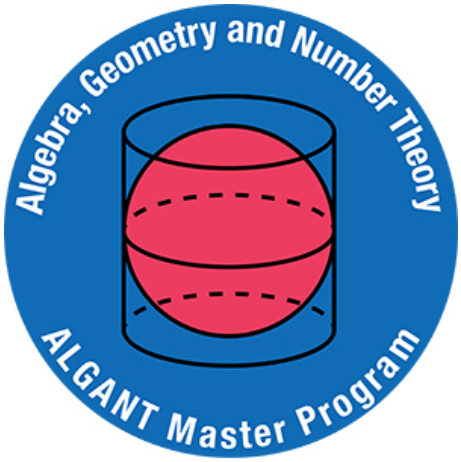


ALGANT Master Thesis in Mathematics

THE BRAUER-MANIN OBSTRUCTION TO STRONG APPROXIMATION

Sebastiano Tronto

Advised by Dr. Martin J. Bright

UNIVERSITÀ DI MILANO

UNIVERSITEIT LEIDEN

Academic year 2017/2018
25 June 2018

Contents

Introduction

Our goal is, broadly speaking, to study Diophantine Equations. They are, in a sense, simple questions about the most fundamental mathematical objects: integer numbers, with their natural operations (addition and multiplication). This means that we are given a polynomial with integer coefficients $F(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ and we want to study the set of solutions of

$$F(x_1, \dots, x_n) = 0 \quad \text{in } x_1, \dots, x_n \in \mathbb{Z}.$$

This kind of problem is so simple in its formulation that it has been considered at least since the III century A.D., by Diophantus of Alexandria (hence the name "Diophantine").

However, as often happens in Mathematics in general, and in Number Theory in particular, a simple question doesn't necessarily have a simple answer. A famous example is *"Fermat's Last Theorem"*, that should now be referred to as Wiles' Theorem.

Theorem 0.1. *Let $n \geq 3$ be an integer. The equation*

$$x^n + y^n = z^n \quad \textit{in } x, y, z \in \mathbb{Z}_{>0}$$

has no solution.

The Theorem was conjectured by Fermat in 1637, but the first correct proof was given by Wiles in 1994, after three and a half centuries of effort by mathematicians. In his proof, Wiles uses advanced geometric techniques.

To see how geometry can come into play, consider the following example. Assume we want to compute *Pythagorean triples*, that is positive integer solutions (a, b, c) to the equation

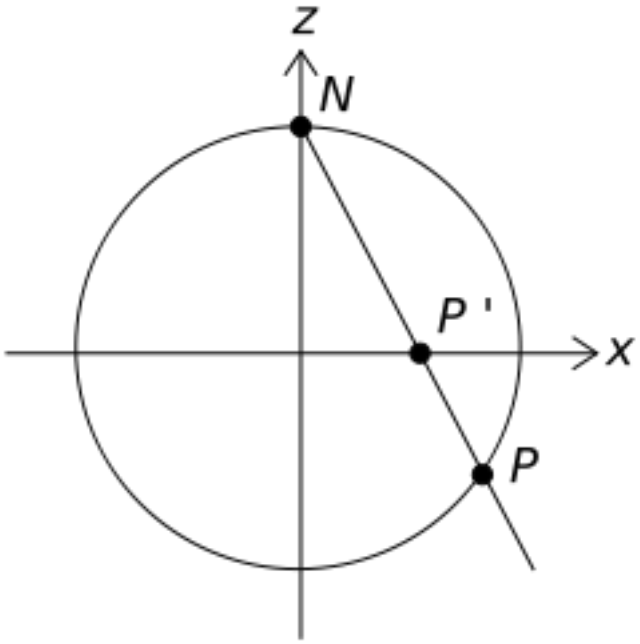
$$a^2 + b^2 = c^2.$$

Since the equation is homogeneous, we have that if (a, b, c) is a solution, then for any $\lambda \in \mathbb{Z}_{>0}$ also $(\lambda a, \lambda b, \lambda c)$ is a solution. Vice versa, if a, b and c have a common factor d, we can divide them by d to get another solution. We conclude that we can restrict our attention to *coprime* solutions, that is such that $\gcd(a, b, c) = 1$. These are also called *primitive* Pythagorean triples.

Now we can divide by c and look for rational solutions $(x, z) = \left(\frac{a}{c}, \frac{b}{c}\right)$ of the equation

$$x^2 + z^2 = 1.$$

This equation defines a circle in the Cartesian plane, and we can use the stereographic projection from $N = (0, 1)$ to parametrize its *rational points*, that is points with rational coordinates.



That is, if $P' = \left(\frac{m}{n}, 0\right)$ for some coprime integers m, n, the image of P' is

$$P = \left(\frac{2mn}{m^2+n^2}, \frac{m^2-n^2}{m^2+n^2}\right)$$

so every rational point on the unit circle can be written in this form for some pair of coprime integers (m, n).

Let $a = 2mn$, $b = m^2 - n^2$ and $c = m^2 + n^2$, so that $a^2 + b^2 = c^2$. It can be seen that $\gcd(a, b, c) = 1$ if and only if m and n are coprime and not both odd, and that up to swapping a and b all primitive triples can be obtained in this way.

This gives what is known as *Euler's formula*: all primitive Pythagorean triples (a, b, c) are of the form

$$a = 2mn \qquad b = m^2 - n^2 \qquad c = m^2 + n^2$$

for some pair of distinct coprime integers (m, n), not both odd.

The circle in the Cartesian plane is an example of *algebraic variety*, a geometric object defined by a polynomial equation. Given this geometric object, what we are interested in is the set of its rational points, which are the solutions to the equation we started with.

With this connection between Geometry and Arithmetic in mind, we are going to use geometric techniques to study the set of solutions of Diophantine equations. More precisely, we will be concerned with the study of *projective quadric surfaces*, that are two-dimensional varieties defined by a single homogeneous polynomial equation of degree two.

The first four chapters are devoted to the prerequisites; we will cite most of the results without giving proofs. After a first chapter of geometric background, we are going to introduce Hasse's local-global principle in Chapter 2, which will be our guiding principle. In Chapters 3 and 4 we develop the theory necessary to define the Brauer group and the Brauer-Manin obstruction.

In the last chapter, the only one containing some original work, we approach the main topic of this thesis. Given a projective quadric surface Y defined over a number field K, we study the integral points of the punctured affine cone X over Y. If $K = \mathbb{Q}$, this is equivalent to studying coprime integer solutions to a degree two equation in four variables. More precisely, we describe, under certain hypotheses, a Brauer-Manin obstruction to Strong Approximation away from infinity on X. In some cases, this explains why some *local solutions* (for example, solutions modulo a prime p) do not lift to coprime integer solutions.

Notation and Conventions

We collect here some notational conventions and definitions that we will use throught the text. Most of them are standard, some are specified to avoid confusion.

Set Theory and Categorical Notation

The inclusion symbol "$\subset$" will always mean "contained in or equal to".

We denote the cardinality of a set X by $\#X$. We will generally avoid talking about the cardinality of infinite sets.

Set difference is denoted by "$\setminus$", that is if X is a set and $A, B \subset X$ are two subsets, we define $A \setminus B := \{x \in A \,|\, x \notin B\}$.

If I is a (possibly infinite) set and $\mathcal{X} = \{X_i \,|\, i \in I\}$ is a family of sets indexed by I, an element of the product $P = \prod_{i\in I} X_i$ will be denoted by $(x_i)_{i\in I}$, or by (x_i). Given a subset $U_i \subset X_i$ for every $i \in I$, we denote by

$$\widehat{\prod}_{i\in I}(X_i, U_i) = \left\{ (x_i) \in \prod_{i\in I} X_i \,|\, x_i \in U_i \text{ for all but finitely many } i \in I \right\}$$

the *restricted product* of the X_i with respect to the U_i. See [5], Section II.13.

Let $\mathbf{C}$ be a category. If A and B are two objects of $\mathbf{C}$, we denote by $\mathrm{Hom}(A, B)$ the set (or class) of morphisms from A to B. We will use the notation $\mathrm{End}(A)$ for $\mathrm{Hom}(A, A)$ and $\mathrm{Aut}(A)$ for the set (or class) of isomophisms from A to A. If the latter is a set, it will be considered a group via composition of morphisms. The identity map $A \to A$ will be denoted by id_A.

If $\mathbf{C}$ is the category of schemes, S is a scheme and A and B are S-schemes, $\mathrm{Hom}_S(A, B)$ will denote the set of morphisms of S-schemes from A to B, that is morphisms in the slice catgeory $\mathbf{C}/S$.

If $\mathbf{C}$ is the category of rings, R is a commutative ring and A and B are R-algebras (see below), $\mathrm{Hom}_R(A, B)$ will denote the set of morphisms of R-algebras from A to B, that is morphisms in the coslice category $R\backslash\mathbf{C}$.

Groups

If G is a group and H a subgroup we will denote by $[G : H]$ the index of H in G, that is the cardinality of the coset set G/H.

If G is a group and $n \in \mathbb{N}_{>0}$, we will denote by $G[n]$ the n-torsion part $\{g \in G \mid g^n = 1\}$ of G. If G is abelian, $G[n]$ is a subgroup. A group G will be called *torsion* if every element has finite order, that is if $G = \bigcup_{n\in\mathbb{N}_{>0}} G[n]$.

If S is a set, we will denote by $\langle S\rangle$ the free group on S. If $S = \{x_1, \ldots, x_n\}$ is finite, we let $\langle x_1, \ldots, x_n\rangle := \langle S\rangle$. For example, $\langle x\rangle$ will denote the infinite cyclic group generated by x.

Rings

By *ring* we will always mean a ring with unit, and we will assume that morphism of rings preserve the unit. We will not assume that rings are commutative.

If A is a ring and $B \subset A$ is any subset, we will denote by $C(B)$ its *centralizer*, that is $C(B) = \{c \in A \mid cb = bc \forall b \in B\}$. The centralizer $C(A)$ of A itself is called the *centre* of A and will be denoted by $Z(A)$.

If A is a commutative ring, an *A-algebra* is a (not necessarily commutative) ring B equipped with a map $\varphi : A \to B$ such that $\varphi(A) \subset Z(B)$.

The set of *units* (that is, invertible elements) of a ring A will be denoted by $A^\times$. It will be considered a group via the multiplication of A. Notice that in general $A^\times$ is smaller than $A \setminus \{0\}$.

A *division ring*, also called *skew field*, is a (not necessarily commutative) ring D such that every non-zero element has a multiplicative inverse, that is such that $D^\times = D \setminus \{0\}$. A *field* is a commutative division ring.

If A is any ring, we denote by A^{op} the ring that has the same additive structure and multiplication reversed. That is, if $A = (A, +, \cdot)$ then $A^{\mathrm{op}} = (A, +, *)$, where

$$\begin{aligned} * : A \times A &\to A \\ (a, b) &\mapsto a * b := b \cdot a. \end{aligned}$$

By *local ring* we mean a **commutative** ring that has a unique maximal ideal. If A is a commutative ring and P a prime ideal, we denote by R_P the localization of R at P. If A is a local ring with maximal ideal $\mathfrak{m}$, we denote by $\hat{A}_\mathfrak{m}$ the *completion* of A, i.e $\hat{A}_\mathfrak{m} = \varprojlim_i A/\mathfrak{m}^i$.

Linear Algebra

Let R be a ring. The set of $m \times n$ matrices will be denoted by $M_{m,n}(R)$. This set has a natural structure of R-module and if $m = n$ it is a ring with the usual matrix multiplication. We let $M_n(R) := M_{n,n}(R)$.

The transpose of a matrix M will be denoted by M^T. The determinant of a square matrix M will be denoted by $\det M$. The $n \times n$ identity matrix will be denoted by Id_n, or just Id if there is no risk of confusion.

Fields and Galois Theory

Let k be a field. If V is a k-vector space, $\dim_k V$ will denote its dimension (also called *rank*). If A is a k-algebra, we let $[A : k] = \dim_k A$ as a k-vector space.

A field extension L of k will be denoted by $L \mid k$. If $L \mid k$ is *Galois* (that is, normal and separable), we let $\mathrm{Gal}(L \mid k) := \mathrm{Aut}_k(L)$ denote the *Galois group of* $L \mid k$. If $L \mid k$ is infinite, this will be considered a topological group with its natural (Krull) topology (see [5], Chapter V). The extension $L \mid k$ is called *abelian* if its Galois group $\mathrm{Gal}(L \mid k)$ is abelian; it is called *cyclic* if $\mathrm{Gal}(L \mid k)$ is cyclic.

The *norm* and *trace* maps will be denoted by $N_{L \mid k} : L^\times \to k^\times$ and $\mathrm{Tr}_{L \mid k} : L \to k$ respectively.

We will denote a fixed *algebraic closure* of k by $\overline{k}$ and a fixed *separable closure* by k_{sep}. The extension $k_{\mathrm{sep}} \mid k$ is Galois and the Galois group $\mathrm{Gal}(k_{\mathrm{sep}} \mid k)$ is called the *absolute Galois group* of k.

Number Fields

We will usually denote number fields by uppercase Latin letters, often K or L.

Let K be a number field. The *ring of integers* of K will be denoted by $\mathcal{O}_K$, or just by $\mathcal{O}$ if there is no risk of confusion.

The set of all *normalized valuations* of K ([5], §7 and §11) will be denoted by Ω_K and the subset of *non-Archimedean* valuations by Ω_K^∞. Valuations will be usually denoted by the letter v, or similar, but we will use $|x|_v$ to denote the valuation of $x \in K$.

If $v \in \Omega_K^\infty$, we denote by K_v and $\mathcal{O}_{K,v}$ (or $\mathcal{O}_v$) the *completions* of K and its number ring with respect to v. Recall that $\mathcal{O}_v = \{x \in K_v \mid |x|_v \leq 1\}$. The maximal ideal of $\mathcal{O}_v$ will be denoted by $\mathfrak{m}_v$ and the residue field $\mathcal{O}_v/\mathfrak{m}_v$ by k_v, using the lowercase form of the letter naming the field. For a finite subset $S \subset \Omega_K^\infty$ we also let $\mathcal{O}_S := \{x \in K \mid |x|_v \leq 1 \, \forall \, v \in \Omega_K^\infty \setminus S\}$.

The *ring of adeles* of K (see section 1.3 below) will be denoted by $\mathbf{A}_K$ and the ring of *finite* adeles by $\mathbf{A}_K^\infty$.

This notation for completions might cause confusion, if a non-Archimedean valuation v is (legitimately) confused with the corresponding prime ideal $\mathfrak{p}$: above we have defined $\mathcal{O}_\mathfrak{p}$ to be the localization of $\mathcal{O}$ at $\mathfrak{p}$. We will try to always make clear which of the two we mean. For example, if $K = \mathbb{Q}$, $\mathcal{O} = \mathbb{Z}$ and p is a prime, we will denote by $\mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ at the prime ideal (p) and by $\mathbb{Z}_p$ the p-adic integers.

Chapter 1

Varieties and Points

We begin this exposition by collecting some geometric definitions and facts that we will use later. We will make use of the language of schemes, but we hope that the reader familiar only with varieties over non-algebraically closed fields will have little difficulty in understanding the concepts and results. For the basic definitions and facts, we refer to [18], or to the classic [13]. Much of the material of this chapter is taken from [25].

Recall that, if S is a scheme, an *S-scheme* is a pair (X, f), where X is a scheme and $f : X \to S$ is a morphism of schemes, called the *structural morphism* of X. A morphism of S-schemes is a morphism of schemes compatible with the structural morphisms. If R is a commutative ring, by R-scheme we mean a $(\operatorname{Spec} R)$-scheme. An S-scheme (X, f) is called *separated* (or *proper*, *of finite type*, *projective* and so on) if the structural morphism $f : X \to S$ is.

Let k be a field. A *variety over* k is a separated k-scheme of finite type. Notice that we **do not** assume varieties to be reduced or irreducible. If $L \mid k$ is a field extension and X is a k-scheme, we denote by X_L the L-scheme $X \times_k \operatorname{Spec} L$.

1.1 Scheme-valued Points

In this section, we introduce the "functorial point of view", as described for example in [8], I.4 and VI. This is also the point of view adopted in the lecture notes [1] which are, unfortunately, not publicly available.

As a motivating example, consider the equation in n indeterminates given by a polynomial $F(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$:

$$F(X_1, \ldots, X_n) = 0.$$

To find the solutions of such an equation, it is convenient to study the scheme $X = \operatorname{Spec} \mathbb{Q}[X_1, \ldots, X_n]/(F)$, or other related geometric objects. But, in the end, what we want to know are its *rational points*: n-uples $(a_1, \ldots, a_n) \in \mathbb{Q}^n$ such that $F(a_1, \ldots, a_n) = 0$.

These points correspond to maximal ideals $\mathfrak{m} \subset R := \mathbb{Q}[X_1, \ldots, X_n]/(F)$ such that $R/\mathfrak{m} = \mathbb{Q}$, the correspondence being given by

$$(a_1, \ldots, a_n) \longleftrightarrow (X_1 - a_1, \ldots, X_n - a_n).$$

Any of these in turn corresponds to a morphism of schemes $\operatorname{Spec}\mathbb{Q} \to X$, given by the quotient map $R \twoheadrightarrow R/\mathfrak{m} = \mathbb{Q}$.

Motivated by this example, we give the following general definition.

Definition 1.1. Let S be a scheme and X and S-scheme. If T is another S-scheme, a *T-point of X* is a morphism of S-schemes $T \to X$. The set of T-points of X will be denoted by $X(T) := \operatorname{Hom}_S(T, X)$. If $T = \operatorname{Spec} R$ is affine, a T-point of X will also be called an R-point and we set $X(R) := X(\operatorname{Spec} R)$.

If k is a field and X a variety over k, the k-points of X are also called *rational points* of X.

Notice that $X(T) = \operatorname{Hom}_S(T, X)$ is functorial in both T (contravariantly) and X (covariantly):

- For any map of S-schemes $\phi : T' \to T$, we have a map of sets $X(\phi) : X(T) \to X(T')$, given by composition $\psi \mapsto \psi \circ \phi$.
- For any map of S-schemes $f : X \to X'$, we have a map of sets $f(T) : X(T) \to X'(T)$ given by composition $g \mapsto f \circ g$.

Remark 1.2. In Definition 1.1, the base scheme S does not appear in the notation "$X(T)$". It will usually be clear from the context which base scheme we are working over.

Example 1.3. Let k be a field, $L \mid k$ a field extension and X a variety over k. Then the L-points of X_L are the same as the L-points of X, that is $X_L(L) = X(L)$. In fact, any map of k-schemes $\operatorname{Spec} L \to X$ factors through the pullback $X_L = X \times_k \operatorname{Spec} L$. This is just a rephrasing of the universal property of the fibered product in this specific case.

Remark 1.4. Let $L \mid k$ be an algebraic field extension and let X be a k-scheme. The image of any map of k-schemes $\operatorname{Spec} L \to X$ is a point of X, whose residue field is a subfield of L, so we have a well-defined map

$$\psi : X(L) \longrightarrow X.$$

However, this map is, in general, not surjective nor injective. Clearly it can't be surjective if $\dim X > 0$, because points of positive dimension have residue fields of positive transcendence degree over k. If there exists a non-trivial k-automorphism σ of L, then ψ is not injective: in fact, for any fixed morphism of k-schemes $f : \operatorname{Spec} L \to X$, the composition $f \circ \operatorname{Spec}\sigma : L \to X$ has the same set-theoretic image as f, although it defines a different map of schemes.

In practice, if $X = \operatorname{Spec} k[X_1, \ldots, X_n]/I$ is an affine variety over a field k and $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n) \supset I$ is a maximal ideal, we will denote by $(a_1, \ldots, a_n)$ the k-point of X given by $k[X_1, \ldots, X_n]/I \twoheadrightarrow k[X_1, \ldots, X_n]/\mathfrak{m}$. Similarly, if $X = \operatorname{Proj} k[X_0, \ldots, X_n]/I$ is a projective variety and $\mathfrak{m} = (a_i X_j - a_j X_i)_{0 \le i,j \le n}$, we will denote by $(a_0 : \cdots : a_n)$ the k-point of X given by $k[X_0, \ldots, X_n]/I \twoheadrightarrow k[X_0, \ldots, X_n]/\mathfrak{m}$ (see [18], Lemma 2.3.43).

1.1.1 Rational Points over Topological Fields

Let k be a topological field and let X be a variety over k. In our applications, k will be a completion of a number field with its analytic (Euclidean or p-adic) topology. We want to give a new topology to the set $X(k)$ of rational points of X, that we will call the *analytic topology*.

If $X \subset \mathbb{A}^n$ is affine, we have $X(k) \subset \mathbb{A}^n(k) = k^n$ and we give $X(k)$ the subspace topology of the product topology.

If X is not affine, we can cover it with affine open subschemes $\{X_i\}_{i\in I}$, with glueing data $\{(X_{ij}, \varphi_{ij} : X_{ij} \xrightarrow{\sim} X_{ji})\}_{i,j\in I}$. By functoriality of $X_i(k)$, this provides topological spaces $\{X_i(k)\}_{i\in I}$ with glueing data $\{(X_{ij}(k), \varphi_{ij}(k) : X_{ij}(k) \xrightarrow{\sim} X_{ji}(k))\}_{i,j\in I}$. We need to check that the maps of varieties φ_{ij} give rise to continuous maps $\varphi_{ij}(k)$, but this is true because rational maps are continuous with respect to the topology of k. So we can glue the $X_{ij}(k)$ to get a topological space, which coincides set-theoretically with $X(k)$. One can also show that this topology does not depend on the choice of the affine covering $\{X_i\}_{i\in I}$.

Remark 1.5. If $k = \mathbb{C}$ with its Euclidean topology, we can go further and equip $X(\mathbb{C})$ with the stucture of a complex analytic space X^{an}, which will be a complex manifold if X is smooth. Moreover, restricting to the case of projective varieties, we have an equivalence between the category of coherent sheaves on X and that of coherent sheaves of X^{an}, which respects cohomology. This correspondence, due to Serre [28], has been proven very fruitful in the study of algebraic varieties over the complex numbers.

1.2 Models

For the whole section, we let R be an integral domain and K its fraction field.

If X is a K-scheme, or a variety over K, and $\mathfrak{m}$ is a maximal ideal of R with residue field $k = R/\mathfrak{m}$, we would like to be able to talk about the k-scheme defined by the reductions modulo $\mathfrak{m}$ of the equations defining X. To do this, we will need to "spread out" X to an R-scheme. In other words, we need an R-scheme $\mathcal{X}$ such that its *generic fiber* $\mathcal{X} \times_R K$ coincides with X.

Definition 1.6. Let X be a K-scheme. An *R-model* for X is a pair $(\mathcal{X}, \varphi)$ where $\mathcal{X}$ is a flat R-scheme of finite presentation with surjective structural morphism $\mathcal{X} \to \operatorname{Spec} R$ and $\varphi : \mathcal{X} \times_R K \to X$ is an isomorphism.

In practice, we will omit the isomorphism φ from the notation and simply say that "$\mathcal{X}$ is an R-model for X".

In the situation above, an R-model for X might not exist in general. However, if X is of finite presentation, there is always a localization $R[f^{-1}]$ of R such that an $R[f^{-1}]$-model for X exists. See [25], Theorem 3.2.1.

In some specific cases it is actually easy to find models.

Example 1.7. Assume that R is a Dedekind domain and let $X \subset \mathbb{P}^n_K$ be a projective variety over K. Assume that X is reduced and irreducible. Consider the natural inclusion $\mathbb{P}^n_K \hookrightarrow \mathbb{P}^n_R$ and let $\mathcal{X}$ be the closure of X in $\mathbb{P}^n_R$, equipped with its

reduced scheme structure. Then $\mathcal{X}$ is reduced and irreducible, and its generic fiber coincides with X. Moreover, the structural morphism $\mathcal{X} \to \operatorname{Spec} R$ is surjective and flat by [18], Proposition 4.3.9, so that $\mathcal{X}$ is an R-model for X.

For example, if X is an hypersurface defined by a single equation

$$F(X_0, \dots, X_n) = 0 \tag{1.1}$$

for some homogeneous $F \in R[X_0, \dots, X_n]$ such that **the coefficients of F generate the trivial ideal**, we have that the projective R-scheme $\mathcal{X} \subset \mathbb{P}^3_R$ defined by (1.1) is an R-model for X.

Remark 1.8. If X is a K-scheme of finite presentation and $\mathcal{X}_1$, $\mathcal{X}_2$ are two R-models for X, there is a dense open subscheme $U \subset \operatorname{Spec} R$ such that $\mathcal{X}_1 \times_R U \cong \mathcal{X}_2 \times_R U$. In particular, if R is a Dedekind domain, we have $\mathcal{X}_1 \times_R R/\mathfrak{p} \cong \mathcal{X}_2 \times_R R/\mathfrak{p}$ and $\mathcal{X}_1 \times_R \hat{R}_\mathfrak{p} \cong \mathcal{X}_2 \times_R \hat{R}_\mathfrak{p}$ for all but finitely many primes $\mathfrak{p}$ of R.

Let X be a K-scheme and $\mathcal{X}$ an R-model for X. If $\mathfrak{m}$ is a maximal ideal of R and $k = A/\mathfrak{m}$, we call the k-scheme $\tilde{X} = \mathcal{X} \times_R k$ the *reduction* of X modulo $\mathfrak{m}$. In general, this depends on the choice of the R-model $\mathcal{X}$. If X is affine and $P = (P_1, \dots, P_n)$ and $Q = (Q_1, \dots, Q_n)$ are two $\hat{R}_\mathfrak{m}$-points of X, we say that P *is congruent* to Q modulo $\mathfrak{m}$ (in symbols, $P \equiv Q \pmod{\mathfrak{m}}$) if they define the same k-point of $\tilde{X}$, that is if $P_i - Q_i \in \mathfrak{m}$ for $i = 1, \dots, n$. Similarly, if X is projective and $P = (P_0 : \cdots : P_n)$ and $Q = (Q_0 : \cdots : Q_n)$ are two $\hat{R}_\mathfrak{m}$-points of $\tilde{X}$, we say that P is congruent to Q modulo $\mathfrak{m}$ if $P_i - Q_i \in \mathfrak{m}$ for $i = 0, \dots, n$.

Example 1.9. Continuing on Example 1.7 above, let $\mathfrak{p}$ be a maximal ideal of R. Then the reduction $\tilde{X}$ of X modulo $\mathfrak{p}$ is a variety over $k = R/\mathfrak{p}$ of the same dimension of X, but it is not necessarily irreducible or reduced, even though X is (see [18], Theorem 4.3.12).

1.3 Adelic Points

Let K be a number field and let Ω_K denote the set of normalized valuations of K. For $v \in \Omega_K$ we denote by K_v the completion of K with respect to v and, if v is non-Archimedean, by $\mathcal{O}_v$ the ring of integers of K_v.

Recall that the **ring of adeles** of K is the restricted topological product of the K_v's with respect to the $\mathcal{O}_v$'s

$$\mathbf{A}_K := \widehat{\prod}_{v \in \Omega_K} (K_v, \mathcal{O}_v) = \{(\alpha_v)_{v \in \Omega_K} \mid \alpha_v \in \mathcal{O}_v \text{ for all but finitely many } v\}$$

where for v Archimedean we let $\mathcal{O}_v = K_v$. The topology on $\mathbf{A}_K$ is defined by the basis of open sets

$$\mathcal{B} = \left\{ \prod_{v \in \Omega_K} U_v \;\middle|\; U_v \subset K_v \text{ open}, \, U_v = \mathcal{O}_v \text{ for all but finitely many } v \right\}.$$

This makes $\mathbf{A}_K$ a topological ring, with component-wise operations. See [5], II.13 for details.

Let X be a variety over K. As a set, we have already defined $X(\mathbf{A}_K)$ in Section 1.1: in fact, $\mathbf{A}_K$ is a K-algebra via the diagonal embedding of K in $\mathbf{A}_K$. But we would also like to give $X(\mathbf{A}_K)$ a suitable topology. There are several approaches for this, all of them giving the same result; see for example [6] or [19]. Here we follow [25], Section 2.6.3.

Let $\mathcal{X}$ be an $\mathcal{O}_S$-model for X, for some finite subset $S \subset \Omega_K^\infty$. In section 1.1.1 we have endowed $\mathcal{X}(K_v) = X(K_v)$ with a topology. For every $v \in \Omega_K^\infty \setminus S$, we give then $\mathcal{X}(\mathcal{O}_v) \subset \mathcal{X}(K_v)$ the subspace topology and for $v \in S$ we let $\mathcal{X}(\mathcal{O}_v) = X(K_v)$. Then it can be seen that $X(\mathbf{A}_K)$ coincides, as a set, with the restricted product

$$\widehat{\prod}_{v\in\Omega_K} (X(K_v), \mathcal{X}(\mathcal{O}_v))$$

which has a topology, with basis

$$\left\{ \prod_{v\in\Omega_K} U_v \;\middle|\; U_v \subset X(K_v) \text{ open, } U_v = \mathcal{X}(\mathcal{O}_v) \text{ for all but finitely many } v \right\}.$$

We give $X(\mathbf{A}_K)$ this topology.

This construction depends a priori on the choice of the model $\mathcal{X}$. But actually, since any two models differ only at finitely many places of K (see Section 1.2 above), we see that any choice of a model gives rise to the same topology (see [5], II.13, Lemma at the beginning of page 63).

Example 1.10. If X is projective, then any K_v-point of X can be scaled to give an $\mathcal{O}_v$-point of $\mathcal{X}$. This means that $\mathcal{X}(\mathcal{O}_v) = X(K_v)$ for all non-Archimedean v (this also follows from the valuative criterion for properness, see [13] Theorem II.4.7 or [25] Theorem 3.2.12). In particular, $X(\mathbf{A}_K) = \prod_v X(K_v)$ as topological spaces, where the product on the right has the product topology.

1.4 Quadric Surfaces

In this section we wish to collect some definitions and facts about our main geometric object of study, that is projective quadric surfaces over a field.

Let k be any field and $\mathbb{P}^3_k = \operatorname{Proj} k[X_0, X_1, X_2, X_3]$ be the three-dimensional projective space over k. By *quadric surface* over k we mean a projective k-scheme $Y \subset \mathbb{P}^3_k$ given by a single equation

$$F(X_0, X_1, X_2, X_3) = 0 \tag{1.2}$$

for some non-zero polynomial $F \in k[X_0, X_1, X_2, X_3]$, homogeneous of degree 2.

Assume now that $\operatorname{char} k \neq 2$. Then the equation (1.2) can be given in the form

$$\mathbf{x}^T M_Y \mathbf{x} = 0 \tag{1.3}$$

where $\mathbf{x} = (X_0, X_1, X_2, X_3)$ and $M_Y \in M_4(k)$ is a symmetric 4×4 matrix with entries in k, called the matrix associated to Y.

The surface Y is smooth if and only if $\det M_Y \neq 0$, and in this case it is called *non-degenerate*; otherwise it is called *degenerate*.

The determinant $\det M_Y$ of M_Y will be denoted by Δ_Y and called the *discriminant* of Y. Its class in $k^\times/(k^\times)^2$ is easily seen to be invariant under linear changes of coordinates.

Proposition 1.11. *Let k be a field with $\operatorname{char} k \neq 2$ and Y a smooth quadric surface in $\mathbb{P}^3_k$. Assume that $Y(k) \neq \emptyset$. Then Y is rational (that is, birational to $\mathbb{P}^2_k$).*

Proof. Let $P \in Y(k)$ and let $H \subset \mathbb{P}^2_k$ be a hyperplane not containing P. For any $Q \in Y$ different from P, consider the line through P and Q and its intersection $\phi(Q)$ with H. It can be checked that this defines a birational map $Y \dashrightarrow H$.

For a different proof, see [8], Section IV.2.5. □

Note that over a fixed algebraic closure $\overline{k}$ of k, all smooth quadric surfaces are isomorphic. By [13], Exercise I.2.15, such a quadric surface is isomorphic to $\mathbb{P}^1_{\overline{k}} \times \mathbb{P}^1_{\overline{k}}$, and it contains two families of lines.

Proposition 1.12. *Let Y be a smooth quadric surface over a field k with $\operatorname{char} k \neq 2$. Then the two families of lines on $Y \times_k \overline{k}$ are defined over $k(\sqrt{\Delta_Y})$ and are conjugate to each other.*

Proof. See [3], Lemma 2.1 or [8], Section IV.3.2. □

We will need a simple fact about the number of points of quadric surfaces over finite fields.

Proposition 1.13. *Let k be a finite field with q elements, with q odd. Let Y be a smooth quadric surface in $\mathbb{P}^3_k$. Then Y has at least 3 rational points.*

Proof. For an elementary proof, see [15], Theorems 6.26 and 6.27. □

Remark 1.14. We can actually be more precise and say that

$$\#Y(k) = \begin{cases} (q+1)^2 & \text{if } \Delta_Y \in (k^\times)^2, \\ q^2+1 & \text{otherwise.} \end{cases}$$

See [3], Lemma 2.2 for a proof. Notice that the case $\Delta_Y \in (k^\times)^2$ follows trivially from the fact that $Y \cong \mathbb{P}^1_k \times \mathbb{P}^1_k$.

Chapter 2

The Hasse Principle

When studying the rational points of a variety X over $\mathbb{Q}$, it is often convenient to study the behaviour of X at different places of $\mathbb{Q}$, that is to study the set $X(\mathbb{Q}_p)$ of $\mathbb{Q}_p$-points of X, for different primes p. For example, sometimes it is easy to conclude that $X(\mathbb{Q})$ is empty: since $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)$, if $X(\mathbb{Q}_p)$ is empty for some place p, then $X(\mathbb{Q})$ is clearly empty as well!

Example 2.1. Consider the projective conic $X \subset \mathbb{P}^2_{\mathbb{Q}}$ given by the equation $X^2 + Y^2 = 3Z^2$. Assume that $(x : y : z) \in X(\mathbb{Q}_3)$ is a $\mathbb{Q}_3$-point of X. We can assume that x, y and z are in $\mathbb{Z}_3$, and at least one of them is a unit. Working modulo 3, we see that $3 \mid x^2 + y^2$, which implies that $3 \mid x$ and $3 \mid y$, since the only quadratic residues modulo 3 are 0 and 1. But then $x = 3a$ and $y = 3b$ for some $a, b \in \mathbb{Z}_3$, so we have $9a^2 + 9b^2 = 3z^2 \implies 3a^2 + 3b^2 = z^2$. This implies that $3 \mid z$, contradicting the assumption that at least one of x, y and z was a unit in $\mathbb{Z}_3$. So we have $X(\mathbb{Q}_3) = \emptyset$, thus in particular $X(\mathbb{Q}) = \emptyset$.

Of course, we can consider $p = \infty$ as well.

Example 2.2. The conic $X \subset \mathbb{P}^2_{\mathbb{Q}}$ defined by $X^2 + Y^2 + Z^2 = 0$ has no rational point, because $X(\mathbb{R}) = \emptyset$.

It is natural to ask if the converse holds: does the existence of points over every completion imply the existence of a rational point? More precisely, for varieties X over a number field K, does the implication

$$X(K_v) \neq \emptyset \text{ for every place } v \text{ of } K \qquad \implies \qquad X(K) \neq \emptyset \tag{2.1}$$

hold?

Unfortunately, this is not always the case.

Example 2.3 ([10], Problem 121)**.** The equation

$$(X^2 - 2)(X^2 - 17)(X^2 - 34) = 0 \tag{2.2}$$

has a solution in $\mathbb{Q}_p$ for all $p \leq \infty$, but no solutions in $\mathbb{Q}$. To see this, notice first that it has six real solutions, and none of them is in $\mathbb{Q}$. So it remains to show that it has a solution in $\mathbb{Q}_p$ for every prime $p < \infty$. By Proposition 3.11 below, we see that 2 is a square in $\mathbb{Q}_{17}$ (because $6^2 \equiv 2 \pmod{17}$) and that 17 is a square in $\mathbb{Q}_2$, so (2.2) has solutions in $\mathbb{Q}_p$ for $p = 2, 17$. Finally, if $p \neq 2, 17, \infty$ and none of 2 and 17 is a square in $\mathbb{Q}_p$, then $34 = 2 \cdot 17$ must be a square in $\mathbb{Q}_p$, again by Proposition 3.11. So in any case (2.2) has a solution in $\mathbb{Q}_p$.

There are more classical counterexamples, such as the projective genus one curve defined over $\mathbb{Q}$ by the equation

$$2Y^2 = X^4 - 17Z^4$$

discovered independently by Lind [17] and Reichardt [26].

However, there are classes of varieties for which the implication in (2.1) does hold. An example is given by quadric hypersurfaces.

Theorem 2.4 (Hasse-Minkowski)**.** *Let K be a number field and $X \subset \mathbb{P}^n_K$ be a hypersurface defined by a single homogeneous equation of degree 2. Then $X(K) \neq \emptyset$ if and only if $X(K_v) \neq \emptyset$ for every place v of K.*

Proof. See [27], Theorem IV.8. □

For a family of varieties $\mathcal{F}$, we say that *varieties of $\mathcal{F}$ satisfy the* ***local-global principle*** (also called *Hasse principle*) if the implication 2.1 holds for every $X \in \mathcal{F}$. The Theorem above can be rephrased as: *"Projective quadrics satisfy the local-global principle."*

Even if this strong condition doesn't hold, one can still hope that the study of points over the completions can give us information about the rational points. This motivates us to study the solubility of equations over the completions of a number field.

2.1 Hensel's Lemma

Let K be a number field and v a non-Archimedean place of K. We denote the completion of K at v by K_v and the ring of integers of K_v by $\mathcal{O}_v$. Let also $\mathfrak{m}_v$ be the maximal ideal of $\mathcal{O}_v$ and $k_v = \mathcal{O}_v/\mathfrak{m}_v$ the residue field.

In practice, it is often possible to reduce questions about K_v to questions about the residue field k_v. The main tool for this is Hensel's Lemma.

Theorem 2.5 (Hensel's Lemma)**.** *Let $f(X) \in \mathcal{O}_v[X]$ be a polynomial and suppose that there is $x_0 \in \mathcal{O}_v$ such that*

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

Then there is a unique $x \in \mathcal{O}_v$ satisfying

$$f(x) = 0 \qquad \textit{and} \qquad |x - x_0|_v < \frac{|f'(x_0)|_v}{|f(x_0)|_v}.$$

Proof. For a proof in the case $K = \mathbb{Q}$, see [10], Section 3.4. For a proof that works in a more general setting, see [7], Theorem 7.3. □

Remark 2.6. The classical proof of Hensel's Lemma is constructive: the existence of the root x is proven by giving a method to compute a Cauchy sequence converging to it. This construction is the p-adic equivalent of Newton's Method for approximating roots of real-valued functions.

Working with varieties rather than with single equations, we would like to have a higher-dimensional analogue of the result above. In practice, we will often use the following.

Corollary 2.7. *Let $F(X_1,\dots,X_n)\in\mathcal{O}_v[X_1,\dots,X_n]$ be a polynomial and suppose that there is $\mathbf{x}_0\in\mathcal{O}_v^n$ such that*

$$|F(\mathbf{x}_0)|_v<\left|\frac{\partial F}{\partial X_j}(\mathbf{x}_0)\right|_v^2$$

for some j. Then there is $\mathbf{x}\in\mathcal{O}_v^n$ such that $F(\mathbf{x})=0$.

Proof. Write $\mathbf{x}_0=(a_1,\dots,a_n)$ and assume without loss of generality that $j=1$. Apply Hensel's Lemma to $f(X)=F(X,a_2,\dots,a_n)\in\mathcal{O}_v[X]$. □

Remark 2.8. We can easily deduce the following from Corollary 2.7. Let $X\subset\mathbb{P}^n_{K_v}$ be a smooth projective variety over K_v and let $\tilde{X}$ be a reduction of X modulo v (see Section 1.2). Assume that X is a hypersurface given by the zero locus of some homogeneous polynomial $F\in\mathcal{O}_v[X_0,\dots,X_n]$. If $\tilde{x}=(\tilde{x}_0:\cdots:\tilde{x}_n)\in\tilde{X}(k_v)$ is a smooth point of the reduction, then there is $x\in X(K_v)$ that reduces to $\tilde{x}$, that is, such that $x\equiv\tilde{x}\pmod{v}$.

The same result also holds when dealing with systems of polynomial equations.

Proposition 2.9. *Let $F_1,\dots,F_r\in\mathcal{O}_v[X_1,\dots,X_n]$ be polynomials, with $r\leq n$ and let*

$$\mathbf{J}=\left(\frac{\partial F_i}{\partial X_j}\right)_{i,j}$$

be their Jacobian matrix. Let $\mathbf{x}_0\in\mathcal{O}_v^n$ be such that there is an $r\times r$ submatrix M of $\mathbf{J}(\mathbf{x}_0)$ such that

$$\max_i\{|F_i(\mathbf{x}_0)|_v\}<|\det M|_v^2.$$

Then there is $\mathbf{x}\in\mathcal{O}_v^n$ such that

$$F_i(\mathbf{x})=0\text{ for all }i\qquad\text{and}\qquad\max_i|\mathbf{x}_i-(\mathbf{x}_0)_i|_v<|\det M|_v.$$

Proof. See [11], 5.21. □

2.2 Local Solubility

Let again K be a number field and v a non-Archimedean place of K, and let $\mathcal{O}_v$, $\mathfrak{m}_v$ and k_v be as before. Let X be a projective hypersurface in $\mathbb{P}^n_{K_v}$, defined by a single homogeneous polynomial equation with coefficients in $\mathcal{O}_v$

$$F(X_0,\dots,X_n)=0\qquad\text{with }F\in\mathcal{O}_v[X_0,\dots,X_n]\text{ homogeneous.}\tag{2.3}$$

We may assume that at least one of the coefficients of F is in $\mathcal{O}_v^\times$, so that (2.3) also defines an $\mathcal{O}_v$-scheme $\mathcal{X}$.

We can now present an algorithm to determine whether X has any K_v-point. This algorithm can actually be generalized to any smooth projective variety, using Proposition 2.9 instead of Corollary 2.7. A generalization is contained in [4], which is yet unpublished.

First of all, recall that any K_v-point of X can be written as $(a_0 : \cdots : a_n)$ for some $a_0, \ldots, a_n \in \mathcal{O}_v$, at least one of which is in $\mathcal{O}_v^\times$. This implies that $X(K_v) = \mathcal{X}(\mathcal{O}_v)$; in particular, we only need to check for the existence of points of this form. Up to repeating the procedure for every standard affine patch (so $n+1$ times in total), we can assume that X is affine in $\mathbb{A}^n_{K_v}$, given by a single equation

$$f(X_1, \ldots, X_n) = 0 \qquad \text{with } f \in \mathcal{O}_v[X_1, \ldots, X_n], \tag{2.4}$$

and only look for points with integer coordinates in this affine patch. Again we assume that at least one of the coefficients of f is a unit. Let now $\mathcal{X}$ be the model of X over $\mathcal{O}_v$ defined by (2.4).

The procedure goes as follows.

Let $i = 1$ and consider the finitely many (more precisely, $(\#k_v)^{ni}$) points of $(\mathcal{O}_v/\mathfrak{m}_v^i)^n = \mathbb{A}^n_{\mathcal{O}_v}(\mathcal{O}_v/\mathfrak{m}_v^i)$. For each $\mathbf{x}_0 = (x_1, \ldots, x_n) \in (\mathcal{O}_v/\mathfrak{m}_v^i)^n$, it is possible to check if $f(\mathbf{x}_0) \equiv 0 \pmod{\mathfrak{m}_v^i}$.

Now there are two cases in which we can give a definitive answer.

(a) If none of the points of $(\mathcal{O}_v/\mathfrak{m}_v^i)^n$ satisfies our equation then $\mathcal{X}(\mathcal{O}_v/\mathfrak{m}_v^i) = \emptyset$, so also $\mathcal{X}(\mathcal{O}_v) = \emptyset$, and the procedure stops.

(b) For every $\mathbf{x}_0$ such that $f(\mathbf{x}_0) \equiv 0 \pmod{\mathfrak{m}_v^i}$, we can check if it satisfies the condition of Corollary 2.7. If it does, then we can lift it to a point of $\mathcal{X}(\mathcal{O}_v)$.

If we are in neither of the situations above, that is if we do find $(\mathcal{O}_v/\mathfrak{m}_v^i)$-points of $\mathcal{X}$, but we can't say if any one of them lifts to an $\mathcal{O}_v$-point, we can refine the search by looking at a smaller v-adic neighbourhood of the point. In other words, we increase i by one and repeat the procedure.

To see that the procedure stops after finitely many steps, assume by contradiction that for every $m \in \mathbb{N}$ there is $\mathbf{x}_m \in (\mathcal{O}_v/\mathfrak{m}_v^m)^n$ such that $f(\mathbf{x}_m) \equiv 0 \pmod{\mathfrak{m}_v^m}$, but $|f(\mathbf{x}_m)|_v \geq |\partial f/\partial X_j(\mathbf{x}_m)|_v^2$ for every j. We can assume that $\mathbf{x}_m \equiv \mathbf{x}_i \pmod{\mathfrak{m}_v^i}$ for every $i \leq m$. Lifting each $\mathbf{x}_m$ to a point of $\mathcal{O}_v^n$, we get a Cauchy sequence in $\mathcal{O}_v^n$, which then converges to some $\mathbf{x} \in \mathcal{O}_v^n$, which by continuity (polynomial functions are continuous maps on topological rings) satisfies:

$$f(\mathbf{x}) = \lim_{m\to+\infty} f(\mathbf{x}_m) = 0 \quad \text{and} \quad \partial f/\partial X_j(\mathbf{x}) = \lim_{m\to+\infty} \partial f/\partial X_j(\mathbf{x}_m) = 0 \text{ for every } j.$$

But this is a singular point of X, and we assumed that X is smooth. We conclude that the procedure terminates after finitely many steps.

2.2.1 Archimedean Places

For our purpose, that is determining the existence of K_v-points for every place v of K, we also need to address the Archimedean places.

If $K_v \cong \mathbb{C}$, then the existence of K_v-points is a trivial question for hypersurfaces defined by one polynomial. For varieties defined by more equations, we just need to use the Nullstellensatz and see if the polynomials generate the trivial ideal. This can be done for example using Gröbner Bases, see [7], Chapter 15.

If $K_v \cong \mathbb{R}$, there are as well algorithms to determine whether X has K_v-points, but we will not treat them in this thesis. See for example [2], Theorem 13.13.

2.2.2 Everywhere Local Solubility

We have seen that there is a finite procedure to determine the existence of K_v-points of a projective hypersurface, for a fixed place v of K. However, we would like to ask the same question for all of the infinitely many places of K.

Let $X \subset \mathbb{P}^n_K$ be a smooth projective variety over K of dimension d. Our goal is to show that there is a finite and computable set $T \subset \Omega^\infty_K$ such that, for every $v \in \Omega^\infty_K \setminus T$, the reduction of X modulo v has smooth points, that will then lift to K_v-points by Proposition 2.9. This can be done, provided that we know the Betti numbers $b_i(X(\mathbb{C})) = \dim_{\mathbb{C}} H^i(X(\mathbb{C}), \mathbb{C})$ of $X(\mathbb{C})$. The existence of K_v-points for $v \in T$ can be checked with the methods described above, so that in the end we will get a finite procedure to check for the existence of K_v-points for every v, that is, everywhere local solubility.

For simplicity, we will assume that X is a smooth hypersurface given by a single equation

$$f(X_0, \dots, X_n) = 0 \tag{2.5}$$

for some $f \in \mathcal{O}[X_0, \dots, X_n]$, but everything can be generalized easily to the case of varieties defined by a system of polynomial equations.

Let $\mathcal{X}$ be the $\mathcal{O}$-scheme defined by (2.5). Let S be the set of finite primes of K dividing the ideal generated by the coefficients of f, which is finite and computable. Then $\mathcal{X}$ is an $\mathcal{O}_S$-model for X.

Since X is smooth, f together with its partial derivatives generate the trivial ideal in $K[X_0, \dots, X_n]$, so there are polynomials $a, a_0, \dots, a_n \in K[X_0, \dots, X_n]$ such that

$$af + \sum_{i=0}^{n} a_i \frac{\partial f}{\partial X_i} = 1 \qquad \text{in } K[X_0, \dots, X_n] \tag{2.6}$$

and by clearing the denominators we get

$$bf + \sum_{i=0}^{n} b_i \frac{\partial f}{\partial X_i} = N \qquad \text{in } \mathcal{O}[X_0, \dots, X_n] \tag{2.7}$$

for some $N \in \mathcal{O}$ and some $b, b_0, \ldots, b_n \in \mathcal{O}[X_0, \ldots, X_n]$. By considering the reduction of (2.7), we see that $\mathcal{X} \times_{\mathcal{O}_S} k_v$ is smooth for every v not in S and not dividing N.

Let now V be a smooth, projective and geometrically irreducible variety over the finite field with q elements $\mathbb{F}_q$. From the Lefschetz trace formula, one can deduce that

$$\left|\#V(\mathbb{F}_q) - (q^d + 1)\right| \leq \sum_{i=1}^{2d-1} q^{i/2} \dim_{\mathbb{Q}_l} H^i(V_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)$$

where l is a prime not dividing q and $H^i(V_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)$ is the i-th *étale cohomology* group with $\mathbb{Q}_l$ coefficients. See [22], Section VI.12.

If V is the reduction of a variety over a number field, for example in our case $V = \mathcal{X} \times_{\mathcal{O}_S} k_v$ for some $v \in \Omega_K^\infty$, we have that $\dim_{\mathbb{Q}_l} H^i(V_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)$ coincides with the i-th Betti number $b_i(X(\mathbb{C}))$ of X. Thus, knowing the Betti numbers of $X(\mathbb{C})$ enables us to compute a bound M such that for every $v \in \Omega_K^\infty$ with $\#k_v > M$ the reduction of X modulo v has points.

Putting everything together, we see that we can indeed compute a finite set T of places of K such that for every $v \notin T$ we have $X(K_v) \neq \emptyset$. As explained above, we have then a finite procedure to check for everywhere local solubility.

2.3 Approximation Theorems

We recall the following result on the independence of inequivalent valuations.

Theorem 2.10 (Weak Approximation)**.** *Let k be any field and let $v_1, \ldots, v_n$ be non-equivalent, non-trivial valuations on k. For $i = 1, \ldots, n$, let k_i be the topological space consisting of k with the topology induced by v_i. Then the image of the diagonal embedding of k in $\prod_{i=1}^n k_i$ is dense in the product topology.*

Proof. See [5], II.6. □

In other words, given $\alpha_1, \ldots, \alpha_n \in k$ and $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{R}_{>0}$ there is always $x \in k$ such that $|x - \alpha_i|_{v_i} < \varepsilon_i$ for all $i = 1, \ldots, n$.

Let now K be a number field and let

$$\mathbf{A}_K = \widehat{\prod}_{v \in \Omega_K} (K_v, \mathcal{O}_v) = \{(\alpha_v)_{v \in \Omega_K} \mid \alpha_v \in \mathcal{O}_v \text{ for almost all } v\}$$

be the ring of adeles of K (See Section 1.3). Since any $\alpha \in K$ is in $\mathcal{O}_v$ for all but finitely many v, we have a natural inclusion of K into $\mathbf{A}_K$, and the image of K under this map is discrete in $\mathbf{A}_K$ (see [5], Section II.14).

However, as soon as we remove one component from the restricted product, the image of K becomes dense in this smaller ring.

Theorem 2.11 (Strong Approximation)**.** *Let $v_0 \in \Omega_K$ be any valuation. Then the image of the natural embedding*

$$K \hookrightarrow \mathbf{A}_K^{v_0} := \widehat{\prod}_{v \in \Omega_K \setminus \{v_0\}} (K_v, \mathcal{O}_v).$$

is dense in the restricted product topology.

Proof. See [5], II.15. □

We can rephrase this result as follows: given distinct valuations $\{v_1, \dots, v_n\} \in \Omega_K \setminus \{v_0\}$, elements $\alpha_1, \dots, \alpha_n \in K_{v_n}$ and $\varepsilon_1, \dots, \varepsilon_n \in \mathbb{R}_{>0}$, there is $x \in K$ such that $|x - \alpha_i|_{v_i} < \varepsilon_i$ for $i = 1, \dots, n$ and $|x|_v \leq 1$ for $v \notin \{v_0, v_1, \dots, v_n\}$.

As a corollary, and as an example of "Strong Approximation away from infinity", we can prove the following version of the well known Chinese Remainder Theorem.

Corollary 2.12. *Let $p_1, \dots, p_n \in \mathbb{Z}$ be distinct prime numbers, $e_1, \dots, e_n \in \mathbb{N}_{>0}$ and $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$. Then the system of congruences*

$$\begin{cases} x \equiv \alpha_1 \pmod{p_1^{e_1}} \\ x \equiv \alpha_2 \pmod{p_2^{e_2}} \\ \dots \\ x \equiv \alpha_n \pmod{p_n^{e_n}} \end{cases}$$

has a solution $x \in \mathbb{Z}$.

Proof. Apply the (rephrasing of) the theorem above with $K = \mathbb{Q}$, $v_0 = \infty$, $v_i = p_i$ and $\varepsilon_i = p_i^{-e_i}$ for $i = 1, \dots, n$. □

2.3.1 Approximation Theorems for Varieties

Let X be a variety over K. Following Chapter 1, the sets $X(K_v)$ (for any $v \in \Omega_K$) and $X(\mathbf{A}_K)$ of K_v-points and adelic points are topological spaces. We can therefore ask ourselves if X **satisfies Weak or Strong Approximation**, that is if the images of the diagonal maps

$$X(K) \hookrightarrow \prod_{v \in \Omega_K} X(K_v) \qquad \text{(Weak Approximation)}$$

and

$$X(K) \hookrightarrow X(\mathbf{A}_K) \qquad \text{(Strong Approximation)}$$

are dense.

Remark 2.13. If X is projective, the two conditions above are equivalent, since $X(\mathbf{A}_K) = \prod_v X(K_v)$ (Example 1.10).

Strong Approximation is usually too strong a condition. For example, if X is affine, we have that $X(K)$ is discrete in $X(\mathbf{A}_K)$, because K is discrete in $\mathbf{A}_K$ (see

[5], II.14 or [25], Section 2.6.4). This is why we are usually interested in a weaker condition, that we now define.

Let $S \subset \Omega_K$ be a finite subset and define

$$\mathbf{A}_K^S := \widehat{\prod}_{v \in \Omega_K \setminus S} (K_v, \mathcal{O}_v).$$

If S is the set of all Archimedean places of K, we will also write $\mathbf{A}_K^\infty$ in place of $\mathbf{A}_K^S$. Then, choosing an $\mathcal{O}_T$-model $\mathcal{X}$ of X, for some finite set $T \subset \Omega_K^\infty$, we can define a topological space

$$X(\mathbf{A}_K^S) = \widehat{\prod}_{v \in \Omega_K \setminus S} (X(K_v), \mathcal{X}(\mathcal{O}_v))$$

as in Section 1.3.

We say that X **satisfies Strong Approximation away from** S if the image of the diagonal embedding

$$X(K) \hookrightarrow X(\mathbf{A}_K^S)$$

is dense. If S is the set of Archimedean valuations of K, we say that X **satisfies strong approximation away from infinity**.

Remark 2.14. In the above discussion, we haven't paid much attention to the cases where $\prod_v X(K_v)$ or $X(\mathbf{A}_K)$ are empty. In this cases, by convention, we say that X satisfies Weak or Strong Approximation, respectively.

Weak and Strong Approximation are, in a sense, a refinement of the Local-Global Principle: not only we are asking that rational points exist, provided that there are points locally everywhere, but we also want to know if any collection of local points can be approximated by a rational point.

Example 2.15. Let X be a smooth projective quadric hypersurface in $\mathbb{P}_K^n$. Then X satisfies both Weak and Strong Approximation. In fact, assume that X has a K-point (otherwise we are done by Theorem 2.4). Then X is rational (Proposition 1.11) and since satisfying Weak approximation is a birational invariant ([12], Remark 2.1.4), then X satisfies Weak Approximation, because $\mathbb{A}_K^{n-1}$ does. By Remark 2.13, it also satisfies Strong Approximation.

Chapter 3

The Brauer Group of a Field

In this Chapter we introduce the Brauer group of a field, an object that will play a central role in our study of rational points. These ideas will be then extended to schemes in Chapter 4.

A modern text on the subject is [30]. Another reference is Milne's online notes on Class Field Theory [21].

A natural way to study this object is via Group Cohomology. We will use the main results of the subject, and refer to [31] for proofs and other facts.

3.1 Quaternion Algebras

We wish to introduce the theory of central simple algebras by studying the case of quaternion algebras. There are at least two reasons for this: first, it is useful to keep in mind this simple example when dealing with the general case, as many of the important ideas already appear in this context; second, in our main object of study (punctured affine cones over quadric surfaces) this is the only type of central simple algebras that appears (see Proposition 5.1).

We will mainly follow [30], Chapter 1. The reader can find there all the proofs that we omit, as well as other interesting facts.

3.1.1 Basic Facts

We begin by recalling the best known example, the quaternions $\mathbb{H}$.

Example 3.1. Let $\mathbb{H}$ be the four dimensional $\mathbb{R}$-algebra with basis $\{1, i, j, k\}$ and multiplication given by

$$i^2 = j^2 = -1, \qquad ij = -ji = k.$$

Then $\mathbb{H}$ is a division algebra over $\mathbb{R}$. To see this, define the *conjugate* of a quaternion $q = x + yi + zj + wk \in \mathbb{H}$ to be

$$\overline{q} = x - yi - zj - wk$$

and its *norm* to be $N(q) = q\overline{q} = x^2 + y^2 + z^2 + w^2$. Then $N(q) \neq 0$ if and only if $q \neq 0$ and that in this case $\frac{1}{N(q)}\overline{q}$ is a multiplicative inverse for q.

In fact, the algebra $\mathbb{H}$ is the only non-commutative finite-dimensional division algebra over $\mathbb{R}$. This is Frobenius' Theorem (see [9], §14).

Let us now fix an arbitrary field k. We can repeat the construction above in a straightforward way, unless $\operatorname{char} k = 2$. Since our main interest lies in studying quaternion algebras over number fields and their completions, **we will assume that** $\operatorname{char} k \neq 2$.

Definition 3.2. Let $a, b \in k^\times$. The *quaternion algebra* (a, b) is the four dimensional k-algebra with basis $\{1, i, j, h\}$ and multiplication given by

$$i^2 = a \qquad j^2 = b, \qquad ij = -ji = h.$$

Given the introductory example, it is natural to ask whether all quaternion algebras are division algebras. This is not the case.

Example 3.3 (The Matrix Algebra)**.** Let $b \in k^\times$. The quaternion algebra $(1, b)$ is isomorphic to the matrix algebra $M_2(k)$. In fact, the association

$$i \mapsto I := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad j \mapsto J := \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}$$

defines an isomorphism $(1, b) \cong M_2(k)$, because the matrices

$$\mathrm{Id} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad J = \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}, \quad IJ = \begin{bmatrix} 0 & b \\ -1 & 0 \end{bmatrix}$$

are basis for $M_2(k)$ as a k-vector space, and they satisfy the relations

$$I^2 = \mathrm{Id}, \qquad J^2 = b\,\mathrm{Id}, \qquad IJ = -JI.$$

The example above is so important that it deserves a name.

Definition 3.4. A quaternion algebra is called *split* if it is isomorphic to $M_2(k)$ as a k-algebra.

In fact, this is the only case of quaternion algebra that is not a division algebra.

Lemma 3.5. *A quaternion algebra is a division algebra if and only if it is not split.*

Proof. See [30], Proposition 1.1.7. □

The following Proposition will be very helpful in computing when a quaternion algebra is split.

Proposition 3.6. *Let* $a, b, u, v \in k^\times$.

1. *We have* $(a, b) \cong (u^2 a, v^2 b)$ *as* k*-algebras.*
2. *If* a *is a square in* k*, then* (a, b) *is split.*
3. *We have* $(a, b) \cong (b, a)$ *as* k*-algebras.*
4. *The algebra* (a, b) *is split if and only if* b *is the norm of some element in the quadratic field extension* $k(\sqrt{a})$*.*

Proof. For (1), notice that the association $i \mapsto ui$, $j \mapsto vj$ induces an isomorphism $(a,b) \cong (u^2a, v^2b)$. Part (2) follows from (1) and Example 3.3, because if $a = u^2$ then $(1,b) \cong (u^2,b) = (a,b)$. For (3) consider the substitution $i \mapsto abj$, $j \mapsto abi$, which gives $(a,b) \cong (a^2b^3, a^3b^2)$; then the result follows from (1). We omit the proof of (4), see [30], Proposition 1.1.7. □

We have the following structure Theorem. Recall that a k-algebra A is called *central* if $Z(A) = k$. A central division algebra is then a central algebra that is a division ring.

Proposition 3.7. *Every four-dimensional central division algebra over k is isomorphic to the quaternion algebra (a,b) for some $a,b \in k^\times$.*

Proof. See [30], Proposition 1.2.1 □

3.1.2 Field Extensions and Tensor Products

Notice that, if A is a quaternion algebra over k and $L \mid k$ is a field extension, then $A \otimes_k L$ is a quaternion algebra over L. If A is split, then also $A \otimes_k L$ is, but it may happen that A is not split and $A \otimes_k L$ is. In this case, we say that L *splits* A, or that A *is split over* L. In fact, every quaternion algebra is split over some quadratic field extension.

Proposition 3.8. *Let $a,b \in k^\times$. Then $k(\sqrt{a})$ splits (a,b).*

Proof. In fact, $(a,b) \otimes_k k(\sqrt{a})$ is just the quaternion algebra (a,b) defined over the field $k(\sqrt{a})$, and a is a square in this field. □

We now consider tensor products of quaternion algebras. This will give the group structure of the Brauer group as defined in Section 3.2. Notice that the tensor product of two matrix algebras $M_n(k)$ and $M_m(k)$ is isomorphic to $M_{nm}(k)$.

Of course, the tensor product of two quaternion algebras cannot be a quaternion algebra itself, since it has dimension 16 as a k-vector space.

Proposition 3.9. *Let $a,b,c \in k^\times$. Then $(a,b) \otimes_k (a,c) \cong (a,bc) \otimes_k M_2(k)$.*

The proof can be found in [30], Lemma 1.5.2. The next corollary follows easily.

Corollary 3.10. *Let $a,b \in k^\times$. Then $(a,b) \otimes_k (a,b) \cong M_4(k)$.*

Proof. By Proposition 3.9 and Proposition 3.6 we have

$$(a,b) \otimes_k (a,b) \cong (a,b^2) \otimes M_2(k) \cong M_2(k) \otimes_k M_2(k) \cong M_4(k).$$

□

3.1.3 Quaternion Algebras over $\mathbb{Q}_p$

As an example, we consider now the case $k = \mathbb{Q}_p$, where p is a prime number, which will be the most important in our applications. Similar considerations can be made in the case of completions of number fields.

Let $a, b \in \mathbb{Q}_p^\times$ and consider the quaternion algebra $A = (a, b)$ over $\mathbb{Q}_p$. Up to multiplying by squares as in Proposition 3.6(1), we can assume that $a, b \in \mathbb{Z}_p$ and that they are not in the square of the maximal ideal (that is, $p^2 \nmid a, b$).

We recall the following fact, which is just an application of Hensel's Lemma (Theorem 2.5). See also [10], Proposition 3.4.3, Corollary 3.4.4 and Problem 116.

Proposition 3.11. *1. Let $u \in \mathbb{Z}_p^\times$ be a p-adic unit. If $p \neq 2$, then u is a square in $\mathbb{Q}_p$ if and only if its class in the residue field $\mathbb{F}_p$ is a square. If $p = 2$, then u is a square in $\mathbb{Q}_p$ if and only if its class in $\mathbb{Z}_2/8\mathbb{Z}_2$ is 1.*

2. Let $a \in \mathbb{Q}_p^\times$. Then a is a square in $\mathbb{Q}_p$ if and only if it can be written in the form $a = u^2 p^{2m}$, where $u \in \mathbb{Z}_p^\times$ is a p-adic unit and $m \in \mathbb{Z}$.

The proposition above gives a quick way to conclude, in some cases, that A is split (Proposition 3.6(2)). If none of a and b is a square in $\mathbb{Q}_p$, we have to consider the quadratic extension $\mathbb{Q}_p(\sqrt{a}) \,|\, \mathbb{Q}_p$ (or, symmetrically, the extension $\mathbb{Q}_p(\sqrt{b}) \,|\, \mathbb{Q}_p$). Sometimes it is still very easy to check if $A = (a, b)$ is split.

In fact, the following holds. The proof uses techniques from Galois Cohomology, and we omit it. See [29] Proposition XIII.9.

Proposition 3.12. *Let $L \,|\, k$ be a finite, abelian extension of local fields and let $N_{L|k} : L^\times \to k^\times$ be the norm map. Then $[k^\times : N_{L|k}(L^\times)] = [L : k]$.*

Remark 3.13. With the help of the result above, we can also determine the index $[\mathcal{O}_k^\times : N_{L|k}(\mathcal{O}_L^\times)]$. In fact, let $e = e(L \,|\, k)$ be the ramification index and let π be a uniformizer for L, so that π^e is a uniformizer for k. Then $L^\times \cong \langle \pi \rangle \times \mathcal{O}_L^\times$ and $k^\times \cong \langle \pi^e \rangle \times \mathcal{O}_k^\times$, and the norm map sends π to $\pi^{[L:k]}$. We conclude that $[\mathcal{O}_k^\times : N_{L|k}(\mathcal{O}_L^\times)] = e$. For the unramified case, see also [29], Proposition V.3.

Example 3.14. Assume that $p \neq 2$. Then if $a, b \in \mathbb{Z}_p^\times$ are p-adic units, then $\mathbb{Q}_p(\sqrt{a}) \,|\, \mathbb{Q}_p$ is unramified and b is a norm from $\mathbb{Q}_p(\sqrt{a})$ by the results above, so $A = (a, b)$ is split by Proposition 3.6(4).

If $p = 2$, this is not true any more, because $\mathbb{Q}_p(\sqrt{a}) \,|\, \mathbb{Q}_p$ can be ramified even if a is a p-adic unit. Recall in fact that two quadratic extensions $\mathbb{Q}_p(\sqrt{d})$ and $\mathbb{Q}_p(\sqrt{d'})$ of $\mathbb{Q}_p$ are the same if and only if dd' is a square in $\mathbb{Q}_p$, and that, for every n, there is only one unramified extension of $\mathbb{Q}_p$ of degree n ([29], Corollary III.5.2). These facts are true for any p. It follows that $\mathbb{Q}_2$ has one unramified quadratic extension (that is $\mathbb{Q}_2(\sqrt{5})$) and 6 ramified ones (that are $\mathbb{Q}_2(\sqrt{d})$ for $d = 2, 3, 6, 7, 10, 14$), see Proposition 3.11.

Example 3.15. Let $p = 2$, $a = 3$ and $b \in \mathbb{Q}_2^\times$. Consider the quaternion algebra $A = (3, b)$. We want to see for which values of b this algebra is split. This is equivalent to determining which p-adic numbers $b \in \mathbb{Q}_2^\times$ are the norm of some element of $\mathbb{Q}_2(\sqrt{3})$. So we have to determine the image of the norm map $N_{\mathbb{Q}_2(\sqrt{3}) \,|\, \mathbb{Q}_2} : \mathbb{Q}_2(\sqrt{3})^\times \to \mathbb{Q}_2^\times$, which is a subgroup G of index 2 of $\mathbb{Q}_2^\times$ (Remark 3.13).

An element b of $\mathbb{Q}_2^\times$ is a norm from $\mathbb{Q}_2(\sqrt{3})$ if and only if it can be written as $b = x^2 - 3y^2$, for some $x, y \in \mathbb{Q}_2$. Then clearly $(\mathbb{Q}_2^\times)^2 \subset G$, and it is enough to work in the quotient $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$, that is to determine the group $G/(\mathbb{Q}_2^\times)^2$.

Using Proposition 3.11, one can see that $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ can be given by representatives $\{1, 2, 3, 5, 6, 7, 10, 14\}$. Using the following values for $(x, y) \in \mathbb{Q}_2 \times \mathbb{Q}_2$:

$$(1,0), \qquad (0,1), \qquad (3,1), \qquad (1,1)$$

we see that G is represented, modulo squares, by $\{1, 5, 6, 14\}$.

3.2 Central Simple Algebras and The Brauer Group

In order to define the Brauer group of a field, we need to study central simple algebras. In fact, the Brauer group can be seen as the set of such algebras with tensor product as an operation, modulo introducing a suitable equivalence relation.

For this section we fix a base field k, this time with no assumption on the characteristic. We will be only interested in k-algebras that are finite-dimensional over k. Recall that by k-algebra we mean a (not necessarily commutative) ring A, containing k in its centre.

Definition 3.16. Let A be a finite-dimensional k-algebra. Then A is called *central* if $Z(A) = k$. It is called *simple* if it is simple as a ring, that is if it contains no non-trivial two sided ideal. A *central simple algebra* is a finite-dimensional k-algebra that is central and simple.

Notice in particular that **we assume central simple algebras to be finite-dimensional** as k-vector spaces.

Example 3.17. Division rings are simple. Moreover, the centre of a division ring D is a field: it is a commutative subring, and if $x \in Z(D) \setminus \{0\}$ then for every $y \in D$ we have $xy = yx \implies yx^{-1} = x^{-1}y \implies x^{-1} \in Z(D)$. So a division ring is a central simple algebra over its centre K, if it is finite-dimensional as a K-vector space.

Example 3.18. If D is a division ring and $M_n(D)$ is the ring of $n \times n$ matrices with coefficients in D, then $M_n(D)$ is a central simple algebra over $Z(D)$. See [30], Example 2.1.2.

In particular, we see that a quaternion algebra over k is always a central simple algebra: if it is split, this follows from Example 3.18. If it is not, it follows from Example 3.17, noting that its centre must coincide with k: this can be easily seen by imposing the conditions $iq = qi$ and $jq = qj$ on a generic quaternion $q = x + yi + zj + wk$.

We have a converse to Example 3.18.

Theorem 3.19 (Wedderburn)**.** *Every finite-dimensional simple k-algebra A is of the form $M_n(D)$ for some $n \in \mathbb{N}_{\geq 1}$ and some division algebra D, unique up to isomorphism.*

Sketch of proof. Let $L \subset A$ be a left ideal of A. Then L is a simple A-module. By Schur's Lemma, $D = \mathrm{End}_A(L)$ is a division algebra. One then checks that the map $\lambda : A \to \mathrm{End}_D(L)$ sending $a \in A$ to the homomorphism $x \mapsto ax$ is an isomorphism. For the details, see [30], Theorem 2.1.3. □

Example 3.20. If k is algebraically closed, then there is no non-split central simple algebra over k. In fact, in that case there would be a non-trivial finite-dimensional division algebra D over k, as in Wedderburn's Theorem. Assume this holds, and let $d \in D \setminus k$. Since D is finite-dimensional, there is some n such that $\{1, d, \ldots, d^n\}$ is linearly dependent over k. So there is a polynomial $f \in k[X]$ such that $f(d) = 0$. This means that d is algebraic over k. Since k is algebraically closed, we have $d \in k$, a contradiction.

Recall that if A is any ring, we denote by A^{op} the ring that has the same additive structure and multiplication reversed.

Proposition 3.21. *Let A be a central simple k-algebra of dimension n. Then $A \otimes_k A^{\mathrm{op}} \cong M_n(k)$.*

Proof. See [21], Corollary IV.2.9 or [30], Proposition 2.4.8. □

Remark 3.22. The property of Proposition 3.21 can in fact be taken as a definition of central simple algebra: a k-algebra A of dimension n is central and simple if and only if $A \otimes_k A^{\mathrm{op}} \cong M_n(k)$. See [22], Proposition IV.1.1.

Recall that every automorphism of a central simple algebra is inner. This comes from the following more general statement.

Theorem 3.23 (Skolem-Noether)**.** *Let A and B be finite-dimensional k-algebras, with A simple and B central simple, and let $f, g : A \to B$ be two k-algebra homomorphisms. Then there is $b \in B^\times$ such that $f(a) = b^{-1} \cdot g(a) \cdot b$ for all $a \in A$.*

Proof. See [21], Chapter IV, Theorem 2.10. □

Corollary 3.24. *Every automorphism of a central simple algebra A is of the form $x \mapsto a^{-1}xa$ for some invertible $a \in A$.*

Proof. Apply Theorem 3.23 to the given automorphism and the identity map $\mathrm{id}_A : A \to A$. See also [30], Theorem 2.7.2. □

3.2.1 Splitting Fields

The following proposition shows that the Brauer group, as contructed in Section 3.2.2, is functorial in the base field k.

Proposition 3.25. *Let A be a finite-dimensional k-algebra and $L \mid k$ a field extension. Then A is central simple over k if and only if $A \otimes_k L$ is central simple over L.*

Proof. See [30], Lemma 2.2.2. □

There is another characterization of central simple algebras: they are "twisted forms" of matrix algebra.

Proposition 3.26. *Let A be a finite-dimensional k-algebra. Then A is central simple if and only if $A \otimes_k L \cong M_n(L)$ for some n and some finite field extension $L \mid k$.*

Proof. See [30], Theorem 2.2.1. □

Corollary 3.27. *If A is a central simple k-algebra, $[A : k]$ is a square.*

As in the case of quaternion algebras, if A is a central simple k-algebra and $L \mid k$ is a field extension, we say that L *splits* A if $A \otimes_k L \cong M_n(L)$ for some n.

Remark 3.28. Let A be a central simple k-algebra. Since for any field extension $L \mid k$ we have $M_n(k) \otimes_k L \cong M_n(L)$, we have that if L splits A, then every extension $M \mid L$ also splits A. In particular, by taking the normal closure, we can assume that A is split by a finite normal extension. If k is perfect, A is then split by a finite Galois extension.

Moreover, every central simple k-algebra is split by a finite separable extension ([30], Proposition 2.2.5 or [21], Proposition IV.3.8), so the same conclusion holds also when k is not perfect.

We can be more precise and characterize the fields that split a fixed central simple algebra, following [21], Section IV.3. We will need the following result.

Lemma 3.29. *Let A be a central simple k-algebra and let B be a simple k-subalgebra of A. Let $C = C(B)$ be the centralizer of B in A, which is a k-subalgebra of A. Then we have:*

(a) C is simple;

(b) B is the centralizer of C in A;

(c) $[B : k] \cdot [C : k] = [A : k]$.

Proof. See [21], Theorem IV.3.1. □

Proposition 3.30. *Let A be a central simple k-algebra and let L be a field extension of k contained in A. Then the following are equivalent.*

(i) L is its own centralizer in A.

(ii) $[L : k]^2 = [A : k]$.

(iii) L is a maximal commutative k-subalgebra of A.

Moreover, a finite field extension $M \mid k$ splits A if and only if there is a central simple algebra B containing M as a maximal subfield and such that $A \otimes_k M_n(k) \cong B \otimes_k M_m(k)$ for some $m, n \in \mathbb{N}$.

Proof. Since L is commutative, it is contained in its centralizer $C(L)$. By Lemma 3.29 we have $[L : k] \cdot [C(L) : k] = [A : k]$, so (i) $\iff$ (ii).

For (ii) $\implies$ (iii), let L' be a maximal commutative k-subalgebra of A containing L. Then L' is contained in the centralizer of L, so $[A : k] \geq [L : k] \cdot [L' : k] \geq [L : k]^2$, which implies $L = L'$.

For (iii) $\implies$ (i), assume there is $c \in A$ contained in the centralizer of L, but not in L. Then $L[c]$ is a commutative k-subalgebra of A strictly containing L, which contradicts the maximality of L.

For the last part see [21], Corollary IV.3.6. □

3.2.2 First Definition of the Brauer Group

We are now almost ready to define the Brauer group of a field in its explicit form. The following Proposition gives the group operation.

Proposition 3.31. *The tensor product of two central simple k-algebras is a central simple k-algebra.*

Proof. Let A and B be two central simple algebras over k, and let L be an extesion of k that splits both of them. Then

$$\begin{aligned}(A \otimes_k B) \otimes_k L &\cong A \otimes_k (B \otimes_k L) \cong A \otimes_k M_n(L) \cong A \otimes_k (M_n(k) \otimes_k L) \cong \\ &\cong (A \otimes_k L) \otimes_k M_n(k) \cong M_m(L) \otimes_k M_n(k) \cong \\ &\cong (M_m(k) \otimes_k M_n(k)) \otimes_k L \cong M_{mn}(k) \otimes_k L \cong \\ &\cong M_{mn}(L)\end{aligned}$$

so $A \otimes_k B$ is central simple by Proposition 3.26. □

As we mentioned above, we would like the set of isomorphism classes of finite-dimensional central simple k-algebras to form a group under the tensor product. However, this is not possible, unless we quotient this set by some equivalence relation: taking the tensor product of algebras, the dimension can only grow. This is why we introduce the following definition, which we have already used in Proposition 3.30.

Definition 3.32. Two central simple k-algebras A and B are called *(Brauer) equivalent* if there exist m and n such that $A \otimes_k M_n(k) \cong B \otimes_k M_m(k)$.

Remark 3.33. By Wedderburn's Theorem, two central simple k-algebras A and B are Brauer equivalent if and only if they are matrix rings over the same division k-algebra D. Thus, two central simple k-algebras of the same dimension are Brauer equivalent if and only if they are isomorphic.

For a finite Galois extension $L \mid k$, we let $\mathrm{Br}(L \mid k)$ denote the set of Brauer equivalence classes of central simple k-algebras that are split by L. The tensor product $\otimes_k$ clearly defines an associative and commutative operation on $\mathrm{Br}(L \mid k)$ (Proposition 3.31), and if $[A] \in \mathrm{Br}(L \mid k)$ then also A^{op} is split by L: in fact $A^{\mathrm{op}} \otimes_k L \cong (A \otimes_k L^{\mathrm{op}})^{\mathrm{op}} \cong M_n(L)^{\mathrm{op}} \cong M_n(L)$, since L is commutative and a matrix ring is isomorphic to its opposite (see [14], Theorem §8.I).

We conclude that $\mathrm{Br}(L \mid k)$ forms an abelian group under the tensor product. Moreover, by Proposition 3.25, for every finite Galois extension $M \mid k$ containing L we have a natural inclusion map $\lambda_{NM} : \mathrm{Br}(L \mid k) \hookrightarrow \mathrm{Br}(M \mid k)$. The collection $\{\mathrm{Br}(L \mid k), \lambda_{NM}\}$ then forms a filtered directed system of abelian groups indexed by the finite Galois extensions of k, and we can take the direct limit of this sistem.

Definition 3.34. The *Brauer group* of k is the direct limit

$$\mathrm{Br}(k) = \varinjlim_{L \mid k \text{ finite Galois}} \mathrm{Br}(L \mid k) = \bigcup_{L \mid k \text{ finite Galois}} \mathrm{Br}(L \mid k).$$

In other words, it is the set of equivalence classes of central simple k-algebras with the tensor product operation.

Remark 3.35. By Proposition 3.25, we have a map $\mathrm{Br}(k) \to \mathrm{Br}(L)$ given by $A \mapsto A \otimes_k L$. Its kernel is precisely $\mathrm{Br}(L \mid k)$.

3.2.3 Cohomological Description of the Brauer Group

As we said in the introduction, a natural way to study the Brauer group, and to prove many useful facts about it, is via Group Cohomology. This is why we are going to describe $\mathrm{Br}(k)$ as a cohomology group. We will follow Milne's notes [21]; an alternative approach is given in [30], Chapter 4. The one we choose is more explicit, and has the advantage of avoiding non-commutative cohomology sets.

Fix a finite Galois extension $L \mid k$, and let $G = \mathrm{Gal}(L \mid k)$. Let A be a central simple k-algebra containing L as a maximal subfield. See Proposition 3.30.

Let $\sigma \in G$. Applying Theorem 3.23 to $L \xrightarrow{\sigma} L \hookrightarrow A$ and $L \hookrightarrow A$, we see that there is an element $e_\sigma \in A$ such that

$$\sigma(a) = e_\sigma a e_\sigma^{-1} \quad \text{for all } a \in L \tag{3.1}$$

or equivalently

$$e_\sigma a = \sigma(a) e_\sigma. \tag{3.2}$$

Assume $f_\sigma \in A$ is such that (3.1) is satisfied with f_σ in place of e_σ. Then we have $f_\sigma^{-1} e_\sigma a (f_\sigma^{-1} e_\sigma)^{-1} = f_\sigma^{-1} \sigma(a) f_\sigma = a$, so $f_\sigma^{-1} e_\sigma$ is in the centralizer of L in A, which coincides with L by Proposition 3.30. So e_σ is determined by σ up to multiplication by an element in $L^\times$.

Moreover, if we fix $\tau \in G$ and $e_\sigma, e_\tau, e_{\sigma\tau}$ satisfying (3.1) for σ, τ and $\sigma\tau$ respectively, we have that $e_\sigma e_\tau$ also satisfies (3.1) for $\sigma\tau$, so there is $\varphi(\sigma, \tau) \in L^\times$ such that

$$e_\sigma e_\tau = \varphi(\sigma, \tau) e_{\sigma\tau}. \tag{3.3}$$

One can check that $\varphi : G \times G \to L^\times$ is a 2-cocycle, which is normalized if we pick $e_1 = 1$ (see [31], Application 6.5.5 and Example 6.5.7 or [21], Chapter II) and that different choices of the e_σ's lead to cohomologous 2-cocycles. Thus we get a well-defined element $\gamma(A) := \varphi \in H^2(G, L^\times)$. It can be seen that $\gamma(A)$ depends only on the isomorphism class of A ([21], Theorem IV.3.11).

Vice versa, given a normalized 2-cocycle $\varphi : G \times G \to L^\times$, we can define a k-algebra $A(\varphi)$ in the following way. As a k-vector space, let $A(\varphi)$ have basis $\{e_\sigma \mid \sigma \in G\}$ (the e_σ's are now just symbols). Let the multiplicative structure of $A(\varphi)$ be given by (3.2) and (3.3). It can be checked that $A(\varphi)$ is then a central simple k-algebra ([21], Lemma IV.3.13).

If we denote by $\mathcal{A}(L \mid k)$ the set of isomorphism classes of central simple k-algebras containing L as a maximal subfield (warning: this notation is in contrast with the one used in [21]), the maps $[A] \mapsto \gamma(A)$ and $\varphi \mapsto A(\varphi)$ define a

bijection between $\mathcal{A}(L \mid k)$ and $H^2(G, L^\times)$. Moreover, notice that by Proposition 3.30 every algebra containing L as a maximal subfield has dimension $[L : k]^2$ over k. By Remark 3.33, we have then a bijection between $\mathrm{Br}(L \mid k)$ and $\mathcal{A}(L \mid k)$, thus between $\mathrm{Br}(L \mid k)$ and $H^2(G, L^\times)$.

Although not easily, it can be seen (with elementary techiniques) that the map $\varphi \mapsto A(\varphi)$ is a group homomorphism, that is that $A(\varphi + \varphi')$ is Brauer equivalent to $A(\varphi) \otimes_k A(\varphi')$. This is the content of [21], Lemma IV.3.15, where a proof is sketched and other references are given. So we have the following.

Theorem 3.36. *Let $L \mid k$ be a finite Galois extension with Galois group G. Then we have an isomorphism of groups*

$$\mathrm{Br}(L \mid k) \cong H^2(G, L^\times).$$

Moreover, if $\overline{G} = \mathrm{Gal}(k_{\mathrm{sep}} \mid k)$ is the absolute Galois group of k, we have

$$\mathrm{Br}(k) \cong H^2(\overline{G}, k_{\mathrm{sep}}^\times).$$

Proof. The first part follows from the discussion above. For the second part, we just have to take the limit over the directed system of all finite Galois extensions of k. See [21], Corollary IV.3.10, or [31], 6.11.1 and 6.11.17. □

Thanks to this new description of the Brauer group, we can now state some of its properties.

Corollary 3.37. *Let $L \mid k$ be a finite Galois extension of degree n. Then every element of $\mathrm{Br}(L \mid k)$ has order dividing n. In particular, $\mathrm{Br}(k)$ is torsion.*

Proof. The first part holds because it does for cohomology groups, see [31], Theorem 6.5.8. The second part follows because $\mathrm{Br}(k)$ is the direct limit of the $\mathrm{Br}(L \mid k)$'s. □

Corollary 3.38. *Let n be a positive integer coprime to the characteristic of k. Then the n-torsion subgroup of the Brauer group of k is*

$$\mathrm{Br}(k)[n] \cong H^2(G, \mu_n)$$

where G denotes the absolute Galois group of k and μ_n the group of n-th roots of unity in a separable closure k_{sep} of k.

Proof. By the assumption on the characteristic of k, we have an exact sequence

$$1 \to \mu_n \to k_{\mathrm{sep}}^\times \xrightarrow{n} k_{\mathrm{sep}}^\times \to 1$$

and from the cohomology long exact sequence we get

$$H^1(G, k_{\mathrm{sep}}^\times) \to H^2(G, \mu_n) \to H^2(G, k_{\mathrm{sep}}^\times) \xrightarrow{n} H^2(G, k_{\mathrm{sep}}^\times)$$

and the first group is trivial by Hilbert's Theorem 90 (see [31], Theorem 6.11.16). □

Corollary 3.39. *Let $L \mid k$ be a finite cyclic Galois extension. Then we have*

$$\mathrm{Br}(L \mid k) \cong k^\times / N_{L \mid k}(L^\times).$$

Proof. See [31], Theorem 6.2.2. □

3.3 The Brauer Groups of Some Special Fields

We will collect here some results about the Brauer groups of some fields that are particularly interesting for us. The most important result for our applications is Theorem 3.44. We follow again [21], Chapter IV, Section 4.

3.3.1 Finite Fields

Finite fields have trivial Brauer group. One way to see this is using the following result.

Theorem 3.40 (Wedderburn's Little Theorem)**.** *Every finite division ring is a field.*

Proof. See [21], Theorem IV.4.1. □

In particular, if k is a finite field, then every finite-dimensional division algebra over k is a finite division ring, hence it is commutative. Then it must coincide with k by Lemma 3.29. From this it follows that every central simple algebra over k is of the form $M_n(k)$ for some n, hence we have $\mathrm{Br}(k) = 0$.

We can also give a cohomological proof of this fact. Let $q = \#k$ and let $L \mid k$ be any Galois extension of degree n. Let $\alpha \in L^\times$ be a generator of the multiplicative group $L^\times$. So α has order $q^n - 1$ and $N_{L \mid k}(\alpha) = \alpha^{1+q+\cdots+q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}} \in k^\times$ has order $q-1$, so it generates $k^\times$. Thus the norm map $N_{L \mid k} : L^\times \to k^\times$ is surjective. Since $L \mid k$ is a finite extension of finite fields, it is cyclic, so by Corollary 3.39 we have $\mathrm{Br}(L \mid k) = 0$. Since this holds for arbitrary L, we get $\mathrm{Br}(k) = 0$.

3.3.2 Real and Complex Numbers

By Example 3.20, we see that if k is algebraically closed then $\mathrm{Br}(k) = 0$. In particular, $\mathrm{Br}(\mathbb{C}) = 0$.

From Frobenius' Theorem, it follows that $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$: there is only one non-trivial finite-dimensional central division algebra over $\mathbb{R}$ (the quaternions $\mathbb{H}$), and it has order two in the Brauer group of $\mathbb{R}$ by Corollary 3.10. Another way to see that $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ is using Corollary 3.39.

3.3.3 Non-Archimedean Local Fields

Let K be a non-Archimedean local field with ring of integers $\mathcal{O}_K$, maximal ideal $\mathfrak{m}_K$ and finite residue field $k = \mathcal{O}_K/\mathfrak{m}_K$. We will first follow [21], Section III, and compute the cohomology of unramified extensions of K.

Let L be an unramified extension of K, with ring of integers $\mathcal{O}_L$. Suppose first that $[L:k]$ is finite. By Remark 3.13, the norm map

$$N_{L\,|\,K} : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$$

is surjective. Since the Galois group $G = \mathrm{Gal}(L\,|\,K)$ coincides with the Galois group of the residue fields, it is cyclic, so by [31], Theorem 6.2.2, we have $H^n(G, \mathcal{O}_L^\times) = 0$ for $n > 0$. Passing to the limit ([31], Theorem 6.11.13), we see that the same holds even if $[L:k]$ is infinite.

So assume now that $L\,|\,k$ is a, possibly infinite, unramified extension. For any finite subextension $M \subset L$ there is a unique extension $\mathrm{ord}_M : M^\times \to \mathbb{Z}$ of the discrete valuation $\mathrm{ord}_k : k^\times \to \mathbb{Z}$ on k. In particular, for any two finite subextensions $L_1, L_2 \subset L$ we have that the restrictions to $L_1 \cap L_2$ of $\mathrm{ord}_{L_1} : L_1^\times \to \mathbb{Z}$ and $\mathrm{ord}_{L_2} : L_2^\times \to \mathbb{Z}$ coincide. So we get a discrete valuation $\mathrm{ord}_L : L^\times \to \mathbb{Z}$ on L. Then from the exact sequence of G-modules

$$0 \longrightarrow \mathcal{O}_L^\times \longrightarrow L^\times \xrightarrow{\mathrm{ord}_L} \mathbb{Z} \longrightarrow 0$$

where $\mathbb{Z}$ is the trivial G-module, we get an isomorphism

$$\mathrm{ord}_L : H^2(G, L^\times) \xrightarrow{\sim} H^2(G, \mathbb{Z}).$$

Consider the exact sequence of trivial G-modules

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0;$$

since $H^n(G, \mathbb{Q}) = 0$ for $n > 0$ ([31], Corollary 6.5.9) we have that the connection homomorphism

$$\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G, \mathbb{Z})$$

is an isomorphism. Since G is topologically cyclic, by [31], 6.11.15 we have a canonical isomorphism

$$H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

In particular, taking $L = K_{\mathrm{unr}}$ to be the maximal unramified extension of K, we conclude the following.

Lemma 3.41. *We have a canonical isomorphism*

$$\mathrm{inv}_K^{\mathrm{unr}} : \mathrm{Br}(K_{unr}\,|\,K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

It turns out that every central simple algebra over a non-Archimedean local field K with finite residue field is split by an unramified extension. See for example [29], Theorem XII.1 for a cohomological proof. It is also possible to prove this in a more explicit way, as in [29], Section XII.§2 or [21], Section IV.4. This second approach has the advantage of giving an explicit description of the Hasse Invariant Map.

Then we have $\mathrm{Br}(K) = \mathrm{Br}(K_{\mathrm{unr}}\,|\,K)$, and we get the following.

Theorem 3.42. *We have a canonical isomorphism*

$$\mathrm{inv}_K : \mathrm{Br}(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

called the ***Hasse Invariant Map*** *of* K.

Remark 3.43. The result above shows that every central simple algebra over a local field k is *cyclic*, that is it contains a maximal subfield L (which is then a splitting field) that is a cyclic Galois extension of k. It is possible to give a more explicit construction of cyclic algebras, which generalizes that of quaternion algebras. See [30], Section 2.5.

3.3.4 Number Fields

Let now K be a number field. For any $v \in \Omega_K$, we denote by K_v the completion of K with respect to v. If v is non-Archimedean, we denote by $\mathcal{O}_v$ the ring of integers of K_v.

For $v \in \Omega_K$ non-Archimedean, we have defined in the previous section the Hasse Invariant Map

$$\mathrm{inv}_v : \mathrm{Br}(K_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

We want to define a similar map for $v \in \Omega_K$ Archimedean. If $K_v \cong \mathbb{C}$, then $\mathrm{Br}(\mathbb{C}) = 0$ (see Section 3.3.2 above) and we just let $\mathrm{inv}_v : \mathrm{Br}(\mathbb{C}) \to \mathbb{Q}/\mathbb{Z}$ be the zero map. If $K_v \cong \mathbb{R}$, we have a canonical isomorphism $\mathrm{Br}(K_v) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, and we let $\mathrm{inv}_v : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ be the composition

$$\mathrm{Br}(K_v) \xrightarrow{\sim} \frac{1}{2}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

It is possible to show (see the references given below) that if A is a central simple K-algebra, then $A \otimes_K K_v$ is split for all but finitely many $v \in \Omega_K$.

We can prove this easily for quaternion algebras. Let $a, b \in K^\times$ and consider the quaternion algebra (a, b) over K. For all but finitely many non-Archimedean $v \in \Omega_K$, both a and b are units in $\mathcal{O}_v$. This means that b is a norm from the unramified field extension $K_v(\sqrt{a})$ (Remark 3.13), so (a, b) is split over K_v.

We are now ready to state the main result on the Brauer group of number fields.

Theorem 3.44. *There is an exact sequence of abelian groups*

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_{v \in \Omega_K} \mathrm{Br}(K_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Proof. See [21], Chapters VII and VIII or [24], Theorem III.5.8. □

Remark 3.45. The statement above is as deep as the main results of Class Field Theory. There are a few facts that we can deduce from the exact sequence above.

1. The injectivity of the map on the left is the so called *local-global principle for central simple algebras*, also known as the Albert-Brauer-Hasse-Noether Theorem: it tells us that a central simple algebra is split over K (that is, its class in $\mathrm{Br}(K)$ is zero) if and only if it is split over each completion of K.

2. Let $a, b \in K^\times$ and consider the quaternion algebra (a, b) over K. The fact that $\sum \mathrm{inv}_v\left((a, b) \otimes_K K_v\right) = 0$ is a restatement of Hilbert's Product formula for the Hilbert symbol, which in turn is equivalent to the quadratic reciprocity laws. See [27], Chapter III for the case $K = \mathbb{Q}$.

Chapter 4

The Brauer Group of a Scheme

As in the case of fields, the Brauer Group of a scheme X can be defined in two ways. One is more explicit

$$\mathrm{Br}(X) = \{\text{Equivalence classes of Azumaya } \mathcal{O}_X\text{-algebras}\}$$

and the other is cohomological

$$\mathrm{Br}'(X) = H^2_{\text{ét}}(X, \mathbb{G}_m)$$

where $H^2_{\text{ét}}(X, \mathbb{G}_m)$ denotes the second *étale cohomology* group of X with $\mathbb{G}_m$ coefficients (see [22], Chapter III). In fact, if $X = \operatorname{Spec} k$ is the spectrum of a field, the two definitions coincide and give back the Brauer Group that we defined in the previous chapter (see [22], Example II.1.7).

However, for a general scheme X, the two definitions do not always coincide. If X is locally Noetherian, there is a canonical injection $\mathrm{Br}(X) \hookrightarrow \mathrm{Br}'(X)$ (Proposition 4.7), which is an isomorphism in some cases (see Proposition 4.10).

As we did in the previous chapter with Galois cohomology, we will make use of étale cohomology when needed, referring to [22].

4.1 Azumaya Algebras over Local Rings

First of all, we want to extend the definition of central simple algebras over a field to algebras over local rings.

Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field k.

Definition 4.1. Let A be an R-algebra that is free and of finite rank as an R-module. Then A is called an *Azumaya algebra* if $A \otimes_R k$ is a central simple k-algebra.

There is a more classical definition: a finite and free R algebra A is Azumaya if and only if the map $A \otimes_R A^{\mathrm{op}} \to \mathrm{End}_R(A) \cong M_n(R)$ sending $a \otimes a'$ to the R-linear map $x \mapsto axa'$ is an isomorphism. See [22], Propositions IV.1.1 and IV.1.2.

With this definition, many of the results of Section 3.2 can be extended to the case of local rings. For example, by the classical definition above we deduce that Azumaya algebras have a rank over R that is a square. We collect some of these facts in the following proposition. For proofs, see [22], IV.1.

Proposition 4.2. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field k.*

1. *The matrix algebra $M_n(R)$ is an Azumaya R-algebra.*
2. *(Skolem-Noether) Every automorphism of an Azumaya R-algebra is inner.*
3. *If S is a local R-algebra and A is an Azumaya R-algebra, $A \otimes_R S$ is an Azumaya S-algebra.*
4. *If A and B are two Azumaya R-algebras, $A \otimes_R B$ is an Azumaya R-algebra.*
5. *Any Azumaya algebra A is split by a maximal étale subalgebra; that is, there is a commutative étale R-subalgebra $S \subset A$ of rank $n = \sqrt{[A : R]}$ such that $A \otimes_R S \cong M_n(S)$.*

Exactly as in the case of central simple algebras, we say that two Azumaya R-algebras A and B are Brauer equivalent if $A \otimes_R M_n(R) \cong B \otimes_R M_m(R)$ for some n and m. The set of Brauer equivalence classes of Azumaya algebras forms then a group, which we call **the Brauer Group** of R, and denote by $\mathrm{Br}(R)$. This is again a functor on R, by part 3 of the Proposition above.

To conclude this section, we give the following Proposition. Recall that a Noetherian local ring R is called *Henselian* if every finite R-algebra is a direct product of local rings. This is equivalent to the fact that "Hensel's Lemma holds for R", see [22], I.4 for details. In particular, complete Noetherian local rings are Henselian.

Proposition 4.3. *If R is Henselian, the canonical map $\mathrm{Br}(R) \hookrightarrow \mathrm{Br}(k)$, where k is the residue field of R, is injective.*

Proof. See [22], Proposition IV.1.6. □

Corollary 4.4. *If R is a complete Noetherian local ring with finite residue field, then $\mathrm{Br}(R) = 0$.*

Proof. The Brauer group of a finite field is zero, see Section 3.3.1. □

4.2 Azumaya Algebras over Structure Sheaves

For the rest of this section, let X be a **locally Noetherian** scheme with structure sheaf $\mathcal{O}_X$. Recall that a collection of morphism of schemes $(U_i \to X)$ is called an *étale covering* of X if the following conditions are satisfied:

- each $U_i \to X$ is étale;
- the (set-theoretic) union of the images of the $U_i \to X$ is X.

Definition 4.5. Let A be a (not necessarily commutative) $\mathcal{O}_X$-algebra that is a coherent $\mathcal{O}_X$-module. Then A is called an *Azumaya algebra* if it satisfies one of the following equivalent conditions:

(i) For every closed point $x \in X$, the stalk A_x is an Azumaya $\mathcal{O}_{X,x}$-algebra.

(ii) For every point $x \in X$, the stalk A_x is an Azumaya $\mathcal{O}_{X,x}$-algebra.

(iii) For every point $x \in X$, $A(x) := A_x \otimes_{\mathcal{O}_{X,x}} k(x)$ is a central simple algebra over the residue field $k(x)$ of x.

(iv) A is étale-locally split, that is, there is an étale covering $(U_i \to X)$ of X such that for each i we have $A \otimes_{\mathcal{O}_X} \mathcal{O}_{U_i} \cong M_{r_i}(U_i)$ for some r_i. Here $M_{r_i}(U_i)$ denotes the sheaf of $r_i \times r_i$ matrices over $\mathcal{O}_{U_i}$.

For a proof of the equivalence of the conditions above, see [22], Proposition IV.2.1.

We can now define the Brauer group of a locally Noetherian scheme X. Two Azumaya $\mathcal{O}_X$-algebras A and B are called *Brauer equivalent* if there are two non-zero finitely generated locally free $\mathcal{O}_X$-modules $\mathcal{F}$ and $\mathcal{G}$ such that

$$\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{E}nd(\mathcal{F}) \cong \mathcal{B} \otimes_{\mathcal{O}_X} \mathcal{E}nd(\mathcal{G}).$$

Here $\mathcal{E}nd(-)$ denotes the *sheaf* End, defined by

$$(\mathcal{E}nd(F))(U) = \mathrm{End}_{\mathcal{O}_U}(\mathcal{F}_{|U}, \mathcal{F}_{|U}),$$

see [13], Section II.5.

As in the case of fields, the set of equivalence classes of $\mathcal{O}_X$-Azumaya algebras becomes a group under the tensor product, which we denote by $\mathrm{Br}(X)$ and call the **Brauer Group** of X (see [22], IV.2). Clearly $\mathrm{Br}(-)$ is a contravariant functor.

Remark 4.6. If $X = \mathrm{Spec}\, R$ is the spectrum of a Noetherian local ring, then $\mathrm{Br}(X) = \mathrm{Br}(R)$. In particular, $\mathrm{Br}(k) = \mathrm{Br}(\mathrm{Spec}\, k)$ for any field k.

4.2.1 Relation to Étale Cohomology

As we mentioned, the Brauer group of X is related to the étale cohomology of X, but in general it is not equal to its second étale cohomology group with $\mathbb{G}_m$ coefficients, as happens in the case of fields. More precisely, we have the following.

Proposition 4.7. *There is a canonical inclusion* $\mathrm{Br}(X) \hookrightarrow H^2_{\text{ét}}(X, \mathbb{G}_m)$.

Proof. See [22], Theorem IV.2.5. □

This is still enough to draw some conclusions about $\mathrm{Br}(X)$ in the general case, for example the following.

Corollary 4.8. *If X has finitely many connected components,* $\mathrm{Br}(X)$ *is torsion.*

Proof. See [22], Proposition IV.2.7. □

However, we will only be interested in more specific classes of schemes X. For example, we will almost always be able to use the following facts.

Proposition 4.9. *Let X be a regular, integral and locally Noetherian scheme and let K be its function field. Then the map* $\mathrm{Br}(X) \to \mathrm{Br}(K)$ *given by the inclusion of the generic point is injective.*

Proof. See [22], Corollary IV.2.6. □

Proposition 4.10. *If X is a regular and quasi-projective variety over a field, then* $\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_m)$.

Proof. See [25], Corollary 6.6.19. □

4.3 The Brauer-Manin Obstruction

For this section, we let K be a number field with ring of integers $\mathcal{O}$.

The idea of using the Brauer group of a variety over a global field to explain the failure of the local-global principle was first introduced by Manin in [20].

Let X be a K-scheme, $L \mid K$ a field extension and $P : \operatorname{Spec} L \to X$ be an L-point of X. By functoriality, this induces a map $\mathrm{Br}(X) \to \mathrm{Br}(L)$, which we call *evaluation at* P and denote by ev_P. If $A \in \mathrm{Br}(X)$, we will also write $A(P)$ for $\mathrm{ev}_P(A)$.

Lemma 4.11. *Let X be a variety over K. If $(x_v) \in X(\mathbf{A}_K)$ and $A \in \mathrm{Br}(X)$, then $A(x_v) = 0$ in $\mathrm{Br}(K_v)$ for all but finitely many v.*

Proof. By [25], Corollary 6.6.11 there are a finite set $S \subset \Omega_K^\infty$, an $\mathcal{O}_S$-model $\mathcal{X}$ for X and an $\mathcal{A} \in \mathrm{Br}(\mathcal{X})$ that maps to A under the map $\mathrm{Br}(\mathcal{X}) \to \mathrm{Br}(X)$ given by the inclusion of X as the generic fiber of $\mathcal{X}$ (see also Section 1.2). We may assume that $x_v \in \mathcal{X}(\mathcal{O}_v)$ for all $v \notin S$. For $v \notin S$ the following diagram commutes

$$\begin{array}{ccc} \mathrm{Br}(\mathcal{X}) & \longrightarrow & \mathrm{Br}(\mathcal{O}_v) \\ \downarrow & & \downarrow \\ \mathrm{Br}(X) & \xrightarrow{\mathrm{ev}_{x_v}} & \mathrm{Br}(K_v) \end{array}$$

where the map $\mathrm{Br}(\mathcal{X}) \to \mathrm{Br}(\mathcal{O}_v)$ is obtained by applying the functor Br to the map $x_v : \mathcal{O}_v \to \mathcal{X}$. By Corollary 4.4 the group $\mathrm{Br}(\mathcal{O}_v)$ is trivial, so we have $A(x_v) = 0$ for all $v \notin S$. □

Let now $A \in \mathrm{Br}(X)$. Thanks to the Lemma above, we can extend the exact sequence of Theorem 3.44 to a commutative diagram

$$\begin{array}{ccccccccc} & & X(K) & \hookrightarrow & X(\mathbf{A}_K) & & & & \\ & & \downarrow{\scriptstyle A(-)} & & \downarrow & & & & \\ 0 & \longrightarrow & \mathrm{Br}(K) & \longrightarrow & \bigoplus_v \mathrm{Br}(K_v) & \xrightarrow{\sum_v \mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

and we can give the following definition.

Definition 4.12. For $A \in \mathrm{Br}(X)$ we define

$$X(\mathbf{A}_K)^A := \left\{ (x_v) \in X(\mathbf{A}_K) \mid \sum_v \mathrm{inv}_v\, A(x_v) = 0 \right\}$$

and

$$X(\mathbf{A}_K)^{\mathrm{Br}} := \bigcap_{A \in \mathrm{Br}(X)} X(\mathbf{A}_K)^A.$$

The set $X(\mathbf{A}_K)^{\mathrm{Br}}$ is called the *Brauer set* of X. If S is a finite set of places of K, we also define $X(\mathbf{A}_K^S)^{\mathrm{Br}}$ (see Section 2.3.1) to be the image of $X(\mathbf{A}_K)^{\mathrm{Br}}$ under the projection map $X(\mathbf{A}_K) \to X(\mathbf{A}_K^S)$.

By Theorem 3.44, we have $X(K) \subset X(\mathbf{A}_K)^{\mathrm{Br}}$. Thus, if we have $X(\mathbf{A}_K) \neq \emptyset$ but $X(\mathbf{A}_K)^{\mathrm{Br}} = \emptyset$ and so $X(K) = \emptyset$, we say that **there is a Brauer-Manin obstruction to the existence of rational points of** X.

Thanks to the following results, the Brauer group can also be used to determine the failure of Strong Approximation for X.

Proposition 4.13. *Let K_v be a local field, X a variety over K_v and $A \in \mathrm{Br}(X)$. Then the map $A(-) : \mathrm{Br}(X) \to \mathrm{Br}(K_v)$ is locally constant.*

Proof. See [25], Proposition 8.2.9. □

Corollary 4.14. *Let X be a variety over K and $A \in \mathrm{Br}(X)$. Then the sets $X(\mathbf{A}_K)^A$ and $X(\mathbf{A}_K)^{\mathrm{Br}}$ are closed in $X(\mathbf{A}_K)$.*

Since, as we said, we have $X(K) \subset X(\mathbf{A}_K)^{\mathrm{Br}}$, we see that the closure $\overline{X(K)}$ of the set of rational points is contained in $X(\mathbf{A}_K)^{\mathrm{Br}}$. Thus, if $X(\mathbf{A}_K)^{\mathrm{Br}} \neq X(\mathbf{A}_K)$ Strong Approximation fails for X, and we say that **there is a Brauer-Manin obstruction to Strong Approximation on** X. Similarly, if $X(\mathbf{A}_K^S)^{\mathrm{Br}} \neq X(\mathbf{A}_K^S)$ we say that there is a Brauer-Manin obstruction to Strong Approximation away from S.

Remark 4.15. In general, it is of course possible that there is no Brauer-Manin obstruction (to the existence of rational points or to Weak/Strong Approximation), but that the local-global principle still fails.

There are however other kinds of obstructions, finer the the Brauer-Manin one, that can explain the failure of the local-global principle. See for example [25], Chapter 8.

Chapter 5

The Case of Quadric Surfaces

We are finally ready to approach the core of this thesis: describing the failure of Strong Approximation away from infinity on punctured affine cones over quadric surfaces.

We will follow very closely the article [3] by Bright and Kok, and generalize the result to projective quadrics over number fields. In fact, one could argue that there is actually nothing new in this chapter that wasn't already proved in [3].

After a general description of the Brauer-Manin obstruction mentioned above, we deduce the result of [3] as a particular case. With this method, we can also explain an example found by Lindqvist in [16].

5.1 Failure of Strong Approximation on Affine Cones

For this section, we let K be a number field with ring of integers $\mathcal{O}$. As usual, we will denote by Ω_K the set of all normalized valuations of K. For $v \in \Omega_K$, we let K_v be the completion of K with respect to v. If v is non-Archimedean, we let $\mathcal{O}_v$ be the ring of integers of K_v and k_v the residue field.

Let $Y \subset \mathbb{P}^3_K$ be a smooth projective quadric surface, defined by the equation

$$F(X_0, X_1, X_2, X_3) = 0 \tag{5.1}$$

for some homogeneous $F \in \mathcal{O}[X_0, X_1, X_2, X_3]$ of degree 2.

Let $\mathcal{Y} \subset \mathbb{P}^3_{\mathcal{O}}$ be the model for Y described in Example 1.7.

Let X be the *punctured affine cone* over Y, that is the complement of the point $(0,0,0,0)$ in the affine scheme $\operatorname{Spec} K[X_0, X_1, X_2, X_3]/(F)$.

Recall that for any affine scheme $S = \operatorname{Spec} R$, any projective R-scheme V is of the form $\operatorname{Proj} B$ for some graded R-algebra B (see [18], Sections 2.3.3 and 3.3.3). If V is of finite type, we can take $B = R[X_0, \dots, X_n]/I$ for some homogeneous ideal $I \subset R[X_0, \dots, X_n]$. Then the scheme $C(V) = \operatorname{Spec} B \setminus V(B_+)$, where $B_+ = \bigoplus_{d>0} B_d$ is the positive-degree part of B, is called the *punctured affine cone over* V. It is the complement of the R-point $(0,0,0,0)$ in $\operatorname{Spec} B$, and there is a natural projection map $p : C(V) \to V$.

Let $\mathcal{X} \subset \mathbb{P}^3_{\mathcal{O}}$ be the punctured affine cone over $\mathcal{Y}$. Then $\mathcal{X}$ is an $\mathcal{O}$-model for X. By abuse of notation, we denote by π both projection maps $X \to Y$ and $\mathcal{X} \to \mathcal{Y}$; in fact, the former is the restriction of the latter to the generic fibers.

Using the procedure described in Section 2.2.2, we can check whether (5.1) is everywhere locally soluble, that is if $Y(K_v) \neq \emptyset$ for all $v \in \Omega_K$. If it is not, we can conclude immediately that $Y(K) = \emptyset$. So we assume that $Y(K_v) \neq \emptyset$ for all $v \in \Omega_K$. By Theorem 2.4, this implies that $Y(K) \neq \emptyset$, thus in particular $\mathcal{X}(\mathcal{O}) \neq \emptyset$, so we can fix $P \in \mathcal{X}(\mathcal{O})$, which we can write as $P = (P_0, P_1, P_2, P_3) \in \mathcal{O}^4$. This also defines a K-point of X. Let moreover $g_P \in \mathcal{O}[X_0, X_1, X_2, X_3]$ be a linear form defining the tangent hyperplane to X at the point P. Notice that g_P also defines the tangent hyperplane to Y at $\pi(P)$.

Let $\Delta_Y \in K^\times$ be the discriminant of Y (see Section 1.4). In what follows we will be interested in the class of Δ_Y in $K^\times/(K^\times)^2$, which is invariant under linear transformations. Let A_P be the quaternion algebra (Δ_Y, g_P) over the function field $K(X)$ of X. We have the following result.

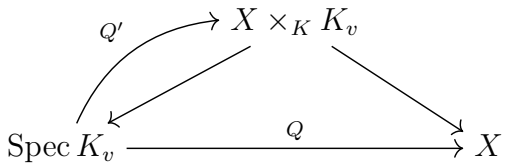
Proposition 5.1. *The class of the quaternion algebra A_P in $\operatorname{Br} K(X)$ belongs to $\operatorname{Br} X$. The quotient group $\operatorname{Br} X/\operatorname{Br} K$ is generated by A_P. It is trivial if and only if Δ_Y is a square in K.*

Proof. See [3], Lemma 3.1. □

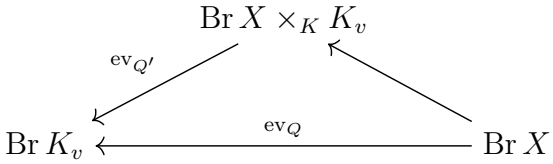
We are now going to evaluate the Hasse invariant of the algebra $A_P(Q)$, for $Q \in X(K_v)$, at the different places v of K. The following simple Lemma will be useful.

Lemma 5.2. *Let v be a place of K and $Q \in X(K_v)$. If Δ_Y is a square in K_v, then $A_P(Q)$ is split over K_v.*

Proof. The point Q is a map of K-schemes $Q : \operatorname{Spec} K_v \to X$. This factors as $Q' : \operatorname{Spec} K_v \to X \times_K K_v$



and passing to the Brauer groups this gives a commutative diagram



and since A_P is split in $\operatorname{Br} X_{K_v} \subset \operatorname{Br} K_v(X)$, we have that $A_P(Q)$ is split. □

5.1.1 Archimedean Places

Let $v \in \Omega_K$ be an Archimedean place of K. If v is complex, that is, if $K_v \cong \mathbb{C}$, then $\operatorname{Br}(K_v) = 0$, so $\operatorname{inv}_v A_P(Q) = 0$ for all $Q \in X(K_v)$, and there is nothing to do.

So assume that v is a real place of K, that is, $K_v \cong \mathbb{R}$. If the image of Δ_Y in K_v is positive, then by Lemma 5.2 we have $\operatorname{inv}_v A_P(Q) = 0$ for every $Q \in X(K_v)$.

If there is at least one real place $v \in \Omega_K$ such that $\Delta_Y < 0$ in K_v, we have the following.

Proposition 5.3. *Assume $v_0 \in \Omega_K$ is Archimedean and such that $K_{v_0} \cong \mathbb{R}$ and $\Delta_Y < 0$ in K_{v_0}. Then the restriction of the projection map $X(\mathbf{A}_K)^{\mathrm{Br}} \to X(\mathbf{A}_K^\infty)$ is surjective. In particular, there is no Brauer-Manin obstruction to Strong Approximation away from infinity on X.*

Proof. Let $Q = (Q_v)_{v\in\Omega_K^\infty} \in X(\mathbf{A}_K^\infty)$ be a finite adelic point of X. Choose also, for every Archimedean place v of K, a point $Q_v \in X(K_v)$. If $\sum_v \mathrm{inv}_v A_P(Q_v) = 0$, then $Q' = (Q_v)_{v\in\Omega_K}$ is in the Brauer set $X(\mathbf{A}_K)^{\mathrm{Br}}$ and maps to $Q \in X(\mathbf{A}_K^\infty)$, so we are done.

Assume then that $\sum_v \mathrm{inv}_v A_P(Q_v) = \frac{1}{2}$, and consider the quaternion algebra $A_P(Q_{v_0}) = (\Delta_Y, g_P(Q_{v_0}))$ over K_{v_0}. Since $\Delta_Y < 0$, this is split if and only if $g_P(Q_{v_0}) > 0$. Notice that $-Q_{v_0} \in X(K_v)$ as well, and that by linearity $g_P(-Q_{v_0}) = -g_P(Q_{v_0})$, so that replacing Q_{v_0} by $-Q_{v_0}$ in $Q' = (Q_v)_{v\in\Omega_K}$ we change the Hasse invariant of $A_P(Q_{v_0})$, thus the sum above becomes zero. As before, $Q' = (Q_v)_{v\in\Omega_K}$ is now in the Brauer set $X(\mathbf{A}_K)^{\mathrm{Br}}$ and maps to $Q \in X(\mathbf{A}_K^\infty)$, so we are done. □

Remark 5.4. If $L \mid K$ is an extension of global fields and φ is a real place of K that extends to a complex, non-real, place ψ of L, some authors say that φ *ramifies* in L. Thus, the Proposition above can be rephrased as "If there is a real place of K that ramifies in L, there is no Brauer-Manin obstruction to Strong Approximation away from infinity on X".

We will see that, also for the finite places of K, ramification plays a key role in determining the Brauer-Manin Obstruction.

5.1.2 Finite Places

We divide the set of finite places v of K into four subsets, according to the behaviour of Y over K_v.

First of all, we let $\mathcal{Q}$ be the set of finite places of K such that Δ_Y is a square in K_v. By Lemma 5.2, if $v \in \mathcal{Q}$ we have $\mathrm{inv}_v A_P(Q) = 0$ for every $Q \in X(K_v)$

Let $\mathcal{R}$ be the set of finite places $v \in \Omega_K \setminus \mathcal{Q}$ that are not in $\mathcal{Q}$ and such that $K_v(\sqrt{\Delta_Y}) \mid K_v$ is ramified. This is a finite set: a prime $\mathfrak{p} \subset \mathcal{O}$ ramifies in $K(\sqrt{\Delta_Y})$ if and only if $\mathfrak{p}$ divides the *discriminant* $\mathfrak{d}$ of the extension, which is an ideal of $\mathcal{O}$ ([23], Theorem II.2.12). We call $\mathcal{R}$ the set of *ramified places*.

Let $\mathcal{B}$ be the set of finite places v, not in $\mathcal{Q}$ or in $\mathcal{R}$, such that either the residue field k_v has characteristic 2, or the reduction of Y modulo v is singular. We will call this the set of *bad places*. The set $\mathcal{B}$ is also finite: for a finite prime v, the quadric $\tilde{Y} = \mathcal{Y} \times_{\mathcal{O}} k_v$ can be singular only if $\Delta_{\tilde{Y}} = (\Delta_Y \mod v) \in k_v$ is zero, which happens only for the finitely many primes v that divide Δ_Y. This fact actually holds in general: if $\mathcal{V}$ is a scheme of finite presentation over an integral scheme S, such that the generic fiber is smooth, then there is an open neighbourhood $U \subset S$ of the generic fiber such that $\mathcal{V} \times_S U$ is smooth. See [25], Theorem 3.2.1.

Finally, let $\mathcal{G}$ be the set of finite places of K that are not in any of the three sets $\mathcal{Q}$, $\mathcal{R}$ or $\mathcal{B}$ defined above. We will call it the set of *good places*.

Before describing the beheaviour of the algebra A_P at the four subsets of places, we note the following fact, that will be useful later.

Remark 5.5. Let v be a finite place of K and assume that $K_v(\sqrt{\Delta_Y}) \mid K_v$ is unramified. By Remark 3.13, every $\lambda \in \mathcal{O}_v^\times$ is the norm of some element in $K_v(\sqrt{\Delta_Y})^\times$. Thus for any $Q \in \mathcal{X}(\mathcal{O}_v)$ and any $\lambda \in \mathcal{O}_v^\times$, by Proposition 3.6(4) we have

$$\operatorname{inv}_v A_P(\lambda Q) = \operatorname{inv}_v(\Delta_Y, \lambda g_P(Q)) = \operatorname{inv}_v A_P(Q) + \operatorname{inv}_v(\Delta_Y, \lambda) = \operatorname{inv}_v A_P(Q).$$

In other words, the fact that $A_P(Q)$ is split or not depends only on the image of Q in $Y(K_v)$.

Assume instead that $K_v(\sqrt{\Delta_Y}) \mid K_v$ is ramified. Then it still holds that

$$\operatorname{inv}_v A_P(\lambda Q) = \operatorname{inv}_v(\Delta_Y, \lambda g_P(Q)) = \operatorname{inv}_v A_P(Q) + \operatorname{inv}_v(\Delta_Y, \lambda)$$

but, since the norm group $N\left(\mathcal{O}^\times_{K(\sqrt{\Delta_Y}),v}\right)$ has index two in $\mathcal{O}_v^\times$, we see that the algebra (Δ_Y, λ) is split over K_v for half of the values of $\lambda \in \mathcal{O}_v^\times$.

More precisely, assume that $\operatorname{char} k_v \neq 2$. Notice that (Δ_Y, λ) is split over K_v if and only if the class $\tilde{\lambda} \in k_v$ of λ is a square in the residue field. In fact, assume $\lambda = a^2 - \Delta_Y b^2$ is a norm from $K_v(\sqrt{\Delta_Y})$. Since the extension is ramified, we have $\Delta_Y = 0$ in k_v, so $\tilde{\lambda} = \tilde{a}^2$ is a square. Conversely, if $\tilde{\lambda}$ is a square in k_v, then λ is a square in K_v by Proposition 3.11.

Geometrically, half of the points of X on the line through Q and the origin split the algebra A_P and half don't.

Ramified Places

Let $v \in \mathcal{R}$ and let $Q \in \mathcal{X}(\mathcal{O}_v)$. By the second Remark 5.5, half of the points Q' on the line through Q and the origin (those that map to $\pi(Q)$ in $Y(K_v)$) are such that the algebra $A_P(Q_v)$ is split. Then we define the subsets

$$U_v^0 := \{Q \in \mathcal{X}(\mathcal{O}_v) \mid \operatorname{inv}_v A_P(Q) = 0\} \quad \text{and} \quad U_v^{\frac{1}{2}} = \{Q \in \mathcal{X}(\mathcal{O}_v) \mid \operatorname{inv}_v A_P(Q) = \tfrac{1}{2}\}.$$

Clearly, in this case both U_v^0 and $U_v^{\frac{1}{2}}$ are open (Proposition 4.13) and not empty, they are disjoint and $\mathcal{X}(\mathcal{O}_v) = U_v^0 \cup U_v^{\frac{1}{2}}$. We will use these sets to show that there is a Brauer-Manin obstruction to Strong Approximation away from infinity.

Remark 5.6. If $K = \mathbb{Q}$, there is alway some finite prime v such that $\mathbb{Q}_v(\sqrt{\Delta_Y}) \mid \mathbb{Q}$ is ramified, thus the set $\mathcal{R}$ is not empty. However, if the class group of K is not trivial, it may happen that the extension $K_v(\sqrt{\Delta_Y}) \mid K_v$ is unramified for all v. See Example 5.12 below for a case with $\mathcal{R} = \emptyset$.

Bad Places

Let $v \in \mathcal{B}$ be one of the bad places. Recall that we assumed that $K_v(\sqrt{\Delta_Y}) \mid K_v$ is unramified for such a v. We define

$$V_v^0 := \{Q \in \mathcal{X}(\mathcal{O}_v) \mid \operatorname{inv}_v A_P(Q) = 0\} \quad \text{and} \quad V_v^{\frac{1}{2}} = \{Q \in \mathcal{X}(\mathcal{O}_v) \mid \operatorname{inv}_v A_P(Q) = \tfrac{1}{2}\}.$$

In general, we can't say much about these sets, except that they are both open and closed in $\mathcal{X}(\mathcal{O}_v)$. Since their union is the whole $\mathcal{X}(\mathcal{O}_v)$, at least one of the two is always going to be non-empty.

By Remark 5.5, we also know that the splitting behaviour of $A_P(Q)$ depends only on the image of Q in $Y(K_v)$. Thus, each of V_v^0 and $V_v^{\frac{1}{2}}$ is the preimage of its projection in $Y(K_v)$.

Good Places

Let $v \in \mathcal{G}$. Recall that, by definition of the set $\mathcal{G}$, the reduction $\tilde{Y} = \mathcal{Y} \times_{\mathcal{O}} k_v$ of Y modulo v is a smooth quadric and that $K_v(\sqrt{\Delta_Y}) \mid K_v$ is unramified.

Following [3], we first prove a Lemma.

Lemma 5.7. *If $Q \in \mathcal{X}(\mathcal{O}_v)$ is such that $\pi(Q) \not\equiv \pi(P) \pmod{v}$, then $\operatorname{inv}_v A_P(Q) = 0$.*

Proof. The proof is taken from [3], Lemma 3.3.

If $g_P(Q) \in \mathcal{O}_v^\times$, then it is a norm from $K_v(\sqrt{\Delta_Y})^\times$, so $\operatorname{inv}_v A_P(Q) = 0$. Suppose then that $g_P(Q) \equiv 0 \pmod{v}$, and let $\tilde{P}, \tilde{Q} \in \tilde{Y}(k_v)$ be the reductions of the points $\pi(P), \pi(Q) \in Y(K_v)$. Notice that the reduction of g_P modulo v defines the tangent plane of $\tilde{Y}$ at $\tilde{P}$. By Proposition 1.12, we have that $\tilde{Y} \cap \{g_P = 0\}$ consists of two lines conjugate over $k_v(\sqrt{\Delta_Y})$, so the only k_v-point at which g_P vanishes is $\tilde{P}$, implying $\pi(Q) \equiv \pi(P) \pmod{v}$, against the assumption. □

At this point, in the example by Bright and Kok, the authors prove that, for any two points $P, P' \in \mathcal{X}(\mathcal{O})$, the two quaternion algebras A_P and $A_{P'}$ lie in the same class in $\operatorname{Br} X$, and not just in $\operatorname{Br} X / \operatorname{Br} K$ ([3], Lemma 3.4). Unfortunately, this is not true in general, as the following example shows.

Example 5.8. Let $Y \subset \mathbb{P}^3_{\mathbb{Q}}$ be the smooth quadric surface defined by the equation

$$X_0^2 + 7X_1^2 = 11X_2^2 + (7 \times 11 \times 3)X_3^2.$$

We can take $\mathcal{Y} \subset \mathbb{P}^3_{\mathbb{Z}}$ to be the projective $\mathbb{Z}$-scheme defined by the equation above. Consider the points $P = (2,1,1,0)$ and $P' = (4,13,5,2)$ in $\mathcal{X}(\mathbb{Z})$, with respective linear forms defining tangent hyperplanes at P and P'

$$\begin{aligned} g_P(X_0, X_1, X_2, X_3) &= 2X_0 + 7X_1 - 11X_2, \\ g_{P'}(X_0, X_1, X_2, X_3) &= 4X_0 + 91X_1 - 55X_2 - (11 \times 7 \times 3 \times 2)X_3^2. \end{aligned}$$

Let moreover $Q \in \mathcal{X}(\mathbb{Z})$ be the point $(1,5,4,0)$. We are going to show that the algebras $A_P(Q)$ and $A_{P'}(Q)$ have different invariants at $v = 2$, so the class of A_P and $A_{P'}$ in $\operatorname{Br} X$ is different.

In fact, we have $A_P(Q) = (3,-7)$ and $A_{P'}(Q) = (3,239)$. Since $-7 \equiv 1 \pmod{8}$ and $-239 \equiv 1 \pmod{8}$ are squares in $\mathbb{Q}_2$, we have that $A_P(Q) = (3,-7) \cong (3,1)$ and $A_{P'}(Q) = (3,239) \cong (3,-1)$ over $\mathbb{Q}_2$. By Example 3.15, we see that $A_P(Q)$ is split, while $A_{P'}(Q)$ is not, and we conclude.

However, any two quaternion algebras of this form are going to give the same local invariant at the good places.

Lemma 5.9. *Let v be a finite place of K that is not in $\mathcal{B}$ or in $\mathcal{R}$. Let $P' \in \mathcal{X}(\mathcal{O})$, let $g_{P'} \in \mathcal{O}[X_0, X_1, X_2, X_3]$ be a linear form defining the tangent hyperplane to X at P' and let $A_{P'} = (\Delta_Y, g_{P'})$ be the associated quaternion algebra. Then we have $\operatorname{inv}_v A_P(Q) = \operatorname{inv}_v A_{P'}(Q)$ for all $Q \in \mathcal{X}(\mathcal{O}_v)$.*

Proof. If $v \in \mathcal{Q}$, this follows from Remark 5.5.

Let then $v \in \mathcal{G}$. By Proposition 1.13 there is $\tilde{Q}$ in the reduction of Y modulo v distinct from the reductions of $\pi(P)$ and $\pi(P')$. Since $v \notin \mathcal{B}$ this point is smooth and by Corollary 2.7 we can lift it to some $Q \in \mathcal{X}(\mathcal{O}_v)$. Then by Lemma 5.7 we have $\operatorname{inv}_v A_P(Q) = 0 = \operatorname{inv}_v A_{P'}(Q)$.

But by Proposition 5.1, the difference $A_P - A_{P'}$ lies in $\operatorname{Br} K$, so it is constant. Therefore $\operatorname{inv}_v A_P(Q) = \operatorname{inv}_v A_{P'}(Q)$ for any $Q \in \mathcal{X}(\mathcal{O}_v)$. □

Corollary 5.10. *For any $v \in \mathcal{G}$ we have $\operatorname{inv}_v A_P(Q) = 0$ for all $Q \in \mathcal{X}(\mathcal{O}_v)$.*

Proof. If $\pi(Q) \not\equiv \pi(P) \pmod{v}$, the conclusion follows from Lemma 5.7, so assume that $\pi(Q) \equiv \pi(P) \pmod{v}$. By Propostion 1.13, the reduction of Y modulo v has a point $\tilde{P}'$ different from the reduction of P. By weak approximation on Y, this point $\tilde{P}'$ lifts to some $P' \in \mathcal{X}(\mathcal{O})$, and we can choose a linear form $g_{P'} \in \mathcal{O}[X_0, X_1, X_2, X_3]$ defining the tangent hyperplane to X at P' and let $A_{P'} = (\Delta_Y, g_{P'})$ be the associated quaternion algebra. Since $\pi(Q) \not\equiv \pi(P') \pmod{v}$, by Lemma 5.7 we have $\operatorname{inv}_v A_{P'}(Q) = 0$, and we conclude using Lemma 5.9. □

5.1.3 The Obstruction

Assume now that $K_v(\Delta_Y) \mid K_v$ is ramified for at least one finite place $v \in \Omega_K^\infty$, so that $\mathcal{R} \neq \emptyset$. Then there exits at least one element

$$\varepsilon = (\varepsilon_v) \in \Pi := \prod_{v \in \mathcal{R}} \frac{\frac{1}{2}\mathbb{Z}}{\mathbb{Z}} \times \prod_{v \in \mathcal{B}} \frac{\frac{1}{2}\mathbb{Z}}{\mathbb{Z}}$$

such that the following conditions are satisfied:

(i) for every $v \in \mathcal{B}$ we have $V_v^{\varepsilon_v} \neq \emptyset$;

(ii) we have $\sum_{v \in \mathcal{R} \cup \mathcal{B}} e_v = \frac{1}{2}$.

We let $E \subset \Pi$ be the set of $\varepsilon \in \Pi$ satisfying the conditions (i) and (ii). Then we can define a set

$$U := \bigcup_{\varepsilon \in E} U^\varepsilon \subset X(\mathbf{A}_K^\infty)$$

where

$$U^{(\varepsilon_v)} := \prod_{v \in \mathcal{Q} \cup \mathcal{G}} \mathcal{X}(\mathcal{O}_v) \times \prod_{v \in \mathcal{R}} U_v^{\varepsilon_v} \times \prod_{v \in \mathcal{B}} V_v^{\varepsilon_v}.$$

Then U is an open subset of $X(\mathbf{A}_K^\infty)$, which is non-empty and does not meet $X(\mathbf{A}_K^\infty)^{\mathrm{Br}}$, proving that there is a Brauer-Manin obstruction to strong approximation away from infinity on X. We have proved the following.

Theorem 5.11. *Let $Y \subset \mathbb{P}^3_K$ be a smooth projective quadric surface over a number field K and let X be the punctured affine cone over Y. Assume that Y has at least one rational point. Assume moreover that Δ_Y is not a square in K and that the extension $K_v(\sqrt{\Delta_Y}) \mid K_v$ is ramified for at least one finite place v of K. Then there is a Brauer-Manin obstruction to Strong Approximation away from infinity on X if and only if Δ_Y is positive in K_v for all the real places v of K.*

Example 5.12. The ramification of the extension $K(\sqrt{\Delta_Y}) \mid K$ is necessary. In fact, we will now give an example where the extension is everywhere unramified, and there is no Brauer-Manin obstruction.

Let $K = \mathbb{Q}(\sqrt{-17})$ and consider the quadric Y given by

$$X_0^2 + X_1^2 + X_2^2 - X_3^2 = 0$$

and let $\mathcal{Y}$ be the projective $\mathcal{O}$-scheme defined by the equation above. Its discriminant is $\Delta_Y = -1$, which is not a square in K, and it can be checked that the extension $K(\sqrt{-1}) \mid K$ is everywhere unramified. It's easy to see that $\mathcal{X}$ has integral points: for example $P = (1,0,0,1)$, $Q = (0,1,0,1)$ and $R = (0,0,1,1)$.

The only prime ideal of K above (2) is $v_2 = (2, 1+\sqrt{-17})$, and we have $v_2 \in \mathcal{Q}$: in fact, 17 is a square in $\mathbb{Q}_2^\times$ (Proposition 3.11), so it is a square in $K_{v_2}^\times$, and we have $-1 = 17/(\sqrt{-17})^2 \in (K_2^\times)^2$. Since $\Delta_Y \in \mathcal{O}^\times$, we have that the reduction of Y modulo any prime of K is a smooth quadric. Then we conclude that $\mathcal{B} = \mathcal{R} = \emptyset$. Following the discussion in the previous section, we see that for any $P \in \mathcal{X}(\mathcal{O})$, any $v \in \Omega_K$ and any $Q \in \mathcal{X}(\mathcal{O}_v)$ we have $\mathrm{inv}_v\, A_P(Q) = 0$. So there is no Brauer-Manin obstruction to Strong Approximation away from infinity on X.

5.2 The Example of Bright and Kok

In [3], Bright and Kok consider the polynomial $F \in \mathbb{Z}[X_0, X_1, X_2, X_3]$ given by

$$F(X_0, X_1, X_2, X_3) = X_0^2 + 47X_1^2 - 103X_2^2 - (17 \times 47 \times 103)X_3^2. \tag{5.2}$$

It can be checked, for example via the procedure descibed in Section 2.2.2, that $Y(\mathbb{Q}_p) \neq \emptyset$ for every prime $p \leq \infty$. Let X and Y be as above. Moreover, we let $\mathcal{Y}$ be the projective $\mathbb{Z}$-scheme defined by 5.2, which is a $\mathbb{Z}$-model for Y, and $\mathcal{X}$ be the punctured affine cone over $\mathcal{Y}$, which is a $\mathbb{Z}$-model for X.

We have $\Delta_Y = 17 > 0$, and clearly $\mathbb{Q}_{17}(\sqrt{17}) \mid \mathbb{Q}_{17}$ is ramified, so by Theorem 5.11 there is a Brauer-Manin obstruction to Strong Approximation away from infinity on the punctured affine cone X.

With the notation introduced above, we have $\mathcal{R} = \{17\}$ and $\{2, 47, 103\} \subset \mathcal{Q}$, so $\mathcal{B} = \emptyset$. Then the subset $U \subset X(\mathbf{A}_K^\infty)$ defining the obstruction is

$$U = \prod_{p \neq 17} \mathcal{X}(\mathbb{Z}_p) \times \left\{ Q \in \mathcal{X}(\mathbb{Z}_{17}) \mid \mathrm{inv}_{17}\, A_P(Q) = \frac{1}{2} \right\}.$$

Note that the only non-smooth points of $\mathcal{X} \times_{\mathbb{Z}} \mathbb{F}_{17}$ are those of the form $(0,0,0,a)$, and that they don't lift to points of $\mathcal{X}(\mathbb{Z}_{17})$, so the points of $\mathcal{X}(\mathbb{F}_{17})$ that lift to $\mathcal{X}(\mathbb{Z}_{17})$ are precisely the smooth ones.

So we can give a very precise description of the obstruction in this case: for every smooth point $\tilde{Q} \in \mathcal{X}(\mathbb{F}_{17})$, exactly half of the scalar multiples of $\tilde{Q}$ lie in the image of U, so they do not lift to coprime integer solutions of (5.2). Notice in fact that if $\tilde{Q}$ is smooth then $g_P(Q) \in \mathbb{Z}_{17}$, and it is a norm from $\mathbb{Q}(\sqrt{17})$ if and only if its reduction modulo 17 is a square in $\mathbb{F}_{17}$ (see Remark 5.5); so $\mathrm{inv}_{17} A_P(Q)$ only depends on the reduction $\tilde{Q}$ of Q modulo 17.

5.3 The Example of Lindqvist

In [16], Lindqvist remarked that certain quadric equations don't have the expected number of primitive integer solutions, if some congruence conditions are imposed. In particular, she considers the following example.

Let p and q be distinct prime numbers congruent to 1 modulo 8. Consider the quadric $Y \subset \mathbb{P}^3_{\mathbb{Q}}$ given by the equation

$$X_0^2 - pqX_1^2 - X_2X_3 = 0 \tag{5.3}$$

and let $Y, X, \mathcal{Y}, \mathcal{X}$ be as above ($\mathcal{Y}$ is the projective $\mathbb{Z}$-scheme defined by 5.3). Notice that $\Delta_Y = pq$.

Let $k \in \mathbb{Z}$ be an integer not divisible by p or q, and assume that k is a square modulo p, but not modulo q. For example, we could take $p = 41$, $q = 17$ and $k = 10$. Consider the point $\tilde{\mathbf{k}} = (k, 0, k, k) \in \mathcal{X}(\mathbb{Z}/pq\mathbb{Z})$. In [16], Lindqvist showed that there is no primitive integer solution of (5.3) congruent to $\tilde{\mathbf{k}}$ modulo pq, i.e. that $\tilde{\mathbf{k}}$ doesn't lift to a point of $\mathcal{X}(\mathbb{Z})$. We are going to explain this as a failure of Strong Approximation on X, using Theorem 5.11.

With our usual notation, we have $\mathcal{R} = \{p, q\}$ and $\mathcal{B} = \emptyset$, because $2, \infty \in \mathcal{Q}$, since $p \equiv q \equiv 1 \pmod 8$ and $pq > 0$.

Consider the point

$$P = (1, 1, 1, 1 - pq) \in \mathcal{X}(\mathbb{Z})$$

and the linear form giving the tangent space at P

$$g_P(X_0, X_1, X_2, X_3) = 2X_0 - 2pqX_1 - (1 - pq)X_2 - X_3$$

that we can use to define our algebra $A_P = (pq, g_P)$.

Consider now any finite adelic point $\alpha = (\alpha_v) \in X(\mathbf{A}^{\infty}_{\mathbb{Q}})$ such that α_p is a lift of the reduction of $\tilde{\mathbf{k}}$ modulo p and α_q is a lift of the reduction of $\tilde{\mathbf{k}}$ modulo q. Then lifting α to an integer point X is equivalent to finding a primitive integer solution to (5.3) congruent to $\tilde{\mathbf{k}}$ modulo pq.

Again $\mathrm{inv}_p A_P(\alpha_p)$ and $\mathrm{inv}_q A_P(\alpha_q)$ only depend on the classes of α_p modulo p and of α_q modulo q respectively. So we only need to compute the invariants at p

and q of

$$\begin{aligned} A_P(\mathbf{k}) =& (pq, 2k - (1-pq)k - k) = (pq, pqk) = \\ =& (q,p)^{\otimes 2} \otimes (p,p) \otimes (q,q) \otimes (pq,k) = (p,p) \otimes (q,q) \otimes (pq,k). \end{aligned}$$

Since $p \equiv q \equiv 1 \pmod 4$, we have that -1 is a square modulo p and modulo q, so $\mathrm{inv}_p(a,a) = \mathrm{inv}_q(a,a) = 0$ for any $a \in \mathbb{Q}^\times$.

On the other hand $\mathrm{inv}_p(pq,k) = 0$ (because k is a square mod p, so it is a square in $\mathbb{Q}_p$) while $\mathrm{inv}_q(pq,k) = \frac{1}{2}$. In fact, if k were a norm form $\mathbb{Q}_q(\sqrt{pq})$, it would be of the form $k = a^2 - pqb^2$ for some integers a, b. But then it would be a square mod q, against our assumption.

We conclude that, for our choice of $\alpha \in \mathcal{X}(\mathbf{A}_{\mathbb{Q}}^{\infty})$, we have $\mathrm{inv}_v A_P(\alpha) = 0$ if and only if $v \neq q$. Thus

$$\sum_v \mathrm{inv}_v A_P(\alpha) = \frac{1}{2}$$

showing that α can't lift to an integer point of X.

Bibliography

[1] F. Andreatta, L. Barbieri-Viale. *Commutative Algebra*. Unpublished lecture notes, 2014.

[2] S. Basu, R. Pollack, M.-F. Roy. *Algorithms in Real Algebraic Geometry*. Springer, 2006.

[3] M. J. Bright, I. Kok. *Failure of Strong Approximation on an Affine Cone*. Preprint, arXiv:1707.04177v2, 2018.

[4] M. J. Bright, D. Testa, R. van Luijk. *Geometry and Arithmetic of Surfaces*. Forthcoming.

[5] J. W. S. Cassels, A, Frölich. *Algebraic Number Theory*. Academic Press, 1967.

[6] B. Conrad. *Weil and Grothendieck Approaches to Adelic Points*. European Mathematical Society Publishing House, Volume 58, 2012.

[7] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, 1994.

[8] D. Eisenbud, J. Harris. *The Geometry of Schemes*. Springer, 2001.

[9] F. G. Frobenius. *Über lineare Substitutionen und bilineare Formen*. Journal für die reine und angewandte Mathematik 84:1–63, 1878.

[10] F. Q. Gouvêa. *p-adic Numbers*. Springer, 2003.

[11] M. J. Greenberg. *Lectures on Forms in Many Variables*. W. A. Benjamin, INC.

[12] D. Harari. *Weak Approximation on Algebraic Varieties*. Arithmetic of Higher-dimensional Algebraic Varieties, p. 43-60, Progress in Mathematics, Vol. 226, 2004.

[13] R. Hartshorne. *Algebraic Geometry*. Springer, 1977.

[14] A. I. Kostrikin, I. R. Shafarevich. *Basic Notions of Algebra*. Springer, 1990.

[15] R. Lidl, H. Niederreiter. *Finite Fields*. Cambridge University Press, 1997.

[16] S. Lindqvist. *Weak Approximation Results for Quadratic Forms in Four Variables*. Preprint, arXiv:1704.00502, 2017.

[17] C.-E. Lind. *Untersuchungen Über di Rationalen Punkte der Ebenen Kubischen Kurven vom Geschlecht Eins*. Thesis, University of Uppsala, 1940, 97.

[18] Q. Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, 2006.

[19] O. Lorscheid, C. Salgado. *Schemes as Functors on Topological Rings*. Preprint, arXiv:1410.1948v2, 2015.

[20] Y. I. Manin. *Le Groupe de Brauer-Grothendieck en Géométrie Diophantienne*. Actes du Congrès International des Mathématiciens, Tome 1, 1971.

[21] J. S. Milne. *Class Field Theory*. Online notes, available at http://www.jmilne.org/math/CourseNotes/cft.html, 2013.

[22] J. S. Milne. *Étale Cohomology*. Princeton University Press, 1980.

[23] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.

[24] J. Neukirch. *Class Field Theory*. Springer, 2013.

[25] B. Poonen. *Rational Points on Varieties*. American Mathematical Society, 2017.

[26] H. Reichardt. *Einige im Kleinen Überall Lösbare, im Grossen Unlösbare Diophantische Gleichungen*. J. Reine Angew. Math., 184, 12-18, 1942.

[27] J.-P. Serre. *A Course in Arithmetic*. Springer, 1973.

[28] J.-P. Serre. *Géométrie Algebrique et Géométrie Analytique*. Annales de l'Institut Fourier, 1956.

[29] J.-P. Serre. *Local Fields*. Springer, 1979.

[30] T. Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge University Press, 2006.

[31] C. A. Weibel. *An Introduction to Homological Algebra*. Cambridge University Press, 1997.