THE BRAUER-MANIN OBSTRUCTION AND THE HASSE PRINCIPLE

by

ERIC PAUL ROBERT

BScKin(2000) - UNB Fredericton
BEd (2002) - UNB Fredericton

A Thesis Submitted in Partial Fulfilment of
the Requirements for the Degree of

MASTER OF SCIENCE

in the Graduate Academic Unit of Mathematics and Statistics

Supervisor:	Prof. Colin Ingalls, (Mathematics), UNB
Examining Board:	Prof. Rodney Cooper, (Computer Science), UNB
	Prof. Colin Ingalls, (Mathematics), UNB
	Prof. Hugh Thomas, (Mathematics), UNB
External Examiner:	Prof. Rodney Cooper, (Computer Science), UNB

This thesis is accepted

. . . . . .

Dean of Graduate Studies

THE UNIVERSITY OF NEW BRUNSWICK

April 2009

University Library Release Form

University of New Brunswick

Harriet Irving Library

This is to authorize the Dean of Graduate Studies to deposit two copies of my thesis/report in the University Library on the following conditions:

The author agrees that the deposited copies of this thesis/report may be made available to users at the discretion of the University of New Brunswick.

Date	Signature of Author
Signature of Supervisor	Signature of the Dean of Graduate Studies

BORROWERS must give proper credit for any use made of this thesis, and obtain the consent of the author if it is proposed to make extensive quotations, or to reproduce the thesis in whole or in part.

Abstract

For systems of polynomial equations where the Hasse principle holds, there exists a finite process through which enough local (p-adic) information can be gathered to decide the existence of a global (rational) solution. For instances where the Hasse principle fails, knowledge of obstructions to global solutions may advance the problem asking for a similar finite process. The first chapters of this thesis consist of an expository development of the background content on p-adic numbers, the Brauer group, the Brauer-Manin obstruction and the Hasse principle. The final chapter describes an example of a variety for which the Hasse principle does not hold and another example where the failure of the Hasse principle is explained by the Brauer-Manin obstruction.

Acknowledgements

I am forever indebted to all those who came in contact with me while I was writing this thesis. I want to thank Dr. Ingalls for all his time and the patience he has shown during the whole process. I also want to thank the members of the Department of Mathematics and Statistics at the University of New Brunswick for all their help and advice. Finally, I want to thank my wife Naomi for her unselfish support through all this.

Table of Contents

Introduction

The tenth of David Hilbert's celebrated problems asks if there exists a finite process to decide whether any multivariate polynomial equation with integral coefficients has integral solutions or not. Although this problem was negatively put to rest in the early 1970's [13], a similar problem concerned with the solubility over the rational numbers still remains unsolved today. This open problem provides some of the motivation behind the research into the topic with which this thesis is concerned.

Looking more closely at this second problem, we can make some progress by searching for solutions in 'natural' extensions of $\mathbb{Q}$ called the fields of p-adic numbers, denoted $\mathbb{Q}_p$ (one for each of the infinitely many primes p), and in the field of real numbers $\mathbb{R}$ (which we will, from time to time, refer to as $\mathbb{Q}_\infty$). A particularly desirable property of these p-adic fields is, as will be seen later, that deciding the existence of a p-adic solution to a multivariate polynomial equation, is a finite problem. In fact, although this leaves infinitely many p-adic fields to verify, it is still a finite problem to decide if there exist any which do not contain a solution to the given equation. This finite process will sometimes be enough to prove the non-existence of rational solutions. If any of the p-adic fields fail to contain a solution, then there can be no rational solutions since rational numbers are also p-adic numbers (by virtue of the extension through which all fields $\mathbb{Q}_p$ came to be and which will be described later).

What is much more remarkable is that in situations where the Hasse principle is said to hold, if there exist non-trivial solutions to an equation in all infinitely many p-adic fields and in $\mathbb{R}$, then there has to exist a non-trivial solution in $\mathbb{Q}$. The unfortunate fact is that it is not always clear if the equation we are studying is such that the Hasse principle holds.

Hasse himself, (to whom we can attribute the said principle) was aware of the

existence of some counter-examples to his principle. In 1970, Yuri Manin [12] brought together all counter-examples to the Hasse principle known until then, and explained them by the presence of a particular obstruction called the Brauer-Manin obstruction. Since then, some have proposed new obstructions which cannot be explained by Manin's work [18].

The first three chapters of this thesis will develop the required material to describe the Brauer-Manin obstruction. This will include a construction of the p-adic fields, a description of their elements, and results related to computations. We will then prove that verifying the solubility of Diophantine problems over all p-adic fields is a finite process and will describe Hensel's lemma and the role it plays in the proof. We will also build the Brauer group of a field as well as of a ring and make some connections with Galois cohomology. In part to help motivate the rest of the content, a trivial example of a failure of the Hasse principle will also be included. We will then see the fundamental exact sequence of global class field theory, bring together all previous chapters and discuss the Brauer-Manin obstruction before we finally dissect two examples of failures of the Hasse principle. Throughout the chapters, will assume exposure to standard results from introductory number theory (such as quadratic reciprocity), algebraic geometry and abstract algebra.

Chapter 1
p-adic Numbers

This chapter will describe three areas of the theory of p-adic numbers, developing a crucial foundation for many results which will be required in later chapters. This will include a general introduction to the p-adic numbers, some details on Hensel's lemma (an indispensable tool for working over $\mathbb{Q}_p$), as well as a discussion of the finitude of the problem of deciding the solubility of a system of polynomial equations over all p-adic fields and over $\mathbb{R}$. Often, only a sketch of a proof will be included, or the proof may altogether be omitted and simply referenced.

1.1 Construction

The methods used to build each p-adic field $\mathbb{Q}_p$ are very similar to the ones used to build the real numbers $\mathbb{R}$ from the rational numbers $\mathbb{Q}$. The following definitions will provide a starting point.

Definition 1.1.1. *An absolute value over a field* $\Bbbk$ *is a function* $|\cdot| : \Bbbk \to \mathbb{R}_+$*, where* $|x| = 0$ *iff* $x = 0$*,* $|xy| = |x| \cdot |y|$ *for all* $x,\ y \in \Bbbk$*, and* $|x+y| \leq |x|+|y|$ *for all* $x,\ y \in \Bbbk$*.*

We denote the usual absolute value $|\cdot|_\infty$ where

$$|x|_\infty = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0. \end{cases}$$

For a choice of prime p, if we let $x = p^{\operatorname{ord}_p x} \cdot \frac{a}{b}$, where $p \nmid ab$, one can verify that the following function $|x|_p = p^{-\operatorname{ord}_p x}$ is an absolute value regardless of the choice of p. Note also that setting $|x| = 1$ if $x \neq 0$ and $|0| = 0$ gives yet another absolute value. For obvious reasons, this last example is referred to as the trivial absolute value. A theorem by Ostrowski states that every non-trivial absolute value on $\mathbb{Q}$ is equivalent to one of the absolute values $|\cdot|_p$ where p is a prime or $p = \infty$. A proof of this theorem can be found on page 44 of [6].

As we will soon be concerned with the convergence of sequences in a field, we need the following definition.

Definition 1.1.2. *Let $\Bbbk$ be a field. A sequence of elements of $\Bbbk$ is Cauchy with respect to an absolute value $|\cdot|_p$, if for every $\varepsilon > 0$ there exists $M \in \mathbb{N}$ such that for all $m, n \geq M$, $|x_n - x_m|_p \leq \varepsilon$.*

Although many Cauchy sequences will converge in a field, being Cauchy is not a sufficient condition to guarantee convergence in some fields. As the following definition implies, it is possible to enlarge the base field to force every Cauchy sequence to converge in the new field.

Definition 1.1.3. *A field $\Bbbk$ is complete with respect to an absolute value $|\cdot|_p$ if every Cauchy sequence of elements of $\Bbbk$ has a limit in $\Bbbk$.*

Intuitively, this is saying that in a complete field, every sequence which "should" converge, actually converges. The field $\mathbb{Q}$ is not complete under the usual absolute value $|\cdot|_\infty$ since $3, 3.1, 3.14, \ldots$ (where the n^{th} term is the first n digits of the decimal expansion of π), is a Cauchy sequence of rational numbers whose limit is $\pi \notin \mathbb{Q}$. The completion of a field $\Bbbk$ with respect to a certain absolute value is the smallest field which contains $\Bbbk$ and is also complete with respect to the same absolute value. We

thus construct $\mathbb{R}$ as the completion of $\mathbb{Q}$ under the usual absolute value by defining $\mathbb{R}$ to be equivalent to the set of all limits of rational Cauchy sequences (with respect to $|\cdot|_\infty$) modulo an equivalence relation. This equivalence relation treats two Cauchy sequences $s_1 = \{a_i\}$, and $s_2 = \{b_i\}$ as equivalent if $|a_i - b_i|_\infty \to 0$ as $i \to \infty$.

It is clear that this construction of the real numbers from the rational numbers is dependent on a choice of absolute value. Next, we define the fields of interest in this chapter.

Definition 1.1.4. *Using term-wise addition and multiplication, let C_p be the ring of rational Cauchy sequences with respect to $|\cdot|_p$. Let N_p be the ideal generated by all rational (trivially Cauchy) sequences that tend to zero with respect to $|\cdot|_p$. Then $\mathbb{Q}_p := C_p/N_p$.*

Note that N_p is a maximal ideal in C_p and hence C_p/N_p is a field. We also see that we have an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ for any prime p since for $x \in \mathbb{Q}$, we can take the constant, (trivially Cauchy) sequence $(x, x, x, ...)$ as a representative of x in $\mathbb{Q}_p$. Details about this definition can be found in p26-28 of [1].

In preparation for the next theorem, we make the following definition.

Definition 1.1.5. *The set of p-adic integers is $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$.*

In an effort to provide a concrete description of the elements of $\mathbb{Q}_p$, we see the following theorem.

Theorem 1.1.6. *Every equivalence class α in $\mathbb{Z}_p$ has exactly one representative Cauchy sequence of the form $\{\alpha_i\}$ for which $0 \leq \alpha_i < p^i$, and $\alpha_i \equiv \alpha_{i+1} \pmod{p^i}$ for all $i \in \mathbb{N}$.*

A proof of this can be found in [9], p.11-13.

To extend the previous description to all p-adic numbers, notice that if $|a|_p > 1$, then $|a \cdot |a|_p|_p \leq 1$. Theorem 1.1.6 provides a representative sequence for $a \cdot |a|_p$, and we thus get a convenient description of elements of $\mathbb{Q}_p$ as infinite base p expansions with $m \in \mathbb{Z}$ as $\alpha = \frac{a_0}{p^m} + \frac{a_1}{p^{m-1}} + \ldots + \frac{a_{m-1}}{p} + a_m + a_{m+1}p + a_{m+2}p^2 + \ldots$. We can also represent α as its canonical abbreviated p-adic expansion $a_0 a_1 \ldots \ a_{m-1}.a_m a_{m+1} a_{m+2} \ldots$.

1.2 Hensel's Lemma

At this point it seems natural to seek a solution to a polynomial equation over $\mathbb{Q}_p$.

Example 1.2.1. *Solve $x^2 = q$ over $\mathbb{Q}_p$ where $0 \leq q < p$, $q \in \mathbb{Z}$. Equivalently, we require a p-adic expansion $a_0 a_1 a_2 a_3 \ldots$, such that $0 \leq a_i < p$, $a_i \in \mathbb{Z}$, and $(a_0 + a_1 \cdot p + \ldots + a_i \cdot p^i + \ldots)^2 \equiv q + 0 \cdot p + 0 \cdot p^2 + \ldots \pmod{p^m}$ for every $m \in \mathbb{N}$. From our definition of the p-adic expansion, if there exists a solution to the equation above, we can find a_0 by solving $(a_0)^2 \equiv q \pmod{p}$. Knowing a value for a_0, we can repeat the process seeking a_i in $(a_0 + a_1 \cdot p + \ldots + a_i \cdot p^i)^2 \equiv q \pmod{p^{i+1}}$ for increasing values of i.*

In a sense, each step of the process utilized in Example 1.2.1 provides an approximation to the solution while an exact solution would come from infinitely many iterations. Unfortunately, for some (potentially very large) values of i in the process above, it is possible that no value of a_i allows for the approximation to continue. The following theorem does however give conditions under which we are guaranteed a p-adic solution for a polynomial equation over $\mathbb{Q}_p$.

Theorem 1.2.2 (Hensel's lemma)**.** *Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ \ldots \ + a_k x^k$ be a polynomial with integral coefficients and suppose that there exists $\alpha_0 \in \mathbb{Z}$ and some $N \in \mathbb{N}$ such that $f(\alpha_0) \equiv 0 \pmod{p^N}$ while $f'(\alpha_0) \not\equiv 0 \pmod{p^M}$ where f' is the*

formal derivative of $f(x)$ *and* $M \leq \frac{1}{2}N$. *Then there exists* $\alpha \in \mathbb{Z}_p$ *such that* $\alpha \equiv \alpha_0 \pmod{p^M}$ *and* $f(\alpha) = 0$.

Proof. To complete the proof, we show that under the theorem's conditions, we can construct

$$\alpha = \lim_{n\to\infty} \alpha_n, \text{ with } \alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)},$$

and that α is as required. We therefore will show that for all n, $f(\alpha_n) \equiv 0 \pmod{p^{N+n}}$ hence $f(\alpha) = 0$. We will also show that $\alpha_{n+1} \equiv \alpha_n \pmod{p^{M+n}}$, and therefore $\alpha \equiv \alpha_0 \pmod{p^M}$. This last congruence ensures that $f'(\alpha_n)$ is always nonzero.

First, we start by showing that given α_n, we can find the required α_{n+1}. Assuming $f(\alpha_n) \equiv 0 \pmod{p^{N+n}}$ and $f'(\alpha_n) \not\equiv 0 \pmod{p^M}$, then $|f(\alpha_n)|_p \leq p^{-N-n}$ and $|f'(\alpha_n)|_p > p^{-M}$. From this, we are assured that

$$\left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right|_p = \frac{|f(\alpha_n)|_p}{|f'(\alpha_n)|_p} < \frac{p^{-N-n}}{p^{-M}} = p^{-N+M-n}.$$

Therefore $\left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right|_p \leq p^{-N+M-n-1}$ and there exists $k_n \in \mathbb{Z}_p$ such that $\frac{f(\alpha_n)}{f'(\alpha_n)} = k_n p^{N-M+n+1}$. Setting

$$b_n = -k_n p^{N-M+n+1},$$

we find that

$$f(\alpha_n) + f'(\alpha_n) b_n = 0. \tag{1.1}$$

Now, if $\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$, then

$$\begin{aligned} f(\alpha_{n+1}) &= f(\alpha_n + b_n) \\ &= f(\alpha_n) + f'(\alpha_n)b_n + \frac{f''(\alpha_n)(b_n)^2}{2!} + \frac{f'''(\alpha_n)(b_n)^3}{3!} + \cdots \\ &= \frac{f''(\alpha_n)(b_n)^2}{2!} + \frac{f'''(\alpha_n)(b_n)^3}{3!} + \cdots \text{(by equation 1.1)} \\ &\equiv 0 \pmod{p^{N+n+1}}. \end{aligned}$$

We also find that $\alpha_{n+1} = \alpha_n + b_n = \alpha_n - k_n p^{N-M+n+1} \equiv \alpha_n \pmod{p^{M+n}}$, hence $f'(\alpha_{n+1}) \neq 0$.

The case for $n = 0$ follows from our assumption, and we have therefore shown inductively that given α_0 such that $f(\alpha_0) \equiv 0 \pmod{p^N}$ and $f'(\alpha_0) \not\equiv 0 \pmod{p^M}$, it is possible to find $\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$ for larger and larger n constructing the required α.

This completes the proof of Hensel's lemma. □

While this version of the theorem is for a univariate polynomial equation, an analogue for a multivariate equation is similarly available on page 67 of [7] as is a further generalization for k equations in r variables.

1.3 Finitude of the Problem

We have seen so far that under some relatively relaxed conditions (for details on how they could be relaxed even further, see p.3185 of [5]) we can guarantee a solution to a polynomial equation (or even to a system of multivariate polynomial equations) over some p-adic field. The problem now is that as mentioned earlier, we would like to be able to decide if there exist non-trivial solutions over

every such field (including $\mathbb{Q}_\infty = \mathbb{R}$) but since there are infinitely many p-adic fields, the task seems daunting. Further, if there were no non-trivial solutions to a multivariate polynomial equation in some $\mathbb{Q}_p$, it is not clear how many times we might find solutions $(\alpha_i) \pmod{p^{i+1}}$ where the derivative condition is not met for increasing i before we failed and decidedly found that no non-trivial solutions existed over that particular field. It is therefore somewhat spectacular that given a system of polynomial equations $f_m(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, we can verify whether or not there exist solutions $(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq (0, 0, \ldots, 0)$ such that $f_1(\alpha_1, \alpha_2, \ldots, \alpha_n) = f_2(\alpha_1, \alpha_2, \ldots, \alpha_n) = \ldots = f_m(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ in all p-adic fields in finitely many steps. Before we can advance any further, we introduce some useful language and notation from algebraic geometry.

Definition 1.3.1. *Let $\mathbb{K}$ be a field. For any ideal $I \triangleleft \mathbb{K}[x_1, x_2, \ldots, x_n]$, we say $Z(I) = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{K}^n \mid f_i(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ for all $f_i \in I\}$ is an algebraic subset of $\mathbb{K}^n$. Then an algebraic $\mathbb{K}$-variety V is an algebraic subset of $\mathbb{K}^n$ which is not a union of two proper algebraic subsets of $\mathbb{K}^n$. If $\Bbbk \subset \mathbb{K}$, we will write $V(\Bbbk)$ for $\{(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \Bbbk^n \mid f_i(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ for all $f_i \in I\}$. Note that this definition of a variety is sometimes referred to more specifically as an affine variety. Projective varieties can similarly be defined and therefore the rest of this thesis could have been written in the language of projective geometry.*

With the concept of a variety defined, we can now move ahead to gain some insight in the finite process of deciding whether or not a system of polynomial equations has non-trivial solutions in every completion of $\mathbb{Q}$. We look at the next two theorems in the case of a single polynomial equation. The first of these theorems, due to Cassels, can be found on page 204 of [3] and reduces the number of p-adic fields which need to be considered.

Theorem 1.3.2. *Given $f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, there exists some $P \in \mathbb{Z}$, computable in terms of f, such that for all primes $p > P$, there exists some $0 \neq (x_1, x_2, \ldots, x_n) \in \mathbb{Q}_p^n$ with $f(x_1, x_2, \ldots, x_n) = 0$*

Proof. For all but a finite set of primes A, every nonsingular point of the variety defined by f over the rational numbers, gives rise to a nonsingular point of the variety defined by f over the field of p elements. By a result of Lang and Weil, [10], the number of points of $V(\mathbb{Z}/p\mathbb{Z})$ is equal to $p^r + O(p^{r-\frac{1}{2}})$ where r is the dimension of $V(\mathbb{Q})$ and $O(p^{r-\frac{1}{2}})$ can be computed explicitly. Since the singular points of $V(\mathbb{Z}/p\mathbb{Z})$ are on a proper subvariety, there are $O(p^{r-1})$ such points which leads to the conclusion that for all primes larger than the largest prime in A and sufficiently large to make $p^r + O(p^{r-\frac{1}{2}}) - O(p^{r-1}) > 0$, we find that $V(\mathbb{Z}/p\mathbb{Z})$ has nonsingular points which, by Hensel's lemma lead to p-adic points. □

There are now only finitely many p-adic fields left to verify. Although we have reduced the number of cases to a finite one, we still need to show that we can decide whether or not a polynomial equation has a non-trivial solution in each $\mathbb{Q}_p$ in a finite number of steps. This time, we will look at the case of a univariate polynomial. Hensel's lemma is a crucial part of the process but because of the possibility of finding solutions $\alpha_i \pmod{p^{i+1}}$ for larger and larger values of i where for each i, $f'(\alpha_i) \equiv 0 \pmod{p}$ we will use the following theorem of Cassels from p.203 of [3].

Theorem 1.3.3. *Let $f(x) \in \mathbb{Z}[x]$ be irreducible in $\mathbb{Q}[x]$. Then there exists an N which can be given explicitly in terms of $f(x)$ such that if $f(\alpha) \equiv 0 \pmod{p^N}$, then $f'(\alpha) \not\equiv 0 \pmod{p^{\lfloor \frac{N}{2} \rfloor - 1}}$.*

Proof. If $f(x)$ is irreducible in $\mathbb{Q}[x]$, then $f(x)$ and $f'(x)$ are coprime in $\mathbb{Q}[x]$. By the Euclidean algorithm in $\mathbb{Q}[x]$, there then exist $p(x)$ and $q(x)$ such that $p(x)f(x) +$

$q(x)f'(x) = GCD(f(x), f'(x)) \in \mathbb{Q} \subset \mathbb{Q}[x]$. By clearing denominators, we can find $r(x)$ and $s(x)$ in $\mathbb{Z}[x]$ such that $r(x)f(x) + s(x)f'(x) = t \in \mathbb{Z}$. If $f(\alpha) \equiv 0 \pmod{p^N}$ and $f'(\alpha) \equiv 0 \pmod{p^{\lfloor \frac{N}{2} \rfloor - 1}}$ for all N, then $t \equiv r(\alpha)f(\alpha) + s(\alpha)f'(\alpha) \equiv 0 \pmod{p^{\lfloor \frac{N}{2} \rfloor - 1}}$ for every N which is impossible. We therefore find that when there exists an α such that $f(\alpha) \equiv 0 \pmod{p^N}$ with $p^{\lfloor \frac{N}{2} \rfloor - 1}$ larger than the t found by clearing denominators, we are guaranteed that $f'(x) \not\equiv 0 \pmod{p^{\lfloor \frac{N}{2} \rfloor - 1}}$. □

Given an α as in Theorem 1.3.3, Hensel's lemma then allows us to deduce a p-adic solution to $f(x)$. Theorem 1.3.3 along with Theorem 1.3.2 then confirm that the solubility of a univariate polynomial equation over all the p-adic fields can be verified in a finite number of steps. Both of the previous theorems could be proven in more generality, to include systems of multivariate polynomial equations. For details surrounding the more general cases, see page 204 of [3].

Finally, the case where $p = \infty$, (or $\mathbb{Q}_p = \mathbb{R}$) is handled by Tarski's results on decidability in elementary algebra [20] which imply that the process of deciding if $f(x_1, x_2, \ldots, x_n) = 0$ has any non-trivial solutions over $\mathbb{R}^n$ is finite. These results also take care of the situation involving a system of multivariate polynomial equations since solving $f_1 = f_2 = \ldots = f_m = 0$ is equivalent to solving $f_1^2 + f_2^2 + \ldots + f_m^2 = 0$. We have hence seen that we can verify whether or not a system of multivariate polynomial equations has non-trivial solutions over $\mathbb{Q}_p$ (for primes p and $p = \infty$) in a finite (albeit possibly excruciatingly large) number of operations.

Chapter 2
The Brauer Group

As it has already been hinted, the Brauer groups of fields and rings play a vital role in the description of the Brauer Manin-Obstruction. In Section 2.1, we state definitions and results required to construct the Brauer group. In Section 2.2, we construct the Brauer group of a field $\Bbbk$, denoted $Br(\Bbbk)$, and via crossed product algebras and Galois cohomology, find ways of describing elements of $Br(\Bbbk)$. Finally, in Section 2.3, we construct the Brauer group of a commutative ring which allows us to discuss the Brauer group of an affine variety.

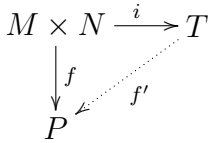
2.1 Preliminaries

Unless specified otherwise, for the remainder of this section, we will assume that R is a commutative ring. Material from this chapter is adapted from [4] and most proofs of theorems are omited.

To get started, the following theorem provides a description of the tensor product, an operation which will be needed later.

Theorem 2.1.1. *: Let M and N be R-modules. Then there exists an R-module T, and a bilinear map $i : M \times N \longrightarrow T$ such that given any R-module P, and any bilinear map $f : M \times N \longrightarrow P$, there exists a unique homomorphism f' such that the*

following diagram commutes:



T is referred to as the tensor product of M and N over R, denoted $M \otimes_R N$ and is unique up to isomorphism.

For a proof of Theorem 2.1.1, see [4] p.12-13.

We next define some special rings and modules.

Definition 2.1.2. *: Let R be a ring and A be a ring which is also an R-module. If $x(ab) = (xa)b = a(xb)$ for all $x \in R,\ a, b\ \in A$, then A is an R-algebra.*

We then extend the concept of homomorphisms and tensor products to algebras.

Definition 2.1.3. *: Let A and B be R-algebras. If $f : A \longrightarrow B$ is an R-module homomorphism, and a compatible ring homomorphism, then f is an R-algebra homomorphism.*

Theorem 2.1.4. *: Let $\Bbbk$ be a field and R and S be $\Bbbk$-algebras. If we let*

$$(r \otimes s) \cdot (r' \otimes s') = rr' \otimes ss'$$

for all $r, r' \in R$ and $s, s' \in S$, then $R \otimes_\Bbbk S$ is a $\Bbbk$-algebra.

For a proof, see [4] p.81-82.

The next proposition extends an algebra to another related algebra.

Proposition 2.1.5. *If R is a $\Bbbk$-algebra, and $\mathbb{K}$ is a field extension of $\Bbbk$, then $\mathbb{K} \otimes_\Bbbk R$ is a $\mathbb{K}$-algebra. We say $\mathbb{K} \otimes_\Bbbk R$ is the extension of scalars.*

For a proof, see [4] p.83.

With $\Bbbk$-algebras and some related concepts defined, we discuss division rings and simple algebras in preparation for the Wedderburn-Artin theorem.

Definition 2.1.6. *A division ring D is a ring (not necessarily commutative) where $1 \neq 0$ and every non-zero element is invertible. A commutative division ring is therefore a field.*

Definition 2.1.7. *A $\Bbbk$-algebra S is simple if, as a ring, it contains no proper, non-zero two-sided ideals.*

Theorem 2.1.8 (Wedderburn-Artin)**.** *Let S be a finite dimensional simple $\Bbbk$-algebra. Then $S \simeq M_n(D)$ for some division ring D where D is unique up to isomorphism.*

For a proof, see [8] p.48.

The next three definitions will be necessary to describe an equivalence relation used in the definition of the Brauer group.

Definition 2.1.9. *The center of a $\Bbbk$-algebra S is $Z(S) := \{x \in S \mid xs = sx \text{ for all } s \in S\}$.*

Definition 2.1.10. *S is a central $\Bbbk$-algebra if $Z(S) = \Bbbk$. S is central simple if it is central and simple.*

Definition 2.1.11. *Let S and T be finite dimensional central simple $\Bbbk$-algebras and D and E be division rings. We say S and T are similar if whenever $S \simeq M_n(D)$ and $T \simeq M_m(E)$ then $D \simeq E$.*

As we are about to see, the next definition will allow the description of the inverses of elements of the Brauer group.

Definition 2.1.12. *Let A be a central simple $\Bbbk$-algebra. The opposite algebra of A, A° is the algebra whose set and addition of elements are the same as those of A, but whose multiplication $*$ gives $a * b = ba$ for $a, b \in A$.*

The following theorem will be useful in describing elements of the Brauer group via crossed product algebras.

Theorem 2.1.13 (Skolem-Noether)**.** *Let S be a finite dimensional central simple $\Bbbk$-algebra and let A, B be simple $\Bbbk$-subalgebras of S. Given any isomorphism $\alpha : A \longrightarrow B$ where $\alpha(k) = k$ for all $k \in \Bbbk$, there exists $x \in S$ such that, for all $a \in A$, $\alpha(a) = x^{-1}ax$.*

Putting $S = A = B$, we find that every automorphism of S which leaves elements of $\Bbbk$ fixed (that is every $\Bbbk$-automorphism of S) is an inner automorphism. For a proof, see [8] p.99-100.

2.2 The Brauer Group of a Field

We are now ready for the construction of the Brauer group of a field $\Bbbk$

Definition/Theorem 2.2.1. *The Brauer group of a field $\Bbbk$, denoted $Br(\Bbbk)$ is the group of equivalence classes of finite dimensional central simple $\Bbbk$-algebras where the tensor product over $\Bbbk$ is the group operation, the equivalence class of $\Bbbk$, denoted $[\Bbbk]$ is the identity element, and $S \sim T$ if S and T are similar according to Definition 2.1.11. Furthermore, for the equivalence class $[A]$ of a central simple $\Bbbk$-algebra A, the inverse is $[A^\circ]$.*

Theorem 2.2.2. *Let $\Bbbk$ and $\mathbb{K}$ be fields, and $\phi : \Bbbk \longrightarrow \mathbb{K}$ be a field homomorphism. Then there is a group homomorphism $Br(\phi) : Br(\Bbbk) \longrightarrow Br(\mathbb{K})$ given by $A \mapsto A \otimes_\Bbbk \mathbb{K}$ such that $Br(\phi \circ \psi) = Br(\phi) \circ Br(\psi)$ and $Br(id) = id$.*

Theorem 2.2.2 is stating, using category theory language, that $Br(\cdot)$ is a covariant functor. A proof of this theorem can be found in [11] on pages 28 and 29. The group homomorphism we obtain will provide us access to $Br(\mathbb{K}/\Bbbk)$, the relative Brauer group of $\mathbb{K}$ over $\Bbbk$ which, as we will see later is in many ways easier to work with.

Definition 2.2.3. *Using the group homomorphism from Theorem 2.2.2, the relative Brauer group of* $\mathbb{K}$ *over* $\Bbbk$ *is* $Br(\mathbb{K}/\Bbbk) := ker(Br(\Bbbk) \longrightarrow Br(\mathbb{K}))$.

Elements of $Br(\mathbb{K}/\Bbbk)$ are therefore finite dimensional central simple $\Bbbk$-algebras whose tensor product over $\Bbbk$ with $\mathbb{K}$ is isomorphic to matrices over $\mathbb{K}$.

Definition 2.2.4. *Let* $\mathbb{K}/\Bbbk$ *be a finite field extension. We say* $\mathbb{K}/\Bbbk$ *is a normal extension if every irreducible polynomial in one variable with coefficients in* $\Bbbk$ *and a root in* $\mathbb{K}$ *has all its roots in* $\mathbb{K}$. *We also say* $\mathbb{K}/\Bbbk$ *is a separable extension if for every* $k \in \mathbb{K}$, *every monic polynomial of least degree satisfying* $f(k) = 0$ *has distinct roots in* $\bar{\mathbb{K}}$ *the algebraic closure of* $\mathbb{K}$. *Finally,* $\mathbb{K}/\Bbbk$ *is a Galois extension if it is both normal and separable.*

Definition 2.2.3 and 2.2.4 allows a fresh new look at $Br(\Bbbk)$.

Theorem 2.2.5. *With* $Br(\mathbb{K}/\Bbbk)$ *as in Definition 2.2.3, we have* $Br(\Bbbk) \simeq \bigcup_{\mathbb{K}} Br(\mathbb{K}/\Bbbk)$ *where the union is taken over all finite Galois extensions* $\mathbb{K}$ *of* $\Bbbk$.

Sketch of proof. The fact that $Br(\Bbbk) \supseteq \bigcup_{\mathbb{K}} Br(\mathbb{K}/\Bbbk)$ is clear since elements of $Br(\mathbb{K}/\Bbbk)$ are by definition in $Br(\Bbbk)$. We have the other inclusion since given an element $A \in Br(\Bbbk)$, we can find a division ring D such that $A \simeq M_n(D)$ (by Theorem 2.1.8), therefore $A \sim D$ and hence $[A] = [D]$. Since $A \in Br(\Bbbk)$, $Z(A) = \Bbbk$ hence $Z(D) = Z(M_n(D)) = \Bbbk$. From such a D, we can always find a finite Galois extension $\mathbb{K}/\Bbbk$ for which $A' \in [D]$ is such that $\mathbb{K} \otimes_{\Bbbk} A' \simeq M_n(\mathbb{K})$ hence $A' \in Br(\mathbb{K}/\Bbbk)$. For a more complete argument, see [4] (p.109-117). □

As we are about to see, we can find ways of describing the structure of $Br(\mathbb{K}/\Bbbk)$ by way of factor sets and crossed product algebras. In preparation, we need these following definitions.

Definition 2.2.6. *For any algebra A and subset $\mathbb{K} \subseteq A$, the centralizer of $\mathbb{K}$ in A is* $C_A(\mathbb{K}) := \{a \in A \mid xa = ax \text{ for all } x \in \mathbb{K}\}$

Definition 2.2.7. *Given a simple $\Bbbk$-algebra A, a subfield $\mathbb{K} \subseteq A$ containing $\Bbbk$ with $C_A(\mathbb{K}) = \mathbb{K}$, is a maximal subfield of A.*

While a more natural definition of maximality might be expected to come from inclusion of subfields, the definitions agree for division algebras, but not in general. For examples pointing out some of the differences, see p. 114 of [4].

Definition 2.2.8. *The Galois group of a field extension $\mathbb{K}/\Bbbk$ is the set of $\Bbbk$-automorphisms of $\mathbb{K}$ with composition as an operation.*

A proof that this set actually forms a group under this operation can be found in [19] p.91.

Theorem 2.2.9. *Let $\mathbb{K}/\Bbbk$ be a finite Galois extension, G be the Galois group of this extension, and A be a central simple $\Bbbk$-algebra which contains $\mathbb{K}$ as a maximal subfield. Then for any $\Bbbk$-automorphism $\sigma \in G$, Theorem 2.1.13 guarantees an $x_\sigma \in A$ such that $x_\sigma a(x_\sigma)^{-1} = \sigma(a)$ for all $a \in \mathbb{K}$. If also $x_\sigma{}' a(x_\sigma{}')^{-1} = \sigma(a)$, then $(x_\sigma(x_\sigma{}')^{-1})a(x_\sigma(x_\sigma{}')^{-1})^{-1} = x_\sigma(\sigma)^{-1}(a)(x_\sigma)^{-1} = a$ for all $a \in A$. This means that $x_\sigma(x_\sigma{}')^{-1} \in C_A(\mathbb{K})$, which is equivalent to*

$$x_\sigma = k_\sigma x_\sigma{}' \tag{2.1}$$

for some $k_\sigma \in \mathbb{K}^*$, hence, x_σ is unique up to multiplication by an element of $\mathbb{K}^*$.

Definition 2.2.10. *With composition being the operation in G, we find that $\sigma\tau(a) = \sigma(\tau(a))$ and therefore*

$$x_\sigma x_\tau = k_{\sigma,\tau} x_{\sigma\tau} \tag{2.2}$$

for some $k_{\sigma,\tau} \in \mathbb{K}^*$. For a choice of $\{x_\sigma\}_{\{\sigma\in G\}}$, we define a factor set of A relative to $\mathbb{K}$ to be $\{k_{\sigma,\tau}\}_{\{\sigma,\tau\in G\}}$.

Naturally, the choices we make in selecting $\{x_\sigma\}_{\{\sigma\in G\}}$ will have an effect on the factor set we obtain. We can nevertheless describe the relationship that will hold between corresponding elements of all factor sets of A relative to $\mathbb{K}$.

Theorem 2.2.11. *If $\{k_{\sigma,\tau}\}$ and $\{k_{\sigma,\tau}{}'\}$ are two factor sets of A relative to $\mathbb{K}$ which came from different choices of $\{x_\sigma\}_{\{\sigma\in G\}}$, then there exists $\{k_\sigma\}_{\{\sigma\in G\}}$ such that*

$$k_{\sigma,\tau}{}' = \frac{k_\sigma \sigma(k_\tau)}{k_{\sigma\tau}} k_{\sigma,\tau}. \tag{2.3}$$

for some $k_\sigma, \sigma(k_\tau), k_{\sigma\tau} \in \mathbb{K}^*,\ k_{\sigma,\tau} \in \{k_{\sigma,\tau}\},\ k_{\sigma,\tau}{}' \in \{k_{\sigma,\tau}{}'\}$.

Proof.

$$\begin{aligned}
k_{\sigma,\tau}{}' k_{\sigma\tau} x_{\sigma\tau} &= k_{\sigma,\tau}{}' x_{\sigma\tau}{}' && \text{(by equation 2.1)} \\
&= x_\sigma{}' x_\tau{}' && \text{(by equation 2.2)} \\
&= k_\sigma x_\sigma k_\tau x_\tau && \text{(by equation 2.1)} \\
&= k_\sigma \sigma(k_\tau) x_\sigma x_\tau && \text{(by Theorem 2.1.13)} \\
&= k_\sigma \sigma(k_\tau) k_{\sigma,\tau} x_{\sigma\tau} && \text{(by equation 2.2)}
\end{aligned}$$

Hence $k_{\sigma,\tau}{}' k_{\sigma\tau} = k_\sigma \sigma(k_\tau) k_{\sigma,\tau}$, which implies the result. □

It can be shown that as long as a set $\{k_{\sigma,\tau}\} \subset \mathbb{K}^*$ satisfies the following constraint,

(due to the required associativity)

$$\rho(k_{\sigma,\tau})k_{\rho,\sigma\tau} = k_{\rho,\sigma}k_{\rho\sigma,\tau} \tag{2.4}$$

then the set is a factor set relative to $\mathbb{K}$ for a central simple $\Bbbk$-algebra. For a proof of this claim, see [4] p.119.

Definition 2.2.12. *The central simple $\Bbbk$-algebra referred to above is called the crossed product algebra of $\mathbb{K}$ and G relative to the factor set $\{k_{\sigma,\tau}\}$, denoted*

$$\{\mathbb{K}, G, k_{\sigma,\tau}\} := \bigoplus_{\sigma\in G} \mathbb{K}x_\sigma$$

with multiplication defined by $x_\sigma k = \sigma(k)x_\sigma$ for all $k \in \mathbb{K}$ and $x_\sigma x_\tau = k_{\sigma\tau}x_{\sigma\tau}$.

It can also be shown that crossed product algebras of $\mathbb{K}$ and G relative to factor sets related by equation 2.3 are isomorphic, and furthermore, elements of $Br(\mathbb{K}/\Bbbk)$ are in one-to-one correspondence with equivalence classes of factor sets relative to $\mathbb{K}$ with the equivalence relation given by equation 2.3. For proofs of the claims in this last section, see [4] p.119-122.

This last correspondence is the final result needed to change perspective in our study of elements of $Br(\mathbb{K}/\Bbbk)$. We will gain new insights in the inner workings of elements of this group by combining results. The following point of view comes from homological algebra, more specifically, Galois cohomology. We will first start by defining the objects of interest. Then we will show how the second Galois cohomology group of the extension $\mathbb{K}/\Bbbk$ with coefficients in $\mathbb{K}^*$ relates to $Br(\mathbb{K}/\Bbbk)$.

Definition 2.2.13. *Given a finite Galois extension $\mathbb{K}/\Bbbk$, and $G = Gal(\mathbb{K}/\Bbbk)$, we define the n^{th} cochain group of G with coefficients in $\mathbb{K}^*$, to be $C^n(G, \mathbb{K}^*) = \{f \mid f :$*

$G^n \longrightarrow \mathbb{K}^*\}$ *where the group operation is pointwise multiplication of functions. The elements of* $C^n(G, \mathbb{K}^*)$ *are called the* n*-cochains of* G *with coefficients in* $\mathbb{K}^*$.

Definition 2.2.14. *Next, we define homomorphisms called* n*-boundary maps* $\delta_n : C^n(G, \mathbb{K}^*) \longrightarrow C^{n+1}(G, \mathbb{K}^*)$ *by*

$$\begin{aligned}
\delta_n(f)(g_1, g_2, \ldots, g_{n+1}) &= g_1\big(f(g_2, \ldots, g_{n+1})\big) \\
&\times \prod_{i=1}^{n} \big[f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, \ldots, g_{n+1})^{(-1)^i}\big] \\
&\times f(g_1, g_2, \ldots, g_n)^{(-1)^{n+1}}
\end{aligned}$$

for $n > 0$, *and,*

$$\delta_0(f)(g_1) = g_1(f) \times f^{-1}.$$

Definition 2.2.15. *We then define a cochain complex as a sequence* $(C^n)_{n\in\mathbb{Z}}$ *of abelian groups with homomorphisms* ϕ_n *taking the* n^{th} *abelian group of the sequence to the* $n+1^{st}$, *and satisfying* $\phi_n \circ \phi_{n+1} = 0$.

From the previous definitions, we can see that the cochain groups of G with coefficients in $\mathbb{K}^*$, and $C^n(G, \mathbb{K}^*)$ along with the n-boundary maps δ_n form a cochain complex.

Definition 2.2.16. *The group of* n*-cocycles, denoted* Z^n, *is defined to be* $ker(\delta_n)$ *while* $im(\delta_{n-1})$ *denoted* B^n *is defined to be the group of* n*-coboundaries. Since* $B^n \subseteq Z^n$, *and* Z^n *is abelian, we can define* $Z^n/B^n = H^n(G, \mathbb{K}^*)$, *the* n^{th} *Galois cohomology group of* G *with coefficients in* $\mathbb{K}^*$.

It is the 2^{nd} Galois cohomology group which gives us a new look into $Br(\mathbb{K}/\Bbbk)$. Elements of Z^2 are functions f for which $\delta_2(f) = 1$ (when writing $\mathbb{K}^*$ multiplicatively).

This is nothing more than satisfying equation 2.4, hence, 2-cocycles of $C^2(G, \mathbb{K}^*)$ are factor sets relative to $\mathbb{K}$. Elements of B^2 are functions in the image of $\delta_1(f)(\sigma, \tau) = f(\sigma)\sigma(f(\tau))f(\sigma\tau)^{-1}$. This implies that elements of $H^2(G, \mathbb{K}^*)$ are factor sets relative to $\mathbb{K}$ where factor sets represent the same element if they are related by equation 2.3. Since equivalence classes of factor sets relative to $\mathbb{K}$ are in one-to-one correspondence with elements of $Br(\mathbb{K}/\Bbbk)$, we can now see that elements of $H^2(G, \mathbb{K}^*)$ and $Br(\mathbb{K}/\Bbbk)$ are in one-to-one correspondence. We could further show that the correspondence is an isomorphism of groups with $H^2(G, \mathbb{K}^*) \simeq Br(\mathbb{K}/\Bbbk)$. For details regarding this relationship, see [4] p126.

2.3 The Brauer Group of an Affine Variety

While the close relationship between elements of $Br(\mathbb{K}/\Bbbk)$ and $H^2(G, \mathbb{K}^*)$ can be very useful, we will also describe the Brauer group of an affine variety. We will achieve this construction by extending our definition of the Brauer group of a field to the Brauer group of a general commutative ring. In order to do this, we need a few more definitions.

First, to extend the concept of finite dimensional central simple $\Bbbk$-algebras, we make the following definitions.

Definition 2.3.1. *An R-module M is projective if it is the direct summand of a free module.*

Definition 2.3.2. *An R-module M is faithful if its annihilator, $\{r \in R \mid rm = 0$ for all $m \in M\}$, is zero.*

Definition 2.3.3. *Given an R-algebra A, the enveloping algebra of A is defined to be $A^e := A \otimes_R A^\circ$.*

Definition 2.3.4. *An R-algebra A is called an Azumaya algebra if A is finitely generated, projective and faithful as an R-module, and if $A^e \simeq End_R(A)$.*

Note that a finite-dimensional $\Bbbk$-algebra is an Azumaya $\Bbbk$-algebra if and only if it is a finite-dimensional central simple $\Bbbk$-algebra and we can see that Definition 2.3.4 is a generalization of algebras over commutative rings which agrees with our earlier definitions. Now that Azumaya algebras are in place, we add another definition to prepare for an equivalence relation in the Brauer group of a commutative ring.

Definition 2.3.5. *Given Azumaya algebras A and B, A is equivalent to B, denoted $A \sim B$ if there exist faithfully projective R-modules P and Q such that $A \otimes_R End_R(P) \simeq B \otimes_R End_R(Q)$.*

Definition/Theorem 2.3.6. *The Brauer group of a commutative ring R, denoted $Br(R)$, is the group of equivalence classes of Azumaya R-algebras where the tensor product over R is the group operation, the equivalence class of R, denoted $[R]$ is the identity element, and the equivalence relation comes from Definition 2.3.5. Furthermore, for the equivalence class of $[A]$ of an Azumaya R-algebra A, the inverse is $[A^\circ]$.*

A proof of the claim that the set forms a group can be found in [4] p.186-192. As dicussed for the case of fields in Theorem 2.2.2, we could show that $Br(\cdot) : Br(A) \longrightarrow Br(B)$ is also functorial for the case of commutative rings (See [4] p.192).

Finally, take a $\mathbb{Q}$-variety V defined by a set of polynomials $\{f_j\}$ and the coordinate ring $R := \mathbb{Q}[x_1, x_2, \ldots, x_n]/(g_j)$, where (g_j) is the ideal generated by the generators of $Rad(\{f_j\})$. Note that Hilbert's Basis Theorem ensures the existence of a finite set of generators for $Rad(\{f_j\})$ and the solutions to $f_1 = f_2 = \cdots = f_r = 0$ with $f_i \in \{f_j\}$

are the same as those of $g_1 = g_2 = \cdots = g_s = 0$ with $g_i \in (g_j)$. We can now define the Brauer group of a variety.

Definition 2.3.7. *The Brauer group of a variety, is defined as* $Br(V) := Br(R)$ *where* R *is as defined immediately above.*

Chapter 3
The Brauer-Manin Obstruction

Using the material defined and constructed in the previous two chapters, we are now ready to describe the Brauer-Manin obstruction as it relates to a failure of the Hasse principle. We will start by giving the context within which we study the Hasse principle and then describe a sufficient condition for this principle not to hold.

If (x) is a rational point of $V(\mathbb{Q})$, then the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ forces the existence of points (x_p) of $V(\mathbb{Q}_p)$ for all primes p. The contrapositive of this last statement can be somewhat useful for instances where some $V(\mathbb{Q}_p) = \varnothing$. Since it is possible to decide if $V(\mathbb{Q}_p) = \varnothing$ for all primes p in finitely many steps (see discussion in Section 1.3), we arrive at a finite process showing that in this case, $V(\mathbb{Q}) = \varnothing$.

The converse of the initial statement is much more interesting and does not necessarily hold in general. If $V(\mathbb{Q}_p)$ being non-empty for all p implies $V(\mathbb{Q}) \neq \varnothing$, then using local information (about each $\mathbb{Q}_p$) we deduce global information (about $\mathbb{Q}$) and we say the Hasse principle holds. Hasse and Minkowski are responsible for a proof that this principle holds for quadratic forms (see [17] p.41) but as mentioned previously, many counter-examples have been known for quite some time (see [12] p.401). A first type is more trivial and can be seen from the polynomial $f(x) = (x^2 - 3)(x^2 + 3)(x^2 + 1)(x^2 + 23)$, found on page 169 of [15]. For all primes p greater than 3, at least one of 3, -3, or -1 is a square modulo p and by Hensel's

lemma, is a p-adic square. Also, -23 is a 2-adic and a 3-adic square and $\sqrt{3} \in \mathbb{R}$ hence $f(x)$ has non-trivial solutions in every p-adic field and clearly no non-trivial rational solutions and therefore, the Hasse principle fails for this example. Such examples result from a union of finitely many varieties V_i with special properties. First, for each prime p, there exists at least one i such that $V_i(\mathbb{Q}_p) \neq \varnothing$ and therefore, there is a local non-trivial solution for each p-adic field. Secondly, for each i, there exists some p such that $V_i(\mathbb{Q}_p) = \varnothing$ hence $V_i(\mathbb{Q})$ has no non-trivial solutions. Then $\cup V_i$ has a non-trivial p-adic point for all primes p and since none of the V_i have non-trivial rational points, neither does $\cup V_i$.

As we will see later in this chapter, not all obstructions are trivial, but the simple existence of such counterexamples partly motivates their classification. We will start this chapter by setting up the remainder of the necessary material to complete our discussion of the Brauer-Manin obstruction and then, we will finally see its description.

3.1 The Ring of Adèles

As the p-adic numbers were in some sense an abstraction of the rational numbers, a further abstraction gives us adèles.

Definition 3.1.1. *The ring of adèles $\mathbb{A}_\mathbb{Q}$ is $\prod_p'(\mathbb{Q}_p)$ where the restricted product indicates that all but finitely many a_p in $(a_\infty, a_2, a_3, \ldots, a_i, \ldots)$ are p-adic integers.*

Definition 3.1.2. *The adèlic space of a variety, denoted $V(\mathbb{A}_\mathbb{Q})$ consists of all adèles for which each a_p in $(a_\infty, a_2, a_3, \ldots, a_i, \ldots)$ is also in $V(\mathbb{Q}_p)$.*

The inclusion of $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ now provides the inclusion $\mathbb{Q} \hookrightarrow \mathbb{A}_\mathbb{Q}$, by sending $x \in \mathbb{Q}$ to the adèle all of whose $a_p = x$. The result is in fact an adèle since for a given rational x, only finitely many a_p are not in $\mathbb{Z}_p$. This then implies that non-trivial

rational points give rise to non-zero adelic points and $V(\mathbb{Q}) \hookrightarrow V(\mathbb{A}_{\mathbb{Q}})$. By previous discussions, (see Section 1.3) deciding the vacuity of $V(\mathbb{A}_{\mathbb{Q}})$ is a finite problem but the existence of trivial obstructions responsible for failures of the Hasse principle suggests that we might want to seek a refinement of this inclusion by finding a set X such that $V(\mathbb{Q}) \subseteq X \subseteq V(\mathbb{A}_{\mathbb{Q}})$ to explain the failure. If we verify that $V(\mathbb{A}_{\mathbb{Q}}) \neq \varnothing$ but $X = \varnothing$, then $V(\mathbb{Q}) = \varnothing$, and we have found an obstruction which causes the Hasse principle to fail.

3.2 The Brauer-Manin obstruction

The case where, as will be seen in this section, we can find $X = V(\mathbb{A}_{\mathbb{Q}})^{Br} = \varnothing$ describes a Brauer-Manin obstruction. To complete its description, we need a few final details.

For every $(x_p) \in V(\mathbb{Q}_p)$, we get a ring homomorphism from

$$R := \mathbb{Q}[x_1, x_2, \ldots, x_n]/(g_j) \longrightarrow \mathbb{Q}_p$$

as in the end of Chapter 2. We can think of this map as evaluation of the polynomials in R at (x_p). This, provides a map $Br(V) \longrightarrow Br(\mathbb{Q}_p)$ (see the discussion of the ring analogue to Theorem 2.2.2 in Section 2.3). We then have a map $V(\mathbb{Q}_p) \times Br(V) \longrightarrow Br(\mathbb{Q}_p)$, hence for a choice of $A \in Br(V)$, we get a map $\Phi_A : V(\mathbb{Q}_p) \longrightarrow Br(\mathbb{Q}_p)$ and further, a map $V(\mathbb{A}_{\mathbb{Q}}) \longrightarrow \prod_p Br(\mathbb{Q}_p)$. The image of this last map, is contained in $\bigoplus_p Br(\mathbb{Q}_p)$ (for complete details on this, see [15], p.175). We also state for future use that for a choice of $A \in Br(V)$, we similarly get a map $\Phi_A : V(\mathbb{Q}) \longrightarrow Br(\mathbb{Q})$.

We also need to use a description of $Br(\mathbb{Q}_p)$.

Theorem 3.2.1. *There exists an isomorphism* $\mathrm{inv}_p : Br(\mathbb{Q}_p) \longrightarrow \mathbb{Q}/\mathbb{Z}$.

(For details see [17] section XIII.3)

The following result comes from class field theory.

Theorem 3.2.2 (Fundamental Theorem of Global Class Field Theory)**.** *The following is a short exact sequence.*

$$0 \longrightarrow Br(\mathbb{Q}) \longrightarrow \bigoplus_p Br(\mathbb{Q}_p) \xrightarrow{\sum_p \mathrm{inv}_p} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

For a proof of Theorem 3.2.2, see p.235 of [14].

Definition 3.2.3. *Let A be an Azumaya R-algebra. We define*

$$V(\mathbb{A}_\mathbb{Q})^A = \{(x_p) \in V(\mathbb{A}_\mathbb{Q}) \mid \sum_p \mathrm{inv}_p \Phi_A(x_p) = 0\}.$$

We also define $V(\mathbb{A}_\mathbb{Q})^{Br} = \bigcap_{A \in Br(V)} V(\mathbb{A}_\mathbb{Q})^A$

We can now clearly see that by definition, $V(\mathbb{A}_\mathbb{Q})^{Br} \subseteq V(\mathbb{A}_\mathbb{Q})$. We next make use of the following theorem.

Theorem 3.2.4. $V(\mathbb{Q}) \subseteq V(\mathbb{A}_\mathbb{Q})^{Br}$.

Proof. First, we examine the following diagram.

$$\begin{array}{ccccccccc} & & V(\mathbb{Q}) & \xhookrightarrow{i} & V(\mathbb{A}_\mathbb{Q}) & & & & \\ & & \downarrow{\scriptstyle \Phi_A} & & \downarrow{\scriptstyle \Phi_A} & & & & \\ 0 & \longrightarrow & Br(\mathbb{Q}) & \xrightarrow{j} & \bigoplus_p Br(\mathbb{Q}_p) & \xrightarrow{\sum_p \mathrm{inv}_p} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

For any $A \in Br(V)$ the above diagram commutes and therefore $\Phi_A \circ i = j \circ \Phi_A$. Since the bottom row is exact by Theorem 3.2.2, $(\sum_p \mathrm{inv}_p) \circ j = 0$ hence $(\sum_p \mathrm{inv}_p) \circ$

$j \circ \Phi_A = (\sum_p \mathrm{inv}_p) \circ \Phi_A \circ i = 0$. As a result, for every $x \in V(\mathbb{Q})$ and for every $A \in Br(V)$, we find that $(\sum_p \mathrm{inv}_p) \circ \Phi_A \circ i(x) = 0$, therefore $V(\mathbb{Q}) \subseteq V(\mathbb{A}_{\mathbb{Q}})^{Br}$. $\square$

Chapter 4
Examples

In this section, we will describe two examples of varieties for which the Hasse principle fails. In the first, (an original example inspired by one found on page 169 of [2]) we make use of more basic arguments. In the second example, we use more powerful machinery to show that the failure of the Hasse principle is due to a Brauer-Manin obstruction.

4.1 Example 1

Theorem 4.1.1. *The variety V, a smooth del Pezzo surface of degree 4 defined by*

$$uv = x^2 - 17y^2, \tag{4.1}$$

$$(u + 2v)(u + 15v) = x^2 - 17z^2 \tag{4.2}$$

has non-trivial points in every p-adic field without having non-trivial rational points.

Proof. We start by noting that using software such as Macaulay 2, we can show that V is indeed smooth. Since V is smooth, we know that it is irreducible and hence not a trivial example as seen in the introduction of Chapter 3. We will continue by showing that V has non-trivial points in every p-adic field. First, we notice that in

$\mathbb{Q}_2$, integers congruent to 1 (mod 8) are squares. This follows from the fact that for any $k \in \mathbb{Z}$, $r = 0$ is a solution to $r^2 + r - 2k \equiv 0 \pmod 2$ while $2r + 1 \not\equiv 0 \pmod 2$. Hensel's lemma then forces the existence of a 2-adic solution to $r^2 + r - 2k = 0$ which is also a solution to

$$\begin{aligned} 0 &= 4r^2 + 4r - 8k \\ &= (2r+1)^2 - (8k+1). \end{aligned}$$

Letting $k = 2$, we therefore find that 17 is a 2-adic square and $(17, 0, 17, \sqrt{17}, 0)$ is a point of V in $\mathbb{Q}_2$.

Now, notice that the following three points (u, v, x, y, z) satisfy equation 4.1 and equation 4.2 :
$A = (17, 0, 0, 0, \sqrt{-17}), \qquad B = (17, 0, 17, \sqrt{17}, 0), \qquad C = (-8, 1, 5\sqrt{-1}, \sqrt{-1}, 1).$
By quadratic reciprocity, for all primes p, at least one of -1, 17, or -17 is a square in $\mathbb{Z}/p\mathbb{Z}$. For $p \neq 2$ and for $q = 1$, -17 or 17, this implies that there exists an $r \in \mathbb{Z}$ such that $r^2 - q \equiv 0 \pmod p$ and since $2r \not\equiv 0 \pmod p$, Hensel's lemma guarantees that one of -1, 17, or -17 is a p-adic square. In turn, this implies that one of A, B, or C is a point of V in $\mathbb{Q}_p$. Since $\sqrt{17} \in \mathbb{R}$, we find that $B \in V(\mathbb{R})$ and we have shown that V has non-trivial points in every p-adic field.

Next, we show that V has no non-trivial rational points. We start by assuming (u, v, x, y, z) to be a rational point of V. We know that u and v cannot be zero since then, $x^2 - 17y^2$ would be zero but $\sqrt{17}$ is irrational and the only possible point would be $(0, 0, 0, 0, 0)$. Note also that we can scale any solution by a rational factor, therefore we assume that u and v are coprime integers. Next, we notice that 17 does not divide

uv since if it did, it would divide x^2-17y^2 and also x^2, x^2-17z^2 and $(u+2v)(u+15v)$ which is a contradiction with u and v being coprime integers. Reversing the argument from equation 4.2 to equation 4.1, we find that 17 does not divide $(u+2v)(u+15v)$. Furthermore, uv is not exactly divisible by an odd power of a prime

$$p \equiv 3, 5, 6, 7, 10, 11, 12, 14 \pmod{17},$$

which are the quadratic nonresidues modulo 17. Assuming it was, and $2n+1$, $n \in \mathbb{N}$ was the largest power of a quadratic nonresidue modulo 17 dividing uv, then

$$x^2 - 17y^2 \equiv 0 \pmod{p^{2n+1}}. \tag{4.3}$$

Since p is not a square modulo 17 and $17 \equiv 1 \pmod 4$, by quadratic reciprocity 17 is also not a square modulo p, hence not a square $\pmod{p^{2n+1}}$. The only possible solution to equation 4.3 is hence $x \equiv y \equiv 0 \pmod{p^{2n+1}}$. This would mean that $x^2 - 17y^2 \equiv uv \equiv 0 \pmod{p^{2(2n+1)}}$ which contradicts the assumption that $2n+1$ is maximal. This means that u and v are products of quadratic residues and of even powers of quadratics nonresidues which necessarily implies that u and v are squares modulo 17, as well as being coprime. Again, reversing the argument from equation 4.2 to equation 4.1 we find that $(u+2v)$ and $(u+15v)$ are also squares modulo 17 but this is also a contradiction since for all squares u and v modulo 17, an exhaustive check of all cases shows that $(u+2v)$ and $(u+15v)$ cannot be simultaneously squares modulo 17. This shows that V has no non-trivial rational points and completes the proof of the theorem. □

4.2 Example 2

The next example is due to Peyre and appears on page 171 of [15] but before we describe it, we need a few more results.

Definition 4.2.1. *The Hilbert symbol* $(a,b)_p$ *for* $a,b \in \mathbb{Q}_p^*$ *is* 1 *if* $z^2 - ax^2 - by^2 = 0$ *has a non-trivial solution in* $\mathbb{Q}_p^3$*, and is* -1 *otherwise.*

To compute the Hilbert symbol, the following definition will be useful.

Definition 4.2.2. *Let* n *be an odd integer. Then*

$$e(n) = \begin{cases} 0 & \text{if } n \equiv 1 \pmod 4 \\ 1 & \text{if } n \equiv 3 \pmod 4 \end{cases}$$

The next proposition contains properties of the Hilbert symbol.

Proposition 4.2.3.

$$\begin{aligned} (a,-1)_p &= (-1)^{\mathrm{ord}_p(a)e(p)} \text{ where } p \text{ is a prime, } p \neq 2 \\ (a,-1)_2 &= (-1)^{e(u)} \text{ where } u \text{ is such that } a = 2^{\mathrm{ord}_2 a} \cdot u, 2 \nmid u \\ (a,-1)_\infty &= \frac{a}{|a|_\infty} \\ (a,c^2)_p &= 1 \\ (a,bc)_p &= (a,b)_p(a,c)_p \end{aligned}$$

A proof of the proposition can be found on pages $11-14$ of [11]. With this result in mind, we are ready to describe the next example.

Theorem 4.2.4. *Let V be the smooth variety corresponding to $y^2+z^2 = (3-x^2)(x^2-2)$. Then the Hasse principle fails for V and there is a Brauer-Manin obstruction for V so $V(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$ and $V(\mathbb{A}_{\mathbb{Q}})^{Br} = \emptyset$.*

Seeking a proof for Theorem 4.2.4, we need the following lemmas.

Lemma 4.2.5. *For all primes p, there exists $x \neq \pm\sqrt{2}, \pm\sqrt{3}, \in \mathbb{Q}_p$ such that, $((3-x^2)(x^2-2), -1)_p = 1$.*

Proof. The proof of Lemma 4.2.5 will follow in 4 cases.

Case 1 : $p \equiv 1 \pmod 4$

First, notice that for all $p \equiv 1 \pmod 4$, $((3-x^2)(x^2-2), -1)_p = 1$ since $e(p) = 0$.

Case 2 : $p \equiv 3 \pmod 4$

For all $p \equiv 3 \pmod 4$, any x with $\mathrm{ord}_p\, x < 0$ will be sufficient since then $x = \frac{a}{p^k}$, $(p \nmid a)$, and then $\mathrm{ord}_p(3-x^2) = -2k = \mathrm{ord}_p(x^2-2)$ hence $((3-x^2), -1)_p = (-1)^{\mathrm{ord}_p(3-x^2)} = (-1)^{\mathrm{ord}_p(x^2-2)} = ((x^2-2), -1)_p$ and $((3-x^2), -1)_p \cdot ((x^2-2), -1)_p = ((3-x^2)(x^2-2), -1)_p = 1$.

Case 3 : $p = 2$

For $p = 2$, setting $x = 0$ gives $(3, -1)_2 = (-1)^{e(3)} = -1 = (-1)^{e(-1)} = (-2, -1)_2$ hence $((3-x^2)(x^2-2), -1)_p = ((3-0^2), -1)_2 \cdot ((0^2-2), -1)_2 = 1$.

Case 4 : $p = \infty$

For $p = \infty$, we get $\frac{3-x^2}{|3-x^2|_\infty} = \frac{x^2-2}{|x^2-2|_\infty}$ as long as $(3-x^2)(x^2-2) > 0$, or for $x \in \{(-\sqrt{3}, -\sqrt{2}) \cup (\sqrt{2}, \sqrt{3})\}$. We thus find that there exists $x \in \mathbb{Q}_\infty$ with $((3-x^2)(x^2-2), -1)_\infty = 1$ and have therefore shown that there exists $x \in \mathbb{Q}_p$ such that $((3-x^2)(x^2-2), -1)_p = 1$ for all primes p. □

Lemma 4.2.6. *For every solution (x, y, z) to $y^2 + z^2 = (3-x^2)(x^2-2)$ and for all primes $p \neq 2$, $(3-x^2, -1)_p = 1$ while $(3-x^2, -1)_2 = -1$.*

Proof. The proof of Lemma 4.2.6 will similarly proceed in 4 cases.

Case 1 : $p \equiv 1 \pmod 4$

For all $p \equiv 1 \pmod 4$, $(3 - x^2, -1)_p = 1$ by the same argument as in Lemma 4.2.5.

Case 2 : $p \equiv 3 \pmod 4$

First, notice that for every p-adic solution to $y^2 + z^2 = (3 - x^2)(x^2 - 2)$, we have $((3 - x^2)(x^2 - 2), -1)_p = 1$, hence we get $(3 - x^2, -1)_p = (x^2 - 2, -1)_p$ for all p. For all $p \equiv 3 \pmod 4$, all x for which $(3-x^2, -1)_p = (x^2-2, -1)_p$ force $(3-x^2, -1)_p = 1$ since as before, if $\mathrm{ord}_p\, x < 0$, the relation is automatic but even if $\mathrm{ord}_p\, x \geq 0$, the fact that $(3 - x^2) + (x^2 - 2) = 1$ implies that $\min(\mathrm{ord}_p(3 - x^2), \mathrm{ord}_p(x^2 - 2)) \leq \mathrm{ord}_p(3 - x^2 + x^2 - 2) = \mathrm{ord}_p(1) = 0$. We can then say that either $\mathrm{ord}_p(3 - x^2) \leq 0$ or $\mathrm{ord}_p(x^2 - 2) \leq 0$. But $\mathrm{ord}_p(3 - x^2) \geq \min(\mathrm{ord}_p(3), \mathrm{ord}_p(x^2)) = 0$ and $\mathrm{ord}_p(x^2 - 2) \geq \min(\mathrm{ord}_p(x^2), \mathrm{ord}_p(-2)) = 0$, therefore $\min(\mathrm{ord}_p(3 - x^2), \mathrm{ord}_p(x^2 - 2)) = 0$ and we must have either $\mathrm{ord}_p(3 - x^2) = 0$ or $\mathrm{ord}_p(x^2 - 2) = 0$, but since $(3 - x^2, -1)_p = (x^2 - 2, -1)_p$ we must have $(3 - x^2, -1)_p = 1$.

Case 3 : $p = 2$

If $p = 2$, then $(3 - x^2, -1)_2 = -1$. To see why, we remember that $(3 - x^2, -1)_p$ must equal $(x^2-2, -1)_p$ and we notice that $\mathrm{ord}_2(x) \neq 0$ since if it was, we would get $x \in \mathbb{Z}_2$, $x \equiv 1, 3, 5, 7 \pmod 8$ and $x^2 \equiv 1 \pmod 8$. Then $3 - x^2 \equiv 2 \pmod 8$ and $\frac{3-x^2}{2} \equiv 1 \pmod 4$ hence $1 = (\frac{3-x^2}{2}, -1)_2 = (\frac{1}{2}, -1)_2 \cdot (3-x^2, -1)_2 = (-1)^{e(1)}(3-x^2, -1)_2 = (3-x^2, -1)_2$. Similarly, since $x^2 - 2 \equiv 7 \pmod 8 \equiv 3 \pmod 4$, then $(3 - x^2, -1)_2 = -1$. This is a contradiction since $(3 - x^2, -1)_p = (x^2 - 2, -1)_p$ therefore $\mathrm{ord}_2(x) \neq 0$. If $\mathrm{ord}_2(x) > 0$, then $3 - x^2 \equiv 3 \pmod 4$ and $(3 - x^2, -1)_2 = -1$ while if $\mathrm{ord}_2(x) < 0$, then $\frac{3}{x^2} - \frac{x^2}{x^2} \equiv 3 \pmod 4$ and $-1 = (\frac{3}{x^2} - 1, -1)_2 = (x^2(\frac{3}{x^2} - 1), -1)_2 = (3-x^2, -1)_2$ and $(3 - x^2, -1)_2 = -1$ and therefore $(3 - x^2, -1)_2 = -1$ for every solution (x, y, z) to $y^2 + z^2 = (3 - x^2)(x^2 - 2)$.

Case 4 : $p = \infty$

Finally, if $(3-x^2,-1)_\infty = (x^2-2,-1)_\infty$, then $\frac{3-x^2}{|3-x^2|_\infty} = \frac{x^2-2}{|x^2-2|_\infty}$ and $x \in (-\sqrt{3},\sqrt{3})$ which gives us $(3-x^2,-1)_\infty = 1$.
This shows that for all x such that (x,y,z) is a solution to $y^2+z^2 = (3-x^2)(x^2-2)$, and for all primes $p \neq 2$ we have $(3-x^2,-1)_p = 1$ while $(3-x^2,-1)_2 = -1$ and concludes the proof of Lemma 4.2.6 □

The next definition describes a generalization of the real quaternions.

Definition 4.2.7. *Let*

$$\left(\frac{\alpha,\beta}{R}\right) := \frac{R<i,j,k>}{(i^2-\alpha, j^2-\beta, ij+ji, ij-k)}.$$

This algebra is referred to as a quaternion R-algebra and forms an Azumaya R-algebra with dimension 4 over R. We can find a proof of this claim on page 49 of [16]. A particular example which will be revisited soon is $\left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right)$ which, by previous comments, is a central simple $\mathbb{Q}_p$-algebra. The next two lemmas will provide the final details to complete the proof of Theorem 4.2.4.

Lemma 4.2.8. $(\alpha,\beta)_p = 1$ *if and only if* $\left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right)$ *is not a division algebra.*

Proof. To begin, $(\alpha,\beta)_p = 1$ if and only if $\alpha x^2+\beta y^2-z^2 = 0$ has a non-trivial solution in $\mathbb{Q}_p^3$ but there exists such a solution to $\alpha x^2+\beta y^2-z^2=0$ if and only if $\alpha x^2+\beta y^2-z^2-\alpha\beta w^2 = 0$ has a non-trivial solution in $\mathbb{Q}_p^4$. The last forward implication is clear but its converse eminates from the fact that if $\alpha x^2+\beta y^2-z^2-\alpha\beta w^2=0$ has a non-trivial solution in $\mathbb{Q}_p^4$, then $\alpha = \frac{z^2-\beta y^2}{x^2-\beta w^2} = \left(\frac{xz-\beta yw}{x^2-\beta x^2}\right)^2 - \beta\left(\frac{wz-yx}{x^2-\beta x^2}\right)^2$ and therefore $\alpha x^2+\beta y^2-z^2=0$ has a non-trivial solution in $\mathbb{Q}_p^3$. We finally want to show that $\alpha x^2+\beta y^2-z^2-\alpha\beta w^2=0$ has a non-trivial solution in $\mathbb{Q}_p^4$ if and only if $\left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right)$ is not a division algebra. With this intent, we will show that for any

$0 \neq a \in \left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right)$, a is invertible if and only if $a\overline{a} \neq 0$ where if $a = z - ix - jy - kw$, then $\overline{a} = z + ix + jy + kw$. If a^{-1} exists, then $\overline{a} \neq 0$ and $a^{-1}a\overline{a} = \overline{a} \neq 0$ therefore $a\overline{a} \neq 0$. Since $a\overline{a} = z^2 - \alpha x^2 - \beta y^2 + \alpha\beta w^2$, we know that $\alpha x^2 + \beta y^2 - z^2 - \alpha\beta w^2 \neq 0$. Conversely, for any $0 \neq a \in \left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right)$ with $a\overline{a} \neq 0$, $a\overline{a} \in \mathbb{Q}_p$. Therefore $(a\overline{a})^{-1}$ exists, but $\big((a\overline{a})^{-1}\overline{a}\big)a = (a\overline{a})^{-1}a\overline{a} = 1$ and $a\big((a\overline{a})^{-1}\overline{a}\big) = a\big((\overline{a}a)^{-1}\overline{a}\big) = a(a^{-1}\overline{a}^{-1})\overline{a} = 1$ hence $a^{-1} = (a\overline{a})^{-1}\overline{a}$ exists and finally,$(\alpha,\beta)_p = 1$ if and only if $\left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right)$ is not a division algebra.

□

The next lemma describes possible elements in $Br(\mathbb{Q}_p)$.

Lemma 4.2.9. $\left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right) \otimes_{\mathbb{Q}_p} \left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right) \cong M_4(\mathbb{Q}_p)$.

Proof. Using Theorem 2.1.8, Definition/Theorem 2.2.1 and the fact that quaternion algebras are isomorphic to their opposite algebra, $\left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right)$ and $\left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right)^{\circ}$ are inverses in $Br(\mathbb{Q}_p)$ and therefore $\left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right) \otimes_{\mathbb{Q}_p} \left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right) \cong M_4(\mathbb{Q}_p)$. □

We are now ready to prove Theorem 4.2.4.

Proof of Theorem 4.2.4. To prove that the Hasse principle fails, we need to show that V has non-zero adelic points, while having no rational points. To begin, note that Lemma 4.2.5 shows that there exists $x \neq \pm\sqrt{2}, \pm\sqrt{3} \in \mathbb{Q}_p$ such that, $((3 - x^2)(x^2 - 2), -1)_p = 1$ for all p. For such values of x, we see that $Z^2 + Y^2 = (3 - x^2)(x^2 - 2)X^2$ has a non-trivial solution over $\mathbb{Q}_p^3$ for all p, which is equivalent to $z^2 + y^2 = (3 - x^2)(x^2 - 2)$ having a solution over $\mathbb{Q}_p^2$. Therefore $((3 - x^2)(x^2 - 2), -1)_p = 1$ for all p is ultimately equivalent to V having an non-trivial adelic point and $V(\mathbb{A}_{\mathbb{Q}}) \neq \varnothing$.
By Lemmas 4.2.6 and 4.2.8, we conclude that every adelic point $(x_p) \in V(\mathbb{A}_{\mathbb{Q}})$ maps,

(via Φ_A in Figure 3.2 with $A = \left(\frac{3-x^2,-1}{R}\right)$) to

$$(M_2(\mathbb{Q}_\infty), D, M_2(\mathbb{Q}_3), M_2(\mathbb{Q}_5), \ldots) \in \bigoplus Br(\mathbb{Q}_p)$$

where D is a division algebra since $\left(\frac{3-x^2,-1}{\mathbb{Q}_p}\right)$ is only a division algebra for $p = 2$. By Lemma 4.2.9 and with $\sum_p \text{inv}_p$ from Theorem 3.2.2, we see that

$$(M_2(\mathbb{Q}_\infty), D, M_2(\mathbb{Q}_3), M_2(\mathbb{Q}_5), \ldots) \in \bigoplus Br(\mathbb{Q}_p)$$

maps to $(0 + \frac{1}{2} + 0 + 0 + ...) \in \mathbb{Q}/\mathbb{Z}$ which is nonzero. We therefore find that $V(\mathbb{A}_\mathbb{Q})^A = \varnothing$ and so $\cap_{A \in Br(V)} V(\mathbb{A}_\mathbb{Q})^A = \varnothing$. By Theorem 3.2.4, $V(\mathbb{Q}) \subseteq V(\mathbb{A}_\mathbb{Q})^{Br}$ and therefore there can be no rational solutions and this failure of the Hasse principle is fully explained by the Brauer-Manin obstruction. □

Bibliography

[1] George Bachman. *Introduction to p-adic Numbers and Valuation Theory*. Academic Press, 1964.

[2] Bryan J. Birch and Sir Peter Swinnerton-Dyer. The Hasse Problem for Rational Surfaces. *Journal für die Reine und Angewandte Mathematik*, 274:164–174, 1975.

[3] John William Scott Cassels. Diophantine Equations with Special Reference to Elliptic Curves. *Journal of London Mathematical Society*, 41:193–291, 1966.

[4] Benson Farb and R. Keith Dennis. *Noncommutative Algebra*. Springer-Verlag, 1993.

[5] Benji Fisher. A Note on Hensel's Lemma in Several Variables. *Proceedings of the American Mathematical Society*, 125:3185–3189, 1997.

[6] Fernando Q. Gouvea. *p-adic Numbers: An Introduction*. Springer, 1997.

[7] Marvin J. Greenberg. *Lectures on Forms in Many Variables*. W.A.Benjamin, Inc., 1969.

[8] Israel Nathan Herstein. *Noncommutative Rings*. The Mathematical Association of America, 1971.

[9] Neil Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer-Verlag, 1977.

[10] Serge Lang and Andre Weil. Number of Points of Varieties in Finite Fields. *American Journal of Mathematics*, 76:819–827, 1954.

[11] Boris Lerner. The Brauer-Manin Obstruction to the Hasse Principle. web.maths.unsw.edu.au/˜danielch/thesis/boris.pdf (accessed : Aug, 2008), 2007.

[12] Yuri Ivanovich Manin. Le Groupe de Brauer-Grothendieck en Géométrie Diophantienne. *Actes du Congrès International des Mathématiciens (Nice, 1970)*, 1:401–411, 1971.

[13] Yuri V. Matiyasevich. *Hilbert's Tenth Problem*. MIT Press, 1993.

[14] J.S. Milne. Class Field Theory. www.jmilne.org/math version 4.00(Accessed : Sept. 2008), 1997.

[15] Emmanuel Peyre. *Obstructions au Principe de Hasse et à l'Approximation Faible*, pages 165–193. Société Mathématique de France, 2005.

[16] David J. Saltman. *Lectures on Division Algebras*. American Mathematical Society, 1999.

[17] Jean-Pierre Serre. *A Course in Arithmetic*. Springer-Verlag, 1973.

[18] Alexei N. Skorobogatov. Beyond the Manin Obstruction. *Inventiones Mathematicae*, 135:399–424, 1999.

[19] Sir Ian Stewart. *Galois Theory*. Chapman & Hall / CRC, third edition, 2004.

[20] Alfred Tarski. *A Decision Method for Elementary Algebra and Geometry*. RAND Corporation, 1948.