university of groningen / faculty of science and engineering / mathematics and applied mathematics

Brauer groups and the Brauer-Manin obstruction

Bachelor's Project Mathematics

July 2023

Student: M.L. van Hattum

First supervisor: Prof. dr. C. Salgado

Second assessor: Prof. dr. J.S. Müller

Abstract

In this thesis, the ultimate goal is to introduce the Brauer group of a variety and understand how it can be used to detect an obstruction to the Hasse principle. We provide an overview of the fundamental theory, including the necessary background in advanced algebra, algebraic geometry, and number theory. In the central part of this paper, we study the Brauer groups of fields, rings, and varieties, without introducing cohomology. The theory is applied to an example of a surface first considered by Swinnerton-Dyer. We conclude by confirming that for this example, despite the presence of points everywhere locally, there is a Brauer-Manin obstruction to the presence of global points.

Contents

Introduction **4**

1 Preliminaries **5**
1.1 Advanced algebra . . . 5
1.1.1 Module theory . . . 5
1.1.2 Tensor products . . . 7
1.1.3 Algebras over a field . . . 9
1.2 Algebraic geometry . . . 12
1.2.1 Projective varieties . . . 12
1.2.2 The Zariski topology . . . 14
1.2.3 Local rings and function fields . . . 15
1.3 Algebraic number theory . . . 16
1.3.1 Absolute values and valuations . . . 17
1.3.2 Local and global fields . . . 18
1.3.3 More on p-adic numbers . . . 19

2 A closer look at algebras **22**
2.1 Tensor products of algebras . . . 22
2.2 Wedderburn's theorems . . . 26

3 Quaternion algebras **31**
3.1 Definition and properties . . . 31
3.2 Relation to conics . . . 33
3.3 Tensor products of quaternion algebras . . . 34

4 Brauer groups of fields **36**
4.1 Definition of the Brauer group of a field . . . 36
4.2 Examples of Brauer groups of fields . . . 37
4.3 The Hasse invariant map . . . 40

5 Brauer groups of rings **42**
5.1 Azumaya algebras . . . 42
5.2 Definition of the Brauer group of a ring . . . 44

6 Brauer groups of varieties **48**
6.1 Definition of the Brauer group of a variety . . . 48
6.2 The Brauer group of a del Pezzo surface of degree 4 . . . 48

7 The Brauer-Manin obstruction **51**
7.1 The Hasse principle . . . 51
7.2 The Brauer-Manin obstruction . . . 53
7.3 Application to a del Pezzo surface of degree 4 . . . 55

8 Conclusion **60**

References **61**

Introduction

A central topic in arithmetic geometry is the study of solutions to a system of equations such that all coordinates lie in $\mathbb{Q}$. The set of solutions to such a system forms a geometrical object when we consider all solutions over an algebraically closed field. This object is known as an algebraic variety, and the solutions are called points on the variety. The points with all coordinates in $\mathbb{Q}$ are specifically called the $\mathbb{Q}$-rational points of the variety. As an illustrative example, the equation

$$3x^3 + 4y^3 + 5z^3 = 0$$

defines a variety known as Selmer's cubic. The remarkable fact about this elegant equation, as proved by Selmer in 1951 [38], is that it has no $\mathbb{Q}$-rational points (disregarding the zero solution[1]), while it does have $\mathbb{R}$-rational points (points with all coordinates in $\mathbb{R}$) as well as rational points over all other completions of $\mathbb{Q}$: those are the fields $\mathbb{Q}_p$ of p-adic numbers for a prime p.

It turns out to be easier to check if the variety has rational points over each completion of $\mathbb{Q}$, than checking if it has a rational point over $\mathbb{Q}$ itself. Given that $\mathbb{Q}$ is embedded in each completion, the existence of $\mathbb{Q}$-rational points naturally implies the existence of rational points over each completion. It would be useful to know when the converse also holds: that a variety has a $\mathbb{Q}$-rational point if and only if it has a rational point over all its completions. When this is the case, the variety is said to satisfy the *Hasse principle*. Selmer's cubic clearly does not satisfy the Hasse principle, nor do many other varieties. It is natural to wonder whether these varieties observe a shared phenomenon that obstructs the presence of a $\mathbb{Q}$-rational point, despite these varieties having rational points over all completions of $\mathbb{Q}$. Such a phenomenon is referred to as an obstruction to the Hasse principle on the variety.

In 1971, Yuri Manin discovered that for certain varieties, an obstruction to the Hasse principle can be detected using the Brauer group of the variety [26]. This obstruction became known as the Brauer-Manin obstruction. The Brauer group of a field, originally defined by the algebraist Richard Brauer in 1932 [3], is a group consisting of equivalence classes of central simple algebras. This definition was later generalized to the Brauer group of a scheme by Alexander Grothendieck in 1968 [19]. Motivated by our interest in understanding this obstruction to the Hasse principle, the aim of this thesis is to study Brauer groups of fields, rings, and varieties in detail, provide examples, and to apply this knowledge to understand the Brauer-Manin obstruction.

It takes a few pages to show that the definition of the Brauer group of a field is indeed a well-defined group. But once we have worked through the details and considered some examples, we pick up the speed and generalize our definition to the Brauer group of a commutive ring. Using this definition, we then define the Brauer group of a variety, and finish off with a chapter on its application to the Brauer-Manin obstruction. Before we can study Brauer groups, however, we need a foundational understanding of (central simple) algebras, and, specifically, quaternion algebras. In addition, at the beginning of the thesis, a full chapter is dedicated to provide the necessary prerequisites from algebra, algebraic geometry, and number theory.

The reader may notice that the chapter of preliminaries is quite dense, with many new definitions introduced one after the other. However, it is not necessary to memorize each definition before one can read the other chapters. Chapters 2 to 5, so everything up to Brauer groups of rings, can be understood with knowledge of tensor products and algebras, both of which are discussed in the first section of chapter 1. The concepts from algebraic geometry and number theory are only used in a few examples within chapters 3 to 5, which can also be skipped over at first. These concepts really find their application in chapters 6 and 7, so the reader is free to consult the remaining sections of the preliminaries once needed.

[1]The zero solution does not define a $\mathbb{Q}$-rational point, because we look at points in projective space, which requires the point to be nonzero

1 Preliminaries

Throughout this thesis, rings are denoted by R and are assumed to be unitary. Fields are denoted by k and a choice of a fixed algebraic closure by $\overline{k}$.

This chapter covers some preliminary theory from advanced algebra, algebraic geometry, and algebraic number theory. The reader that is already familiar in any of these realms, is free to skip over their respective sections. In any case, it may not be worthwhile to study the preliminaries in detail upfront. Some definitions are never directly used in the rest of the thesis, and are only included for the sake of completion. For example, the definition of a coordinate ring is necessary for defining the local ring of a variety, but only the latter term returns in later chapters. To provide a self-contained paper, both of these definitions are still included. The advise is then to use this chapter merely as a compendium, something one can refer back to when necessary. A quick glance at the first section (Advanced algebra) should be sufficient for reading up until chapter 5.

Most proofs are omitted in this chapter, however, every section lists a few references which the reader can consult for finding these proofs.

1.1 Advanced algebra

1.1.1 Module theory

Prior knowledge of module theory is advised, but all necessary definitions and results are repeated in this section. The theory is extracted from the notes [42], unless indicated otherwise.

Definition 1.1. (Left R-module)
A *left R-module* M is an abelian group $(M, +, 0)$ together with a map

$$R \times M \to M, \quad (a, m) \mapsto a \cdot m$$

satisfying the following conditions for all $a, b \in R$ and $m, n \in M$:

(1) $a \cdot (m + n) = a \cdot m + a \cdot n$;

(2) $(a + b) \cdot m = a \cdot m + b \cdot m$;

(3) $a \cdot (b \cdot m) = (ab) \cdot m$;

(4) $1 \cdot m = m$.

The map $\cdot$ is also called *scalar multiplication* or the *action* of R on M.

Remark 1.2.

(a) Similarly a *right R-module* is defined. If R is commutative, the left and right R-modules coincide. If R is not commutative, an *R-module* is assumed to be a left R-module.

(b) If R is a field, the above definition is precisely that of an R-vector space.

(c) For any ring R, R forms an R-module by defining the scalar multiplication as the usual ring multiplication.

(d) From the axioms we obtain the properties $0 \cdot m = 0$ and $(-a) \cdot m = -(a \cdot m) = a \cdot (-m)$, which we define as $-am$.

Example 1.3.
Let $(M, +, 0)$ be any abelian group. Then M is a $\mathbb{Z}$-module via the map $\mathbb{Z} \times M \to M$ defined by

$$(a, x) \mapsto a \cdot x \coloneqq \begin{cases} x + \cdots + x \ (a \text{ times}) & \text{if } a > 0 \\ 0 & \text{if } a = 0 \\ -((-a)x) & \text{if } a < 0. \end{cases}$$

Definition 1.4. (Submodule)
A *submodule* of a left R-module M is a subgroup N of M closed under the action of R.

Example 1.5.

(a) If k is a field and V a k-vector space, the k-submodules of V are precisely the k-subspaces of V.

(b) The R-submodules of the R-module R are precisely the ideals of R.

Definition 1.6. (Left vector space over a division ring) [36, Page 536]
For a division ring D, a left D-module is also called a *left vector space* over D.

Definition 1.7. (R-module homomorphism)
Let M and N be R-modules. An *R-module homomorphism* is a homomorphism $f \colon M \to N$ of abelian groups which is also R-linear. In other words, for all $r \in R$ and $x, y \in M$, it satisfies

$$f(x + y) = f(x) + f(y) \text{ and } f(r \cdot x) = r \cdot f(x).$$

The notions of *R-module isomorphisms, endomorphisms* and *automorphisms* are defined in the usual way.

Remark 1.8.

(a) The set of R-module homomorphisms $M \to N$ is denoted by $\mathrm{Hom}_R(M, N)$. It is an abelian group with addition defined by $(f+g)(m) \coloneqq f(m)+g(m)$ for $f, g \in \mathrm{Hom}_R(M, N)$, $m \in M$.

(b) The set of R-module endomorphisms on M is denoted by $\mathrm{End}_R(M) \coloneqq \mathrm{Hom}_R(M, M)$. It is a ring with multiplication defined by $(fg)(m) \coloneqq (f \circ g)(m) = f(g(m))$.

(c) If k is a field with k-vector spaces V and W, the k-module homomorphisms $V \to W$ are precisely the k-linear transformations $V \to W$. When $\dim_k(V) = n < \infty$ and $\dim_k(W) = m < \infty$, the linear transformations can be represented by matrices, so we have $\mathrm{Hom}_k(V, W) \cong M_{m \times n}(k)$.

(d) For an R-module homomorphism $f \colon M \to N$, $\ker(f)$ and $\mathrm{im}(f)$ are submodules of M and N respectively.

Definition 1.9. (Quotient module)
Let N be a submodule of an R-module M. The quotient group M/N is an R-module via the map

$$R \times M/N \to M/N, \quad (r, m + N) \mapsto rm + N.$$

It is called the *quotient module*.

Theorem 1.10. (First isomorphism theorem) [36, Thm 7.8]
If $f \colon M \to N$ is a homomorphism of R-modules, then there is an R-isomorphism

$$\begin{aligned} \phi \colon M/\ker(f) &\to \mathrm{im}(f) \\ m + \ker(f) &\mapsto f(m). \end{aligned}$$

Theorem 1.11. (Second isomorphism theorem) [36, Thm 7.9]
If S and T are submodules of an R-module M, then there is an R-isomorphism

$$S/(S \cap T) \cong (S + T)/T.$$

Theorem 1.12. (Third isomorphism theorem) [36, Thm 7.10]
If $T \subseteq S \subseteq M$ is a tower of submodules, then there is an R-isomorphism

$$(M/T)/(S/T) \cong M/S.$$

Definition 1.13. (Direct sum)
Let I be a nonempty set and $\{M_i\}_{i \in I}$ a set of R-modules. The *direct sum* defined as

$$\bigoplus_{i \in I} M_i \coloneqq \{(x_i)_{i \in I} : x_i \in M_i,\ x_i \neq 0 \text{ for finitely many } i \in I\}$$

is an R-module.

Definition 1.14.
Let S be a subset of an R-module M. Then S is called

- *linearly independent* if for all finite sums $\sum_{s \in S} r_s \cdot s$ where $r_s \in R$, the sum being zero implies $r_s = 0$ for all s.
- a *generating set* if $\langle S \rangle \coloneqq \{\text{finite sums } \sum_{s \in S} r_s \cdot s : r_s \in R\} = M$.
- a *basis* if it is a linearly independent generating set.

If M has a basis it is called *free*. It is called *finitely generated* if there exists a finite $S \subset M$ such that $\langle S \rangle = M$. Finally, M is called *cyclic* if $M = \langle \{x\} \rangle = Rx$ for some $x \in M$.

Definition 1.15. (Simple module) [36, Page 431]
A module M is called *simple* if $M \neq \{0\}$ and its only submodules are $\{0\}$ and M.

Proposition 1.16. [36, Cor 7.14]
An R-module M is simple if and only if $M \cong R/I$, where I is a maximal ideal.

Definition 1.17. (Projective module)
An R-module P is called *projective* if for every surjective R-module homomorphism $f \colon M \to N$ and for every R-module homomorphism $h \colon P \to N$, there exists an R-module homomorphism $\tilde{h} : P \to M$ such that $f\tilde{h} = h$.

Proposition 1.18. [42, VII.4.2]
A free R-module is projective.

Proposition 1.19. [36, Page 477]
Let R be a PID and P a projective R-module. Then P is free.

1.1.2 Tensor products

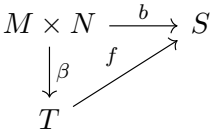
As the group law of Brauer groups turns out to be induced by the tensor product, we recap some basic theory about tensor products that is relevant to our discussion. The definitions and results are taken from the notes [42] and [9], which also contain any proofs.

Throughout this section, R is assumed to be a commutative ring and M, N some R-modules.

Definition 1.20. (Bilinear map)
Let S be an R-module. A map $b\colon M \times N \to S$ is called *bilinear* if for every $m \in M$ and $n \in N$, $b(m,-) \in \mathrm{Hom}_R(N,S)$ and $b(-,n) \in \mathrm{Hom}_R(M,S)$.

Tensor products are defined by their universal property:

Definition 1.21. (Tensor product)
A *tensor product* of M and N is a pair (T,β) where T is an R-module and $\beta\colon M \times N \to T$ a bilinear map, such that for any pair (S,b) of an R-module S and a bilinear map $b\colon M \times N \to S$, there exists a unique map $f \in \mathrm{Hom}_R(T,S)$ such that $b = f \circ \beta$. In other words, the diagram on the right commutes.



Theorem 1.22. (Uniqueness of tensor product) [42, VII.3.4]
If (T,β) and (T',β') are tensor products of M and N, then there exists a unique R-module isomorphism $g\colon T \to T'$ such that $\beta' = g \circ \beta$.

Theorem 1.23. (Existence of tensor product) [42, VII.3.6]
For any R-modules M and N, a tensor product (T,β) exist.

Because a tensor product exists and it is unique, we speak of *the* tensor product of M and N.

Remark 1.24.

(a) The unique tensor product (T,β) for M and N is denoted by $M \otimes_R N$. When the ring R is clear from the context, $\otimes_R$ is often replaced by $\otimes$.

(b) For any $(m,n) \in M \times N$, the element $\beta(m,n) \in T$ is also denoted by $m \otimes n$. These elements $m \otimes n$ are called *elementary tensors*. The elementary tensors generate $M \otimes N$: any element in $M \otimes N$ can be written as an R-linear combination $r_1(m_1 \otimes n_1) + \cdots + r_k(m_k \otimes n_k)$.

Remark 1.25. (Properties of elementary tensors)
As with any bilinear map, $m \otimes n$ satisfies the following properties:

- $(rm) \otimes n = r(m \otimes n) = m \otimes (rn)$ for any $r \in R$;
- $(-m) \otimes n = -(m \otimes n) = m \otimes (-n)$ and $(-m) \otimes (-n) = m \otimes n$;
- $m \otimes 0 = 0$ and $0 \otimes n = 0$;
- $m \otimes n = 0$ does *not* imply $m = 0$ or $n = 0$.

To clarify the last item above, take $\mathbb{Z}$-modules $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Q}$ (both are abelian groups, so they are $\mathbb{Z}$-modules by example 1.3). Since any nonzero $m \in \mathbb{Z}/3\mathbb{Z}$ has order 3, we find, for any nonzero $n \in \mathbb{Q}$,

$$m \otimes n = m \otimes \left(3 \cdot \frac{1}{3} \cdot n\right) = (3 \cdot m) \otimes \left(\frac{1}{3} \cdot n\right) = 0 \otimes \left(\frac{1}{3} \cdot n\right) = 0.$$

Theorem 1.26. [9, Thm 3.3]
If R-modules M and N are spanned by $\{x_i\}_{i\in I}$ and $\{y_j\}_{j\in J}$ respectively, then $M \otimes N$ is spanned by $\{x_i \otimes y_j\}_{(i,j)\in I\times J}$.

Theorem 1.27. [42, VII.3.11]
Let V and W be vector spaces over a field k, with bases $\{e_i\}_{i\in I}$ and $\{f_j\}_{j\in J}$ respectively. Then $V \otimes W$ is a k-vector space with basis $\{e_i \otimes f_j\}_{(i,j)\in I\times J}$.
In particular, if $\dim_k(V) = n < \infty$ and $\dim_k(W) = m < \infty$, we have $\dim_k(V \otimes W) = n \cdot m$.

Theorem 1.28. [9, Thm 4.25]
Let R be a domain and F and F' be free R-modules. If $x \in F$ and $x' \in F'$ are nonzero, then $x \otimes x' \neq 0$ in $F \otimes_R F'$. This holds in particular for vector spaces over a field.

Finally, two properties that we often use without referring to them:

Proposition 1.29. [42, VII.3.7]
For any R-modules M and N, $M \otimes N \cong N \otimes M$.

Proposition 1.30. [42, VII.3.9]
For any R-module M, $R \otimes M \cong M$.

1.1.3 Algebras over a field

In this section we introduce the notion of an algebra over a field. Much like for rings, groups and modules, we can define algebra homomorphisms, the center of an algebra, and when an algebra is simple. The definitions are taken from chapter 18 of the book [35]. Properties of certain algebras are further explored in chapter 2.

Recall that k always denotes a field, unless stated otherwise.

Definition 1.31. (Algebra over a field)
An *(associative) algebra A over k*, also called a *k-algebra*, is a nonempty set A with the operations addition, multiplication and scalar multiplication (denoted by $\cdot$), such that

(A1) A is a vector space over k under addition and scalar multiplication,

(A2) A is a ring with identity under addition and multiplication,

(A3) For all $r \in k$, $a, b \in A$, we have $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$.

An algebra is called *finite dimensional* if it is finite dimensional as a k-vector space.

When the field k is clear from the context, k-algebras are sometimes simply called algebras.

Notice that a k-algebra A is in particular a k-module under scalar multiplication. The k-subspaces of A are therefore precisely the k-submodules of A. But although the ideals of A form the A-submodules of A, they are not necessarily k-submodules of A.

Definition 1.32. (Algebra homomorphism)
Let A and B be k-algebras. A map $f\colon A \to B$ is called a *k-algebra homomorphism* if it is a ring homomorphism and k-linear. So, for all $a, a' \in A$ and $r \in k$, we have

- $f(a + a') = f(a) + f(a')$;
- $f(r \cdot a) = r \cdot f(a)$;
- $f(aa') = f(a)f(a')$;
- $f(1) = 1$.

The notions of *k-algebra isomorphisms, endomorphisms* and *automorphisms* are defined in the usual way.

Since a k-algebra A has both a ring structure and a k-module structure, the above definition of a k-algebra homomorphism makes sense: it is both a ring homomorphism and a k-module homomorphism. This allows us to extend a result from module theory about a set of endomorphisms:

Proposition 1.33.
For a k-algebra A and A-module M, the set $\mathrm{End}_A(M)$ of endomorphisms on M is also a k-algebra.

Proof. By remark 1.8 (b), the set $\mathrm{End}_A(M)$ is a ring with multiplication defined by $f \circ g$. Consider the map

$$\begin{aligned} k \times \mathrm{End}_A(M) &\to \mathrm{End}_A(M) \\ (r, f) &\mapsto r * f \coloneqq (m \mapsto r \cdot m), \end{aligned}$$

where $\cdot$ denotes the scalar multiplication of k on A. This map turns $\mathrm{End}_A(M)$ into a k-module and hence a k-vector space. Using that elements in $\mathrm{End}_A(M)$ are A-linear, one can show

$$r * (f \circ g) = f \circ (r * g) = (r * f) \circ g$$

for any $f, g \in \mathrm{End}_A(M)$ and $r \in k$, which proves that $\mathrm{End}_A(M)$ is a k-algebra. □

To see the relation of module theory and ring theory with the following definition, recall that a module M is called simple if the only submodules of M are $\{0\}$ and M itself, and that a ring R is called simple if its only two-sided ideals are (0) and R. These definitions agree with the same definition for algebras:

Definition 1.34. (Simple algebra)
A k-algebra A is called *simple* if the only two-sided ideals of A are (0) and A.

Definition 1.35. (Division algebra)
A *division algebra* is an algebra that is a division ring.

Since division rings are simple, it follows that division algebras are simple as well.

Definition 1.36. (Center)
Let A be a k-algebra. The *center* of A is defined as

$$Z(A) \coloneqq \{a \in A : ab = ba \ \forall b \in A\}.$$

The image of the k-algebra homomorphism $\phi\colon k \to A,\ x \mapsto x \cdot 1$ is always contained in $Z(A)$: Using property (A3) from definition 1.31, we find

$$(x \cdot 1)b = x \cdot (1b) = x \cdot b = x \cdot (b1) = b(x \cdot 1) \quad \text{for every } b \in A.$$

Definition 1.37. (Central algebra)
A k-algebra A is called *central* if $Z(A) = \{x \cdot 1 : x \in k\}$, that is, the center of A is trivial.

We have thus defined central simple k-algebras: algebras that have no nontrivial two-sided ideals, and whose center contains only the image of k. Such algebras form the elements of the Brauer group of the field k, under an equivalence relation, as we will see in chapter 4. The inverse element of the equivalence class of such an element A will be the equivalence class of the opposite algebra of A:

Definition 1.38. (Opposite algebra)
Let A be a k-algebra. The *opposite algebra* of A denoted by A° is the k-algebra obtained from A by reversing the order of multiplication. That is, $a \cdot b \coloneqq ba$, where the right-hand side is multiplication in A.

Proposition 1.39.
For a central simple algebra A, its opposite algebra A° is central and simple as well.

Proof. We have $Z(A) = Z(A^\circ)$, since the order of multiplication does not affect which elements commute with one another. Moreover, the two-sided ideals of A° are precisely the two-sided ideals of A. To clarify this, note that since the multiplication axb in A is the same as bxa in A°, it follows that if x is a generator of a two-sided ideal in A, then it is also a generator of the same ideal in A°. □

Proposition 1.40. (Matrix algebra)
Let $n \in \mathbb{Z}_{>0}$ be arbitrary. The set $M_n(k)$ consisting of all $n \times n$ matrices over k forms a finite dimensional k-algebra. Moreover, for any finite dimensional k-algebra A, $M_n(A)$ is a finite dimensional k-algebra. We call algebras of this form *matrix algebras.*

Proof. We show the more general statement that $M_n(A)$ is a finite dimensional k algebra for any finite dimensional k-algebra A. $M_n(A)$ receives a k-module structure from the k-module structure on A via the map

$$k \times M_n(A) \to M_n(A), \quad (r, (a_{ij})) \mapsto (r \cdot a_{ij})$$

where $\cdot$ denotes the scalar multiplication of k on A. This turns $M_n(A)$ into a vector space over k with finite basis $\{a_l E_{ij}\}$ where $\{a_l\}$ is a basis for A and E_{ij} denotes the elementary matrix with a 1 in the (i,j)th position. Checking that it is a ring with ordinary matrix multiplication is straightforward, using that A is a ring itself. Lastly, one can show $r \cdot (MN) = (r \cdot M)N = M(r \cdot N)$ for any $r \in k$ and $M, N \in M_n(A)$ using that A satisfies condition (A3) from definition 1.31 as well. □

A more interesting result is the following:

Proposition 1.41.
For any central simple algebra A, its matrix algebra $M_n(A)$ is central and simple as well.

Proof. We first show $Z(M_n(A)) \cong Z(A)$. Take any matrix $M \in Z(M_n(A))$. Since M has to satisfy

$$\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ m_{i,1} & \cdots & m_{i,n} \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix} = E_{ii}M = ME_{ii} = \begin{bmatrix} 0 & \cdots & m_{1,i} & \cdots & 0 \\ & & & & \\ \vdots & & \vdots & & \vdots \\ & & & & \\ 0 & \cdots & m_{n,i} & \cdots & 0 \end{bmatrix}$$

for all $1 \leq i \leq n$, M is diagonal. One can also check that the condition $E_{ij}M = ME_{ij}$ for all i and j implies that all diagonal entries have to be equal. So $M = aI$ for some $a \in A$, where I denotes the identity matrix. But since M has to satisfy $baI = (bI)M = M(bI) = abI$ for all $b \in A$, we must have $a \in Z(A)$. Conversely, for any $a \in Z(A)$, the matrix aI commutes with all of $M_n(A)$. So $Z(M_n(A)) = \{aI : a \in Z(A)\} \cong Z(A)$. Hence, $M_n(A)$ is central.

To show simplicity, take a nonzero two-sided ideal J of $M_n(A)$. The aim is to show that J contains the identity matrix, after which we conclude $J = M_n(A)$, so $M_n(A)$ is simple.

Take a nonzero matrix $M \in J$, with nonzero entry m_{ij}. Multiplying $E_{ii}ME_{jj}$ yields a matrix with only m_{ij} in entry (i,j) and zeros everywhere else. Denote this matrix by N. N lies in J since J is a two-sided ideal. Multiplying $E_{1i}NE_{j1}$ yields a matrix with m_{ij} in entry $(1,1)$ (and zeros everywhere else). Similarly, for any $1 \leq k \leq n$, multiplying $E_{ki}NE_{jk}$ puts m_{ij} in entry (k,k). Since J is a two-sided ideal, we have that $\sum_k E_{ki}NE_{jk} \in J$. This diagonal matrix with m_{ij} on the diagonal we call D. Since A is simple, the two-sided ideal $(m_{ij}) = \{\sum xm_{ij}y : x, y \in A\}$ in A equals A. So there exist elements $\{x_r\}$ and $\{y_s\}$ in A such that $\sum_{r,s} x_r m_{ij} y_s = 1$. Then $\sum_{r,s}(x_rI)D(y_sI)$ is also an element of J and it equals I. □

1.2 Algebraic geometry

The field of algebraic geometry is vast, and any summary of its foundations cannot truly do it justice. The reader that is interested in learning some of the fundamentals is encouraged to look into the notes of Gathmann [16]. This section is also based on these notes, but only defines what is necessary for the purposes of this thesis.

Note, however, that Gathmann's notes only define varieties (and all subsequent definitions) over an algebraically closed field. Since this thesis works out an example of a variety over $\mathbb{Q}$, we require the definitions to be extended to any field. These more general definitions can be recognized from the addition *over* k, where k denotes any field, not necessarily algebraically closed. They are taken from [4, Chapter 3] and adapted to our setting.

1.2.1 Projective varieties

A projective variety is essentially the set of solutions in projective space to a system of homogeneous polynomials considered over an algebraically closed field. There is also the definition of an affine variety, for which the solutions are considered in affine space and the polynomials do not need to be homogeneous. The examples discussed in this thesis only involve projective varieties, so we introduce the following theory in terms of projective varieties and disregard the affine case. However, it should be noted that most of these statements can be adapted to hold for affine varieties as well. In chapter 6, we define the Brauer group of varieties, regardless of whether they are affine or projective. But also in that chapter, we only work with examples of projective varieties.

Recall that k denotes a field and $\overline{k}$ a choice of a fixed algebraic closure of k. We begin by defining projective space:

Definition 1.42. (Projective space)
The set of 1-dimensional linear subspaces of the vector space k^{n+1} is called the *projective n-space* over k and is denoted by $\mathbb{P}^n_k$, or $\mathbb{P}^n$ if the field is clear from the context.

Notation 1.43. (Homogeneous coordinates)
Since a 1-dimensional linear subspace of k^{n+1} is uniquely determined by a nonzero vector in k^{n+1} up to scalar multiplication, we can equivalently define $\mathbb{P}^n$ as the space $k^{n+1} \setminus \{0\}$ modulo an equivalence relation $\sim$ defined as

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \quad \iff \quad x_i = \lambda y_i \text{ for some } \lambda \in k^\times \text{ for all } i.$$

So the convention is to see $\mathbb{P}^n$ as the set containing equivalence classes of $(x_0, \ldots, x_n) \in k^n$. Such an equivalence class is denoted by $(x_0 : \ldots : x_n)$. The x_i are called the *homogeneous coordinates* of the point $(x_0 : \ldots : x_n) \in \mathbb{P}^n$.

For the cases $n = 1$ and $n = 2$, $\mathbb{P}^1$ is also called the *projective line* and $\mathbb{P}^2$ the *projective plane*.

Definition 1.44. (Homogeneous polynomial)
A polynomial is called *homogeneous* if all its monomials have the same total degree. The *total degree* of a monomial $x_0^{i_0} \cdots x_n^{i_n}$ in $k[x_0, \ldots, x_n]$ is defined as the sum of the exponents of each variable: $i_0 + \cdots + i_n$.

For example, $f(x, y, z) = x^2y^3 + xz^4 + xy^2z^2 \in k[x, y, z]$ is homogeneous because all monomials have total degree 5, but $g(x, y, z) = x^2y^3 + 1$ is not.

Definition 1.45. (Projective variety)
For a subset $S \subset k[x_0, \ldots, x_n]$ of homogeneous polynomials, the set

$$V(S) \coloneqq \{P \in \mathbb{P}^n_{\overline{k}} : f(P) = 0 \text{ for all } f \in S\} \subset \mathbb{P}^n_{\overline{k}}$$

is called the *projective zero locus over k* of S. Subsets of $\mathbb{P}^n_{\overline{k}}$ of this form are called *projective (algebraic) varieties over k*.

Throughout this thesis, all considered varieties are algebraic, so from now on we drop this adjective and simply refer to them as (projective) varieties.

Note that we can also consider a projective variety over k as a variety over $\overline{k}$: the subset $S \subset k[x_0, \ldots, x_n]$ that defines the porjective variety over k, is also a subset of $\overline{k}[x_0, \ldots, x_n]$, and hence defines a variety over $\overline{k}$.

If the field k is itself algebraically closed, there is no need to specify that the variety is defined over k.

Notation 1.46. (Points and rational points)
A projective variety is usually denoted by X. Elements of X are called *points* on X. If we want to specify a subfield $\ell \subset \overline{k}$ over which the points are defined, we often use the notation $X(\ell)$. For a variety $X \subset \mathbb{P}^n_{\overline{k}}$, this denotes the set of points $(a_0 : \ldots : a_n) \in X$ such that $a_i \in \ell$ for all i. These points are also called *ℓ-rational points*.

Definition 1.47. (Ideal of a variety)
For a projective variety $X \subset \mathbb{P}^n_{\overline{k}}$ over k, the set

$$I(X) \coloneqq \langle f \in k[x_0, \ldots, x_n] \text{ homogeneous} : f(P) = 0 \text{ for all } P \in X \rangle \trianglelefteq k[x_0, \ldots, x_n]$$

is called the *ideal of X*.

Definition 1.48. (Coordinate ring)
For a projective variety $X \subset \mathbb{P}^n_{\overline{k}}$ over k, the quotient ring

$$\Gamma(X) \coloneqq k[x_0, \ldots, x_n]/I(X)$$

is called the *(homogeneous) coordinate ring* of X.

Definition 1.49. (Projective subvariety)
Let X be a projective variety. For a homogeneous ideal $J \trianglelefteq \Gamma(X)$, the set

$$V(J) \coloneqq \{P \in X : f(P) = 0 \text{ for all homogeneous } f \in J\} \subset X$$

is called the *zero locus* of J. Subsets of X of this form are called *projective subvarieties* of X.

1.2.2 The Zariski topology

For a projective variety X, defining closed sets to be its subvarieties gives a topology on X:

Definition 1.50. (Zariski topology)
Let X be a projective variety over k. The topology on X whose closed sets are the projective subvarieties of X is called the *k-Zariski topology*. If k is algebraically closed, it is simply called the *Zariski topology*.

With this definition of closed sets in place, we can define notions like irreducibility and dimension.

Definition 1.51. (Reducible/Irreducible variety)
Let X be a projective variety over k. If X can be written as $X = X_1 \cup X_2$ for closed subsets (in the k-Zariski topology) $X_1, X_2 \subsetneq X$, then X is called *reducible over k*. Otherwise it is called *irreducible over k*. If k is algebraically closed, we simply say X is reducible/irreducible.

Definition 1.52. (Geometrically irreducible)
A projective variety X over k is called *geometrically irreducible* if X is irreducible over k, and X considered as a variety over $\overline{k}$ is irreducible.

Proposition 1.53. (Irreducible decomposition) [16, Prop 2.14]
A projective variety X can be written as a finite union $X = X_1 \cup \cdots \cup X_r$ of nonempty irreducible subvarieties. If one assumes $X_i \not\subset X_j$ for all $i \neq j$, then the X_i are unique up to permutation and called the *irreducible components* of X.

Definition 1.54. (Dimension, codimension and pure dimension)
Let X be a nonempty projective variety.

- The supremum over all $n \in \mathbb{N}$ such that there is a chain

  $$\emptyset \neq Y_0 \subsetneq \cdots \subsetneq Y_n \subset X$$

  of length n of irreducible closed subsets of X, is called the *dimension* of X and is denoted by $\dim(X)$.

- For a nonempty irreducible closed subset $Y \subset X$, the supremum over all $n \in \mathbb{N}$ such that there is a chain

  $$Y \subset Y_0 \subsetneq \cdots \subsetneq Y_n \subset X$$

  of length n of irreducible closed subsets of X containing Y, is called the *codimension* of Y in X and is denoted by $\operatorname{codim}_X Y$.

- If every irreducible component of X has dimension n, X is said to be of *pure dimension n*.

Definition 1.55. (Curve, surface, hypersurface)
A projective variety is called

- a *curve* if it is of pure dimension 1;
- a *surface* if it is of pure dimension 2;
- a *hypersurface* in a pure-dimensional projective variety Y if it is a projective subvariety of Y of pure dimension $\dim(Y) - 1$.

Proposition 1.56. [16, Rmk 6.33]
For a projective hypersurface X, its ideal is principal. So $I(X) = \langle f \rangle$ for some $f \in k[x_0, \ldots, x_n]$.

Definition 1.57. (Degree of a hypersurface)
Let X be a projective hypersurface with ideal $I(X) = \langle f \rangle$. Then the *degree* of X is defined as the degree of f and denoted by $\deg(X)$. If X has degree 1,2 or 3, it is called a *linear*, *quadric* or *cubic* hypersurface, respectively.

Definition 1.58. (Conic)
A quadric curve is also called a *conic*.

1.2.3 Local rings and function fields

As will be explained in chapter 6, the Brauer group of a variety is closely related to the Brauer group of its function field and the Brauer group of certain local rings. We first define local rings:

Definition 1.59. (Local ring and residue field) [40, Tag 07BI]
A *local ring* is a ring R with exactly one maximal ideal $\mathfrak{m}$. The quotient ring $R/\mathfrak{m}$ is called its *residue field*.

Definition 1.60. (Local ring of a variety at a point)
Let X be a projective variety and P be a point on X. The ring

$$\mathcal{O}_{X,P} \coloneqq \left\{ \frac{f}{g} : f, g \in \Gamma(X) \text{ with } g(P) \neq 0 \right\}$$

is a local ring with unique maximal ideal

$$I_P \coloneqq \left\{ \frac{f}{g} : f, g \in \Gamma(X) \text{ with } f(P) = 0 \text{ and } g(P) \neq 0 \right\}.$$

It is called the *local ring of X at P*.

Definition 1.61. (Smoothness) [16, Rmk 10.10 (a)]
Let X be a projective variety and P a point on X. If the dimension of I_P/I_P^2 as a vector space over the residue field $\mathcal{O}_{X,P}/I_P$ equals $\operatorname{codim}_X\{P\}$, we say P is *smooth*. If every point on X is smooth, we call X itself *smooth*.

Definition 1.62. (Function field) [4, Rmk 3.2.15]
Let $X \subset \mathbb{P}^n_k$ be a projective variety over k. The *function field* $\kappa(X)$ of X is the set of quotients of two homogeneous polynomials $F, G \in k[x_0, \ldots, x_n]$ of the same degree, where two quotients F/G and F'/G' represent the same element in $\kappa(X)$ if and only if $FG' - F'G \in I(X)$. The elements of $\kappa(X)$ are called *rational functions* on X.

One useful application of function fields is that it helps to classify projective curves:

Proposition 1.63.
Two smooth projective curves are isomorphic if and only if their function fields are.

Proof. This follows from combining the results [14, Chapter 6, Prop 12] and [14, Chapter 7, Thm 3]. □

Let us finish with an example, combining definitions from the whole section:

Example 1.64. (Del Pezzo surface of degree 4)
Consider the projective variety in $\mathbb{P}^4_{\mathbb{Q}}$ (with coordinates u, v, x, y, z) over $\mathbb{Q}$ defined by the equations

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

This defines a smooth surface [41, Thm 3] which is an example of a so-called *del Pezzo surface of degree 4*. It is the first del Pezzo surface of degree 4 for which it was shown that it violates the Hasse principle, as was done by Birch and Swinnerton-Dyer in 1975 [41, Thm 3]. We revisit this surface in chapters 6 and 7 to prove that it is indeed a counterexample to the Hasse principle, by applying Manin's method, which uses the Brauer group of the surface. To be precise, we show that there is a Brauer-Manin obstruction to the Hasse principle on this surface. These terms are properly defined in chapter 7.

Let us return to the example. Denoting the surface by X, we find its coordinate ring

$$\Gamma(X) = \mathbb{Q}[u, v, x, y, z]/I(X) = \mathbb{Q}[u, v, x, y, z]/\langle uv - x^2 + 5y^2, (u+v)(u+2v) - x^2 + 5x^2 \rangle.$$

And its function field given by

$$\kappa(X) = \left\{ \frac{F}{G} : F, G \in \mathbb{Q}[u, v, x, y, z] \text{ homogeneous and of same degree} \right\} / \sim$$

where $F/G \sim F'/G'$ if and only if $FG' - F'G \in \langle uv - x^2 + 5y^2, (u+v)(u+2v) - x^2 + 5x^2 \rangle$.

1.3 Algebraic number theory

For chapter 7 on the Brauer-Manin obstruction, we need an understanding of local and global fields. Especially of the field of p-adic numbers $\mathbb{Q}_p$, a completion of $\mathbb{Q}$ which is also a local field, so that we can work with such numbers in an example. Before we can introduce the notions of a completion, local fields, and global fields, we first define absolute values and valuations, and what it means for these to be equivalent.

Most theory, but in particular the part on p-adic numbers, is taken from Gouvêa's book [18][2]. Some gaps in the theory for general fields are filled with theory from Neukirch's book on algebraic number theory [32] or Milne's lecture notes [28].

Before we start looking at absolute values and valuations, first two general definitions:

Definition 1.65. (Number field)
An *(algebraic) number field* is a finite extension of $\mathbb{Q}$.

Definition 1.66. (Algebraic integer and ring of integers)
Let k be a number field. An element of k that is a root of a monic polynomial in $\mathbb{Z}[X]$ is called an *algebraic integer* in k. The ring consisting of all algebraic integers in k is called the *ring of integers* of k.

[2] This is a good reference for the reader who wants to learn more about different ways to define p-adic numbers.

1.3.1 Absolute values and valuations

Definition 1.67. (Absolute value)
An *absolute value* on a field k is a function $|\ |\colon k \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in k$

- $|x| = 0$ if and only if $x = 0$;
- $|xy| = |x||y|$;
- $|x + y| \leq |x| + |y|$.

If moreover $|x+y| \leq \max\{|x|, |y|\}$ holds, the absolute value is called *non-archimedean*. Otherwise it is called *archimedean*.

Each field has a trivial absolute value defined by $|x| = 1$ for all $x \neq 0$. Usually we do not consider this one.

Example 1.68. (p-adic absolute value)
On $\mathbb{Q}$ we can define two types of (nontrivial) absolute values:

- The usual absolute value which we denote by $|\ |_\infty$ (and which also extends to $\mathbb{R}$);
- The so-called *p-adic absolute value* for a prime p, defined by $|x|_p \coloneqq p^{-m}$, where m is the unique (possibly negative) integer such that $x = p^m \frac{a}{b}$ where $p \nmid ab$.

Note that $|\ |_\infty$ is archimedean and $|\ |_p$ is non-archimedean for each prime p. For convenience, we refer to ∞ as the *prime at infinity*. This allows us to talk about all absolute values on $\mathbb{Q}$ without making a distincion between the archimedean and the non-archimedean ones. We then also refer to both kinds of absolute values using the short notation $p \leq \infty$.

An absolute value $|\ |$ defines a metric on k given by $d(x, y) = |x - y|$. This turns k into a topological space, which allows us to give the following definition:

Definition 1.69.
Two absolute values on k are called *equivalent* if they define the same topology on k.

An equivalence class of absolute values on k is called a *place* of k [28, Page 111].

Theorem 1.70. (Ostrowski) [33]
Let $|\ |$ be a nontrivial absolute value on $\mathbb{Q}$. Then $|\ |$ is equivalent to either $|\ |_\infty$ or $|\ |_p$ for exactly one prime p.

For a number field k, a place of k coming from a non-archimedean absolute value is called a *finite place*. Otherwise it is called an *infinite place*.

Closely related to absolute values are so-called *valuations*[3] on a field:

Definition 1.71. (Valuation)
A *valuation* on a field k is a function $v\colon k \to \mathbb{R} \cup \{\infty\}$ such that for all $x, y \in k$

- $v(x) = \infty$ if and only if $x = 0$;
- $v(xy) = v(x) + v(y)$;
- $v(x + y) \geq \min\{v(x), v(y)\}$.

[3]Some references (including Neukirch's book) call absolute values *valuations* and valuations *exponential valuations*. However, we prefer to work with the terminology of Gouvêa, as this is more commonly used.

Again, we usually disregard the trivial valuation defined by $v(x) = 0$ for all $x \neq 0$.

Definition 1.72.
Two valuations v_1 and v_2 on k are called *equivalent* if $v_1 = sv_2$ for some real number $s > 0$.

If v is a valuation on a field k, we obtain an absolute value on k defined by $|x|_v = q^{-v(x)}$ for some fixed real number $q > 1$. Conversely, if $|\ |$ is a non-archimedean absolute value on k, setting $v(x) = -\log|x|$ for $x \neq 0$ and $v(0) = \infty$ defines a valuation on k associated to $|\ |$. For a fixed q, if v_1 and v_2 are equivalent valuations on k, the associated absolute values $q^{-v_1(\ )}$ and $q^{-v_2(\ )}$ are equivalent as well [32, Page 120].

Example 1.73. (p-adic valuation)
From the p-adic absolute value, we obtain the *p-adic valuation* on $\mathbb{Q}$: for $x \in \mathbb{Q}$, we define $v_p(x) \coloneqq -\log|x|_p = m$, where m is again the integer such that $x = p^m \frac{a}{b}$ where $p \nmid ab$.

1.3.2 Local and global fields

We first define the notion of a completion of a valued field, which is related to local and global fields in proposition 1.81.

Definition 1.74. (Completion)
For a field k with absolute value $|\ |$, we say a field $\hat{k}$ is a *completion* of k with respect to $|\ |$ if

- there exists an injective homomorphism $k \hookrightarrow \hat{k}$;
- the absolute value $|\ |$ extends to $\hat{k}$;
- L is complete with respect to the extended absolute value;
- k is dense in $\hat{k}$.

Theorem 1.75. [28, Thm 7.23, Rmk 7.24(a)]
For a field k with absolute value $|\ |$, a completion $\hat{k}$ with respect to $|\ |$ exists and it is unique up to unique isomorphism.

For a place v of k, we write k_v for the completion with respect to v. Because there is an inclusion map from the field k to its completion k_v, we can identify k with its image under this map and see it as a subfield of k_v.

Definition 1.76. (Field of p-adic numbers)
For each prime p, the completion of $\mathbb{Q}$ with respect to the p-adic absolute value is called the *field of p-adic numbers* and is denoted by $\mathbb{Q}_p$.

In the next section we define p-adic numbers in a more concrete way.

By Ostrowski's theorem, the completions of $\mathbb{Q}$ are $\mathbb{R}$ (with respect to $|\ |_\infty$) and the p-adic numbers $\mathbb{Q}_p$ for each prime p.

The following result is also known as Ostrowski's theorem, but to avoid confusion, we only refer to the previous version as Ostrwoski's theorem.

Theorem 1.77. [28, Rmk 7.49(a)] [33]
Let k be a field that is complete with respect to an archimedean absolute value. Then k is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ and the absolute value is equivalent to the usual absolute value.

The following proposition helps us to define a local field:

Proposition 1.78. [32, Prop 3.8]
Let $|\ |_v$ be a non-archimedean absolute value on k and v the associated valuation. The subset

$$\mathcal{O} = \{x \in k : |x|_v \leq 1\} = \{x \in k : v(x) \geq 0\}$$

is a local ring with unique maximal ideal

$$\mathfrak{p} = \{x \in k : |x|_v < 1\} = \{x \in k : v(x) > 0\}.$$

We call $\mathcal{O}$ the *valuation ring*, $\mathfrak{p}$ the *valuation ideal*, and the quotient ring $\mathcal{O}/\mathfrak{p}$ the *residue field* of k with respect to $|\ |_v$.

Definition 1.79. (Local field)
A *local field* is a field k which is complete with respect to an absolute value $|\ |$ and whose residue field is finite.

Since $\mathbb{Q}_p$ is complete with respect to the p-adic absolute value and its residue field is finite [18, Cor 4.2.7], it is a local field.

Definition 1.80. (Global field)
A *global field* is a field which falls in one of the two categories:

- Algebraic number fields.
- Function fields in one variable over a finite field, i.e., finite extensions of $\mathbb{F}_q(T)$ for some q.

In this paper we are mainly interested in the first case, so the global fields that are finite extensions of $\mathbb{Q}$.

Proposition 1.81. [32, Page 134]
The completions of a global field are local fields.

So $\mathbb{Q}$ is a global field with corresponding local fields $\mathbb{R}$ and $\mathbb{Q}_p$ for each prime p.

1.3.3 More on p-adic numbers

In order to work with p-adic numbers in an example later, we provide a more hands-on definition of $\mathbb{Q}_p$ that gives an expression of its elements, and that makes it more clear how we can see $\mathbb{Q}$ as a subfield of $\mathbb{Q}_p$.

Throughout this section, let p be a prime number.

For a rational number x, we can write it uniquely as a series

$$x = b_{n_0}p^{n_0} + b_{n_0+1}p^{n_0+1} + \cdots = \sum_{n \geq n_0} b_n p^n$$

where $b_n \in \mathbb{Z}$, $0 \leq b_n \leq p-1$. For example, taking $p = 3$, we can write 25 as $1 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2$. One can find such an expression for any rational number.

Notice that n_0 (which could be negative) denotes the "multiplicity" of p in x: it is the unique integer m such that $x = p^m \frac{a}{b}$ where $p \nmid ab$. Recall that this equals $v_p(x)$. For the expression of 25 in powers of 3 above, we have $n_0 = 0$, and indeed, $v_3(25) = 0$ because 25 is not divisible by 3.

Definition 1.82. (p-adic expansion)
Let $x \in \mathbb{Q}$. We call the series $\sum_{n \geq n_0} b_n p^n$ that represents x the *p-adic expansion* of x.

More generally, we call any series $\sum_{n \geq n_0} b_n p^n$ with $b_n \in \mathbb{Z}$, $0 \leq b_n \leq p-1$, a *p-adic expansion*, regardless of whether it represents an element in $\mathbb{Q}$. For example, the series

$$\sum_{n=0}^{\infty} p^{n^2} = 1 + p^2 + p^4 + \dots$$

is not an element of $\mathbb{Q}$ [18, Page 18], but we still call it a p-adic expansion.

We can define operations such as addition and multiplication of p-adic expansions[4]. This turns the set of all p-adic expansions into a field:

Definition 1.83. (Field of p-adic numbers)
The field of all p-adic expansions, we denote by $\mathbb{Q}_p$. The elements of $\mathbb{Q}_p$ are also called *p-adic numbers*.

Since every $x \in \mathbb{Q}$ has a p-adic expansion, we have an inclusion map:

$$\begin{aligned} \mathbb{Q} &\hookrightarrow \mathbb{Q}_p \\ x &\mapsto \text{the } p\text{-adic expansion of } x. \end{aligned}$$

Remark 1.84.
It may seem strange that we are allowed to sum infinitely many positive powers of p. For example, the 3-adic expansion of -1 is $2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + \dots$ (adding 1 to the series gives 0). Doing this computation in $\mathbb{R}$, it blows up and the series is divergent. However, we choose to look at this series over $\mathbb{Q}_p$, where it does converge and so we can identify it with -1. The reason that the series converges in $\mathbb{Q}_p$ is that $|p^n|_p \to 0$ as $n \to \infty$.

With this definition of $\mathbb{Q}_p$, it is a completion of $\mathbb{Q}$ with respect to $|\ |_p$ [18, Thm 3.2.14], and by theorem 1.75 it is unique up to unique isomorphism.

For our purposes in chapter 7, we want to work with p-adic numbers as a re-scaling of p-adic integers:

Definition 1.85. (p-adic integers)
The ring of *p-adic integers* is defined as the valuation ring of $\mathbb{Q}_p$:

$$\mathbb{Z}_p \coloneqq \{x \in \mathbb{Q}_p : |x|_p \leq 1\} = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}.$$

The maximal ideal of $\mathbb{Z}_p$ (so the valuation ideal of $\mathbb{Q}_p$) is the principal ideal

$$p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\} = \{x \in \mathbb{Q}_p : v_p(x) > 0\}.$$

Furthermore, we define the *p-adic units* as the invertible elements of $\mathbb{Z}_p$:

$$\mathbb{Z}_p^\times \coloneqq \{x \in \mathbb{Q}_p : |x|_p = 1\} = \{x \in \mathbb{Q}_p : v_p(x) = 0\}.$$

Note that via the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, an element $\frac{a}{b} \in \mathbb{Q}$ is in $\mathbb{Z}_p^\times$ if and only if $p \nmid ab$.

[4] For more information on how to find p-adic expansions and how to do arithmetic with them, see [18, Chapter 1]. This provides multiple examples and analogies which lead to a better intuition of p-adic numbers.

Proposition 1.86.
For any $n \geq 1$, we have

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Theorem 1.87. (Hensel's lemma) [20]
Let $F(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial in $\mathbb{Z}_p[x]$. Suppose there exists $a_1 \in \mathbb{Z}_p$ such that

$$F(a_1) \equiv 0 \mod p\mathbb{Z}_p \quad \text{and} \quad F'(a_1) \not\equiv 0 \mod p\mathbb{Z}_p.$$

Then there exists a unique $a \in \mathbb{Z}_p$ such that $a \equiv a_1 \mod p\mathbb{Z}_p$ and $F(a) = 0$.

Just as there is an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ with the image of $\mathbb{Q}$ dense in $\mathbb{Q}_p$, there is an inclusion map $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ under which the image of $\mathbb{Z}$ is dense in $\mathbb{Z}_p$: for any $x \in \mathbb{Z}$, we can map x to its p-adic expansion, which is an element in $\mathbb{Z}_p$. This is easier to see with the following proposition describing the elements of $\mathbb{Z}_p$:

Proposition 1.88. [18, Cor 4.3.3, 4.3.4]
Any $x \in \mathbb{Z}_p$ can be written in a unique way as

$$x = b_0 + b_1p + b_2p^2 + \cdots = \sum_{n\geq 0} b_np^n$$

with $0 \leq b_n \leq p-1$. Similarly, any $x \in \mathbb{Q}_p$ can be written in a unique way as

$$x = b_{n_0}p^{n_0} + b_{n_0+1}p^{n_0+1} + b_{n_0+2}p^{n_0+2} + \cdots = \sum_{n\geq n_0} b_np^n$$

with $0 \leq b_n \leq p-1$ and $n_0 = v_p(x)$ possibly negative.

Remark 1.89.
As a consequence, for any $x \in \mathbb{Q}_p$ there exists a $y \in \mathbb{Z}_p$ and an integer m such that $x = p^m y$. This was meant by re-scaling p-adic integers to obtain p-adic numbers, which will be used in examples in chapter 7.

Note that the proposition above gives an analogy between $\mathbb{Q}_p$ and $\mathbb{R}$, the other completion of $\mathbb{Q}$: Any $x \in \mathbb{R}$ can be written (albeit not in a unique way) as

$$x = b_{n_0}10^{n_0} + b_{n_0-1}10^{n_0-1} + b_{n_0-2}10^{n_0-2} + \ldots.$$

So in $\mathbb{Q}_p$, the rational numbers are essentially written as an expansion with base p, instead of the usual base 10. The only difference is that 10 is not a prime, which means $\mathbb{R}$ has a very different structure (it is an archimedean valued field, after all) than each $\mathbb{Q}_p$. But both kinds of fields complete $\mathbb{Q}$. When we introduce the Hasse principle in chapter 7, it is useful to see $\mathbb{Q}$ as a subfield of $\mathbb{R}$ and each $\mathbb{Q}_p$ in this way.

2 A closer look at algebras

In this chapter we prove several properties for certain types of algebras, in order to have a toolbox ready for the next chapters. We first take a closer look at tensor products of algebras in section 2.1. The statements covered in this section enable us to define the Brauer group of a field in chapter 4. In section 2.2, we turn our attention to division rings and division algebras, and prove two theorems by Wedderburn. These are also applied in chapter 4, namely, to determine the Brauer group of certain classes of fields.

2.1 Tensor products of algebras

We start with a powerful property of matrix algebras that we often use without referring back to.

Proposition 2.1. [12, Lem 4.1]
Let A be a k-algebra and $n, m \in \mathbb{Z}_{>0}$. Then the following hold:

(i) $M_n(A) \cong A \otimes M_n(k)$.

(ii) $M_m(k) \otimes M_n(k) \cong M_{mn}(k)$.

Proof.

(i) We prove this using the universal property of the tensor product. But first, note that the following map is a homomorphism of k-algebras: $\phi\colon M_n(k) \to M_n(A),\ (m_{ij}) \mapsto (m_{ij} \cdot 1)$.

Now consider the map

$$\begin{aligned} \beta\colon A \times M_n(k) &\to M_n(A) \\ (a, M) &\mapsto a\phi(M) \end{aligned}$$

which can be checked to be bilinear over k. Let S be any k-module and $b\colon A \times M_n(k) \to S$ any bilinear map. We then need to show the existence and uniqueness of a map $f \in \mathrm{Hom}_k(M_n(A), S)$ such that $f \circ \beta = b$.
In what follows, let E_{ij} and e_{ij} denote the elementary matrices of $M_n(A)$ and $M_n(k)$ respectively. Then, any $M \in M_n(A)$ and $R \in M_n(k)$ can be written as $M = \sum_{i,j} m_{ij}E_{ij}$ and $R = \sum_{i,j} r_{ij}e_{ij}$ for some unique $m_{ij} \in A$, $r_{ij} \in k$.

For existence, define $f\colon M_n(A) \to S$ by $f(M) = \sum_{i,j} b(m_{ij}, e_{ij})$, which is well-defined by uniqueness of the coefficients m_{ij}. We first prove that f is a k-module homomorphism. For arbitrary $M, N \in M_n(A)$ we have:

$$\begin{aligned} f(M+N) &= f\left(\sum (m_{ij} + n_{ij})E_{ij}\right) = \sum b(m_{ij} + n_{ij}, e_{ij}) \overset{1}{=} \sum b(m_{ij}, e_{ij}) + b(n_{ij}, e_{ij}) \\ &= \sum b(m_{ij}, e_{ij}) + \sum b(n_{ij}, e_{ij}) = f(M) + f(N). \end{aligned}$$

Equality 1 uses that b is bilinear. For arbitrary $r \in k$, $M \in M_n(A)$ we have:

$$\begin{aligned} f(r \cdot M) &= f\left(r \cdot \sum m_{ij}E_{ij}\right) \overset{1}{=} f\left(\sum (r \cdot m_{ij})E_{ij}\right) = \sum b(r \cdot m_{ij}, e_{ij}) \\ &\overset{2}{=} \sum r \cdot b(m_{ij}, e_{ij}) \overset{3}{=} r \cdot \left(\sum b(m_{ij}, e_{ij})\right) = r \cdot f(M). \end{aligned}$$

Equality 1 relies on the k-algebra structure of $M_n(A)$, equality 2 uses bilinearity of b, and equality 3 that S is a k-module.
To show that $f \circ \beta = b$, let $a \in A$ and $R \in M_n(k)$ be arbitrary. We have

$$\phi(R) = \sum_{i,j} (r_{ij} \cdot 1)\phi(e_{ij}) = \sum_{i,j} (r_{ij} \cdot 1)E_{ij}.$$

This gives

$$f(\beta(a,R)) = f(a\phi(R)) = f\left(a\left(\sum r_{ij}\cdot E_{ij}\right)\right) \overset{1}{=} f\left(\sum (r_{ij}\cdot a)E_{ij}\right) = \sum b(r_{ij}\cdot a, e_{ij})$$
$$\overset{2}{=} \sum r_{ij}\cdot b(a,e_{ij}) \overset{3}{=} \sum b(a, r_{ij}e_{ij}) \overset{4}{=} b\left(a, \sum r_{ij}e_{ij}\right) = b(a,R).$$

Here, equality 1 again uses that $M_n(A)$ is a k-algebra. Equality 2, 3 and 4 are by bilinearity of b.

For uniqueness, assuming we have an $f \in \mathrm{Hom}_k(M_n(A), S)$ satisfying $f \circ \beta = b$, then for any $M \in M_n(A)$ we have:

$$f(M) = f\left(\sum m_{ij}E_{ij}\right) = \sum f(m_{ij}E_{ij}) = \sum f(\beta(m_{ij}, E_{ij})) = \sum b(m_{ij}, E_{ij}).$$

This concludes the proof.

(ii) *Based on the proof given in* [12, Lem 4.1]
Let $A \coloneqq M_m(k)$. Then by (i), we have

$$M_m(k) \otimes M_n(k) \cong M_n(M_m(k))$$

which is isomorphic to $M_{nm}(k)$ in the natural sense if we 'remove' the lines that indicate the block matrices.

□

A consequence of (ii) is that for every $m, n \in \mathbb{Z}_{>0}$, we have

$$k \otimes M_{mn}(k) \cong M_{mn}(k) \cong M_m(k) \otimes M_n(k) \tag{1}$$

where the first isomorphism is by proposition 1.30. This property will return later when we define equivalence classes of central simple algebras.

Example 2.2. *We present and work out some details of the statements given in* [12, Page 82]
In this example we look at some properties of the tensor product of k-algebras.

(i) The tensor product of algebras over k is itself a k-algebra:
For k-algebras A and B, their tensor product $A \otimes B$ forms a ring with multiplicative identity $1_A \otimes 1_B$ and multiplication defined by

$$(a_1 \otimes a_2)(b_1 \otimes b_2) \coloneqq a_1b_1 \otimes a_2b_2.$$

Since the tensor product is a k-module and k is a field, it follows that it is a vector space over k. Lastly, it can be checked that $A \otimes B$ satisfies (A3) from definition 1.31 using that A and B satisfy this condition.

(ii) In order to identify another structure on the tensor product, first consider the following two maps:

$$\begin{aligned} i\colon A &\to A \otimes B, & j\colon B &\mapsto A \otimes B \\ a &\mapsto a \otimes 1 & b &\mapsto 1 \otimes b. \end{aligned}$$

It can easily be checked that both maps are k-algebra homomorphisms. Now, $A \otimes B$ can be seen as a (left) B-module via the map j, meaning we define the action of B on $A \otimes B$ as

$$\begin{aligned} &B \times (A \otimes B) \to A \otimes B \\ &(b', a \otimes b) \quad \mapsto b' \cdot (a \otimes b) \coloneqq j(b')(a \otimes b) = (1 \otimes b')(a \otimes b) = a \otimes b'b. \end{aligned}$$

It can be verified that this map indeed turns $A \otimes B$ into a B-module. In a similar fashion, $A \otimes B$ is an A-module via the map i.

(iii) One more observation necessary for following proofs: If a set $\{a_i\}$ in A is linearly independent over k, then the set $\{i(a_i)\}$ is linearly independent in $A \otimes B$ as B-module. To prove this, assume $\sum b_i \cdot i(a_i) = 0$ for some arbitrary $\{b_i\} \subset B$. Let $\{e_\ell\}$ be a k-basis for B and write $b_i = \sum c_{i,\ell} e_\ell$ where $c_{i,\ell} \in k$. We have:

$$\begin{aligned} 0 &= \sum_i b_i \cdot i(a_i) = \sum_i j(b_i) i(a_i) = \sum_i (1 \otimes b_i)(a_i \otimes 1) = \sum_i a_i \otimes b_i \\ &= \sum_i a_i \otimes (\sum_\ell c_{i,\ell} e_\ell) = \sum_i \sum_\ell c_{i,\ell} (a_i \otimes e_\ell) \end{aligned}$$

Since $\{a_i\} \subset A$ and $\{e_\ell\} \subset B$ are both linearly independent over k, $\{a_i \otimes e_\ell\}_{i,\ell} \subset A \otimes B$ is linearly independent over k (this follows from theorem 1.27 when $\{a_i\}$ is extended to a basis of A). This implies $c_{i,\ell} = 0$ for all i and ℓ, so $b_i = 0$ for all i, which proves the statement.

The following two results are necessary to prove proposition 2.5, which states that the tensor product of algebras preserves simplicity and centrality. The proofs of lemma 2.3 and theorem 2.4 align with the proofs given in [12, Lem 3.7] and [12, Thm 3.5 (1.)], respectively. They are slightly modified for completion and contain additional elaboration on some arguments.

Lemma 2.3. [12, Lem 3.7]
Let S be a central simple algebra and A any algebra. If J is a nonzero two-sided ideal of $A \otimes S$, then $J \cap i(A) \neq (0)$.

Proof. Take a nonzero $x \in J$ such that $x = \sum_{i=1}^{l} a_i \otimes s_i$ with l minimal. Note that the set $\{a_i\}$ must be linearly independent over k, for otherwise we could write x as a sum of elementary tensors $a_j \otimes s'_j$ where $\{a_j\}$ is a linearly independent subset of $\{a_i\}$, contradicting the minimality of l. Similarly, $\{s_i\}$ is linearly independent over k. Therefore, $s_1 \neq 0$. By simplicity of S, we then have that the two-sided ideal $(s_1) = Ss_1S = \{\sum x_j s_1 y_j : x_j, y_j \in S\}$ must equal S since it is nonzero. So, there exist $m \in \mathbb{N}$ and $x_j, y_j \in S$ such that $1 = \sum_{j=1}^{m} x_j s_1 y_j$.

Consider $x' = \sum_{j=1}^{m} (1 \otimes x_j) x (1 \otimes y_j)$ which is an element of J since J is a two-sided ideal containing x. We can rewrite it as follows:

$$\begin{aligned} x' &= \sum_{j=1}^{m} (1 \otimes x_j)(\sum_{i=1}^{l} a_i \otimes s_i)(1 \otimes y_j) \\ &= \sum_{j=1}^{m} \sum_{i=1}^{l} a_i \otimes (x_j s_i y_j) \\ &= \sum_{i=1}^{l} a_i \otimes (\sum_{j=1}^{m} x_j s_i y_j) \end{aligned}$$

Defining $s'_i = \sum_{j=1}^{m} x_j s_i y_j \in S$, we have $x' = \sum_{i=1}^{l} a_i \otimes s'_i$. By part (iii) of example 2.2 we know that $\{i(a_i)\} = \{a_i \otimes 1\}$ is linearly independent over S, so since $s'_1 = 1$, we have $x' \neq 0$.
We show that $x' \in i(A)$ to conclude $J \cap i(A) \neq (0)$. First, let $s \in S$ be arbitrary. Then,

$$\begin{aligned} (1 \otimes s)x' - x'(1 \otimes s) &= \sum_{i=1}^{l} a_i \otimes s s'_i - \sum_{i=1}^{l} a_i \otimes s'_i s \\ &= \sum_{i=1}^{l} a_i \otimes (s s'_i - s'_i s). \end{aligned}$$

Since $s_1' = 1$, the first term vanishes, so we get $(1 \otimes s)x' - x'(1 \otimes s) = \sum_{i=2}^{l} a_i \otimes (ss_i' - s_i's)$. This is an element in J since $x' \in J$, so by minimality of l, it has to be zero. Once again using that $\{i(a_i)\}$ is linearly independent over S, $\sum_{i=2}^{l} a_i \otimes (ss_i' - s_i's)$ being zero implies $ss_i' - s_i's = 0$ for all i. Since s was assumed to be arbitrary, this gives $s_i' \in Z(S) = \{x \cdot 1 : x \in k\}$ (since S is assumed to be simple). Writing $s_i' = \overline{s_i} \cdot 1$ for $\overline{s_i} \in k$, we have

$$a_i \otimes s_i' = a_i \otimes (\overline{s_i} \cdot 1) = \overline{s_i}(a_i \otimes 1) = \overline{s_i} \cdot (a_i 1) \otimes 1 = a_i(\overline{s_i} \cdot 1) \otimes 1 = a_i s_i' \otimes 1.$$

Finally, we can rewrite $x' = \sum a_i \otimes s_i'$ as $\sum a_i s_i' \otimes 1 = (\sum a_i s_i') \otimes 1$ which is in $i(A)$. □

Theorem 2.4. [12, Thm 3.5 (1.)]
Let S be a central simple algebra and A any algebra. Then every two-sided ideal of $A \otimes S$ is of the form $I \otimes S$ where I is a two-sided ideal of A. In particular, if A is simple, then $A \otimes S$ is simple.

Proof. Let J be a two-sided ideal of $A \otimes S$ and define $I = \{a \in A : a \otimes 1 \in J\}$. Note that I is then a two-sided ideal of A: for any $a, a' \in A$ and $x \in I$, we have $(x \otimes 1) \in J$, so also $(axa' \otimes 1) = (a \otimes 1)(x \otimes 1)(a' \otimes 1) \in J$, which shows $axa' \in I$.

We want to show $J = I \otimes S$. We already have $J \supseteq I \otimes S$: if $a \otimes s \in I \otimes S$, then $a \otimes 1 \in J$ by definition of I, so also $a \otimes s = (a \otimes 1)(1 \otimes s) \in J$. In what follows we show that $I \otimes S$ is not a proper subset of J.

First, consider the natural map

$$\begin{aligned} A \otimes S &\to (A/I) \otimes S \\ a \otimes s &\mapsto \overline{a} \otimes s. \end{aligned}$$

We show that its kernel equals $I \otimes S$. First note that any element $i \otimes s \in I \otimes S$ is indeed mapped to $\overline{0} \otimes s = 0$. For showing the reverse inclusion, let $\{x_i\}$ be a k-basis for I and extend it to a basis $\{x_i\} \cup \{y_i\}$ for A. Then $\{\overline{y_i}\}$ is a basis for A/I. Now, let $a \otimes s = (\sum a_i x_i + \sum b_j y_j) \otimes s$ be any element in the kernel, so $\overline{a} \otimes s = 0$. By proposition 1.28, then either $s = 0$, which gives us the trivial element in $A \otimes S$, or $\overline{a} = \sum b_j \overline{y_i} = \overline{0}$, in which case $b_j = 0$ for all j. Hence, $a \otimes s \in I \otimes S$.

Since the map is surjective, the homomorphism theorem gives $(A \otimes S)/(I \otimes S) \cong (A/I) \otimes S$. We now look at the natural map

$$\begin{aligned} J \to (A \otimes S)/(I \otimes S) &\cong (A/I) \otimes S \\ a \otimes b &\mapsto \overline{a \otimes b}. \end{aligned}$$

Suppose J would contain $I \otimes S$ properly. Then the above map is nonzero, so the image of J under this map is a nonzero ideal of $(A/I) \otimes S$. Lemma 2.3 then gives $\mathrm{im}(J) \cap i(A/I) \neq (0)$. But this contradicts with our choice of I: if we take a nonzero $\overline{a} \otimes 1 \in i(A/I)$, then $a \notin I$, so $a \otimes 1 \notin J$ and $\overline{a} \otimes 1 \notin \mathrm{im}(J)$. So the intersection is in fact trivial, so this contradiction implies $J = I \otimes S$, which finishes the proof. □

Proposition 2.5.
If A and B are central simple algebras, then $A \otimes B$ is central and simple as well.

Proof. The tensor product $A \otimes B$ being simple follows from the previous theorem. To prove that it is central, we show $Z(A \otimes B) = Z(A) \otimes Z(B)$, using the argument from [40, Tag 0749]. To show $Z(A) \otimes Z(B) \subseteq Z(A \otimes B)$ is straightforward: for any $r \in Z(A)$ and $s \in Z(B)$, $r \otimes s$ commutes with any element $a \otimes b \in A \otimes B$.

For the converse, note that every element in $r \otimes s \in Z(A \otimes B)$ in particular commutes with any $a \otimes 1 \in A \otimes B$. This gives

$$ra \otimes s = (r \otimes s)(a \otimes 1) = (a \otimes 1)(r \otimes s) = ar \otimes s$$

so $(ra - ar) \otimes s = 0$. By proposition 1.28 this implies $ra = ar$, so $Z(A \otimes B) \subseteq Z(A) \otimes B$. Similarly, $Z(A \otimes B) \subseteq A \otimes Z(B)$. Combining this, we find

$$Z(A \otimes B) \subseteq (Z(A) \otimes B) \cap (A \otimes Z(B)) = Z(A) \otimes Z(B).$$

□

Proposition 2.6.
Let A be a finite dimensional central simple algebra with $\dim_k(A) = n$. Then $A \otimes A^\circ \cong M_n(k)$.

Proof. Inspired by the proofs in [12, Cor 1.17] *and* [40, Tag 074I]
Consider the following homomorphism of k-algebras:

$$\begin{aligned} A \otimes A^\circ &\to \mathrm{End}_k(A) \\ a \otimes b &\mapsto (x \mapsto axb) \end{aligned}$$

By proposition 2.5 and recalling proposition 1.39, $A \otimes A^\circ$ is simple. So the kernel of this map is either (0) or $A \otimes A^\circ$. The map is nonzero, so the former must be true, which means the map is injective. Since $\mathrm{End}_k(A) \cong M_n(k)$ we have $\dim(\mathrm{End}_k(A)) = \dim(M_n(k)) = n^2$. This equals the dimension of $A \otimes A^\circ$, so we conclude the map is also surjective, and hence provides an isomorphism between $A \otimes A^\circ$ and $\mathrm{End}_k(A) \cong M_n(k)$. □

2.2 Wedderburn's theorems

In this section, we prove two theorems by Wedderburn. We start with the one known as Wedderburn's little theorem [24], a powerful result that tells us that finite division rings are fields, and which we use on many occasions later on. Wedderburn's main theorem [25] states that any finite dimensional simple k-algebra is isomorphic to the matrix algebra over some division algebra over k. To prove this second theorem, we first shortly look at composition series and the Jordan-Hölder theorem, and prove lemmas by Schur and Rieffel.

Theorem 2.7. (Wedderburn's little theorem) [12, Thm 3.18]
Every finite division ring is commutative.

Proof. We work out in detail the proof given in [22, Page 214, 215]
Let D be a finite division ring and define $F \coloneqq Z(D)$. Then F is a finite field since $Z(D)$ forms a subring of the division ring D and all elements in the center commute. Let $q = |F|$. Since F contains 0 and 1, q is a prime power ≥ 2. Seeing D as a finite vector space over F (note that $F \subset D$ is a finite field extension), denote $n = \dim_F(D)$. Once we show $n = 1$, it follows that D is a field.

For now assume $n > 1$. Note that $D^\times = D \setminus \{0\}$ is a finite group of size $q^n - 1$ with subgroup $Z(D^\times) = Z(D \setminus \{0\}) = F \setminus \{0\} = F^\times$ of size $q - 1$. We determine the *class equation* [36, Page 104] of $D^\times$. The class equation is defined as

$$|D^\times| = |Z(D^\times)| + \sum_a [D^\times : C_{D^\times}(a)]$$

where one a is chosen from each conjugacy class of $D^\times$ that contains more than one element. Let $a \in D^\times$ be a representative of such a non-singleton conjugacy class. Then $a \notin Z(D^\times)$, because otherwise its conjugacy class contains only a. The centralizer $C_{D^\times}(a) = \{g \in D^\times : ga = ag\}$ is a subgroup of $D^\times$. For all $g \in C_{D^\times}(a)$, we have $g^{-1} \in C_{D^\times}(a)$, so comparing definitions we see

$$(C_D(a))^\times = \{g \in C_D(a) : g^{-1} \text{ exists and } g^{-1} \in C_D(a)\} = C_{D^\times}(a).$$

Since $C_D(a)$ is a (proper, since $a \notin Z(D^\times)$) subgroup of D, by Lagrange's theorem, $|C_D(a)| = q^{r_a}$ for some $1 \leq r_a < n$ dividing n. So $|C_{D^\times}(a)| = q^{r_a} - 1$. Then the class equation becomes

$$q^n - 1 = q - 1 + \sum_a \frac{q^n - 1}{q^{r_a} - 1}.$$

We have $x^{r_a} - 1 \mid x^n - 1$ in $\mathbb{Z}[X]$ since $r_a \mid n$. The nth cyclotomic polynomial $\Phi_n(x)$ also divides $x^n - 1$. Since $\Phi_n(x)$ is irreducible, $x^{r_a} - 1 \nmid \Phi_n(x)$, and by definition of $\Phi_n(x)$, $\Phi_n(x) \nmid x^{r_a} - 1$ since $r_a < n$. So we obtain the following factorization in $\mathbb{Z}[x]$:

$$x^n - 1 = \Phi_n(x)(x^{r_a} - 1)h(x) \quad \text{for some } h(x) \in \mathbb{Z}[x].$$

Setting $x = q$ gives $(q^n - 1)/(q^{r_a} - 1) = \Phi_n(q)h(q) \in \mathbb{Z}$, so for each a, $(q^n - 1)/(q^{r_a} - 1)$ is an integer divisible by $\Phi_n(q)$. Then it follows from the class equation that $\Phi_n(q) \mid q - 1$. This implies

$$q - 1 \geq |\Phi_n(q)| = |\prod q - \zeta_n^i| = \prod |q - \zeta_n^i|$$

where the ζ_n^i are the primitive nth roots of unity. But since $n > 1$ and $q \geq 2$, $|q - \zeta_n^i| > q - 1 \geq 1$ for each ζ_n^i, so this is a contradiction. □

Definition 2.8. (Composition series) [11]
Let A be a k-algebra and V an A-module. A *composition series* of V is a finite chain of A-submodules

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

such that each quotient module V_i/V_{i-1} is simple.

Theorem 2.9. (Jordan-Hölder Theorem)
Let A be a k-algebra. Suppose an A-module V has two composition series

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

$$0 = W_0 \subset W_1 \subset \cdots \subset W_m = V.$$

Then $n = m$, and there is a permutation σ of $\{1, \ldots, n\}$ such that $V_i/V_{i-1} \cong W_{\sigma(i)}/W_{\sigma(i)-1}$ for each $i = 1, \ldots, n$.

Proof. A proof can be found in [11, Thm 3.11]. □

Example 2.10. *Inspired by* [11, Ex 3.7 (4)]
Let D be a division algebra over k. In this example we find a composition series for $M_n(D)$. Define the subring

$$I_r = \{(m_{ij}) \in M_n(D) : m_{ij} = 0 \text{ for all } j \neq r\}$$

of $M_n(D)$ for each $1 \leq r \leq n$. We first show that each I_r is a simple left $M_n(D)$-submodule of the module $M_n(D)$.

Observe that each I_r is a left ideal of $M_n(D)$. Also, each I_r does not contain a nonzero proper (left) subideal:
Suppose that $J \subseteq I_r$ is a nonzero left ideal. Then it contains a matrix $M = (m_{ij})$ with at least one $m_{ir} \neq 0$, so since D is a division ring, there exists $m_{ir}^{-1} \in D$. Note that $E_{ir}M = m_{ir}E_{ir}$ since all columns of M are zero except for the rth column. So $E_{ir} = (m_{ir})^{-1}E_{ir}M \in J$ since J is a left ideal. Then also $E_{jr} = E_{ji}E_{ir} \in J$ for any $1 \leq j \leq n$. Since every element of I_r is a D-linear combination of all E_{jr}, we find $I_r \subseteq J$.

So I_r as a left $M_n(D)$-module is simple. Since $M_n(D) = \bigoplus_r I_r$, we have a chain of submodules:

$$0 \subset I_1 \subset I_1 \oplus I_2 \subset \cdots \subset I_1 \oplus \cdots \oplus I_n = M_n(D). \tag{2}$$

By the second isomorphism theorem for modules we have for each quotient module the relation

$$(I_1 \oplus \cdots \oplus I_k)/(I_1 \oplus \cdots \oplus I_{k-1}) \cong I_k/I_k \cap (I_1 \oplus \cdots \oplus I_{k-1}) \cong I_k/\{0\} \cong I_k.$$

So each quotient module is simple, and so, the above chain is a composition series for $M_n(D)$.

In the next example, we determine all simple left submodules of $M_n(D)$, a necessary result for the proof of Wedderburn's theorem.

Example 2.11. *We work out in detail the argument given in* [17, Ex 2.1.4]
Let D be a division algebra over k. In the previous example we showed that each I_r is a simple left $M_n(D)$-submodule of $M_n(D)$. This yielded a composition series (equation (2)) for $M_n(D)$ where each quotient module is isomorphic to one of the I_r. To show that all simple left $M_n(D)$-submodules of the module $M_n(D)$ are isomorphic to some I_r, we apply Jordan-Hölder's theorem to this series and the one we construct below.

Suppose M is a simple left $M_n(D)$-submodule. Then it is isomorphic to a quotient $M_n(D)/\mathfrak{m}$ where $\mathfrak{m}$ is a maximal ideal by proposition 1.16. Take a series of $M_n(D)$ containing $\mathfrak{m}$. By [1, Prop 6.7], this series can be refined (i.e., adding extra submodules in between) to a composition series. Since $\mathfrak{m}$ is maximal, it appears as the largest proper submodule in the refined series:

$$0 \subset \cdots \subset \mathfrak{m} \subset M_n(D).$$

By Jordan-Hölder's theorem, $M \cong M_n(D)/\mathfrak{m} \cong I_r$ for some $1 \leq r \leq n$.

One final example about the matrix algebra over a division algebra:

Example 2.12.
By part (c) of remark 1.8, we have $\mathrm{End}_k(V) \cong M_n(k)$ for a field k and an n-dimensional vector space V over k. Now consider D^n as a left vector space over a division ring D. Then we can also define an isomorphism $\mathrm{End}_D(D^n) \cong M_n(D)$:
For any matrix $A \in M_n(D)$, the map

$$D^n \to D^n,\ v \mapsto (v^T A)^T$$

is D-linear and completely determined by A. Conversely, any map in $\mathrm{End}_D(D^n)$ can be described in this way for a matrix in $M_n(D)$.
The same holds for any left vector space M over D of dimension n.

To prove Wedderburn's main theorem, we require two more lemmas. First, we look at a simplified version of Schur's lemma. The original formulation and proof can be found in [37].

Lemma 2.13. (Schur's Lemma) [17, Lem 2.1.5]
For a simple module M over a k-algebra A, $\mathrm{End}_A(M)$ is a division algebra.

Proof. For any $f \in \mathrm{End}_A(M)$, $\ker(f)$ is either (0) or M since M is simple. So, if f is nonzero, it is injective, in which case it is also surjective since it maps from M to itself. So any nonzero element in $\mathrm{End}_A(M)$ has an inverse, and hence, $\mathrm{End}_A(M)$ is a division algebra. □

Lemma 2.14. (Rieffel) [34]
Let R be a simple ring, let M be any nonzero left ideal in R, and view M as a left R-module. Then R coincides with the *bicommutant* of M. That is, if $R' \coloneqq \mathrm{End}_R(M)$, then $R \cong \mathrm{End}_{R'}(M)$.

Proof. We closely follow the proof presented by Rieffel himself in [34]
Define the natural homomorphism from R to $R'' \coloneqq \mathrm{End}_{R'}(M)$

$$\begin{aligned} L\colon R &\to R'' \\ r &\mapsto L_r\colon m \mapsto rm. \end{aligned}$$

Note that the maps L_r are indeed in R'': for any $f \in \mathrm{End}_R(M)$ and $m \in M$, we have $L_r(f(m)) = r \cdot f(m) = f(rm) = f \circ L_r(m)$.

We show that L is a bijection. Since L maps 1_R to $1_{R''}$ it is a nonzero map, so by simplicity of R, it has trivial kernel and is hence injective.

To prove surjectivity, we first claim that $L(M)$ is a left ideal in R'':
Let $\phi \in R''$, $L_m \in L(M)$ and $x \in M$ be arbitrary. We show $\phi \circ L_m \in L(M)$. Defining $\lambda_x \in \mathrm{End}_R(M)$ to denote right multiplication by x, we have

$$(\phi \circ L_m)(x) = \phi(mx) = \phi(\lambda_x \circ m) = \lambda_x \circ \phi(m) = \phi(m)x$$

using that ϕ is $\mathrm{End}_R(M)$-linear. So $\phi \circ L_m = L_{\phi(m)} \in L(M)$.

Now, since the product ideal MR is a two-sided ideal, by simplicity of R we have $MR = R$. Then $L(R) = L(MR) = L(M)L(R)$. The last equality can be derived using the definition of the product ideal: An arbitrary element $\sum L_{m_i} \circ L_{r_j}$ in $L(M)L(R)$ maps $x \in M$ to

$$(\sum L_{m_i} \circ L_{r_j})(x) = \sum (L_{m_i} \circ L_{r_j})(x) = \sum m_i r_j x$$

so this equals the map $L_{\sum m_i r_j}$ in $L(MR)$.

Using that $L(M)$ is a left ideal in R'', it follows that $L(R)$ is a left ideal in R''. Since $1_{R''} \in L(R)$, we have $L(R) = R$, concluding the proof. □

Theorem 2.15. (Wedderburn's Theorem) [17, Thm 2.1.3]
For a finite dimensional simple k-algebra A, there exists $n \in \mathbb{Z}_{>0}$ and a division algebra D over k, such that $A \cong M_n(D)$. This D is unique up to isomorphism.

Proof. We work out in detail the proof given in [17, Thm 2.1.3]
Since A is a finite dimensional vector space over k, it contains a subspace of dimension 1, which can also be seen as a cyclic k-module. We call this module M. Since M is a nonzero subspace of minimal dimension, and the submodules of A coincide with its subspaces, M is a simple submodule. By Schur's lemma, $D = \mathrm{End}_A(M)$ is a division algebra. M is in particular a left submodule of A and since A is a ring, its submodules coincide with its ideals, so M is also a left ideal of A. This allows us to apply Rieffel's lemma, which gives $A \cong \mathrm{End}_D(M)$.

Now note that M also forms a left D-module via the map

$$\begin{aligned} \mathrm{End}_A(M) \times M &\to M \\ (f, m) &\mapsto f(m). \end{aligned}$$

So we can also view M as a left vector space over D, since D is a division algebra. M being finite dimensional over k, it is also finite dimensional over D. Denoting $n = \dim_D(M)$, we have $\mathrm{End}_D(M) \cong M_n(D)$ as discussed in example 2.12.

To show D is unique up to isomorphism, suppose D' is another division ring such that $A \cong M_m(D')$ for some $m \in \mathbb{Z}_{>0}$. We claim that our submodule M satisfies $D^n \cong M \cong D'^m$. Namely, by example 2.11, M is isomorphic to some $I_r \subset M_n(D)$, which is isomorphic to D^n, and similarly for D'.

Next, using that $A \cong M_n(D)$ we can show $D \cong \mathrm{End}_A(D^n)$:
Let $f \in \mathrm{End}_A(D^n)$ be arbitrary and let $v = (v_1, \ldots, v_n) \in D^n$. Write $w = (w_1, \ldots, w_n) = f(v)$. Since f has to be A-linear, we have $f(Mv) = Mf(v) = Mw$ for any matrix $M \in M_n(D)$. Taking M to be the elementary matrix E_{ii} gives $f(0, \ldots, v_i, \ldots, 0) = (0, \ldots, w_i \ldots, 0)$. Since f is linear, $w_i = \alpha v_i + \beta$ for some $\alpha, \beta \in D$, but since in particular $f(\overline{0}) = \overline{0}$, β must be zero. Hence, $f(v) = (\alpha_1 v_1, \ldots, \alpha_n v_n)$ for some $\alpha_i \in D$. Taking M to be E_{ij} with distinct i and j gives that

$$(0, \ldots, \alpha_j v_j, \ldots, 0) = E_{ij} f(v) = f(E_{ij} v) = (0, \ldots, \alpha_i v_j, \ldots, 0)$$

where the nonzero coordinate is in the ith position. This gives $\alpha_i = \alpha_j$ since D is a division ring. So $f(v) = \alpha v$ and can hence be associated with an element in D. Conversely, for any $\alpha \in D$, the map $v \mapsto \alpha v$ is indeed an element of $\mathrm{End}_A(D^n)$.

Using this result for both D and D', we finally find

$$D \cong \mathrm{End}_A(D^n) \cong \mathrm{End}_A(M) \cong \mathrm{End}_A(D'^m) \cong D'.$$

□

3 Quaternion algebras

3.1 Definition and properties

In this section we study the basics of quaternion algebras, which provide concrete examples of certain elements of Brauer groups, as we will see in the next chapter. The definitions and examples in this chapter are taken from [17, Chapter 1].

Throughout this chapter, k is assumed to be a field of characteristic unequal to 2.

Definition 3.1. (Quaternion algebras)
For $a, b \in k^\times$, the *quaternion algebra* (a, b) is defined as the 4-dimensional k-algebra with basis $1, i, j, ij$ and multiplication according to the rules

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

Given an element $q = x + yi + zj + wij \in (a, b)$ (here, x, y, z, w are in k), we define its *conjugate* by $\overline{q} = x - yi - zj - wij$ and its *norm* by $N(q) = q\overline{q} = x^2 - ay^2 - bz^2 + abw^2 \in k$.

One can check that for any $q_1, q_2 \in (a, b)$ we have $N(q_1 q_2) = N(q_1)N(q_2)$. With this we can show the following property:

Proposition 3.2. [17, Lem 1.1.3]
An element $q \in (a, b)$ is invertible if and only if $N(q) \neq 0$. It follows that (a, b) is a division algebra if and only if the norm map $N\colon (a, b) \to k$ does not vanish outside of 0.

Proof. For an invertible element q with inverse q^{-1}, we have $N(q)N(q^{-1}) = N(qq^{-1}) = N(1) = 1$, so $N(q) \neq 0$. Conversely, if $N(q) \neq 0$, defining $q^{-1} = \overline{q}/N(q) \in (a, b)$ yields an inverse for q. □

Example 3.3. (Hamilton's quaternions)
If $k = \mathbb{R}$ and $a = b = -1$, we obtain Hamilton's quaternions, which are denoted by $\mathbb{H}$. Since the norm map $N(q) = x^2 + y^2 + z^2 + w^2$ is zero if and only if $q = 0$, $\mathbb{H}$ is a division algebra by the previous result.

An element $q \in (a, b)$ is called a *pure quaternion* if $q^2 \in k$ but $q \notin k$. Such elements are precisely the ones of the form $yi + zj + wij$. So any element $q \in (a, b)$ can be written uniquely as $q_1 + q_2$ with $q_1 \in k$ and q_2 a pure quaternion. With this notation, $\overline{q} = q_1 - q_2$ and $N(q) = q_1^2 - q_2^2$. So conjugation and the norm are independent of the choice of basis [17, Rmk 1.1.4].

Example 3.4. [17, Rmk 1.1.5]
The matrix algebra $M_2(k)$ is a quaternion algebra isomorphic to $(1, b)$. Namely, the matrices

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

form a k-basis for $M_2(k)$ and satisfy $I^2 = \mathrm{Id}$, $J^2 = b\mathrm{Id}$, $IJ = -JI$. So identifying i, j of $(1, b)$ with I, J respectively, yields an isomorphism.

Identifying i with ui and j with vj for any $u, v \in k^\times$ yields another isomorphism of quaternion algebras:

Proposition 3.5. [17, Rmk 1.1.2]
For all $u, v \in k^\times$, $(a, b) \cong (u^2 a, v^2 b)$.

So whenever a or b is divisible by a square in $k^\times$, we can "take the square out".

Corollary 3.6.
For any quaternion algebra (a, b), we have $(a, b) \cong (b, a)$.

Proof. Based on [17, Rmk 1.1.2]
Mapping $i \mapsto abj$ and $j \mapsto abi$ gives an isomorphism $(a, b) \cong (a^2b^3, a^3b^2)$. Taking $u = v = ab$ in the previous proposition yields $(a^2b^3, a^3b^2) \cong (b, a)$. □

Definition 3.7. (Split)
A quaternion algebra is called *split* if it is isomorphic to $M_2(k)$ as k-algebra.

It is clear from the above definition that all split quaternion algebras are isomorphic. Over the field $\mathbb{R}$, the non-split quaternion algebras are also isomorphic, as is explained after proposition 4.15. However, in general this is not true. For example, over the field $\mathbb{Q}$, there are infinitely many non-isomorphic quaternion algebras [7, Page 10].

Proposition 3.8. [17, Prop 1.1.7]
For a quaternion algebra (a, b) the following statements are equivalent:

(1) (a, b) is split;

(2) (a, b) is not a division algebra;

(3) The norm map $N\colon (a, b) \to k^\times$ has a nontrivial zero;

(4) The element b is a norm from the field extension $k(\sqrt{a})/k$.

Proof. We work out in detail the proof given in [17, Prop 1.1.7]
From (1) to (2) is clear as there are nonsingular matrices in $M_2(k)$. From (2) to (3) is part of lemma 3.2.

For showing (3) to (4), recall that the norm map $k(\sqrt{a}) \to k$ is given by $x + y\sqrt{a} \mapsto x^2 - ay^2$. Denoting this map by $N_{k(\sqrt{a})}$ we have to show $b \in \operatorname{im}\left(N_{k(\sqrt{a})}\right)$.

In the case that $a = \alpha^2$ is a square in k, we can take $x = (b+1)/2$ and $y = (1-b)/2\alpha$ such that

$$N_{k(\sqrt{a})}(x + y\sqrt{a}) = x^2 - ay^2 = (x + \alpha y)(x - \alpha y) = 1b = b.$$

Assuming a is not a square, take a nonzero $q = x + yi + zj + wij \in (a, b)$ with zero norm. Then, $0 = N(q) = x^2 - ay^2 - bz^2 + abw^2$ gives $(z^2 - aw^2)b = x^2 - ay^2$, so

$$N_{k(\sqrt{a})}(z + w\sqrt{a})b = N_{k(\sqrt{a})}(x + y\sqrt{a}).$$

Note that $N_{k(\sqrt{a})}(z + w\sqrt{a}) = z^2 - aw^2 \neq 0$, for otherwise a is a square: if $w \neq 0$ we have $a = (z/w)^2$; if $w = 0$ then $z = 0$ so $y \neq 0$ (otherwise $N(q) = x^2 \neq 0$) which gives $a = (x/y)^2$.

So since $N_{k(\sqrt{a})}(z + w\sqrt{a}) \neq 0$ we find

$$b = \frac{N_{k(\sqrt{a})}(x + y\sqrt{a})}{N_{k(\sqrt{a})}(z + w\sqrt{a})} = N_{k(\sqrt{a})}(x + y\sqrt{a}) \cdot N_{k(\sqrt{a})}((z + w\sqrt{a})^{-1})$$

which is a norm by multiplicativity of $N_{k(\sqrt{a})}$.

To show (1) from (4), in the case that a is a square we have $(a,b) \cong (1,b)$ by proposition 3.5, and hence $(a,b) \cong M_2(k)$ by example 3.4. Assuming a is not a square, we have the norm map $N_{k(\sqrt{a})}$ as defined above. If $b \in \text{im}\left(N_{k(\sqrt{a})}\right)$, then so is b^{-1}, so we can find $r,s \in k$ such that $b^{-1} = r^2 - as^2$. Defining $u = rj + sij$ and $v = (1+a)i + (1-a)ui$ we find

$$u^2 = r^2j^2 + rs(-ij^2 + ij^2) + s^2(ij)^2 = r^2b - abs^2 = b(r^2 - as^2) = bb^{-1} = 1,$$

$$ui = rji + siji = -rij - si^2j = -iu,$$

$$uv = (1+a)ui + (1-a)u^2i = -(1+a)iu + (1-a)i = -vu,$$

$$v^2 = (1+a)^2i^2 + (1+a)(1-a)(-ui^2 + ui^2) + (1-a)^2(ui)^2 = (1+a)^2a - (1-a)^2a = 4a^2.$$

So mapping $i \mapsto u$, $j \mapsto v$, gives an isomorphism $(a,b) \cong (1,4a^2)$, after which example 3.4 yields the isomorphism with $M_2(k)$. □

With this we can prove a nice property of quaternion algebras relevant to our discussion of Brauer groups.

Proposition 3.9.
A quaternion algebra (a,b) is central and simple, and its opposite algebra is equal to itself.

Proof. In the case that (a,b) is split, it is clearly central and simple by example 1.41. If it is not split, it is a division algebra by the previous result, so it is simple as well.

We show that any quaternion algebra (a,b) is central:
Let $x + yi + zj + wij \in Z((a,b))$. Then $(x + yi + zj + wij)i = i(x + yi + zj + wij)$ implies $zji + wiji = zij + wi^2j$. Rewriting gives $2waj + 2zij = 0$ and since $\{1,i,j,ij\}$ is a k-basis, we must have $z = w = 0$. Similarly, $(x + yi + zj + wij)j = j(x + yi + zj + wij)$ gives $y = 0$. So $Z((a,b)) \subseteq k$ and since any element in k commutes with all quaternions, we obtain equality. Hence, (a,b) is central.

Finally, to prove that $(a,b)^\circ \cong (a,b)$, recall that the opposite algebra $(a,b)^\circ$ only differs from (a,b) in the order of multiplication: in $(a,b)^\circ$, the multiplication $i \cdot j$ is defined as the ordinary multiplication ji from (a,b). So $i \cdot j \coloneqq ji = -ij =: -j \cdot i$. Hence, with $\cdot$ as multiplication operator, $(a,b)^\circ$ has the same structure as (a,b). □

Another two interesting results, of which the proofs can be found in [17]:

Proposition 3.10. [17, Prop 1.2.1]
A 4-dimensional division algebra D is isomorphic to a quaternion algebra.

Proposition 3.11. [17, Lem 1.4.4]
If (a,b) is a quaternion algebra and $c \in k^\times$ is a norm from the field extension $k(\sqrt{a})/k$, then $(a,b) \cong (a,bc)$.

3.2 Relation to conics

A nice characterization of quaternion algebras is by its *associated conic*. From this definition the utility of quaternion algebras in algebraic geometry becomes clear when we look at proposition 3.13 and a theorem by Witt.

Definition 3.12. (Associated conic)
For the quaternion algebra (a, b), we define its *associated conic* $C(a, b)$ by the projective plane curve defined by $ax^2 + by^2 = z^2$.

Proposition 3.13. [17, Prop 1.3.2]
The quaternion algebra (a, b) is split if and only if the associated conic $C(a, b)$ has a k-rational point.

Proof. Based on the proof given in [17, Prop 1.3.2]
Suppose $(x_0 : y_0 : z_0)$ is a k-rational point on $C(a, b)$, so $ax_0^2 + by_0^2 = z_0^2$. If $y_0 \neq 0$, this gives $b = (z_0/y_0)^2 - a(x_0/y_0)^2$, so (4) of proposition 3.8 is satisfied, and hence, (a, b) is split. If $y_0 = 0$, then x_0 must be nonzero, so we have $a = (z_0/x_0)^2$ which lies in im $\left(N_{k(\sqrt{b})}\right)$. In this case, (4) is again satisfied by symmetry in a and b.
For the converse direction, if (a, b) is split, (4) of proposition 3.8 guarantees the existence of $r, s \in k$ such that $b = r^2 - as^2$. We conclude that $(s : 1 : r)$ is a k-rational point on $C(a, b)$. □

Note that conics always have a rational point over a degree 2 extension of the field: the conic $ax^2 + by^2 = z^2$ has $(1 : 0 : \sqrt{a})$ as a $k(\sqrt{a})$-rational point. It follows that any quaternion algebra becomes split over a degree 2 extension of the field.

The following theorem was originally proven by Witt in [46].

Theorem 3.14. (Witt) [17, Thm 1.4.2]
Let $Q_1 = (a_1, b_1)$ and $Q_2 = (a_2, b_2)$ be quaternion algebras, and let $C_i = C(a_i, b_i)$ be the associated conics. The algebras Q_1 and Q_2 are isomorphic over k if and only if the function fields $k(C_1)$ and $k(C_2)$ are isomorphic over k.

By proposition 1.63, this theorem gives an equivalence between quaternion algebras and their associated conics. In particular, it tells us that all conics with k-rational points are isomorphic: If C_1 and C_2 are conics with a k-rational point, then their associated quaternion algebras Q_1 and Q_2 are split, so $Q_1 \cong M_2(k) \cong Q_2$. Hence, by Witt's theorem, C_1 and C_2 are isomorphic. Recall that non-split quaternion algebras are not necessarily isomorphic, so this does not hold for conics without a k-rational point.

3.3 Tensor products of quaternion algebras

We present a few statements that are useful for classifying elements of Brauer groups in the next chapter.

Proposition 3.15. [17, Lem 1.5.2]
For any $a, b, b' \in k^\times$ we have

$$(a, b) \otimes (a, b') \cong (a, bb') \otimes M_2(k).$$

Proof. A proof can be found in [17, Lem 1.5.2]. □

Proposition 3.16. [17, Cor 1.5.3]
For a quaternion algebra (a, b) we have $(a, b) \otimes (a, b) \cong M_4(k)$.

Proof. This follows from the previous proposition, together with propositions 3.5 and 2.1, and example 3.4:

$$(a,b) \otimes (a,b) \cong (a,b^2) \otimes M_2(k) \cong (a,1) \otimes M_2(k) \cong M_2(k) \otimes M_2(k) \cong M_4(k).$$

□

We say that a finite dimensional division algebra D over a field k has *period 2* when there exists an $n \in \mathbb{Z}_{>0}$ such that $D \otimes D \cong M_n(k)$. The previous result shows quaternion algebras satisfy this definition. For central division algebras of period 2, the following theorem by Merkurjev [27] relates them to quaternion algebras. We will see in the next chapter that this provides a classification of the order 2 elements of a Brauer group.

Theorem 3.17. (Merkurjev) [17, Thm 1.5.8]
Let D be a central division algebra of period 2 over a field k. There exist positive integers m_1, m_2, n and quaternion algberas $Q_1, \ldots, Q_n$ over k such that

$$D \otimes M_{m_1}(k) \cong Q_1 \otimes Q_2 \otimes \cdots \otimes Q_n \otimes M_{m_2}(k).$$

4 Brauer groups of fields

4.1 Definition of the Brauer group of a field

With all preliminary theory in place, we are ready to define the Brauer group of a field. We first define the elements of such a group and prove a few properties to make sure the group law is well defined. Up until definition 4.5, we follow the theory as presented by Farb and Dennis in [12, Chapter 4][5].

Definition 4.1.
Let A and B be finite dimensional central simple algebras over a field k. They are called *similar* if there exist positive integers m and n such that $A \otimes M_n(k) \cong B \otimes M_m(k)$.
In this case we write $A \sim B$.

Proposition 4.2.
Similarity $\sim$ defines an equivalence relation.

Proof. Reflexivity and symmetry are trivial. For proving transitivity, let A, B, and C be finite dimensional central simple algebras such that $A \sim B$ and $B \sim C$. Then there exist integers m, n, p, q such that

$$A \otimes M_n(k) \cong B \otimes M_m(k), \qquad B \otimes M_p(k) \cong C \otimes M_q(k).$$

This leads to the following sequence of isomorphisms:

$$\begin{aligned} A \otimes M_{mp}(k) &\cong A \otimes M_m(k) \otimes M_p(k) \\ &\cong B \otimes M_n(k) \otimes M_p(k) \\ &\cong B \otimes M_p(k) \otimes M_n(k) \\ &\cong C \otimes M_q(k) \otimes M_n(k) \\ &\cong C \otimes M_{qn}(k) \end{aligned}$$

where we use (ii) of proposition 2.1 and commutativity of the tensor product. Hence, $A \sim C$, which proves transitivity. □

The term *central simple algebra* will sometimes be abbreviated by *CSA*. The equivalence class of a finite dimensional CSA A is denoted by $[A]$.

Recalling our earlier observation in equation 1, we see that $[k] = [M_n(k)]$ for every $n \in \mathbb{Z}_{>0}$.

Proposition 4.3. [12, Lem 4.2]
If $A_1 \sim A_2$ and $B_1 \sim B_2$ for finite dimensional CSAs A_i and B_i, then $A_1 \otimes B_1 \sim A_2 \otimes B_2$.

Proof. A different proof using an equivalent definition of similarity can be found in [12, Lem 4.2]
Take integers m, n, p, q such that

$$A_1 \otimes M_n(k) \cong A_2 \otimes M_m(k), \qquad B_1 \otimes M_p(k) \cong B_2 \otimes M_q(k).$$

Again using commutativity of tensor products and (ii) of proposition 2.1, we obtain:

$$\begin{aligned} (A_1 \otimes B_1) \otimes M_{np}(k) &\cong A_1 \otimes M_n(k) \otimes B_1 \otimes M_p(k) \\ &\cong A_2 \otimes M_m(k) \otimes B_2 \otimes M_q(k) \\ &\cong (A_2 \otimes B_2) \otimes M_{mq}(k). \end{aligned}$$

□

[5] This book is a nice reference for studying Brauer groups of fields from scratch. The authors include necessary background material theory on modules, tensor products, and algebras, before introducing Brauer groups. It has been a reliable first resource for the author of this thesis.

Theorem 4.4. [12, Prop 4.3]
The set of equivalence classes of finite dimensional central simple k-algebras forms an abelian group with group law $[A] \bullet [B] := [A \otimes B]$ and the class $[k]$ as identity element.

Proof. Based on the proof given in [12, Prop 4.3]
By proposition 4.3, the group law is well-defined. The tensor product of finite dimensional CSAs is itself a finite dimensional CSA by theorem 1.27 and proposition 2.5, so the set is closed under the group law. Associativity and commutativity of the group law follows from the respective properties of the tensor product. The class $[k]$ indeed acts as identity since for any k-algebra A we have $A \otimes k \cong A$ by proposition 1.30. Recalling from proposition 2.6 that $A \otimes A^\circ \cong M_n(k)$ for $n = \dim_k(A)$, and using the observation $[k] = [M_n(k)]$ for any n, we conclude that every element $[A]$ has an inverse: $[A] \bullet [A^\circ] = [A \otimes A^\circ] = [M_n(k)] = [k]$. □

Definition 4.5. (Brauer group of a field)
The group of equivalence classes of finite dimensional central simple k-algebras, as defined in the statement of theorem 4.4, is called the *Brauer group* of the field k and is denoted by $\mathrm{Br}(k)$.

Remark 4.6.
By Wedderburn's theorem, every central simple algebra A over k is isomorphic to $M_n(D) \cong D \otimes M_n(k)$ for some division algebra D and some n. Since A is central and $Z(D) \cong Z(M_n(D))$, D is central as well. So we observe that $[D] = [A]$ is an element of $\mathrm{Br}(k)$. Moreover, since for every CSA A such a D exists, we find that *every element of the Brauer group is the class of some central division algebra over k.*

Remark 4.7.
To see the connection of Brauer groups with quaternion algebras, recall from the previous chapter that any quaternion algebra (a, b) over a field k with $\mathrm{char}(k) \neq 2$ is a central simple algebra, that it equals its opposite algebra, and that $(a, b) \otimes (a, b) \cong M_4(k)$. In other words, $[(a, b)]$ is an element of $\mathrm{Br}(k)$ of order at most 2 (the order is 1 if (a, b) is split). We also have $[(a, b)] \bullet [(a, b')] = [(a, bb')]$ for any $a, b, b' \in k^\times$ by proposition 3.15.

By proposition 3.10, every element of $\mathrm{Br}(k)$ (for a field k of $\mathrm{char}(k) \neq 2$) that is the class of a four-dimensional CSA, is equal to the class of some quaternion algebra, and hence of order 2.
To top it off, using Merkurjev's theorem in the light of remark 4.6, we have that for any class $[A] \in \mathrm{Br}(k)$ of order 2, there exist quaternion algebras $Q_1, \ldots, Q_n$ such that $[A] = [Q_1 \otimes \cdots \otimes Q_n]$. So every order 2 element in the Brauer group can be expressed as the class of a tensor product of quaternion algebras.

In the next section we determine the Brauer groups for specific fields, using the theory from previous chapters.

4.2 Examples of Brauer groups of fields

Proposition 4.8. [12, Chapter 4, Ex 1]
For any finite field $\mathbb{F}_q$, $\mathrm{Br}(\mathbb{F}_q) = 0$. That is, its Brauer group is the trivial group, containing only the identity element $[\mathbb{F}_q]$.

Proof. Let A be any finite dimensional CSA over $\mathbb{F}_q$. As a finite vector space over a finite field, A is finite itself. By Wedderburn's theorem there exists a unique division algebra D over k such that $A \cong M_n(D)$ for some n. We have $Z(A) = Z(M_n(D)) \cong Z(D)$. Since A is central, D is central as well, so $Z(D) \cong \mathbb{F}_q$.

Also, since A is finite, D has to be finite, so by Wedderburn's little theorem, D is in particular a field. But since the center of a field is the field itself, it follows that $D \cong \mathbb{F}_q$. So we have $[A] = [\mathbb{F}_q]$. Hence the Brauer group is trivial. □

Proposition 4.9. [12, Chapter 4, Ex 2]
For any algebraically closed field $\overline{k}$, $\mathrm{Br}(\overline{k}) = 0$.

Proof. We work out in detail the proof given in [17, Cor 2.1.7]
We show there are no finite dimensional division algebras over $\overline{k}$ except for $\overline{k}$ itself. Then Wedderburn's theorem yields that for any CSA A over $\overline{k}$, we must have $A \cong M_n(\overline{k})$ for some n. So $[A] = [\overline{k}]$, and hence, the Brauer group is trivial.

Assume D is a finite dimensional division algebra over $\overline{k}$ not equal to the homomorphic image $\phi(\overline{k}) = \{x \cdot 1 : x \in \overline{k}\}$ of $\overline{k}$ in D. Note that this image is still an algebraically closed field. For ease of notation we denote this field by K.

Take $d \in D \setminus K$. Since D is finite dimensional over $\overline{k}$, and hence also over K, the powers $1, d, d^2, \cdots, d^{\dim(D)}$ are certainly linearly dependent over K. Let m be the smallest integer such that $1, d, d^2, \cdots, d^m$ are linearly dependent. Then there exists a polynomial $f \in K[x]$ of degree m such that $f(d) = 0$. Since its coefficients are in a field, we may assume f to be monic. Note that f is irreducible: If $f = gh$ for $g, h \in K[x]$ non-units, then $f(d) = 0$ implies either $g(d) = 0$ or $h(d) = 0$ since D contains no zero divisors. But this contradicts the minimality of the degree of m.

So d is algebraic over K with minimal polynomial f. Then $K[x]/(f) \cong K(d)$, and since K is algebraically closed, $K(d) = K$. Considering the map

$$\begin{aligned} \psi \colon K \cong K[x]/(f) &\to D \\ x &\mapsto d \end{aligned}$$

which can be checked to be a K-algebra homomorphism, we see that $d \in \mathrm{im}(\psi)$. But $K \subset D$, so ψ is an inclusion map, contradicting that $d \notin K$. □

In fact, the above two examples fall into a larger category of fields that have trivial Brauer group. These are so-called C_1-fields:

Definition 4.10. (C_1-field) [17, Def 6.2.1]
A field k is called C_1 if every homogeneous polynomial $f \in k[x_1, \ldots, x_n]$ with $\deg(f) < n$ has a nontrivial zero in k^n.

These fields are also known as *quasi-algebraically closed* fields.

Theorem 4.11.
For a C_1-field k, $\mathrm{Br}(k) = 0$.

Proof. A C_1-field has no nontrivial finite dimensional division algebras over them [23, Page 374], so as shown in the proof of proposition 4.9, its Brauer group is trivial. □

Since algebraically closed fields are quasi-algebraically closed, proposition 4.9 also follows from this theorem. Similarly for finite fields, which are C_1 as showed by Chevalley and Warning [5].

Theorem 4.12. (Tsen's theorem) [43]
Let k be an algebraically closed field. The function field of a curve over k is C_1.

Proof. A proof can be found in [17, Thm 6.2.8]. □

Proposition 4.13.
Let C be a curve over an algebraically closed field and let $\kappa(C)$ be its function field. Then $\mathrm{Br}(\kappa(C)) = 0$.

Proof. This follows from the previous two theorems. □

Having seen a few trivial Brauer groups, we now turn our attention to more interesting examples, the simplest of which is the Brauer group of $\mathbb{R}$. To find this group, we use the following theorem:

Theorem 4.14. (Frobenius theorem) [13]
A finite dimensional division algebra over $\mathbb{R}$ is isomorphic to either $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

Proof. A proof can be found in [12, Thm 3.20]. □

Proposition 4.15. [12, Chapter 4, Ex 3]
$\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. Let A be a finite dimensional CSA over $\mathbb{R}$. By Wedderburn's theorem and using Frobenius theorem, $A \cong M_n(D)$ for a unique $D \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$ and for some n. If $A \cong M_n(\mathbb{R})$, then $[A] = [\mathbb{R}]$ is the identity element. If $A \cong M_n(\mathbb{C})$, then $Z(A) \cong Z(\mathbb{C}) = \mathbb{C}$, which contradicts with A being central, so this is not possible. Finally, if $A \cong M_n(\mathbb{H}) \cong \mathbb{H} \otimes M_n(\mathbb{R})$ this works out nicely: $\mathbb{H}$ is central over $\mathbb{R}$ and $\mathbb{H}^\circ = \mathbb{H}$ by proposition 3.9, so $\mathbb{H} \otimes \mathbb{H}^\circ = \mathbb{H} \otimes \mathbb{H} \cong M_4(\mathbb{R})$ by proposition 3.16. Therefore, $[A] = [\mathbb{H}]$ is an element in $\mathrm{Br}(\mathbb{R})$ of order 2. □

Example 4.16. (Conics over $\mathbb{R}$)
As a consequence of proposition 4.15, any quaternion algebra (a, b) over $\mathbb{R}$ satisfies either

- $[(a, b)] = [\mathbb{R}] = [(1, 1)]$, if it is split; or
- $[(a, b)] = [\mathbb{H}] = [(-1, -1)]$, if it is non-split.

In the first case, the associated conic $ax^2 + by^2 = z^2$ has an $\mathbb{R}$-rational point and is (by our discussion after Witt's theorem) isomorphic to the conic $x^2 + y^2 = z^2$ associated to the split quaternion algebra $(1, 1)$.

If (a, b) is non-split, its associated conic necessarily has a rational point over a degree 2 extension of $\mathbb{R}$, which can only be $\mathbb{C}$. It follows that (a, b) is split over $\mathbb{C}$, so $(a, b) \cong M_2(\mathbb{C}) \cong (-1, -1)$ as $\mathbb{C}$-algebras. By Witt's theorem, the associated conic is then isomorphic to the conic $-x^2-y^2 = z^2$ over $\mathbb{C}$. Since both conics have no $\mathbb{R}$-rational points, they are also isomorphic over $\mathbb{R}$.

Note that every conic over $\mathbb{R}$ can be given by a diagonal quadratic form, and is thus associated to some quaternion algebra. The above observation then implies that there are two conics over $\mathbb{R}$ up to isomorphism: those with an $\mathbb{R}$-rational point that are isomorphic to $x^2 + y^2 = z^2$, and those that acquire a point over $\mathbb{R}(i) = \mathbb{C}$ and are isomorphic to the conic $-x^2 - y^2 = z^2$.

Proposition 4.17. [29, IV.4]
For a non-archimedean local field K, $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$.

Proof. A construction of the isomorphism can be found in [29, IV.4], which falls outside the scope of this paper. □

We look at the isomorphism of proposition 4.17 in more detail in the next section.

4.3 The Hasse invariant map

In this section we introduce and state some properties of the Hasse invariant map, which plays an important role in the Brauer-Manin obstruction of chapter 7. Throughout this section, we use some definitions from section 1.3 on algebraic number theory. The new theory is taken from [4, Chapter 10].

If k is a number field (so a global field) and v a finite place of k, the completion k_v is a non-archimedean local field by proposition 1.81. The canonical isomorphism $\mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$ of proposition 4.17 is then denoted by inv_v and called the *Hasse invariant map*.

We extend the definition of the Hasse invariant map to infinite places:

- If v is a real place of k, then $k_v \cong \mathbb{R}$ by theorem 1.77. So $\mathrm{Br}(k_v) \cong \mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ which is isomorphic to the subgroup $\{0, \frac{1}{2}\}$ of $\mathbb{Q}/\mathbb{Z}$. We therefore define $\mathrm{inv}_v \colon \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$ as the injective homomorphism defined by $[\mathbb{R}] \mapsto 0$ and $[\mathbb{H}] \mapsto \frac{1}{2}$.
- If v is a complex place, theorem 1.77 gives $k_v \cong \mathbb{C}$, so $\mathrm{Br}(\mathbb{C}) = 0$ by proposition 4.9. In this case we define inv_v as the zero map.

Having defined the invariant map at all places v of k, we can state a well-known result of Brauer groups of number fields:

Theorem 4.18. [4, Thm 10.4.5]
Let k be a number field. The sequence

$$0 \to \mathrm{Br}(k) \to \bigoplus_v \mathrm{Br}(k_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}$$

is exact. In the direct sum, v ranges over all places of k, and $\mathrm{Br}(k) \to \bigoplus_v \mathrm{Br}(k_v)$ is the diagonal map induced by the inclusion maps $k \hookrightarrow k_v$.

In particular, recalling Ostrowski's theorem, we have the following exact sequence for $k = \mathbb{Q}$:

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{p \leq \infty} \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\sum_p \mathrm{inv}_p} \mathbb{Q}/\mathbb{Z}.$$

In chapter 7, we compute the value of the invariant map of some quaternion algebras over a local field. It turns out, as becomes clear when we prove proposition 4.21, that we can do this by computing a *Hilbert symbol* instead.

Definition 4.19. (Hilbert symbol)
Let k be a number field and v a place of k. For $a, b \in k_v^\times$ we define their *Hilbert symbol* at v by

$$(a,b)_v = \begin{cases} 1 & \text{if the conic } ax^2 + by^2 = z^2 \text{ has a } k_v\text{-rational point;} \\ -1 & \text{otherwise.} \end{cases}$$

In our example in chapter 7, we only have to compute the Hilbert symbol at finite places v of the number field $\mathbb{Q}$. This can be done using the formulas in the following proposition:

Proposition 4.20. [4, Prop 10.1.6 (ii), (iii)]

(i) Let p be an odd prime. Let $a, b \in \mathbb{Q}_p^\times$ and write $a = p^\alpha u$ and $b = p^\beta v$ with $u, v \in \mathbb{Z}_p^\times$. Write $\epsilon(p) = (p-1)/2$. Then

$$(a,b)_p = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

In particular, $(u,v)_p = 1$ if $u, v \in \mathbb{Z}_p^\times$.
(Here, $\left(\frac{u}{p}\right)$ denotes the Legendre symbol $\left(\frac{\overline{u}}{p}\right)$, where $\overline{u}$ is the image of u under the map of reduction modulo p: $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times$.)

(ii) Let $a, b \in \mathbb{Q}_2^\times$ and write $a = 2^\alpha u$ and $b = 2^\beta v$ with $u, v \in \mathbb{Z}_2^\times$. For $x \in \mathbb{Z}_2^\times$, write $\epsilon(x) = (x-1)/2 \bmod 2$ and $\omega(x) = (x^2-1)/8 \bmod 2$. Then

$$(a,b)_2 = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)}.$$

Proof. A proof can be found in [39, Chapter III, 1.2, Thm 1]. □

Finally, the Hilbert symbol can be used to compute the value of the Hasse invariant map of certain quaternion algebras:

Proposition 4.21. [4, Exc 10.4.4]
Let v be a valuation of $\mathbb{Q}$ and $a, b \in \mathbb{Q}_v^\times$. Write $(a,b)_{\mathbb{Q}_v}$ for the quaternion algebra over $\mathbb{Q}_v$. Then

$$\mathrm{inv}_v[(a,b)_{\mathbb{Q}_v}] = \begin{cases} 0 & \text{if } (a,b)_v = 1; \\ \frac{1}{2} & \text{if } (a,b)_v = -1. \end{cases}$$

Proof. If $(a,b) = 1$, the conic $ax^2 + by^2 = z^2$ has a $\mathbb{Q}_v$-rational point. Proposition 3.13 gives that the quaternion algebra $(a,b)_{\mathbb{Q}_v}$ is split, so isomorphic to $M_2(\mathbb{Q}_v)$. The equivalence class of $(a,b)_{\mathbb{Q}_v}$ in $\mathrm{Br}(\mathbb{Q}_v)$ is then equal to the identity, and hence, $\mathrm{inv}_v[(a,b)_{\mathbb{Q}_v}] = 0$.

If $(a,b) = -1$, we have that the order of $[(a,b)_{\mathbb{Q}_v}]$ in $\mathrm{Br}(\mathbb{Q}_v)$ equals 2 (see remark 4.7). Then,

$$\mathrm{inv}_v[(a,b)_{\mathbb{Q}_v}] + \mathrm{inv}_v[(a,b)_{\mathbb{Q}_v}] = \mathrm{inv}_v[(a,b)_{\mathbb{Q}_v} \otimes (a,b)_{\mathbb{Q}_v}] = \mathrm{inv}_v[M_4(\mathbb{Q}_v)] = 0.$$

Since inv_v is injective and $[(a,b)_{\mathbb{Q}_v}]$ is not the identity, we find $\mathrm{inv}_v(a,b)_{\mathbb{Q}_v}] = \frac{1}{2}$. □

5 Brauer groups of rings

In this chapter we extend the definition of the Brauer group of a field to the one of a commutative ring. Instead of classes of CSAs, the elements of the Brauer group of a ring are the classes of so-called *Azumaya algebras*. In the case that the ring is a field, the Azumaya algebras are exactly the finite dimensional central simple algebras. So as we will see later, the definition of the Brauer group of a ring indeed coincides with the one of the Brauer group of a field in case the ring is itself a field. Before we define the group, we introduce the notion of an algebra over a commutative ring so that we can define Azumaya algebras. Just as in the previous chapter, we find an equivalence relation between Azumaya algebras over the ring, after which the group structure becomes clear.

Throughout this chapter, a ring R is assumed to be commutative. Proofs are often omitted, as we are mostly interested in the definition of the Brauer group of a ring to be able to define the Brauer group of a variety in the next chapter and use this for the Brauer-Manin obstruction in chapter 7. We mostly follow the theory from [12, Chapter 8], with some additions from [4, Chapter 11].

5.1 Azumaya algebras

We start this chapter by extending the definitions from section 1.1.3 about algebras over a field to algebras over a commutative ring. The definition of such an R-algebra depends on the reference. We assume the one used by Farb and Dennis in [12, Chapter 0], and adapt the formulation to fit the style of definition 1.31.

Definition 5.1. (Algebra over a commutative ring)
An *(associative) algebra over R*, also called an *R-algebra*, is a nonempty set A with the operations addition, multiplication $*$ and scalar multiplication $\cdot$, such that

(A1) A is an R-module under addition and scalar multiplication,

(A2) A is a ring with identity under addition and multiplication,

(A3) For all $r \in R$, $a, b \in A$, we have $r \cdot (a * b) = (r \cdot a) * b = a * (r \cdot b)$.

An *R-algebra homomorphism* is defined in the same way as definition 1.32 for the case of fields: it is an R-module homomorphism that is also a ring homomorphism.

Example 5.2.
For an R-algebra A we define the map

$$\begin{aligned} \phi_A \colon A \otimes_R A^\circ &\to \mathrm{End}_R(A) \\ a \otimes b &\mapsto (x \mapsto axb) \end{aligned}$$

which can be checked to be a homomorphism of R-algebras. Recall that the same map was used in the proof of proposition 2.6 for the case that R is a field.

One of the conditions for an R-algebra A to be an Azumaya algebra is that this map ϕ_A is an isomorphism. Another is that it has to be *faithful*:

Definition 5.3. (Faithful)
An R-module M is called *faithful* if the natural map

$$\begin{aligned} R &\to \mathrm{End}_R(M) \\ r &\mapsto (m \mapsto r \cdot m) \end{aligned}$$

is injective. Equivalently, for any $r, s \in R$, there exists an $m \in M$ such that $r \cdot m \neq s \cdot m$.

To reduce the amount of adjectives in what follows, we introduce the following terminology:

Definition 5.4. (Faithfully projective)
An R-module A that is finitely generated, projective and faithful, is called *faithfully projective*.

Definition 5.5. (Azumaya algebra)
An *Azumaya algebra* over R is an R-algebra that is faithfully projective as R-module and for which the map ϕ_A of example 5.2 is an isomorphism.

The following lemma provides a nice way to check if an algebra is Azumaya when it is known that it is finitely generated and projective.

Lemma 5.6. [4, Lem 11.2.1]
Let A be an R-algebra, and suppose that A is finitely generated and projective as R-module. Then A is faithful if and only if the natural map $R \to A$, $r \mapsto r \cdot 1_A$ is injective.

Another way to check this is given in the following proposition. To understand this statement in full generality requires some knowledge on localization (the interested reader is referred to [1, Chapter 3]), but for our purposes it is sufficient to know the definition of reduction in the case of a local ring:

Definition 5.7. (Reduction) [4]
For a local ring R and an R-algebra A, the *reduction* of A modulo the maximal ideal $\mathfrak{m}$ of R is defined as the algebra $A(\mathfrak{m}) \coloneqq A \otimes_R k_\mathfrak{m}$ where $k_\mathfrak{m} = R/\mathfrak{m}$ is the residue field.

Proposition 5.8. [4, Prop 11.2.3]
Let R be a local ring and A an R-algebra that is finitely generated and projective as R-module. Then A is Azumaya over R if and only if the reduction $A(\mathfrak{m})$ modulo the maximal ideal $\mathfrak{m}$ of R is central and simple over the residue field $k_\mathfrak{m}$.

To see the relation between Brauer groups of fields and Brauer groups of rings later on, consider the following statement:

Proposition 5.9.
The finite dimensional CSAs over a field k are precisely the Azumaya algebras over k.

Proof. Let A be a finite dimensional CSA over k. Then, since it has a finite basis, it is finitely generated and free. By proposition 1.18 it is therefore projective. To show it is faithful we apply lemma 5.6. Suppose the natural map is not injective, i.e., there exists a nonzero $r \in k$ such that $r \cdot 1_A = 0$. Since k is a field, r^{-1} exists, and so we arrive at a contradiction via

$$1_A = 1 \cdot 1_A = (r^{-1}r) \cdot 1_A = r^{-1} \cdot (r \cdot 1_A) = r^{-1} \cdot 0 = 0.$$

As shown in the proof of proposition 2.6, ϕ_A is an isomorphism. So A is Azumaya.

Now assume A is an Azumaya algebra over k. Being finitely generated implies it is finite dimensional over k. Finally, in the proof of [4, Prop 10.2.14] it is shown that ϕ_A being an isomorphism implies that A is central and simple. □

The following proposition and consecutive example are useful for determining the identity element of the Brauer group of R.

Proposition 5.10. [12, Prop 8.3]
For any faithfully projective R-module P, the endomorphism ring $\mathrm{End}_R(P)$ is an Azumaya algebra.

Example 5.11.
Consider the R-module R^n. It is finite dimensional and free and therefore, finitely generated and projective. Defining multiplication component-wise gives it the structure of a ring with multiplication satisfying (A3) of definition 5.1. So it is an R-algebra. The natural map $R \to R^n$, $r \mapsto r \cdot (1, \ldots, 1)$ is injective, so by lemma 5.6, it is faithful. So we have that $\mathrm{End}_R(R^n)$ is an Azumaya algebra by the above proposition.

Just as with the Brauer group of a field, the equivalence class of $M_n(R) \cong \mathrm{End}_R(R^n)$ acts as the identity element of the Brauer group of R. In fact, the identity element is the class of $\mathrm{End}_R(P)$ for any faithfully projective module P, as will become clear soon.

To show that the group law for the Brauer group of a ring is well-defined, we require the isomorphism from the next proposition:

Proposition 5.12. [12, Prop 8.2]
Let P and Q be finitely generated projective R-modules. Then the map

$$w\colon \mathrm{End}_R(P) \otimes \mathrm{End}_R(Q) \to \mathrm{End}_R(P \otimes Q)$$

defined by $w(f \otimes g) = f \otimes g$ extended linearly is an isomorphism.

5.2 Definition of the Brauer group of a ring

We now turn our attention to the equivalence relation with which we can define the elements of the Brauer group.

Definition 5.13.
Let A and B be Azumaya algebras over a commutative ring R. They are called *equivalent* if there exist faithfully projective R-modules P and Q such that $A \otimes \mathrm{End}_R(P) \cong B \otimes \mathrm{End}_R(Q)$ as R-modules. In this case we write $A \sim B$.

It can be checked that $\sim$ defines an equivalence relation: reflexivity and symmetry are trivial, and proving transitivity is very similar to the proof of proposition 4.2 using the isomorphism from proposition 5.12.
We denote the equivalence class of an Azumaya algebra A by $[A]$.

With this definition we observe that $[\mathrm{End}_R(P)] = [R]$ for any faithfully projective module P.

Remark 5.14.
To see the relation to similarity as defined in definition 4.1, let A and B be finite dimensional CSAs over a field k that are similar. Then A and B are Azumaya over k by proposition 5.9 and there exist integers m, n such that $A \otimes M_m(k) \cong B \otimes M_n(k)$. Since $M_m(k) \cong \mathrm{End}_k(k^m)$, we have $A \otimes \mathrm{End}_k(k^m) \cong B \otimes \mathrm{End}_k(k^n)$. So A and B are equivalent Azumaya algebras.

Conversely, if A and B are equivalent Azumaya algebras over a field k, then they are finite dimensional CSAs over k (again by proposition 5.9) that are similar:

Let P and Q be faithfully projective modules such that $A \otimes \mathrm{End}_k(P) \cong B \otimes \mathrm{End}_k(Q)$. Because k is a field, projective modules are free by proposition 1.19, so since P and Q are finitely generated, there exist integers m and n such that $P \cong k^m$ and $Q \cong k^n$. Hence,

$$A \otimes M_m(k) \cong A \otimes \mathrm{End}_k(k^m) \cong B \otimes \mathrm{End}_k(k^n) \cong B \otimes M_n(k).$$

So the definitions of similar and equivalent match if R is a field.

As you might expect, the group operation of the Brauer group of R will be induced by the tensor product again. To show that this operation is well-defined and that the Brauer group is closed, we require two more properties:

Proposition 5.15.
If $A_1 \sim A_2$ and $B_1 \sim B_2$ for Azumaya algebras A_i and B_i, then $A_1 \otimes B_1 \sim A_2 \otimes B_2$.

Proof. Take faithfully projective modules M, N, P, Q such that

$$A_1 \otimes \mathrm{End}_R(M) \cong A_2 \otimes \mathrm{End}_R(N), \qquad B_1 \otimes \mathrm{End}_R(P) \cong B_2 \otimes \mathrm{End}_R(Q).$$

Using the isomorphism from proposition 5.12, we obtain:

$$\begin{aligned}(A_1 \otimes B_1) \otimes \mathrm{End}_R(M \otimes P) &\cong A_1 \otimes \mathrm{End}_R(M) \otimes B_1 \otimes \mathrm{End}_R(P) \\ &\cong A_2 \otimes \mathrm{End}_R(N) \otimes B_2 \otimes \mathrm{End}_R(Q) \\ &\cong (A_2 \otimes B_2) \otimes \mathrm{End}_R(N \otimes Q).\end{aligned}$$

□

Proposition 5.16. [12, Prop 8.4]
If A and B are Azumaya algebras, then $A \otimes B$ is an Azumaya algebra.

Theorem 5.17. [12, Thm 8.5]
The set of equivalence classes of Azumaya R-algebras forms an abelian group with group law $[A] \bullet [B] \coloneqq [A \otimes B]$ and the class $[R]$ as identity element.

Proof. Based on the proof given in [12, Thm 8.5]
By proposition 5.15, the group law is well-defined and by proposition 5.16, the set is closed under the group law. Associativity and commutativity of the group law follows from the respective properties of the tensor product. The class $[R]$ indeed acts as identity since for any module A over R we have $A \otimes R \cong A$ by proposition 1.30. Since the map ϕ_A is an isomorphism for Azumaya algebras, we have that $A \otimes A^\circ \cong \mathrm{End}_R(A)$. So since $[\mathrm{End}_R(P)] = [R]$ for any faithfully projective module P and one can show that A° is Azumaya for any Azumaya algebra A, we find that every element $[A]$ has an inverse:

$$[A] \bullet [A^\circ] = [A \otimes A^\circ] = [\mathrm{End}_R(A)] = [R].$$

□

Definition 5.18. (Brauer group of a ring)
The group defined in the statement of theorem 5.17 is called the *Brauer group* of the commutative ring R and is denoted by $\mathrm{Br}(R)$.

In the case that R is a field, the elements of $\mathrm{Br}(R)$ are precisely the classes of finite dimensional CSAs over R, by proposition 5.9 and remark 5.14. The group law and identity element coincide as well, so the definition of the Brauer group of a ring is indeed an extension of the one of the Brauer group of a field.

For certain rings R we can identify an injective map from $\mathrm{Br}(R)$ to $\mathrm{Br}(K)$, where K is the field of fractions of R. This property, which is stated in theorem 5.20, holds for so-called *regular* integral domains, of which we will see an example in the next chapter. First a proposition that holds for general integral domains:

Proposition 5.19. [4, Rmk 11.2.4]
Let R be an integral domain with field of fractions K. For any Azumaya algebra A over R, the K-algebra $A \otimes_R K$ is central and simple over K.

Theorem 5.20. [2, Thm 7.2]
If R is a regular integral domain with field of fractions K, then the natural homomorphism

$$\begin{aligned} \mathrm{Br}(R) &\to \mathrm{Br}(K) \\ [A] &\mapsto [A \otimes_R K] \end{aligned}$$

is injective.

Recall that for the Brauer group of a field (of characteristic unequal to 2), classes of quaternion algebras provide elements of order 2. Although this property does not extend to the Brauer group of a ring (see also remark 5.22 below), there is a generalization of the definition of quaternion algebras for a ring, so-called *Hamilton algebras*:

Definition 5.21. (Hamilton algebra) [4, Def 11.3.2]
For $a, b \in R$, the *Hamilton algebra* $(a, b)_R$ is defined as the R-algebra freely generated by $1, i, j, ij$ as an R-module and multiplication according to the rules

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

Remark 5.22. [4, Page 134]
Hamilton algebras over a ring generalize quaternion algebras over a field: if k is a field with $\mathrm{char}(k) \neq 2$, then the Hamilton algebra $(a, b)_k$ satisfies the definition of the quaternion algebra (a, b) over k. However, it is important to note that not all Hamilton algebras are Azumaya. So unlike quaternion algebras, whose classes are elements of the Brauer group of the field, Hamilton algebras do not necessarily give classes that lie in the Brauer group of the ring. For an example of a Hamilton algebra that is Azumaya, see section 6.2.

Proposition 5.23. [4, Page 134]
If $f\colon R \to S$ is an homomorphism of commutative rings and $a, b \in R$, then the natural homomorphism

$$(a, b)_R \otimes_R S \to (f(a), f(b))_S$$

is an isomorphism of S-algebras.

More generally:

Proposition 5.24. [4, Page 133]
If $f\colon R \to S$ is an homomorphism of commutative rings, it induces a group homomorphism

$$\begin{aligned} f_*\colon \mathrm{Br}(R) &\to \mathrm{Br}(S) \\ [A] &\mapsto [A \otimes_R S] \end{aligned}$$

Just as in the previous chapter, there are examples of Brauer groups of rings that are trivial:

Proposition 5.25. [31]
$\mathrm{Br}(\mathbb{Z}) = 0$.

Proposition 5.26. [4, Cor 11.3.13]
Let k be a finite extension of the field of p-adic numbers $\mathbb{Q}_p$ and let R be the ring of integers in k. Then $\mathrm{Br}(R) = 0$.

6 Brauer groups of varieties

After having defined the Brauer group of a ring, we can use this definition to introduce the Brauer group of a variety. In this chapter, X denotes a smooth geometrically irreducible variety, $\kappa(X)$ its function field, $\mathcal{O}_{X,P}$ the local ring at a point P of X, and $X(k)$ the set of k-rational points on X. Note that X can be either a projective or affine variety, even though we only properly defined the former. However, the main example of a variety of which we want to study its Brauer group, is the del Pezzo surface from example 1.64, which is projective.

6.1 Definition of the Brauer group of a variety

Most references define the Brauer group of a variety using cohomology, which is studied in some graduate level courses. To avoid introducing this theory, we define it in an easier way, following the lecture notes of Bright, Testa and van Luijk [4, Chapter 12].

For a smooth point $P \in X(\overline{k})$, the local ring $\mathcal{O}_{X,P}$ is a so-called *regular local ring*, which is studied in commutative algebra [16, Rmk 10.10]. Such a ring is an integral domain [15, Prop 11.40] and since X is irreducible over $\overline{k}$, the field of fractions of $\mathcal{O}_{X,P}$ is isomorphic to the function field $\kappa(X)$ [10, Exc 4.7.17]. Knowing this, theorem 5.20 gives an injective homomorphism

$$\mathrm{Br}(\mathcal{O}_{X,P}) \hookrightarrow \mathrm{Br}(\kappa(X)).$$

Under this map, $\mathrm{Br}(\mathcal{O}_{X,P})$ can be seen as a subgroup of $\mathrm{Br}(\kappa(X))$.

The elements of $\mathrm{Br}(\kappa(X))$ in the image of $\mathrm{Br}(\mathcal{O}_{X,P})$ are called *unramified* at P. The other elements are called *ramified* at P.

The Brauer group of X is then defined as follows:

Definition 6.1. (Brauer group of a variety)
Let X be a smooth geometrically irreducible variety over k. The *Brauer group* of X is defined as the subgroup of $\mathrm{Br}(\kappa(X))$ consisting of the elements that are unramified at all $P \in X(\overline{k})$. In other words,

$$\mathrm{Br}(X) \coloneqq \bigcap_{P \in X(\overline{k})} \mathrm{Br}(\mathcal{O}_{X,P}),$$

where each $\mathrm{Br}(\mathcal{O}_{X,P})$ is seen as a subgroup of $\mathrm{Br}(\kappa(X))$.

Proposition 6.2. [4, Thm 12.3.1]
Let C be a smooth irreducible curve over an algebraically closed field. Then $\mathrm{Br}(C) = 0$.

Proof. This follows from proposition 4.13 in which we showed $\mathrm{Br}(\kappa(C)) = 0$, and the fact that $\mathrm{Br}(C)$ is a subgroup of $\mathrm{Br}(\kappa(C))$. □

6.2 The Brauer group of a del Pezzo surface of degree 4

In this section we work out an example from the notes by Bright et al. [4, Ex 12.1.2]. We look at the Brauer group of the del Pezzo surface of degree 4 which was introduced in example 1.64.

Denoting this surface by X, recall that $X \subset \mathbb{P}^4_{\mathbb{Q}}$ is a projective variety over $\mathbb{Q}$ defined by the equations

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

This is a smooth and geometrically irreducible variety [44], so its Brauer group $\mathrm{Br}(X)$ is well-defined as a subgroup of $\mathrm{Br}(\kappa(X))$.

Recalling the function field $\kappa(X)$ from example 1.64, note that the rational functions 5 and $u/(u+v)$ are elements in $\kappa(X)$, since they are both fractions of homogeneous polynomials of the same degree. So we can define the following quaternion algebra over $\kappa(X)$:

$$\mathcal{A} \coloneqq \left(5, \frac{u}{u+v}\right).$$

Although we are not able to give the Brauer group of X explicitly, we can show that the class of $\mathcal{A}$, which is an element of $\mathrm{Br}(\kappa(X))$, lies in $\mathrm{Br}(X)$. To do this, we show that for any point $P \in X(\overline{\mathbb{Q}})$, $[\mathcal{A}]$ lies in the image of $\mathrm{Br}(\mathcal{O}_{X,P}) \hookrightarrow \mathrm{Br}(\kappa(X))$.

First, let $P \in X(\overline{\mathbb{Q}})$ be a point with $u(P) \neq 0$ and $u(P) + v(P) \neq 0$. Then 5 and $u/(u+v)$ are elements of the local ring $\mathcal{O}_{X,P}$, so we can define the Hamilton algebra

$$\mathcal{A}_P \coloneqq \left(5, \frac{u}{u+v}\right)_{\mathcal{O}_{X,P}}$$

over $\mathcal{O}_{X,P}$. We show that it is Azumaya using proposition 5.8. First note that the algebra is finitely generated and free. By proposition 1.18 it is then also projective. So the only thing left to show is that its reduction modulo the maximal ideal I_P of $\mathcal{O}_{X,P}$ is central and simple over the residue field.

Denote the residue field $\mathcal{O}_{X,P}/I_P$ by k_P. Recall that the reduction modulo I_P of $\mathcal{A}_P$ is defined as the tensor product

$$\mathcal{A}_P \otimes_{\mathcal{O}_{X,P}} k_P = \left(5, \frac{u}{u+v}\right)_{\mathcal{O}_{X,P}} \otimes_{\mathcal{O}_{X,P}} k_P.$$

Consider the homomorphism

$$\begin{aligned} f \colon \mathcal{O}_{X,P} &\to k_P \\ \frac{g}{h} &\mapsto \frac{g(P)}{h(P)} + I_P. \end{aligned}$$

Using proposition 5.23 with this map f gives

$$\left(5, \frac{u}{u+v}\right)_{\mathcal{O}_{X,P}} \otimes_{\mathcal{O}_{X,P}} k_P \cong \left(f(5), f\left(\frac{u}{u+v}\right)\right)_{k_P} = \left(5 + I_P, \frac{u(P)}{u(P)+v(P)} + I_P\right)_{k_P}.$$

Since $u(P) \neq 0$, we have $u(P)/(u(P)+v(P)) \notin I_P$, so $f(5)$ and $f(u/(u+v))$ are nonzero in k_P. Therefore, the algebra above defines a quaternion algebra over k_P. By proposition 3.9, it is central and simple, and hence, by proposition 5.8, $\mathcal{A}_P$ is an Azumaya algebra over $\mathcal{O}_{X,P}$.

Considering the natural map $g \colon \mathcal{O}_{X,P} \hookrightarrow \kappa(X)$ (recall that $\kappa(X)$ is the field of fractions of $\mathcal{O}_{X,P}$), proposition 5.23 gives

$$\mathcal{A}_P \otimes_{\mathcal{O}_{X,P}} \kappa(X) \cong \left(g(5), g\left(\frac{u}{u+v}\right)\right)_{\kappa(X)} = \left(5, \frac{u}{u+v}\right) = \mathcal{A}.$$

Since the inclusion map $\mathrm{Br}(\mathcal{O}_{X,P}) \hookrightarrow \mathrm{Br}(\kappa(X))$ as defined in theorem 5.20 maps $[\mathcal{A}_P]$ to $[\mathcal{A}_P \otimes_{\mathcal{O}_{X,P}} \kappa(X)] = [\mathcal{A}]$, the class of $\mathcal{A}$ lies indeed in the image of $\mathrm{Br}(\mathcal{O}_{X,P})$.

Now we want to show the same for points $P \in X(\overline{\mathbb{Q}})$ that have either $u(P) = 0$ or $u(P)+v(P) = 0$. Recall from example 1.64 that two rational functions F/G and F'/G' define the same element in $\kappa(X)$ if and only if

$$FG' - F'G \in I(X) = \langle uv - x^2 + 5y^2, (u+v)(u+2v) - x^2 + 5z^2 \rangle.$$

Since $uv^2 - (x^2 - 5y^2)v = (uv - x^2 + 5y^2)v \in I(X)$. we have

$$\frac{u}{v} = \frac{x^2 - 5y^2}{v^2} \in \kappa(X).$$

This equals the norm $N_{\kappa(X)(\sqrt{5})}((x + \sqrt{5}y)/v)$ from the field extension $\kappa(X)(\sqrt{5})/\kappa(X)$. So, by proposition 3.11, we have

$$\mathcal{A} = \left(5, \frac{u}{u+v}\right) \cong \left(5, \frac{u}{u+v}\left(N_{\kappa(X)(\sqrt{5})}\left(\frac{x+\sqrt{5}y}{v}\right)\right)^{-1}\right) = \left(5, \frac{u}{u+v}\frac{v}{u}\right) = \left(5, \frac{v}{u+v}\right).$$

Similarly,

$$\frac{u+v}{u+2v} = \frac{x^2 - 5z^2}{(u+2v)^2} = N_{\kappa(X)(\sqrt{5})}\left(\frac{x+\sqrt{5}z}{u+2v}\right).$$

So $\mathcal{A}$ is also isomorphic to the quaternion algebras

$$\left(5, \frac{u}{u+v}\frac{u+v}{u+2v}\right) = \left(5, \frac{u}{u+2v}\right) \quad \text{and} \quad \left(5, \frac{u}{u+2v}\frac{v}{u}\right) \cong \left(5, \frac{v}{u+2v}\right).$$

Depending on whether $u(P) = 0$ or $u(P) + v(P) = 0$, we can take one representative of $\mathcal{A}$, i.e., one of the three quaternion algebras isomorphic to $\mathcal{A}$, and repeat the same argument as before to show that the class of this algebra lies in the image of $\mathrm{Br}(\mathcal{O}_{X,P})$.

It remains to show that for a point $P \in X(\overline{\mathbb{Q}})$ with both $u(P) = 0$ and $v(P) = 0$, $[\mathcal{A}]$ lies in the image of $\mathrm{Br}(\mathcal{O}_{X,P})$. In this case we have $x^2(P) = 5y^2(P) = 5z^2(P)$, so this gives four possible points in $\mathbb{P}^4_{\mathbb{Q}}$ that we need to check: $(0 : 0 : \sqrt{5} : \pm 1 : \pm 1)$. For this we show that $\mathcal{A}$ is isomorphic to the quaternion algebra

$$\left(5, \frac{2u + 3v + 2x}{u + v + 2x}\right).$$

Then, for each of the points $P = (0 : 0 : \sqrt{5} : \pm 1 : \pm 1)$ we can repeat the same argument as before to show that the class of this algebra lies in the image of $\mathrm{Br}(\mathcal{O}_{X,P})$, which finishes the proof.

Consider the function

$$g = \frac{u + v + x - \sqrt{5}z}{u + x - \sqrt{5}y} \in \kappa(X)(\sqrt{5}).$$

Computing the norm from the field extension $\kappa(X)(\sqrt{5})/\kappa(X)$ of g gives

$$N_{\kappa(X)(\sqrt{5})}(g) = \frac{(u+v+x)^2 - 5z^2}{(u+x)^2 - 5y^2} = \frac{(u+v)^2 + 2x(u+v) + x^2 - 5z^2}{u^2 + 2ux + x^2 - 5y^2}.$$

Recall that in $\kappa(X)$ we have $x^2 - 5z^2 = (u+v)(u+2v)$ and $x^2 - 5y^2 = uv$, so the above expression in $\kappa(X)$ equals

$$\frac{(u+v)^2 + 2x(u+v) + (u+v)(u+2v)}{u^2 + 2ux + uv}.$$

Using proposition 3.11 again, we find after some arithmetic:

$$\mathcal{A} \cong \left(5, \frac{u}{u+v}N_{\kappa(X)(\sqrt{5})}(g)\right) = \left(5, \frac{2u+3v+2x}{u+v+2x}\right).$$

This shows that also for the points $P \in X(\overline{\mathbb{Q}})$ with $u(P) = v(P) = 0$, the class $[\mathcal{A}]$ lies in the image of $\mathrm{Br}(\mathcal{O}_{X,P})$.

To conclude, $[\mathcal{A}]$ lies in the image of the map $\mathrm{Br}(\mathcal{O}_{X,P}) \hookrightarrow \mathrm{Br}(\kappa(X))$ for any $P \in X(\overline{\mathbb{Q}})$. Hence, $[\mathcal{A}]$ defines an element in the Brauer group of X.

7 The Brauer-Manin obstruction

In this chapter, we look at an application of Brauer groups in algebraic geometry. Given a variety X which has local points everywhere, the Brauer group of X can in some cases be used to determine that X still has no global point. When this is indeed the case, we say there is a Brauer-Manin obstruction to the Hasse principle on X.

We first define the Hasse principle in the next section, relying on [4, Chapter 2]. Then, in section 7.2, we introduce the Brauer-Manin obstruction, using mostly the theory from [4, Chapter 13]. Finally, we apply this to the example of our del Pezzo Surface in section 7.3.

7.1 The Hasse principle

Let k be a number field. As discussed in section 1.3.2, there is an embedding of k in each completion k_v, where v denotes a place of k. Consequentially, for a variety X over k, if X has a k-rational point, it also has a k_v-rational point for each v. So we have an implication

$$X(k) \neq \emptyset \implies X(k_v) \neq \emptyset \text{ for each place } v.$$

A very simple example for the number field $\mathbb{Q}$: if X has a $\mathbb{Q}$-rational point, it obviously has an $\mathbb{R}$-rational point. Here, $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the infinite place $v = \infty$. Since $\mathbb{Q}$ is moreover embedded in the field of p-adic numbers $\mathbb{Q}_p$ for each prime p, the condition also implies X has a $\mathbb{Q}_p$-rational point for each p.

We call the rational points over the local fields k_v the *local points* of X and the rational points over the global field k the *global points* of X.

So far we know that a global point implies a local point everywhere, that is, a rational point over each of the k_v. Equivalently, the absence of a local point at some place always implies the absence of a global point. For example, the projective curve defined by $x^2 + y^2 = 0$ has no $\mathbb{R}$-rational points (recall that the solution $x = y = 0$ does not define a point in $\mathbb{P}^2$), and, therefore, it has no $\mathbb{Q}$-rational points.

However, a variety could have local points everywhere and still lack a global point. The projective curve $3x^3 + 4y^3 + 5z^3 = 0$, known as Selmer's cubic, has rational points over $\mathbb{R}$ and each $\mathbb{Q}_p$, but not over $\mathbb{Q}$ [38][6]. But for other varieties, having local points everywhere *does* imply the existence of a global point. For such varieties, the existence of local points everywhere is hence not only a necessary condition, but also a sufficient condition for having a global point.

We would like to know when this is the case: when for a variety X the absence or existence of a global point can be detected by checking if there are local points everywhere. In other words, when there is also a reverse implication:

$$X(k) \neq \emptyset \impliedby X(k_v) \neq \emptyset \text{ for each place } v.$$

When the implication indeed goes in both directions, we say that the variety satisfies the Hasse principle:

Definition 7.1. (Hasse principle)
Let X be a variety over a number field k. If the condition $X(k_v) \neq \emptyset$ for all places v of k implies $X(k) \neq \emptyset$, then X is said to *satisfy the Hasse principle*. If this is not the case, we say that X is a *counterexample to the Hasse principle*.

[6] See also Conrad's notes [8] for a proof.

It has been shown that del Pezzo surfaces of degree at least 5 satisfy the Hasse principle [45, Thm 2.1]. For del Pezzo surfaces of degree 4, this is not the case: The surface introduced in example 1.64 is a counterexample, as was first shown by Birch and Swinnerton-Dyer in [41]. A proof will be worked out in detail in section 7.3. There are also examples of del Pezzo surfaces of degree 4 that do satisfy the Hasse principle: in [30], a family of such surfaces is given of which most satisfy the Hasse principle.

To make it easier to refer to the local points of a variety at every place, we introduce some new terminology.

Definition 7.2. (Adèles and adelic points)
Let k be a number field. The ring of *adèles* of k is the subring $\mathbb{A}_k$ of the direct product $\prod_v k_v$ consisting of the tuples (x_v), where x_v is an algebraic integer for all but finitely many places v.

Let X be a variety over k. The set of *adelic points* of X is the subset $X(\mathbb{A}_k)$ of the direct product $\prod_v X(k_v)$ consisting of the tuples (P_v), where $P_v \in X(k_v)$ has coordinates which are algebraic integers in k_v, for all but finitely many places v.

Proposition 7.3. [4, Page 7]
If X is a projective variety, then $X(\mathbb{A}_k) = \prod_v X(k_v)$.

So for a projective variety X, we have that $X(\mathbb{A}_k)$ is nonempty if and only if $X(k_v)$ is nonempty for each place v. As a consequence, a projective variety X satisfies the Hasse principle if the condition $X(\mathbb{A}_k) \neq \emptyset$ implies $X(k) \neq \emptyset$.

A theorem by Hasse and Minkowski states that quadratic forms satisfy the Hasse principle:

Theorem 7.4. (Hasse-Minkowski theorem) [4, Thm 2.3.1]
Let X be a projective variety over a number field k defined by one quadratic form. If $X(\mathbb{A}_k)$ is nonempty, then $X(k)$ is nonempty.

Proof. A proof can be found in [39, Chapter IV, 3.2, Thm 8]. □

If a smooth projective variety X over a number field k satisfies the Hasse principle, it can be easier to check whether $X(k)$ is nonempty. Namely, checking whether $X(\mathbb{A}_k)$ is nonempty is a finite process [4, Page 10].

If a tool helps to show that the Hasse principle fails for a given variety, we speak of an *obstruction* to the Hasse principle. The method we develop in the next section using Brauer groups, can lead to an obstruction that we refer to as the Brauer-Manin obstruction. When we work out an example of this in the last section, we often work with rational points over $\mathbb{Q}_p$ by relating them to rational points over $\mathbb{Z}/p^n\mathbb{Z}$ for some $n \geq 1$. The next proposition allows us to do this.

Proposition 7.5.
Let X be a projective variety defined by polynomials with coefficients in $\mathbb{Z}$. If $X(\mathbb{Z}/p^n\mathbb{Z})$ is empty for some $n \geq 1$, then $X(\mathbb{Q}_p)$ is empty.

Proof. Suppose $P = (x_0 : \ldots : x_k)$ is a point in $X(\mathbb{Q}_p)$. By remark 1.89, each coordinate can be re-scaled to a p-adic integer by multiplying it with a power of p. Multiplying the homogeneous coordinates by a sufficiently high power of p gives homogeneous coordinates in $\mathbb{Z}_p$ for P. So P defines a point in $X(\mathbb{Z}_p)$. Reducing the equations modulo $p^n\mathbb{Z}_p$, still guarantees a point in $X(\mathbb{Z}_p/p^n\mathbb{Z}_p)$. By proposition 1.86, this gives a point in $X(\mathbb{Z}/p^n\mathbb{Z})$. Hence, we have a contradiction. □

As an example, consider the projective conic $x^2 + y^2 = 3z^2$. One can check that $X(\mathbb{Z}/4\mathbb{Z})$ is empty [4, Ex 2.1.2]. Therefore, by the proposition, $X(\mathbb{Q}_2)$ is empty as well.

Similarly, one can show that an integer $a \in \mathbb{Z}$ is not a square in $\mathbb{Q}_p$ by showing it is not a square in $\mathbb{Z}/p^n\mathbb{Z}$ for some $n \geq 1$: If the equation $x = a^2$ has no solutions over $\mathbb{Z}/p^n\mathbb{Z}$, the proposition implies it has no solution over $\mathbb{Q}_p$.

7.2 The Brauer-Manin obstruction

Let X denote a smooth, projective, geometrically irreducible variety over a field k. We first define a map that evaluates classes in $\mathrm{Br}(X)$ at a point:

Proposition 7.6. [4, Page 144]
Let $\ell \supset k$ be a field extension. For each $P \in X(\ell)$, there is a group homomorphism

$$\mathrm{ev}_P \colon \mathrm{Br}(X) \to \mathrm{Br}(\ell)$$

induced by the ring homomorphism $\mathcal{O}_{X,P} \to \ell$ that evaluates $f/g \in \mathcal{O}_{X,P}$ at P. For a class $\alpha \in \mathrm{Br}(X)$, we denote its image $\mathrm{ev}_P(\alpha)$ also by $\alpha(P)$.

Proof. The evaluation homomorphism $\mathcal{O}_{X,P} \to \ell$ induces a group homomorphism

$$\mathrm{ev}_P \colon \mathrm{Br}(\mathcal{O}_{X,P}) \to \mathrm{Br}(\ell)$$

by proposition 5.24. We claim that this map restricts to a group homomorphism

$$\mathrm{ev}_P \colon \mathrm{Br}(X) \to \mathrm{Br}(\ell).$$

In the case $P \in X(\overline{k})$, $\mathrm{Br}(X)$ is contained in the image of the embedding

$$\phi \colon \mathrm{Br}(\mathcal{O}_{X,P}) \hookrightarrow \mathrm{Br}(\kappa(X))$$

as discussed in section 6.1. So we can restrict the map as follows:

$$\mathrm{Br}(X) \xhookrightarrow{\phi^{-1}} \mathrm{Br}(\mathcal{O}_{X,P}) \to \mathrm{Br}(\ell).$$

In the case $P \in X(\ell) \setminus X(\overline{k})$, we have $\mathcal{O}_{X,P} \cong \kappa(X)$, since at least one coordinate of P is transcendental over k, and hence every regular function $F/G \in \kappa(X)$ is such that $G(P) \neq 0$. So since $\mathrm{Br}(X)$ is a subgroup of $\mathrm{Br}(\kappa(X)) \cong \mathrm{Br}(\mathcal{O}_{X,P})$, we have a restriction coming from the natural inclusion of $\mathrm{Br}(X)$ into $\mathrm{Br}(\mathcal{O}_{X,P})$. □

Example 7.7.
Recall the example discussed in section 6.2 with the field extension $\ell := k_P = \mathcal{O}_{X,P}/I_P \supset \mathbb{Q}$. For a certain point $P \in X(\overline{\mathbb{Q}})$, we had a ring homomorphism

$$\begin{aligned} f \colon \mathcal{O}_{X,P} &\to k_P \\ \frac{g}{h} &\mapsto \frac{g(P)}{h(P)} + I_P. \end{aligned}$$

It induced a group homomorphism

$$\mathrm{Br}(X) \to \mathrm{Br}(k_p)$$

which sends the class of the quaternion algebra $\mathcal{A} = \left(5, \frac{u}{u+v}\right)$ to the class of the quaternion algebra $\left(5 + I_P, \frac{u(P)}{u(P)+v(P)} + I_P\right)$.

Let k be a number field. Recall that for each place v of k, we can see k as a subfield of k_v via the injection $k \hookrightarrow k_v$. By proposition 7.6, we thus obtain a group homomorphism $\mathrm{Br}(X) \to \mathrm{Br}(k_v)$ that evaluates a class $\alpha \in \mathrm{Br}(X)$ at a point $P \in X(k_v)$ to get a class $\alpha(P) \in \mathrm{Br}(k_v)$.

From a different perspective, for each class $\alpha \in \mathrm{Br}(X)$, we have an evaluation map

$$\begin{aligned} X(k_v) &\to \mathrm{Br}(k_v) \\ P &\mapsto \alpha(P) \end{aligned}$$

which we denote by α. Recalling the Hasse invariant map $\mathrm{inv}_v \colon \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$ from section 4.3, we can pre-compose inv_v with α to obtain a map

$$X(k_v) \xrightarrow{\alpha} \mathrm{Br}(k_v) \xrightarrow{\mathrm{inv}_v} \mathbb{Q}/\mathbb{Z},$$

which we call the *local invariant map*. Proposition 7.3 gives $X(\mathbb{A}_k) = \prod_v X(k_v)$, so we can combine the local invariant maps of each place v to obtain a map

$$X(\mathbb{A}_k) \to \bigoplus_v \mathrm{Br}(k_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}.$$

We refer to this as the *adelic evaluation map*. It takes an adelic point $(P_v) \in X(\mathbb{A}_k)$ and maps it to $\sum_v \mathrm{inv}_v \alpha(P_v) \in \mathbb{Q}/\mathbb{Z}$.

Since $X(k)$ is a subset of each $X(k_v)$, we obtain a diagonal embedding $X(k) \hookrightarrow X(\mathbb{A}_k)$, which allows us to state another property:

Proposition 7.8. [4, Prop 13.1.4]
Let α be a class in $\mathrm{Br}(X)$. Then $X(k)$ lies in the kernel of the adelic evaluation map.

Proof. A proof can be found in [4, Prop 13.1.4], which uses the exact sequence of theorem 4.18. □

Definition 7.9.
Let α be a class in $\mathrm{Br}(X)$ and B a subset of $\mathrm{Br}(X)$. We define the sets

$$\begin{aligned} X(\mathbb{A}_k)^\alpha &\coloneqq \{(P_v) \in X(\mathbb{A}_k) : \sum_v \mathrm{inv}_v \alpha(P_v) = 0\}; \\ X(\mathbb{A}_k)^B &\coloneqq \{(P_v) \in X(\mathbb{A}_k) : \sum_v \mathrm{inv}_v \alpha(P_v) = 0 \text{ for all } \alpha \in B\}. \end{aligned}$$

If $B = \mathrm{Br}(X)$ we write $X(\mathbb{A}_k)^{\mathrm{Br}}$ instead of $X(\mathbb{A}_k)^B$.

By proposition 7.8, $X(k)$ lies in $X(\mathbb{A}_k)^\alpha$ for each class $\alpha \in \mathrm{Br}(X)$. As a consequence, we can show that $X(k)$ is empty by showing that $X(\mathbb{A}_k)^B$ is empty for some subset $B \subset \mathrm{Br}(X)$, even if the set of adelic points $X(\mathbb{A}_k)$ is itself nonempty. This is the idea behind the Brauer-Manin obstruction, which is defined as follows:

Definition 7.10. (Brauer-Manin obstruction)
Let X be a smooth, projective, geometrically irreducible variety over a number field k. Let B be a subset of $\mathrm{Br}(X)$. If $X(\mathbb{A}_k)^B$ is empty but $X(\mathbb{A}_k)$ is nonempty, we say there is a *Brauer-Manin obstruction to the Hasse principle* on X coming from B. In the case $B = \mathrm{Br}(X)$, we simply say there is a Brauer-Manin obstruction to the Hasse principle on X.

So by finding $X(\mathbb{A}_k)^B$ for an effective $B \subset \mathrm{Br}(X)$, one can obtain a Brauer-Manin obstruction on the given variety. Finding a small B that does the job is a different problem. However, for some varieties, it is even possible to determine $X(\mathbb{A}_k)^B$ with $B = \mathrm{Br}(X)$ [4, Page 167]. In the next section we find $X(\mathbb{A}_k)^\alpha$ for a (given) effective $\alpha \in \mathrm{Br}(X)$ to show there is a Brauer-Manin obstruction. But first, we require one more property of the map α:

Proposition 7.11. [4, Prop 13.1.9]
Let X be a smooth variety over a local field k_v and α a class in $\mathrm{Br}(X)$. The evaluation map $\alpha\colon X(k_v) \to \mathrm{Br}(k_v)$ is locally constant for the analytic topology on $X(k_v)$, that is, the topology induced by the topology on k_v combined with the product topology.

7.3 Application to a del Pezzo surface of degree 4

In this section we revisit our del Pezzo surface from example 1.64 and show there is a Brauer-Manin obstruction on this surface following the procedure in [4, Example 13.2.1].

Recall that the surface $X \subset \mathbb{P}^4_{\mathbb{Q}}$ over $\mathbb{Q}$ is defined by the equations

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

In section 6.2 we also defined the quaternion algebra

$$\mathcal{A} \coloneqq \left(5, \frac{u}{u+v}\right)$$

over $\kappa(X)$ and showed that its class is an element of $\mathrm{Br}(X)$. Let us denote this class by α. We show that there is a Brauer-Manin obstruction on X coming from α. In other words, we show

$$X(\mathbb{A}_\mathbb{Q})^\alpha = \{(P_v) \in X(\mathbb{A}_\mathbb{Q}) : \sum_v \mathrm{inv}_v\, \alpha(P_v) = 0\}$$

is empty while $X(\mathbb{A}_\mathbb{Q})$ is nonempty.

To show $X(\mathbb{A}_\mathbb{Q})^\alpha$ is empty, we determine the value of the local invariant map $\mathrm{inv}_v\, \alpha(P_v)$ at each place v of $\mathbb{Q}$ for an arbitrary adelic point $(P_v) \in X(\mathbb{A}_\mathbb{Q})$. The sum of these values should then be nonzero for $X(\mathbb{A}_\mathbb{Q})^\alpha$ to be empty. We look at different places v seperately:

$\mathbf{v = \infty}$, the real place

Here, $\mathbb{Q}_p = \mathbb{R}$. Let $P = (u_0 : v_0 : x_0 : y_0 : z_0)$ be a point in $X(\mathbb{R})$ such that u_0 and v_0 are nonzero. The ring homomorphism

$$f\colon \mathcal{O}_{X,P} \to \mathbb{R}$$

which maps $\frac{u}{u+v}$ to $\frac{u_0}{u_0+v_0}$ induces, by proposition 7.6, a group homomorphism

$$\mathrm{ev}_P\colon \mathrm{Br}(X) \to \mathrm{Br}(\mathbb{R}).$$

This maps α to $\alpha(P)$, the class of the quaternion algebra

$$\left(f(5), f\left(\frac{u}{u+v}\right)\right)_\mathbb{R} = \left(5, \frac{u_0}{u_0+v_0}\right)_\mathbb{R}$$

by propositions 5.23 and 5.24.

Since 5 is a square in $\mathbb{R}$, proposition 3.5 gives that this quaternion algebra is isomorphic to

$$\left(1, \frac{u_0}{u_0 + v_0}\right)$$

which is then isomorphic to $M_2(\mathbb{R})$ by example 3.4. So $\alpha(P)$ is the identity element in $\mathrm{Br}(\mathbb{R})$, which gives $\mathrm{inv}_\infty \alpha(P) = 0$. Because the map $\alpha\colon X(\mathbb{R}) \to \mathrm{Br}(\mathbb{R})$ is locally constant and the set of points P with u_0 and v_0 nonzero is dense in $X(\mathbb{R})$, it follows that $\alpha(P) = [\mathbb{R}]$ for all $P \in X(\mathbb{R})$, and, thus, we also have $\mathrm{inv}_\infty \alpha(P) = 0$ for all $P \in X(\mathbb{R})$.

v corresponding to an odd prime p such that 5 is a square in $\mathbb{Q}_\mathbf{p}$

The same argument as above shows that $\mathrm{inv}_p \alpha(P) = 0$ for all $P \in X(\mathbb{Q}_p)$.

v corresponding to an odd prime p $\neq$ 5 such that 5 is not a square in $\mathbb{Q}_\mathbf{p}$

The assumption that 5 is not a square in $\mathbb{Q}_p$ implies that it is also not a square in $\mathbb{Z}/p\mathbb{Z}$: Suppose $F = x^2 - 5$ has a solution in $\mathbb{Z}/p\mathbb{Z}$, i.e., there exists an $a_1 \in \mathbb{Z} \subset \mathbb{Z}_p$ such that $F(a_1) \equiv 0 \bmod p$. Since $p \neq 2$, $F'(a_1) = 2a_1 \not\equiv 0 \bmod p$. Then Hensel's lemma guarantees the existence of an element $a \in \mathbb{Z}_p \subset \mathbb{Q}_p$ such that $F(a) = 0$, so a is a root of 5 in $\mathbb{Q}_p$, which is a contradiction.

Now let P be a point in $X(\mathbb{Q}_p)$ and choose homogeneous coordinates $(u_0 : v_0 : x_0 : y_0 : z_0)$ that all lie in $\mathbb{Z}_p$ and are not all divisible by p. We can do this by multiplying the coordinates with a power of p:

- If all coordinates satisfy $v_p(\cdot) > 0$ and m is the smallest of the p-adic valuations of the coordinates, multiply all coordinates by p^{-m} to obtain at least one coordinate with $v_p(\cdot) = 0$ (so it is not divisible by p).
- If $n \in \mathbb{Z} < 0$ is the smallest integer such that one of the coordinates has $v_p(\cdot) = n$, multiply all coordinates by p^{-n} so that all coordinates lie in $\mathbb{Z}_p$ and at least one has $v_p(\cdot) = 0$.

Substituting the coordinates of P into the equations defining X and reducing both equations modulo p, we see that u_0 and v_0 cannot both be divisible by p: Otherwise,

$$\begin{cases} 0 \equiv x_0^2 - 5y_0^2 \bmod p \\ 0 \equiv x_0^2 - 5z_0^2 \bmod p, \end{cases}$$

where x_0, y_0, z_0 not all congruent to $0 \bmod p$. Then at least one of x_0/y_0 and x_0/z_0 is a square root of 5 in $\mathbb{Z}/p\mathbb{Z}$, which contradicts with our earlier observation.

The same argument shows at least one of $u_0 + v_0$ and $u_0 + 2v_0$ is not divisible by p. Remember that all of u_0, v_0, $u_0 + v_0$, $u_0 + 2v_0$ are in $\mathbb{Z}_p$. Any of them being not divisible by p implies it is an element of the group of units $\mathbb{Z}_p^\times$. Therefore, at least one of the expressions

$$b = \frac{u_0}{u_0 + v_0}, \quad \frac{v_0}{u_0 + v_0}, \quad \frac{u_0}{u_0 + 2v_0}, \quad \frac{v_0}{u_0 + 2v_0}$$

is such that $b \in \mathbb{Z}_p^\times$. Taking that b, the quaternion algebra $(5, b)$ over $\mathbb{Q}_p$ has its class in $\mathrm{Br}(\mathbb{Q}_p)$ equal to $\alpha(P)$. This is because, as shown in section 6.2, the quaternion algebra $\mathcal{A}$ over $\kappa(X)$ also has four different representations, all isomorphic:

$$\left(5, \frac{u}{u+v}\right), \quad \left(5, \frac{v}{u+v}\right), \quad \left(5, \frac{u}{u+2v}\right), \quad \left(5, \frac{v}{u+2v}\right).$$

So evaluating the class α of the right expression of $\mathcal{A}$ at P gives the class $\alpha(P)$ of the quaternion algebra $(5, b)$ for our choice of b.

Since 5 and b are both in $\mathbb{Z}_p^\times$ (note that 5 is not divisible by p), proposition 4.20 (i) gives the Hilbert symbol $(5,b)_p = 1$. Then proposition 4.21 gives $\mathrm{inv}_p\,\alpha(P) = 0$. Note that P was taken to be arbitrary, so this holds for all $P \in X(\mathbb{Q}_p)$.

v corresponding to the prime p = 2

Let P be a point in $X(\mathbb{Q}_2)$ and choose homogeneous coordinates $(u_0 : v_0 : x_0 : y_0 : z_0)$ that all lie in $\mathbb{Z}_2$ and are not all divisible by 2. Substituting the coordinates of P into the equations defining X, we reduce both equations modulo 8. Again we aim to show that u_0 and v_0 cannot both be divisible by 2.

Suppose they are both divisible by 2. Then each of u_0 and v_0 is congruent to one of

$$\{0 \bmod 8, 2 \bmod 8, 4 \bmod 8, 6 \bmod 8\}.$$

It follows that at least one of u_0v_0 and $(u_0+v_0)(u_0+2v_0)$ is congruent to $0 \bmod 8$. So, at least one of $x_0^2 - 5y_0^2$ and $x_0^2 - 5z_0^2$ is congruent to $0 \bmod 8$. Without loss of generality, assume the first is the case. The only solutions $(x_0 \bmod 8, y_0 \bmod 8)$ to $x_0^2 - 5y_0^2 \equiv 0 \bmod 8$ are

$$\{(0,0),(0,4),(2,2),(2,6),(4,0),(4,4),(6,2),(6,6)\}.$$

So all of u_0, v_0, x_0, y_0 are divisible by 2. This gives that z_0 is also divisible by 2, but this contradicts our choice of coordinates for P.

So at least one of u_0 and v_0 is not divisible by 2. A very similar argument shows at least one of u_0+v_0 and u_0+2v_0 is not divisible by 2. Just as in the previous part, at least one of the expressions

$$b = \frac{u_0}{u_0+v_0}, \quad \frac{v_0}{u_0+v_0}, \quad \frac{u_0}{u_0+2v_0}, \quad \frac{v_0}{u_0+2v_0}$$

is such that $b \in \mathbb{Z}_2^\times$. Taking that b again, the quaternion algebra $(5,b)$ over $\mathbb{Q}_2$ has its class in $\mathrm{Br}(\mathbb{Q}_2)$ equal to $\alpha(P)$. Since 5 and b are both in $\mathbb{Z}_2^\times$, proposition 4.20 (ii) gives

$$(5,b)_2 = (-1)^{\epsilon(5)\epsilon(b)} = (-1)^{0\epsilon(b)} = 1,$$

after which proposition 4.21 again yields $\mathrm{inv}_2\,\alpha(P) = 0$.

v corresponding to the prime p = 5

For this final place, we start with the same setting: Let P be a point in $X(\mathbb{Q}_5)$ and choose homogeneous coordinates $(u_0 : v_0 : x_0 : y_0 : z_0)$ that all lie in $\mathbb{Z}_5$ and are not all divisible by 5. Substituting the coordinates of P into the equations defining X we reduce both equations modulo 5:

$$\begin{cases} u_0v_0 \equiv x_0^2 \bmod 5 \\ (u_0+v_0)(u_0+2v_0) \equiv x_0^2 \bmod 5. \end{cases} \tag{3}$$

The equation $u_0v_0 \equiv (u_0+v_0)(u_0+2v_0)$ has the following solutions $(u_0 \bmod 5, v_0 \bmod 5)$:

$$A \coloneqq \{(0,0),(1,1),(2,2),(3,3),(4,4)\}, \qquad B \coloneqq \{(1,3),(2,1),(3,4),(4,2)\}.$$

The solutions in B give that $x_0^2 \equiv u_0v_0$ is congruent to either $2 \bmod 5$ or $3 \bmod 5$. But these are not squares in $\mathbb{Z}/5\mathbb{Z}$, so these choices for u_0 and v_0 do not give solutions for our system (3). The solutions in A do work.

Let us look more carefully at the solution $u_0 \equiv v_0 \equiv x_0 \equiv 0 \bmod 5$. This means all of u_0, v_0, x_0 are divisible by 5. Then, each of u_0v_0, $(u_0+v_0)(u_0+2v_0)$, and x_0^2 is divisible by 25, so reducing our original system of equations defining X modulo 25 gives

$$\begin{cases} 0 \equiv -5y_0^2 \bmod 25 \\ 0 \equiv -5z_0^2 \bmod 25. \end{cases}$$

This implies that both y_0 and z_0 are also divisible by 5, but this contradicts our choice of coordinates of P again. So $u_0 \equiv v_0 \equiv x_0 \equiv 0 \bmod 5$ does not give a solution to (3) coming from $P \in X(\mathbb{Q}_5)$.

For all other solutions $(u_0 \bmod 5, v_0 \bmod 5, x_0 \bmod 5)$ to (3), we have that $u_0 \equiv v_0 \equiv \pm x_0^2 \bmod 5$. Any choice for b from

$$\frac{u_0}{u_0+v_0}, \quad \frac{v_0}{u_0+v_0}, \quad \frac{u_0}{u_0+2v_0}, \quad \frac{v_0}{u_0+2v_0}$$

gives $b = \frac{1}{2} \equiv 3 \bmod 5$ or $b = \frac{1}{3} \equiv 2 \bmod 5$. So b is not divisible by 5 and hence an element in $\mathbb{Z}_5^\times$. The Legendre symbols $\left(\frac{2}{5}\right)$ and $\left(\frac{3}{5}\right)$ both equal -1 since 2 and 3 are non-squares in $\mathbb{Z}/5\mathbb{Z}$. So using the formula from proposition 4.20 (i) gives

$$(5, b)_5 = (5^1 \cdot 1, 5^0 \cdot b) = (-1)^0 \left(\frac{5}{5}\right)^0 \left(\frac{3}{5}\right)^1 = -1.$$

In this case, proposition 4.21 gives $\mathrm{inv}_5(P) = \frac{1}{2}$.

Conclusion

Summing all values of $\mathrm{inv}_v \alpha(P_v)$ at each place v of $\mathbb{Q}$ yields $\sum_v \mathrm{inv}_v \alpha(P_v) = \frac{1}{2}$. We thus conclude $X(\mathbb{A}_\mathbb{Q})^\alpha$ is empty. In [4, Example 2.3.5], the authors state that $X(\mathbb{A}_\mathbb{Q})$ is nonempty:

- $(10 : -10 : 5 : 5 : \sqrt{5})$ defines a point in $X(\mathbb{R})$ and $X(\mathbb{Q}_p)$ for each prime p such that 5 is a square in $\mathbb{Q}_5$;
- For primes $p \neq 2$ such that 5 is not a square in $\mathbb{Q}_p$, one of $(1 : 1 : 1 : 0 : \sqrt{-1})$ and $(5 : 0 : 0 : 0 : \sqrt{-5})$ gives a point in $X(\mathbb{Q}_p)$;
- And $(-25 : 5 : 0 : 5 : 2\sqrt{-15})$ defines a point in $X(\mathbb{Q}_2)$.

We have thus obtained a Brauer-Manin obstruction to the Hasse principle on our surface X, hence, proving that X has rational points over every completion $\mathbb{Q}_v$, but not over $\mathbb{Q}$.

Discussion

One may wonder whether the same method works if the 5 in the equations defining X is replaced by another odd prime q. In that case, taking α to be the class of the algebra $(q, \frac{u}{u+v})$ gives the same results for the first cases treated above: For any place v corresponding to an odd prime unequal to q (including the real place), the same arguments show that $\mathrm{inv}_v \alpha(P_v) = 0$ for any $P_v \in X(\mathbb{Q}_v)$.

For the place v corresponding to the prime 2, the same argument works if and only if q is not congruent to $1 \bmod 8$. This is because the equation $x_0^2 - q y_0^2 \equiv 0 \bmod 8$ also has odd solutions if $q \equiv 1 \bmod 8$, but only even solutions if $q \equiv 3$, 5, or 7. So for example, the argument does not work for the prime $q = 17$.

Finally, for the place v corresponding to the prime q, the same argument works only if the equation

$$u_0 v_0 \equiv (u_0 + v_0)(u_0 + 2v_0) \mod q$$

has a nonzero solution. So for the primes 3, 7, and 11, it does not work. But in this case, when there is only the zero solution, it follows that $X(\mathbb{Z}/q\mathbb{Z})$ is empty, implying that $X(\mathbb{Q}_q)$ is empty as well. Then X misses a local point and therefore also has no global points, so it is useless to check for a Brauer-Manin obstruction on X.

Taking the prime $q = 13$, it could work: q is not congruent to $1 \bmod 8$ and the equation

$$u_0 v_0 \equiv (u_0 + v_0)(u_0 + 2v_0) \bmod 13$$

does have nonzero solutions. Indeed, Colliot-Thélène pointed out that when the 5 is replaced by 13, the variety X is a counterexample to the Hasse principle [41, Page 169].

In [21], the authors considered the more general surface $S \coloneqq S^{D;A,B}$ over a field k defined by the equations

$$\begin{cases} uv = x^2 - Dy^2 \\ (u + Av)(u + Bv) = x^2 - Dz^2 \end{cases}$$

for $A, B, D \in k$. If S is smooth, it is a del Pezzo surface of degree 4, and, under a list of extra conditions, it is a counterexample to the Hasse principle [21, Thm 6.1]. Taking $D = 17$, $A = 9$, and $B = 11$, for example, these conditions are indeed satisfied, as shown in [21, Ex 6.3], so the surface S satisfies $S(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$ but $S(\mathbb{Q}) = \emptyset$.

8 Conclusion

This thesis provided definitions and examples of Brauer groups of fields, commutative rings, and smooth, geometrically irreducible varieties. Using this, the Brauer-Manin obstruction to the Hasse principle was introduced and applied to an example.

The Brauer group of a field was defined as the set of equivalence classes of finite dimensional central simple algebras. We have seen that each equivalence class can be represented by a division algebra, and that, if the field is of characteristic unequal to 2, the order 2 elements of its Brauer group can be classified by tensor products of quaternion algebras. Replacing central simple algebras by Azumaya algebras yielded a generalization of this definition as the Brauer group of a commutative ring. Finally, the Brauer group of a smooth, geometrically irreducible variety was defined as a subgroup of the Brauer group of its function field, consisting of the classes that lie in the image of the Brauer group of the local ring of the variety, at each point. An example with a del Pezzo surface illustrated the procedure for checking that a class of the Brauer group of the function field indeed lies in the Brauer group of the surface. This example also helped to show there is a Brauer-Manin obstruction on the surface, proving that the surface lacks a global point although it has local points everywhere.

For further research it would be interesting to study how to determine the full Brauer group of the del Pezzo surface considered in this thesis, as well as to look at other examples of varieties for which there might be a Brauer-Manin obstruction. A conjecture proposed by Colliot-Thélène and Sansuc suggests that for any del Pezzo surface, failure of the Hasse principle can always be detected by a Brauer-Manin obstruction [6]. Further investigation into why this theory appears plausible would be an interesting next project.

Lastly, the author is interested in the choice of an effective element in the Brauer group of a variety for showing that there is a Brauer-Manin obstruction. For the particular example discussed in this thesis, the class of the algebra $(5, f)$ with rational function $f = u/u + v$ turned out to be effective, and this choice of f was deliberate, as can be understood from [41, Page 174]. It would be worthwhile to study how this algebra was obtained and guaranteed to be successful. In its complete formulation, Manin's method only requires the algebraic geometer to consider a finite amount of algebras for finding a Brauer-Manin obstruction [41, Page 171]. To be able to study this method in its totality, however, some understanding of cohomology is needed and it therefore presents an appealing opportunity for future exploration.

References

[1] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley series in mathematics. Addison-Wesley Publishing Company, 1969.

[2] M. Auslander and O. Goldman. The Brauer group of a commutative ring. *Transactions of the American Mathematical Society*, 97(3):367–409, 1960.

[3] R. Brauer. Über die algebraische Struktur von Schiefkörpern. *Journal für die reine und angewandte Mathematik*, 1932(166):241–248, 1932.

[4] M. Bright, T. Damiano, and R. van Luijk. Geometry and Arithmetic of Surfaces. `http://homepages.warwick.ac.uk/~maskal/surfaces/2021-01-03_surfaces.pdf`, 2021.

[5] C. Chevalley and E. Warning. Bemerkung zur vorstehenden Arbeit. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 11, pages 76–83. Springer, 1935.

[6] J.-L. Colliot-Thélène and J.-J. Sansuc. La descente sur les variétés rationnelles, II. *Duke Mathematical Journal*, 54(2):375 – 492, 1987.

[7] K. Conrad. Quaternion algebras. `https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf`.

[8] K. Conrad. Selmer's example. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf`.

[9] K. Conrad. Tensor products. `https://kconrad.math.uconn.edu/blurbs/linmultialg/tensorprod.pdf`.

[10] B. Edixhoven, D. Holmes, M. Kool, and L. Taelman. Algebraic Geometry, 2022.

[11] K. Erdmann and T. Holm. *Algebras and Representation Theory*. Springer, 2018.

[12] B. Farb and R. Dennis. *Noncommutative Algebra*, volume 144. Springer Science & Business Media, 1993.

[13] H. Frobenius. Über lineare Substitutionen und bilineare formen. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1878(84):1–63, 1878.

[14] W. Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*, volume 54. Addison-Wesley Publishing Company, 2008.

[15] A. Gathmann. Commutative Algebra. `https://agag-gathmann.math.rptu.de/class/commalg-2013/commalg-2013.pdf`, 2013.

[16] A. Gathmann. Algebraic Geometry. `https://agag-gathmann.math.rptu.de/class/alggeom-2021/alggeom-2021.pdf`, 2021.

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

[18] F.Q. Gouvêa. *p-adic Numbers*. Springer, 2020.

[19] A. Grothendieck. Le groupe de Brauer, I, II, III. *Dix exposés sur la cohomologie des schémas*, 3(46-66):15, 1968.

[20] K. Hensel. *Theorie der algebraischen Zahlen*, volume 1. B.G. Teubner, 1908.

[21] J. Jahnel and D. Schindler. Del Pezzo surfaces of degree four violating the Hasse principle are Zariski dense in the moduli scheme. *Annales de l'Institut Fourier*, 67(4):1783–1807, 2017.

[22] T.Y. Lam. *A First Course in Noncommutative Rings*. Graduate Texts in Mathematics. Springer New York, 2012.

[23] S. Lang. On Quasi Algebraic Closure. *Annals of Mathematics*, 55(2):373–390, 1952.

[24] J.H. Maclagan Wedderburn. A theorem on finite algebras. *Transactions of the American Mathematical Society*, 6(3):349–352, 1905.

[25] J.H. Maclagan Wedderburn. On hypercomplex numbers. *Proceedings of the London Mathematical Society*, 2(1):77–118, 1908.

[26] Y.I. Manin. Le groupe de Brauer–Grothendieck en géométrie diophantienne. *Actes du Congrès International des Mathématiciens*, 1:401–411, 1971.

[27] A.S. Merkurjev. On the norm residue symbol of degree 2. In *Doklady Akademii Nauk*, volume 261, pages 542–547. Russian Academy of Sciences, 1981.

[28] J.S. Milne. Algebraic Number Theory (v3.08). `www.jmilne.org/math/`, 2020.

[29] J.S. Milne. Class Field Theory (v4.03). `www.jmilne.org/math/`, 2020.

[30] V. Mitankin and C. Salgado. Rational points on del Pezzo surfaces of degree four. *International Journal of Number Theory*, 18(09):2099–2127, 2022.

[31] R.A. Morris. On the Brauer group of Z. *Pacific Journal of Mathematics*, 39(3):619–630, 1971.

[32] J. Neukirch. *Algebraic Number Theory*, volume 322. Springer Berlin, Heidelberg, 1999.

[33] A. Ostrowski. Über einige Lösungen der Funktionalgleichung $\psi(x) \cdot \psi(x) = \psi(xy)$. *Acta Mathematica*, 41:271 – 284, 1916.

[34] M.A. Rieffel. A general Wedderburn theorem. *Proceedings of the National Academy of Sciences*, 54(6):1513–1513, 1965.

[35] S. Roman. *Advanced Linear Algebra*, volume 135. Springer Science & Business Media, 1992.

[36] J. Rotman. *Advanced Modern Algebra*, volume 114. American Mathematical Society, 2003.

[37] I. Schur. Neue begründung der theorie der gruppencharaktere. In *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, pages 406–432. Deutsche Akademie der Wissenschaften zu Berlin, 1905.

[38] E.S. Selmer. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Mathematica*, 85:203 – 362, 1951.

[39] J.-P. Serre. *A Course in Arithmetic*, volume 7. Springer Science & Business Media, 1996.

[40] The Stacks Project Authors. Stacks project. `https://stacks.math.columbia.edu`, 2018.

[41] H.P.F. Swinnerton-Dyer and B.J. Birch. The Hasse problem for rational surfaces. *Journal für die reine und angewandte Mathematik*, 0274_0275:164–174, 1975.

[42] J. Top. Advanced Algebraic Structures, 2017.

[43] C.C. Tsen. Divisionsalgebren über Funktionenkörpern. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, pages 335–339, 1933.

[44] R. van Luijk. Lecture notes on del Pezzo Surfaces. `https://homepages.warwick.ac.uk/~maseap/arith/notes/delpezzo.pdf`.

[45] A. Várilly-Alvarado. Arithmetic of del Pezzo surfaces. In *Birational geometry, rational curves, and arithmetic*, pages 293–319. Springer, 2013.

[46] E. Witt. Über ein Gegenbeispiel zum Normensatz. *Mathematische Zeitschrift*, 39:462–467, 1935.