\partial f}{\partial X_j}(x_0,\dots,x_n)\right)$$
$$m = v_p(f(x_0,\dots,x_n)).$$

Then there exists $\alpha \in \mathbf{Q}_p$ such that, replacing x_j by α, we have

$$f(x_0,\dots,\alpha,\dots,x_n) = 0$$

and α is congruent to x_j modulo p^{m-k}.

Proof See Serre (1973, Chapter 2, 2.2, Theorem 1). □

In particular, Hensel's Lemma shows this: let $\bar{f}$ be the polynomial over $\mathbf{F}_p$ obtained by reducing f modulo p; then each smooth point of the variety over $\mathbf{F}_p$ defined by $\bar{f}$ lifts to a point of the variety over $\mathbf{Q}_p$ defined by f.

If p is an odd prime not dividing $a_0a_1a_2a_3$, then reducing the equation (16.2) modulo p gives a smooth surface over $\mathbf{F}_p$. In this case, to show that X is soluble in $\mathbf{Q}_p$, it is enough to show that the reduction has a point over $\mathbf{F}_p$.

The number of solutions over $\mathbf{F}_p$ to a polynomial equation is related to the topology of the complex variety defined by that equation, in a series of deep results known as the Weil conjectures. In particular, the Weil conjectures allow us to bound the number of solutions to an equation over $\mathbf{F}_p$.

Theorem 16.2.2. *The Weil conjectures.*

Corollary 16.2.3. *Let X be the diagonal quartic surface* (16.2)*. Let $p \ge 23$ be a prime not dividing $a_0a_1a_2a_3$. Then $Y(\mathbf{Q}_p) \ne \emptyset$.*

Proof Deduce this from the Weil conjectures. □

If we were looking at a diagonal *quadratic* form instead of a quartic one, then we would not have to resort to the Weil conjectures: in that case, a solution over $\mathbf{F}_p$ is guaranteed by the following theorem.

Theorem 16.2.4 (Chevalley–Warning)**.** *Let $f(x_1,\dots,x_n)$ be a homogeneous polynomial of degree d in n variables over a finite field. If $n > d$, then f has a non-trivial solution.*

192: Check precise hypotheses

Proof Reference to Serre (1973). □

When looking at a prime $p \equiv 3 \pmod 4$, we can make use of this.

Lemma 16.2.5. *Let X be defined the diagonal quartic surface* (16.2)*, and let p be a prime not dividing $a_0a_1a_2a_3$, such that $p \equiv 3 \pmod 4$. Then $X(\mathbf{Q}_p) \neq \emptyset$.*

Proof Recall that $p \equiv 3 \pmod 4$ implies that -1 is not a square in $\mathbf{F}_p$. Now the squares in $\mathbf{F}_p$ are all fourth powers: for if a is a square, with square roots $\pm x$, then the fact that -1 is not a square means that either x or $-x$ must be a square, and so a is a fourth power. Hence the surface (16.2) has a point over $\mathbf{F}_p$ if and only if there is a non-trivial solution to the equation

$$a_0X_0^2 + a_1X_1^2 + a_2X_2^2 + a_3X_3^2 = 0.$$

But this equation has a non-trivial solution, by the Chevalley–Warning theorem. □

So, for primes p not dividing $a_0a_1a_2a_3$, we can guarantee solutions in $\mathbf{Q}_p$ if $p \equiv 3 \pmod 4$ or if $p \geq 23$. Let us polish off a couple more small primes.

Lemma 16.2.6. *Let X be the diagonal quartic surface* (16.2)*. If $13 \nmid a_0a_1a_2a_3$, then $X(\mathbf{Q}_{13}) \neq \emptyset$. If $17 \nmid a_0a_1a_2a_3$, then $X(\mathbf{Q}_{17}) \neq \emptyset$.*

Proof In either case, it is a finite problem to verify that this is true. The reduction of X modulo 13 must be one of the finitely many smooth diagonal quartic surfaces over $\mathbf{F}_{13}$, and a computer search reveals that they all admit a point over $\mathbf{F}_{13}$; by Hensel's Lemma, X has a point over $\mathbf{Q}_{13}$. Similarly for 17. □

The only odd prime not addressed by either Corollary 16.2.3, Lemma 16.2.5 or Lemma 16.2.6 is 5. It turns out that there is indeed a smooth diagonal quartic over $\mathbf{F}_5$ which has no point over $\mathbf{F}_5$, namely the Fermat quartic with coefficients $(1,1,1,1)$. A computer search shows that this is the only such example, proving the following lemma.

Lemma 16.2.7. *Let X be the diagonal quartic* (16.2)*. If $5 \nmid a_0a_1a_2a_3$ and the a_i are not all equal modulo 5, then $X(\mathbf{Q}_5) \neq \emptyset$.* □

Next, we describe a method for testing solubility in $\mathbf{Q}_p$ when p does divide $a_0a_1a_2a_3$. We may assume that the coefficients a_i are coprime integers, and that no a_i is divisible by a fourth power. If we multiply each a_i by p and then remove any factors of p^4 which might have appeared, we obtain a new equation which clearly has rational solutions if and only if the original one has; but the new equation has a different reduction modulo p. Repeating this process gives four polynomials over $\mathbf{F}_p$ which are all "valid reductions modulo p" of the original variety X. We call these polynomials $\bar{f}_j$, where j takes values from 0 to 3. They might be described thus:

$$\bar{f}_j(X_0,X_1,X_2,X_3) = b_{0j}X_0^4 + b_{1j}X_1^4 + b_{2j}X_2^4 + b_{3j}X_3^4$$

where

$$b_{ij} \equiv \begin{cases} p^{-v_p(a_i)}a_i & \text{if } v_p(a_i) \equiv j \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 16.2.8. *Let p be an odd prime. The equation* (16.2) *has a solution in $\mathbf{Q}_p$ if and only if there exists a smooth point on one of the four varieties over $\mathbf{F}_p$ defined by the polynomials $\bar{f}_j$.*

Proof If there is such a smooth point, we can apply Hensel's Lemma to lift it to a point in $\mathbf{Q}_p$.

Conversely, suppose that there is a solution P in $\mathbf{P}^3(\mathbf{Q}_p)$. Write f for the defining equation of X. By continuity, we can find integers (x_0,x_1,x_2,x_3) such that

$$f(x_0,x_1,x_2,x_3) = a_0x_0^4 + a_1x_1^4 + a_2x_2^4 + a_3x_3^4$$

has arbitrarily high p-adic valuation. Now choose i_0 such that $v_p(4a_{i_0}x_{i_0}^3)$ is minimal. We may in addition ensure that $v_p(x_{i_0}) = 0$, since no a_i has valuation higher than 3 by our earlier assumptions; so, if $p \mid x_{i_0}$, then $v_p(4a_{i_0}x_{i_0}^3)$ is at least as great as any $v_p(4a_ix_i^3)$ where $p \mid x_i$, of which there is at least one. Write j for $v_p(a_{i_0})$. We now define new coefficients a_i' by

$$a_i' = \begin{cases} p^{-j}a_i & \text{if } v_p(a_i) \geq j \\ p^{4-j}a_i & \text{if } v_p(a_i) < j \end{cases}$$

and new values x_i' by

$$x_i' = \begin{cases} x_i & \text{if } v_p(a_i) \geq j \\ x_i/p & \text{if } v_p(a_i) < j \end{cases}$$

where the expression x_i/p is an integer, because otherwise we would have chosen i_0 differently. The polynomial

$$f'(X_0,X_1,X_2,X_3) = a'_0X_0^4 + a'_1X_1^4 + a'_2X_2^4 + a'_3X_3^4$$

reduces modulo p to $\bar{f}_j$. The new point (x'_0,x'_1,x'_2,x'_3) is a solution to $\bar{f}_j$ provided that we chose our original integer solution close enough to the p-adic solution; and moreover $4a'_{i_0}(x'_{i_0})^3$ is a unit in $\mathbf{F}_p$, so the point is smooth. □

For $p = 2$, small changes are needed. To apply Hensel's Lemma, we need a solution in the ring $\mathbf{Z}/32\mathbf{Z}$ with not all the a_ix_i divisible by 2. If we replace $\mathbf{F}_p$ by $\mathbf{Z}/32\mathbf{Z}$, then the same argument works, though, and we obtain

Proposition 16.2.9. *The equation* (16.2) *has a solution in* $\mathbf{Q}_2$ *if and only if one of the polynomials* $\bar{f}_j$*, considered over the ring* $\mathbf{Z}/32\mathbf{Z}$*, has a solution* (x_0,x_1,x_2,x_3) *where some* a_ix_i *is not divisible by* 2. □

Together, these last two propositions give an algorithm for testing the solubility of any diagonal quartic surface over $\mathbf{Q}$. Let us apply them to our original surface (16.1).

- At all primes p except 2 and 3, the surface X defined by (16.1) has a local solution. This comes from Corollary 16.2.3 for $p \geq 23$, Lemma 16.2.5 for $p = 3,7,11,19$, Lemma 16.2.6 for $p = 13,17$, and Lemma 16.2.7 for $p = 5$.
- The reduction of the equation (16.1) modulo 3 gives a variety over $\mathbf{F}_3$ defined by the equation $X_0^4 + X_1^4 = 0$, geometrically a union of four planes meeting in a common line. Since -1 is not a fourth power in $\mathbf{F}^3$, this variety has no points apart from those on the singular line.

  However, we can multiply the equation through by $3^3 = 27$ and remove fourth powers from a_2, a_3 to obtain the surface

$$27X_0^4 + 27X_1^4 = 2X_2^4 + 4X_3^4. \tag{16.3}$$

  The reduction of this is the variety over $\mathbf{F}_3$ defined by $X_2^4 + 2X_3^4 = 0$, which has many smooth points since -2 is a fourth power in $\mathbf{F}^3$. Therefore the equation (16.3) has solutions over $\mathbf{Q}_3$, and so does our original equation (16.1).
- To show solubility in $\mathbf{Q}_2$, Proposition 16.2.9 shows that it is enough to find a solution to (16.1) in $\mathbf{Z}/32\mathbf{Z}$ such that either X_0 or X_1 is odd. The only fourth powers in $\mathbf{Z}/32\mathbf{Z}$ are 0, 1, 16 and 17, and so it is very quick to search for solutions with a computer. The point $[1:3:1:1]$ satisfies our requirements, and so $X(\mathbf{Q}_2)$ is not empty.

Therefore the surface X is indeed everywhere locally soluble.

16.3 The Picard group

In this section we calculate the Picard group of the surface $\bar{X}$ and the Galois action on it.

To determine the Picard group over the algebraic closure, we once again put ourselves in the case of a general diagonal quartic surface (16.2). Firstly, observe that there are 48 obvious straight lines, defined over $\bar{\mathbf{Q}}$, contained in $\bar{X}$. Indeed, writing

$$a_0X_0^4 = -a_1X_1^4 \quad \text{and} \quad a_2X_2^4 = -a_3X_3^4$$

gives sixteen straight lines. These lines will be labelled L_{mn}^{123}, where m and n run through the values 1, 3, 5 and 7. In the equations of these lines, we write (as we will throughout this chapter) ε for a fixed primitive eighth root of unity, and α_{ij} for a fixed fourth root of a_i/a_j. We will choose the α_{ij} such that $\alpha_{ij}\alpha_{jk} = \alpha_{ik}$. The lines are then given by

$$L_{mn}^{123} : X_0 = \varepsilon^m\alpha_{10}X_1, \quad X_2 = \varepsilon^n\alpha_{32}X_3. \tag{16.4}$$

Similarly we define the lines

$$L_{mn}^{231} : X_0 = \varepsilon^m\alpha_{20}X_2, \quad X_3 = \varepsilon^n\alpha_{13}X_1 \tag{16.5}$$

$$L_{mn}^{312} : X_0 = \varepsilon^m\alpha_{30}X_3, \quad X_1 = \varepsilon^n\alpha_{21}X_2 \tag{16.6}$$

making 48 straight lines in all.

Proposition 16.3.1. *The 48 straight lines L_{mn}^{ijk} generate the Picard group of $\bar{X}$.*

Since this is a statement about $\bar{X}$, we may prove it for any diagonal quartic surface – they are all isomorphic over $\bar{\mathbf{Q}}$. For a highbrow proof of the proposition using reduction to a finite field, see **?**. For a more explicit proof which relies on viewing X as an elliptic fibration over $\mathbf{P}^1$, see Bright (2002).

Using the knowledge that the 48 lines generate the Picard group, we can easily prove

Proposition 16.3.2. *The Picard group of $\bar{X}$ is free of rank* 20.

Proof On a K3 surface, divisors are linearly equivalent if and only if they are numerically equivalent. The intersection matrix of the 48 lines is straightforward to write down: two lines have intersection number 1 if they meet, and 0 otherwise. The self-intersection number of a straight line is -2, as can be seen from the Riemann–Roch theorem. Let Λ denote the free $\mathbf{Z}$-module generated by the 48 lines. We can write down the 48×48 intersection matrix $\mathbf{Q}$, and the subgroup $\Lambda^0 \subset \Lambda$ of principal divisors is the kernel of $\mathbf{Q}$. The Picard group is isomorphic to the quotient of Λ by Λ^0, so is naturally isomorphic to the image

193: Find a reference or prove this.

space of $\mathbf{Q}$. Reducing $\mathbf{Q}$ to echelon form, we find that it has rank 20. This shows that $\operatorname{Pic}\bar{X}$ is free of rank 20, and gives a 20×48 matrix representing the quotient map $\Lambda\to\operatorname{Pic}\bar{X}$. A further calculation in linear algebra gives a basis for $\operatorname{Pic}\bar{X}$ consisting of integer linear combinations of the 48 lines. □

Now let us return to the specific surface (16.1). The 48 lines are all defined over the field

$$K=\mathbf{Q}(\varepsilon,\sqrt[4]{2},\sqrt[4]{3})$$

which is an extension of degree 32 over $\mathbf{Q}$. Therefore $\operatorname{Pic}\bar{X}=\operatorname{Pic}X_K$, and the Galois action of $\operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $\operatorname{Pic}\bar{X}$ factors through $\operatorname{Gal}(K/\mathbf{Q})$. As in **??**, we deduce that the inflation map $\operatorname{Infl}:\mathrm{H}^1(\operatorname{Gal}(K/\mathbf{Q}),\operatorname{Pic}X_K)\to\mathrm{H}^1(\mathbf{Q},\operatorname{Pic}\bar{X})$ is an isomorphism. Fortunately, the Galois group of $K/\mathbf{Q}$ is easy to describe, since K is a Kummer extension of $\mathbf{Q}(i)$. For background information on Kummer extensions, see [somewhere]. The general theory gives the following result.

194: Find reference

Proposition 16.3.3. *The Galois group* $\operatorname{Gal}(K/\mathbf{Q})$ *is of order 32, generated by the following three elements:*

$$\begin{aligned}
&\tau\colon i\mapsto -i, && \sqrt[4]{2}\mapsto\sqrt[4]{2}, && \sqrt[4]{3}\mapsto\sqrt[4]{3};\\
&\sigma_1\colon i\mapsto i, && \sqrt[4]{2}\mapsto i\sqrt[4]{2}, && \sqrt[4]{3}\mapsto\sqrt[4]{3};\\
&\sigma_2\colon i\mapsto i, && \sqrt[4]{2}\mapsto\sqrt[4]{2}, && \sqrt[4]{3}\mapsto i\sqrt[4]{3}.
\end{aligned}$$

The group structure is defined by

$$\begin{gathered}
\tau^2=1,\quad \sigma_1^4=1,\quad \sigma_2^4=1;\\
\sigma_1\sigma_2=\sigma_2\sigma_1,\quad \tau\sigma_1\tau=\sigma_1^{-1},\quad \tau\sigma_2\tau=\sigma_2^{-1}.
\end{gathered}$$

Proof The first statement is Kummer theory; the second follows by direct calculation from the first. □

Since we know how the generators of the Galois group act on K, we know how they act on the coefficients in the defining polynomials of the 48 lines, and hence on the 48 lines themselves, and on the free $\mathbf{Z}$-module Λ which they generate. Since the Galois action preserves intersection numbers, $\operatorname{Gal}(K/\mathbf{Q})$ also acts on the quotient of Λ by the kernel of the intersection matrix, which is isomorphic to $\operatorname{Pic}X_K$. Some linear algebra gives us three 20×20 matrices describing how τ,σ_1,σ_2 act on our chosen basis of $\operatorname{Pic}X_K$.

So we now have an explicit finite group $G=\operatorname{Gal}(K/\mathbf{Q})$, a finitely generated free $\mathbf{Z}$-module $\operatorname{Pic}X_K$ with an explicit basis, and explicit matrices for the action of G on that basis. It is therefore a straightforward, though large, calculation

in linear algebra to write down matrices for the maps

$$C^0(G,\mathrm{Pic}\,X_K) \xrightarrow{d_0} C^1(G,\mathrm{Pic}\,X_K) \xrightarrow{d_1} C^2(G,\mathrm{Pic}\,X_K)$$

between cochain groups, which are finitely generated $\mathbf{Z}$-modules, and hence calculate the cohomology group $\mathrm{H}^1(G,\mathrm{Pic}\,X_K)$. We find:

Proposition 16.3.4. $\mathrm{H}^1(G,\mathrm{Pic}\,X_K) \cong \mathrm{H}^1(\mathbf{Q},\mathrm{Pic}\,\bar{X})$ *has order* 2. □

Of course, we also find explicitly a generator for $\mathrm{H}^1(G,\mathrm{Pic}\,X_K)$; but it would be neither informative nor attractive to reproduce it here.

16.4 An Azumaya algebra

16.4.1 A smaller splitting field

At this stage we know that $\mathrm{Br}\,X/\mathrm{Br}\,\mathbf{Q}$ has order 2, and that an Azumaya algebra on X representing the non-trivial class is split by the extension $K/\mathbf{Q}$ of the base field. But dealing with cohomology groups is much easier for extensions of small degree, and so we might hope that there is some smaller splitting field contained in K. The best possible outcome would be to find a cyclic extension of $\mathbf{Q}$ which splits the algebra. In that case, we will be able to use Proposition **??** to write the Azumaya algebra as a cyclic algebra over $\kappa(X)$, which will make things easier when it comes to evaluating the obstruction.

195: Is this conjectured to always exist? Period-index problem; proved by de Jong for alg. closed base field.

The search for a splitting field can be done purely algebraically, as follows. Any normal subgroup H of G corresponds to a Galois field extension $l/\mathbf{Q}$ contained in K, and we have the inflation-restriction exact sequence:

196: Add reference for inf-res

$$0 \to \mathrm{H}^1(\mathrm{Gal}(l/\mathbf{Q}),(\mathrm{Pic}\,X_K)^H) \xrightarrow{\mathrm{Infl}} \mathrm{H}^1(G,\mathrm{Pic}\,X_K) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(H,\mathrm{Pic}\,X_K).$$

Recall from **??** that, since X has points everywhere locally, $(\mathrm{Pic}\,X_K)^H = \mathrm{Pic}\,X_l$. It is again a matter of linear algebra to compute $\mathrm{H}^1(H,\mathrm{Pic}\,X_K)$ in the same way as we found $\mathrm{H}^1(G,\mathrm{Pic}\,X_K)$, and to find the restriction map between the two groups explicitly.

To look for a cyclic splitting field, we list all normal subgroups H of G such that the quotient G/H is cyclic. There are 7 of these, all of index 2, corresponding to the 7 quadratic extensions of $\mathbf{Q}$ contained in K. Calculating the restriction map for each one reveals that there are two quadratic extensions which split the non-trivial element of $\mathrm{H}^1(G,\mathrm{Pic}\,X_K)$: they are $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{2})$. From now we will take the splitting field to be $l = \mathbf{Q}(i)$. We have strengthened Proposition 16.3.4 to the following:

Proposition 16.4.1. *The inflation map* $\mathrm{Infl} : \mathrm{H}^1(l/\mathbf{Q}, \mathrm{Pic}\, X_l) \to \mathrm{H}^1(\mathbf{Q}, \mathrm{Pic}\, \bar{X})$ *is an isomorphism, and both groups have order* 2. □

16.4.2 A quaternion algebra

Now that we are in the happy position of knowing that the non-constant class of algebraic Azumaya algebras on X is represented by a quaternion algebra, we would like to write down that algebra. Recall from Proposition **??** that we are looking for a quaternion algebra over $\kappa(X)$, the function field of X, of the form $(-1, f) = (l/\mathbf{Q}, f)$. Here f should be a rational function on X such that $(f) = N_{l/\mathbf{Q}} D$, where $D \in \mathrm{Div}\, X_l$ is a non-principal divisor defined over l. In other words, the norm of the class $[D] \in \mathrm{Pic}\, X_l$ is the trivial class. Recall the notation of Exercise 14.5.1: letting σ denote a generator of $\mathrm{Gal}(l/\mathbf{Q})$, we denote $\sigma + 1$ by N and $\sigma - 1$ by Δ. One way to find a suitable D would be to follow through the isomorphisms

$$\mathrm{H}^1(G, \mathrm{Pic}\, X_K) \cong \mathrm{H}^1(l/\mathbf{Q}, \mathrm{Pic}\, X_l) \cong {}_N\mathrm{Pic}\, X_l / \Delta \mathrm{Pic}\, X_l$$

but there is no need to do this. We can compute the quotient ${}_N\mathrm{Pic}\, X_l / \Delta \mathrm{Pic}\, X_l$ from scratch, knowing that it will be of order 2, and take D to a representative of the non-trivial class. (There is a unique isomorphism between any two groups of order 2, so we don't have to worry!)

Recall that we know $\mathrm{Pic}\, X_K$ explicitly as a quotient of the free Abelian group on the 48 lines, and we have matrices describing the action of $G = \mathrm{Gal}(K/\mathbf{Q})$ on that quotient. Given generators for H, that allows us to compute $\mathrm{Pic}\, X_l$ as a subgroup of $\mathrm{Pic}\, X_K$. We find that $\mathrm{Pic}\, X_l$ has rank 3. The quotient G/H is generated by complex conjugation τ, and after a little more linear algebra we compute a 3×3 matrix $\mathbf{M}$ for the action of τ on $\mathrm{Pic}\, X_l$. Now ${}_N\mathrm{Pic}\, X_l / \Delta X_l$ is explicitly presented as the quotient of $\ker(\mathbf{M} + \mathbf{I_3})$ by $\mathrm{Im}(\mathbf{M} - \mathbf{I_3})$, and this indeed turns out to have order 2.

Unfortunately, there is another obstacle to writing down our quaternion algebra. What our calculations have given us is a divisor class $[D] \in \mathrm{Pic}\, X_l$. Now, since our surface X has points everywhere locally, this divisor class contains a divisor D defined over l (see Section 4.2). Since $N_{l/\mathbf{Q}} D$ is principal, there is a function f defined over $\mathbf{Q}$ with $(f) = N_{l/\mathbf{Q}} D$, and the Azumaya algebra we are looking for is $(l/\mathbf{Q}, f)$. However, we have not yet found the divisor D. Let us recall the situation so far. We have Λ, a free Abelian group of rank 48 with an action of the finite group G, representing the subgroup of $\mathrm{Div}\, X_K$ generated by the 48 lines. We have a G-invariant linear map $c\colon \Lambda \to \mathrm{Pic}\, X_K$, represented explicitly as a 20×48 integer matrix, taking a sum of lines to its divisor class. And we have, in $\mathrm{Pic}\, X_K$, an element $[D]$ which is fixed by $H = \mathrm{Gal}(K/l)$ such

that $N_{l/\mathbf{Q}}[D] = 0$. Although every divisor class on X can be represented by a sum of lines, we are seeking a divisor D defined over l, and there is absolutely no reason to believe that the divisor class $[D]$ contains a sum of lines defined over l. In fact, we can verify that this is not the case: restricting the linear map c to the subgroup of Λ fixed by H, we find that $[D]$ does not lie in the image $c(\Lambda^H)$.

¡¡¡¡¡¡¡ example.tex The problem of finding l-rational divisors in l-rational divisor classes comes down, theoretically, to explicitly finding rational points on a Severi–Brauer variety which is known to have points everywhere locally. For curves, this problem has been approached by Bruin and Flynn (2004). For surfaces, the theory is the same, but a general algorithm would be significantly more complicated than the one described there. In our case we are lucky in that, although there is no sum of lines in the class $[D]$ defined over l, there is a sum of lines in that equivalence class defined over a quadratic extension of l. This makes the next step of the calculation much easier than having to start from a representative defined only over K.

To find this out, we can do the following. Let H' run through all subgroups of index 2 in H. For each, compute $\Lambda^{H'}$ and test whether $[D]$ lies in the image $c(\Lambda^{H'})$. Fortunately one H' passes this test, which is the subgroup corresponding to the field $L = l(\sqrt{2}) = \mathbf{Q}(\varepsilon)$. Taking the inverse image of $[D]$ under the map c gives a representative defined over L:

Proposition 16.4.2. *The divisor*

$$D_L = L_{33}^{123} + L_{37}^{123} + L_{53}^{123} + L_{57}^{123} - L_{71}^{123} - L_{73}^{123} - L_{75}^{123} - L_{77}^{123}$$

is defined over L and lies in the divisor class $[D]$. □

The next step is to find a divisor linearly equivalent to D_L but which is defined over l. In Section 6.1 we saw how to describe the family of *effective* divisors equivalent to a given divisor. However, using the intersection numbers of the lines, we can see that $D \cdot H = 0$, where H is any plane section; so any effective divisor linearly equivalent to D would have to satisfy this property too. The only such effective divisor is the zero divisor, and we already know that D_L is not principal. Therefore D_L is not equivalent to any effective divisor. The way round this is to use Example 6.5.4: by adding a hyperplane section to D_L, we ensure that there are effective divisors equivalent to it. A hyperplane section which will work very well is

$$H_L = L_{71}^{123} - L_{73}^{123} - L_{75}^{123} - L_{77}^{123}$$

which is defined over L, and has the advantage that adding it to D_L produces a

simpler-looking (and indeed effective) divisor. We set

$$D^+ = D_L + H_L = L_{33}^{123} + L_{37}^{123} + L_{53}^{123} + L_{57}^{123}.$$

Let σ denote the non-trivial automorphism of L/l. As D_L represents a divisor class fixed by σ, we know that $(D_L)^\sigma$ lies in the same divisor class. The same applies to D^+, bearing in mind that the hyperplane class is also fixed by σ. So we already know two distinct effective divisors in the class $[D^+]$: they are D^+ itself and its conjugate $(D^+)^\sigma$. This means that we also know two linearly independent elements of the vector space $L(D^+)$: the constant function 1 and the rational function h (unique up to multiplication by a constant) such that $(h) = (D^+)^\sigma - D^+$. To actually write down h, we can do the following:

(i) Pick a positive integer d, which we hope will be the degree of the numerator and denominator of h.
(ii) Try, by linear algebra, to find a homogeneous form G of degree d in X_0, X_1, X_2, X_3 which vanishes on D^+. If no such form exists, increase d and try again. (We will succeed eventually. Why?)
(iii) Although G vanishes on D^+, it also vanishes elsewhere on X; compute this residual divisor E.
(iv) By linear algebra, find a homogeneous form F of degree d which vanishes on both E and $(D^+)^\sigma$.
(v) The rational function $h = F/G$ satisfies $(h) = (D^+)^\sigma - D^+$.

Carrying this out, we find that $d = 2$ suffices, and produce the rational function

$$h = \frac{X_0^2 - \sqrt{2}X_0X_1 + X_1^2}{X_2^2 + i\sqrt{2}X_3^2}$$

This function has the curious property that $N_{L/l}h$ is constant on X, since its divisor is 0. Indeed, multiplying out gives

$$\begin{aligned} N_{L/l}h &= \left(\frac{X_0^2 - \sqrt{2}X_0X_1 + X_1^2}{X_2^2 + i\sqrt{2}X_3^2}\right)\left(\frac{X_0^2 + \sqrt{2}X_0X_1 + X_1^2}{X_2^2 - i\sqrt{2}X_3^2}\right) \\ &= \frac{X_0^4 + X_1^4}{X_2^4 + 2X_3^4} = 6. \end{aligned}$$

Having our hands on two independent elements of $L(D^+)$ means that we now have many effective divisors linearly equivalent to D^+: as described in Section 6.1, any function of the form $a + bh$, where $a, b \in L$, has a pole of order 1 along D^+ and vanishes along an effective divisor linearly equivalent to D^+. We have not proved that $L(D^+)$ has dimension exactly 2, although this is

actually true; but the fact that L/l is of degree 2 means that we won't have to look any further for a divisor defined over l.

Proposition 16.4.3. *Let $a \in L$ such that $N_{L/l}a = N_{L/l}h$. Then the rational function $(h-a)$ has a pole along D^+ and vanishes along a divisor defined over l.*

Proof We have

$$h(h-a)^\sigma = N_{L/l}h - ha^\sigma = N_{L/l}a - ha^\sigma = -a^\sigma(h-a).$$

Let D_a denote the divisor of vanishing of $(h-a)$. Taking divisors on both sides gives

$$((D^+)^\sigma - D^+) + (D_a - D^+)^\sigma = (D_a - D^+)$$

and so $D_a^\sigma = D_a$, meaning that D_a is defined over l. □

Solving the equation $N_{L/l}(a) = 6$ can be viewed as finding a rational point on a conic defined over l: see **?**. In this particular case, it is easy enough to solve by inspection: we seek $\alpha, \beta \in \mathbf{Q}(i)$ such that $\alpha^2 - 2\beta^2 = 6$. A solution is $\alpha = 2, \beta = i$ and so $a = 2 + i\sqrt{2}$.

The existence of such an a is a consequence of the fact that X is everywhere locally soluble: for each place w of L lying over a place v of l, there is a point in $X(L_w)$ and so, by the p-adic inverse function theorem, a point P_w of $X(L_w)$ not lying on either D^+ or $(D^+)^\sigma$. Evaluating h at such a point gives $N_{L_w/l_v}(h(P_w)) = (N_{L/l}h)(P_w) = 6$, so there exists an element of L_w with norm 6. Since L/l is cyclic, the Hasse norm theorem (**?**) implies that there is an element of L having norm 6. ======= It is here that the algorithm described in **??** comes to our rescue. Trying all subgroups $H' \subset H$ of index 2 in H, we find one such H' with the property that there is indeed an element of $\Lambda^{H'}$ mapping to $[D]$ under c. The fixed field of H' is $L = l(\sqrt{2}) = \mathbf{Q}(i, \sqrt{2})$, and the sum of lines

$$D' = L^? + L^? + L^? + L^? - (L^? + L^? + L^? + L^?)$$

is fixed by H' (and hence defined over L), and lies in our favoured divisor class $[D]$.

¿¿¿¿¿¿¿ 1.9

Appendix A

Summary of algebraic properties

- Tensor products and hom stuff.
- Diagram 1
- Diagram 2
- Hairy properties of Brauer groups, relationships between different definitions, counterexamples to naïve properties.

  ... such as:

- Make sure Br is defined as Br_{Az} as Damiano does in his chapter.
- Define $\mathrm{Br}_{\text{ét}} X = H^2_{\text{ét}}(X, \mathbb{G}_m)$.
- Structure of Brauer group, defining $\mathrm{Br}_1 X = \ker \mathrm{Br} X \to \mathrm{Br} \bar{X}$.
-

$$\begin{array}{ccccc} \mathrm{Br} X & \longrightarrow & \mathrm{Br}_{\text{ét}} X & \longrightarrow & \mathrm{Br}\,\kappa(X) \\ \uparrow & & \uparrow & & \uparrow{=} \\ (\mathrm{Br} X)_{\mathrm{tors}} & \longrightarrow & (\mathrm{Br}_{\text{ét}} X)_{\mathrm{tors}} & \longrightarrow & (\mathrm{Br}\,\kappa(X))_{\mathrm{tors}} \end{array}$$

  left vertical arrow is equality if only finitely many components. top-right horizontal arrow is injective when X is regular, integral and noetherian. bottom-left horizontal arrow is isomorphusm if X is quasi-projective over a noetherian ring A (de Jong).

- $$\begin{array}{ccccc}
\mathrm{Br}\,\bar{X} & \longrightarrow & \mathrm{Br}_{\text{ét}}\,\bar{X} & \longrightarrow & H^2(\kappa(\bar{X}), \overline{\kappa(X)}^{\times}) \\
\uparrow & & \uparrow & & \uparrow \\
\mathrm{Br}\,X & \longrightarrow & \mathrm{Br}_{\text{ét}}\,X & \longrightarrow & H^2(\kappa(X), \overline{\kappa(X)}^{\times}) \\
\uparrow & & \uparrow & & \\
\mathrm{Br}_1\,X & \longrightarrow & \mathrm{Br}_{\text{ét}\,1}X & \longrightarrow & H^2(\kappa(\bar{X})/\kappa(X), \kappa(\bar{X})^{\times}) \longrightarrow H^2(k, \mathrm{Div}\,\bar{X})
\end{array}$$

  vertical sequences are exact, last part of bottom sequence is exact. Isn't $\mathrm{Br}_{\text{ét}\,1}X$ always torsion? I.e., under which conditions is $\mathrm{Br}_1 / \mathrm{Br}_0$ isomorphic to $\mathrm{H}^1(k, \mathrm{Pic}\,\bar{X})$?

References

Antieau, Benjamin, and Williams, Ben. 2014. Unramified division algebras do not always contain Azumaya maximal orders. *Invent. Math.*, **197**(1), 47–56.

Atiyah, M. F., and Macdonald, I. G. 1969. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont.

Auslander, Bernice. 1966. The Brauer group of a ringed space. *J. Algebra*, **4**, 220–273.

Auslander, Maurice, and Brumer, Armand. 1968. Brauer groups of discrete valuation rings. *Nederl. Akad. Wetensch. Proc. Ser. A 71=Indag. Math.*, **30**, 286–296.

Auslander, Maurice, and Buchsbaum, David A. 1957. Homological dimension in local rings. *Trans. Amer. Math. Soc.*, **85**, 390–405.

Auslander, Maurice, and Goldman, Oscar. 1960. The Brauer group of a commutative ring. *Trans. Amer. Math. Soc.*, **97**, 367–409.

Azumaya, Gorô. 1951. On maximally central algebras. *Nagoya Math. J.*, **2**, 119–150.

Bass, Hyman. 1967. *Lectures on topics in algebraic K-theory*. Notes by Amit Roy. Tata Institute of Fundamental Research Lectures on Mathematics, No. 41. Tata Institute of Fundamental Research, Bombay.

Bass, Hyman. 1968. *Algebraic K-theory*. W. A. Benjamin, Inc., New York-Amsterdam.

Basu, Saugata, Pollack, Richard, and Roy, Marie-Françoise. 2006. *Algorithms in real algebraic geometry*. Second edn. Algorithms and Computation in Mathematics, vol. 10. Springer-Verlag, Berlin.

Beauville, Arnaud. 1996. *Complex algebraic surfaces*. Second edn. London Mathematical Society Student Texts, vol. 34. Cambridge: Cambridge University Press. Translated from the 1978 French original by R. Barlow, with assistance from N. I. Shepherd-Barron and M. Reid.

Birch, B. J., and Swinnerton-Dyer, H. P. F. 1975. The Hasse problem for rational surfaces. *J. Reine Angew. Math.*, **274/275**, 164–174. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III.

Bourbaki, N. 2012. *Éléments de mathématique. Algèbre. Chapitre 8. Modules et anneaux semi-simples*. Springer, Berlin. Second revised edition of the 1958 edition [MR0098114].

Bourbaki, Nicolas. 1998. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Berlin: Springer-Verlag. Translated from the French, Reprint of the 1989 English translation.

Bright, Martin. 2002. *Computations on Diagonal Quartic Surfaces*. Ph.D. thesis, University of Cambridge. .

Bright, Martin J. 2013. Brauer groups of singular del Pezzo surfaces. *Michigan Math. J.*, **62**(3), 657–664.

Bright, Martin James, and Swinnerton-Dyer, Sir Peter 2004. Computing the Brauer–Manin obstructions. *Math. Proc. Cambridge Philos. Soc.*, **137**(1), 1–16.

Bruin, N., and Flynn, E. V. 2004. Rational divisors in rational divisor classes. Pages 132–139 of: *Algorithmic number theory*. Lecture Notes in Comput. Sci., vol. 3076. Berlin: Springer.

Cassels, J. W. S. 1986. *Local fields*. London Mathematical Society Student Texts, vol. 3. Cambridge University Press, Cambridge.

Châtelet, François. 1944. Variations sur un thème de H. Poincaré. *Ann. Sci. École Norm. Sup. (3)*, **61**, 249–300.

Childs, Lindsay N. 1976. On Brauer groups of some normal local rings. Pages 1–15. Lecture Notes in Math., Vol. 549 of: *Brauer groups (Proc. Conf., Northwestern Univ., Evanston, Ill., 1975)*. Springer, Berlin.

Colliot-Thélène, J.-L. 1980. Formes quadratiques multiplicatives et variétés algébriques: deux compléments. *Bull. Soc. Math. France*, **108**(2), 213–227.

Colliot-Thélène, J.-L. 1995. Birational invariants, purity and the Gersten conjecture. Pages 1–64 of: *K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992)*. Proc. Sympos. Pure Math., vol. 58. Providence, RI: Amer. Math. Soc.

Colliot-Thélène, Jean-Louis, and Swinnerton-Dyer, Sir Peter 1994. Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties. *J. Reine Angew. Math.*, **453**, 49–112.

Cox, David A., Little, John, and O'Shea, Donal. 2015. *Ideals, varieties, and algorithms*. Fourth edn. Undergraduate Texts in Mathematics. Springer, Cham. An introduction to computational algebraic geometry and commutative algebra.

de Jong, A.J. *A result of Gabber*. `http://www.math.columbia.edu/~dejong/papers/2-gabber.pdf`.

Deligne, Pierre. 1974. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, 273–307.

Demazure, Michel. 1980. Surfaces de Del Pezzo - II. *Séminaire sur les Singularités des Surfaces*, **777**, viii+339. eds. Demazure, Michel and Pinkham, Henry Charles and Teissier, Bernard, Held at the Centre de Mathématiques de l'École Polytechnique, Palaiseau, 1976–1977.

DeMeyer, F. R., and Ford, T. J. 1992. Nontrivial, locally trivial Azumaya algebras. Pages 39–49 of: *Azumaya algebras, actions, and modules (Bloomington, IN, 1990)*. Contemp. Math., vol. 124. Providence, RI: Amer. Math. Soc.

DeMeyer, Frank, and Ingraham, Edward. 1971. *Separable algebras over commutative rings*. Lecture Notes in Mathematics, Vol. 181. Springer-Verlag, Berlin-New York.

Eisenbud, David. 1995. *Commutative algebra with a view toward algebraic geometry*. Graduate Texts in Mathematics, vol. 150. New York: Springer-Verlag.

Eisenbud, David, and Harris, Joe. 2000. *The geometry of schemes*. Graduate Texts in Mathematics, vol. 197. New York: Springer-Verlag.

Enriques, Federigo. 1897. 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**(1), 1–23.

Fisher, Benji. 1997. A note on Hensel's lemma in several variables. *Proc. Amer. Math. Soc.*, **125**(11), 3185–3189.

Freitag, Eberhard, and Kiehl, Reinhardt. 1988. *Étale cohomology and the Weil conjecture*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 13. Springer-Verlag, Berlin. Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné.

Gille, Philippe, and Szamuely, Tamás. 2006. *Central simple algebras and Galois cohomology*. Cambridge Studies in Advanced Mathematics, vol. 101. Cambridge: Cambridge University Press.

Greenberg, Marvin J. 1969. *Lectures on forms in many variables*. W. A. Benjamin, Inc., New York-Amsterdam.

Grothendieck, Alexander. 1968. Le Groupe de Brauer I, II, III. Pages 46–188 of: Giraud, Jean, et al. (eds), *Dix Exposés sur la Cohomologie des Schémas*. Advanced studies in mathematics, vol. 3. Amsterdam: North-Holland.

Harari, David. 1994. Méthode des fibrations et obstruction de Manin. *Duke Math. J.*, **75**(1), 221–260.

Hartshorne, Robin. 1977. *Algebraic geometry*. Graduate Texts in Mathematics, vol. 52. New York: Springer-Verlag.

Hoobler, Raymond T. 1980. A cohomological interpretation of Brauer groups of rings. *Pacific J. Math.*, **86**(1), 89–92.

Hoobler, Raymond T. 1982. When is $\mathrm{Br}(X) = \mathrm{Br}'(X)$? Pages 231–244 of: *Brauer groups in ring theory and algebraic geometry (Wilrijk, 1981)*. Lecture Notes in Math., vol. 917. Berlin: Springer.

Kollár, János. 1996. *Rational curves on algebraic varieties*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 32. Springer-Verlag, Berlin.

Kollár, János. 2002. Unirationality of cubic hypersurfaces. *J. Inst. Math. Jussieu*, **1**(3), 467–476.

Kollár, János, Smith, Karen E., and Corti, Alessio. 2004. *Rational and nearly rational varieties*. Cambridge Studies in Advanced Mathematics, vol. 92. Cambridge: Cambridge University Press.

Kresch, Andrew, and Tschinkel, Yuri. 2008. Effectivity of Brauer-Manin obstructions. *Adv. Math.*, **218**(1), 1–27.

Lang, Serge, and Weil, André. 1954. Number of points of varieties in finite fields. *Amer. J. Math.*, **76**, 819–827.

Lind, Carl-Erik. 1940. Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins. *Thesis, University of Uppsala,*, **1940**, 97.

Manin, Y. I. 1971. Le groupe de Brauer-Grothendieck en géométrie diophantienne. Pages 401–411 of: *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*. Paris: Gauthier-Villars.

Manin, Yu. I. 1986. *Cubic forms*. Second edn. North-Holland Mathematical Library, vol. 4. Amsterdam: North-Holland Publishing Co. Algebra, geometry, arithmetic, Translated from the Russian by M. Hazewinkel.

Merkurjev, A. S. 1981. On the norm residue symbol of degree 2. *Dokl. Akad. Nauk SSSR*, **261**(3), 542–547.

Merkurjev, A. S., and Suslin, A. A. 1982. K-cohomology of Severi-Brauer varieties and the norm residue homomorphism. *Izv. Akad. Nauk SSSR Ser. Mat.*, **46**(5), 1011–1046, 1135–1136.

Millar, Judith R. 2010. *K-theory of Azumaya algebras*. Ph.D. thesis, Queen's University, Belfast. arXiv:1101.1468.

Milne, James S. 1980. *Étale cohomology*. Princeton Mathematical Series, vol. 33. Princeton, N.J.: Princeton University Press.

Milne, James S. 2008. *Class Field Theory*. `http://www.jmilne.org/math/CourseNotes/math776.html`.

Néron, André. 1964. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Inst. Hautes Études Sci. Publ.Math. No.*, **21**, 128.

Platonov, Vladimir, and Rapinchuk, Andrei. 1994. *Algebraic groups and number theory*. Pure and Applied Mathematics, vol. 139. Academic Press, Inc., Boston, MA. Translated from the 1991 Russian original by Rachel Rowen.

Poonen, Bjorn. 2008. *Rational points on varieties*. `http://math.mit.edu/~poonen/math274.html`.

Reichardt, Hans. 1942. Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen. *J. Reine Angew. Math.*, **184**, 12–18.

Roquette, Peter. 2005. *The Brauer-Hasse-Noether theorem in historical perspective*. Schriften der Mathematisch-Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften [Publications of the Mathematics and Natural Sciences Section of Heidelberg Academy of Sciences], vol. 15. Springer-Verlag, Berlin.

Serre, Jean-Pierre. 1968. *Corps locaux*. Paris: Hermann. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

Serre, Jean-Pierre. 1973. *A course in arithmetic*. New York: Springer-Verlag. Translated from the French, Graduate Texts in Mathematics, No. 7.

Serre, Jean-Pierre. 2006. *Lie algebras and Lie groups*. Lecture Notes in Mathematics, vol. 1500. Springer-Verlag, Berlin. 1964 lectures given at Harvard University, Corrected fifth printing of the second (1992) edition.

Shatz, Stephen S. 1972. *Profinite groups, arithmetic, and geometry*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo. Annals of Mathematics Studies, No. 67.

Skorobogatov, Alexei. 2001. *Torsors and rational points*. Cambridge Tracts in Mathematics, vol. 144. Cambridge: Cambridge University Press.

Stacks Project. 2015. *Stacks Project*. `http://stacks.math.columbia.edu`.

Swinnerton-Dyer, H. P. F. 1962. Two special cubic surfaces. *Mathematika*, **9**, 54–56.

Swinnerton-Dyer, H. P. F. 1972. Rational points on del Pezzo surfaces of degree 5. Pages 287–290 of: *Algebraic geometry, Oslo 1970 (Proc. Fifth Nordic Summer School in Math.)*. Groningen: Wolters-Noordhoff.

Várilly-Alvarado, Anthony. 2013. Arithmetic of del Pezzo surfaces. Pages 293–319 of: *Birational geometry, rational curves, and arithmetic*. Springer, New York.

Weibel, Charles A. 2013. *The K-book*. Graduate Studies in Mathematics, vol. 145. American Mathematical Society, Providence, RI. An introduction to algebraic K-theory.

Weil, André. 1948. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris.