THE BRAUER-MANIN OBSTRUCTION TO THE HASSE PRINCIPLE

Boris Lerner

Supervisor: Dr Daniel Chan

School of Mathematics,
The University of New South Wales.

November 2007

Submitted in partial fulfillment of the requirements of the degree of
Bachelor of Science with Honours

Acknowledgements

My greatest gratitude goes out to my supervisor Dr Daniel Chan. He helped me pick the topic for this thesis which turned out to be extremely interesting, helped me with the writing of this thesis and most importantly never refused to spend time with me to help me learn mathematics. I thank him deeply for this.

I would to also like thank my high school maths teacher Ian Denton for getting me interested in mathematics to begin with. Similarly, a special thanks goes to Dr Ian Doust who, in response to my email requesting permission to avoid doing any algebra courses replied: "I'm not going to let you out of here with a pure maths degree without seeing some proper group theory!". I hope this thesis shows that I have learnt the basics of group theory, and Ian will let me graduate.

Thank you to Kenneth and Hugo, for helping me throughout this year, and thank you to Anna for being supportive and putting up with me. Special thanks also goes to my family.

Contents

Introduction

A Diophantine problem over $\mathbb{Z}$ is concerned with finding rational or integral solutions to polynomial equations with coefficients in $\mathbb{Z}$. These problems have been studied by mathematicians since the third century and some of the most famous problems of all time, for example Fermat's Last Theorem, have been of this kind. In general, solving a Diophantine problem is extremely hard and in fact Hilbert's tenth problem[1] was to find an algorithm that could, in a finite number of steps, determine whether a given Diophantine equation had an integral solution. In 1970, Matiyasevich's theorem showed that no such algorithm can exist. However, it is crucial to note that this does not imply that an algorithm can not be found that finds *rational* solutions to a general Diophantine equation. The existence of such an algorithm is still an open problem today.

Hilbert's problem motivated much research in solving Diophantine problems. One obvious way to prove that a Diophantine problem does not have an integral solution is to show it does not have a solution modulo p^n for some prime p and positive integer n. This is easily generalised to saying that a Diophantine problem does not have a rational solution if it does not have one in any completions $\mathbb{Q}_v$ of $\mathbb{Q}$.[2] It is thus natural to ask the converse of this: if we know that a Diophantine problem has a solution over all $\mathbb{Q}_v$ does that mean it has one over $\mathbb{Q}$? In more modern language this could be rephrased as follows: given a variety V, if $V(\mathbb{Q}_v) \neq \varnothing$ for all $\mathbb{Q}_v$ does that imply that $V(\mathbb{Q}) \neq \varnothing$? If the implication is true then the variety is said to verify the **Hasse principle**. Advancements in algebraic number theory caused the Hasse principle to be restated more generally, involving not necessarily looking for rational solutions but solutions in an algebraic number field; I will not go into this in this thesis, but I will occasionally bring this point up later. Of course it is well known, and many examples are available, that not all varieties verify the Hasse principle. The purpose of this thesis is to classify most of the currently known obstructions.

The remarkable result, which has been the driving force behind much of the research in this area, is that determining whether $V(\mathbb{Q}_v)$ is empty or not for all $\mathbb{Q}_v$, is a problem that can always be solved in a finite number of steps. The main reason for this, is that $V(\mathbb{Q}_v)$ can only be empty for a finite number of completions. Further, determining whether $V(\mathbb{Q})$ is empty for a particular completion, is also a finite-step process.

The fact that $V(\mathbb{Q}_v)$ is almost always non-empty is a consequence of the Weil conjectures (which were proven by 1974 thanks to the works of Alexander Grothendieck

[1] In 1900 Hilbert put forth 23 problems, unsolved at that time. He presented 10 of them at the International Congress of Mathematicians in Paris. Solving Diophantine problems was number 10 on the list, but did not get presented at the conference.

[2] See Chapter 1 for the formal definition.

and his students), but it also follows from weaker results known much earlier. As a result, finding varieties that verify the Hasse principle, and consequently classifying ones that do not, is seen as a crucial necessity in the study of Diophantine problems. For example, the Hasse-Minkowski Theorem states that all quadratic forms obey the Hasse principle, which implies that to determine whether a quadratic form has a rational solution, it sufficient to check whether it has a solution in all completions of $\mathbb{Q}$.

In first half of the 20th century, many examples of obstructions to the Hasse principle began to emerge. However, no connection was evident between them, and it was the work of Manin who, in 1970, published the Brauer-Manin obstruction to the Hasse principle and showed that all obstructions known at that time were examples of this type. The purpose of this thesis is to describe the Brauer-Manin obstruction. There was little hope that all obstructions to the Hasse principle would be incorporated by the Brauer-Manin obstruction, however it was only in 1999 (see [Sko99]) that an obstruction not of the Brauer-Manin type were constructed.

The motivation behind this thesis is the paper [Pey05] published by Peyre, in which he outlines the Brauer-Manin obstruction to the Hasse principle. The thesis is structured in such a way that the reader learns precisely the mathematics required to understand those obstructions which fall under this framework.

0.1 Outline

In Chapter 1, I will introduce the field of p-adic numbers, which will form the completions of $\mathbb{Q}$. The main text I used for this chapter is [Ser73]. However a very different, more analytic approach can also be found in [Gou97]. We will also prove Hensel's Lemma which will allow us to solve polynomial equations over these fields.

In Chapter 2, I will introduce the Hilbert symbol and show how various properties of it, in particular a certain product formula, can be used to construct obstructions to the Hasse principle. The main reference I used for this chapter is [Ser73] and the article which motivated this thesis [Pey05]. In fact, in the last section of this chapter I give an example of an obstruction to the Hasse principle which is a a generalisation of the example given in [Pey05]. This example can not be found elsewhere in literature.

The remainder of the thesis, concentrates on understanding the *fundamental exact sequence of global class field theory*

$$0 \longrightarrow \mathrm{Br}(\mathbb{Q}) \longrightarrow \oplus_v \mathrm{Br}(\mathbb{Q}_v) \stackrel{\Sigma_v \mathrm{inv}_v}{\longrightarrow} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

The reason we are interested in this is, as we shall see, that hidden in this exact sequence, is the product formula which gave us the previous obstruction. Thus using this sequence we can formulate a more general criterion for a variety to be an obstruction to the Hasse principle, known as the Brauer-Manin obstruction. (It was in fact Manin, who realised how to group all the obstructions known at the time under this one framework.)

In chapter 3, I will introduce the Brauer group which as we can see appears in the exact sequence above. The main reference I used for this was [FD93]. A more comprehensive (and harder to follow) treatment of central simple algebras and the

Brauer group can be found in [Row88a] and [Row88b] (I have taken some of the proofs from there.)

In chapter 4 I will introduce homological algebra, which will give an alternate way of looking at the Brauer group of a field. A good reference to study this topic is [Har77] (this is the bible of algebraic geometry), however, the development of the theory which I give, is more general then what is found in this book. The main source I used to study homological algebra are lecture notes from university, and so I can not provide a reference. The section on Galois cohomology is covered well in [FD93].

Finally in Chapter 5, we combine all of our knowledge from the previous two chapters to prove the existence of the "invariant map" which appears in the exact sequence. Thus we will understand all the maps involved in the sequence, however, th exactness of this sequence is a very deep theorem in class field theory and I will not prove it. A great source to learn more about this topic, and class field theory in general is [Mil97]. Finally we will of course demonstrate how the exact sequence, does in fact generalise the product formula.

0.2 Assumed Knowledge

When writing this thesis I have assumed the reader has studied all the courses that I studied in UNSW. In order to understand the thesis in its entirety, the reader should know basic facts about groups, rings, modules, vector spaces, tensor products, some topology and elementary number theory. A slightly deeper understanding of Galois theory is required to fully understand some of the proofs. If the reader has not met these concepts before, and would still like to understand the content of this thesis (I must say I would feel rather honoured) then I advise to keep a copy of [Lan02] and [Art91] within arm's reach.

0.3 Notation

Most of the notation used in this thesis, is standard notation found in modern algebra books. Here is a list of (some) of the conventions and notation that I will use:

- $X := Y$ will mean X is defined to be Y or is equal to it by definition.
- $A \simeq B$ will mean A is isomorphic to B
- $A \sim B$ will denote A is equivalent to B under a pre-specified equivalence relation
- $[A]$ will denote the equivalence class of A under a pre-specified equivalence relation
- $M_1 \otimes_R M_2$ will denote the tensor product of two R-modules see page 12 of [FD93] for the definition
- $[V : k]$ will denote the dimension of a V as vector space over k
- $\mathcal{M}_n(R)$ will denote the algebra of $n \times n$ matrices with entries from R
- k^{al} will denote the algebraic closure of a field k.
- k^* will denote the group $k - \{0\}$ where k is a field.
- All rings have an identity element

I will usually re-iterate some of these points when they come up.

Chapter 1

Completions of $\mathbb{Q}$

The field of p-adic numbers arose naturally from number theory, or more specifically from the lifting theorem, which is an analogue of Newton's method, which gives a criterion for the existence of a solution to $f(x) \equiv 0 \,(\mathrm{mod}\, p^{n+1})$ given that we know one exists for $f(x) \equiv 0 \,(\mathrm{mod}\, p^n)$. The lifting theorem thus produced a sequence of numbers $\{x_n\}$ each of which was root of $f(x)$ modulo p^n with the extra property that $x_n \equiv x_{n-1} \,(\mathrm{mod}\, p^n)$. The problem was, that the sequence $\{x_n\}$ certainly did not need to converge to an element in $\mathbb{R}$ under the usual metric associated with it. The need for the sequence to converge motivated Kurt Hensel in 1902 to create a metric under which the sequence did converge in a certain extension of $\mathbb{Q}$. These extensions, together with this metric is what is called the field of p-adic numbers.

However, the construction of p-adic numbers that I give here, is slightly different, for we will not begin with a sequence of numbers in $\mathbb{Q}$ and then define a metric (and a space) such that the sequence converges. Our approach, will be much slicker, but less motivating at first. Of course we will show, that our treatment is the same as the one described above.

1.1 The Field of p-adic Numbers

We begin first by constructing the ring p-adic integers. Let p be a prime. We let $A_n := \mathbb{Z}/p^n\mathbb{Z}$ and define the map:

$$\begin{aligned} \phi_n \colon A_n &\longrightarrow A_{n-1} \\ x + p^n\mathbb{Z} &\longmapsto x + p^{n-1}\mathbb{Z} \end{aligned}$$

Thus we have the projective system:

$$\ldots \longrightarrow A_n \xrightarrow{\phi_n} A_{n-1} \xrightarrow{\phi_{n-1}} \ldots \longrightarrow A_2 \xrightarrow{\phi_2} A_1$$

Note that:

$$ker(\phi_n) = p^{n-1}A_n$$

Once we have a projective system, we can take its inverse limit, and get:

Definition 1.1.1. *The ring of* p**-adic integers** *is defined as:*

$$\mathbb{Z}_p := \varprojlim(A_n, \phi_n)$$

In other words, $\mathbb{Z}_p$ is a subring of $\prod_{n\geq 1} A_n$ consisting of elements which satisfy the property that if $x = (x_m)$ then $\phi_{n+1}(x_{n+1}) = x_n$ for all $n \geq 1$ (all operations are performed point-wise.)

Example 1.1.2. We can view elements of $\mathbb{Z}_p$ as formal Taylor series in p. Consider, for example, $q = \sum_{i=0}^{\infty} a_i p^i$ where $a_i \in \{0, 1, \ldots, p-1\}$. Then q represents an element of $\mathbb{Z}_p$ as as follows:

$$\cdots \longrightarrow \mathbb{Z}/p^3\mathbb{Z} \xrightarrow{\phi_3} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\phi_2} \mathbb{Z}/p\mathbb{Z}$$

$$\cdots \longmapsto a_0 + a_1 p + a_2 p^2 + p^3\mathbb{Z} \longmapsto a_0 + a_1 p + p^2\mathbb{Z} \longmapsto a_0 + p\mathbb{Z}$$

and thus q represents $([a_0], [a_0 + a_1 p], [a_0 + a_1 p + a_2 p^2], \ldots)$ where $[x]$ denotes the equivalence class of x. Conversely, it is easy to see that every element of $\mathbb{Z}_p$ can be represented in this way.

Note also that there is a natural inclusion map $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, mapping every integer into the p-adic integer whose n^{th}-component is the image of the integer in A_n.

Example 1.1.3. $59 = 2 + 1 \times 3 + 0 \times 3^2 + 2 \times 3^3$ and so the map $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ would send 59 to

$$([2], [5], [5], [59], [59], [59], \ldots)$$

Proposition 1.1.4. *Let $\epsilon_n : \mathbb{Z}_p \to A_n$ be the natural projection map. Then:*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\epsilon_n} A_n \longrightarrow 0$$

is an exact sequence of abelian groups.

Proof. Multiplication by p and hence p^n is injective, since if $x = (x_m)$ and $px = 0$ then $px_{m+1} = 0$ for all $m \geq 1$. Hence, x_{m+1} is of the form $p^m y_{m+1}$ with $y_{m+1} \in A_{m+1}$. However, $x_m = \phi_{m+1}(x_{n+1})$ which implies x_m is also divisible by p^m and is thus zero. Now to find $\ker(\epsilon_n)$. Clearly, $p^n\mathbb{Z}_p \subseteq \ker(\epsilon_n)$. Conversely, if $x = (x_m) \in \ker(\epsilon_n)$ then $x_n \equiv 0 \pmod{p^n}$ which implies $x_m = 0$ for $m < n$ and $x_m \equiv 0 \pmod{p^n}$ for $m \geq n$. Thus $x_m = p^n y_{m-n}$ for $m \geq n$. Now since $x_m \in A_m$ implies $y_{m-n} \in A_{m-n}$. However, since $A_{m-n} \simeq p^n\mathbb{Z}/p^m\mathbb{Z} \subset A_m$ the y_{m-n} define elements of A_m and since $\phi_n(y_j) = y_{j-1}$ for all j, if we let $y = (\ldots, \phi_n(y_1), y_1, y_2, \ldots) \in \mathbb{Z}_p$ then $p^n y = x$. □

Proposition 1.1.4 implies that $\mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$ and thus we can make an association between elements of one group and the other. We need this notion for Hensel's Lemma and its corollaries.

We would also like to have a notion of "distance" in $\mathbb{Z}_p$ so that we can talk about completions. We will thus now define a metric on $\mathbb{Z}_p$. I will use the standard notation of $\mathbb{F}_p$ to denote a field of p elements.

Proposition 1.1.5. (i) *$x \in \mathbb{Z}_p$ is invertible if and only if $p \nmid x$.*

(ii) *Let $\mathbb{U}_p$ denote all the units in $\mathbb{Z}_p$. Any $x \in \mathbb{Z}_p$, $x \neq 0$ can be written as $p^n u$ such that $n \geq 0$ and $u \in \mathbb{U}_p$.*

Proof. (i) Suppose $x \in \mathbb{Z}_p$ is invertible. Then, since multiplication is performed coordinate-wise, its image in $A_1 = \mathbb{F}_p$ is also invertible. This implies $p \nmid x$.

Conversely, suppose $p \nmid x$. This implies $x_n \notin pA_n$ for all n and thus the image of x_n in $\mathbb{F}_p$ is invertible. Thus there exists y such that $x_n y \equiv 1 \,(\mathrm{mod}\, p)$. I.e. $x_n y = 1 - pz$ for some $z \in A_n$. However:

$$\begin{aligned}(1-pz)(1+pz+\cdots+p^{n-1}z^{n-1}) &= 1\\ x_n y(1+pz+\cdots+p^{n-1}z^{n-1}) &= 1\end{aligned}$$

i.e. x_n is invertible.

(ii) Since $x \in \mathbb{Z}_p$ is not-zero, there exists a smallest n such that the image of the n^{th} component of x in A_n is non-zero. Then $x = p^n u$ with $p \nmid u$. By (i) this implies $u \in \mathbb{U}_p$.

□

Definition 1.1.6. *The value of n defined in part (ii) above, will be called the* **the p-adic valuation of** x *and will be denoted by $v_p(x)$. Put $v_p(0) = +\infty$.*

Note that $v_p : \mathbb{Z}_p \to \mathbb{N}$. Following on from this, for all $x \in \mathbb{Z}_p$, we can define:

$$|x|_p := e^{-v_p(x)}$$

called the **p-adic absolute value** of x. This turns $\mathbb{Z}_p$ into a complete metric space via

$$d_p(x,y) := |x-y|_p \qquad \text{for all } x, y \in \mathbb{Z}_p$$

We drop the p if it clear from the context.

Under this metric, $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. See [Ser73] page 12 for a proof. Also, numbers which have a higher power of p dividing into them (i.e. have a higher valuation) are considered smaller. Thus, it can easily be shown that series such as

$$1 + p + p^2 + p^3 \ldots$$

actually converge in $\mathbb{Z}_p$.

Corollary 1.1.7. *$\mathbb{Z}_p$ is a domain.*

Proof. Clearly the product of two elements in $\mathbb{U}_p$ is always non-zero. By the previous proposition every element in $\mathbb{Z}_p$ can be written in the form $p^n u$ with $u \in \mathbb{U}_p$. Proposition 1.1.4 guarantees that multiplication by p^n is injective and hence the result follows. □

Definition 1.1.8. *The* **field of p-adic numbers** *denoted by $\mathbb{Q}_p$ is fraction field of $\mathbb{Z}_p$.*

We can immediately see that $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$ and thus elements of $\mathbb{Q}_p$ can be thought of as simply Laurent series in p. We can easily extend the definition of $v_p(\cdot)$ to all of $\mathbb{Q}_p$, by defining $v_p(x)$ to be the unique integer such that $x = p^{v_p(x)}u$, where $u \in \mathbb{U}_p$. In fact, it is easy to see that if $\frac{a}{b} \in \mathbb{Q}_p$ with $a, b \in \mathbb{Z}_p$ then $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$. Consequently, we can now extend $d_p(\cdot,\cdot)$ to all of $\mathbb{Q}_p$ which turns it into a complete metric space (see [Ser73] page 13 for a proof). This metric

is **nonarchimedean** for it satisfies a stronger version got the triangular inequality, namely:

$$|x+y|_p \leq \max\{|x|_p, |y|_p\} \quad \text{for all } x, y \in \mathbb{Q}_p$$

Furthermore, $\mathbb{Q}$ maps naturally into $\mathbb{Q}_p$ and is in fact also dense in it and so $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ with respect to the p-adic metric. Finally the following theorem assures us that these are the only completion of $\mathbb{Q}$:

Theorem 1.1.9 (Ostrowski). *The only non-equivalent metrics (i.e. ones which induces different topologies) on $\mathbb{Q}$ are $d_p(\cdot,\cdot)$ and the usual absolute value.*

Proof. See [Mil98] page 95 for this. □

Note that if we complete $\mathbb{Q}$ under the "usual" absolute value, then we get $\mathbb{R}$. In light of this, if we talk about a completion of $\mathbb{Q}$ we can only be referring to $\mathbb{Q}_p$ for some prime p, or $\mathbb{R}$. In general, we will simply use this notation:

Notation 1.1.10. Let $M_{\mathbb{Q}} = \{p \mid p \text{ is prime }\} \cup \{\infty\}$ and $\mathbb{Q}_\infty = \mathbb{R}$. We will write $\mathbb{Q}_v$ for $v \in M_{\mathbb{Q}}$ to denote $\mathbb{Q}_p$ or $\mathbb{Q}_\infty$.

Remark 1.1.11. The reason we write $M_{\mathbb{Q}}$ and not simply M is that in general, we can construct completions, in an analogous way, for any finite algebraic extension $K/\mathbb{Q}$. In this case the set of prime elements together with the "infinite primes" (of which there may be several in general) would then be denoted by M_K. Despite the fact that we will not need this, I wanted the notation to be consistent with the general case.

I will also need the following property regarding the topology induced on $\mathbb{Q}_p$:

Proposition 1.1.12. *A sequence $\{u_n\}_{n=1}^{\infty} \subset \mathbb{Q}_p$ is Cauchy if and only if*

$$\lim_{n\to\infty} |u_{n+1} - u_n| = 0$$

Proof. Let $m > n$. Then the proposition follows straight from the fact that:

$$|u_m - u_n| \leq \max\{|u_m - u_{m-1}|, \ldots, |u_{n+1} - u_n|\}.$$

□

1.2 Hensel's Lemma

Now that we have constructed the p-adic numbers, the next natural topic of interest is equations over this new field. We would like to develop some tools for solving equations over $\mathbb{Q}_p$. In this section I will prove Hensel's Lemma, which is the Newton's method analogue for finding roots of polynomial equations in $\mathbb{Q}_p$. As mentioned before, historically, the topic was approached in reverse order, and it was this lemma (restricted to just $\mathbb{Q}$) that motivated the construction of p-numbers in the first place.

Lemma 1.2.1 (Hensel's Lemma). *Let $f \in \mathbb{Z}_p[X]$. Suppose there exists $x \in \mathbb{Z}_p$ and $n, k \in \mathbb{Z}$, such that $0 \leq 2k < n$, $f(x) \equiv 0\,(mod p^n)$ and $v_p(f'(x)) = k$. Then there exists $y \in \mathbb{Z}_p$ such that:*

$$f(y) \equiv 0\,(mod p^{n+1}), \quad v_p\,(f'(y)) = k \quad \text{and} \quad y \equiv x\,(mod p^{n-k}).$$

Note that for if we restrict the lemma just to $\mathbb{Z}$ then we get precisely the lifting theorem.

Proof. Let $y = x + p^{n-k}$, $z \in \mathbb{Z}_p$. Recall Taylor's formula:

$$f(x+h) = f(x) + hf'(x) + \frac{h^2}{2!}f''(x) + \dots$$

Apply this to $f(y)$:

$$\begin{aligned} f(y) &= f(x + p^{n-k}z) \\ &= f(x) + p^{n-k}zf'(x) + p^{2n-2k}a \qquad \text{with } a \in \mathbb{Z}_p \end{aligned}$$

However, $f(x) = p^n b$ for some $b \in \mathbb{Z}_p$ and $f'(x) = p^k c$ for some $c \in \mathbb{U}_P$. Since c is invertible, we can choose z such that $b + zc \equiv 0 \pmod{p}$. This implies:

$$\begin{aligned} f(y) &= p^n b + p^n zcf'(x) + p^{2n-2k}a \\ &= p^n (bz + c) + p^{2n-2k}a \\ &\equiv 0 \pmod{p^{n+1}} \qquad \text{as } 2k < n \implies 2n - 2k > n \end{aligned}$$

Finally,

$$\begin{aligned} f'(y) &= f'(x) + f''(x)p^{n-k}z + \dots \\ &\equiv p^k c \pmod{p^{n-k}} \end{aligned}$$

Since $n - k > k$ we get $v_p(f'(y)) = k$. □

Thus using the above lemma, we can generate a sequence $\{x_i\}$ such that each x_n is a solution to a polynomial equation modulo p^n. As mentioned earlier, normally this sequence does not converge in $\mathbb{Q}$. However, as we are about to see, it does converge in $\mathbb{Q}_p$ and thus we can use this lemma to solve polynomial over $\mathbb{Q}_p$.

Theorem 1.2.2. *Let $f \in \mathbb{Z}_p[X_1, \dots, X_m]$ and $x = (x_i) \in \mathbb{Z}_p^m$. Let $j, n, k \in \mathbb{Z}$ such that $1 \le j \le m$ and $0 \le 2k < n$. Suppose:*

$$f(x) \equiv 0 \,(mod p^n) \qquad \textit{and} \qquad v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k$$

Then there exists $y \in \mathbb{Z}_p^m$ such that

$$f(y) = 0 \qquad \textit{and} \qquad y \equiv x \,(mod p^{n-k})$$

Proof. We prove the theorem by induction on m. Suppose $m = 1$. Applying Hensel's Lemma to $x^{(0)} = x$ we get $x^{(1)} \in \mathbb{Z}_p$ such that

$$x^{(1)} \equiv x^{(0)} \pmod{p^{n-k}}, \qquad f\left(x^{(1)}\right) \equiv 0 \pmod{p^{n+1}} \qquad \text{and} \qquad v_p\left(f'\left(x^{(1)}\right)\right) = k$$

We then apply the lemma again, this time to $x^{(1)}$ after replacing n with $n+1$. We proceed inductively, and construct $x^{(0)}, x^{(1)}, \ldots, x^{(q)}, \ldots$ with the property that:

$$x^{(q+1)} \equiv x^{(q)} \left(\mathrm{mod}\, p^{n+q-k}\right) \qquad \text{and} \qquad f\left(x^{(q)}\right) \equiv 0 \left(\mathrm{mod}\, p^{n+q}\right)$$

This sequence is Cauchy since:

$$\begin{aligned} \lim_{n\to\infty} |x^{n+1} - x^n| &= \lim_{n\to\infty} |x^{(n)} + kp^{n+q-k} - x^{(n)}| \qquad \text{for some } k \in \mathbb{Z}_p \\ &\leq \lim_{n\to\infty} e^{-(n+q-k)} = 0 \end{aligned}$$

and by Proposition 1.1.12 this is a sufficient condition to check. Since $\mathbb{Z}_p$ is complete, the sequence must converge to some element $y \in \mathbb{Z}_p$. Then $f(y) = 0$ (since $f(x) \equiv 0 \left(\mathrm{mod}\, p^{n+q}\right)$ for all q) and $y \equiv x \left(\mathrm{mod}\, p^{n-k}\right)$. This proves the case of $m = 1$. If $m > 1$ then the case easily reduces down to the case where $m = 1$ by the following argument: let $\tilde{f} \in \mathbb{Z}_p[X_j]$ be the polynomial (in one variable) obtained by substituting $x_i \in \mathbb{Z}_p$ for X_i, $i \neq j$. Thus, by the above, there exists $y_j \in \mathbb{Z}_p$ such that $y_j \equiv x_j \left(\mathrm{mod}\, p^{n-k}\right)$ satisfying $\tilde{f}\left(y_j\right) = 0$. Moreover, if we let $y_i = x_i$ for $i \neq j$, the element $y = (y_j) \in \mathbb{Z}_p^m$ satisfies $f(y) = 0$ and $y \equiv x \left(\mathrm{mod}\, p\right)^{n-k}$. □

We use the above theorem to lift solutions modulo p to solutions in $\mathbb{Z}_p^m$. This is a standard way of solving polynomial equations with coefficients in $\mathbb{Z}_p$.

Corollary 1.2.3. *Let $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ such that there exists $x \in \mathbb{Z}_p^m$ with $f(x) \equiv 0 \left(mod p\right)$ and $\frac{\partial f}{\partial X_j}(x) \neq 0$ for at least one $j \in \{1, \ldots, m\}$. Then x lifts to a zero of f.*

Proof. Simply apply the above theorem to the case where $n = 1$ and note that $\frac{\partial f}{\partial X_j}(x) \neq 0$ implies that $v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = 0$ (i.e. $k = 0$ in the above theorem). □

Chapter 2

The Hasse Principle

In the previous chapter we saw that Hensel's Lemma is a powerful tool for checking whether a polynomial equation, in n variables, has a solution in the field of p-adic numbers. We also know, that since $\mathbb{Q}$ embeds in $\mathbb{Q}_p$, for all prime numbers p, that if a polynomial equation has a solution over $\mathbb{Q}^n$ (that is, it has a **global** solution) then it must have a solution for all $\mathbb{Q}_p^n$ (that is, it must have a **local** solution at every prime number). The Hasse principle is the converse of this: it is said to hold true if a local solution implies a global solution. More formally:

Definition 2.0.1. A polynomial $P \in \mathbb{Q}[X_1, \ldots, X_n]$ is said to obey the **Hasse principle** if given the fact that it has a zero in $\mathbb{Q}_v^n$ for all completions $\mathbb{Q}_v$ of $\mathbb{Q}$, then it has a zero over $\mathbb{Q}^n$.

There is a more general (and more modern) formulation of the Hasse principle (formulated not by Hasse) that replaces $\mathbb{Q}$ with any finite extension of $\mathbb{Q}$ and $\mathbb{Q}_p$ with its corresponding completions. We will discuss these fields later, but only in order to understand $\mathbb{Q}_p$ better. (As we will see, studying the extension of $\mathbb{Q}_p$ will play a vital role later on; analogously to how the study of complex numbers yields many results regarding real numbers.) Also, the Hasse principle can be restated more neatly using the language of varieties, which is what we will do in the first section.

It is known that all quadratic forms obey the Hasse principle (see [Ser73] page 41). In this thesis however, I will be concerned with finding **obstructions** to the principle, that is, examples when it does not hold.

In this chapter I will demonstrate that there are some trivial examples of obstructions, and will classify all such examples. I will then introduce the Hilbert symbol, and will show how a certain product formula associated with it will give rise to a non-trivial obstruction.

2.1 Affine Varieties

In this section we will introduce affine varieties so that we can phrase some of our definitions in a more elegant way.

Fix a field K. The **affine n-space**, denoted by $\mathbb{A}^n(K)$ is just the set K^n. Given a finite set of polynomials $\{f_1, \ldots, f_r\} \subseteq K[X_1, \ldots, X_n]$, we define the corresponding **K-affine variety** V, as the functor

$$\begin{array}{rcl} V : \{\text{field extensions of } K\} & \longrightarrow & \{\text{sets}\} \\ L & \longmapsto & V(L) \end{array}$$

where

$$V(L) := \{(x_1, \ldots, x_n) \in \mathbb{A}^n(L) \mid f_i(x_1, \ldots, x_n) = 0 \text{ for all } 1 \leq i \leq r\}$$

If L'/K and L/K are both extensions of K and $\phi\colon L' \to L$ then $V(\phi)$ is the obvious inclusion map $V(L') \hookrightarrow V(L)$. This clearly implies that if 1_L is the identity on L, then $V(1_L)$ is the identity on $V(L)$. Further, if $L' \xrightarrow{\phi} L \xrightarrow{\psi} L''$ are all extensions of K then clearly $V(\psi \circ \phi) = V(\psi) \circ V(\phi)$ and so V is indeed a functor.

Remark 2.1.1. Given a finite set of K-varieties, $\{V_i\}_{i \in I}$ we can form the K-variety $V := \bigcup V_i$ by defining $V(L) := \bigcup V_i(L)$ where L is an extension of K. Note that if, for example $f_1, f_2, f_3 \in K[X_1, \ldots, X_n]$ with V_1 the variety corresponding to $\{f_1, f_2\}$ and V_2 corresponds to $\{f_3\}$, then $V_1 \cup V_2$ corresponds to $\{f_1 f_3,\ f_2 f_3\}$. It clear how this is generalised to all finite unions of arbitrary varieties.

Note that this is not the standard definition of variety; the main reason for this is because usually, varieties are only defined over algebraically closed fields. This definition is, however, consistent with other, more common definitions and in fact is more intuitive if one was to study schemes, which generalise varieties.

This allows us to rephrase the Hasse principle as follows:

Definition 2.1.2. *An affine $\mathbb{Q}$-variety V is said to* **verify the Hasse principle** *if*

$$(\textit{for all } v \in M_{\mathbb{Q}},\ V(\mathbb{Q}_v) \neq \varnothing) \implies V(\mathbb{Q}) \neq \varnothing$$

2.2 Trivial Example

In this section we will classify some obvious example of obstructions to the Hasse principle i.e when a variety does not verify the Hasse principle. The main tools we will need for this are the Legendre symbol, and the quadratic law of reciprocity. This section is self-contained, but I have excluded the proofs of the basic properties for they are taught in every elementary number theory course.

Definition 2.2.1. *Let p be an odd prime and $a \in \mathbb{F}_p^*$. The* **Legendre symbol** *of a, denoted by $\left(\frac{a}{p}\right)$ is defined to be $a^{\frac{p-1}{2}} = \pm 1$.*

We also define $\left(\frac{0}{p}\right) = 0$. Note that Fermat's Little Theorem assures that $\left(\frac{a}{p}\right)$ is in fact ± 1 and that $\left(\frac{a}{p}\right) = 1$ if and only if $X^2 \equiv a \,(\mathrm{mod}\, p)$ has a solution in $\mathbb{F}_p^*$. We can extend the Legendre symbol to all of $\mathbb{Z}$ by defining, for all $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) := \left(\frac{a'}{p}\right)$ where a' is the image of a in $\mathbb{F}_p$.

If n is an odd integer I will use the following two functions:

$$\epsilon(n) \equiv \frac{n-1}{2} \,(\mathrm{mod}\, 2) = \begin{cases} 0 & \text{if } n \equiv 1 \,(\mathrm{mod}\, 4) \\ 1 & \text{if } n \equiv -1 \,(\mathrm{mod}\, 4) \end{cases}$$

$$\omega(n) \equiv \frac{n^2-1}{8} \,(\mathrm{mod}\, 2) = \begin{cases} 0 & \text{if } n \equiv \pm 1 \,(\mathrm{mod}\, 8) \\ 1 & \text{if } n \equiv \pm 5 \,(\mathrm{mod}\, 8) \end{cases}$$

The following theorem, states all the important results that we will need regarding the Legendre symbol:

Theorem 2.2.2 (Properties of the Legendre symbol). *Let p, q be odd primes and $a, b \in \mathbb{Z}$.*

(i) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(ii) $\left(\frac{1}{p}\right) = 1$

(iii) $\left(\frac{-1}{p}\right) = (-1)^{\epsilon(p)}$

(iv) $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$

(v) **(Gauss' quadratic law of reciprocity)**

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\epsilon(q)\epsilon(p)}$$

Proof. The proof of $(i), (ii), (iii), (iv)$ is straight forward. The proof of (v) is more complicated and can be found in [Ser73] pages 6-7. □

We now extend the Legendre symbol to p-adic units. Let $u \in \mathbb{U}_p$. Define $\left(\frac{u}{p}\right) = \left(\frac{u'}{p}\right)$ where u' is the image of u in $\mathbb{Z}_p/p\mathbb{Z}_p$ which is isomorphic to $\mathbb{F}_p$ by Proposition 1.1.4.

Finally, the following theorem gives an easy criterion for checking whether a p-adic number is a square:

Theorem 2.2.3. *Let p be an odd prime. Let $a = p^n u$ be an element of $\mathbb{Q}_p^*$ with $n \in \mathbb{Z}$ and $u \in \mathbb{U}_p$. Then $X^2 = a$ has a solution in $\mathbb{Q}_p$ if and only if n is even and $\left(\frac{u}{p}\right) = 1$. Further, if $p = 2$ then then $X^2 = a$ has a solution in $\mathbb{Q}_2$ if and only if $u \equiv 1 \,(mod 8)$ and n is even.*

I will not prove this theorem, because the proof is far too long and requires the development of some theory that we do not need for anything else. For a proof see [Ser73] pages 17-18.

We are now in a position to understand the trivial obstructions to the Hasse principle.

Example 2.2.4. Consider the polynomial equation:

$$P(X) = (X^2 - 5)(X^2 + 5)(X^2 + 1)(X^2 + 23)$$

Let us consider the roots of this polynomial over all completions of $\mathbb{Q}$. If $p > 5$ then the image of 5 in $\mathbb{Q}_p$ is $([5], [5], \dots)$ which is a unit in $\mathbb{Q}_p$. Similarly for -5 and -1. Thus $X^2 - 5 = 0$ has a solution in $\mathbb{Q}_p$ if and only if $\left(\frac{5}{p}\right) = 1$. Similarly $X^2 + 1 = 0$ has a solution if and only if $\left(\frac{-1}{p}\right) = 1$. But if they both equal -1 then $\left(\frac{-5}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{-1}{p}\right) = (-1) \times (-1) = 1$. This shows that at least one of the first three factors $P(X)$ has a zero over $\mathbb{Q}_p$ for $p > 5$. If $p = 5$ then $\left(\frac{-1}{5}\right) = 1$ since $3^2 \equiv -1 \,(\mathrm{mod}\, 5)$ and thus $X^2 + 1 = 0$ has a solution in $\mathbb{Q}_5$. If $p = 3$ then the image of $-23 = -2 - 3 - 2 \times 3^2$ in $\mathbb{Q}_3$ is $([-2], [-5], [-23], [-23], \dots)$. This is a unit in $\mathbb{Q}_3$ and $\left(\frac{-2}{3}\right) = \left(\frac{1}{3}\right) = 1$. If $p = 2$ then $-23 = -1 - 1 \times 2 - 1 \times 2^2 - 0 \times 2^3 - 1 \times 2^4$ and so the image of -23 in $\mathbb{Q}_2$ is $u = ([-1], [-2], [-7], [-7], [-23], [-23] \dots)$. Now

$u \equiv 1 \pmod 8$ and so $X^2 + 23 = 0$ has a solution in $\mathbb{Q}_2$. Finally in $\mathbb{R}$, $X^2 - 5 = 0$ has a solution. Thus $P(X)$ has a zero over every completion of $\mathbb{Q}$ but clearly has no solution over $\mathbb{Q}$.

It is easy to see how the above example can be generalised. All that is needed is a finite set $\{V_i\}_{i\in I}$ of $\mathbb{Q}$-varieties such that

$$\text{for all } v \in M_{\mathbb{Q}}, \text{ there exists } i \in I \text{ such that } V_i(\mathbb{Q}_v) \neq \varnothing \tag{1}$$

and

$$\text{for all } i \in I, \text{ there exists } v \in M_{\mathbb{Q}} \text{ such that } V_i(\mathbb{Q}_v) = \varnothing \tag{2}$$

This will guarantees that $V := \bigcup_{i\in I} V_i$ is an obstruction to the Hasse principle since (1) assures $V(\mathbb{Q}_v) \neq \varnothing$ for all $v \in M_{\mathbb{Q}}$ and (2) clearly implies $V(\mathbb{Q}) = \varnothing$

Example 2.2.5. Let us see how the previous Example fits into this generalisation. We let $P_1 = X - 5$ and V_1 be the corresponding variety, and similarly for P_i and V_i for $i = 2, 3, 4$. Now we saw that for each $v \in M_{\mathbb{Q}}$ at least one of the P_i's had a zero in $\mathbb{Q}_v$ which implies for all $v \in M_{\mathbb{Q}}$, one of $V_i(\mathbb{Q}_v) \neq \varnothing$ this is condition (1). Further, it is easy to see that for every $v \in M_{\mathbb{Q}}$ at least one of $V_i(\mathbb{Q}_v) = \varnothing$ for $i = 1, 2, 3, 4$; this is condition (2). Finally, the variety corresponding to $\prod P_i$ is precisely $V := \bigcup V_i$ and so we see that we have indeed generalised the previous example.

2.3 Hilbert Symbol

In this section I will develop the theory of the Hilbert symbol in order to give non-trivial examples of obstructions to the Hasse principle.

Definition 2.3.1. *Let $a, b \in \mathbb{Q}_v^*$. The* **Hilbert symbol** *of a and b relative to $\mathbb{Q}_v$, denoted by $(a, b)_v$, for $v \in M_{\mathbb{Q}}$ is defined as follows:*

$$(a,b)_v = \begin{cases} 1 & \text{if } Z^2 - aX^2 - bY^2 = 0 \text{ has a solution } (z,x,y) \text{ in } \mathbb{Q}_v^{*3} \\ -1 & \text{otherwise} \end{cases}$$

Note that the subscript v on the Hilbert symbol indicates the field over which we are considering the equation. If v is prime then the equation is over $\mathbb{Q}_p$ and if $v = \infty$ the the field is $\mathbb{R}$. We drop the subscript if the field is clear.

Remark 2.3.2. It is clear that for $a, b, n, m \in \mathbb{Q}_v$ $(a, b)_v = (an^2, bm^2)$ and thus $(\cdot, \cdot)_v$ defines a map $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2} \times \mathbb{Q}_v^*/\mathbb{Q}_v^{*2} \to \{\pm 1\}$

Let K/k be a finite field extension of degree n, i.e. $K \simeq k^n$ as vector spaces. Each $\alpha \in K$ defines an isomorphism $K \to K$ via multiplication by α. Since $K \simeq k^n$, α corresponds to an $n \times n$ matrix with coefficients in k. We define the **norm** of α, denoted $N_{K/k}(\alpha)$ to be the determinant of this matrix. Note that the norm of an element is well defined since the matrix corresponding to each element is unique up to conjugation and the determinant function is conjugation invariant. We also let $N_{K/k}K^* = \left\{N_{K/k}(\alpha) \mid \alpha \in K^*\right\}$. We drop the subscript K/k if the fields are clear.

Proposition 2.3.3. *Let K/k be a finite field extension. Then NK^* is a subgroup of k^*.*

Proof. All that needs to be shown is that $N : K^* \to k^*$ is a group homomorphism. Note that $N(1) = 1$. If α corresponds to the matrix M_α and β corresponds to M_β then clearly $\alpha\beta$ corresponds to (up to conjugation) $M_\alpha M_\beta$. Thus we have:

$$N(\alpha\beta) = \det(M_\alpha M_\beta) = \det(M_\alpha)\det(M_\beta) = N(\alpha)N(\beta)$$

□

Example 2.3.4. Let $b \in \mathbb{Q}_v$ such that b is not a square in $\mathbb{Q}_v$. Then:

$$\mathbb{Q}_v(\sqrt{b}) = \mathbb{Q}_v \oplus \mathbb{Q}_v\sqrt{b}$$

Let $x, y \in \mathbb{Q}_v$. $(x + y\sqrt{b}) \cdot 1 = x + y\sqrt{b}$ and $(x + y\sqrt{b}) \cdot (\sqrt{b}) = by + x\sqrt{b}$ Thus:

$$x + y\sqrt{b} \longleftrightarrow \begin{pmatrix} x & by \\ y & x \end{pmatrix}$$

and so $N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}(x + y\sqrt{b}) = x^2 - by^2$.

We are now going to establish various properties regarding the Hilbert symbol. My goal in this and the next section, is to show the close relationship between the Hilbert symbol and the Legendre symbol.

Proposition 2.3.5. *Let $a, b \in \mathbb{Q}_v^*$ and let $\mathbb{Q}_{v_b} = \mathbb{Q}_v(\sqrt{b})$. Then $(a, b)_v = 1$ if and only if $a \in N\mathbb{Q}_{v_b}^*$.*

Proof. If b is a square of an element $c \in \mathbb{Q}_v$ then the equation $Z^2 - aX^2 - bY^2 = 0$ has a solution $(c, 0, 1)$ which implies $(a, b) = 1$. The proposition is then clearly true since, $\mathbb{Q}_{v_b} = \mathbb{Q}_v$ which implies $N\mathbb{Q}_{v_b}^* = \mathbb{Q}_v^*$. Suppose b is not a square in $\mathbb{Q}_v$. If $a \in N\mathbb{Q}_{v_b}^*$ then by Example 2.3.4, there exists $z + y\sqrt{b} \in \mathbb{Q}_{v_b}$, $z, y \in \mathbb{Q}_v$, such that $a = z^2 - by^2$. This implies $Z^2 - aX^2 - bY^2 = 0$ has a solution $(z, 1, y)$ and thus $(a, b)_v = 1$. Conversely, if $(a, b)_v = 1$ then there exists $(z, x, y) \in \mathbb{Q}_v^{*3}$ such that $z^2 - ax^2 - by^2 = 0$. Now, $a \neq 0$, as otherwise b is a square in $\mathbb{Q}_v^*$, and thus $a = N\left(\frac{z}{x} + \frac{y}{b}\sqrt{b}\right)$.

□

With this proposition we can now prove:

Proposition 2.3.6. *Let $a, a', b, c \in \mathbb{Q}_v^*$ and if $1 - a$ appears in a formula below then $a \neq 1$. The following hold:*

(i) $(a, b) = (b, a)$
(ii) $(a, c^2) = 1$
(iii) $(a, -a) = 1$
(iv) $(a, 1 - a) = 1$
(v) $(a, b) = 1 \implies (aa', b) = (a', b)$
(vi) $(a, b) = (a, -ab) = (a, (1 - a)b)$

Proof. (i) and (ii) are obvious. $(0, 1, 1)$ is a root of $Z^2 - aX^2 + aY^2 = 0$ which proves (iii). $(1, 1, 1)$ is a root of $Z^2 - aX^2 - (1 - a)Y^2 = 0$ which proves (iv). To prove (v) we note by Proposition 2.3.5 $a \in N\mathbb{Q}_{v_b}^*$ and since by Proposition 2.3.3

NK_b^* is a group, $a' \in N\mathbb{Q}_{v_b}^* \iff aa' \in N\mathbb{Q}_{v_b}^*$ and so (v) follows. (vi) follows easily from the previous parts. □

2.4 Calculating the Hilbert Symbol

The goal of this section is to prove two major results regarding the Hilbert symbol. The first major result will give an easy criterion for calculating the Hilbert symbol of two elements $a, b \in \mathbb{Q}_v^*$. The second will be crucial in constructing a non-trivial obstruction. This section, is unfortunately a little dry, the intermediate results are not particularly interesting, but are needed in order to prove the main theorems.

Let $q = p^m$ where, p is prime and $m \in \mathbb{Z}^+$. Let $\mathbb{F}_q$ be a field with q elements.

Lemma 2.4.1. *Let $u \geq 0$. Then*

$$S(X^u) := \sum_{x \in \mathbb{F}_q} x^u = \begin{cases} -1 & \text{if } u \geq 1 \text{ and divisible by } (q-1) \\ 0 & \text{otherwise} \end{cases}$$

Note that we are defining $x^0 = 0$ for all $x \in \mathbb{F}_q$, even if $x = 0$ and that all arithmetic is performed modulo p, since that is the characteristic of $\mathbb{F}_q$.

Proof. If $u = 0$, $S(X^u) = q \cdot 1 = 0$. If $u \geq 1$ and divisible by $(q-1)$, by Fermat's Little theorem, $x^u = 1$ for all $x \neq 0$ and $0^u = 0$. Thus $S(X^u) = q - 1 = -1$. If $u \geq 1$ but not divisible by $q-1$ then the fact that $\mathbb{F}_q^*$ is cyclic of order $(q-1)$ implies there exists $y \in \mathbb{F}_q^*$ such that $y^u \neq 1$. Thus we have:

$$S(X^u) = \sum_{x \in \mathbb{F}_q} x^u = \sum_{x \in \mathbb{F}_q} y^u x^u = y^u \sum_{x \in \mathbb{F}_q} x^u = y^u S(X^u)$$

Since $y^u \neq 1$ it must be that $S(X^u) = 0$. □

Keeping the same notation as in the above lemma,we can now prove the following theorem:

Proposition 2.4.2. *Let $f_\alpha \in \mathbb{F}_q[X_1, \ldots, X_n]$ be polynomials such that $\sum_\alpha \deg f_\alpha < n$ and let W be the set of their common zeroes in $\mathbb{F}_q^n$. Then $p \,|\text{card}(W)$.*

Proof. Let $P = \prod_\alpha \left(1 - f_\alpha^{q-1}\right)$. Note that by Fermat's Little theorem $f_\alpha^{q-1}(x) = 1$ if $x \notin W$ and 0 otherwise. This implies that:

$$P(x) = \begin{cases} 1 & \text{if } x \in W \\ 0 & \text{if } x \notin W \end{cases}$$

Thus if we define $S(P) = \sum_{x \in \mathbb{F}_q^n} P(x)$, then we have:

$$\text{Card}(W) \equiv S(P) \,(\text{mod}\, p)$$

and so all that we need to show is that $S(P) = 0$. The fact that $\sum_\alpha \deg f_\alpha < n$ implies that $\deg P < n(q-1)$ and thus P must be a linear combination of monomials $X^u = X_1^{u_1} \dots X_n^{u_n}$ with $\sum_i u_i < n(q-1)$. Thus it suffices to show that for such a monomial X^u we have $S(X^u) = 0$. This, however, follows from the above lemma since at least one of u_i is less that $q-1$. □

The point of proving this theorem, is that later we will need the following corollary:

Corollary 2.4.3. *All quadratic forms over $\mathbb{F}_q$ in at least three variables, have a non-trivial zero.*

Proof. Apply the above proposition with $n \geq 3$ to a homogeneous polynomial of degree 2. Since it definitely has one zero, namely the trivial one, the theorem implies it has to have more since p divides the number of zeros. □

Notation 2.4.4. Given a polynomial $f \in \mathbb{Z}_p[X_1, \dots, X_m]$, then for $n \geq 1$ we denote by f_n the polynomial with coefficients in A_n obtained by reduction of the coefficients of f modulo p^n.

Definition 2.4.5. *A point $x = (x_1, \dots, x_m) \in \mathbb{Z}_p^m$ (respectively $(A_n)^m$) is called* **primitive** *if at least one x_i is invertible in $\mathbb{Z}_p^m$ (respectively $(A_n)^m$).*

Proposition 2.4.6. *Let $f^{(i)} \in \mathbb{Z}_p[X_1, \dots X_m]$ be homogeneous polynomials. The following are equivalent:*

(i) *The $f^{(i)}$ have a common, non-trivial, zero in $\mathbb{Q}_p^m$*
(ii) *The $f^{(i)}$ have a common primitive zero in $\mathbb{Z}_p^m$*
(iii) *for all $n > 1$ the the $f_n^{(i)}$ have a common primitive zero in $(A_n)^m$.*

Proof. $((i) \Rightarrow (ii))$: If $x = (x_1, \dots, x_m)$ is a common zero then, since the polynomials are homogeneous, $x' = p^{-i}(x_1, \dots, x_m)$ is a zero for all $i \in \mathbb{Z}$. Setting $i = min\{v_p(x_1), v_p(x_2), \dots, v_p(x_m)\}$ guarantees x' is primitive. $((ii) \Rightarrow (i))$ is obvious. $((ii) \Leftrightarrow (iii))$: Let D_n be the set of common zeroes of f_n^i. Then $D := \varprojlim D_n$ is non empty if and only if the D_n are non empty.[1] □

With this we prove:

Lemma 2.4.7. *Let $v \in \mathbb{U}_p$ be a p-adic unit. If $Z^2 - pX^2 - vY^2 = 0$ has a non-trivial solution in $\mathbb{Q}_p^3$ then it has a solution (z, x, y) such that $z, y \in \mathbb{U}_p$ and $x \in \mathbb{Z}_p$.*

Proof. By the above proposition, $Z^2 - pX^2 - vY^2 = 0$ has a primitive solution (z, x, y). Suppose y or z are not in $\mathbb{U}_p$. Thus either $y \equiv 0 \pmod p$ or $z \equiv 0 \pmod p$. From the assumption we have $z^2 - vy^2 \equiv 0 \pmod p$ and $p \nmid v$, which implies that both y and $z \equiv 0 \pmod p$. However, this means that $px^2 \equiv 0 \pmod{p^2}$ which implies $x \equiv 0 \pmod p$. This contradicts (z, x, y) being primitive.

□

We are now in a position to prove the first major result regarding the Hilbert symbol. Recall the definition of $\epsilon(\cdot)$ and $\omega(\cdot)$ from page 8.

[1] This is a property of inverse limits. See [Ser73] page 13 for a proof of this.

Theorem 2.4.8 (Computing the Hilbert symbol). *If $\mathbb{Q}_v = \mathbb{R}$ then $(a,b)_\infty = 1$ if either a or b is positive. Otherwise, $(a,b)_\infty = -1$.*
If $\mathbb{Q}_v = \mathbb{Q}_p$, and $a = p^\alpha u$ and $b = p^\beta v$ are elements of $\mathbb{Q}_v$ with $u, v \in \mathbb{U}_p$ then:

$$\begin{aligned}(a,b)_p &= (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \quad \text{if } p \neq 2 \\ (a,b)_p &= (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)} \quad \text{if } p = 2\end{aligned}$$

Proof. If $\mathbb{Q}_v = \mathbb{R}$ the theorem follows straight from the definition of the Hilbert symbol and the fact that every positive number has a square root in $\mathbb{R}$.

Suppose $\mathbb{Q}_v = \mathbb{Q}_p$ with $p \neq 2$. From the formula we are trying to prove it is clear that it is not the actual value of α and β that plays a part in determining (a,b) but whether they are odd or even. This, together with the fact that the Hilbert symbol is symmetrical, means we have 3 cases to check:

Case 1: Suppose $\alpha = \beta = 0$. Let $f = Z^2 - uX^2 - vY^2$. By Corollary 2.4.3 $f \equiv 0 \pmod p$ has a non-trivial solution (z,x,y). However, since u, v are units, we know that one of the partial derivatives of f evaluated at (z,x,y) is non-zero modulo p. By Corollary 1.2.3 this solution lifts to a solution in $\mathbb{Z}_p^3$. Thus $(a,b) = 1$ and the theorem is verified in this case.

Case 2: Suppose $\alpha = 1$ and $\beta = 0$. We need to check that $(pu, v) = \left(\frac{v}{p}\right)$. Since $(u,v) = 1$ (by Case 1) we have, by Proposition 2.3.6 $(pu,v) = (p,v)$. Thus it suffices to check $(p,v) = \left(\frac{v}{p}\right)$. If v is a square then $Z^2 - pX^2 - vY^2 = 0$ has a solution $(\sqrt{v}, 0, 1)$, implying $(p,v) = 1$. In this case it is also clear that $\left(\frac{v}{p}\right) = 1$. If v is not a square then Theorem 2.2.3 says that $\left(\frac{v}{p}\right) = -1$. Now suppose $Z^2 - pX^2 - vY^2 = 0$ has a non-trivial solution (z,x,y). Then $z^2 \equiv vy^2 \pmod p$ which means $z, y \notin \mathbb{U}_p$ (for then v would be a square). But this contradicts Lemma 2.4.7. Thus (a,b) is also -1.

Case 3: Suppose $\alpha = \beta = 1$. We need to check whether $(pu, pv) = (-1)^{\frac{p-1}{2}} \left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$. By Proposition 2.3.6 $(pu, pv) = (pu, -p^2uv) = (pu, -uv) \overset{\text{Case 2}}{=\!=} \left(\frac{-uv}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$ $= (-1)^{\frac{p-1}{2}} \left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$

Now we need to check that the theorem is true for $p = 2$. By looking at the formula we are trying to prove we see that we again have the same cases:

Case 1: Suppose $\alpha = \beta = 0$. We need to show $(u,v) = (-1)^{\epsilon(u)\epsilon(v)}$. Suppose at first that $u \equiv 1 \pmod 4$. In this case $\epsilon(u) = 0$ and so we need to show $(u,v) = 1$. If $u \equiv 1 \pmod 8$ then u is a square (by Theorem 2.2.3) and thus $(u,v) = 1$. If $u \equiv 5 \pmod 8$ then $u + 4v \equiv 1 \pmod 8$ since $v \equiv 1$ or $3 \pmod 4$. By Theorem 2.2.3 there exists $w \in \mathbb{Q}_2$ such that $w^2 = u + 4v$. Thus $Z^2 - uX^2 - vY^2 = 0$ has a solution $(w, 1, 2)$ implying $(u,v) = 1$. Now suppose that both $u, v \equiv -1 \pmod 4$. In this case $\epsilon(u) = \epsilon(v) = 1$ so we need to show that $(u,v) = -1$. If (z,x,y) is a non-trivial solution of $Z^2 - uX^2 - vY^2 = 0$ then by Proposition 2.4.6 we can assume that it is primitive. Also, we have that $z^2 + x^2 + y^2 \equiv 0 \pmod 4$ and since the only squares in $\mathbb{Z}/4\mathbb{Z}$ are 0 and 1, this implies $z, x, y \equiv 0 \pmod 2$. This contradicts (z,x,y) being primitive. Thus, we do not have a non-trivial solution, and so $(u,v) = -1$.

Case 2: Suppose $\alpha = 1$ and $\beta = 0$. We need to check that $(2u, v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)}$. First, I'll show that $(2, v) = (-1)^{\omega(v)}$, i.e. that $(2, v) = 1 \iff v \equiv \pm 1 \,(\mathrm{mod}\, 8)$. If $(2, v) = 1$ then there exists a non-trivial solution (z, x, y) to $z^2 - 2x^2 - vy^2 = 0$. Moreover, Lemma 2.4.7 implies that we can assume $y, z \in \mathbb{U}_2$ and so Theorem 2.2.3 implies that $y^2, z^2 \equiv 1 \,(\mathrm{mod}\, 8)$. Therefore we have $1 - 2x^2 - v \equiv 0 \,(\mathrm{mod}\, 8)$ and since the only square in $\mathbb{Z}/8\mathbb{Z}$ are $[0], [1]$ and $[4]$, we have that $v \equiv \pm 1 \,(\mathrm{mod}\, 8)$. Conversely, if $v \equiv 1 \,(\mathrm{mod}\, 8)$ then v is a square so $(2, v) = 1$. If $v \equiv -1 \,(\mathrm{mod}\, 8)$ then $f := Z^2 - 2X^2 - vY^2 \equiv 0 \,(\mathrm{mod}\, 8)$ has a solution $(1, 1, 1)$. Note that $\frac{\partial f}{\partial Z}(1, 1, 1) = 2$ and so we apply Theorem 1.2.2 to f with $n = 3$ and $k = 1$. This guarantees that $(2, v) = 1$. We now show that $(2u, v) = (2, v)(u, v)$. By Proposition 2.3.6 this is true if either $(2, v)$ or $(u, v) = 1$. If $(2, v) = -1$ then $v \equiv 3, 5 \,(\mathrm{mod}\, 8)$ (Theorem 2.2.3) and if $(u, v) = -1$ then $u, v \equiv 3 \,(\mathrm{mod}\, 4)$ (Case 1 above). Thus if $(2, v) = (u, v) = -1$ then $v \equiv 3 \,(\mathrm{mod}\, 8)$ and $u \equiv 3$ or $-1 \,(\mathrm{mod}\, 8)$. Since multiplying u or v by a square does not change $(2, v)$ or (u, v) we can assume that $u = -1$ and $v = 3$ or that $u = 3$ and $v = -5$.[2] But $Z^2 + 2X^2 - 3Y^2 = 0$ and $Z^2 - 6X^2 + 5Y^2 = 0$ have solution $(1, 1, 1)$ and so $(2u, v) = 1$.

Case 3: Suppose $\alpha = \beta = 1$. We need to check that:

$$(2u, 2v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(u)+\omega(v)}$$

Theorem 2.2.3 implies that $(2u, 2v) = (2u, -4uv) = (2u, -uv)$ (since 4 is a square). From Case 2 we know that $(2u, -uv) = (-1)^{\epsilon(u)\epsilon(-uv)+\omega(-uv)}$. Now we note the following: $(-1)^{\epsilon(xy)} = (-1)^{\epsilon(x)}(-1)^{\epsilon(y)}$ for $x, y \in \mathbb{U}_2$, and the same is true for $\omega(\cdot)$ (this is not "obvious" but can easily be checked). Also, it is clear that $\epsilon(u)(1 + \epsilon(u)) = 0$. And so:

$$(-1)^{\epsilon(u)\epsilon(-uv)+\omega(-uv)} = (-1)^{\epsilon(u)\epsilon(v)+\omega(u)+\omega(v)}$$

This completes the proof. □

Corollary 2.4.9. *For $a, b, c \in \mathbb{Q}_v^*$*

$$(ab, c) = (a, c)(b, c)$$

This Corollary says that the Hilbert symbol is bilinear.

Proof. This is clear from the above theorem and Theorem 2.2.2 (i). □

The following is the second major result of this section. What makes the result so important, is that it will give us a non-trivial obstruction to the Hasse principle. In fact the goal of this thesis will ultimately be to generalise this result. Recall that $\mathbb{Q}$ is a subfield of $\mathbb{Q}_v$ for all v and that $M_{\mathbb{Q}}$ denotes the set of all primes together with ∞.[3]

[2] For example, since $v \equiv 3 \,(\mathrm{mod}\, 8)$ then if we set $v' = v \cdot 3^{-1}$ then $v' \equiv 1 \,(\mathrm{mod}\, 8)$ and thus it is a square in $\mathbb{Q}_2$ and so is v'^{-1}. Also, $vv'^{-1} = 3$. Similarly, we can multiply v by the inverse of $v \cdot (-5)^{-1}$, which is also a square to get, -5. Similarly for u.

[3] See definition on page 4.

Theorem 2.4.10 (Product formula). *Let $a, b \in \mathbb{Q}^*$. Then $(a,b)_v = 1$ for all, except a finite number, of $v \in M_{\mathbb{Q}}$. Also, we have*

$$\prod_{v \in M_{\mathbb{Q}}} (a,b)_v = 1$$

Proof. In light of the bilinearity of the Hilbert symbol, it suffices to prove the theorem for $a, b = -1$ or p, for some prime p. Thus we have 3 cases:

Case 1: $a = b = -1$. We have $(-1,-1)_\infty = -1$, since $Z^2 + X^2 + Y^2 = 0$ has no non-trivial solutions over $\mathbb{R}$. $(-1,-1)_2 = (-1)^{\epsilon(-1)\epsilon(-1)} = (-1)^1 = -1$. For a prime $p \neq 2$, $(-1,-1)_p = (-1)^0 \left(\frac{-1}{p}\right)^0 \left(\frac{-1}{p}\right)^0 = 1$, since $\alpha = \beta = 0$ in the above theorem. Thus the theorem is verified in this case.

Case 2: $a = -1$, $b = l$, for a prime l. If $l = 2$ then $(-1,2)_\infty = 1$ since $Z^2 + X^2 - 2Y^2 = 0$ clearly has a non-trial solution over $\mathbb{R}$. $(-1,2)_2 = (-1)^{\epsilon(-1)\epsilon(1)+0+1\cdot\omega(-1)} = 1$. If $l \neq 2$ then $(-1,l)_2 = (-1)^{\epsilon(-1)\epsilon(l)+0+0} = (-1)^{\epsilon(l)}$ and $(-1,l)_l = (-1)^0 \left(\frac{-1}{l}\right)^1 \left(\frac{1}{l}\right) = \left(\frac{-1}{l}\right) = (-1)^{\epsilon(l)}$. If $v \neq 2, l$ then $(-1,l)_v = 1$ as $\alpha = \beta = 0$ in the above theorem and also, since $l > 0$ we have $(-1,l)_\infty = 1$. The theorem is thus verified since, $(-1,l)_v = -1$, either zero or exactly two times.

Case 3: $a = l$, $b = l'$, where l, l' are both prime. If $l = l'$ then Proposition 2.3.6(vi) implies that $(l,l)_v = (l,-l^2)_v = (l,-1)_v$ which is Case 2. If $l \neq l'$ and $l' = 2$ then:
for $v \neq l, 2$ we have $(l,2)_v = 1$ (since $\alpha = \beta = 0$);
for $v = 2$, $(l,2)_2 = (-1)^{\epsilon(l)\epsilon(1)+0+1\cdot\omega(l)} = (-1)^{\omega(l)}$;
for $v = l$, $(l,2)_l = (-1)^0 \left(\frac{2}{l}\right)\left(\frac{1}{l}\right) = (-1)^{\omega(l)}$ by Theorem 2.2.2 ;
Clearly $(l,2)_\infty = 1$ and so the theorem is verified in this special case.
If $l \neq l'$ both $l, l' \neq 2$ then:
If $p \neq 2, l, l'$ then $(l,l')_p = (-1)^0 \left(\frac{l}{p}\right)^0 \left(\frac{l'}{p}\right)^0 = 1$ and $(l,l')_\infty = 1$;
If $v = 2$ then $(l,l')_2 = (-1)^{\epsilon(l)\epsilon(l')}$ (since $\alpha = \beta = 0$ in the previous theorem);
If $v = l$ then $(l,l')_l = (-1)^0 \left(\frac{l'}{l}\right)\left(\frac{1}{l}\right) = \left(\frac{l'}{l}\right)$;
Similarly, if $v = l'$ then $(l,l')_{l'} = \left(\frac{l}{l'}\right)$.
Thus the theorem is proven provided that

$$\left(\frac{l'}{l}\right)\left(\frac{l}{l'}\right) = (-1)^{\epsilon(l)\epsilon(l')}$$

However, this is assured by the Quadratic Law of Reciprocity (Theorem 2.2.2). □

Note that Case 3 in the above proof holds if and only if the Quadratic Law of Reciprocity holds. Thus the product formula is just an equivalent statement to the quadratic law of reciprocity.

2.5 A Non-Trivial Obstruction

Recall from Section 2.2 the class of obstructions that we have classified as being "trivial". In this section we shall see how the product formula, which was proven in the previous section, plays a vital role in generating examples of non-trivial obstructions.

Define $f(X) \in \mathbb{Z}[X]$ to be:

$$f(X) = -X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_2X^2 + 3$$

such that the following hold:

(i) $4 \mid n$, in particular n, the degree of f, is even;
(ii) $8 \mid a_i$ for all i;
(iii) $3, -3, 2, -2$ are not zeros of f.

Note that the "X" term is missing; the reason for this will become evident soon.

Define $g(X) = 1 - f(X)$.

Theorem 2.5.1.

$$Y^2 + Z^2 = f(X)g(X)$$

is a non-trivial obstruction to the Hasse principle.

Proof. We will first prove that $Y^2 + Z^2 = f(X)g(X)$ has a non-trivial solution over all $\mathbb{Q}_v^3$. Let $x \in \mathbb{Q}_v$ such that $f(x)g(x) \neq 0$. Then:

$$Y^2 + Z^2 = f(x)g(x)$$

has a solution in $\mathbb{Q}_v^2$ if and only if:

$$Y^2 + Z^2 = f(x)g(x)X^2$$

has a solution in $\mathbb{Q}_v^3$. However, $Y^2 + Z^2 = f(x)g(x)X^2$ has a solution in $\mathbb{Q}_v^3$ if and only if $(-1, f(x)g(x))_v = 1$ (from the definition of the Hilbert symbol) which is equivalent to $(-1, f(x))_v(-1, g(x))_v = 1$(by Corollary 2.4.9), which is the same condition as:

$$(-1, f(x))_v = (-1, g(x))_v \qquad (*)$$

A special case of Theorem 2.4.8 gives that for $a = p^{v_p(a)}u \in \mathbb{Q}_v^*$, $u \in \mathbb{U}_p$ we have:

$$\begin{aligned} (-1, a)_p &= (-1)^{v_p(a)\epsilon(p)} \quad \text{for } p \neq 2 \\ (-1, a)_2 &= (-1)^{\epsilon(u)} \\ (-1, a)_\infty &= \frac{a}{|a|} \end{aligned}$$

If $p \equiv 1 \pmod 4$, then $\epsilon(p) = 0$ and so $(-1, f(x))_p = (-1)^{\epsilon(p)} = 1$ and similarly, $(-1, g(x))_p = 1$ and so $(*)$ is verified.

If $p \equiv 3 \pmod 4$, then $\epsilon(p) = 1$. Thus to verify $(*)$ we need to show:

$$(-1)^{v_p(f(x))} = (-1)^{v_p(g(x))}$$

I claim that provided $v_p(x) < 0$ then, in fact, $v_p(f(x)) = v_p(g(x))$. To see this, let $x = p^{-k}u$ with $k > 0$ and $u \in \mathbb{U}_p$. Then:

$$\begin{aligned} f(x) &= -(p^{-k}u)^n + a_{n-1}(p^{-k}u)^{n-1} + \cdots + 3 \\ &= -p^{-kn}u^n + a_{n-1}p^{-k(n-1)}u^{n-1} + \cdots + 3 \\ &= p^{-kn}\left(-u^n + a_{n-1}p^k u^{n-1} + \cdots + 3p^{kn}\right) \end{aligned}$$

And since $(-u^n + a_{n-1}p^k u^{n-1} + \cdots + 3p^{kn}) \in \mathbb{U}_p$, $v_p(f(x)) = -kn$. And exactly the same procedure shows thar $v_p(g(x)) = -kn$. (The main reason for the equality is the fact that f and g have the same degree.) Thus for $p \equiv 3 \pmod 4$ $(*)$ is verified provided $v_p(x) < 0$ and $f(x), g(x) \neq 0$. Clearly, it is possible to find such an $x \in \mathbb{Q}_p$.

If $p = 2$, then letting $x = 0$ we get: $(-1, f(0))_2 = (-1, 3)_2 = (-1)^{\epsilon(3)}$ and $(-1, g(0))_2 = (-1, -1)_2 = (-1)^{\epsilon(-1)}$. Since $3 \equiv -1 \pmod 4$ the two are equal and so $(*)$ is verified for $p = 2$.

If $v = \infty$, $(*)$ is verified provided there exists $x \in \mathbb{R}$ such that $\frac{f(x)}{|f(x)|} = \frac{g(x)}{|g(x)|}$. i.e. such that $f(x)$ and $g(x)$ are both positive or both negative. Clearly such an x exists since f has an x-intercept.

Thus we have shown that $Y^2 + Z^2 = f(X)g(X)$ has a solution in $\mathbb{Q}_v^3$ for all $v \in M_{\mathbb{Q}}$.

Now we will show that $Y^2 + Z^2 = f(X)g(X)$ has no solutions in $\mathbb{Q}^3$. Suppose, on the contrary, that there exists $(x, y, z) \in \mathbb{Q}^3$ such that $y^2 + z^2 = f(x)g(x)$. We now calculate $(-1, f(x))_v$ for all $v \in M_{\mathbb{Q}}$.

Note firstly that $f(x)g(x) \neq 0$ since the only rational zeros that f or g could have are $3, -3, 2, -2$ all of which are excluded by assumption. This implies that $(*)$ holds.

If $p \equiv 1 \pmod 4$ then, from before $(-1, f(x))_p = 1$.

If $p \equiv 3 \pmod 4$, and $v_p(x) < 0$ then from before $(-1, f(x))_p = (-1)^{v_p(f(x))} = 1$ since the degree of f is even (from above $v_p(f(x)) = -kn$ where n is the degree). If $v_p(x) \geq 0$ then the fact that $f(x) = 1 - g(x)$ implies that either $v_p(f(x))$ or $v_p(g(x)) = 0$ and so one of $(-1, f(x))_p$ or $(-1, g(x))_p$ must be $(-1)^0 = 1$. This together with $(*)$ implies that $(-1, f(x))_p = 1$.

Suppose now that $p = 2$. In order to calculate $(-1, f(x))_2$ we need to write $f(x)$ in the form $2^n u$ where $u \equiv 1 \pmod 2$ (i.e. $u \in \mathbb{U}_2$). If $v_2(x) > 0$ then since f has no "X" term, and the constant term of f is 3, we have $f(x) \equiv 3 \pmod 4$. Thus $f(x) \in \mathbb{U}_2$ and $\epsilon(f(x)) = 1$ which implies $(-1, f(x))_2 = -1$. If $v_p(x) < 0$ then

$$\begin{aligned} f(x) &= -x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + 3 \\ &= x^n \underbrace{\left(-1 + a_{n-1}x^{-1} + \cdots + a_2x^{2-n} + 3x^{-n}\right)}_{u} \end{aligned}$$

Now, since n is even x^n must be a square in $\mathbb{Q}_2$. Also $u \in \mathbb{U}_2$, and thus we have $(-1, f(x))_2 = (-1, x^n u)_2 = (1, u)_2 = (-1)^{\epsilon(u)} = -1$, since $u \equiv -1 \pmod 3$.

Finally, if $v_2(x) = 0$ then we can write $x = 1 + 2k$ with $k \in \mathbb{Z}_2$. Thus

$$x^n = (1 + 2k)^n = 1 + n2k + \binom{n}{2}(2k)^2 + \binom{n}{3}(2k)^3 + \ldots$$

and so:

$$\begin{aligned} f(x) &= 3 - x^n + 8(j) \qquad j \in \mathbb{Z}_2 \text{ since } 8 \mid a_i \\ &= 2 - 2nk - \binom{n}{2}4k^2 - \binom{n}{3}8k^3 - \cdots + 8j \\ &= 2\underbrace{\left(1 - nk - \binom{n}{2}2k^2 - \binom{n}{3}4k^2 - \cdots + 4j\right)}_{u} \end{aligned}$$

Now $u \in \mathbb{U}_2$ since n is even. We need to determine $\epsilon(u)$. So working modulo 4:

$$\begin{aligned} u &= 1 - nk - \binom{n}{2}2k^2 \\ &= 1 - 2\left(\frac{n}{2}k + \binom{n}{2}k^2\right) \\ &= 1 - 2\left(k\left(\frac{n}{2} + \binom{n}{2}k\right)\right) \end{aligned}$$

Now $k\left(\frac{n}{2} + \binom{n}{2}k\right) \equiv 0 \pmod 2$ since $4 \mid n$ and so $u \equiv 1 \pmod 4$ which implies $(-1, f(x))_2 = 1$. However:

$$\begin{aligned} g(x) &= 1 - f(x) \\ &= x^n - 2 - 8j \\ &= 1 + 2nk + \binom{n}{2}(2k)^2 + \binom{n}{3}(2k^3) + \cdots - 2 - 8j \\ &= \underbrace{-1 + 2nk + \binom{n}{2}(2k)^2 + \binom{n}{3}(2k^3) + \cdots - 8j}_{u'} \end{aligned}$$

Now, $u' \in \mathbb{U}_2$ and $\epsilon(u) = 0$, which implies that $(-1, g(x))_2 = -1$. This contradicts $(*)$ and so we conclude that $v_2(x) \neq 0$ and $(-1, f(x))_2 = -1$.

Finally, if $v = \infty$ then I claim that $f(x) > 0$. Recall that $(-1, f(x))_\infty = 1$ if and only if $Z^2 + X^2 - f(x)Y^2 = 0$ has a solution in $\mathbb{R}^3$. This is true if and only if $f(x) > 0$ (since $f(x) \neq 0$). Suppose $f(x) < 0$; this implies $-f(x) > 0$ and so $1 - f(x) = g(x) > 0$. This means $(-1, g(x))_\infty = 1$ which by $(*)$ implies $(-1, f(x))_\infty = 1$, which is a contradiction. Thus $f(x) > 0$ and so $(-1, f(x))_\infty = 1$.

Thus so we have:

$$(-1, f(x))_v = \begin{cases} -1 & \text{if } v = 2 \\ 1 & \text{otherwise} \end{cases}$$

This contradicts the product formula (Theorem 2.4.10) and so $Y^2 + Z^2 = f(X)g(X)$ does not have a solution in $\mathbb{Q}^3$. □

This theorem is my own generalisation of the example given by Peyre in [Pey05]. Notice that the fact that n had to be divisible by 4 only came in when we required

$k\left(\frac{n}{2}+\binom{n}{2}k\right) \equiv 0 \,(\mathrm{mod}\, 2)$, at all other instances n being even was sufficient. However, $k\left(\frac{n}{2}+\binom{n}{2}k\right) \equiv 0 \,(\mathrm{mod}\, 2)$ is also true if $n = 2$. In this case $f(x) = -X^2 + 3$ which is precisely the example given by Peyre.

Chapter 3

The Brauer Group

We now seek to generalise the product formula. As it will turn out, the place to look for a generalisation is to determine the Brauer group of $\mathbb{Q}_p$. This is certainly not the obvious place to look; the Brauer group was not introduced to tackle the problem at hand; in fact it initially arose in an attempt to classify division algebras over a field. Thus it is perhaps not surprising that despite having numerous examples of obstructions to the Hasse principle, it took a long time for Manin to find this link. The key point will be that once we determine the Brauer group of $\mathbb{Q}_p$ we will see that we can identify the Hilbert symbol of two elements with an element of this group. This will alow us to see how the fundamental exact sequence of class field theory is a generalisation of the product formula.

The aim of this chapter is, as the name suggests, to define the Brauer group of a field and establish some basic properties.

3.1 Some Ring Theory

In this section I briefly introduce concepts from ring theory which we will need later. Recall the Artin-Wedderburn theorem regarding semisimple rings:

Theorem 3.1.1 (Artin-Wedderburn). *Let R be a semisimple ring. Then*

$$R \simeq \mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_k}(D_k)$$

where D_i is a division ring.

Proof. See page 40 of [FD93]. □

Definition 3.1.2. *We say a ring R is* **simple** *if the only two sided ideals of R are 0 and R.*

Note that if R is simple then its centre, denoted by $Z(R)$, is a field. Also if R is a division ring then it is clearly simple.

Remark 3.1.3. A corollary Artin-Wedderburn theorem says that every simple, artinian ring R, is isomorphic to $\mathcal{M}_n(D)$ for some n and division ring D. Further, R has a unique simple module (up to isomorphism). See page 44 of [FD93] for a proof of this.

Thus, if we want to study simple artinian rings, it is sufficient to restrict our attention to matrix rings with entries from a division ring. Now if D is commutative (i.e. it is a field) then linear algebra theory says that $\mathcal{M}_n(D)$ is isomorphic to the ring $\mathrm{End}_D D^n := \mathrm{Hom}_D(D^n, D^n)$. In general, this is not quite true and the need to create an analogous result motivates the following definition:

Definition 3.1.4. *Given a ring R, define the* **opposite ring** *of R, denoted by R°, to be the ring consisting of the same elements as R, having the same additive structure, but having multiplication done in the reverse order. That is for $x, y \in R^\circ$, $x \cdot y = yx$.*

Proposition 3.1.5. *Let R be a ring. Then*

$$\mathrm{End}_R R \simeq R^\circ$$

Proof. Let $r \in R$ and define $T_r : R \to R$ to be a map such that $T_r s = sr$ for all $s \in R$. This gives a function:

$$\begin{array}{rccc} \phi: & R^\circ & \longrightarrow & \mathrm{End}_R R \\ & r & \longmapsto & T_r \end{array}$$

Note that T_r is in fact R-linear. This would not have been the case had we defined $T_r s = rs$. First we check that this a homomorphism of rings. Let $r, s, x \in R$. $\phi(r \cdot s)(x) = T_{r \cdot s} x = T_{sr} x = xsr$. Also $(\phi(r)\phi(s))x = \phi(r)\left(\phi(s)x\right) = \phi(r)xs = xsr$, and thus ϕ is a homomorphism. Note that the reverse order of multiplication was crucial. Further, it is injective since $T_r = T_s$ implies $r = T_r(1) = T_s(1) = s$ and surjective since for any $f \in \mathrm{End}_R R$, $f = T_{f(1)}$. Thus ϕ is an isomorphism. □

If D is a division ring, then the theory of modules over D is very similar to that over vector spaces over a field. In fact, if one were to go through the derivation of the fact that endomorphisms of a n-dimensional vector space over k correspond to multiplication by $n \times n$ matrices with coefficients in k, but replacing k with D, one would find that the theory is almost identical, except for the fact that the opposite ring appears in various places, as seen in the above proposition. More specifically:

Proposition 3.1.6. *Let D be a division ring. Then:*

$$\mathrm{End}_D(D^n) \simeq \mathcal{M}_n(D^\circ)$$

Proof. When $n = 1$ this was proven in Proposition above. The rest is the same as for vector spaces over a field. For a complete proof see [FD93] pages 34-36. □

Definition 3.1.7. *An* **algebra** *over a commutative ring R, or simply an R-algebra, is a ring A, which is also a R-module such that the following holds:*

$$x(ab) = (xa)b = a(xb) \qquad \text{for all } x \in R,\ a, b \in A$$

Note that R maps into A via $R \to A$ where $r \mapsto r1_A$. Usually we will only be dealing with those cases where R is a field. *Unless otherwise stated, from now on, all algebras are assumed to be finite dimensional over their respective rings.* That is, if A is an R-algebra there exist $\{x_1, \ldots x_n\} \subseteq A$ such that:

$$A = Rx_1 \oplus \cdots \oplus Rx_n$$

If A, B, C are k-algebras then $A \otimes_k B$ is also a k-algebra, where we identify k with $k(1 \otimes 1)$. Note that for $a, a' \in A$ and $b, b' \in B$, $(a \otimes b)(a' \otimes b') := (aa' \otimes bb')$. We also have $A \otimes_k B \simeq B \otimes_k A$ and $A \otimes_k (B \otimes_k C) \simeq (A \otimes_k B) \otimes_k C$ via the obvious canonical maps.

Here are a few more elementary results:

Remark 3.1.8.

(i) Let k be a field. Observe that for $m, n \geq 1$

$$\mathrm{End}_k\,(k^n) \otimes_k \mathrm{End}_k(k^m) \simeq \mathrm{End}_k\,(k^n \otimes_k k^m) \simeq \mathrm{End}_k k^{mn}$$

so we have the isomorphism

$$\mathcal{M}_n(k) \otimes_k \mathcal{M}_m(k) \simeq \mathcal{M}_{mn}(k)$$

(ii) If $A \simeq \mathcal{M}_n(D)$ then $A^\circ \simeq \mathcal{M}_n(D^\circ)$.
(iii) If A is a k-algebra, A° is also a k-algebra.
(iv) If A is a k-algebra $A \otimes_k \mathcal{M}_n(k) \simeq \mathcal{M}_n(A)$
(v) If A is a simple k-algebra, the Artin-Wedderburn Theorem says that $A \simeq \mathcal{M}_n(D)$ for some n and division ring D. And so we have:

$$\begin{array}{ccc} k & \longrightarrow & \mathcal{M}_n(D) \\ \alpha & \longmapsto & \alpha I_n \end{array}$$

Also, $k \subseteq Z(\mathcal{M}_n(D)) \subseteq Z(D)$, where we identify, D with DI_n. And so: $k \subseteq D$. Thus D is itself, a finite dimensional k-algebra.

3.2 Central Simple Algebras and the Brauer Group

The Brauer group will consist of equivalence classes of central simple k-algebras, where multiplication is given by the tensor product. In this section we will formalise this. Note that for any algebra A, over a field k, we always have: $k \subseteq Z(A)$. The case where we have equality, motivates the following definition:

Definition 3.2.1. *A k-algebra A is* **central** *if $Z(A) = k$.*

We thus say a k-algebra A, is a **central simple k-algebra**, if it is both central, and simple when regarded as a ring. Note that since A is finite dimensional over k, by Remark 3.1.3 we know that $A \simeq \mathcal{M}_n(D)$ for some $n > 0$ and division ring D.

Example 3.2.2. The classic example of a central simple k-algebra, is the quaternions:

$$\mathbb{H} := \frac{\mathbb{R}\langle i, j, k\rangle}{(i^2 + 1,\ j^2 + 1,\ k^2 + 1,\ ijk + 1)}$$

which is a central simple $\mathbb{R}$-algebra.[1] To see this, note that it is clearly central, since $Z(\mathbb{H}) = \mathbb{R}$ and it is simple since it is in fact a division ring. This fact also verifies Remark 3.1.3 since $\mathbb{H} = \mathcal{M}_n(D)$ by simply putting $n = 1$ and $D = \mathbb{H}$. I will give a more general construction of a quaternion algebra later.

We now seek to establish various properties regarding central simple algebras which will later form the basis for the definition of the Brauer group. We first prove that the tensor product of two central simple k-algebras is a central simple k-algebra.

[1] Recall that $\mathbb{R}\langle i, j, k\rangle$ is the ring of non-commuting polynomials in i, j, k

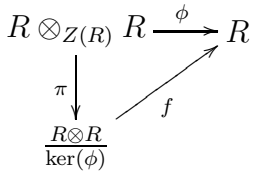
Lemma 3.2.3. *Let R be a simple ring. Suppose $a, b \in R$ are linearly independent over $Z(R)$. Then there exist $r_{i1}, r_{i2} \in R$ with $1 \leq i \leq k$ (for some suitable k) such that:*

$$\sum_{i=1}^{k} r_{i1} a r_{i2} \neq 0 \quad \textit{and} \quad \sum_{i=1}^{k} r_{i1} b r_{i2} = 0$$

Proof. Suppose the claim is false. Let $\phi : R \otimes_{Z(R)} R \to R$ be the map

$$\phi(r_1 \otimes r_2) = r_1 a r_2$$

Thus we have the following commutative diagram:



Where f is the unique, well-defined map that makes the diagram commute, whose existence is guaranteed by the universal properties of quotient groups. However, $\text{im}\,(\phi) = RaR$ and:

$$\begin{aligned} \ker(\phi) &= \left\{ \sum r_{i1} \otimes r_{i2} \mid \sum r_{i1} a r_{i2} = 0 \right\} \\ &= \left\{ \sum r_{i1} \otimes r_{i2} \mid \sum r_{i1} b r_{i2} = 0 \right\} \quad \text{from the assumption} \end{aligned}$$

This implies:

$$\frac{R \otimes_{Z(R)} R}{\ker(\phi)} \simeq RbR$$

Thus we have a well defined map $f : RbR \to R$ given by $f(\sum r_{i1} b r_{i2}) = \sum r_{i1} a r_{i2}$. But $RbR = R$ (since R is simple). Let $z = f(1)$. Since f is both left and right R linear we have for $r \in R$: $zr = (f(1))r = f(1r) = f(r1) = r(f(1)) = rz$. Thus $z \in Z(R)$. But $a = f(1b) = (f(1))b = zb$. This contradicts the assumption that a and b are linearly independent. □

Proposition 3.2.4. *Let k be a field. Let A be a central simple k-algebra and B a k-algebra. Then every non-zero two sided ideal of $A \otimes_k B$ contains an element of the form $1 \otimes b \neq 0$.*

Proof. Let I be a non-zero two sided ideal of $A \otimes_k B$ and $0 \neq a = \sum_{j=1}^{u} a_j \otimes b_j \in I$ with u minimal. By the lemma above, it is possible to find $\{r_{i1}, r_{i2}\}_{i=1}^{k} \subseteq A$ such that we can define $s_j = \sum_{i=1}^{k} r_{i1} a_j r_{i2} \in A$ with $s_{u-1} \neq 0$ and $s_u = 0$. (Note the

minimality of u assures that the a_j's are linearly independent over $Z(A)$.) So we have:

$$\begin{aligned}\sum_{j=1}^{u-1} s_j \otimes b_j &= \sum_{j=1}^{u}\sum_{i=1}^{k} r_{i1} a_j r_{i2} \otimes b_j \\ &= \sum_{i=1}^{k} (r_{i1} \otimes 1) a (r_{i2} \otimes 1) \in I\end{aligned}$$

Thus we can assume $u = 1$. Let $0 \neq a \otimes b \in I$. Then, since A is simple:

$$0 \neq 1 \otimes b \in (R \otimes 1)(a \otimes b)(R \otimes 1) \subseteq I$$

□

Theorem 3.2.5. *Let k be a field and A, B be central simple k-algebras. Then $A \otimes_k B$ is a central simple k-algebra.*

Proof. In the above proposition we showed that since A is simple, any two sided ideal of $A \otimes_k B$ must contain an element of the form $1_A \otimes b$. Arguing in the same way as in the proof above, the simplicity of B gives:

$$1_A \otimes 1_B \in (1_A \otimes B)(1_A \otimes b)(1_A \otimes B)$$

Thus every non-trivial ideal must contain $1_A \otimes 1_B$, and thus must be all of $A \otimes_k B$.

We now show that $A \otimes_k B$ is a k-algebra with centre k. Clearly $k \subseteq Z(A \otimes_k B)$, where we identify k with $k(1 \otimes 1)$, and thus $A \otimes_k B$ is in fact a k algebra. Let $z = \sum a_i \otimes b_i \in Z(A \otimes_k B)$. Without loss of generality we can assume the b_i's are linearly independent. Let $a \in A$. Then:

$$\begin{aligned}0 &= (a \otimes 1)z - z(a \otimes 1) \\ &= \sum (a \otimes 1)(a_i \otimes b_i) - \sum (a_i \otimes b_i)(a \otimes 1) \\ &= \sum (aa_i - a_i a) \otimes b_i\end{aligned}$$

Thus, since the b_i's are linearly independent, we must have $aa_i - a_i a = 0$ which implies $a_i \in Z(A)$ and so $a_i \in k$. Therefore $z = \sum a_i \otimes b_i = \sum 1 \otimes a_i b_i = 1 \otimes b$, for some non-zero $b \in B$ (non-zero by linear independence). Also, for all $x \in B$

$$\begin{aligned}0 &= (1 \otimes x)z - z(1 \otimes x) \\ &= (1 \otimes x)(1 \otimes b) - (1 \otimes b)(1 \otimes x) \\ &= 1 \otimes (xb - bx)\end{aligned}$$

and so $b \in Z(B)$ which implies $b \in k$. Thus $z \in k(1 \otimes 1)$. □

In the Brauer group, the inverse of a central simple algebra, will be the opposite algebra. For this we need the following theorem:

Theorem 3.2.6. *Let A be a central simple k-algebra. Then $A \otimes_k A^\circ \simeq \mathcal{M}_n(k)$ where $n = [A : k]$.*

Proof. Let:

$$S_1 = \{L_a \in \mathrm{End}_k(A) \mid L_a(x) = ax,\ a \in A\}$$
$$S_2 = \{T_a \in \mathrm{End}_k(A) \mid T_r(a) = ra,\ a \in A\}$$

The fact that $S_2 \simeq A^\circ$ and $S_1 \simeq A$ as rings, can be easily proven in an analogous way to Proposition 3.1.5, Also, $L_{a_1}(T_{a_2}(x)) = a_1 x a_2 = T_{a_2}(L_{a_1}(x))$ by associativity of A. We can thus define a map:

$$\begin{array}{ccc} A \otimes_k A^\circ & \longrightarrow & \mathrm{End}_k(A) \\ a_1 \otimes a_2 & \longmapsto & L_{a_1} \circ T_{a_2} \end{array}$$

$A \otimes_k A^\circ$ is simple, by Theorem 3.2.5 and so this map must be injective. Also,

$$[A \otimes_k A^\circ : k] = [A : k]^2 = n^2 = [\mathrm{End}_k(A) : k]$$

and so the map is surjective and thus an isomorphism. Since $\mathrm{End}_k(A) \simeq \mathcal{M}_n(k)$, the proof is complete. □

Let k be a field. We define an equivalence relation, $\sim$ on central simple k-algebras, by saying two central simple algebras A and B are equivalent, (written $A \sim B$) if $A \simeq \mathcal{M}_n(D)$ and $B \simeq \mathcal{M}_m(D')$ with $D \simeq D'$. This clearly defines an equivalence relation, and we denote the equivalence class of A with $[A]$.

Definition 3.2.7. *Let k be a field. The* **Brauer group** *of k, denoted* $\mathrm{Br}(k)$ *is the set of equivalences classes of central simple k-algebras with* $[A] \cdot [B] := [A \otimes_k B]$.

Proposition 3.2.8. *The above action is well-defined and* $\mathrm{Br}(k)$ *is in fact a group under this action.*

Proof. Note firstly that the tensor product of two central simple k-algebras is a central simple k-algebra, so we do have a group action. We now show that it is well-defined. Suppose A, A', B, B' are central simple k-algebras such that $A_1 \sim A_2$ with $A_i \simeq \mathcal{M}_{n_i}(D)$ and $B_1 \sim B_2$ with $B_i \simeq \mathcal{M}_{m_i}(D')$ for $i = 1, 2$. We then have:

$$\begin{aligned} A_1 \otimes_k B_1 &\simeq (D \otimes_k \mathcal{M}_{n_1}(k)) \otimes_k (D' \otimes_k \mathcal{M}_{m_1}) \qquad \text{By Remark 3.1.8(iii)} \\ &= (D \otimes_k D') \otimes_k (\mathcal{M}_{n_1}(k) \otimes_k \mathcal{M}_{m_1}(k)) \\ &\simeq (D \otimes_k D') \otimes_k \mathcal{M}_{m_1 n_1}(k) \qquad \text{By Remark 3.1.8(iii)} \\ &\simeq \mathcal{M}_{m_1 n_1}(D \otimes_k D') \end{aligned}$$

And similarly $A_2 \otimes_k B_2 \simeq \mathcal{M}_{n_2 m_2}(D \otimes_k D')$ and so $A \otimes_k B \sim A' \otimes_k B'$ and thus the operation is well defined. Also since $k \sim \mathcal{M}_n(k)$ and $A \otimes_k k \simeq A$, $[k][A] = [A] = [A][k]$ and so $[k]$ is the identity in the group. Theorem 3.2.6 assures that $[A^\circ]$ is the inverse $[A]$ under the group the multiplication. Associativity is obvious. □

An important fact about central simple algebras, is that all automorphisms are **inner** (i.e. conjugation by a fixed element). This is the Skolem-Noether theorem, which we will now prove. This theorem plays a crucial role in the proofs of Frobenius' theorem (that the only division algebras over $\mathbb{R}$ are $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$) and Wedderburn's theorem (that every finite division ring is a field). These theorems

play no role in our topic so we will not be proving them. However, we will need the Skolem-Noether theorem later when we introduce factor sets. First we need a quick lemma:

Lemma 3.2.9. *Let R be a finite dimensional algebra over k. If M_1 and M_2 are finite dimensional R-modules of the same dimension over k, then $M_1 \simeq M_2$*

Proof. Since R is finite dimensional, and hence artinian, by Remark 3.1.3, R has a unique simple submodule M (up to isomorphism). Thus (since M_1 and M_2 need not be simple) $M_1 \simeq M^{l_1}$ and $M_2 \simeq M^{l_2}$ for some l_1, l_2. M_1 and M_2 have the same dimension over k, implies $l_1 = l_2$ and we are done. □

Theorem 3.2.10 (Skolem-Noether). *Let A be a central simple k-algebra and R a simple k algebra. If $\phi, \psi : R \to A$ are algebra homomorphisms, then there exists and inner automorphism, α of A corresponding to conjugation by $h \in A$ such that $\alpha \circ \phi = \psi$. In particular, any automorphism of A is inner.*

Proof. Since $D^{\circ\circ} = D$ we know that $A \simeq \mathcal{M}_n(D^\circ)$ which, by Proposition 3.1.6 is isomorphic to $\mathrm{End}_D V$ (where $V = D^n$), for some division algebra D. Note that $k = Z(A) = Z(\mathcal{M}_n(D^\circ)) = Z(D)$, by Remark 3.1.8 (v) and the fact that A is central. Also note that since $A \simeq \mathrm{End}_D V$, every $a \in A$ can be viewed as an endomorphism of V. Thus for all $r \in R$ we can define the following two actions of R on V:

$$r \cdot v = \phi(r)(v)$$
$$r \times v = \psi(r)v$$

Note that both actions defined above commute with the action of D on V since $\phi(r)$ and $\psi(r)$ are D linear maps. Thus we can make V into a $R \otimes_k D$ module in two different ways:

$$(r \otimes d)v := r \cdot (dv) = d(r \cdot v) \qquad \text{and}$$
$$(r \otimes d)v := r \times (dv) = d(r \times v)$$

But $R \otimes_k D$ is finite dimensional and simple by Theorem 3.2.5 and thus by the above lemma the two module structures on V are isomorphic. Therefore there exists a $R \otimes_k D$-module isomorphism $h : V \to V$, which by definition must satisfy:

$$h(\phi(r)v) = \psi(r)h(v)$$
$$h(dv) = dh(v)$$

The second equation implies that $h \in \mathrm{End}_D(V) \simeq A$ and the first equation says that $h\phi(r) = \psi(r)h$ i.e. $h\phi(r)h^{-1} = \psi(r)$. Thus conjugation by h defines an inner automorphism. Finally, if we let $R = A$ and let ϕ to be the identity, we see that any other automorphism ψ is inner.

□

3.3 Splitting Fields

Later when we will introduce group cohomology (from which we will get an exact sequence which will generalise the product formula) we will be dealing primarily with relative Brauer groups of a field extension. In order to define this, we first need a quick proposition before we proceed with the definitions.

Proposition 3.3.1 (Extension of the base field). *If A is a central simple k-algebra, and K/k a field extension (not necessarily finite), then $A \otimes_k K$ is a central simple K-algebra.*

Proof. $A \otimes_k K$ is clearly central. To see that it is simple, note that the proof of Proposition 3.2.4 we did not need B to be finite dimensional over k. Thus setting $B = K$ in that proposition, we see that every non-trivial two sided ideal must contain $1 \otimes x$ with $x \in K$ and hence must contain $1 \otimes 1$. Thus $A \otimes_k K$ is simple. □

Definition 3.3.2. *Let A be a central simple k algebra. Say A is* **split** *if $A \simeq \mathcal{M}_n(k)$ for some n. A field extension K/k is a* **splitting field** *of A if the central simple K-algebra $A \otimes_k K$, is split.*

Proposition 3.3.3. *Any simple algebra, A over an algebraically closed field K is split.*

Proof. We know that $A \simeq \mathcal{M}_n(D)$ with $K \subseteq D$ by Remark 3.1.8 for some division ring D. Thus we know that D is an integral domain that is finite dimensional over K, and since K is algebraically closed, $D = K$. □

The latter two propositions imply that if A is a central simple k-algebra, then $A \otimes_k k^{al} \simeq \mathcal{M}_n(k^{al})$ for some n.

Example 3.3.4. If k is algebraically closed then $\mathrm{Br}(k) = \{1\}$ since all algebras are split and are thus the identity in the group.

Corollary 3.3.5. *If A is a central simple k-algebra then $[A : k] = n^2$ for some n.*

Proof. $[A : k] = [A \otimes_k k^{al} : k \otimes_k k^{al}] = [A \otimes_k k^{al} : k^{al}] = n^2$ since $A \otimes_k k^{al} \simeq \mathcal{M}_n(k^{al})$. □

Proposition/Definition 3.3.6. $\mathrm{Br}(\cdot)$ *is a functor, from the category of fields to the category of groups. In particular, given a field homomorphism $\phi : K \to L$, we have the induced group homomorphism map:*

$$\begin{array}{rccc} \mathrm{Br}(\phi): & \mathrm{Br}(K) & \longrightarrow & \mathrm{Br}(L) \\ & [A] & \longmapsto & [A \otimes_K L] \end{array}$$

The kernel of this map, denoted by $\mathrm{Br}(L/K)$ is called the **relative Brauer group** *of L/K.*

In other words $\mathrm{Br}(L/K)$ is the set of equivalence classes of central simple K algebras split by L. Note, as a consequence if A is split then all of $[A]$ is split.

Proof. First, we check that the map is well defined. Suppose we have two equivalent central simple K-algebras, $\mathcal{M}_n(D) \sim \mathcal{M}_m(D)$. Then tensoring with L we get $\mathcal{M}_m(D) \otimes_K L \simeq \mathcal{M}_m(D \otimes_K L) \simeq \mathcal{M}_m(\mathcal{M}_l(D')) \simeq \mathcal{M}_{ml}(D')$ for some division algebra D'. Similarly $\mathcal{M}_n(D) \otimes_K L \simeq \mathcal{M}_{nl}(D')$ and so $\mathcal{M}_n(D) \otimes_K L \sim \mathcal{M}_m(D) \otimes_K L$, and so the map is well defined.

Let $[A], [B] \in \mathrm{Br}(K)$. Let $\tilde{\phi} := \mathrm{Br}(\phi)$, we need to check it is indeed a group homomorphism. We have $\tilde{\phi}([A][B]) = \tilde{\phi}([A \otimes_K B]) = [(A \otimes_K B) \otimes_K L]$. On the other hand, $\tilde{\phi}([A])\tilde{\phi}([B]) = [A \otimes_K L][B \otimes_K L] = [(A \otimes_K L) \otimes_L (B \otimes_K L)] = [A \otimes_k L \otimes_L L \otimes_K B] = [(A \otimes_K B) \otimes_K L]$, and so $\tilde{\phi}$ is a group homomorphism. It it clear that if 1_K is the identity on K then $\mathrm{Br}(1_K)$ is the identity on $\mathrm{Br}(K)$. Finally, if $L' \xrightarrow{\phi} L \xrightarrow{\psi} L''$ are fields, then it is left as an (easy) exercise for the reader to check that $\mathrm{Br}(\psi \circ \phi) = \mathrm{Br}(\psi) \circ \mathrm{Br}(\phi)$. Thus $Br(\cdot)$ is a functor. □

As it will turn out when we introduce cohomology, calculating the relative Brauer group, is significantly easier then calculating the Brauer group directly. What we would like to do, is find a way to express the Brauer group as a union of relative Brauer groups.

Definition 3.3.7. *Let R be an algebra and S a subset of R. The* **centraliser** *of S in R, is defined to be:*

$$C_R(S) = \{r \in R \mid rs = sr \text{ for all } s \in S\}$$

We drop the subscript R if the algebra is clear. Note that $C(S)$ is a sub-algebra of R. We then have the following important theorem:

Theorem 3.3.8 (Double Centraliser Theorem). *Let A be a central simple k-algebra and R a simple sub-algebra of A. Then the following hold:*

(i) *$C(R)$ is simple.*
(ii) *If $A \simeq \mathcal{M}_{n_1}(D_1)$ and $R \otimes_k D_1^\circ \simeq \mathcal{M}_{n_2}(D_2)$, then $C(R) \simeq \mathcal{M}_{n_3}(D_2^\circ)$.*
(iii) *$[A : k] = [R : k][C(R) : k]$.*
(iv) *$C(C(R)) = R$.*

where D_i are division algebras.

Proof. See [FD93] page 94. □

Definition 3.3.9. *Let S be a simple k-algebra. A* **maximal subfield** *of S is defined to be a field $K \subseteq S$ containing k such that $C(K) = K$*

This definition is slightly different to the "usual" notion of maximal, i.e. maximal with respect to inclusion. If S is a division ring then these two definitions coincide[2] and the maximal subfield exists. If S is not a division ring, then $C(K)$ need not be a field, and in fact, if S is not a division ring, then a maximal subfield may not even exist.

Theorem 3.3.10. *Let A be a central simple k-algebra, with $[A; k] = n^2$. Then any maximal subfield K of A is a splitting field for A, and $[A : K] = [K : k] = n$. Conversely, given any field extension K/k with $[K : k] = n$, any element of $\mathrm{Br}(K/k)$ has a unique representative A with $[A : k] = n^2$ which contains K as a maximal subfield.*

[2] This is very easy to check.

Proof. Recall also that Corollary 3.3.5 implies that $[A : k]$ is indeed a square. Apply Theorem 3.3.8 (*iii*) with $R = K$ and since $C(K) = K$ we get $n^2 = [K : k]^2$ and so $[K : k] = n$. Also, $n^2 = [A : k] = [A : K][K : k]$ implies $[A : K] = n$. To show K splits A, we first impose an $A - K$ bimodule structure on A (with the obvious actions) and note that by associativity of A these actions commute. Thus we define the map:

$$\phi : A \otimes_k K \longrightarrow \mathrm{End}_K(A) \simeq \mathcal{M}_n(K)$$

where $\phi(a \otimes x)(a') = aa'x$. Since $A \otimes_k K$ is simple by Proposition 3.3.1, and ϕ is clearly non-zero, it must have a trivial kernel, implying it is one-to-one. Also since, $[A \otimes_k K : k] = [A : k][K : k] = n^3$ and $[\mathcal{M}_n(K) : k] = n^3$ we deduce the map is onto. Thus ϕ is an isomorphism and so $A \otimes_k K \simeq \mathcal{M}_n(K)$ and so K splits A.

Conversely, suppose K/K is a field extension. Pick an element of $\mathrm{Br}(K/k)$ and let D be the representative of the chosen equivalence class. Then, by definition $K \otimes_k D \simeq \mathcal{M}_m(K)$ for some m, which also implies that $K \otimes_k D^\circ \simeq \mathcal{M}_m(K)$. Computing the dimensions of both sides over K gives $[K : k][D^\circ : k] = m^2[K : k]$ which implies that

$$[D^\circ : k] = m^2$$

We know that $K \otimes_k D^\circ$ has a unique (up to isomorphism) simple left module, and we denote it by V. Thus it we see that $K \otimes_k D^\circ \simeq V^m$. Therefore, computing the dimensions over k of both sides we get that $[K : k][D^\circ : k] = m \cdot [V : D][D : k]$ and so:

$$m \cdot [V : D] = [K : k]$$

Now if we associate K with $K \otimes_k 1$ and D° with $1 \otimes_k D^\circ$ we see that actions of K and D° on V must commute since $(x \otimes 1)(1 \otimes d) = (1 \otimes d)(x \otimes 1)$. Thus the action of K on V defines a homomorphism

$$K \longrightarrow End_{D^\circ}(V) \overset{3.1.6}{\simeq} \mathcal{M}_{[V:D]}(D)$$

The map is injective since K is a field. Now let $A = \mathcal{M}_{[V:D]}(D)$ and note that K is a sub-algebra of A. Then since $A \sim D$ we have:

$$[A : K] = [V : D]^2[D : k] = [V : D]^2 m^2 = ([V : D] \cdot m)^2 = [K : k]^2$$

Now we apply the Double Centraliser Theorem and get:

$$[K : k]^2 = [A : k] = [K : k][C(K) : k]$$

and thus $[K : k] = [C(K) : k]$ and since $K \subseteq C(K)$ we have $C(K) = K$. Uniqueness follows from the dimension of A. □

Remark 3.3.11. Note that despite the fact that we are not guaranteed the existence of a maximal subfield of A we are guaranteed one for D when D is a division ring. So suppose A is a central simple k-algebra isomorphic to $\mathcal{M}_n(D)$ with K being a maximal subfield of D. By the above theorem K splits D and thus all of $[A]$ since $[A] = [D]$.

Thus we have found ways to split central simple algebras. However, when we introduce cohomology, or more precisely, Galois cohomology, it will be crucial for us to know that not only do splitting fields exists, but that we can always find one that is Galois. This fact will be corollary to the following theorem:

Theorem 3.3.12 (Jacobson-Noether). *If D is a division algebra over k, then D contains a maximal subfield K which is a separable extension of k.*

Proof. Separability is always guaranteed if the characteristic of k is zero. So suppose the characteristic of k is p. Suppose D has no separable extensions over k. Then every $\beta \in D - k$ is purely inseparable. Take such a β whose minimal polynomial has smallest degree. The minimal polynomial must be of the form $a_0 + a_1 x^p + a_2 x^{2p} + \dots a_n x^{np}$ to guarantee that its derivative is zero. Then $\beta^p \in k$ for otherwise it would have a minimal polynomial of a smaller degree. We define a map $\phi : D \to D$ by $\phi(d) := [\beta, d] := \beta d - d\beta$. Then:

$$\phi^p(d) = \sum_{i=0}^{p} (-1)^i \beta^{p-1} d \beta^i = \beta^p d - d\beta^p = 0$$

and the last equality holds since $\beta^p \in K$ which means that it commutes with d. Now ϕ is not the zero map since $\beta d - d\beta \neq 0$ and so there exist $i \geq 1$ and $x \in D$ such that $\phi^i(z) = y \neq 0$ and $\phi^{i+1}(z) = 0$; i.e. $[\beta, x] = \beta x - x\beta = y \neq 0$ and $[\beta, y] = 0$. This implies:

$$[\beta, xy^{-1}] = \beta x y^{-1} - x y^{-1} \beta = (y + x\beta) y^{-1} - x b y^{-1} = 1$$

and hence $[\beta, \beta x y^{-1}] = \beta$. Let $\omega = \beta x y^{-1}$. Then we have $\beta = \beta\omega - \omega\beta$ and so $\beta\omega\beta^{-1} = 1 + \omega$. However, there exist $r > 0$ such that if we let $q = p^r$, then $\omega^q \in K$ and hence commutes with β. Thus we have:

$$\omega^q = \beta \omega^q \beta^{-1} = \left(\beta \omega \beta^{-1}\right)^q = (1 + \omega)^q = 1 + \omega^q$$

which is a contradiction.

□

Corollary 3.3.13. *Let D be a division algebra with centre k and let $n^2 = [D : k]$. Then there exists a finite Galois extension K/k which splits D.*

Proof. The Jacobson-Noether Theorem guarantees the existence of a maximal subfield $L \subset D$ which is separable over k. It is finite dimensional over k since D is. Let K be the normal closure of L/k. Galois theory assures K/k is finite and Galois. Furthermore, we have: $D \otimes_k K \simeq (D \otimes_k L) \otimes_L K \simeq \mathcal{M}_n(L) \otimes_L K \simeq \mathcal{M}_n(K)$. □

Corollary 3.3.14. *Let k be a field. Then:*

$$\mathrm{Br}(k) \simeq \bigcup_K \mathrm{Br}(K/k)$$

where K ranges over all finite Galois extensions of k.

Proof. Follows immediately from the above corollary and Remark 3.3.11. □

A quick summary: given a central simple k-algebra A, the Wedderburn Artin Theorem implies that there exists a division ring D such that $A \sim D$. Corollary 3.3.13 assures that we can find a finite Galois extension K/k such that D is split by K. Of course D may not contain K (since in the proof we took the normal closure of the maximal subfield). Remark 3.3.11 says that K also splits A. And finally Theorem 3.3.10 assures that there exists an $A' \sim A$ which actually contains K as a maximal subfield. With this we proceed.

3.4 Factor Sets and Crossed Product Algebras

The goal of this section is to give a different way of looking at elements of the group $\mathrm{Br}(K/k)$ for a Galois field extension K/k. We will see straight away the Skolem-Noether Theorem in action and will also see why we required Galois splitting fields. Using the Galois group of K/k we will define factor sets and use them to construct central simple k-algebras, called crossed product algebras. We will show that there is a one-to-one correspondence between crossed product algebras and $\mathrm{Br}(K/k)$, and later, when we introduce cohomology, we will see that in fact, the correspondence is an isomorphism of groups.

Fix a Galois field extension K/k and A a representative of $[A] \in \mathrm{Br}(K/k)$ containing K as a maximal subfield. Let $G := \mathrm{Gal}(K/k)$. Then, by the Skolem-Noether Theorem, for any $\sigma \in G$ there exists $x_\sigma \in A$ such that

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

or equivalently $x_\sigma a = \sigma(a) x_\sigma$. Note that x_σ is only unique up to scalar multiplication by non-zero elements of K; this can be see by noting that if both x_σ and x'_σ satisfy 3.1 then for all $a \in K$

$$x'_\sigma x_\sigma^{-1} a \left(x'_\sigma x_\sigma^{-1}\right)^{-1} = a$$

since $\sigma^{-1}(a) = x_\sigma^{-1} a x_\sigma$. Thus $x'_\sigma x_\sigma^{-1} \in C(K) = K$ and so there exist $f_\sigma \in K^*$ such that:

$$x'_\sigma = f_\sigma x_\sigma \tag{3.2}$$

Thus, since for $\sigma, \tau \in G$ and $a \in K$, $(\sigma\tau)(a) = \sigma(\tau(a))$ there exists $a_{\sigma,\tau} \in K^*$

$$x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau} \tag{3.3}$$

Notation 3.4.1. We abbreviate $\{x_\sigma \mid \sigma \in G\}$ with $\{x_\sigma\}$ and $\{a_{\sigma,\tau} \mid \sigma, \tau \in G\}$ with $\{a_{\sigma,\tau}\}$.

Definition 3.4.2. *The collection $\{a_{\sigma,\tau}\}$ is called the* **factor set** *of A relative to K.*

As discussed before, since the set $\{x_\sigma\}$ is not unique neither is the factor set. So suppose we have have $\{x_\sigma\}$ with factor set $\{a_{\sigma,\tau}\}$ and $\{x'_\sigma\}$ with factor set $\{b_{\sigma,\tau}\}$,

both being factor sets of A relative to K. With this setup we say that the two factor sets are **equivalent**, written as $\{a_{\sigma,\tau}\} \sim \{b_{\sigma,\tau}\}$. Note that:

$$\begin{array}{ll} x'_\sigma x'_\tau = f_\sigma x_\sigma f_\tau x_\tau & \text{by 3.2} \\ b_{\sigma,\tau} x'_{\sigma,\tau} = f_\sigma \sigma(f_\tau) x_\sigma x_\tau & \text{by 3.3 and 3.1} \\ b_{\sigma,\tau} f_{\sigma\tau} x_{\sigma\tau} = f_\sigma \sigma(f_\tau) a_{\sigma,\tau} x_{\sigma\tau} & \text{by 3.2 and 3.3} \end{array}$$

and so the relationship between the two equivalent factor sets is:

$$b_{\sigma,\tau} = \frac{f_\sigma \sigma(f_\tau)}{f_{\sigma\tau}} a_{\sigma,\tau} \tag{3.4}$$

Definition 3.4.3. *If we choose $x_{id} = 1$ then $a_{id,\sigma} = a_{\sigma,id} = 1$ for all $\sigma \in G$. Such a factor set is called* **normalised**.

Proposition 3.4.4. *$\{x_\sigma\}$ is a basis for A over K.*

Proof. Note that $|G| = [K : k] = [A : K]$ where the first equality is coming from the fact that G is Galois and the second from Theorem 3.3.10. Thus we only need to show linear independence. We argue by contradiction. Suppose that $\{x_\sigma\}$ are not independent. Let $H \subsetneq G$ be maximal such that $\{x_\tau \mid \tau \in H\}$ is independent. Let $\sigma \in G - H$. Then

$$x_\sigma = \sum_{\tau \in H} a_\tau x_\tau \quad \text{with } a_\tau \in K \tag{$\dagger$}$$

and so for any $r \in K$ we have $x_\sigma r = \sum a_\tau x_\tau r$ which by 3.1 implies

$$\sigma(r) x_\sigma = \sum_{\tau \in H} a_\tau \tau(r) x_\tau \tag{$*$}$$

If, however, we multiply both sides of ($\dagger$) on the left by $\sigma(r)$ and compare coefficients of x_τ with that of ($*$) we get that $a_\tau \tau(r) = \sigma(r) a_\tau$ for all $\tau \in H$, $r \in K$. Since $x_\sigma \neq 0$ there exists $\tau \in H$ with $a_\tau \neq 0$. Thus $\tau(r) = \sigma(r)$ for all $r \in K$. This implies $\sigma = \tau \in H$, contradicting the choice of σ. □

This proposition shows that any cental simple k-algebra which contains its maximal subfield K such that K/k is Galois with Galois group G can be written as

$$A = \bigoplus_{\sigma \in G} K x_\sigma$$

with

$$\begin{aligned} x_\sigma a &= \sigma(a) x_\sigma \quad \text{for all } a \in K \\ x_\sigma x_\tau &= a_{\sigma,\tau} x_{\sigma\tau} \end{aligned}$$

Of course, the far more interesting question is the converse of the above result: given a Galois field extension K/k what conditions must be imposed on an arbitrary set $\{a_{\sigma,\tau}\} \subseteq K^*$ such that we can can construct a central simple k algebra as above. The following theorem answers that question:

Theorem 3.4.5. *Let K/k be a Galois field extension with Galois group G. A set $\{a_{\sigma,\tau}\} \subset K^*$ is a factor set relative to K of a central simple k-algebra A if and only if the following holds:*

$$\rho(a_{\sigma,\tau})a_{\rho,\sigma\tau} = a_{\rho,\sigma}a_{\rho\sigma,\tau} \quad \textit{for all } \rho,\sigma,\tau \in G \tag{3.5}$$

Moreover, A contains K as a maximal subfield.

Proof. ($\Rightarrow$) The fact that A contains K as a maximal subfield is part of the definition of a factor set. Let $\rho,\sigma,\tau \in G$. We get that

$$\begin{array}{lll} & x_\rho(x_\sigma x_\tau) = (x_\rho x_\sigma)x_\tau & \text{by associativity of } A \\ \Longrightarrow & x_\rho a_{\sigma,\tau}x_{\sigma\tau} = a_{\rho,\sigma}x_{\rho\sigma}x_\tau & \text{by Equation 3.3} \\ \Longrightarrow & \rho(a_{\sigma,\tau})a_{\rho,\sigma\tau}x_{\rho\sigma\tau} = a_{\rho,\sigma}a_{\rho\sigma,\tau}x_{\rho\sigma\tau} & \text{by Equation 3.1 and 3.3} \\ \Longrightarrow & \rho(a_{\sigma,\tau})a_{\rho,\sigma\tau} = a_{\rho,\sigma}a_{\rho\sigma,\tau} & \end{array}$$

and we are done.
($\Leftarrow$) Our goal is to construct a central simple k-algebra with the given factor set. Let A be a vector space over K with basis $\{e_\sigma \mid \sigma \in G\}$. We define multiplication by $(\alpha e_\sigma)(\beta e_\tau) := \alpha\sigma(\beta)a_{\sigma,\tau}e_{\sigma\tau}$ and claim that A becomes an algebra with identity $a_{1,1}^{-1}e_1$. We now prove this claim. Note firstly that Equation 3.5 implies that $1_G(a_{1,\sigma})a_{1,\sigma} = a_{1,1}a_{1,\sigma}$ and so $a_{1,1} = a_{1,\sigma}$. This implies $(a_{1,1}^{-1}e_1)e_\sigma = a_{1,1}^{-1}a_{1,\sigma}e_\sigma = a_{1,1}^{-1}a_{1,1}e_\sigma = e_\sigma$. Similarly, Equation 3.5 implies that $\sigma(a_{1,1})a_{\sigma,1} = a_{\sigma,1}a_{\sigma,1}$ and so $\sigma(a_{1,1}) = a_{\sigma,1}$ and since σ is a field homomorphism we get $\sigma(a_{1,1}^{-1}) = a_{\sigma,1}^{-1}$. From this we get that $e_\sigma(a_{1,1}^{-1})e_1 = \sigma(a_{1,1}^{-1})a_{\sigma,1}e_\sigma = a_{\sigma,1}^{-1}a_{\sigma,1}e_\sigma = e_\sigma$ an thus $a_{1,1}^{-1}e_1$ is indeed the identity. To show the associativity we note that

$$\begin{aligned}(\alpha e_\sigma \beta e_\tau)\gamma e_\rho &= \alpha\sigma(\beta)a_{\sigma,\tau}e_{\sigma\tau}\gamma e_\rho \\ &= \alpha\sigma(\beta)a_{\sigma,\tau}\sigma(\tau(\gamma))a_{\sigma\tau,\rho}e_{\sigma\tau\rho}\end{aligned}$$

And similarly:

$$\begin{aligned}\alpha e_\sigma(\beta e_\tau \gamma e_\rho) &= \alpha e_\sigma(\beta\tau(\gamma)a_{\tau,\rho}e_{\tau\rho}) \\ &= \alpha\sigma(\beta\tau(\gamma)a_{\tau,\rho})a_{\sigma,\tau\rho}e_{\tau\rho} \\ &= \alpha\sigma(\beta)\sigma(\tau(\gamma))\sigma(a_{\tau,\rho})a_{\sigma,\tau\rho}e_{\sigma\tau\rho}\end{aligned}$$

and so associativity will follow provided we have $\sigma(a_{\tau,\rho})a_{\sigma,\tau\rho} = a_{\sigma,\tau}a_{\sigma\tau,\rho}$; but this follows from, Equation 3.5.
Distributive laws follow immediately from the definition.
Now, K is a subfield of A when identified with $K(a_{1,1}^{-1}e_1)$. To show it is maximal, we need to show that $C_A(K) = K$. Suppose $\sum_{\sigma\in G}\alpha_\sigma e_\sigma \in C(K)$. Then:

$$\begin{aligned}x\left(\sum \alpha_\sigma e_\sigma\right) &= \left(\sum \alpha_\sigma e_\sigma\right)x \quad \text{for all } x \in K \\ &= \sum \alpha_\sigma\sigma(x)e_\sigma\end{aligned}$$

and so $x\alpha_\sigma = \alpha_\sigma\sigma(x)$ for all $x \in K$. If $\alpha_\sigma \neq 0$ then $x = \sigma(x)$ i.e σ is the identity in G and so $\alpha_\sigma = 0$ if σ is not the identity. Thus $\sum \alpha_\sigma e_\sigma = a_1e_1 \in K$. So $C(K) \subseteq K$,

and since reverse inclusion is obvious, $C(K) = K$.
Similarly we now show that $Z(A) = k$. Let $\sum_{\sigma \in G} \alpha_\sigma e_\sigma \in Z(A)$. The same argument as above shows that $\sum \alpha_\sigma e_\sigma = \alpha_1 e_1$ with $\alpha_1 \in K^*$. Now, for all $\tau \in G$:

$$\begin{array}{ll} & e_\tau \alpha_1 e_1 = \alpha_1 e_1 e_\tau \\ \implies & \tau(\alpha_1) a_{\tau,1} e_\tau = \alpha_1 a_{1,\tau} e_\tau \\ \implies & \alpha_1 = \tau(\alpha_1) \quad \text{for all } \tau \in G \quad (\text{Since } a_{1,\tau} = a_{\tau,1}) \\ \implies & \alpha_1 \in k \end{array}$$

and so $Z(A) \subseteq k$ and since reverse inclusion is obvious, $Z(A) = k$.
Now to show A is simple. Suppose $I \neq A$ is a two sided ideal. Since $I \cap K = \varnothing$ we get that $K \hookrightarrow A/I$ is an injection. Let $\bar{e}_\sigma$ be the image of e_σ under this map. The proof that $\{\bar{e}_\sigma\}$ is a basis for A/I is the the same as the proofs that e_σ is a basis for A, and so $I = 0$. Thus A is a central simple k-algebra, containing K as a maximal subfield.

□

Note that in light of the above theorem, any set of elements $\{a_{\sigma,\tau}\} \subseteq K^*$ satisfying 3.5 will be called a **factor set** relative to K, i.e. there is no need to give an algebra of which it is a factor set, since we know a unique one exists.[3] Moreover, we can now say that two factor sets $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ are **equivalent**, written $\{a_{\sigma,\tau}\} \sim \{b_{\sigma,\tau}\}$, if there exists $\{f_\sigma \mid \sigma \in G\}$ such that 3.4 holds. The construction in the above theorem, motivates the following definition:

Definition 3.4.6. *With the notion as in the above theorem, the constructed central simple k-algebra containing K, is called the* **crossed product algebra** *of K and G relative to the factor set $\{a_{\sigma,\tau}\}$ and is denoted by $(K, G, \{a_{\sigma,\tau}\})$.*

Of course we would like to say that equivalent factor sets give rise to isomorphic central simple algebras. The following proposition says precisely that:

Proposition 3.4.7. *Let K/k be a Galois field extension with Galois group G. Suppose $\{a_{\sigma,\tau}\} \sim \{b_{\sigma,\tau}\}$ are factor sets relative to K. Then $(K, G, \{a_{\sigma,\tau}\}) \simeq (K, G, \{b_{\sigma,\tau}\})$.*

Proof. Let $\{x'_\sigma\}$ be the basis for $(K, G, \{b_{\sigma,\tau}\})$ as constructed in Theorem 3.4.5 and $\{x_\sigma\}$ a basis for $(K, G, \{a_{\sigma,\tau}\})$. Note that for some $\{f_\sigma \mid \sigma \in G\}$ 3.4 holds. We define the following map:

$$\begin{array}{rcl} \phi : (K, G, \{b_{\sigma,\tau}\}) & \longrightarrow & (K, G, \{a_{\sigma,\tau}\}) \\ x'_\sigma & \longmapsto & f_\sigma x_\sigma \end{array}$$

extend ϕ linearly to all of $(K, G, \{b_{\sigma,\tau}\})$. We claim that ϕ is a k-algebra homomorphism. The only thing that needs checking is whether given $\alpha \in K$ and $\sigma, \tau \in G$ we have $\phi(x_\sigma \alpha x'_\tau) = \phi(x'_\sigma)\phi(\alpha x'_\tau)$; the rest follows by definition of ϕ. Now

$$\begin{aligned} \phi(x_\sigma \alpha x'_\tau) &= \phi\left(\sigma\left(\alpha\right) b_{\sigma,\tau} x'_{\sigma\tau}\right) \\ &= \sigma(\alpha) b_{\sigma,\tau} f_{\sigma\tau} x_{\sigma\tau} \end{aligned}$$

[3] Unique by Theorem 3.3.10.

And

$$\begin{aligned}\phi(x'_\sigma)\phi(\alpha x'_\tau) &= f_\sigma x_\sigma \alpha f_\tau x_\tau \\ &= f_\sigma \sigma(\alpha) x_\sigma f_\tau x_\tau \\ &= f_\sigma \sigma(\alpha)\sigma(f_\tau) a_{\sigma,\tau} x_{\sigma\tau}\end{aligned}$$

The two expression are equal precisely when

$$b_{\sigma,\tau} f_{\sigma\tau} = f_\sigma \sigma(f_\tau) a_{\sigma,\tau}$$

which is exactly Equation 3.4. Injectivity and surjectivity are obvious, and so we are done. □

Thus, we have essentially proven the following crucial theorem:

Theorem 3.4.8. *Let K/k be a Galois field extension. Then there is a one-to-one correspondence between elements of* $\mathrm{Br}(K/k)$ *and equivalence classes of factor sets relative to K.*

Proof. Theorem 3.3.10 says that there exists a unique central simple k-algebra A which has K as a maximal subfield, and $[A] \in \mathrm{Br}(K/k)$. We thus have the map

$$\begin{array}{rcl}\mathrm{Br}(K/k) & \longrightarrow & \{\text{equivalence class of factor sets}\} \\ [A] & \longmapsto & \{\text{factor set of } A \text{ relative to } K\}\end{array}$$

This map is well-defined since there is only one element in each equivalence class through which it is defined and if K embeds in A on more than one way, then by the Skolem-Noether Theorem the embedding is unique up to conjugation, implying they give rise to equivalent factor sets.

Conversely, given an equivalence class of factor sets, with $\{a_{\sigma,\tau}\}$ being an element of the equivalence class we have the map

$$\begin{array}{rcl}\{\text{equivalence class of factor sets}\} & \longrightarrow & \mathrm{Br}(K/k) \\ \{a_{\sigma,\tau}\} & \longmapsto & [(K, G, \{a_{\sigma,\tau}\})]\end{array}$$

and this map is well defined by Proposition 3.4.7. The two maps are clearly inverses. □

Thus we have established a strong relationship between crossed product algebras and the relative Brauer group. What is more surprising is that we will discover that not only is there an isomorphism between the relative Brauer group and the corresponding crossed product algebras when regarded as sets, but also as abelian groups (after of course we give the set of crossed product algebras an abelian group structure). In order to do this, we need to introduce cohomology and, as we will see, there is an isomorphism of abelian groups between a certain cohomology group and the set of crossed product algebras. We could launch into that theory very quickly, but since we will need even deeper knowledge of homological algebra later, it is better to develop that theory first in general, and then apply it to the problem at hand.

Chapter 4

Homological Algebra

In the first section of this chapter, I will develop the theory of homological algebra through category theory. Category theory takes the viewpoint that in order to study objects, we should study the morphism between them, and not the objects themselves directly. We will see that this approach will be in many ways a very natural one for it avoids, both in the definitions and in the proofs, having to pick specific elements. For example we will define the kernel of a map without having to refer to any elements, namely the ones that get mapped to zero. The downside is that we need many new definitions. As we will see, a lot of the objects that we will define we would have already met before, such as the already mentioned kernel of a map. The definitions given here will always coincide with the previous ones, in the cases where they both make sense. In the latter section, we will see a direct application of this theory, and develop Galois cohomology.

4.1 Category Theory

A **category** $\mathscr{C}$ consists of the following data:

(I) a class $|\mathscr{C}|$ of objects;

(II) for each ordered pair of objects (A, B) of $|\mathscr{C}|$ a set $\mathrm{Hom}_{\mathscr{C}}(A, B)$ or $[A, B]_{\mathscr{C}}$ of objects called the set of **morphisms** from A to B. We drop the subscript if the category is clear;

(III) for each ordered triple (A, B, C) of objects a map:

$$[B, C] \times [A, B] \longrightarrow [A, C]$$

sending $(g, f) \mapsto g \circ f$ called the composition of morphisms. We usually just write gf.

Further, the data is subject to the following conditions

(a) The sets $[A, B]$ are pairwise disjoint for all $A, B \in |\mathscr{C}|$;

(b) for all $f, g, h \in [A, B]$ we have $(hg)f = h(gf)$;

(c) for all $A \in |\mathscr{C}|$ there exists $1_A \in [A, A]$ such that $1_A f = f$ and $g1_A = g$ whenever the composition is defined.

We define

$$\mathrm{Mor}\, \mathscr{C} = \bigcup_{A,B \in |\mathscr{C}|} [A, B]$$

Example 4.1.1. We have already met many examples. The class of rings, together with ring homomorphisms, form a category; as do the class of R-modules together with R-module homomorphisms. The class of sets also form a category.

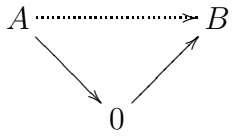
The category of R-modules (and most other categories we have met) contains a trivial module, namely the module 0. An important property of this module, is that it is isomorphic to a submodule of every other module in the category. We extend this to a general category $\mathscr{C}$ by saying an object $P \in |\mathscr{C}|$ is **terminal** if for all $A \in |\mathscr{C}|$, there exists a unique morphism $A \to P$. Similarly, an object $Q \in |\mathscr{C}|$ is **initial** if for all $A \in |\mathscr{C}|$, there exists a unique morphism $Q \to A$. An object that is both terminal and initial is called a **zero** object; note that there may be more than one of these.

We now aim to define the notion of an isomorphism. We say a morphism $m \in \operatorname{Mor} \mathscr{C}$ is a **monomorphism** if for all $f, g \in \operatorname{Mor} \mathscr{C}$, $mf = mg$ implies $f = g$. We say a morphism $e \in \operatorname{Mor} \mathscr{C}$ is a **epimorphism** if for all $f, g \in \operatorname{Mor} \mathscr{C}$, $fe = ge$ implies $f = g$. Finally, we say a morphism $f \in [A, B]$ is an **isomorphism** if there exists $g \in [B, A]$ such that $gf = 1_A$ and $gf = 1_B$.

Remark 4.1.2. It follows immediately that if $\mathscr{C}$ has a zero object, then:

(i) there exists a unique isomorphism between any pair of zero objects. So we can fix one zero object and denote it by 0;

(ii) if $A, B \in |\mathscr{C}|$ then there exists a unique morphism $A \to B$ which factors through zero. That is the following diagram commutes.



We call this the zero morphism and denote it by 0_{AB} or simply 0.

In the previous chapters we have used the term "functor" twice already, assuming the reader was familiar with it. We can now define it, in the most abstract setting.

Definition 4.1.3. *Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be two categories. A* **covariant functor** *$F : \mathscr{C}_1 \to \mathscr{C}_2$ consists of two maps $F\colon |\mathscr{C}_1| \to |\mathscr{C}_2|$ and $F\colon \operatorname{Mor} \mathscr{C}_1 \to \operatorname{Mor} \mathscr{C}_2$ such that for $g\colon A \to B$ in $\operatorname{Mor} \mathscr{C}_1$, $F(g)\colon F(A) \to F(B)$ is in $\operatorname{Mor} \mathscr{C}_2$, $F(1_A) = 1_{F(A)}$ and for every $h\colon B \to C$ in $\operatorname{Mor} \mathscr{C}$ we have $F(hg) = F(h)F(g)$.*

Diagrams play a crucial role in category theory; as we will see, some concepts are defined through diagrams. We thus need to formalise our diagrams to remove any ambiguity.

An **oriented graph**, Σ consists of two sets $Ve(\Sigma)$ and $Ar(\Sigma)$, (vertices and arrows, written simply as Ve and Ar if Σ is clear from the context), and two maps $o, e : Ar \to Ve$, (origin and end). A **diagram of type** Σ in a category $\mathscr{C}$ is a map $D : \Sigma \to \mathscr{C}$ such that:

(a) for all $i \in Ve$, $D(i) \in \mathscr{C}$;

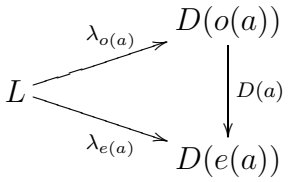
(b) for all $a \in Ar$, $D(a)\colon D(o(a)) \to D(e(a)) \in \operatorname{Mor} \mathscr{C}$.

So in a diagram, vertices correspond to object in $|\mathscr{C}|$ and arrows to morphism in $\operatorname{Mor} \mathscr{C}$ between the objects.

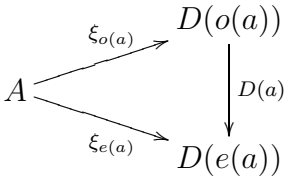
As mentioned earlier, we will define the kernel (and many other concepts) of a morphism in a general category through the corresponding universal property which it satisfies in the case of R-modules. For this we need the following definition:

Definition 4.1.4. *Let Σ be an oriented graph, and D a diagram, in a category $\mathscr{C}$ of type Σ. A* **limit** *of $D : \Sigma \to \mathscr{C}$ consists of an object $L \in |\mathscr{C}|$ and morphism $\lambda_i : L \to D(i)$ for all $i \in Ve$ such that:*

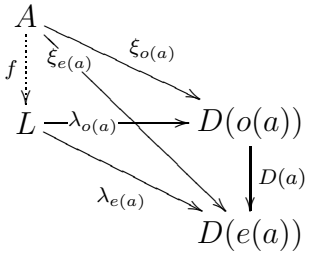
(a) *for every $a \in Ar$ the following diagram commutes:*



(b) *for any (other) object $A \in |\mathscr{C}|$, and morphisms $\xi_i : A \to D(i)$ making the following diagram commute for every $a \in Ar$*



there exists a unique morphism $f \in [A, L]$ such that



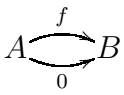
commutes.

Once we have the definition of a limit, we can define the **colimit** of D, by "reversing all the arrows in a sensible way".[1] More precisely, the **colimit** of a diagram $D : \Sigma \to \mathscr{C}$ consists of an object $M \in |\mathscr{C}|$, and morphism $\lambda_i : D(i) \to M$ for all $i \in Ve$ such that:

(a) for every $a \in Ar$ the corresponding diagram (as in the definition of limit but with the two diagonal arrows reversed) commutes:

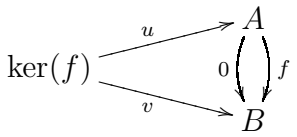
(b) for any (other) object $A \in |\mathscr{C}|$, and morphisms $\xi_i : D(i) \to A$ making the corresponding diagram commute for every $a \in Ar$, there exists a unique morphism $f \in [M, A]$ such that the corresponding diagram commute.

Example/Definition 4.1.5. Let $\mathscr{C}$ be a category with a zero object and $A, B \in |\mathscr{C}|$. Let $f \in [A, B]$. Then the **kernel** of f, denoted $\ker(f)$, is defined to be the limit of the following diagram:

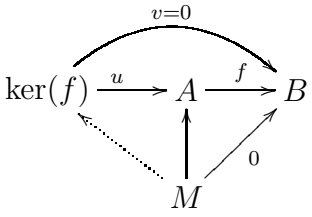


[1] In category theory, this is a very common technique for getting definitions of new concepts out of pre-existing ones.

To see why this agrees with the more familiar universal property of kernels, suppose that $\mathscr{C}$ is the category of R-modules. Then, if we unravel the definitions we get:



Now, part (a) of the definition implies $v = 0u = 0$. And part (b) implies that for any other R-module M, satisfying (a) there exists a unique map $M \to \ker(f)$ such that



commutes. This is precisely the universal property of kernels (in the old sense), and so the universal property coincides with the definition.

Similarly, we define the cokernel of f, denoted by $\operatorname{coker}(f)$, as the colimit of the same diagram as in the example above. In the case of R-modules this is just $B/\operatorname{im}(f)$, and so we have generalised the concept of a quotient. It can also be shown that both kernel and cokernel are unique up to a unique isomorphism. The above also suggests we need a categorical definition of image:

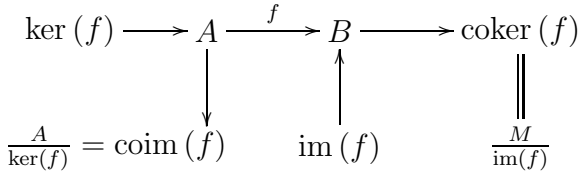
Definition 4.1.6. *Let $\mathscr{C}$ be a category, $A, B \in |\mathscr{C}|$ and $f \in [A, B]$. By the definition of kernel and cokernel there exists a map $\ker(f) \to A$ and $B \to \operatorname{coker}(f)$. We define the* **image** *of f, denoted by $\operatorname{im}(f)$ to be;*

$$\operatorname{im}(f) := \ker(B \longrightarrow \operatorname{coker}(f))$$

and the **coimage** *of f, denoted by $\operatorname{coim}(f)$ to be:*

$$\operatorname{coim}(f) := \operatorname{coker}(\ker(f) \longrightarrow A)$$

Let us compare this with the definitions we know if $\mathscr{C}$ is the category of R-modules. The fact that the definitions of image coincides is obvious, since $\operatorname{coker}(f) = B/\operatorname{im}(f)$. We can also immediately see that in the R-modules case, $\operatorname{coim}(f) = A/\ker(f)$, and so we have the following diagram:



In light of the first isomorphism theorem, we would like to know whether $\operatorname{im}(f) \simeq \operatorname{coim}(f)$. In general, the answer is of course no; we are not even guaranteed the existence of a zero object, let alone images and coimages. In order to fix this

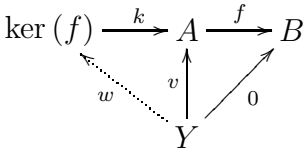
problem, we will need to define an abelian category - one in which the existence of such objects is guaranteed. First, however we shall prove that there is a canonical map from $\operatorname{coim}(f) \to \operatorname{im}(f)$, provided all the required objects exist.

Proposition 4.1.7. *Let $|\mathscr{C}|$ be a category, $A, B \in |\mathscr{C}|$ and $f \in [A, B]$. Assuming all the required objects exist, $k : \ker(f) \to A$ is monomorphism and $c : B \to \operatorname{coker}(f)$ is an epimorphism.*

Proof. Suppose $w_1, w_2 \in [Y, \ker(f)]$ for some $Y \in |\mathscr{C}|$ such that $kw_1 = kw_2$ (we want to show $w_1 = w_2$). That is, we have:

$$Y \underset{w_2}{\overset{w_1}{\rightrightarrows}} \ker(f) \xrightarrow{k} A$$

Let $v = kw_1 = kw_2$. Then $fv = fkw_1 = 0w_1 = 0$. From the definition of kernel, there exists a unique map $w \colon Y \to \ker(f)$ such that the following diagram commutes:

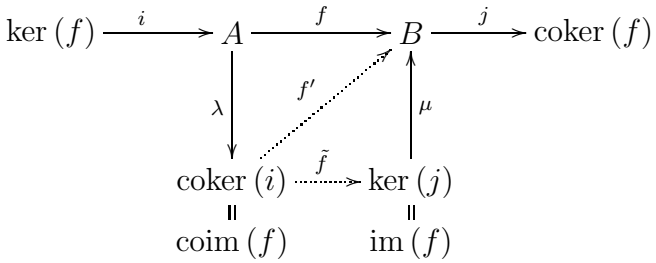


So we have $v = kw$. By the uniqueness of w, we must have $w_1 = w = w_2$. A very similar proof (with arrows reversed) shows c is an epimorphism. □

Note that in the proof, we did not pick specific elements from any object. We only concentrated on the maps between them. We can now prove the existence of a unique (canonical) map $\operatorname{coim}(f) \to \operatorname{im}(f)$.

Proposition 4.1.8. *Let $|\mathscr{C}|$ be a category, $A, B \in |\mathscr{C}|$ and $f \in [A, B]$. Then, assuming all the required objects exist, there exists a unique morphism $\tilde{f} : \operatorname{coim}(f) \to \operatorname{im}(f)$ such that f has a unique decomposition $A \xrightarrow{\lambda} \operatorname{coim}(f) \xrightarrow{\tilde{f}} \operatorname{im}(u) \xrightarrow{\mu} B$.*

Proof. Consider the following diagram,



Since $fi = 0$ there exists a unique morphism $f' : \operatorname{coker}(i) \to B$ (by definition of $\operatorname{coker}(i)$), such that $f = f'\lambda$. Now, $jf'\lambda = jf = 0 = 0\lambda$. By the previous proposition, λ is an epimorphism and so $jf' = 0$. Thus, by definition of $\ker(j)$, there exists a unique map $\tilde{f} : \operatorname{coker}(i) \to \ker(j)$. To show uniqueness, suppose there exists $\tilde{f}_1$ such that $\mu\tilde{f}_1\lambda = \mu\tilde{f}\lambda$. Then, since λ is an epimorphism we get that $\mu\tilde{f}_1 = \mu\tilde{f}$ and since μ is a monomorphism $\tilde{f}_1 = \tilde{f}$. □

We are now almost ready to define an abelian category, however we will need a preliminary definition first.

Definition 4.1.9. *Let $\mathscr{C}$ be a category and $A, B \in |\mathscr{C}|$. The* **product** *of A and B, denoted by $A \times B$ is defined to be the limit of $D : \Sigma \to \mathscr{C}$ with $Ve(\Sigma) = \{A, B\}$ and $Ar(\Sigma) = \varnothing$. The* **sum***, denoted by $A \oplus B$ is defined to be the colimit of this diagram.*

Since these concepts are only needed for the following definition, and play no role in our future discussion, I have no need to elaborate on them.

Definition 4.1.10. *An* **abelian category***, is a category $\mathscr{A}$, with the following properties:*

(a) *For any $L, M, N \in |\mathscr{A}|$, the set $\mathrm{Hom}(L, M)$ is an abelian group and the composition $\mathrm{Hom}(L, M) \times \mathrm{Hom}(M, N) \to \mathrm{Hom}(L, N)$ is $\mathbb{Z}$-linear;*

(b) *$\mathscr{A}$ has a zero object;*

(c) *For any two objects $L, M \in |\mathscr{A}|$, $L \oplus M$ and $L \times M$ exist;*

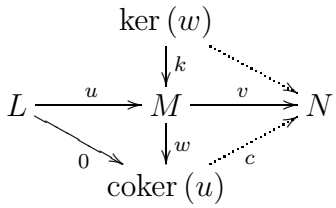
(d) *For any morphism $u \in Mor\mathscr{A}$ there exists $\ker(u)$ and $\mathrm{coker}(u)$;*

(e) *For any morphism $u \in Mor\mathscr{A}$ the unique morphism $\mathrm{coim}(u) \to \mathrm{im}(u)$ is an isomorphism.*

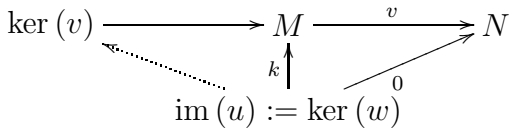
Note that the existence of $\ker(u)$ and $\mathrm{coker}(u)$ for all morphisms guarantees the existence of $\mathrm{im}(u)$ and $\mathrm{coim}(u)$ since they are defined through kernels and cokernel. Also, if we relax the definition, and get rid of (d) and (e) then we get an **additive category**, but we will not be interested in them, since in all later discussions we will most certainly be needing kernels.

Proposition 4.1.11. *Let $\mathscr{A}$ be an abelian category. Consider the following sequence with objects and morphisms from $\mathscr{A}$: $L \xrightarrow{u} M \xrightarrow{v} N$ such that $vu = 0$. There exists a unique (canonical) morphism $\mathrm{im}(u) \to \ker(v)$.*

Proof. Consider first the following commutative diagram:



Note that since $wu = 0$ and $vu = 0$, by definition of cokernel, there exists a unique map $c\colon \mathrm{coker}(u) \to N$. Thus, since $wk = 0$ (by definition of kernel), $cwk = 0$ and so in order for the diagram to commute, the map $\ker(w) \to N$ must be the zero map. Therefore we have:



By definition of kernel, there exists a unique map $\mathrm{im}(u) \to \ker v$.

□

We say that the sequence from the above proposition is **exact** if the canonical morphism $\ker(v) \to \operatorname{im}(u)$ is an isomorphism. When this happens, we usually abuse notation slightly and simply write $\ker(v) = \operatorname{im}(u)$ as objects in $\mathscr{A}$.

The following lemma is crucial in category theory, and very often used.

Lemma 4.1.12 (Snake Lemma). *Let $\mathscr{A}$ be an abelian category. Consider the following commutative diagram, with objects and morphisms from $\mathscr{A}$.*

$$\begin{array}{ccccccc} & & L' & \xrightarrow{i} & L & \xrightarrow{p} & L'' \longrightarrow 0 \\ & & \downarrow{\scriptstyle u'} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle u''} \\ 0 & \longrightarrow & M' & \xrightarrow{i'} & M & \xrightarrow{p'} & M'' \end{array}$$

where all the rows are exact. Then there exists a unique morphism

$$\delta \colon \ker(u'') \to \operatorname{coker}(u)$$

such that the sequence:

$$\ker(u') \to \ker(u) \to \ker(u'') \xrightarrow{\delta} \operatorname{coker}(u') \to \operatorname{coker}(u) \to \operatorname{coker}(u'')$$

is exact.

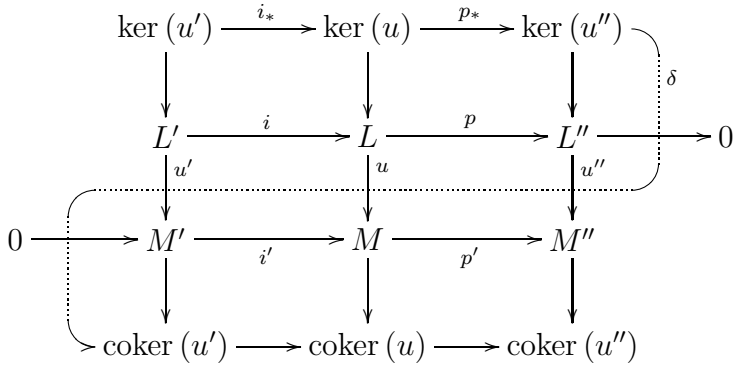
Proof. I will not be giving a complete proof (see page 159 for [Lan02] for this), since it is too long as there are too many things to check (after all we need to check that the sequence is exact!). However, I will comment briefly on what the maps in the sequence are, at least if $\mathscr{A}$ is the category of R-modules.

If $\mathscr{A}$ is the category of R-modules then $\delta : \ker(u'') \to M'/\operatorname{im}(u')$. For $c \in \ker(u'')$ we define $\delta(c) := (i')^{-1}up^{-1}(c) + \operatorname{im}(u')$. Then one checks that δ is in fact well defined with the right image; this is not obvious, as i' and p are not injective, when one takes their inverse a choice needs to be made and so we must make sure that δ is independent of that choice.

Then if we define $i_* := i\,|_{\ker(u')}$ and $p_* := p\,|_{\ker(u)}$ it can easily be verified that

$$\ker(u') \xrightarrow{i_*} \ker(u) \xrightarrow{p_*} \ker(u'')$$

is also exact and similarly for all the other remaining maps. If we combine all the maps together, we see where the lemma gets its name from:



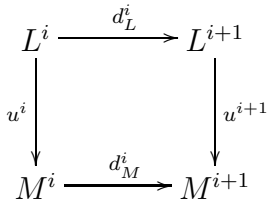
4.2 Cohomology

Now that we have defined the language of category theory, and established some important results, we are ready to introduce cohomology. We will see, using the Snake Lemma, how short exact sequences of complexes give rise to long exact sequences of cohomology. Note that analogous to what we introduce here, there is a homology theory which is identical to what we do here but with all the arrows reversed in a sensible way and the prefix "co" removed from all the definitions. However, as it will turn out, it is cohomology that we will need.

From now on, we let $\mathscr{A}$ denote an abelian category.

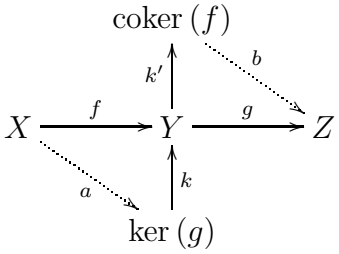
Definition 4.2.1. *A* **complex** *of $\mathscr{A}$, denoted by $L^\bullet$, consists of objects $\{L^i\} \subseteq |\mathscr{A}|$ called* **cochains**, *and morphisms $\{d^i\} \subseteq \operatorname{Mor} \mathscr{A}$ with $d^i : L^i \to L^{i+1}$ called* **differentials**, *such that $d^{i+1} \circ d^i = 0$ for all $i \in \mathbb{Z}$.*

We define a morphism $u : L^\bullet \to M^\bullet$, between two complexes $L^\bullet$ and $M^\bullet$, to be a family of morphisms $u^i : L^i \to M^i$ such that for each i the following diagram commutes:



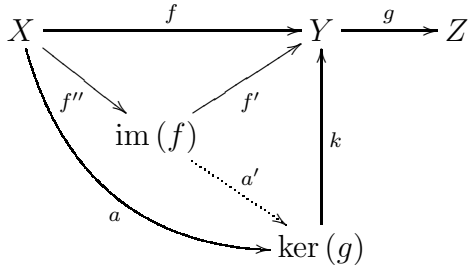
In order to define cohomology in a categorical way, we need the following proposition.

Proposition 4.2.2. *Consider the following commutative diagram with objects and morphisms from $\mathscr{A}$:*



with $gf = 0$. Then there exists unique morphisms b and a as shown. Furthermore, $\operatorname{coker}(a) \simeq \ker(b)$.

Proof. We know that $gf = 0$ and $gk = 0$ and so by definition of kernel the map a exists as shown. Similarly, we see that b exists. I would like to reduce to the case where f is a monomorphism and g is an epimorphism. Recall that by Proposition 4.1.8, f factors through its image as follows:



Note that a' exists as shown since $gf'f'' = gf$ and since f'' is an epimorphism $gf' = 0$ and thus by definition of kernel (of g) a' exists as shown. Note also that $gf'f'' = gf = 0$ and since f'' is an epimorphism, $gf' = 0$. We claim that $\operatorname{coker}(a) \simeq \operatorname{coker}(a')$ up to a unique isomorphism. To see this we show that $\operatorname{coker}(a)$ satisfies the two conditions required to be $\operatorname{coker}(a')$ and since cokernels are unique up to unique isomorphism, the claim will follow. We have the following diagram:

$$\begin{array}{ccccc} X & \xrightarrow{a} & \ker(g) & \xrightarrow{c_a} & \operatorname{coker}(a) \\ {\scriptstyle f''}\downarrow & & \| & & \\ \operatorname{im}(f) & \xrightarrow{a'} & \ker(g) & \xrightarrow{c_{a'}} & \operatorname{coker}(a') \end{array}$$

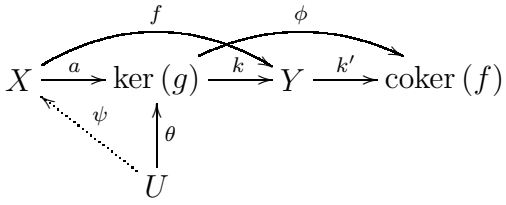
Now we know that $c_a a' f'' = c_a a = 0$ and since f'' is an epimorphism we have $c_a a' = 0$ and so $\operatorname{coker}(a)$ satisfies the first condition required to be $\operatorname{coker}(a')$. Also, suppose that there exists and object N and morphism $n\colon \ker(g) \to N$ such that $na' = 0$. Then $na = na'f'' = 0f'' = 0$ and so $\operatorname{coker}(a) \simeq \operatorname{coker}(a)'$.

Thus, in order to prove $\operatorname{coker}(a) \simeq \ker(b)$, we can replace X with $\operatorname{im}(f)$, a with a' and f with f', which is a monomorphism. Equivalently, this is saying that without loss of generality, we can assume f is a monomorphism. The dual of this result says that without loss of generality, we may assume that g is an epimorphism.

Let $\phi = k'k$ and note that it has the following decomposition:

$$\ker(g) \longrightarrow \operatorname{coim}(\phi) \xrightarrow{\sim} \operatorname{im}(\phi) \longrightarrow \operatorname{coker}(f)$$

Since $\operatorname{coim}(\phi) := \operatorname{coker}(\ker(\phi) \to \ker(g))$ and $\operatorname{im}(\phi) := \ker(\operatorname{coker}(f) \to \operatorname{coker}(\phi))$ we will be done provided we can show that $\operatorname{coker}(a) \simeq \operatorname{coker}(\ker(\phi) \to \ker(g))$ and $\ker(b) \simeq \ker(\operatorname{coker}(f) \to \operatorname{coker}(\phi))$. To show the first part it is sufficient to show that $(X, a) \simeq \ker(\phi)$ and the second part will follow by the dual result. Thus we have:



(I will define U soon). Now, $\phi a = k'ka = k'f = 0$ and so (X, a) satisfies the first condition of being $\ker(\phi)$. Suppose there exists an object U and a morphism $\theta\colon U \to \ker(g)$ such that $\phi\theta = 0$. This implies $k'(k\theta) = 0$. The fact that f is a monomorphism implies that $(X, f) = \ker k'$ and so by definition of kernel, there exists a unique map ψ such that $k\theta = f\psi = ka\psi$. Since k is a monomorphism, $\theta = a\psi$ and so (X, a) satisfies the second condition required to be $\ker(\phi)$, and so we are done. □

Definition 4.2.3. *Given a complex $L^\bullet$ we define:*

$$Z^iL^\bullet := \ker\left(d^i\colon L^i \to L^{i+1}\right)$$
$$B^iL^\bullet := \operatorname{im}\left(d^{i-1}\colon L^{i-1} \to L^i\right)$$
$$H^iL^\bullet := \operatorname{coker}\left(a^{i-1}\right) = \ker\left(b^i\right) \quad \textit{as defined in the above proposition}$$

*$Z^iL^\bullet$ is called the i^{th}-**cocyle**, $B^iL^\bullet$ the i^{th}-**coboundary** and $H^iL^\bullet$ the i^{th}-**cohomology**. Simply write Z^i and B^i if the complex is clear from the context.*

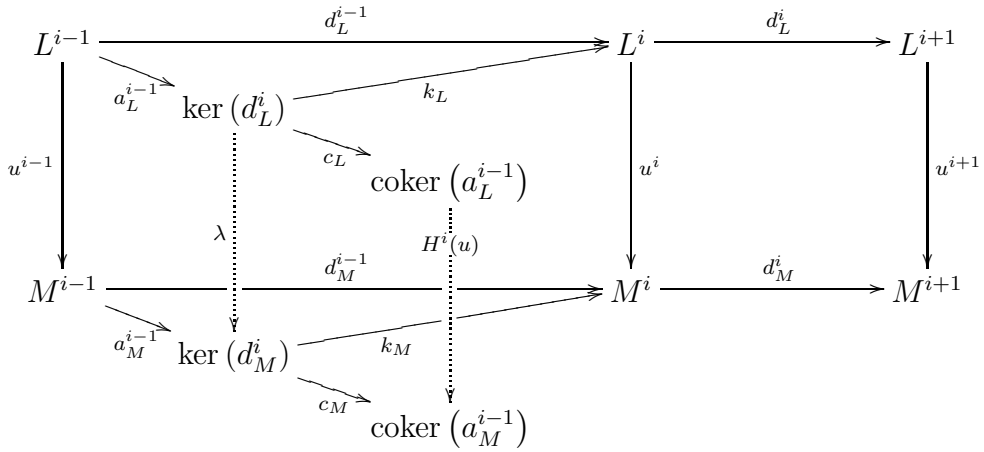
In the case where $\mathscr{A}$ is the is the category of R-modules we have

$$H^iL^\bullet = \ker\left(b^i\right) = \ker\left(L^i/\operatorname{im}\left(d^{i-1}\right) \to L^{i+1}\right) = \ker\left(d^i\right)/\operatorname{im}\left(d^{i-1}\right) = Z^iL^\bullet/B^iL^\bullet$$

We can thus see that the cohomology groups are measuring the obstruction to $L^\bullet$ being exact.

Proposition 4.2.4. *Let $L^\bullet$ and $M^\bullet$ be complexes of $\mathscr{A}$. A morphism $u\colon L^\bullet \to M^\bullet$ induces a (natural) morphism $H^i(u)\colon H^iL^\bullet \to H^iM^\bullet$.*

Proof. Consider the following diagram:



We have to show the existence of unique maps λ and $H^i(u)$ which make the diagrams commute. Recall that the maps a_L^{i-1} and a_M^{i-1} are those defined in Proposition 4.2.2. We know that $d_M^ik_M = 0$ by the definition of kernel. Similarly $d_L^ik_L = 0$ and so $u^{i+1}d_L^ik_L = 0$. By commutivity, this implies that $d_M^iu^ik_L = 0$, and thus by the definition of kernel (of d_M^i) there exists a unique map $\lambda\colon \ker(d_L^i) \to \ker(d_M^i)$ such that the diagram commutes. Now, we know that $c_Ma_M^{i-1} = 0$, by the definition of cokernel, and so $c_Ma_M^{i-1}u^{i-1} = 0$ which by commutivity of the diagram, implies that $c_M\lambda a_L^{i-1} = 0$. Thus, by definition of cokernel (of a_L^{i-1}) there exists a unique map $H^i(u)\colon \operatorname{coker}\left(a_L^{i-1}\right) \to \operatorname{coker}\left(a_M^{i-1}\right)$. Since by definition, $H^iL^\bullet := \operatorname{coker}\left(a_L^{i-1}\right)$ and $H^iM^\bullet := \operatorname{coker}\left(a_M^{i-1}\right)$, the result follows. □

Now that we have seen how, a morphism between two complexes gives rise to a morphism between the corresponding cohomologies, and so we are ready to prove the main theorem of this section.

Let $L^{\bullet\prime}, L^{\bullet}$ and $L^{\bullet\prime\prime}$ be complexes of $\mathscr{A}$. By an exact sequence of complexes

$$0 \longrightarrow L^{\bullet\prime} \xrightarrow{u} L^{\bullet} \xrightarrow{v} L^{\bullet\prime\prime} \longrightarrow 0$$

we mean that for every i we have an exact sequence :

$$0 \longrightarrow L'^{i} \xrightarrow{u^i} L^{i} \xrightarrow{v^i} L''^{i} \longrightarrow 0$$

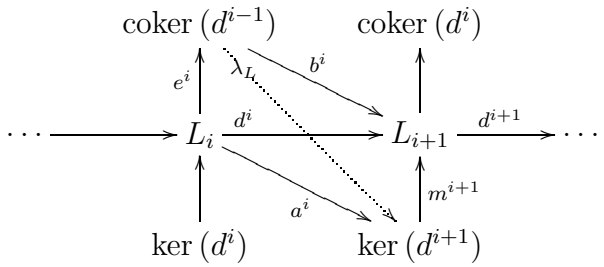
Theorem 4.2.5. *Given an exact sequence of complexes*

$$0 \longrightarrow L^{\bullet\prime} \xrightarrow{u} L^{\bullet} \xrightarrow{v} L^{\bullet\prime\prime} \longrightarrow 0$$

there exists a canonical **long exact sequence** *of cohomology.*

$$\cdots \longrightarrow H^i L^{\bullet\prime} \xrightarrow{H^i(u)} H^i L^{\bullet} \xrightarrow{H^i(v)} H^i L^{\bullet\prime\prime} \xrightarrow{\delta^i} H^{i+1} L^{\bullet\prime} \longrightarrow H^{i+1} L^{\bullet} \longrightarrow \cdots$$

Proof. Note firstly, that given a complex $L^{\bullet}$ we have the following diagram:



We know that $d^{i+1}b^ie^i = d^{i+1}d^i = 0$ and since e^i is an epimorphism, $d^{i+1}b^i = 0$ which by the definition of kernel implies that there exists a map $\lambda_L \colon \text{coker}\,(d^{i-1}) \to \ker\,(d^{i+1})$. We claim that $\ker\,(\lambda_L) \simeq \ker\,(b^i)$. We prove this by checking that the $\ker\,(b^i)$ satisfies the required definion to be $\ker\,(\lambda_L)$ and since kernels are unique up to undue isomorphism, the claim will follow. We have the following commutative diagram:

$$\begin{array}{ccccc} \ker\,(\lambda_L) & \xrightarrow{f} & \text{coker}\,(d^{i-1}) & \xrightarrow{\lambda_L} & \ker\,(d^{i+1}) \\ & & \| 1 & & \downarrow m^{i+1} \\ \ker\,(b^i) & \xrightarrow{g} & \text{coker}\,(d^{i-1}) & \xrightarrow{b^i} & L^{i+1} \end{array}$$

We know that $m^{i+1}\lambda_L 1 g = b^i g = 0$ and since m^{i+1} is a monomorphism, $\lambda_L g = 0$. Thus $\ker\,(b^i)$ satisfies the first condition of being $\ker\,(\lambda_L)$. Now suppose there exists another object N and a map n: $N \to \text{coker}\,(d^{i-1})$ such that $\lambda_L n = 0$. Then $b^i n = m^{i+1}\lambda_L n = 0$ and so by the definition of kernel (of b^i) there exists a unique map $N \to \ker\,(b^i)$ and so $\ker\,(b^i)$ satisfies the second condition required to be $\ker\,(\lambda_L)$. Thus the claim is proven. Similarly, reversing all arrows $\text{coker}\,(\lambda_L) = \text{coker}\,(a^i)$.

By Proposition 4.2.4 the exact sequence of complexes gives rise in a natural way to:

$$\begin{array}{ccccccc} & & \operatorname{coker}\left(d_{L'}^{i-1}\right) & \longrightarrow & \operatorname{coker}\left(d_{L}^{i-1}\right) & \longrightarrow & \operatorname{coker}\left(d_{L''}^{i-1}\right) \longrightarrow 0 \\ & & \downarrow{\scriptstyle \lambda_{L'}} & & \downarrow{\scriptstyle \lambda_{L}} & & \downarrow{\scriptstyle \lambda_{L''}} \\ 0 \longrightarrow & \ker\left(d_{L'}^{i+1}\right) & \longrightarrow & \ker\left(d_{L}^{i+1}\right) & \longrightarrow & \ker\left(d_{L''}^{i+1}\right) & \end{array}$$

Now we apply the Snake Lemma and by using the fact that $\ker(\lambda_L) = \ker(b_L^i) = H^i L^\bullet$ and $\operatorname{coker}(\lambda_L) = \operatorname{coker}(a_L^i) = H^{i+1} L^\bullet$ the result follows.

□

4.3 Galois Cohomology

This section will serve both as an example of the theory developed in the previous section and also produce an important theorem, namely that the correspondence that we established between relative Brauer groups and factor sets is in fact an abelian group homomorphism. In order to apply the ideas of the previous section, we will need to specify the category of interest to us, and then we will need to establish a complex of this category, which will require us to define the differential maps, so that finally we will be able to calculate the cohomologies of the complex. What we will discover is that the second cohomology of the complex we establish, will be isomorphic to the $\mathrm{Br}(K/k)$ which will be the crucial step in the correspondence we are aiming to establish.
We fix a finite group G and a G-module M. We define, for all $n \geq 1$

$$C^n(G, M) := \{f \mid f \colon G^n \to M\}$$

We also define $C^0(G, M) := M$. We turn $C^n(G, M)$ into an abelian group by declaring that $(f + h)(g_1, \ldots, g_n) := f(g_1, \ldots, g_n) + h(g_1, \ldots, g_n)$ for all $g_i \in G$ and $f, h \in C^n(G, M)$. We aim to form a complex where the $C^n(G, M)$ will be the cochains. In order to do so, we need to define the differentials d^n, that will be group homomorphisms with the propery that $d^{n+1} \circ d^n = 0$. We do so, by defining $d^n \colon C^n(G, M) \to C^{n+1}(G, M)$ to be such that:

$$\begin{aligned} (d^n f)(g_1, \ldots, g_{n+1}) \;:=\; & g_1 f(g_2, \ldots, g_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, \ldots, g_{n+1}) \\ & + (-1)^{n+1} f(g_1, \ldots, g_n) \end{aligned}$$

for all $n \geq 1$ and

$$(d^0 f)(g_1) = g_1 f - f$$

recall that $f \in M$ in the case where $n = 0$, so this makes sense.

Example 4.3.1. When $n = 1$ we have:

$$(d^1 f)(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1)$$

When $n = 2$ we have:

$$(d^2 f)(g_1, g_2, g_3) = g_1 f(g_2 g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2)$$

Proposition 4.3.2. *Given the setup as above, $d^n : C^n(G, M) \to C^{n+1}(G, M)$ is a group homomorphism for all $n \geq 0$. Further, $d^{n+1} \circ d^n = 0$.*

Proof. The fact that d^n is a group homomorphism is obvious since we defined the addition of functions to be pointwise. The fact that $d^{n+1} \circ d^n = 0$ is too tedious to prove here, but does no require anything other then careful expansion. □

We thus have the following complex $C^\bullet$:

$$0 \longrightarrow C^0(G, M) \xrightarrow{d^0} C^1(G, M) \xrightarrow{d^1} C^2(G, M) \xrightarrow{d^2} \dots$$

We let $H^n(G, M)$ denote $H^n C^\bullet$; recall that since we are in an environment where a quotient of two objects makes sense, this is just $Z^n/B^n = \ker(d^n)/\mathrm{im}(d^{n-1})$.

Example 4.3.3. Let G be a group and M a G-module with a trivial action. That is $gm = m$ for all $g \in G,\ m \in M$. Let us compute $H^1(G, M) = \ker(d^1)/\mathrm{im}(d^0)$. First of all, if $f \in \ker(d^1)$ then

$$\begin{aligned} 0 = (d^1 f)(g_1, g_2) &= g_1 f(g_2) - f(g_1 g_2) + f(g_1) \\ &= f(g_2) - f(g_1 g_2) + f(g_1) \quad \text{since the action of } G \text{ is trivial} \end{aligned}$$

and hence we obtain that $f(g_1 g_2) = f(g_1) + f(g_2)$, which is the condition for f to be a group homomorphism. Also note that for $h \in C^0(G, M) := M$

$$(d^0 h)(g_1) = g_1 h - g_1 = g_1 - g_1 = 0$$

and so $\mathrm{im}(d^0)$ consist of only the zero function. Thus

$$H^1(G, M) = \mathrm{Hom}(G, M)$$

The following theorem will play a very important role later.

Theorem 4.3.4. *Let G be a finite group, and M a G-module. Then $|G| H^n(G, M) = 0$ for all $n \geq 1$.*

Proof. Let $f \in Z^n$. Then

$$\begin{aligned} 0 = (d^n f)(g_1, \dots, g_{n+1}) = g_1 f(g_2, \dots, g_{n+1}) &+ \sum_{i=1}^{n} f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \dots, g_n) \end{aligned}$$

and so:

$$(-1)^n f(g_1, \dots, g_n) = g_1 f(g_2, \dots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) \quad (4.1)$$

Also note that for any $h \in C^{n-1}(G, M)$ we have:

$$(d^{n-1}h)(g_1, \ldots, g_n) = g_1 h(g_2, \ldots, g_n) + \sum_{i=1}^{n-1} (-1)^i h(g_1, \ldots, g_i g_{i+1}, \ldots, g_n) + (-1)^n h(g_1, \ldots, g_{n-1}).$$

Now we define a specific h as follows:

$$h(g_2, \ldots, g_n) := \sum_{g_{n+1} \in G} f(g_2, \ldots, g_{n+1)}$$

From now on we introduce notation and let $\hat{g}_i := g_i g_{i+1}$. Now summing over all $g_{n+1} \in G$ in Equation 4.1 we get:

$$\begin{aligned}(-1)^n |G| f(g_1, \ldots, g_n) &= \sum_{g_{n+1} \in G} \Big(g_1 f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, \hat{g}_i, \ldots, g_{n+1}) \Big) \\ &= \sum_{g_{n+1}} \Big(g_1 f(g_2, \ldots, g_{n+1}) + \sum_{i=0}^{n-1} (-1)^i f(g_1, \ldots, \hat{g}_i, \ldots, g_{n+1}) \\ &\qquad + (-1)^n f(g_1, \ldots, g_n g_{n+1}) \Big)\end{aligned}$$

Note that

$$\sum_{g_{n+1}} f(g_1, \ldots, \hat{g}_i, \ldots, g_{n+1}) = h(g_1, \ldots, \hat{g}_i, \ldots, g_n)$$

and that

$$\sum_{g_{n+1}} f(g_1, \ldots, g_{n-1}, g_n g_{n+1}) = \sum_{g_{n+1}} f(g_1, \ldots, g_{n-1}, g_{n+1}) = h(g_1, \ldots, g_{n-1})$$

Therefore we have:

$$\begin{aligned}(-1)^n |G| f(g_1, \ldots, g_n) &= g_1 h(g_2, \ldots, g_n) + \sum_{i=0}^{n-1} (-1)^i h(g_1, \ldots, \hat{g}_i, \ldots, g_n) \\ &\qquad + (-1)^n h(g_1, \ldots, g_{n-1}) \\ &= (d^{n-1}h)(g_1, \ldots, g_n) \in B^n\end{aligned}$$

Thus $|G| Z^n(G, M) \subseteq B^n(G, M)$ and so $|G| H^n(G, M) = 0$. □

Given a sequence of G-modules, we would like to find a natural way of obtaining a sequence of complexes, so that we can then calculate its cohomology. The following proposition shows how one can do this:

Proposition 4.3.5. *A short exact sequence of G-modules*

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

gives rise, in a natural way, to the following exact sequence:

$$0 \longrightarrow C^\bullet(G, M') \longrightarrow C^\bullet(G, M) \longrightarrow C^\bullet(G, M'') \longrightarrow 0$$

Proof. We define $u' : C^\bullet(G, M') \to C^\bullet(G, M)$ such that for each n we get a map, $u'^n : C^n(G, M') \to C^n(G, M)$ with $u'^n(f) = u \circ f$. First we need to make sure that this is indeed a morphism of complexes. That is we need to check that for every n the following diagram commutes:

$$\begin{array}{ccc} C^n(G, M') & \xrightarrow{u'^n} & C^n(G, M) \\ \Big\downarrow{\scriptstyle d^n_{M'}} & & \Big\downarrow{\scriptstyle d^n_M} \\ C^{n+1}(G, M') & \xrightarrow{u'^{n+1}} & C^{n+1}(G, M) \end{array}$$

However, the commutivity of the diagram is obvious, and comes straight from the fact that u is a G-module morphism. Similarly we define the map $v' : C^\bullet(G, M) \to C^\bullet(G, M'')$ and we get the desired sequence of complexes whose exactness is obvious from the exactness of the original sequence of G-modules. □

The above proposition, together with Theorem 4.2.5 imply that any short exact sequence of G-modules, gives rise, in a natural way, to a long exact sequence of cohomology groups. This fact will prove vital for us in the future.

Corollary 4.3.6. *Let G be a finite group with an action defined on $\mathbb{Q}$, giving $\mathbb{Q}$ a G-module structure. Then $H^n(G, \mathbb{Q}) = 0$ for all $n \geq 1$.*

Proof. Let $m = |G|$. Then, clearly multiplication by m defines an isomorphism, $m : \mathbb{Q} \to \mathbb{Q}$ which by Proposition 4.3.5 (and the comment after it) induces an isomorphism $H(m') : H^n(G, \mathbb{Q}) \to H^n(G, \mathbb{Q})$ which is also multiplication by m. Since, this is an isomorphism of groups and by Theorem 4.3.4 $mH^n(G, \mathbb{Q}) = 0$ we must have $H^n(G, \mathbb{Q}) = 0$ for all $n \geq 1$. □

We now restrict our attention to a specific G-module. Let k be a field and K/k a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$. We let $M = K^*$. We will show that $H^2(G, K^*) \simeq \mathrm{Br}(K/k)$. At this stage, the reader is advised to review the definitions, theorems and notation introduced in Section 3.4.

Remark 4.3.7. We can identify the factor set $\{a_{\sigma,\tau}\}$ with a 2-cochain, i.e a function $a : G \times G \to K^* \ : \ a(\sigma, \tau) = a_{\sigma,\tau}$ and the set $\{f_\sigma\}$ with a 1-cochain $f : G \to K^* \ : \ f(\sigma) = f_\sigma$.

Since $H^2(G, K^*) \simeq Z^2/B^2$, we begin by calculating Z^2. We also switch to multiplicative notation. Note first that $a \in Z^2$ if and only if it is in the kernel of d^2. That is:

$$\begin{aligned} 1 &= (d^2 a)(\rho, \sigma, \tau) \\ &= \rho\left(a(\sigma, \tau)\right) a(\rho\sigma, \tau)^{-1} a(\rho, \sigma\tau) a(\rho, \sigma)^{-1} \end{aligned}$$

for all $\rho, \sigma, \tau \in G$ (using Example 4.3.1 written multiplicatively). This is equivalent to

$$\rho\left(a(\sigma, \tau)\right) a(\rho, \sigma\tau) = a(\rho, \sigma) a(\rho\sigma, \tau)$$

Note that by the above remark this is precisely the relationship from Theorem 3.4.5. Thus we have shown that that Z^2 consists of factor sets relative to K.
Now B^2 consists of precisely those functions which lie in the image of d^1. Note that

$$(d^1 f)(\sigma, \tau) = \sigma\left(f(\tau)\right) f(\sigma\tau)^{-1} f(\sigma)$$

from Example 4.3.1 written multiplicatively. Thus elements of $H^2(G, K^*)$ consist of factor sets, modulo the equivalence relationship, where $a \sim b$ in Z^2 if there exists a 1-cochain f such that:

$$\begin{aligned} b(\sigma, \tau) &= (d^1 f)(\sigma, \tau) \cdot a(\sigma, \tau) \\ &= \sigma\left(f(\tau)\right) f(\sigma\tau)^{-1} f(\sigma) \cdot a(\sigma, \tau) \end{aligned}$$

and in light of Remark 4.3.7 we can rewrite this as:

$$b_{\sigma,\tau} = \frac{f_\sigma \sigma(f_\tau)}{f_{\sigma\tau}} a_{\sigma,\tau}$$

This is precisely the condition 3.4 from page 33. Thus by Theorem 3.4.8 there is a one-to-one relationship between $\mathrm{Br}(K/k)$ and $H^2(G, K^*)$. In fact, as the next theorem will show, they are in fact isomorphic as groups.

Theorem 4.3.8. *Let K/k be a finite Galois field extension, with Galois group G. Then*

$$H^2(G, K^*) \simeq \mathrm{Br}(K/k)$$

Proof. Define

$$\begin{aligned} \psi : H^2(G, K^*) &\longrightarrow \mathrm{Br}(K/k) \\ a &\longmapsto [(K, G, a)] \end{aligned}$$

As discussed earlier, we know that ψ is one-to-one and onto. What remains to show is that it is a group homomorphism. In other words we need to show that given two factor sets $a = \{a_{\sigma,\tau}\}$ and $b = \{b_{\sigma,\tau}\}$ then

$$[(K, G, a)][(K, G, b)] = [(K, G, c)]$$

where $c = ab = \{a_{\sigma,\tau} b_{\sigma,\tau}\}$. Note that c is indeed a factor set, for it clearly satisfies the condition of Theorem 3.4.5.

From Definition 3.4.3 we can assume both $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ are normalised since equivalent factor sets give rise to equivalent algebras. We let $A = (K, G, a)$, $B = (K, G, b)$ and $C = (K, G, c)$ and we aim to show $A \otimes_k B \sim C$.

Let $M = A^\circ \otimes_K B$ (Note that this makes sense since since A and B contain K). Recall that $a \cdot a'$ in A° equals $a'a$ in A. Thus for all $x \in K,\ a \in A,\ b \in B$:

$$a \otimes xb = a \cdot x \otimes b = xa \otimes b \tag{4.2}$$

We turn M into a right $A \otimes_k B$ module via right multiplication:

$$(a' \otimes b')(a \otimes b) = (a'a \otimes b'b) \in M \quad \text{for all } a, a' \in A,\ b, b' \in B$$

Now we also turn M into a left C-module as follows: let $\{u_\sigma\}, \{v_\sigma\}, \{w_\sigma\}$ be bases over K of A, B and C respectively (the ones constructed in Theorem 3.4.5). We define

$$(xw_\sigma)(a \otimes b) = xu_\sigma a \otimes v_\sigma b \quad \text{for all } x \in K, \sigma \in G, a \in A, b \in B$$

We need to check that this operation indeed makes M into a left C-module. We will check associativity here; the other axioms are similar. Let $y, x \in K$ $a \in A$, $b \in B$, and $\sigma, \tau \in G$. Then:

$$\begin{aligned}(yw_\tau)[(xw_\sigma)(a \otimes b)] &= (yw_\tau)(xu_\sigma a \otimes v_\sigma b) \\ &= yu_\tau xu_\sigma a \otimes v_\tau v_\sigma b \\ &= y\tau(x)a_{\tau,\sigma}u_{\tau\sigma}a \otimes b_{\tau,\sigma}v_{\tau\sigma}b \\ &= y\tau(x)a_{\tau,\sigma}b_{\tau,\sigma}u_{\tau\sigma}a \otimes v_{\tau\sigma}b \quad \text{by 4.2} \\ &= y\tau(x)c_{\tau,\sigma}u_{\tau\sigma}a \otimes v_{\tau\sigma}b\end{aligned}$$

Also

$$\begin{aligned}[(yw_\tau)(xw_\sigma)](a \otimes b) &= (y\tau(x)c_{\tau,\sigma}w_{\tau\sigma})(a \otimes b) \\ &= y\tau(x)c_{\tau,\sigma}u_{\tau\sigma}a \otimes v_{\tau\sigma}b\end{aligned}$$

and so we have shown associativity. Note that the fact that $M = A^\circ \otimes_K B$ and not $A \otimes_K B$ played a crucial role in the proof, for we needed Equation 4.2. The two actions on M also respect each other since (sticking with the previous notation):

$$\begin{aligned}xw_\sigma[(a' \otimes b')(a \otimes b)] &= xw_\sigma(aa' \otimes b'b) \\ &= xu_\sigma a'a \otimes v_\sigma b'b \\ &= (xu_\sigma a' \otimes v_\sigma b')(a \otimes b) \\ &= [xw_\sigma(a' \otimes b')](a \otimes b)\end{aligned}$$

Thus we have given M a $C - A \otimes_k B$-bimodule structure. This enables us to define:

$$\begin{aligned}\phi : (A \otimes_k B)^\circ &\longrightarrow \mathrm{End}_C(M) \\ x &\longmapsto f_x\end{aligned}$$

where $f(x) = mx$ for all $m \in M$, $x \in A \otimes_k B$. Note that ϕ is a homomorphism since M is a $C - (A \otimes_k B)-$bimodule, and the need to make the domain of ϕ $(A \otimes_k B)^\circ$ and not $(A \otimes_k B)$ arises for the same reason as in the proof of Proposition 3.1.5. Since $A \otimes_k B$ is simple, so is $(A \otimes_k B)^\circ$ an so ϕ is injective. Thus, to show ϕ is an isomorphism it suffices to show that the domain and range have the same dimension over k. Let $n = [K : k] = [A : K] = [B : K] = [C : K]$, all the equalities hold since K is a maximal subfield of A, B and C. Thus $[M : K] = [A : K][B : K] = n^2$ and so $[M : k] = [M : K][K : k] = n^3 = n[C : k]$. By Remark 3.1.3, since M has a unique module (up to isomorphism), we must have $M \simeq C^n$. Therefore:

$$\mathrm{End}_C M \simeq \mathrm{End}_C C^n \simeq \mathcal{M}_n(\mathrm{End}_C C) \simeq \mathcal{M}_n C^\circ \simeq C^\circ \otimes_k \mathcal{M}_n(k)$$

and so

$$\dim_k (\mathrm{End}_C M) = n^2 \dim_k C^\circ = n^4 = \dim_k (A \otimes_k B)$$

Thus ϕ is an isomorphism, and so $(A \otimes_k B)^\circ \simeq C^\circ \otimes_k \mathcal{M}_n(k)$ and so, $A \otimes_k B \sim C$. This proves the theorem. $\square$

Combining this theorem, together with Corollary 3.3.14 we get:

$$\mathrm{Br}(k) \simeq \bigcup_K \mathrm{Br}(K/k) \simeq \bigcup_K H^2(\mathrm{Gal}(K/k), K^*)$$

where the unions are over all finite Galois extensions of k. In fact, we could have taken the above to be the definition of the Brauer group and derived all the other properties from this.

The above result suggests that in order to study $\mathrm{Br}(\mathbb{Q}_p)$ we should revert our attention to $\mathrm{Br}(K/\mathbb{Q}_p)$ for a finite, Galois extension $K/\mathbb{Q}_p$. Further, instead of calculating $\mathrm{Br}(K/\mathbb{Q}_p)$ directly, the result suggests we should calculate $H^2(\mathrm{Gal}(K/\mathbb{Q}_p), K^*)$. In order to do so, we need to study finite extensions of $\mathbb{Q}_p$. We move on to do just this.

Chapter 5

Generalising the Product Formula

The aim of this chapter is bring together all the ideas I have developed so far and to generalise the product formula.

5.1 Finite Extensions of $\mathbb{Q}_p$

As mentioned earlier, we begin by studying finite extension of $\mathbb{Q}_p$, for a prime p. The case of the "infinite prime" i.e. the case of $\mathbb{Q}_\infty$ is well known; the only finite extension of $\mathbb{Q}_\infty := \mathbb{R}$ is $\mathbb{C}$.

Definition 5.1.1. *Let $K/\mathbb{Q}_p$ be a finite extension. An element $\alpha \in K$ is* **integral** *over $\mathbb{Z}_p$ if it satisfies a monic polynomial with coefficients in $\mathbb{Z}_p$. The set of elements in K that are integral over $\mathbb{Z}_p$ is called the* **integral closure** *of K over $\mathbb{Z}_p$ and is denoted by $\mathcal{O}_K$.*

Proposition 5.1.2. *If K is a finite extension of $\mathbb{Q}_p$ then $\mathcal{O}_K$ discrete valuation ring (a principal ideal domain with a unique, non-zero, prime ideal). Further, $\mathcal{O}_K$ is finitely generated as a module over $\mathbb{Z}_p$.*

Proof. See [Ser79] page 28 for a proof of this. □

Note that a discrete valuation ring is clearly a local ring and so $\mathcal{O}_K$ has a unique maximal ideal.

Example 5.1.3. Take a trivial extension, that is we let $K = \mathbb{Q}_p$ then, $\mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$ and it has a unique maximal ideal $p\mathbb{Z}_p$.

Since the quotient of a ring by a maximal ideal is a field, we have the following definition:

Definition 5.1.4. *Let $K/\mathbb{Q}_p$ be a finite field extension and $\mathfrak{m}_K \trianglelefteq \mathcal{O}_K$ be the unique maximal ideal of $\mathcal{O}_K$. We define the* **residue field** *of K, denoted by $\bar{K}$ to be $\mathcal{O}_K/\mathfrak{m}_K$.*

Example 5.1.5. If we proceed with the previous example we see that the residue field of $\mathbb{Q}_p$ is $\overline{\mathbb{Q}}_p = \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$. In fact, $\bar{K}$ is always a finite field if K is a finite extension of $\mathbb{Q}_p$ since $\mathcal{O}_K$ is a finitely generated over $\mathbb{Z}_p$ which implies $\mathcal{O}_K/\mathfrak{m}_K$ is finitely generated over $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$. The following diagram can help visualise what is going on:

$$\begin{array}{ccccccc} & & \mathbb{Q}_p & \subseteq & K & & \\ & & \cup\mathrm{I} & & \cup\mathrm{I} & & \\ p\mathbb{Z}_p & \lhd & \mathbb{Z}_p & \subseteq & \mathcal{O}_K & \rhd & \mathfrak{m}_K \end{array}$$

Recall the close relationship between $\mathrm{Br}(\mathbb{Q}_p)$ and $H^2(\mathrm{Gal}(K/\mathbb{Q}_p), K^*)$. From this we can see that $\mathrm{Gal}(K/\mathbb{Q}_p)$ plays an important role in understanding $\mathrm{Br}(\mathbb{Q}_p)$. As we shall see, $\mathrm{Gal}(K/\mathbb{Q}_p)$ is especially nice for a certain type of extension.

Consider the same setup as in Definition 5.1.4. Since $\mathcal{O}_K$ is a Discrete valuation ring, we must have that $(p\mathbb{Z}_p)\mathcal{O}_K = \mathfrak{m}_K^e$ for some integer e. We say $K/\mathbb{Q}_p$ is an **unramified** extension if $e = 1$.

Unramified extension have many nice properties. In order to establish one crucial such property we need the following well-known lemma.

Lemma 5.1.6 (Nakayama's Lemma). *Let R be a local Noetherian ring, with maximal ideal $\mathfrak{m}$ and I a proper ideal of R. Let M be a finitely generated R-module, and define:*

$$IM := \left\{ \sum r_i m_i \mid r_i \in I,\ m_i \in M \right\}.$$

(i) *If $IM = M$, then $M = 0$.*
(ii) *If $m_1, \ldots, m_n \in M$ have images in M/IM that generate it as an R-module, then $m_1, \ldots, m_n$ generate M as an R-module.*

Proof. (i) Suppose $M \neq 0$. Choose a set of generators $\{m_1, \ldots, m_k\}$ of M having the fewest elements. Since $IM = M$, we know that

$$m_k = r_1 m_1 + \cdots + r_k m_k \quad \text{for some } r_i \in I.$$

Then

$$(1 - r_k)m_k = r_1 m_1 + \cdots + r_{k-1} m_{k-1}$$

However, $r_k \in I \subseteq \mathfrak{m}$ and so $1 - r_k \notin \mathfrak{m}$, and hence, by the maximality of $\mathfrak{m}$, must be a unit. Thus $\{m_1, \ldots, m_{k-1}\}$ generates M. This is a contradiction and hence $M = 0$.

(ii) Let $L := (\sum_{i=1}^m Rm_i)$ and $N = M/L$. Now $IN = I(M/L) = (IM + L)/L$ and so $N/IN = (M/L)/[(IM + L)/L] = M/\left(IM + (\sum_i Rm_i)\right) = M/M = 0$ and so $IN = N$. Using part (i) we see that $N = 0$ and hence $M = \sum_i Rm_i$.

□

Note that if we put $I = \mathfrak{m}$ in the above lemma, then saying the images of m_i in $M/\mathfrak{m}M$ generate it as an R-module is equivalent to saying the images of m_i generate $M/\mathfrak{m}M$ as a $R/\mathfrak{m}$ vector space since the action of $R/\mathfrak{m}$ on $M/\mathfrak{m}M$ is defined to be:

$$(r + \mathfrak{m})(m_i + \mathfrak{m}M) := rm_i + \mathfrak{m}M.$$

Proposition 5.1.7. *Let K be a finite unramified extension of $\mathbb{Q}_p$, for some prime p. Then*

$$[K : \mathbb{Q}_p] = \left[\bar{K} : \mathbb{F}_p\right]$$

Proof. It may help to turn to Example 5.1.5 to help visualise the situation. Let n the minimum number of generators of $\mathcal{O}_K$ as a $\mathbb{Z}_p$ module. By Nakayama's Lemma

$$\begin{aligned} n &= \dim_{\mathbb{Z}_p/p\mathbb{Z}_p} \frac{\mathcal{O}_K}{(p\mathbb{Z}_p)\mathcal{O}_K} \\ &= \dim_{\mathbb{F}_p} \frac{\mathcal{O}_K}{\mathfrak{m}_K} \quad \text{since } K \text{ is unramified} \\ &:= \left[\bar{K} : \mathbb{F}_p\right] \end{aligned}$$

Also since $\mathcal{O}_K$ is a PID, and torsion free (since it is a subset of a field) and so we must have

$$\mathcal{O}_K \simeq \mathbb{Z}_p^n$$

as $\mathbb{Z}_p$ modules. Tensoring with $\mathbb{Q}_p$ we get

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{O}_K \simeq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p^n \simeq \mathbb{Q}_p^n$$

I claim that $K \simeq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{O}_K$. To see this, define the map

$$\begin{aligned} \psi \colon \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{O}_K &\longrightarrow K \\ a \otimes b &\longmapsto ab \end{aligned}$$

First we check ψ is injective. Let $x = (\sum_{i=1}^m a_i \otimes b_i)$ and suppose $\psi(x) = 0$. Let $n = \min\{v_p(a_i)\}$ and so $x = \sum p^{-n}\hat{a}_i \otimes b_i = p^{-n} \otimes \sum \hat{a}_i b_i$ with $\hat{a}_i \in \mathbb{Z}_p$. Thus $0 = \psi(x) = p^{-n} \sum \hat{a}_i b_i$ and hence $\sum \hat{a}_i b_i = 0$ and so $x = 0$.
Now check ψ is surjective. Let $\alpha \in K$. Since $K/\mathbb{Q}_p$ is a finite extension, α has a minimal polynomial and hence, there exists $a_i \in \mathbb{Q}_p$ such that $0 = \alpha^n + a_1\alpha^{n-1} + \cdots + a_n$. Multiplying by p^{nm} for some m we see that

$$0 = (p^m\alpha)^n + a_1 p^m (p^m\alpha)^{n-1} + a_2 p^{2m} (p^m\alpha)^{n-2} \cdots + a_{n-1} p^{(n-1)m} (p^m\alpha)^1 + a_n p^{nm}$$

For a large enough m, $a_i p^{mi} \in \mathbb{Z}_p \subseteq$ and so $p^m\alpha \in \mathcal{O}_K$ since it satisfies a monic polynomial with coefficients in $\mathbb{Z}_p$. Thus $\alpha = p^{-m}x$ with $x \in \mathcal{O}_K$ and hence lies in the images of ψ. Thus ψ is an isomorphism and so $K \simeq \mathbb{Q}_p^n$. Hence, $[K : \mathbb{Q}_p] = n$ and we are done. □

Note that the above result need not be true if K in not unramified. Of course we are interested in $\mathrm{Gal}(K/\mathbb{Q}_p)$ so we would hope we can strengthen the above result, to give us information about the Galois groups. The following proposition does just that.

Proposition 5.1.8. *With the same setup as in the previous proposition:*

$$\mathrm{Gal}(K/\mathbb{Q}_p) \simeq \mathrm{Gal}(\bar{K}/\mathbb{F}_p)$$

Proof. Since $\mathrm{Gal}(K/\mathbb{Q}_p)$ fixes $\mathcal{O}_K$ we get a map

$$\begin{aligned} \mathrm{Gal}(K/\mathbb{Q}_p) &\longrightarrow \mathrm{Aut}(\bar{K}/\mathbb{F}_p) \\ \sigma &\longmapsto \sigma' \end{aligned}$$

such that $\sigma'(x) = \sigma(x)/\mathfrak{m}_K$ for $x \in \mathcal{O}_K$. Write $\bar{K} = \mathbb{F}_p(a)$, (where a is, for example, the generator of $\bar{K}^*$) and let $g(X) \in \mathbb{Z}_p[x]$ be the monic polynomial such that the polynomial $\bar{g}(X) \in \mathbb{F}_p[X]$, attained by reducing the coefficients of $g(X)$ modulo $p\mathbb{Z}_p$, is the minimum polynomial of a. Let $\alpha \in \mathcal{O}_K$ be the unique root of $g(X)$ such that $\bar{\alpha} := \alpha \pmod{\mathfrak{m}_K} = a$. Note that $\bar{K}/\mathbb{F}_p$ is Galois and let $f := [\bar{K} : \mathbb{F}_p] = [K : \mathbb{Q}_p] = \deg g(X) = |\mathrm{Gal}(K/\mathbb{Q}_p)| = |\mathrm{Gal}(\bar{K}/\mathbb{F}_p)|$ and $\alpha_1, \ldots, \alpha_f$ be the roots of $g(X)$. Then

$$\{\alpha_1, \ldots, \alpha_f\} = \{\sigma\alpha \mid \sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)\}.$$

Since $\bar{g}(X)$ is separable, the α_i are distinct modulo $\mathfrak{m}_K$ and this shows that every element $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$ gives a distinct element $\sigma' \in \mathrm{Gal}(\bar{K}/\mathbb{F}_p)$ and hence $\mathrm{Gal}(K/\mathbb{Q}_p) \to \mathrm{Gal}(\bar{K}/\mathbb{F}_p)$ is an isomorphism. □

Thus if K is a finite unramified extension of $\mathbb{Q}_p$ the above proposition, together with Example 5.1.5 and Galois theory imply that $\mathrm{Gal}(K/\mathbb{Q}_p)$ is a cyclic group generate by the Frobenius element $\mathrm{Frob}_{K/\mathbb{Q}_p}$. The crucial result is that considering unramified extensions is sufficient for us. More formally, we have the following theorem which strengthens Corollary 3.3.14.

Theorem 5.1.9.

$$\mathrm{Br}(\mathbb{Q}_p) \simeq \bigcup_K \mathrm{Br}(K/\mathbb{Q}_p)$$

where K ranges through all finite, Galois, unramified extensions of $\mathbb{Q}_p$.

Proof. See [Ser79] page 181. □

The theorem says that every central simple $\mathbb{Q}_p$-algebra is split by some finite, Galois, unramified extension of $\mathbb{Q}_p$.

Finally, given a finite (not even necessarily unramified) extension $K/\mathbb{Q}_p$ we would like to define a valuation on it, analogously to our treatment of $\mathbb{Q}_p$. We do this as follows: let U_K denote the group of units in $\mathcal{O}_K$ and π be the element which generate $\mathfrak{m}_K$. Then it can be shown (in almost identical way to Proposition 1.1.5) that every element $x \in K^*$ can be written uniquely in the form $u\pi^n$ with $u \in U_K$. We define $v_K(x) = n$.

5.2 The Invariant Map

As we have seen, in order to calculate the Brauer group of $\mathbb{Q}_p$ what we really need to study is $\mathrm{Br}(K/\mathbb{Q}_p)$ for an unramified extension $K/\mathbb{Q}_p$. In order to study, that, we are led down the path of Galois cohomology.

Let $K/\mathbb{Q}_p$ be a finite, unramified extension with Galois group G. We get the following exact sequence of G-modules

$$0 \longrightarrow U_K \longrightarrow K^* \xrightarrow{v_K(\cdot)} \mathbb{Z} \longrightarrow 0$$

Now we applying the cohomology theory we developed, and more specifically, Proposition 4.3.5 and the comment after it, we obtain the following long exact sequence

of cohomology:

$$\cdots \longrightarrow H^2(G, U_K) \longrightarrow H^2(G, K^*) \longrightarrow H^2(G, \mathbb{Z}) \longrightarrow H^3(G, U_K) \longrightarrow \cdots$$

Proposition 5.2.1. *Let $K/\mathbb{Q}_p$ be a finite unramified extension. The $H^n(G, U_K) = 0$ for all $n \geq 1$.*

Proof. See [Mil97] page 80. □

The above proposition, together with the previous long exact sequence gives an isomorphism:

$$\phi : H^2(G, K^*) \xrightarrow{\sim} H^2(G, \mathbb{Z})$$

Now consider the following exact sequence, with all the maps being the obvious ones:

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

We can regard $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ as G-modules with the trivial G-action. Now, this short exact sequence gives rise to the following exact sequence:

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

We have shown (Corollary 4.3.6) that $H^n(G, \mathbb{Q}) = 0$ and hence we obtain an isomorphism:

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

We can already see that if we combine the above two isomorphism we get that $H^2(G, K^*) \simeq H^1(G, \mathbb{Q}/\mathbb{Z})$. In Example 4.3.3 we have shown that

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

Finally we have the map:

$$\begin{array}{rcl} \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \dfrac{1}{n}\mathbb{Z}/\mathbb{Z} < \mathbb{Q}/\mathbb{Z} \\ f & \longmapsto & f(\mathrm{Frob}_{K/\mathbb{Q}_p}) \end{array}$$

where $n = [K : \mathbb{Q}_p] = |\mathrm{Gal}(K/\mathbb{Q}_p)| = ord(\mathrm{Frob}_{K/\mathbb{Q}_p})$. This is clearly an isomorphism and so putting all the above maps together we get:

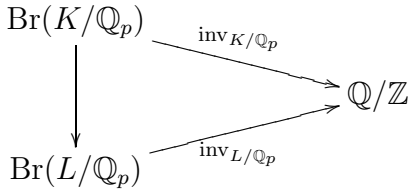
$$H^2(K/\mathbb{Q}_p) \xrightarrow{\phi} H^2(G, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

where we have used $H^2(K/\mathbb{Q}_p)$ to denote $H^2(\mathrm{Gal}(K/\mathbb{Q}_p), K^*)$ and $G = \mathrm{Gal}(K/\mathbb{Q}_p)$. The composition of all those maps, together with Theorem 4.3.8, defines a homomorphism

$$\mathrm{inv}_{K/\mathbb{Q}_p} : \mathrm{Br}(K/\mathbb{Q}_p) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

called the **invariant map**.

Also, if $\mathbb{Q}_p \subseteq K \subseteq L$ is a tower of finite field extensions such that $K/\mathbb{Q}_p$ and $L/\mathbb{Q}_p$ are unramified extensions, we have the map $\mathrm{Br}(K/\mathbb{Q}_p) \to \mathrm{Br}(L/\mathbb{Q}_p)$ (see Proposition 3.3.6) and by functoriality of $\mathrm{Br}(\cdot)$ the following diagram commutes:



(See [Mil97] page 82 for a more rigorous proof of this)

Thus, because we know every central simple $\mathbb{Q}_p$-algebra is split by some unramified extension of $\mathbb{Q}_p$, and because the above diagram commutes we have a well defined homomorphism:

$$\mathrm{inv}_p \colon \mathrm{Br}(\mathbb{Q}_p) = \bigcup_K \mathrm{Br}(K/\mathbb{Q}_p) \xrightarrow{\mathrm{inv}_{K/\mathbb{Q}_p}} \mathbb{Q}/\mathbb{Z}$$

which is in fact an isomorphism.[1]

Note also that since the only devision algebras over $\mathbb{R}$ are $\mathbb{R}, \mathbb{C}$ and $\mathbb{H}$, and that since $\mathbb{C}$ is not a central R-algebra, we must have

$$\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}.$$

Thus

$$\begin{aligned} \mathrm{inv}_\infty \colon \mathrm{Br}(\mathbb{R}) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ [\mathbb{R}] &\longmapsto 0 + \mathbb{Z} \\ [\mathbb{H}] &\longmapsto \frac{1}{2} + \mathbb{Z} \end{aligned}$$

We are finally ready to state the main theorem of this thesis. Unfortunately, we will not be proving it for that would take another thesis on its own.

Theorem 5.2.2 (Fundamental Exact Sequence of Global Class Field Theory). *The following is an exact sequence of abelian groups:*

$$0 \longrightarrow \mathrm{Br}(\mathbb{Q}) \longrightarrow \oplus_v \mathrm{Br}(\mathbb{Q}_v) \xrightarrow{\Sigma_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

where v ranges over all $M_\mathbb{Q}$.

Note that it is not even obvious that because we have a map $\mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(\mathbb{Q}_v)$ that this induces a map $\mathrm{Br}(\mathbb{Q}) \to \oplus_v \mathrm{Br}(\mathbb{Q}_v)$ as by definition, an element in $\oplus_v \mathrm{Br}(\mathbb{Q}_v)$ must be non-zero in all but a finite number of coordinates. The fact that this is the case means that an element of $\mathrm{Br}(\mathbb{Q})$ is split by "almost all" $\mathbb{Q}_v$. This also means when we apply the $\sum_v \mathrm{inv}_v$ map, we are only summing a finite number of non-zero terms. What remains now, is to see how the above exact sequence generalises the product formula. The key observation will be that we can view the Hilbert symbol as an element of $\mathrm{Br}(\mathbb{Q}_p)$.

[1] See page 109 of [Mil97].

5.3 Quaternion Algebras

We aim to identify the Hilbert symbol with an element of the Brauer group of $\mathbb{Q}_p$ for each p. Thus given p we need a way to construct a central simple $\mathbb{Q}_p$-algebra, and further a way to identify it with the Hilbert symbol. Of course the Hilbert symbol is a function $k \times k \to \{\pm 1\}$ and so we need a way of constructing a central simple algebra given two elements of a filed k. We proceed to do this.

Let k be a field with characteristic not equal to 2, and $\alpha,\ \beta \in k^*$. Then define:

$$\left(\frac{\alpha, \beta}{k}\right) := \frac{k\langle x, y\rangle}{(x^2 - \alpha, y^2 - \beta, xy + yx)}$$

Algebras of this form are called **quaternion algebras**.

Proposition 5.3.1. $\left(\frac{\alpha, \beta}{k}\right)$ *is a central simple* k*-algebra.*

Proof. It is clearly a k-algebra. Let us show that it is central. Suppose an element $P := a + bx + cy + dz$ with $a, b, c, d \in k$ in the centre. Then:

$$\begin{aligned} 0 &= xP - xP \\ &= (ax + b\alpha + cxy + dxz) - (ax + b\alpha - cxy - dxz) \\ &= 2x(cy + dy) \end{aligned}$$

Since char $k \neq 2$ and x is invertible we must have $cy + dz = 0$ and hence $c = d = 0$. Similarly we show $b = 0$, and so the centre must be k.

To show it is simple, suppose, I is a two sided ideal, and pick a non-zero element $P \in I$ as before and assume that $c \neq 0$. (If $c = 0$ it is clear how to make the proof work, by concentrating on the non-zero coefficient). Then by the same argument as before $cy + dz \in I$. Multiplying on the right by y shows $c\beta + dzy \in I$, multiplying on the left by y shows $c\beta - dzy \in I$. Adding the two elements shows $2c\beta \in I$ which is invertible. So I must be the whole algebra. □

Example 5.3.2. Observe that $\left(\frac{-1, -1}{\mathbb{R}}\right) = \mathbb{H}$.

Example 5.3.3. Let $\alpha,\ \beta \in \mathbb{Q}$ then one can immediately see that:

$$\left(\frac{\alpha, \beta}{\mathbb{Q}}\right) \otimes_{\mathbb{Q}} \mathbb{Q}_p = \left(\frac{\alpha, \beta}{\mathbb{Q}_p}\right)$$

and so the map $\mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(\mathbb{Q}_p)$ sends $\left(\frac{\alpha, \beta}{\mathbb{Q}}\right)$ to $\left(\frac{\alpha, \beta}{\mathbb{Q}_p}\right)$.

Note that $\left(\frac{\alpha, \beta}{k}\right)$ is 4 dimensional over k, and by the Artin-Wedderburn Theorem it must be isomorphic to $\mathcal{M}_n(D)$ (with $k \hookrightarrow D$). Thus it must be the case that $\left(\frac{\alpha, \beta}{k}\right)$ is isomorphic to either $\mathcal{M}_2(k)$ or is a division algebra. The following proposition will tell us how to determine which of these cases occurs.

Proposition 5.3.4. *Let* k *be a field.* $\left(\frac{\alpha, \beta}{k}\right)$ *is a division algebra if and only if* $X^2 - \alpha Y^2 - \beta Z^2 + \alpha\beta T^2$ *has no non-trivial zeros in* k^4*.*

Proof. In order for $\alpha, \beta \in k^*$ to be a division algebra it is necessary and sufficient for every element other then zero to have an inverse. Let $P = a + bx + cy + dz$ as in the previous proof. Define $\bar{P} = a - bx - cy - dz$. A simple calculation shows that $N(P) := P\bar{P} = a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2$. Thus the proposition will be proved provided we can show an element $P \neq 0$ in the algebra is invertible if and only if $N(P) \neq 0$. Suppose P^{-1} exists. Then

$$P^{-1}N(P) = P^{-1}P\bar{P} = \bar{P} \neq 0 \,,$$

and so $N(P) \neq 0$. Conversely, suppose $N(P) \neq 0$. Then $N(P) \in k^*$ (and hence invertible) and so

$$(N(P)^{-1}\bar{P})P = N(P)^{-1}N(P) = 1$$

and similarly $P(N(P)^{-1}\bar{P}) = 1$. Thus P^{-1} exists and in fact we have shown that it is $N(P)^{-1}\bar{P}$. □

Combining all this together we get the following theorem, which links our earlier work regarding the Hilbert symbol, to central simple algebras.

Theorem 5.3.5. *Let $k = \mathbb{Q}_v$ for some prime $v \in M_{\mathbb{Q}}$ and $\alpha, \beta \in \mathbb{Q}_v^*$. Then*

$$(\alpha, \beta)_v = 1 \iff \left(\frac{\alpha, \beta}{\mathbb{Q}_v}\right) \simeq \mathcal{M}_2(\mathbb{Q}_v)$$

Proof. Proposition 2.3.5 implies that $(\alpha, \beta)_v = 1$ if and only if $\beta \in N\mathbb{Q}_v(\sqrt{\alpha})$. I claim that this condition is equivalent to $X^2 - \alpha Y^2 - \beta Z^2 + \alpha\beta T^2 = 0$ having a non-trivial zero in $\mathbb{Q}_v^4$. To see this, suppose $\beta \in N\mathbb{Q}_v(\sqrt{\alpha})$, then $\beta = x^2 - \alpha y^2$ for some $x, y \in \mathbb{Q}_v$ and so the equation has a non-trivial zero $(x, y, 1, 0)$. Conversely, if the equation has a non-trivial zero (x, y, z, t) then (assuming α not a square in $\mathbb{Q}_v$, in which case $\beta \in \mathbb{Q}_v(\sqrt{\alpha}) = \mathbb{Q}_v$ and so trivially, $\beta \in N\mathbb{Q}_v(\sqrt{\alpha})$)

$$\beta = \frac{x^2 - \alpha y^2}{z^2 - \alpha t^2} = \frac{N(x + \sqrt{\alpha}y)}{N(z + \sqrt{\alpha}t)} = N\left(\frac{x + \sqrt{\alpha}y}{z + \sqrt{\alpha}t}\right) \in N\mathbb{Q}_v(\sqrt{\alpha})$$

Thus $(\alpha, \beta)_v = 1$ if and only if $X^2 - \alpha Y^2 - \beta Z^2 + \alpha\beta T^2$ has a non-trivial zero in $\mathbb{Q}_v^4$ but this occurs, by the previous proposition precisely when $\left(\frac{\alpha, \beta}{\mathbb{Q}_v}\right) \simeq \mathcal{M}_2(\mathbb{Q}_v)$. □

This theorem allows us to identify $(\alpha, \beta)_v$ with a specific element in $\mathrm{Br}(\mathbb{Q}_v)$.

The next key point to realise that if $\left(\frac{\alpha, \beta}{\mathbb{Q}_v}\right)$ is zero in $\mathrm{Br}(\mathbb{Q}_v)$ the invariant map must map it to zero. The other question is if $\left(\frac{\alpha, \beta}{\mathbb{Q}_v}\right)$ is a division algebra, then what does that invariant map map it into? We now answer this question.

Proposition 5.3.6. *Let k be a field, $\alpha, \beta \in k^*$ and $A = \left(\frac{\alpha, \beta}{k}\right)$. Then $A \simeq A^\circ$.*

Proof. Use the same notation as in proof of Proposition 5.3.4 and let $P_1, P_2 \in A$. Then, simple (but slightly tedious) expansions shows that $\overline{P_1 P_2} = \overline{P_2}\ \overline{P_1}$. Thus the map $A \to A^\circ$ sending P to $\bar{P}$ is clearly an isomorphism. □

If we combine this proposition, with Theorem 3.2.6 we get that

$$\left(\frac{\alpha,\beta}{\mathbb{Q}_v}\right) \otimes_{\mathbb{Q}_v} \left(\frac{\alpha,\beta}{\mathbb{Q}_v}\right) \simeq \mathcal{M}_n(\mathbb{Q}_v)$$

which is zero in $\mathrm{Br}(\mathbb{Q}_v)$. Thus if $\left(\frac{\alpha,\beta}{\mathbb{Q}_v}\right)$ is a division algebra, then it is not zero in $\mathrm{Br}(\mathbb{Q}_v)$ but its square (in $\mathrm{Br}(\mathbb{Q}_v)$) is, which implies the invariant map, must map it to $\frac{1}{2}+\mathbb{Z}$. We can summarise this in the following, convenient way: let $\alpha,\beta \in \mathbb{Q}_v^*$, then the following diagram commutes:

$$\begin{array}{ccc} (\alpha,\beta) & \longrightarrow & (\alpha,\beta)_v \\ \downarrow & & \begin{array}{c|c} {\scriptstyle -1}\downarrow & {\scriptstyle 1}\downarrow \\ {\scriptstyle \frac{1}{2}+\mathbb{Z}} & {\scriptstyle 0+\mathbb{Z}} \end{array} \\ \mathrm{Br}(\mathbb{Q}_v) \ni \left(\frac{\alpha,\beta}{\mathbb{Q}_v}\right) & \begin{array}{c} \mathcal{M}_2(\mathbb{Q}_v) \longmapsto 0+\mathbb{Z} \\ D \longmapsto \frac{1}{2}+\mathbb{Z} \end{array} & \longrightarrow \mathbb{Q}/\mathbb{Z} \end{array}$$

Now, since the fundamental exact sequence is exact, we must have that when we map

$$\left(\frac{\alpha,\beta}{\mathbb{Q}}\right) \longmapsto \left(\left(\frac{\alpha,\beta}{\mathbb{Q}_\infty}\right), \left(\frac{\alpha,\beta}{\mathbb{Q}_2}\right), \left(\frac{\alpha,\beta}{\mathbb{Q}_3}\right) \dots\right)$$

only a finite, even, number of $\left(\frac{\alpha,\beta}{\mathbb{Q}_v}\right)$'s are non-zero (in the respective Brauer groups). In fact, by Theorem 5.3.5 it is non-zero precisely when $(\alpha,\beta)_v = -1$, and so this can only happen a finite, even, number of times. This is an equivalent statement to

$$\prod_{v \in M_{\mathbb{Q}}} (a,b)_v = 1$$

which is the product formula we met earlier. Thus the fundamental sequence is a generalisation of the product formula.

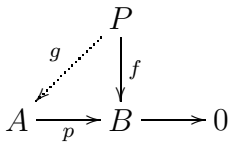
The final question that remains: how can we use the fundamental exact sequence to check whether a variety is an obstruction to the Hasse principle? We answer this in the next section.

5.4 The Brauer Group of an Affine Variety

As the title suggests, to get more obstructions to the Hasse principle, we need to generalise the Brauer group of a field to that of a variety. Recall that the Brauer group of a field consisted of equivalence classes of central simple k-algebras. Let us generalise this to Azumaya algebras. The definition is a little technical and we need some preliminary definitions from module theory.

Definition 5.4.1. *A module P is* **projective** *if the following equivalent conditions hold:*

(i) *Given a homomorphism $f\colon P \to B$ and a surjective homomorphism $p\colon A \to B$ there exists a homomorphism $g\colon P \to A$ such that*



commutes;

(ii) *Every surjective homomorphism $p\colon M \to P$ splits; that is there exists $s\colon P \to M$ such that $ps = 1_P$;*

(iii) *P is a direct summand of some free module.*

We will need this definition when we define Azumaya algebras. From now on, unless otherwise stated, R will denote a commutative ring. We will also need the following:

Definition 5.4.2. *Let A be an R-algebra. The* **enveloping algebra** *of A is defined to be $A^e := A \otimes_R A^\circ$.*

Note that there exists a natural homomorphism

$$\psi\colon A^e \longrightarrow \mathrm{End}_R(A)$$

such that $\psi(a \otimes \alpha)(y) = ay\alpha$.

Definition 5.4.3. *An R-algebra A is called an* **Azumaya algebra** *if the following two conditions hold:*

(i) *A is a finitely generated, projective and faithful (referred to simply as* **faithfully projective***) as an R-module;*[2]

(ii) *The map $\psi\colon A^e \to \mathrm{End}_R(A)$ is an isomorphism.*

We will define the $\mathrm{Br}(R)$ analogously to how we defined $\mathrm{Br}(k)$ for a field k, however instead of consisting of equivalence classes of central simple k-algebras, it will consist of equivalence classes of Azumaya algebras. Before we go on to define this equivalence relation, and subsequently the group action, let us check that in the case of R being a field the two definitions agree.

Proposition 5.4.4. *Let k be a field, and A a k-algebra. Then A is an Azumaya algebra if and only if it a central simple k-algebra.*

Proof. Suppose A is an Azumaya algebra. Then, since it is finite dimensional, $A \simeq k^n$. Thus by the second half of the definition

$$A^e \simeq \mathrm{End}_k(A) \simeq \mathrm{End}_k\left(k^n\right) \simeq \mathcal{M}_n(k).$$

Thus $A^e := A \otimes_R A^\circ$ is a central simple k-algebra and so A must also be a central simple algebra. Conversely, is a central simple k-algebra, then it clearly faithfully projective (since every module over a field is free) and since

$$A^e := A \otimes_k A^\circ \simeq \mathcal{M}_n(k) \simeq \mathrm{End}_k(A)$$

[2] Faithful means it has trivial annihilator.

it is an Azumaya algebra. □

Example 5.4.5. Analogously to how we defined quaternion algebras over a field we can do so for a ring. Let a and b be units in R. Then

$$\left(\frac{a,b}{R}\right) := \frac{R\langle x,y\rangle}{(x^2-a, y^2-b, xy+yx)}$$

is an Azumaya R-algebra. Recall, that in the case of R being a field, we proved that this construction produces a central simple algebra on page 61.

As mention earlier, $\mathrm{Br}(R)$ will consist of equivalence classes of Azumaya algebras, so we need to specify the equivalence relation; the rest will be identical to the case if R is a field.

Proposition 5.4.6. *If P is a faithfully projective R-module then $\mathrm{End}_R(P)$ is an Azumaya R-algebra.*

Proof. See [FD93] page 189. □

We can now define an equivalence relation on Azumaya algebras.

Definition 5.4.7. *Let A and B be Azumaya R-algebras. Say A is equivalent to B, written $A \sim B$, if there exists faithfully projective R-modules P and Q such that $A \otimes_R \mathrm{End}_R(P) \simeq B \otimes_R \mathrm{End}_R(Q)$. The equivalence class of A is denoted by $[A]$.*

The verification that this is indeed an equivalence relation can be found on page 191 of [FD93]. Note that if R is a field then and P and Q are the unique modules of A and B respectively, $\mathrm{End}_R(P) \simeq \mathcal{M}_n(R)$ and $\mathrm{End}_R(Q) \simeq \mathcal{M}_m(R)$ for some n, m and so $A \sim B$ if and only $A \otimes_R \mathcal{M}_n(R) \simeq B \otimes_R \mathcal{M}_m(R)$ which is equivalent to A and B having the same underlying division ring. Thus this definition extends the definition we had earlier.

Proposition/Definition 5.4.8. *The Brauer Group of R denoted by $\mathrm{Br}(R)$ consists of equivalence classes of Azumaya R-algebras, with*

$$[A] \cdot [B] := [A \otimes_R B].$$

This is indeed a well defined group multiplication, with $[A]^{-1} = [A^\circ]$ and $1_{\mathrm{Br}(R)} = [R]$

Proof. See Chapter 8 of [FD93]. We proved the corresponding result for central simple algebras on page 26. □

Note that *a fortiori*, the above implies that the tensor product of two Azumaya R-algebras is an Azumaya R-algebra.

We can now define the Brauer Group of an affine $\mathbb{Q}$-variety V.

Definition 5.4.9. *Let k be a field and $\{f_1, \ldots, f_r\} \subseteq k[X_1, \ldots, X_n]$ and let V be the corresponding variety. Then we can take*

$$R := \frac{k[X_1, \ldots, X_n]}{\mathrm{Rad}(f_1, \ldots, f_r)}$$

in the above definition of $\mathrm{Br}(R)$ and thus define $\mathrm{Br}(V) := \mathrm{Br}(R)$.

Remark 5.4.10.

(i) Recall if R is a ring and $I \trianglelefteq R$ then

$$\text{Rad } I := \{r \in R \mid r^n \in I \text{ for some } n\}.$$

It is an ideal of R.

(ii) By Hilbert's Basis Theorem $\text{Rad}(f_1, \ldots, f_r)$ is finitely generated (see [Eis95] page 26). Note that the generators of $\text{Rad}(f_1, \ldots, f_r)$ have the same common zeros as $\{f_i\}$, and thus define the same variety (for example the zeros of $X^2 - 2XY + Y^2$ are the same as that of $X - Y$ and thus the corresponding varieties are the same). In fact, the most general version of Hilbert's Nullstellensatz states that Rad I is the unique largest ideal with this property. The reason we need to take the radical of the ideal, only becomes clear if a deeper theory of varieties is developed. For our purposes it is best to accept this definition, and note the variety of interest remains unchanged.

We also establish the functoriality of $\text{Br}(\cdot)$ in the same way as for fields. If $f\colon R \to S$ is a commutative ring homomorphism, and A is an Azumaya R-algebra, then it can be shown (page 194 [FD93]) that $A \otimes_R S$ is an Azumaya S-algebra. Thus, in this case, we can define a map from $\text{Br}(R) \to \text{Br}(S) : [A] \mapsto [A \otimes_R S]$ and it can be verified that this is well defined and functorial. Recall that we proved the corresponding result for central simple algebras on page 28.

5.5 The Brauer-Manin Obstruction

We have almost developed all the tools necessary to state the Brauer-Manin obstruction to the Hasse principle. We aim to place a condition on a variety V to have a $\mathbb{Q}$-rational point, given that $V(\mathbb{Q}_v) \neq \varnothing$ for all $v \in M_{\mathbb{Q}}$.

We begin by fixing a $\mathbb{Q}$-variety V corresponding to $\{f_1, \ldots, f_r\} \subseteq \mathbb{Q}[X_1, \cdots, X_n]$. Assume that Rad $(f_1, \ldots, f_r) = (f_1, \ldots, f_r)$, otherwise replace $\{f_1, \ldots, f_r\}$ with a finite set of generators of Rad $(f_1, \ldots, f_r)$. Let

$$R := \frac{\mathbb{Q}[X_1, \cdots, X_n]}{(f_1, \cdots, f_r)}$$

We can form the **adele** associated with V by:

$$V(A_{\mathbb{Q}}) := \{(x_v) \mid x_v \in V(\mathbb{Q}_v)\}$$

Remark 5.5.1. The maps $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$ gives rise to the injection $V(\mathbb{Q}) \hookrightarrow V(A_{\mathbb{Q}})$.

The key point to realise that if $x = (x_v) \in V(A_{\mathbb{Q}})$ then every $x_v = (x_v^{(1)}, \ldots, x_v^{(n)}) \in \mathbb{Q}_v^n$ gives rise to a homomorphism

$$\begin{aligned} R := \frac{\mathbb{Q}[X_1, \ldots, X_n]}{(f_1, \cdots, f_r)} &\longrightarrow \mathbb{Q}_v \\ X_i &\longmapsto x_v^{(i)} \end{aligned}$$

This means that for every $[A] \in \mathrm{Br}(V)$ we can get $[A \otimes_R \mathbb{Q}_v] \in \mathrm{Br}(\mathbb{Q}_v)$ and so for every $x \in V(A_{\mathbb{Q}})$ we can form the map

$$\begin{aligned} \langle \cdot, \cdot \rangle : \mathrm{Br}(V) \times V(A_{\mathbb{Q}}) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ ([A], (x_v)) &\longmapsto \sum_{v \in M_{\mathbb{Q}}} \mathrm{inv}_v \left[A \otimes_R \mathbb{Q}_v \right] \end{aligned}$$

Further we define

$$V(A_{\mathbb{Q}})^{\mathrm{Br}} := \{ x \in V(A_{\mathbb{Q}}) \mid \langle A, x \rangle = 0, \text{ for all } A \in \mathrm{Br}(V) \}$$

The fundamental exact sequence, together with the previous remark assures that $V(\mathbb{Q}) \hookrightarrow V(A_{\mathbb{Q}})^{\mathrm{Br}}$. Thus the assumption that V has a $\mathbb{Q}$-rational point places a necessary condition on $V(A_{\mathbb{Q}})$; namely that $V(A_{\mathbb{Q}})^{\mathrm{Br}} \neq \varnothing$. Thus if $V(A_{\mathbb{Q}})^{\mathrm{Br}} = \varnothing$, whilst $V(A_{\mathbb{Q}}) \neq \varnothing$ then we know that V is an obstruction to the Hasse principle. Obstructions arising in this fashion are classified as **Brauer-Manin Obstructions**.

Example 5.5.2. Lets see how Theorem 2.5.1 is an example of a Brauer Manin obstruction. We let $h := Z^2 + Y^2 - f(X)g(X)$ and V be the corresponding variety. We saw that h has a zero in $\mathbb{Q}_v^3$ for all $v \in M_{\mathbb{Q}}$. i.e. $V(A_{\mathbb{Q}}) \neq \varnothing$. Now assume it has a solution $(x, y, x) \in \mathbb{Q}^3$. Let

$$R := \frac{\mathbb{Q}[X, Y, Z]}{(Z^2 + Y^2 - f(X)g(X))}$$

and $[A] := \left[\left(\frac{-1, f(x)}{R} \right) \right] \in \mathrm{Br}(R)$. (Note that $f(x) \in \mathbb{Q}^*$ so is clearly a unit). Then for all $x \in V(A_{\mathbb{Q}})$

$$\langle A, x \rangle = \sum_v \mathrm{inv}_v \left[A \otimes_R \mathbb{Q}_v \right] = \sum_v \mathrm{inv}_v \left[\left(\frac{-1, f(x)}{\mathbb{Q}_v} \right) \right] \neq 0$$

This implies $V(A_{\mathbb{Q}})^{\mathrm{Br}} = \varnothing$ and so V is an example of a Brauer-Manin obstruction.

Chapter 6

Closing Remarks

The more general version of the Brauer Manin obstruction replaces $\mathbb{Q}$ with a finite field extension and $\mathbb{Q}_v$ with its corresponding completions. The mathematics required for this is not significantly more complicated though the proofs are slightly harder; one essentially replaces primes in $\mathbb{Z}$ with prime elements in the ring of integers of the finite extension. The rest of the theory, concerning the derivation of the fundamental exact sequence, comes out in the same way.

It has been shown (see [Sko99]) that not all obstructions are of the Brauer-Manin type. That is a variety V, such that $V(A_{\mathbb{Q}})^{\mathrm{Br}} \neq \varnothing$ and yet $V(\mathbb{Q}) = \varnothing$ was found. However, a slight generalisation of the Brauer-Manin obstruction has been found that in fact captures the example given in [Sko99]. Recently, examples that even the generalisation does not capture have been found. This motivated the question: what properties must a variety have such that Brauer-Manin obstruction is the only possible obstruction to the Hasse principle? Research into this is also currently being carried out. See for example [Poo06].

One other concept that I did not address in this thesis is that of projective varieties. Obstruction (in fact rather simple ones) to the Hasse principle can be constructed if the variety has a singularity at infinity. The reader should be advised that if he or she were to study the Hasse principle in its entirety, he or she would need to consider projective varieties, not just affine ones as we have done.

References

[Art91] Michael Artin. *Algebra*. Prentice Hall Inc., Englewood Cliffs, NJ, 1991.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[FD93] Benson Farb and R. Keith Dennis. *Noncommutative algebra*, volume 144 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.

[Gou97] Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Mil97] J.S. Milne. *Class Field Theory*. Notes for Math 776 taught at the University of Michigan. Can be obtained for free from: www.math.lsa.umich.edu/ jmilne/, 1997.

[Mil98] J.S. Milne. *Algebraic Number Theory*. Notes for a course taught at the University of Michigan in F92 as Math 676. Can be obtained for free from: www.math.lsa.umich.edu/ jmilne/, 1998.

[Pey05] Emmanuel Peyre. Obstructions au principe de Hasse et à l'approximation faible. *Astérisque*, (299):Exp. No. 931, viii, 165–193, 2005. Séminaire Bourbaki. Vol. 2003/2004.

[Poo06] Bjorn Poonen. Heuristics for the Brauer-Manin obstruction for curves. *Experiment. Math.*, 15(4):415–420, 2006.

[Row88a] Louis H. Rowen. *Ring theory. Vol. I*, volume 127 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1988.

[Row88b] Louis H. Rowen. *Ring theory. Vol. II*, volume 128 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1988.

[Ser73] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Sko99] Alexei N. Skorobogatov. Beyond the Manin obstruction. *Invent. Math.*, 135(2):399–424, 1999.