UNSW
AUSTRALIA

CLASSIFICATION OF QUADRATIC FORMS WITH CLIFFORD ALGEBRAS

Dorothy Cheung

Supervisor: Associate Professor Daniel Chan

School of Mathematics and Statistics
The University of New South Wales

October 2015

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

Plagiarism statement

I declare that this thesis is my own work, except where acknowledged, and has not been submitted for academic credit elsewhere.

I acknowledge that the assessor of this thesis may, for the purpose of assessing it:

- Reproduce it and provide a copy to another member of the University; and/or,
- Communicate a copy of it to a plagiarism checking service (which may then retain a copy of it on its database for the purpose of future plagiarism checking).

I certify that I have read and understood the University Rules in respect of Student Academic Misconduct, and am aware of any potential plagiarism penalties which may apply.

By signing this declaration I am agreeing to the statements and conditions above.

Signed: _____ Date: _____

Acknowledgements

First and foremost, my greatest gratitude goes to my supervisor, Associate Professor Daniel Chan, who has provided much needed guidance throughout the year. He was always more than willing to answer my questions, patiently explaining things on the whiteboard and in general gave me invaluable advice on how to best tackle my Honours years.

Also, I want to give thanks to Professor Jie Du, who was my supervisor for vacation research project. He offered great advice and is always passionate about mathematics. I also want to thank Associate Professor Catherine Greenhill for her insightful feedbacks during the Honours talks.

Thanks also goes to all my fellow Honours students, who are always friendly and happy to help each other. They make the Honours room a great place to learn mathematics. Without them, the Honours year would not be as fun and interesting. Special thanks to Tracy and Ramanan for their help with Latex which saved me heaps of work. I also want to give thanks to Fadi, who has been a great friend throughout my undergraduate study in mathematics.

Last but not least, I want to thank my family for their support throughout the year.

Dorothy Cheung, 30 Octorber 2015.

Abstract

In this thesis, we look at classification of quadratic forms over $\mathbb{Q}_p$ and $\mathbb{Q}$ with invariants. Clifford algebras are useful here. One of the invariant of quadratic forms is the Hasse invariant. The definition and properties of the Hasse invariant are based on quaternion algebras and Clifford algebras. This invariant along with two other invariants, dimension and discriminant, can be used to completely classify quadratic forms over $\mathbb{Q}_p$. Using Hasse-Minkowski Theorem, we can extend the classification of quadratic form over local field $\mathbb{Q}_p$ to the global field $\mathbb{Q}$. This gives a complete set of invariants to classify quadratic forms on $\mathbb{Q}$ with dimension, discriminant, signature and Hasse invariant.

Contents

Chapter 1

Introduction

Quadratic forms appear in many areas of mathematics. We can reduce the classification of certain objects to the classification of quadratic forms. For example, quaternion algebra from Clifford algebra and Killing form in Lie theory. We also use quadratic forms to classify conic and quadric surface.

When considering the problem of classifying quadratic forms, we ask the question: given two quadratic forms Q and Q' over a field, are the two equivalent, that is, can we obtain one from the other with a linear transformation? Such question is easy to answer when we are working over a field such as $\mathbb{R}$ and $\mathbb{C}$. However, as we move away from these fields, it is a lot harder to see. In this thesis, we will look at classifying quadratic forms over $\mathbb{Q}_p$ and $\mathbb{Q}$ using invariants.

An invariant is an object associated to quadratic forms which does not change if a form is replaced by an equivalent form. Typically, invariants are used to distinguish two quadratic forms which are not equivalent, by showing the objects are different. However we are able to obtain a set of invariants which completely classify the quadratic forms over $\mathbb{Q}_p$. Two quadratic forms Q and Q' are equivalent over $\mathbb{Q}_p$ if and only if they have same dimension, discriminant and Hasse invariant. We will also extend from $\mathbb{Q}_p$ to $\mathbb{Q}$ using the Hasse-Minkowski theorem, which will give us a set of invariants that completely classify the quadratic forms over $\mathbb{Q}$. In fact, two quadratics forms with same dimension, discriminant, signature and Hasse invariant are equivalent over $\mathbb{Q}$.

One particularly invariants we will focus on is the Hasse invariant (also called Hasse-Witt invariant). To define and understand this invariant, we need to know about Clifford algebras and the Brauer group, as well as the Hilbert symbol. This is because Hasse-Witt invariant is defined as a product of Hilbert symbol. Hilbert symbol is defined by quaternion algebras (which are Clifford algebras of dimension 2), and takes value in the 2-torsion Brauer group.

Although we will focus on the problem of classifying quadratic forms, we will also see some of the interesting connections between quadratic forms and Clifford algebras.

1.1 Outline

In Chapter 2, we go through the background and basic knowledge of quadratic forms. The main theorems in this chapter are Witt's cancellation theorem and Diagonlisation theorem, which allow us to write equivalent quadratic form in a certain way. Two basic invariants, dimension and discriminant, of quadratic forms is introduced here.

To get more invariants of quadratic form, we will look into the central simple algebras and Brauer group. In Chapter 3, we will introduce central simple algebras and Brauer group, which is formed by equivalence class of central simple algebra. The Brauer group will give us insight on the Hasse invariant. In this chapter, we will mainly give exposition without proof.

In Chapter 4, I first introduce quaternion algebra and generalise it to Clifford algebra using quadratic forms. There is interesting relationships between quadratic form and the Clifford algebra it generates. First, the isomorphism class of $C(Q)$ depends on the quadratic forms. For two equivalent quadratic forms $Q \cong Q'$, the two Clifford algebra $C(Q), C(Q')$ are isomorphic. This implies $C(Q)$ is actually an invariant of Q. Other invariant of quadratic forms, in particular dimension and discriminant, affect the structure of the associated Clifford algebras.

In Chapter 5, I introduce the p-adic field $\mathbb{Q}_p$, which we are working over. I will define the Hilbert symbol with quaternion algebra. We will look at properties and calculation of Hilbert symbol. As Hasse-Witt invariant is defined using Hilbert symbol, these properties and calculation will be helpful when we look at Hasse invariant. We will see that a well-known theorem in number theory, the Quadratic Reciprocity, is equivalent to the Hilbert Reciprocity with Hilbert symbol. I will give an alternate definition of the Hasse-Witt invariant using Clifford algebra.

In Chapter 6, we see classification of quadratic form over $\mathbb{Q}_p$. Two quadratic forms Q and Q' are equivalent over $\mathbb{Q}_p$ if and only if they have the same dimension, discriminant and Hasse-Witt invariant. We can extend this to classification over $\mathbb{Q}$ using Hasse-Minkowski theorem which states that a quadratic form Q is isotropic over $\mathbb{Q}$ if and only if it is isotropic over $\mathbb{Q}_v$ for all v. This allows us to classify quadratic forms Q over $\mathbb{Q}$ using their dimension, discriminant, signature and Hasse invariant.

While Clifford algebras are used in classification of quadratic forms, they also appear in many areas of mathematics such as Lie groups and Lie algebras, Dirac operators, Spin manifold, and other areas. In Chapter 7, we see an interesting application of Clifford algebras on vector field over a sphere. On a sphere S^{n-1}, we show that there are at least $\rho(n)$ linearly independent tangent vector fields where $\rho(n)$ is the Radon-Hurwirz number.

1.2 Assumed knowledge

For this thesis, I assumed the readers have basic knowledge gained in the courses required for a pure mathematics degree at UNSW. In particular, the relevant courses would be Higher Linear Algebra, Higher Algebra, Modules and Representation, and Number Theory courses. Basic knowledge about groups, rings, modules, vector spaces, tensor product, and some finite field and elementary number theory are assumed. There are also some side remarks which assumed readers have knowledge of functors.

1.3 Notation

Unless stated otherwise, I will follow the notation below throughout this thesis.

- k^* is the group $k - 0$ where k is a field.
- k^*/k^{*2} is the square class of k.
- $\mathbb{Z}/p\mathbb{Z}$ will denote the integers ring.
- $\mathbb{Z}_p$ will denote the p-adic integers.
- $\mathbb{U}_p := \mathbb{Z}_p^*$ will denote p-adic units.
- $\mathbb{Q}_p$ will denote the p-adic field where p is prime.
- $\mathbb{Q}_v$ will denote p-adic field but also include $\mathbb{Q}_\infty := \mathbb{R}$.
- Q_v will denote quadratic form Q over $\mathbb{Q}_v$.
- $A \cong B$ will denote A is isomorphic to B.
- $A \backsim B$ will denote A is equivalent to B under a pre-specified equivalence relation.
- $M_n(k)$ will denote $n \times n$ matrix with entries in k.
- A^{opp} is the opposite algebra of A.
- $A \oplus B$ will denote the direct sum of A and B.
- $A \otimes B$ will denote the tensor product of A and B.
- $A \perp B$ will denote the orthogonal sum of A and B.
- $V^\perp$ will denote orthogonal complement of a quadratic space V.
- $Z(A)$ will denote the center of algebra A.
- $C(V, Q), C(V), C(Q)$ will denote Clifford algebra of quadratic space (V, Q).
- (a, b) will denote a quaternion algebra.
- $(a, b)_v$ will denote Hilbert symbol over $\mathbb{Q}_v$, though I may also use (a, b) to denote the Hilbert symbol when it is clear in the context.

Chapter 2

Quadratic forms

In this chapter, I will introduce some basic background knowledge on quadratic forms which we will need in later chapters. The notable theorem in this chapter is the Witt-cancellation theorem, which allows us to decompose quadratic space into orthogonal subspaces. This will be used in later chapter for inductive proofs. Another important theorem is the Diagonlisation theorem, which enables us to write quadratic form in the form $a_1X_1^2 + ... + a_nX_n^2$. where $a_i \in k$. We will also introduce two quadratic invariants, the dimension and the discriminant.

This chapter is based on various sources on quadratic form [19], [9], [7] and [12]. These sources mostly deal with quadratic forms over modules, but instead we will mainly focus on quadratic forms on vector spaces.

2.1 Basic definition

Throughout this section, we will let k be a field and V be any finite dimensional k-vector space. We will first give a summary of basic definitions and notations for quadratic forms over k.

Definition 2.1.1. *A* bilinear form *is a function $\beta : V \times V \to k$ which satisfies the following*

1. $\beta(u + v, w) = \beta(u, w) + \beta(v, w)$
2. $\beta(u, v + w) = \beta(u, v) + \beta(u, w)$
3. $\beta(\lambda u, v) = \beta(u, \lambda v) = \lambda\beta(u, v)$

for all $u, v, w \in V$ and $\lambda \in k$.

Definition 2.1.2. *A* quadratic forms *on V is a function $Q : V \to k$ such that*

1. *$Q(ax) = a^2Q(x)$ for all $a \in k$ and $x \in V$*
2. *The function $\beta_Q(x, y) = Q(x + y) - Q(x) - Q(y)$ is bilinear*

The pair (V, Q) is called a quadratic space *and β_Q is called the* associated bilinear form *of Q.*

From the definition, it is clear that $\beta_Q(x, x) = 2Q(x)$. Hence Q is determined by β_Q, and vice versa, in field of characteristic not 2. We will denote associated bilinear form as β instead of β_Q here after where it is clear.

Example 2.1.3. *An example of a bilinear form is the dot product in Euclidean space. Let $x = (x_1, x_2, x_3)^T, y = (y_1, y_2, y_3)^T$*

$$\langle x, y\rangle = x_1y_1 + x_2y_2 + x_3y_3$$

The norm squared function in Euclidean space is a quadratic function.

$$\|x\|^2 = \langle x, x\rangle = x_1^2 + x_2^2 + x_3^2$$

Definition 2.1.4. *A bilinear form β is* non-degenerate *if $\beta(x, y) = 0$ for all $y \in V$ implies $x = 0$. A quadratic form Q is* non-degenerate *if the associated bilinear form β_Q is non-degenerate.*

Definition 2.1.5. *A quadratic form Q on a vector space V* represent *an element $a \in k$ if there exists an $x \in V$ such that $Q(x) = a$.*

Definition 2.1.6. *Q is called* isotropic *if Q represents 0 non-trivially i.e. there exists $x \neq 0$ such that $Q(x) = 0$. Otherwise Q is called* anisotropic.

Example 2.1.7. *A typical example of isotropic quadratic form is $X_1^2 - X_2^2$, which is called the hyperbolic plane.*

Definition 2.1.8. *Q is called* universal *if it represents all non-zero elements of k.*

We will now introduce orthogonal sums of quadratic forms. This enables us to construct new quadratic forms using existing quadratic forms of lower dimension.

Definition 2.1.9. *We say that $x \in V$ is* orthogonal *to $y \in V$ with respect to Q if $\beta_Q(x, y) = 0$.*

Definition 2.1.10. *If $(V, Q), (V', Q')$ are quadratic spaces, we define the* orthogonal sum *$Q \perp Q'$ on $V \oplus V'$ and associated bilinear form $\beta \perp \beta'$, by the condition*

$$(\beta \perp \beta')(x + x', y + y') = \beta(x, y) + \beta'(x', y')$$

$$(Q \perp Q')(x + x') = Q(x) + Q'(x')$$

for all $x, y \in V$ and $x', y' \in V'$.

The following theorem relates representation of elements in the field and isotropy of quadratic forms. Here, we construct a new quadratic form using orthogonal sum.

Proposition 2.1.11. *Let Q be a non-degenerate quadratic form and let $u \in k$, then u is represented by Q if and only if $Q \perp \langle -u \rangle$ is isotropic.*

Proof. Let $Q = a_1X_1^2 + ... + a_nX_n^2$. If Q represents u, then for some $(x_1, ..., x_n)$, we have $u = a_1x_1^2 + ... + a_nx_n^2$. Then clearly $a_1x_n^2 + ... + a_nx_n^2 + (-u)1^2 = 0$, so the form $Q \perp \langle -u \rangle = a_1X_1^2 + ... + a_nX_n^2 - uX_{n+1}^2$ is isotropic.

Conversely, let $(x_1, ..., x_{n+1})$ be an isotropic vector for $Q \perp \langle -u \rangle$. So $a_1x_1^2 + ... + a_nx_n^2 - ux_{n+1}^2 = 0$. Suppose $x_{n+1} \neq 0$, then $u = a_1(\frac{x_1}{x_{n+1}}) + ... + a_n(\frac{x_n}{x_{n+1}})$. Hence Q represents u. Now suppose $x_{n+1} = 0$, then $x = (x_1, ..., x_n)$ is an isotropic vector for Q, then $Q(x) = 0$. As Q is non-degenerate, then there exist y such that $\beta(x, y) = 1$. If we let $z = y - Q(y)x$, then

$$\begin{aligned} Q(z) &= Q(y - Q(y)x) \\ &= Q(y) + Q(y)Q(x) - \beta_Q(y, Q(y)x) \\ &= Q(y) - Q(y) \\ &= 0. \end{aligned}$$

Also note that $\beta_Q(x,z) = 1$ as

$$\begin{aligned}\beta_Q(x,z) &= \beta_Q(x, y - Q(y)x) \\ &= \beta_Q(x,y) - \beta_Q(x, Q(y)x) \\ &= 1 - 2Q(x)Q(y) \\ &= 1.\end{aligned}$$

Then we can represent u with Q since

$$\begin{aligned}Q(x+uz) &= Q(x) + u^2 Q(z) + \beta_Q(x, x+uz) \\ &= 0 + 0 + u\beta_Q(x,z) \\ &= u.\end{aligned}$$

This is an amended proof from Lam's book [12] Corollary 3.5 p.11 where the case $x_{n+1} = 0$ is treated differently. □

2.2 Equivalence of quadratic forms

Definition 2.2.1. *If $(V,Q),(V',Q')$ are quadratic spaces, then a linear map $f : V \to V'$ is called a* morphism *of quadratic spaces if $Q(f(x)) = Q'(x)$ for all $x \in V$. We say the two quadratic spaces $(V,Q),(V',Q')$ are* equivalent *if there is a isomorphism (a bijective morphism) $f : (V,Q) \to (V',Q')$. We denote this as $(V,Q) \cong (V',Q')$. If $V = V'$, we write $Q \cong Q'$ and say that the two quadratic forms are equivalent.*

We can also say that two quadratic spaces are equivalent if there is an isometry η mapping from V to V'.

Example 2.2.2. *The two quadratic forms with dimension 2*

$$Q = X_1X_2 \text{ and } Q' = Y_1^2 - Y_2^2$$

are equivalent. Consider the linear map f which map $X_1 \to Y_1 + Y_2$ and $X_2 \to Y_1 - Y_2$, then

$$Q(f(X_1X_2)) = Q(Y_1+Y_2, Y_1-Y_2) = (Y_1+Y_2)(Y_1-Y_2) = Y_1^2 - Y_2^2 = Q'$$

Hence it is clear that $Q \cong Q'$.

Witt's cancellation theorem is an important tool which enable us to perform induction on quadratic forms in later proofs.

Definition 2.2.3. *An* orthogonal splitting *of a quadratic space (V,Q), denoted $V = E_1 \perp ... \perp E_r$, is a direct sum decomposition of $V = E_1 \oplus ... \oplus E_r$, such that $\beta(x,y) = 0$ for $x \in E_i$ and $y \in E_j$, where $i \neq j, 1 \leq i,j \leq r$.*

Definition 2.2.4. *Let (V,Q) be a quadratic space and $U \subseteq V$ be a subspace. We define the* orthogonal complement *of U to be $U^\perp = \{x \in V | \beta(x,y) = 0$ for all $y \in U\}$. Also note that $V = U \perp U^\perp$.*

Theorem 2.2.5. *(Witt's cancellation theorem) Let $Q \cong Q'$ be non-degenerate quadratic forms on vector space V over field k with $char(k) \neq 2$. Let U_1 and U_2 be non-degenerate subspaces which are equivalent, then $U_1^\perp$ and $U_2^\perp$ are equivalent.*

Proof. Suppose $U_1 \cong U_2$, and the restriction of Q to U_1 and U_2 are non-degenerate. We shall prove that $U_1^\perp \cong U_2^\perp$ by induction on dimension of U_i.

Firstly, suppose $U_i = ku_i = \langle u_i \rangle$ and $Q(u_i) \neq 0$ as we assume quadratic form is non-degenerate. We may assume that $Q(u_1) = Q(u_2)$. We have

$$\begin{aligned} Q(u_1 \pm u_2) &= Q(u_1) + Q(u_2) \pm \beta(u_1, u_2) \\ &= 2Q(u_1) \pm \beta(u_1, u_2) \end{aligned}$$

Hence $Q(u_1+u_2)+Q(u_1-u_2) = 4Q(u_1) \neq 0$. This implies $Q(u_1+u_2)$ and $Q(u_1-u_2)$ cannot both be 0. Suppose first that $Q(u_1+u_2) \neq 0$. Consider the symmetry $S_{u_1+u_2}$. A symmetry is given by

$$S_u : x \to x - \frac{\beta(x,u)}{Q(u)}u$$

Using bilinearity of β and given that $Q(u_1) = Q(u_2)$,

$$\begin{aligned} \beta(u_1+u_2, u_1-u_2) &= \beta(u_1,u_1) - \beta(u_1,u_2) + \beta(u_2,u_1) - \beta(u_2,u_2) \\ &= Q(u_1) - Q(u_2) \\ &= 0 \end{aligned}$$

It follows that $(u_1-u_2) \perp (u_1+u_2)$, hence $S_{u_1-u_1}(u_1+u_2) = (u_1+u_2)$. On the other hand, $S_{u_1+u_2}(u_1+u_2) = -(u_1+u_2)$. We can write $u_1 = \frac{1}{2}(u_1+u_2) + \frac{1}{2}(u_1-u_2)$, then

$$\begin{aligned} S_{u_1+u_2}(u_1) &= S_{u_1+u_2}\left(\frac{1}{2}(u_1+u_2) + \frac{1}{2}(u_1-u_2)\right) \\ &= \frac{1}{2}(u_1+u_2) - \frac{1}{2}(u_1-u_2) \\ &= u_2 \end{aligned}$$

Also since $\beta(\langle u_1 \rangle, \langle u_1 \rangle^\perp) = 0$. This implies $S_{u_1+u_2}(\langle u_1 \rangle^\perp) = S_{u_1+u_2}(\langle u_1 \rangle)^\perp = \langle u_2 \rangle^\perp$. Hence $U_1^\perp \cong U_2^\perp$ for $\dim U_i = 1$.

Assume the result is true for subspaces of dimension equal to $\leq n$, and consider a non-degenerate subspace U_1 of dimensions $n+1$. Choosing a non-isotropic vector u_1 in U_1, we write $U_1 = \langle u_1 \rangle \perp W_1$. Apply symmetry and we obtain $U_2 = \langle u_2 \rangle \perp W_2$ where $\langle u_1 \rangle \cong \langle u_2 \rangle$ and $W_1 \cong W_2$. We can then represent $V = \langle u_1 \rangle \perp W_1 \perp U_1^\perp = \langle u_2 \rangle \perp W_2 \perp U_2^\perp$. Using the one-dimensional case on $\langle u_1 \rangle$ and $\langle u_2 \rangle$, there exists an isometry $\eta : W_1 \perp U_1^\perp \to W_2 \perp U_2^\perp$. Then we have $W_2 \perp U_2^\perp = \eta(W_1) \perp \eta(U_1^\perp)$. Since $W_2 \cong W_1 \cong \eta(W_1)$. Hence induction hypothesis applies to subspaces W_2 and $\eta(W_1)$ of $W_2 \perp U_2^\perp$ implies that $U_2^\perp \cong \eta(U_1^\perp) \cong U_1^\perp$. This completes the proof by induction. □

Theorem 2.2.6. *(Diagonlisation theorem) If k is a field of characteristic not 2 and V is a finite dimensional vector space over k, we can present any quadratic form on V with*

$$Q \cong a_1X_1^2 + a_2X_2^2 + ... + a_nX_n^2$$

where $n = \dim V$ and $a_i \in k$ for all i.

Proof. We will proceed by induction on dimension n. The case $n = 0$ is trivial. For $n = 1$, there exists $a_1 \in V$ with $Q(a_1) \neq 0$ since we cannot have Q identically zero. Then $W_1 = \langle a_1 \rangle$ is non-degenerate. Now we have $V = W_1 \perp W_1^{\perp} = \langle a_1 \rangle \perp W_1^{\perp}$. The proof is complete by induction as we obtain

$$V = \langle a_1 \rangle \perp \langle a_2 \rangle \perp .... \perp \langle a_n \rangle := \langle a_1, ..., a_n \rangle$$

and thus

$$Q \cong a_1 X_1^2 + a_2 X_2^2 + ... + a_n X_n^2.$$

□

Example 2.2.7. *Consider the fact that* $\mathbb{C}^*/\mathbb{C}^{*2} = 1$ *and* $\mathbb{R}^*/\mathbb{R}^{*2} = \{1, -1\}$. *Then any nonzero quadratic space over* $\mathbb{C}$ *is equivalent to one of the form*

$$X_1^2 + ... + X_n^2$$

and any non-zero quadratic space over $\mathbb{R}$ *is equivalent to one of the form*

$$X_1^2 + ... + X_r^2 - X_{r+1}^2 - .... - X_n^2.$$

Definition 2.2.8. *The* discriminant *of a quadratic form* $Q = a_1 X_1^2 + ... + a_n X_n^2$, *is the squares class of product of coefficients* $a_1 a_2 ... a_n$ *in* k^*/k^{*2}, *we will denote this as* d.

Given an orthogonal base of V, we can also say that the *discriminant* of a quadratic form Q is the squares class of $\prod_{i=1}^{n} Q(v_i)$ in k^*/k^{*2}.

Chapter 3

Central simple algebras and Brauer group

We have seen two invariants of quadratic form, the dimension and discriminant, in the previous chapter. I will soon introduce the Hasse-Witt invariant. To obtain and understand the Hasse-Witt invariant, we first need to know about central simple algebras and the Brauer group. The equivalence classes of central simple algebras form the Brauer group, which is helpful in understanding Hilbert symbol and Hasse-Witt invariant in later chapters. We will see that the two elements of Hilbert symbol can be identified with element from the 2-torsion Brauer group. I will mainly provide exposition without proof in this chapter. The aim of this chapter is to give basic background on central simple algebras and Brauer group.

The main references for this chapter are Gille [4] and Jacobson [9].

3.1 Central simple algebras

The main point of emphasis this section is that, as a consequence of Wedderburn's theorem, we may characterise central simple algebras as finite dimensional algebras which become isomorphic to some full matrix ring over a finite extension of the base field.

Definition 3.1.1. *A k-algebra A is called* simple *if it has no (two sided) ideals other than 0 and A.*

Definition 3.1.2. *A k-algebra A is called* central *if its center equals k, that is $Z(A) = k$.*

Definition 3.1.3. *A finite dimensional k-algebra is a* central simple algebra *if it is simple and central.*

Example 3.1.4. *Hamilton's quaternion algebra is a central simple $\mathbb{R}$-algebra.*

$$\mathbb{H} = \frac{\mathbb{R}\langle 1, i, j, ij\rangle}{\langle i^2 = -1, j^2 = -1, ij = -ji\rangle}$$

We can see that it is clearly central as $Z(\mathbb{H}) = \mathbb{R}$ and it is simple since it is a division ring.

The main theorem here is Wedderburn theorem, which allows us to classify central simple algebra with division algebras.

Theorem 3.1.5. *(Wedderburn) Let A be a finite dimensional simple algebra over field k. Then there exists an integer $n \geq 1$ and a division algebra D subset of k so that A is isomorphic to the matrix ring $M_n(D)$. Moreover the division algebra D is uniquely determined up to isomorphism.*

Proof. A proof can be found in [4] Theorem 2.1.3 p.30. □

Remark 3.1.6. *The Wedderburn structure theorem for simple algebras reduces the classification of these algebras to division algebras.*

3.2 Brauer group

The Brauer group is an abelian group of equivalence classes of central simple algebras with tensor product operation. The determination of $Br(k)$ for a field k is equivalent to a complete classification of the finite dimensional central division algebras over k. We will see the connection between the Brauer group and Hilbert symbol in later chapters. We will also look at the Brauer group of $\mathbb{R}$ and $\mathbb{Q}_p$. The main references for this section are [4] and [9].

Proposition 3.2.1. *If A and B are central simple algebras over k, then $A \otimes_k B$ is a central simple algebra over k.*

Proof. See [4] Lemma 2.4.4 p.43 for a proof. □

Proposition 3.2.2. *If A is a central simple algebra over k, then $A \otimes A^{opp} \cong End_k(A) \cong M_n(k)$ where $n = [A : k]$*

Proof. See [4] p.45 for a proof. □

Definition 3.2.3. *Let A and B be two central simple k-algebras. We say that A and B are* Brauer equivalent *if $M_n(A) \cong M_m(B)$,or equivalently $M_n(k) \otimes A \cong M_m(k) \otimes B$, for some $n, m \in \mathbb{N}$. We denote $A \backsim B$.*

Example 3.2.4. *We can show that $\mathbb{H} \otimes \mathbb{H} \cong M_4(\mathbb{R})$ with the $\mathbb{R}$-linear map*

$$\begin{aligned} \Phi :& \mathbb{H} \times \mathbb{H} \to Hom_{\mathbb{R}}(\mathbb{H}, \mathbb{H}) \cong M_4(\mathbb{R}) \\ & (q_1, q_2) \to \Phi_{q_1,q_2}(x) = q_1 x \bar{q_2}. \end{aligned}$$

By universal property of tensor product, this extends to an algebra homomorphism of $\mathbb{H} \otimes \mathbb{H}$ and $M_2(\mathbb{R})$. Note that $\mathbb{H}$ is central simple. By Proposition 3.2.1, $\mathbb{H} \otimes \mathbb{H}$ is also central simple from Example 3.1.4. Clearly, we have kernel of this map to be 0 and hence it is injective. Also since they have the same dimension 16, this map is bijective and hence we have an isomorphism for $\mathbb{H} \otimes \mathbb{H}$ and $M_2(\mathbb{R})$. Thus $\mathbb{H} \otimes \mathbb{H}$ is Brauer equivalent to $\mathbb{R}$, and we write $\mathbb{H} \otimes \mathbb{H} \backsim \mathbb{R}$.

We can now define a group structure of the equivalence classes of central simple algebra with tensor product, the Brauer group. We denote the equivalence class of central simple algebra A with $[A]$.

Theorem 3.2.5. *A* Brauer group *of k, denote $Br(k)$, is the set of equivalence classes of central simple algebra over k. It has group operation $[A][B] = [A \otimes_k B]$.*

1. *It is well defined since $M_n(k) \otimes_k M_m(k) \cong M_{mn}(k)$*
2. *It is associative and commutative*
3. *$[k] = [M_n(k)]$ is the identity*
4. *$[A^{opp}]$ is the inverse of $[A]$*

Proof. It is clear from above two propositions. For a full proof, see [9] p.227. □

Theorem 3.2.6. *Each Brauer equivalence class contains (up to isomorphism) a unique division algebra.*

Proof. See [9] p.227. □

Remark 3.2.7. *It follows from Wedderburn's theorem and Theorem 3.2.6 that if A and B are two Brauer equivalent k-algebras of the same dimension, then $A \cong B$.*

If k is an algebraically closed field, then $Br(k)$ is trivial, i.e. $Br(k) \cong 1$, since the only finite dimensional division algebra over k is itself. For example $Br(\mathbb{C}) \cong 1$. If $k = \mathbb{R}$, a classical theorem of Frobenius asserts that

$$Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}.$$

The Frobenius theorem classifies all the $\mathbb{R}$-algebra. We will use this theorem to classify all $\mathbb{R}$-algebra in the Brauer group.

Theorem 3.2.8. *(Frobenius) The only finite dimensional division algebras over the field $\mathbb{R}$ of real numbers are the field $\mathbb{R}$ itself, the field $\mathbb{C}$ of complex numbers and the Hamilton's quaternion algebra $\mathbb{H}$.*

Proof. A proof can be found in [15]. □

Theorem 3.2.9. *The Brauer group $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ is a cyclic group of order two.*

Proof. If A is a division algebra over $\mathbb{R}$, then A is isomorphic to either $\mathbb{R}, \mathbb{C}, \mathbb{H}$ by Frobenius Theorem (Theorem 3.2.8). Since $\mathbb{C}$ is not central and $\mathbb{R}$ is an algebra over itself corresponds to the trivial element of $Br(\mathbb{R})$, the only Brauer division algebra over $\mathbb{R}$ which might correspond to a non-trivial element of Brauer group is $\mathbb{H}$. As $\mathbb{H}$ is a division algebra, it cannot lie in the same Brauer group equivalence class as $\mathbb{R}$ by Theorem 3.2.6. Therefore the equivalence class of $\mathbb{H}$ is non-trivial. Since $\mathbb{R}$ and $\mathbb{H}$ are the only central simple division $\mathbb{R}$-algebras, there are only two equivalence classes of central simple $\mathbb{R}$-algebras. Thus, $Br(\mathbb{R})$ has precisely two elements, which means that $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. We can also see from Example 3.2.4 that $\mathbb{H}$ has order two. □

Theorem 3.2.10. *The Brauer group $Br(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$.*

Proof. A proof can be found in [9] Jacobson's Basic Algebra II (Theorem 9.22 p.610). □

Chapter 4

Clifford algebra

Clifford algebras are defined using quadratic forms. We will pay particular attention to quaternion algebras, which are important Clifford algebras of dimension four. We will first introduce quaternion algebras and generalise it to Clifford algebras using quadratic forms. The quaternion algebras are also highly connected to quadratic forms. We can check if a quaternion algebra is split by checking to see the corresponding quadratic form is isotropic. We can construct quaternion algebras with quadratic forms and, for the converse, we can also generate a quadratic form with trace and norm of the quaternion algebra.

Given two equivalent quadratic forms $Q \cong Q'$, the Clifford algebras $C(V,Q) \cong C(V,Q')$ are isomorphic. Clifford algebra is an invariant of quadratic form. We will see that the structure of these Clifford algebra hugely depend on the properties of the associated quadratic form, in particular on the invariants dimension and discriminant.

The relevant sources for this chapter are [9] and [4].

4.1 Quaternion algebra

In this section, we will introduce quaternion algebras and splitting of quaternion algebras. We see that the equivalence classes of quaternion algebras have connection with the ternary quadratic forms. To check if a quaternion algebra is split, we can do this by checking that the corresponding quadratic norm form is isotropic.

Definition 4.1.1. *For any two elements $a, b \in k^*$, define the quaternion algebra (a,b) as the 4-dimensional k-algebra with basis $1, i, j, ij$, multiplication being determined by*

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

Example 4.1.2. *Hamilton's quaternion is a quaternion algebra.*

$$(-1,-1)_{\mathbb{R}} = \frac{\mathbb{R}\langle i^2 = -1, j^2 = -1\rangle}{\langle i^2 = -1, j^2 = -1, ij = -ji\rangle}$$

Remark 4.1.3. *Note that the isomorphism class of the algebra (a,b) depends only on the classes of a and b in the square class k^*/k^{*2}. The substitution*

$$i \to ui, \quad j \to vj$$

induces an isomorphism

$$(a,b) \cong (u^2a, v^2b).$$

We can also see that $(a,b) \cong (b,a)$ with mapping $i \to abj, u \to abi$.

Definition 4.1.4. *For an element $q = x + yi + zj + wij$ of a quaternion algebra (a, b), its* conjugate *is*

$$\bar{q} = x - yi - zj - wij$$

The trace *and the* norm *of q is*

$$T(q) = 2x \qquad N(q) = q\bar{q} = x^2 - ay^2 - bz^2 + abw^2.$$

Note that norm is a multiplicative function and it is also a quadratic form.

Definition 4.1.5. *A quaternion algebra over k is* split *if it is isomorphic to $M_2(k)$ as a k-algebra.*

Example 4.1.6. *The quaternion algebra $(1, b)$ is split since $(1, b) \cong M_2(k)$ given by the map*

$$i \to I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad j \to J = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

which satisfy the required relation $I^2 = Id\ , j^2 = b\ Id\ , IJ = -JI$.

Proposition 4.1.7. *Hamilton's quaternion $\mathbb{H} = (-1, -1)_{\mathbb{R}}$ is a division algebra.*

Proof. To show that it is a division algebra, we want to show that every nonzero element in $\mathbb{H}$ has a multiplicative inverse. Note that every element $q = x + yi + zj + wij$ in $\mathbb{H}$ has conjugate

$$\bar{q} = x - yi - zj - wij$$

and norm $N(q) = q\bar{q}$

$$N(q) = x^2 + y^2 + z^2 + w^2 \in \mathbb{R}$$

So if $q \neq 0$, then the inverse of q is $\frac{\bar{q}}{N(q)}$. □

As $\mathbb{H}$ is a division algebra, it cannot be isomorphic to $M_2(k)$. This implies that $\mathbb{H}$ is not split.

In general, we can determine whether a quaternion algebra (a, b) is division algebra or not by looking at the norm form using the following lemma.

Lemma 4.1.8. *An element q of a quaternion algebra (a, b) is invertible if and only if it has non-zero norm. Hence (a, b) is a division algebra if and only if the norm $N : (a, b) \to k$ does not vanish outside 0.*

Proof. This is clear as the inverse for any quaternion q is $\frac{\bar{q}}{N(q)}$ where $N(q) \neq 0$. □

The following proposition gives equivalent conditions of splitting of a quaternion algebra. We will also need this proposition later on when we encounter the Hilbert symbol.

Proposition 4.1.9. *For a quaternion algebra (a, b) the following are equivalent:*

1. *The quaternion algebra is split*
2. *The algebra (a, b) is not a division algebra*
3. *The norm map $N : (a, b) \to k$ has non-trivial zero*
4. *The element b is a norm form from the field extension $k(\sqrt{a})/k$*

Proof. (1) $\Rightarrow$ (2) This is obvious since $M_2(k)$ has zero divisor.

(1) $\Leftarrow$ (2) By Wedderburn's structure theorem, the simple algebra (a, b) is isomorphic to some matrix algebra $M_n(D)$ where D is a division algebra. Since (a, b) itself is not a division algebra, we need $n \geq 2$, but $\dim_k(a, b) = 4$. Hence we conclude that $n = 2$ and $D = k$. We have $(a, b) \cong M_2(k)$ and it is split.

(2) $\Rightarrow$ (3) This is proven in previous Lemma 4.1.8 above.

(3) $\Rightarrow$ (4) We assume a is not a square in k, otherwise it is clear as $k(\sqrt{a}) = k$. Consider nonzero quaternion $q = x + yi + zj + wij$ with norm 0. Then

$$N(q) = x^2 - ay^2 - bz^2 + abw^2 = 0$$

which means that $(z^2 - aw^2)b = x^2 - ay^2$. Since a is not a square, then $x^2 - ay^2 \neq 0$. It follows that $(z^2 - aw^2) \neq 0$. Now, denote N' as the field norm of $k(\sqrt{a})/k$, we have

$$b = \frac{x^2 - ay^2}{z^2 - aw^2} = N'(x + \sqrt{a}y)N'(z + \sqrt{a}w)^{-1} = N'\left(\frac{x + \sqrt{a}y}{z + \sqrt{a}w}\right).$$

(4) $\Rightarrow$ (2) Assume a is not a square in k. Otherwise we have $a^2 = c$, and $(a - c)(a + c) = 0$. So the element $a - c, a + c$ in quaternion algebra (a, b) has zero divisor, hence (a, b) is not a division algebra. If b is a norm from $k(\sqrt{a})/k$, then

$$b = r^2 - as^2$$

for some $r, s \in k$. Now

$$(r + si + j)(r - si - j) = r^2 - as^2 - b = 0$$

So the element $r + si + j, r - si - j$ in quaternion algebra (a, b) have a zero divisor, this implies (a, b) is not a division algebra.

This is an amended proof from [4] Proposition 1.1.7 p.14. □

Quaternion algebras can be defined with quadratic forms, which we will see in next section on Clifford algebra. We can also obtain a quadratic form from a quaternion algebra. Consider the quaternion algebra (a, b) with element $q = x + yi + zj + wij$ and recall *trace* and *norm* as

$$T(q) = 2x \quad N(q) = x^2 - ay^2 - bz^2 + abw^2,$$

then $q^2 - T(q)q + N(q) = 0$. Let $(a, b)_0$ denote the subspace of elements of trace 0. This has base i, j, ij and has the quadratic norm form

$$N(q) = -ay^2 - bz^2 - abw^2$$

We have seen from previous theorem that (a, b) is split if it contains an nonzero nilpotent element, that is, there exists q_0 such that $q_0^2 = 0$. We can also see this is the case if and only if $T(q_0) = 0$ and $N(q_0) = 0$. This implies that (a, b) is split if and only if the quadratic form on $(a, b)_0$ is isotropic, so $-ay^2 - bz^2 + abw^2 = 0$ has nontrivial solution.

Now, we form a connection between quaternion algebra and quadratic form. We can see that $(a,b)_0$ is a set of elements $q \in (a,b)$ such that $q \notin k$ but $q^2 \in k$. There is an isomorphism of (a,b) onto (c,d) which maps $(a,b)_0$ onto $(c,d)_0$.

Remark 4.1.10. *It follows that if* $(a,b) \cong (c,d)$*, then the quadratic forms*

$$-ay^2 - bz^2 + abw^2 \text{ and } -cz^2 - dy^2 + cdw^2$$

are equivalent.

The converse also holds as the equivalent ternary quadratic forms will generate isomorphic quaternion algebras as we will see in the next Chapter on Clifford algebra. To see the connection, we also have the following theorem.

Theorem 4.1.11. *There is a functorial bijection between the set of isomorphism classes of quaternion algebras over* k *and the set of non-degenerate ternary quadratic spaces over* k*.*

Proof. For proof, see [19] Corollary 4.4.7, p.50. □

In this thesis, we mainly focus on the problem of classifying quadratic forms and will not go further to classification of quaternion algebras. However, the above theorem implies that the problem of classifying quaternion algebras depends on the quadratic forms over the field. There are a lot of interesting connections between quadratic forms and quaternion algebras, and also with Clifford algebras.

4.2 Clifford algebra

To generalise quaternion algebras to higher dimension, William Clifford (1845-1879) developed a way to build algebras from quadratic forms in 1876. This is the Clifford algebras. The properties and the behaviour of quadratic forms is connected to how the corresponding Clifford algebra will behave.

In this section, the main reference will be Jacobson's Basic Algebra II [9]. I will introduce Clifford algebras and give basic background. Since Clifford algebras are tensor product of vector space, we will also look at the basis element and dimension of Clifford algebra. We will also see the relationship between Clifford algebras and quaternion algebras. Clifford algebras are useful in classifying quadratic forms as we see in later chapters when discuss Hasse-Witt invariant.

Definition 4.2.1. *Let* V *be a vector space over field* k *and let* Q *be a quadratic form on* V*. Let*

$$T(V) = k \oplus V \oplus V^{\otimes^2} \oplus V^{\otimes^3} \oplus ...$$

be the tensor algebra defined by V*. Then we define the* Clifford algebra *of the quadratic form* Q *to be the algebra*

$$C(V,Q) = T(V)/I_Q$$

where I_Q *is the ideal of* $T(V)$ *generated by* $\{x \otimes x - Q(x).1 | x \in V\}$*.*

If $a \in T(V)$*, we can write* $\bar{a} = a + I_Q \in C(V,Q)$ *and we have the map* $i : x \to \bar{x}$ *of* V *into* $C(V,Q)$*.*

Remark 4.2.2. *Since $(x+y) \in V$, the ideal I_Q contains $(x+y)\otimes(x+y)-Q(x+y)$ and note that*

$$\begin{aligned}&(x+y)\otimes(x+y)-Q(x+y)\\&=x\otimes x+y\otimes y+(x\otimes y+y\otimes x)-Q(x)-Q(y)-\beta(x,y).\end{aligned}$$

As $x\otimes x-Q(x), y\otimes y-Q(y)\in I_Q$ we see that

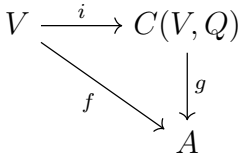
$$x\otimes y+y\otimes x-\beta(x,y).1\in I_Q \quad x,y\in V$$

So we have relation $\bar{x}\bar{y}+\bar{y}\bar{x}=\beta(x,y).1$ as well as $\bar{x}^2=Q(x).1$ in $C(V,Q)$.

Theorem 4.2.3. *(Universal property of Clifford algebra) Suppose $a\in T(V)$, we write $\bar{a}=a+I_Q\in C(V,Q)$ and we have a map $i: x\to\bar{x}$ of V into $C(V,Q)$. If f is a linear map of V into an algebra A such that*

$$f(x)^2=Q(x) \quad x\in V$$

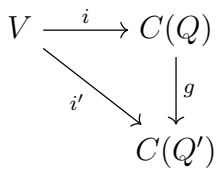
then there exists a unique algebra homomorphism $g: C(V,Q)\to A$ such that the diagram below commutes



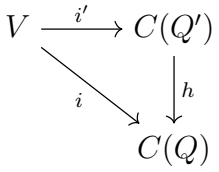
Proof. To see the universal property of Clifford algebra, we can use the universal property of tensor algebra. From this, we know that any linear map f of V into an algebra has a unique extension to an algebra homomorphism f' of $T(V)$ into A. Now for the given f, the kernel of f' contains every element $x\otimes x-Q(x).1, x\in V$, since $f'(x\otimes x-Q(x).1)=f(x)^2-Q(x).1=0$. Hence $I_Q\subseteq\ker f'$ and so we have the induced homomorphism $g:\bar{a}+I_Q\to f'(a)$. In particular, $g(\bar{x})=f'(x)=f(x)$ which gives the commutativity of the diagram. The uniqueness of g is clear since $\bar{x}$ generates $C(V,Q)$. □

Theorem 4.2.4. *The Clifford algebra $C(V,Q)$ exists for each quadratic form Q. For two equivalent quadratic for $Q\cong Q'$, the corresponding Clifford algebra are isomorphic, that is $C(Q)\cong C(Q')$.*

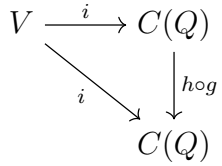
Proof. This follows from universal property of Clifford algebra. Let $i: V\to C(Q)$ and $i': V\to C(Q')$, where $C(Q), C(Q')$ are two Clifford algebras of V. Since $C(Q)$ is a Clifford algebra, there is a unique homomorphism $g: C(Q)\to C(Q')$ such that the following diagram commutes.



Also, since $C(Q')$ is a Clifford algebra, there is a unique homomorphism $h : C(Q') \to C(Q)$ such that the diagram below commutes.



Since $i = h \circ i'$ and $i' = g \circ i$, then we have $i = h \circ g \circ i$ and $i' = g \circ h \circ i'$ by uniqueness. Then, we have $h \circ g : C(Q) \to C(Q)$ which makes the following diagram commute



but so does the identity $1_C : C(Q) \to C(Q)$. Hence $h \circ g = 1_C$ by uniqueness. Similarly, we also have $g \circ h = 1_C$. Thus $g : C(Q) \to C(Q')$ is an isomorphism. We have $C(Q) \cong C(Q')$. □

In other words, the formation of the Clifford algebras is functorial in the quadratic spaces.

Now, we look at an example of a well-known Clifford algebra, the exterior algebra.

Example 4.2.5. *(Exterior algebra) The Clifford algebra with $Q = 0$, zero quadratic form, is the exterior algebra.*

$$C(V, 0) = \frac{k \oplus V \oplus V^{\otimes^2} \oplus V^{\otimes^3} \oplus ...}{\{x \otimes x | x \in V\}} = \Lambda(V)$$

We can define

$$x \wedge y = x \otimes y + \{x \otimes x | x \in V\}$$

and we can see that for all $x, y \in V$ with $x \neq y$, we have following relations of exterior algebras

$$x \wedge x = 0 \qquad x \wedge y = -y \wedge x.$$

4.3 Bases and dimension

Lemma 4.3.1. *(Poincare-Birkoff-Witt) If $\{u_1, u_2, ..., u_n\}$ is the basis for the vector space V over k, then the set*

$$\{u_{i_1} u_{i_2} ... u_{i_k} | 1 \leq i_1 \leq i_2 \leq ... \leq i_k \leq n\}$$

where $0 \leq k \leq n$, forms a basis for $C(V, Q)$ together with $\{1\}$.

Proof. Since $T(V)$ is generated by V and u_i span V, it is clear that u_i generated $T(V)$. This implies that every element of $T(V)$ is a linear combination of 1

and monomials in the u_i of positive degree. Now, we call 1 and the monomials $u_{i_1}u_{i_2}....u_{i_r}$ with $i_1 < i_2... < i_r$ and $1 \leq r \leq n$, *standard*. Let S be the set of these standard monomials.

We want to show by induction on i and the degree of $u \in S$ that $u_i u$ is congruent module the ideal I_Q to a linear combination of standards monomials of degree $\leq \deg u + 1$. This is clear if $\deg u = 0$. Now suppose $u = u_{i_1}u_{i_2}...u_{i_r}$ where $r \geq 1$.

If $i = 1$, the result follows if $i_1 > 1$ since $u_1 u$ is already standard. Suppose $i_1 = 1$, then

$$u_1 u = u_1^2 u_{i_2}....u_{i_r} \equiv Q(u_1)u_{i_2}....u_{i_r} \bmod I_Q$$

Now let $i > 1$. If $i \leq i_1$, it follows similarly as with case $i = 1$. Hence assume $i > i_1$, then using relation

$$x \otimes y + y \otimes x - \beta(x, y)1 \in I_Q \quad x, y \in V$$

we have

$$u_i u_{i_1} = -u_{i_1}u_i + \beta(u_i, u_{i_1}) \bmod I_Q$$

$$u_i u_{i_1} u_{i_2}....u_{i_r} = -u_{i_1}u_i u_{i_2}....u_{i_r} + \beta(u_i, u_{i_1})u_{i_2}....u_{i_r} \bmod I_Q$$

Now, by induction on the degree, $u_i u_{i_2}...u_{i_r}$ is congruent module I_Q to a linear combination of standard monomials of degree $\leq r$. Then induction on the i implies that $u_{i_1}u_i u_{i_2}...u_{i_r}$ and hence $u_i u_{i_1} u_{i_2}...u_{i_r}$ is congruent to linear combination of standards monomials of degree $\leq r + 1$ modulo I_Q.

This implies that if C' is the subspace of $C(V, Q)$ spanned by elements $\bar{1}, \bar{u}_{i_1}\bar{u_{i_2}}...\bar{u}_{i_r}$ where $i_1 < i_2 < .... < i_r$, then $\bar{u}_i C' \subseteq C'$. This implies $C'C' \subseteq C'$ so C' is a subalgebra of $C(V, Q)$. Since C' contains $\bar{V} = \{\bar{x} | x \in V\}$ and $\bar{V}$ generates $C(V, Q)$, then we have $C' = C(V, Q)$.

□

This lemma implies that $\dim C(V, Q) \leq 2^n$, where $n = \dim V$, as this is the number of standard monomials. These standard monomials are in fact distinct and this gives the dimension of $C(V, Q) = 2^n$. Note that we can put monomials in standard order due to the relation $u_i u_j = -u_j u_i$. We will prove the dimensionality properly later in Theorem 4.4.6.

Example 4.3.2. *Consider exterior algebra (Clifford algebra with $Q = 0$) with $V = kx \oplus ky \oplus kz$, so V is generated by x, y, z. We have $\dim V = 3$. The basis for $C(V, Q)$ are*

$$\{1, x, y, z, x \wedge y, x \wedge z, y \wedge z, x \wedge y \wedge z\}$$

and dimension is $2^3 = 8$.

4.4 Structure theorems

We will now look at the structure of these Clifford algebras. Since Clifford algebras are constructed using quadratic forms, invariant of quadratic form also affect the structure of these Clifford algebras.

We will also introduce the discriminant of the associated bilinear form which is two times the discriminant of quadratics form. We will use discriminant of bilinear form in the following theorems, as notation will be clearer.

Definition 4.4.1. *The* discriminant *of the associated bilinear form β with an orthogonal base $(v_1, ..., v_n)$ of V is $\delta = \prod_{i=1}^{n} \beta(v_i, v_i) = 2\prod_{i=1}^{n} Q(v_i)$.*

We can see that a change of base replace δ with δa^2 where $a \neq 0$, which differ by a square in k.

We can now look at the structure of Clifford algebra, starting from lower dimension.

Lemma 4.4.2. *If Q is non-degenerate and $n = 1$, then $\dim C(V, Q) = 2$. Now suppose $V = ku$. If $Q(u)$ is not a square in k, then $C(V, Q)$ is a field. If $Q(u)$ is a square in k, then it is a direct sum of two copies of k.*

Proof. Let $A = k[t]/(t^2 - Q(u))$. A has base $\{1, \bar{t}\}$ where $\bar{t} = t + (t^2 - Q(u))$. Then $\bar{t}^2 = Q(u)$, which implies that the linear map $f : V \to A$ such that $f(u) = \bar{t}$ satisfies $f(x)^2 = Q(x)$. Hence we have a homomorphism of $C(V, Q)$ into A, by universal property of Clifford algebra, such that $\bar{u} \to \bar{t}$. This is surjective. Since $\dim A = 2$ and $\dim C(V, Q) \leq 2$. We have $\dim C(V, Q) = 2$, which implies we now have an isomorphism. If $Q(u)$ is not a square in k, then $t^2 - Q(u)$ is irreducible in $k[t]$ and $C(V, Q)$ is a field. If $Q(u)$ is a square and let $Q(u) = b^2$ and $b \in k$, then $e' = \bar{u} - b$ satisfies

$$\begin{aligned} e'^2 &= \bar{u}^2 - 2b\bar{u} + b^2 \\ &= 2Q(u) - 2b\bar{u} \\ &= -2b(\bar{u} - b\bar{t}) \\ &= -2be' \end{aligned}$$

Hence we can see that $e = -(2b)^{-1}e'$ is a idempotent in $C(V, Q)$, which is not equal to 0 or 1. It follows that we have $C(V, Q) = ke \oplus k(1 - e)$ which is a direct sum of two copies of k. □

Quaternion algebras are an important Clifford algebras. The connection is further highlighted in the following lemma. Every Clifford algebra $C(V, Q)$ with $\dim V = 2$ with non-degenerate quadratic form is a quaternion algebra. We will also see that quaternion algebras are central simple.

Lemma 4.4.3. *If Q is non-degenerate and $\dim V = 2$, then $C(V, Q)$ is a quaternion algebra.*

Proof. Let $n = \dim V$ and suppose $n = 2$. Choose an orthogonal base (u, v) for V. Then $Q(u)Q(v) \neq 0$. Let C' be the Clifford algebra of ku relative to the restriction Q' of Q to ku. Then C' has a base $(1, \bar{u})$ where $\bar{u}^2 = Q(u)$. Consider the matrices

$$u' = \begin{pmatrix} \bar{u} & 0 \\ 0 & -\bar{u} \end{pmatrix} \qquad v' = \begin{pmatrix} 0 & Q(v) \\ 1 & 0 \end{pmatrix}$$

we have

$$u'v' = \begin{pmatrix} 0 & \bar{u} \\ -Q(v)\bar{u} & 0 \end{pmatrix} \qquad v'u' = \begin{pmatrix} 0 & -\bar{u} \\ Q(v)\bar{u} & 0 \end{pmatrix}$$

so $u'v' + v'u' = 0$. It is clear that $u'^2 = \bar{u}^2 = Q(u)$ and $v'^2 = Q(v)$. It follows that $A = k1 + ku' + kv' + ku'v'$ is a subalgebra of $M_2(C')$. We can see from the matrices

that $1, u', v', v'u'$ are independent and hence $\dim A = 4$. The relation on u' and v' implies that there exists a linear map $f : V \to A$ such that $u \to u'$ and $v' \to v'$ and satisfies $f(x)^2 = Q(x)$ for $x \in V$. By universal property of Clifford algebras, this means we have a homomorphism $g : C(V, Q) \to A$ such that $\bar{u} = u'$ and $\bar{v} = v'$. We see that g is surjective. Since $\dim C(V, Q) \leq 4$ and $\dim A = 4$, then we have g is an isomorphism and hence $\dim C(V, Q) = 4$.

We now have an isomorphism of $C(V, Q)$ with algebra A which generated by u' and v' such that $u'^2 = Q(u).1 \neq 0$ and $v'^2 = Q(v).1 \neq 0$ and $u'v' = -v'u'$. Then A, and hence $C(V, Q)$, are quaternion algebras. □

Lemma 4.4.4. *Any quaternion algebra (a, b) is a four-dimensional central simple algebra over k.*

Proof. We already know that quaternion algebra is four-dimensional from previous lemma. Now let I be an ideal which is not equal to the quaternion algebra A. We can let

$$\bar{1} = 1 + I$$
$$\bar{i} = i + I$$
$$\bar{j} = j + I$$

Then we have the relations that $\bar{i}^2 = a\bar{1}, \bar{j}^2 = b\bar{1}, \bar{i}\bar{j} = -\bar{j}\bar{i}$. Hence A/I is a quaternion algebra and must have dimension four. It follows that $I = 0$ and hence A is simple.

Now we want to show that that center is k. Suppose $q = x + yi + zj + \omega ij$ is in the center of (a, b). Then $iq = qi$ immediately implies that $z = \omega = 0$. If $x + yi$ commutes with j, then we need $y = 0$. Hence $q = x$ and the center is k. □

The following lemma allows a Clifford algebra to be deconstructed into two Clifford algebras in which one has dimension 4. This is used in inductive proofs.

Lemma 4.4.5. *Let Q be non-degenerate and $\dim V \geq 3$. Let U be a two-dimensional subspace of V on which the restriction of Q to U is non-degenerate. Write $V = U \oplus U^\perp$ and let Q_1 and Q_2 denote the restriction of Q to U and $U^\perp$ respectively. Then*

$$C(V, Q) \cong C(U, Q_1) \otimes C(U^\perp, -\delta' Q_2)$$

where δ' is a discriminant of the restriction of β_Q to U.

Proof. To prove this lemma, we will use the two universal map properties to produce inverse isomorphism between $C(V, Q)$ and $C(U, Q_1) \otimes C(U^\perp, -\delta' Q_2)$. First, we denote the canonical maps of of U into $C(U, Q_1)$ and of $U^\perp$ into $C(U^\perp, -\delta' Q_2)$ as $i_1 : y \to y'$ and $i_2 : z \to z''$ respectively.

Let (u, v) be an orthogonal base for U and let $\bar{d} = 2\bar{u}\bar{v} \in C(V, Q)$. We have $\bar{u}^2 = Q(u), \bar{v}^2 = Q(v), \bar{u}\bar{v} = -\bar{v}\bar{u}$, so $\bar{d}^2 = 4Q(u)Q(v) = \delta'$ and δ' is the discriminant

of the restriction of β_Q to U defined by the basis (u, v). Now if $y \in U$ and $z \in U^\perp$, then $\bar{y}\bar{d} = -\bar{d}\bar{y}, \bar{y}\bar{z} = -\bar{z}\bar{y}$ and $\bar{d}\bar{z} = \bar{z}\bar{d}$. Hence

$$\bar{y}(\bar{d}\bar{z}) = (\bar{d}\bar{z})\bar{y}, \qquad (\bar{d}\bar{z})^2 = -\delta' Q(z).1 \tag{4.4.1}$$

Since $\bar{y}^2 = Q(y)$ and $(\bar{d}\bar{z})^2 = -\delta' Q(z).1$, the universal map property of Clifford algebras implies that we have a homomorphism of $C(U, Q_1)$ and $C(U^\perp, -\delta' Q_2)$ into $C(V, Q)$ by sending $y' \to \bar{y}, z'' \to \bar{d}\bar{z}$ respectively. The elements $\bar{y}$ and $\bar{d}\bar{z}$ generate the images under the homomorphism and these elements commute by (4.4.1) above. Hence the images under our homomorphism centralise each other, so by the universal property of tensor product, we have a homomorphism $h : C(U, Q_1) \otimes C(U^\perp, -\delta' Q_2) \to C(V, Q)$ such that

$$y' \to \bar{y} \qquad z'' \to \bar{d}\bar{z} \qquad y \in U, z \in U^\perp \tag{4.4.2}$$

Now consider the element $d' = du'v'$ in $C(U, Q_1)$. The calculations made before show that $d'y' = -y'd'$ and $d'^2 = -\delta'$, so δ is invertible in $C(U, Q_1)$. Now consider the element $y' + d'^{-1}z''$ of $C(U, Q_1) \otimes C(U^\perp, -\delta' Q_2)$. We have

$$\begin{aligned}(y' + d'^{-1}z'')^2 &= y'^2 + (y'd^{-1} + d'^{-1}y')z'' + z''^2 \\ &= y'^2 + z''^2 \\ &= Q(y) + Q(z) \\ &= Q(y + z)\end{aligned}$$

Hence by the universal map property of $C(V, Q)$, we have a homomorphism $g : C(V, Q) \to C(U, Q_1) \otimes C(U^\perp, -\delta Q_2)$ such that

$$\bar{y} + \bar{z} \to y' + d'^{-1}z'' \tag{4.4.3}$$

Checking on the generators, by equations (4.4.2), (4.4.3), we see that $gh = 1$ on $C(U, Q_1) \otimes C(U^\perp, -\delta' Q_2)$ and $hg = 1$ on $C(V, Q)$. Hence

$$C(V, Q) \cong C(U, Q_1) \otimes C(U^\perp, -\delta' Q_2).$$

□

We can now prove the dimensionality of Clifford algebra by induction.

Theorem 4.4.6. *If* $\dim V = n$, *then* $\dim C(V, Q) = 2^n$.

Proof. If $n = 1$, the results follows from Lemma 4.4.2. If $n = 2$ it follows from Lemma 4.4.4 and Lemma 4.4.3. Now assume $n > 2$ and we will proceed by induction. Since $n > 2$, we can choose a two dimensional subspace U where restriction of Q to U is non-degenerate. Then $V = U \oplus U^\perp$ and the restriction of Q to $U^\perp$ is also non-degenerate. From Lemma 4.4.5, we have $C(V, Q) \cong C(U, Q_1) \otimes C(U^\perp, -\delta' Q_2)$. By the induction hypothesis, we can assume $\dim C(U^\perp, \delta' Q_2) = 2^{n-2}$. We know $\dim C(U, Q_1) = 4$ since it is a quaternion algebra, then we have $\dim C(V, Q) = \dim C(U, Q_1) \times \dim C(U^\perp, \delta' Q_2) = 2^{n-2}2^2 = 2^n$. □

We can now prove the main theorem on the structure of Clifford algebras.

Theorem 4.4.7. *Let Q be a non-degenerate quadratic form of an n-dimensional vector space over a field k, where char $k \neq 2$. If n is even, then $C(V,Q)$ is central simple. If n is odd, then $C(V,Q)$ is either simple with a two dimensional field as center or is a direct sum of two isomorphic central simple algebras, if δ is not a square in k or $(-1)^{\frac{n-1}{2}}2\delta$ is a square in k respectively where δ is the discriminant of β_Q.*

Proof. If $n = 1$, the results follow from Lemma 4.4.2 and if $n = 2$ they follow from Lemma 4.4.4 and Lemma 4.4.3.

Now assume $n > 2$, we can pick a two-dimensional subspace U on which the restriction of Q is non-degenerate. Then $V = U \oplus U^{\perp}$ and the restriction of Q to $U^{\perp}$ is non-degenerate. By Lemma 4.4.5, $C(V,Q) \cong C(U,Q') \otimes C(U^{\perp}, -\delta' Q'')$ where δ' is a discriminant of the restriction of β_Q to U. Moreover, $C(U,Q)$ is a quaternion algebra, hence, is four dimensional central simple. By induction on dimension, we assume the results for the quadratic form $-\delta' Q''$ on $U^{\perp}$

Suppose $n-2$ is even and $\dim C(U^{\perp}, -\delta' Q'') = 2^{(n-2)}$, then $\dim C(V,Q) = 2^n$ and hence $C(V,Q)$ is central simple as n is even.

Now suppose $n-2$ is odd, then $C(U^{\perp}, -\delta' Q')$ is simple with two-dimensional center or is a direct sum of two isomorphic central simple algebras, if $(-1)^{\frac{n-3}{2}}2(-\delta)^{n-2}\delta''$ is not a square or is a square in k . Now

$$\begin{aligned}(-1)^{\frac{n-3}{2}}2(-\delta)^{n-2}\delta'' &= (-1)^{\frac{n-1}{2}}(\delta)^{n-3}2\delta'\delta'' \\ &= (-1)^{\frac{n-1}{2}}(\delta)^{n-3}2\delta\end{aligned}$$

and since $n-3$ is even this is a square if and only if $(-1)^{\frac{n-1}{2}}2\delta$ is a square. □

We can now give a more explicit connection between any Clifford algebras and quaternion algebras. We can construct Clifford algebras from quaternion algebras with tensor product.

Corollary 4.4.8. *Suppose Q is non-degenerate. Then $C(V,Q)$ is a tensor product of quaternion algebras if n is even and is a tensor product of quaternion algebra and its center if n is odd. Moreover suppose n is odd, let $d = (-1)^{\frac{n-1}{2}}2^{-n}\delta$ then,*

1. *If $\delta \notin k^2$ is not a square, the center $Z(C)$ is two-dimensional of the form $k(\sqrt{\delta})$.*
2. *If $\delta \in k^2$ is a square, then $Z(C)$ is a direct sum of two copies of k.*

Proof. The first statement follows by induction on dimension and the factorisation lemma (Lemma 4.4.5).

To determine the center when n is odd, choose an orthogonal base $(u_1, u_2, ..., u_n)$. Then $u_i u_j = -u_j u_i$ for $i \neq j$. This implies that the element $z = u_1 u_2 ... u_n$ commutes with every u_i. We have $u_i z = z u_i$ as

$$u_i u_1 u_2 ... u_n = u_1 u_2 ... u_n u_i$$

for all i. This is easy to see since n is odd. Hence z is the center and since $z \notin k$ and the center is two-dimensional, the center is $k(z)$. Now

$$\begin{aligned} z^2 = u_1u_2...u_nu_1u_2....u_n &= (-1)^{\frac{n(n-1)}{2}} u_1^2u_2^2....u_n^2 \\ &= (-1)^{\frac{n-1}{2}} \prod_{i=1}^{n} Q(u_i) \\ &= (-1)^{\frac{n-1}{2}} 2^{-n}\delta = d \end{aligned}$$

Then $k(z)$ is a field if d is not a square and $k(z)$ is a direct sum of two copies of k if d is square. □

From above, Clifford algebras with even dimension can be written as tensor product of quaternion algebras. We will see when we introduce Hasse invariant, which is defined by quaternion algebra, that we can associated the Hasse invariant to a certain Clifford algebra.

Chapter 5

Hasse-Witt Invariant

In this chapter, we look at Hasse-Witt invariant which is an important invariant for quadratic forms over the p-adic fields $\mathbb{Q}_p$. Hasse-Witt invariant is used in classification of quadratic forms over $\mathbb{Q}_p$ and also $\mathbb{Q}$ as we will see in the next chapter. To understand this invariant, I will first introduce p-adic fields and define Hilbert symbol over such fields. Hilbert symbol is used in the definition of the Hasse-Witt invariant. The relevant references for this section is [18], [19] and [9]. The proofs for well-known theorems in number theory and finite fields will be omitted in this thesis, as they do not provide any benefit or insight to the topic of this thesis. I will however, give reference to these proofs.

5.1 p-adic fields

I will first introduce p-adic field, denote as $\mathbb{Q}_p$. This is a completion of $\mathbb{Q}$ similar to $\mathbb{R}$. We will denote $\mathbb{R}$ as $\mathbb{Q}_\infty$. The main theorem in this section is Hensel's lemma which allows us to lift a solution from modulo p.

This section on $\mathbb{Q}_p$ only serve to give readers a basic understanding of $\mathbb{Q}_p$ and will not go into details. I will provide expositions without proof and some examples to get a good feel for these p-adic numbers. For further reading about $\mathbb{Q}_p$, a good source would be Serre [18].

Definition 5.1.1. *A* p-adic integers *are series of the form*

$$a_0 + a_1 p + a_2 p^2 + ...$$

where $a_i \in \{0, 1, ..., p-1\}$.

As one would expected, the addition of p-adic numbers is defined as the sum of their series expansions. Similarly, multiplication is defined as the product of their respective series expansions.

Definition 5.1.2. *The* p-adic numbers *are series of the form*

$$a_{-n}\frac{1}{p^n} + a_{-n+1}\frac{1}{p^{n-1}} + ... + a_{-1}\frac{1}{p} + a_0 + a_1 p + a_2 p^2 + ...$$

where $n \in \mathbb{Z}$ *and* $a_i \in \{0, 1, ..., p-1\}$

We can see that $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$. Addition and multiplication follows from p-adic integers. We will see subtraction and division of p-adic numbers in the following example.

Example 5.1.3. *Here, we have some examples of p-adic numbers over* $\mathbb{Q}_3$.

$$\begin{aligned} 59 &= 2 + 1 \times 3 + 0 \times 3^2 + 2 \times 3^3 \\ -1 &= 2 + 2 \times 3 + 2 \times 3^2 + ... \\ \frac{1}{2} &= -\frac{1}{1-3} = -(1 + 3 + 3^2 + ...) \end{aligned}$$

In general, over $\mathbb{Q}_p$ *we can write inverses and negatives with*

$$-1 = (p-1)\sum_{i=1}^{\infty} p^i$$

$$\frac{1}{1-p} = \sum_{i=1}^{\infty} p^i$$

Proposition 5.1.4. *The set of p-adic numbers form a field is called p-*adic fields, *which we denote as* $\mathbb{Q}_p$.

Proposition 5.1.5. *The p-adic field* $\mathbb{Q}_p$ *is the fraction field of* $\mathbb{Z}_p$.

From previous example, we can see that we can write elements in $\mathbb{Q}$ as an elements in $\mathbb{Q}_p$. Now, consider the example below when we consider square root of 7, which clearly does not lie in $\mathbb{Q}$.

Example 5.1.6. *Consider the equation* $X^2 - 7$, *clearly this has no solution over* $\mathbb{Q}$. *Consider solution of* $X^2 - 7$ *in* $\mathbb{Q}_3$. *Suppose* $\alpha = a_0 + a_1 \times 3 + a_2 \times 3^2 + ...$ *is a solution of the equation. Then we need*

$$a_0^2 - 7 \equiv 0 \ mod\ 3$$

The possible value of a_0 *is* 1 *and* 2. *The two values will give two solutions to the equation. Let* $a_0 = 1$. *Then we now need*

$$\begin{aligned} (1 + a_1 \times 3)^2 - 7 &\equiv 0 \ mod\ 3^2 \\ 1 + 6a_1 + 9a_1^2 - 7 &\equiv 0 \ mod\ 3^2 \\ 6a_1 - 6 &\equiv 0 \ mod\ 3^2 \\ a_1 &\equiv 1 \ mod\ 3^2 \end{aligned}$$

One can repeat this process module $3^3, 3^4, ...,$ *to obtain a solution*

$$\alpha = 1 + 3 + 3^2 + 2 \times 3^4 + 2 \times 3^7 + 3^8 + 3^9 + 2 \times 3^{10} + ...$$

In the above example, we solve an equation in the p-adic integers by solving each coefficient one at a time modulo $p, p^2, ...$ *If there is no solution for one coefficient with a given modulo, then there is no solution for the equation.*

We will now introduce an important theorem in p-adic fields, which is the Hensel Lemma. The Hensel's Lemma is the Newton's method analogue for finding roots of polynomial equations in $\mathbb{Q}_p$. With Hensel's Lemma, we obtain a new solution congruent to 0 modulo a higher power of p based on solution found modulo lower power of p.

Lemma 5.1.7. *(Hensel's lemma) Let $f \in \mathbb{Z}_p[X_1, ..., X_m]$ such that there there exists $x \in \mathbb{Z}_p^m$ with $f(x) \equiv 0$ mod p and $\frac{\partial f}{\partial X_j}(x) \neq 0$ for some $j \in \{1, ..., m\}$. Then x lifts to a zero of f.*

Proof. For a proof see Serre [18]. □

Example 5.1.8. *From previous example, we want to see if there is a solution of $f(X) = X^2 - 7$ in $\mathbb{Q}_3$. Now $f(1) = -6 \equiv 0$ mod 3. As $f'(X) = 2X$, we have $f'(1) = 2 \not\equiv 0$ mod 3. Hensel's lemma asserts that there is a unique 3-adic integers such that $\alpha^2 - 7 = 0$ and $\alpha \equiv 1$ mod 3.*

Definition 5.1.9. *The set of unit of $\mathbb{Z}_p$ is denote as $\mathbb{U}_p = \mathbb{Z}_p^*$.*

Proposition 5.1.10. *An element $x \in \mathbb{Z}_p$ is invertible, i.e. $x \in \mathbb{U}_p$, if and only if $p \nmid x$. Let $x \in \mathbb{Z}_p$, then we can write $x = p^n u$ where $n \geq 0$ and $u \in \mathbb{U}_p$.*

Proof. For the first statement, we see that if $x \in \mathbb{U}_p$ and $p \mid x$, then we can write

$$p \times \sum_{i=0}^{\infty} a_i p^i = 1 + 0 \times p + 0 \times p^2 + ...$$

which is impossible when we compare at the coefficient of each power of p. So p is not invertible, this also follows for multiple of p. Now for the converse, suppose x is invertible, then $xy = 1$ for some $y \in \mathbb{Z}_p$. Write $x = x_0 + x_1 p + ...$ and $y = y_0 + y_1 p + ...$ Then reducing it modulo p, we have $x_0 y_0 = 1$, hence x_0 is a unit in $\mathbb{Z}/p\mathbb{Z}$ and hence $p \nmid x_0$. This gives that $p \nmid x$.

For the second statement, since $x \neq 0$, we can find the smallest n such that the coefficient of p^n of x is non-zero. Hence $x = p^n u$ where $p \nmid u$. Thus we can write $x = p^n u$ where $n \in \mathbb{Z}$ and $u \in \mathbb{U}_p$ for all $x \in \mathbb{Z}_p$. □

5.2 Hilbert symbol

Here, I will introduce the Hilbert symbol over the p-adic fields. The Hilbert symbol is connected to the Hasse-Witt invariant which is an important invariant of quadratic form over $\mathbb{Q}_p$. We will also need a few well known theorems or results from number theory which will be stated without proof.

We define the Hilbert symbol as the equivalence class of quaternion algebra in 2-torsion Brauer group. Consider the field $\mathbb{Q}_v$, as $Br(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$ and $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ from earlier chapters. The 2-torsion Brauer group of $\mathbb{Q}_v$ is a group of order 2.

$$Br(\mathbb{Q}_v)_2 \cong \mathbb{Z}/2\mathbb{Z}$$

Definition 5.2.1. *We can define the Hilbert symbol as the Brauer class of quaternion algebra in $Br(\mathbb{Q}_v)_2 \cong \{1, -1\}$, where*

$$(a, b)_v = \begin{cases} 1 & \text{if the quaternion algebra } (a, b) \text{ is split over } \mathbb{Q}_v \\ -1 & \text{otherwise} \end{cases}$$

So Hilbert symbol is a map $(-, -) : k^*/k^{*2} \times k^*/k^{*2} \to Br_2(k)$.

We also have another definition of Hilbert symbol with quadratic forms. Firstly, recall from Proposition 4.1.9 (iii) that a quaternion algebra (a, b) is split if and only if a is a square or b is a norm from $k(\sqrt{a})/k$. Now, consider the following Proposition.

Proposition 5.2.2. *We have $a \in k^{*2}$ or b is a norm from $k(\sqrt{a})/k$ if and only if the quadratic form $X_1^2 - aX_2^2 - bX_3^2$ is isotropic, which means there is a non-zero solution to $X_1^2 - aX_2^2 - bX_3^2 = 0$.*

Proof. ($\Rightarrow$) Suppose a is a square, so let $a = c^2$. The we have $(c, 1, 0)$ is a solution. Suppose b is a norm then for some $z, x \in k$, we have $b = N(z + x\sqrt{a}) = z^2 - ax^2$. It follows that $z^2 - ax^2 - b = 0$. Then we have $(z, x, 1)$ as a solution.

($\Leftarrow$) Suppose we have non-trivial solution (z, x, y) for the quadratic form $X_1^2 - aX_2^2 - bX_3^2 = 0$. Then we have $z^2 - ax^2 - by^2 = 0$, consider two cases where either $y = 0$ or $y \neq 0$. Suppose $y = 0$ and $z, x \neq 0$, then $z^2 - ax^2 = 0$. Hence $a = (\frac{z}{x})^2$ and $a \in k^{*2}$. Suppose $y \neq 0$,then $b = \frac{z^2 - ax^2}{y^2} = (\frac{z}{y})^2 - a(\frac{x}{y})^2$ which is a norm of $k(\sqrt{a})/k$. □

We can also define Hilbert symbol by considering a ternary quadratic form $z^2 - ax^2 - by^2 = 0$. We let $(a, b)_v = 1$ if this equation has a non-trivial solution in $\mathbb{Q}_v$ and -1 otherwise. Similarly, we can say $(a, b)_v = 1$ if and only if the quadratic form $ax^2 + by^2$ represent 1 over $\mathbb{Q}_v$ and -1 else. The two proposition above combine to show the equivalence of the the two definitions of Hilbert symbol. It also shows connection between quaternion algebras and quadratic forms.

Now, we want to prove the bilinearity of Hilbert symbol. The following proof for bilinearity of Hilbert symbol was done with my supervisor.

Proposition 5.2.3. *The Hilbert symbol is bilinear. That is*

$$M_2((a, bc)) \cong (a, b) \otimes (a, c)$$

as algebra so

$$(a, bc)_v = (a, b)_v (a, c)_v$$

as element of the 2-torsion Brauer group.

Proof. Define the quaternion algebras

$$(a, bc) = \frac{k\langle x, y\rangle}{\langle x^2 = a, y^2 = bc, xy = -yx\rangle}$$

$$(a, b) = \frac{k\langle x_1, y_1\rangle}{\langle x_1^2 = a, y_1^2 = b, x_1 y_1 = -y_1 x_1\rangle}$$

$$(a, c) = \frac{k\langle x_2, y_2\rangle}{\langle x_2^2 = a, y_2^2 = c, x_2 y_2 = -y_2 x_2\rangle}$$

Consider the map $f : (a, b) \otimes (a, c) \to M_2((a, bc))$ where f maps

$$x_1 \to \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \qquad y_1 \to \begin{pmatrix} 0 & y \\ c^{-1}y & 0 \end{pmatrix}$$

$$x_2 \to \begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix} \qquad y_2 \to \begin{pmatrix} 0 & c \\ 1 & 0 \end{pmatrix}.$$

It can be verified that it satisfies all required relation. For example, we can check that $y_1^2 = bI_2$ using the relation $y^2 = bc$ in (a, bc).

$$y_1^2 = \begin{pmatrix} 0 & y \\ c^{-1}y & 0 \end{pmatrix} \begin{pmatrix} 0 & y \\ c^{-1}y & 0 \end{pmatrix} = \begin{pmatrix} c^{-1}y^2 & 0 \\ 0 & c^{-1}y^2 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$$

Using relation $xy = -yx$ in (a, bc) we can show that $x_1y_1 = -y_1x_1$.

$$x_1y_1 = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} 0 & y \\ c^{-1}y & 0 \end{pmatrix} = \begin{pmatrix} 0 & xy \\ c^{-1}xy & 0 \end{pmatrix}$$

$$y_1x_1 = \begin{pmatrix} 0 & y \\ c^{-1}y & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 0 & yx \\ c^{-1}yx & 0 \end{pmatrix} = \begin{pmatrix} 0 & -xy \\ -c^{-1}yx & 0 \end{pmatrix} = -x_1y_1$$

Other relations holds similarly. Hence f is an homomorphism. To see it is bijective, note that the dimension of $M_2((a, bc))$ and $(a, b) \otimes (a, c)$ is 16, hence we only need to show it is injective. Consider the kernel of f. As $(a, b) \otimes (a, c)$ is central simple and kernel is an ideal. We have the kernel is either 0 or $(a, b) \otimes (a, c)$. We can see that kernel is 0, hence this is an isomorphism as required.

□

We will now see some other interesting properties of Hilbert symbol. All relevant sources (that I have seen) proved these properties using alternate definition of Hilbert symbol, which depends on the solvability of the quadratic form. We will however prove these by using original definition of Hilbert symbol, which relates to splitting of quaternion algebra.

Proposition 5.2.4. *The Hilbert symbol satisfies the following relationship:*

1. $(a, b) = (b, a)$ *and* $(a, c^2) = 1$
2. $(a, -a) = 1$ *and* $(a, 1 - a) = 1$
3. $(a, b) = (a, -ab) = (a, (1 - a)b)$

Proof. To show that a quaternion algebra is split, that is Hilbert symbol equals 1, it suffices to show there exists an element q such that the norm $N(q)$ equals zero.

1. The symmetry is clear. Suppose quaternion algebra (a, c^2), then we have relation $y^2 = c^2$ where y is one of the generators. Consider $q = c + y$, then $N(q) = (c + y)(c - y) = c^2 - y^2 = 0$. It follows that this is not a division algebra and must be split. Hence, we have shown that $(a, c^2) = 1$.
2. Now consider $q = x + y$ in quaternion algebra $(a, -a)$, then $N(q) = (x + y)(-x - y) = -(x^2 + y^2) = -(a - a) = 0$. Since $N(q) = 0$, the inverse does not exists, hence this quaternion algebra split. This implies $(a, -a) = 1$. Consider $q = 1 + x + y \in (a, 1 - a)$, similarly $N(q) = 0$. Hence $(a, 1 - a) = 1$.
3. This is clear when we consider bilinearity of Hilbert symbol and part (2) of this proposition.

□

I will now introduce the Legendre symbol which will be used in calculation of the Hilbert symbol. We will see that the well-known Quadratic Reciprocity theorem for Legendre symbol is equivalent to Hilbert Reciprocity involving Hilbert symbol.

Definition 5.2.5. *Let u be an odd integer. Define*

$$\varepsilon(u) = \begin{cases} 0 & \text{if } u \equiv 1 \pmod 4 \\ 1 & \text{if } u \equiv -1 \pmod 4 \end{cases} \qquad \omega(u) = \begin{cases} 0 & \text{if } u \equiv \pm 1 \pmod 8 \\ 1 & \text{if } u \equiv \pm 3 \pmod 8 \end{cases}$$

Definition 5.2.6. *Define* Legendre symbol *by*

$$\left(\frac{u}{p}\right) = \begin{cases} 1 & \text{if } u \text{ is a square mod } p \\ -1 & \text{otherwise} \end{cases}$$

where p is an odd prime and $u \in (\mathbb{Z}/p\mathbb{Z})^*$

We can obtain a nicer formula of the Legendre symbol using Euler's criterion.

Theorem 5.2.7. *(Euler's criterion) If p is an odd prime and $p \nmid a$, then $x^2 \equiv a \bmod p$ has a solution if and only if*

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p$$

Proof. For a proof, see [3]. □

Hence we can have this formula for Legendre symbol $\left(\frac{u}{p}\right) = u^{\frac{p-1}{2}} \bmod p$ which allows for easier calculation.

Proposition 5.2.8. *The Legendre symbol is multiplicative.*

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

Proof. It follows immediately from Euler's criterion as

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Theorem 5.2.9. *(Quadratic reciprocity) For all odd primes p, q, we have*

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

together with supplement

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

Proof. For a proof of quadratic reciprocity, see [10] for Theorem 3.2.1, p.53. □

Example 5.2.10. *To compute* $\left(\frac{97}{101}\right)$*, we use quadratic reciprocity for easier calculation.*

$$\left(\frac{97}{101}\right)=\left(\frac{101}{97}\right)=\left(\frac{4}{97}\right)=\left(\frac{2^2}{97}\right)=1$$

We will show later that Quadratic Recirprocity Theorem 5.2.9 is equivalent to Hilbert Reciprocity Theorem 5.2.16. We will now move on to obtain formulas for calculating the Hilbert symbol using Legendre symbol. However, we first need to introduce few theoreams and lemmas that will be used in the proof of the formulas.

Theorem 5.2.11. *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 a is a square solution in $\mathbb{Q}_p$ if and only if n is even and $\left(\frac{u}{p}\right)=1$. Further, if $p = 2$, then a is a square solution in $\mathbb{Q}_2$ if and only if $u \equiv 1$ mod 8 and n is even.*

Proof. For the first statement, suppose $a = p^n u$ and n even. If $\left(\frac{\bar{u}}{p}\right)=1$, this implies we can solve $\bar{x}^2 = \bar{u}$ in $\mathbb{Z}/p\mathbb{Z}$. Using Hensel's lemma Lemma 5.1.7, we can lift to a solution $x^2 = u$ in $\mathbb{Z}_p$ where $a = (p^{\frac{n}{2}}x)^2$. The converse is clear. If a is a square solution in $\mathbb{Q}_p$, we need n to be even and u to be a square modulo p. The case over $\mathbb{Q}_2$ requires a different argument, as we cannot use Hense's lemma to lift the solution. See Serre [18] p.17-18 for a proof of the case where $p = 2$. □

Lemma 5.2.12. *Let $v \in \mathbb{U}_p := \mathbb{Z}_p^*$ be a p-adic unit. If the equation $X_1^2 - pX_2^2 - vX_3^2 = 0$ has nontrivial solution over $\mathbb{Q}_p$, it has solution (z, x, y) such that $z, y \in \mathbb{U}_p$ and $x \in \mathbb{Z}_p$.*

Proof. Detailed proof can be found Page 21 of Serre [18]. A brief outline of the proof is as follows. Suppose we have nontrivial solution, this implies that we have solution (z, x, y) where at least one of z, x, y is not divisible by p. As an element in $\mathbb{Z}_p$ a unit if and only if it is not divisible by p. For a contradiction, suppose z or $y \notin \mathbb{U}_p$, then either $p \mid z$ or $p \mid y$. From the assumption, we have $z^2 - vy^2 \equiv 0 \bmod p$ and $p \nmid v$, hence we need both $p \mid z$ and $p \mid y$. This means $px^2 \equiv 0 \bmod p^2$, which implies $p \mid x$. This will lead to which is a contradiction as we have at least one of z, x, y is not divisible by p. Thus $z, y \in \mathbb{U}_p$ and $x \in \mathbb{Z}_p$. □

The next lemma follows from a well-known theorem in finite field which is the Chevally-Warning Theorem.

Theorem 5.2.13. *(Chevally-Warning) Let $f \in \mathbb{F}_p[X_1, ..., X_n]$ with $deg(f) < n$, then the solution to $f(x_1, ..., x_n) = 0$ is divisible by p.*

Proof. For a proof see [18], Theorem I.2.3, p.5. □

Lemma 5.2.14. *All quadratic forms with at least 3 variables over $\mathbb{F}_p$ have a non-trivial zero.*

Proof. Let $Q = a_1X_1^2 + a_2X_2^2 + a_3X_3^2$ be a quadratic form with $a_i \in \mathbb{F}_p$. Since we have a trivial solution $(0, 0, 0)$ and as the number of solutions must be divisible by p by Theorem 5.2.13, we must have a non-trivial zero. □

Finally, we obtain the following formulas for calculation of Hilbert symbol.

Proposition 5.2.15. *If $a, b \in \mathbb{R}$ then we have*

$$(a,b)_\infty = \begin{cases} 1 & \text{if } a > 0 \text{ or } b > 0 \\ -1 & \text{else} \end{cases}.$$

If $a, b \in \mathbb{Q}_p$, we write $a = p^\alpha u$ and $b = p^\beta v$ with $u, v \in \mathbb{Z}_p^*$ then

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

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

The following proof is based on Serre [18] but provided with greater more details. Also, since we have bilinearity of Hilbert symbol from Proposition 5.2.3, while the proof from Serre did not, we have a different and easier argument for some of the cases. In Serre's book [18], bilinearity was proven using this proposition instead.

Proof. For the first equation, since every $a \in \mathbb{R}$ where $a > 0$ is a square, then from Proposition 5.2.4

$$(a,b)_\infty = (c^2, b)_\infty = 1$$

Now over $\mathbb{Q}_p$ where $p \neq 2$, note that α and β come in only by their residue modulo 2. First consider the right hand side, we have

$$(-1)^{(\alpha+2)\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^{(\alpha+2)} = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right)^\alpha$$

and similarly for $\beta + 2$. Also left hand side, as Hilbert symbol is bilinear and symmetric. We have $(a, p^2) = 1$ from Proposition 5.2.4 and the fact that that Hilbert symbol is bilinear. Multiplying a, b by p^2 have no effect no either side of equation. Thus there are only three cases to consider.

1. $\alpha = 0, \beta = 0$. We only need to show that $(u, v) = 1$. The equation

   $$f = X_1^2 - uX_2^2 - vX_3^2 = 0$$

   has (z, x, y) as non-trivial solution modulo p which exists by Lemma 5.2.14. As u, v are units,we know that $\frac{\partial f}{\partial X_i}(z, x, y) \neq 0$ for at least one $i = 1, 2, 3$. Hence the above solution lifts to a p-adic solution using Hensel's lemma Lemma 5.1.7. Hence $(u, v) = 1$.

2. $\alpha = 1, \beta = 0$. We want to show that $(pu, v) = \left(\frac{v}{p}\right)$. Since $(u, v) = 1$ from case 1, we have $(pu, v) = (p, v)(u, v) = (p, v)$ by bilinearity. Hence, it suffices to check $(p, v) = \left(\frac{v}{p}\right)$. This is clear if v is a square, then the equation $X_1^2 - pX_2^2 - vX_3^2$ has solution $(\sqrt{v}, 0, 1)$. Hence it is clear that $(p, v) = \left(\frac{v}{p}\right) = 1$.

Now suppose v is not a square, then $\left(\frac{v}{p}\right) = -1$ by Theorem 5.2.11. Suppose $X_1^2 - pX_2^2 - vX_3^2 = 0$ has a non-trivial solution (z, x, y), then this implies $z^2 \equiv vy^2 \bmod p$. Hence, $z, y \notin \mathbb{U}_p$ (otherwise v would be square). This is a contradiction to Lemma 5.2.12. Thus, $X_1^2 - pX_2^2 - vX_3^2$ does not have non-trivial zero and so $(p, v) = -1$. Hence $(pu, v) = (p, v) = \left(\frac{v}{p}\right)$.

3. $\alpha = 1, \beta = 1$. We want to show $(pu, pv) = (-1)^{\varepsilon(p)}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$. Again by bilinearity and properties from Proposition 5.2.4,

$$\begin{aligned}(pu, pv) &= (pu, pv)(pu, -pu)\\ &= (pu, -p^2uv)\\ &= (pu, p^2)(pu, -uv)\\ &= (pu, -uv)\end{aligned}$$

then $(pu, pv) = (pu, -uv) = \left(\frac{-uv}{p}\right)$ by case 2. We also have $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$ by definition of Legendre symbol. Hence we obtain that $(pu, pv) = \left(\frac{-uv}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{u}{p}\right)\left(\frac{v}{p}\right) = (-1)^{\varepsilon(p)}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$ as desired.

Now, consider case where $p = 2$. Similarly, there are three cases to consider.

1. $\alpha = 0, \beta = 0$. Since we want to show $(u, v)_2 = (-1)^{\varepsilon(u)\varepsilon(v)}$. By definition of ε, it suffices to check that

$$(u, v)_2 = \begin{cases} 1 & \text{if } u \text{ or } v \equiv 1 \bmod 4 \\ -1 & \text{otherwise} \end{cases}$$

Suppose that $u \equiv 1 \bmod 4$, then $u \equiv 1 \bmod 8$ or $u \equiv 5 \bmod 8$. In the first case, u is a square from Theorem 5.2.11, hence $(u, v) = 1$. In the second case with $u \equiv 5 \bmod 8$, we can write $u + 4v \equiv 1 \bmod 8$ as $2 \nmid v$ (since $v \in \mathbb{U}_2$). So there exists $w \in \mathbb{U}_2$ such that $w^2 = u + 4v$ by Theorem 5.2.11. Then $X_1^2 - uX_2^2 - vX_3^2$ has solution $(w, 1, 2)$ for a zero, hence $(u, v) = 1$. Similarly for when $v \equiv 1 \bmod 4$. Now, suppose $u \equiv v \equiv -1 \bmod 4$. Suppose $X_1^2 - uX_2^2 - vX_3^2 = 0$ has a non-trivial solution (z, x, y). Then by Lemma 5.2.12, at least one of z, x, y is invertible i.e. in $\mathbb{U}_2$. As $z^2 - ux^2 - vy^2 = 0$, then $z^2 + x^2 + y^2 \equiv 0 \bmod 4$. Now, the squares of $\mathbb{Z}/4\mathbb{Z}$ are 0 and 1, this congruence implies that x, y, z are congruent to 0 mod 2, which contradicts one of z, x, y being invertible. Thus we have $(u, v) = -1$ as we do not have non-trivial solution. Hence $(u, v)_2 = (-1)^{\varepsilon(u)\varepsilon(v)}$ as required.
2. $\alpha = 1, \beta = 0$. We want to show $(2u, v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)}$. We first show that $(2, v) = (-1)^{\omega(v)}$. That is, we want to show that $(2, v) = 1$ is equivalent to $v \equiv \pm 1 \bmod 8$. ($\Rightarrow$) Using Lemma 5.2.12, if $(2, v) = 1$, then there exists $x, y, z \in \mathbb{Z}_2$ such that $z^2 - 2x^2 - vy^2 = 0$ where $y, z \not\equiv 0 \bmod 2$. Then $y, z \in \mathbb{U}_2$ and hence $y^2 = z^2 \equiv 1 \bmod 8$ by Theorem 5.2.11. Hence $1 - 2x^2 - v \equiv 0 \bmod$

8. However, the only squares mod 8 are $0, 1$ and 4, these are the only possible value for x^2. So we have $v \equiv \pm 1 \bmod 8$. ($\Leftarrow$) Conversely suppose $v \equiv 1 \bmod 8$, then v is a square by Theorem 5.2.11. By Proposition 5.2.4, $(2, v) = 1$. If $v \equiv -1 \bmod 8$,then $f = X_1^2 - 2X_2^2 - vX_3^2 \equiv 0 \bmod 8$ has solution $(1, 1, 1)$, As $\frac{\partial f}{\partial X_1}(1, 1, 1) = 2$, hence by Hensel's lemma Lemma 5.1.7, this lift to a zero of f. This gives $(2, v) = 1$.
Now by bilinearity of Hilbert symbol, we have $(2u, v) = (2, v)(u, v)$. From above we have shown that $(2, v) = (-1)^{\omega(v)}$. From case 1, we also have $(u, v) = (-1)^{\varepsilon(u)\varepsilon(v)}$. Hence we have $(2u, v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)}$ as required.

3. $\alpha = 1, \beta = 1$. We need to show

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

Using bilinearity and Proposition 5.2.4 together with the fact that $X_1^2 - 2X_2^2 + X_3^2 = 0$ has $(1, 1, 1)$ as a non-trivial solution, that is $(2, -1) = 1$, we have the following

$$\begin{aligned}
(2u, 2v) &= (2u, 2v)(2u, -2u) \\
&= (2u, -4uv) \\
&= (2u, -uv) \\
&= (2u, -1)(2u, uv) \\
&= (2, -1)(u, -1)(2u, uv) \\
&= (u, -1)(2, uv)(u, uv) \\
&= (u, -uv)(2, uv) \\
&= (u, -uv)(u, -u)(2, uv) \\
&= (u, u^2v)(2, uv) \\
&= (u, v)(2, u)(2, v).
\end{aligned}$$

Hence from case 1 and case 2, we have $(2u, 2v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(u)+\omega(v)}$ as required.

□

Another important result in number theory is the Quadratic Reciprocity, we will now show that Hilbert Reciprocity is equivalent to Quadratic Reciprocity Theorem 5.2.9. Unlike Quadratic Reciprocity, Hilbert Reciprocity does not need require extra cases for negatives values and for the prime 2. The Quadratic Reciprocity law is one of the most important theorems of number theory.

I will first introduce the theorem of Hilbert reciprocity

Theorem 5.2.16. *(Hilbert reciprocity) If $a, b \in \mathbb{Q}_v^*$, we have $(a, b)_v = 1$ for all but finitely many v and*

$$\prod_v (a, b)_v = 1$$

We will now prove that Hilbert reciprocity Theorem 5.2.16 is equivalent to Quadratic reciprocity Theorem 5.2.9.

Proof. (Hilbert Reciprocity is equivalent to Quadratic Reciprocity) First note that we can decompose numerator and denominator of a, b into product of primes and -1. As the Hilbert symbol is bilinear, it suffices to prove

$$\prod_v (p,q)_v = 1$$

where p, q are primes or -1. We will use formulas from Proposition 5.2.15 and consider the various cases.

1. $p, q = -1$. Since $a, b < 0$ then $(a,b)_\infty = -1$. $(a,b)_2 = (-1)^1 = -1$. $(a,b)_p = (-1)^0 = 1$ for all primes $p \neq 2$. Hence $\prod_v (-1,-1)_v = 1$. Hence

$$\prod_v (-1,-1)_v = 1.$$

2. $p = -1, q = 2$. Since $z^2 + x^2 - 2y^2 = 0$ has solution $x = y = z = 1$, hence $(2,-1)_v = 1$. Hence

$$\prod_v (-1,2)_v = 1.$$

3. For $q = -1$, p odd prime. Since $p > 0$, then $(a,b)_\infty = 1$. $(a,b)_2 = (-1)^{\varepsilon(p)}$. $(-1,p)_p = \left(\frac{-1}{p}\right)$. Then

$$\prod_v (-1,p)_v = 1 \Leftrightarrow \left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$$

which is the first supplement of quadratic reciprocity Theorem 5.2.9 .

4. For $p, q = 2$. Since $p, 2 > 0$, then $(2,p)_\infty = 1$. $(2,p)_2 = (-1)^{\omega(p)}$. $(2,p)_p = \left(\frac{2}{p}\right)$. Hence

$$\prod_v (2,p)_v = 1 \Leftrightarrow \left(\frac{2}{p}\right) = (-1)^{\omega(p)}$$

which is the second supplement of quadratic reciprocity Theorem 5.2.9 .

5. For $p = q$ odd prime. Since $p > 0$, then $(p,p)_\infty = 1$. $(p,p)_2 = (-1)^{\varepsilon(p)\varepsilon(p)} = (-1)^{\varepsilon(p)}$. $(p,p)_p = (-1)^{\varepsilon(p)} \left(\frac{1}{p}\right)\left(\frac{1}{p}\right) = (-1)^{\varepsilon(p)}$. Hence

$$\prod_v (p,p)_v = 1.$$

6. For $p \neq q$ both odd prime. Since $p, q > 0$,$(p,q)_\infty = 1$. $(p,q)_2 = (-1)^{\varepsilon(p)\varepsilon(q)}$. $(p,q)_p = \left(\frac{q}{p}\right)$,$(p,q)_q = \left(\frac{p}{q}\right)$

$$\prod_v (p,q)_v = 1 \Leftrightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(-1)^{\varepsilon(p)\varepsilon(q)} = 1$$

which is the general statement of quadratic reciprocity Theorem 5.2.9 .

□

What are implications of Hilbert Reciprocity for quaternion algebra? We will introduce a new definition and we have a corollary of the Hilbert Reciprocity theorem on the splitting of quaternion algebra.

Definition 5.2.17. *The place v is* ramified *in $\mathbb{Q}$ if $\mathbb{Q}_v$ is a division ring, otherwise it is unramified (or split).*

Corollary 5.2.18. *Let (a, b) be a quaternion algebra over $\mathbb{Q}$, then the number of places where it is ramified is finite and of even cardinality.*

Proof. Follow immediately from Theorem 5.2.16 by definition of ramified of quaternion algebra and definition of Hilbert symbol. □

5.3 Hasse-Witt invariant

Hasse-Witt invariant is one of the invariant which is essential in classification of quadratic forms over $\mathbb{Q}_p$ and $\mathbb{Q}$. The definition and the properties of Hasse-Witt invariant depends on quaternion algebra. We define Hasse-Witt invariant as an element of the 2-torsion Brauer group.

If $n = 1$, the element is the unit 1 of $Br(\mathbb{Q}_p)_2 \cong \mathbb{Z}/2\mathbb{Z}$. Suppose $n > 1$, let Q a the quadratic form and let $(v_1, ..., v_n)$ be an orthogonal base of Q.

Definition 5.3.1. *We can defined the* Hasse-Witt invariant *of Q, denote as $s(Q)$, as an element of 2-toriosn Brauer group with the product of Hilbert symbol*

$$s(Q) = \prod_{i<j} (Q(v_i), Q(v_j))$$

The Hasse-Witt invariant of a quadratic form $Q = a_1X_1^2 + ... + a_nX_n^2$ over $\mathbb{Q}_p$ can be written as $\prod_{i<j}(a_i, a_j)$. The two definition reconcile since we can choose the basis $(v_1, ...v_n)$ such that $Q(v_1) = a_1, ..., Q(v_n) = a_n$. To see that this is in fact an invariant of quadratic forms, we first want to verify that it is independent of the basis chosen. We can see this by showing that Hasse-Witt invariant can be defined using Clifford algebra.

Theorem 5.3.2. *The Hasse Witt invariant $s(Q)$ does not depend on the choice of orthogonal basis.*

Proof. This proof is based on the proof from Jacobson's Basic algebra II [9], but with greater detail.

We first denote $\backsim$ as equivalence in the 2-torsion Brauer group. Let U be an n-dimensional vector space with quadratic form P which we have an orthogonal base $(u_1, ..., u_n)$ such that $P(u_i) = -1$ where $1 \leq i \leq n$. We can form vector space $W = U \oplus V$ and defined quadratic form R on W by $R(u + v) = P(u) + Q(v), u \in U, v \in V$. Then $W = U \perp V$ and the restrictions of R to U and V are P and Q

respectively. To prove this theorem, it suffices to show that for any orthogonal base $(v_1, ..., v_n)$ for V, we have

$$\prod_{i<j}(Q(v_i), Q(v_j)) \backsim C(W, R) \otimes (d, d)$$

where $C(W, R)$ is the Clifford algebra of R and d is the discriminant of Q. This would imply the theorem as $C(W, R) \otimes (d, d)$ does not depend on the orthogonal basis.

Let $a_i = Q(v_i), d_i = \prod_{j=1}^{n} a_j$, so $d_n = d$. We first show that

$$C(W, R) \backsim \prod_{i=1}^{n}(a_i, d_i).$$

The Clifford algebra $C(W, R)$ is a central simple algebra by Corollary 4.4.8 as it has even dimension. It is generated by the elements $u_i, v_i, 1 \leq i \leq n$, we have the relation $u_i^2 = -1$, $v_i^2 = a_i$, $u_i u_j = -u_j u_i$, $v_i v_j = -v_j v_i$ if $i \neq j$. Also $u_i v_k = -v_k u_i$ for all i, k. Let

$$w_1 = (v_1 u_1)....(v_{n-1} u_{n-1}) v_n \qquad w_2 = v_n u_n.$$

Using above relations, it follows that

$$(v_i u_i)^2 = (v_i u_i)(v_i u_i) = -v_i u_i^2 v_i = -v_i^2 u_i^2 = a_i \tag{5.3.1}$$

$$(v_i u_i)(v_j u_j) = (-1)^2 v_j v_i u_i u_j = (-1)^4 v_j u_j v_i u_i = (v_j u_j)(v_i u_i) \tag{5.3.2}$$

$$v_n(v_i u_i) = (-1)^2 (v_i u_i v_n) = (v_i u_i) v_n \qquad \text{if } i < n \tag{5.3.3}$$

$$v_n w_2 = v_n v_n u_n = (-1) v_n u_n v_n = -w_2 v_n. \tag{5.3.4}$$

This implies that we have

$$\begin{aligned} w_1^2 &= (v_1 u_1)....(v_{n-1} u_{n-1}) v_n (v_1 u_1)....(v_{n-1} u_{n-1}) v_n \\ &= (v_1 u_1)....(v_{n-1} u_{n-1})(v_1 u_1)....(v_{n-1} u_{n-1}) v_n^2 \qquad \text{using (4.3.3)} \\ &= (v_1 u_1)^2....(v_{n-1} u_{n-1})^2 v_n^2 \qquad \text{using (4.3.2)} \\ &= a_1 a_2....a_n \qquad \text{using (4.3.1)} \\ &= d_n = d \end{aligned}$$

and

$$w_2^2 = (v_n u_n)(v_n u_n) = -v_n v_n u_n u_n = a_n.$$

Also,

$$\begin{aligned} w_1 w_2 &= (v_1 u_1)....(v_{n-1} u_{n-1}) v_n w_2 \\ &= -(v_1 u_1)....(v_{n-1} u_{n-1}) w_2 v_n \qquad \text{using (4.3.4)} \\ &= -w_2 (v_1 u_1)....(v_{n-1} u_{n-1}) v_n \qquad \text{using (4.3.2)} \\ &= -w_2 w_1. \end{aligned}$$

Thus, we obtain

$$w_1^2 = d \qquad w_2^2 = a_n, \qquad w_1 w_2 = -w_2 w_1.$$

Hence the sub-algebra generated by w_1 and w_2 is (a_n, d_n). Now

$$C(W, R) \cong (a_n, d_n) \otimes C'$$

where C' is the centralizer in $C(W, R)$ of the sub-algebra generated by w_1 and w_2. The elements $u_i, v_i, 1 \leq i \leq n-1$, commutes with w_1, w_2, as

$$u_i w_1 = u_i(v_1u_1)....(v_{n-1}u_{n-1})v_n = (-1)^{2n-2}(v_1u_1)....(v_{n-1}u_{n-1})v_nu_i = w_1u_i.$$

Similarly for $v_iw_1 = w_1v_i$, $u_iw_2 = w_2u_i$ and $v_iw_2 = w_2v_i$. To see the isomorphisms $C(W, R) \cong (a_n, d_n) \otimes C'$ holds, consider the multiplicative map $C' \otimes (a_n, d_n) \to C(W, R)$ which maps $c' \otimes w$ to $c'w$. This is a clearly a homomorphism. Now, recall that tensor product or two central simple algebras is again simple. Hence the kernel of this map is either 0 or $C' \otimes (a_n, d_n)$, and clearly kernel equals to 0 and hence the map is injective. Similar argument with image of the maps implies the map is subjective. Hence the map is bijective and we have $C(W, R) \cong (a_n, d_n) \otimes C'$.

The sub-algebra C' generated by u_i, v_i is isomorphic to Clifford algebra $C(W', R')$ where $W' = \sum_{i=1}^{n-1} ku_i + \sum_{i=1}^{n-1} kv_i$ and R' is the restriction of R to W'. Now since $[C(W', R') : k] = 2^{2(n-1)}$ and $[C' : k] = 2^{2(n-1)}$, we have $C' \cong C(W,' R')$ and

$$C(W, R) \cong (a_n, d_n) \otimes C(W', R').$$

By induction on n, we obtain

$$C(W, R) \backsim \prod_{i=1}^{n} (a_i, d_i).$$

With bilinearity and symmetry of Hilbert symbol, we have

$$C(W, R) \backsim \prod_{i=1}^{n} (a_i, a_1....a_i) \backsim \prod_{i \leq j} (a_i, a_j) \backsim (d, d) \prod_{i<j} (a_i, a_j).$$

Hence $\prod_{i<j}(a_i, a_j) \backsim C(W, R) \otimes (d, d)$ as required. □

Remark 5.3.3. *In fact, for two quadratic form Q, Q' we have*

$$s(Q \perp Q') = s(Q)s(Q')(d(Q), d(Q')).$$

Example 5.3.4. *Consider the quadratic forms*

$$Q \cong 5X_1^2 + 11X_2^2 - 13X_3^2.$$

We use Proposition 5.2.15 to calculate the Hasse-Witt invariant over $\mathbb{Q}_5$ and we have

$$s(Q) = (5, 11)_5(5, -13)_5(11, -13)_5 = \left(\frac{11}{5}\right)\left(\frac{-13}{5}\right) = \left(\frac{1^2}{5}\right)\left(\frac{2}{5}\right) = -1$$

Chapter 6

Hasse-Minkowski theorem

We will look at the classification of quadratic form over $\mathbb{Q}$ in this section. We assume that all quadratic forms are non-degenerate.

For classification of quadratic forms over $\mathbb{C}$, the *dimension* is enough to classify the quadratic forms. For the classification of quadratic form over $\mathbb{R}$, suppose we have a quadratic form $a_1X_1^2+...+a_nX_n^2$ with all a_i non-zero. We can multiply the a_i by non-zero squares without changing the equivalence class of the form. With this, we can turn all positive a_i into 1's and all negative a_i into -1's. This is because in $\mathbb{R}$ any positive number is a square. This way we see that any form over $\mathbb{R}$ is equivalent to

$$X_1^2 + ... + X_r^2 - Y_1 - ... - Y_s^2$$

for some $r, s \in \mathbb{N}$. Then (r, s) is the *signature* of the form. (Sylvester's law of inertia)

Equivalence over $\mathbb{C}, \mathbb{R}$ are easy using dimension and signature of the form. In $\mathbb{Q}$, it is much harder. As we move further away from algebraic closed fields, equivalence of quadratic forms over a field is harder to see.

In this chapter we will firstly explore the invariants of quadratic forms over $\mathbb{Q}_p$. Using the Hasse-Minkowski theorem, we can extend this result to find invariants of quadratic forms over $\mathbb{Q}$. This is called local-global principle, where we study what occurs locally on $\mathbb{Q}_p$ and extend it to the global field $\mathbb{Q}$.

6.1 Equivalence over $\mathbb{Q}_p$

We will firstly investigate equivalence of quadratic forms over $\mathbb{Q}_p$ where p is prime. We will show in this section, that two quadratic forms are equivalent over $\mathbb{Q}_p$ if and only if they have the same dimension, discriminant and Hasse-Witt invariant.

For this section, the relevant references are Jacobson's Basic algebra II [9] and Lam [12].

Proposition 6.1.1. *Suppose $n \leq 3$, then two non-degenerate quadratic forms on a n-dimensional vector space are equivalent if and only if they have the same discriminant and Hasse invariant.*

Proof. ($\Leftarrow$) The necessity of the condition is clear.

($\Rightarrow$) The sufficiency is clear if $n = 1$. Let $n = 2$ and let $Q = aX_1^2 + bX_2^2$, $Q' = a'X_1^2 + b'X_2^2$ be two quadratic forms. We assume that Q, Q' have same discriminant and Hasse Witt invariant. Then ab and $a'b'$ differs by square and $(a, b) \cong (a', b')$.

Since $(a,b) \cong (a',b')$, this implies that the quadratic forms generated from these quaternion algebras,

$$aX_1^2 + bX_2^2 - abX_3^2 \text{ and } a'X_1^2 + b'X_2^2 - a'b'X_3^2$$

are equivalent from Remark 4.1.10. Since $ab \backsim a'b'$, we have equivalence of $-abX_3^2$ and $-a'b'X_3^2$ and hence

$$aX_1^2 + bX_2^2 \text{ and } a'X_1^2 + b'X_2^2$$

by Witt's cancellation Theorem 2.2.5.

Now let $n = 3$, we have

$$Q = aX_1^2 + bX_2^2 + cX_3^2 \text{ and } Q' = a'X_1^2 + b'X_2^2 + c'X_3^2.$$

We have

$$s(Q) \backsim s(Q')$$

and

$$d = abc \text{ and } d' = a'b'c'$$

differs by a square so we can assume $d = d'$. It suffices to show that $-dQ$ and $-dQ'$, which have discriminant -1, are equivalent. Since

$$\begin{aligned}
\prod_{i<j}(-da_i, -da_j) &= \prod_{i<j}(-d,-d)(a_i,-d)(-d,a_j)(a_i,a_j) \\
&= s(Q)\prod_{i<j}(-d,-d)(a_i,-d)(-d,a_j) \\
&= s(Q)(-d,-d)^{\sum_{i<j}1}\prod_{i<j}(a_i,-d)(-d,a_j) \\
&= s(Q)(-d,-d)^3\prod_{i=1}^{n}(-d,a_i)^2 \\
&= s(Q)(-d,-d)
\end{aligned}$$

This gives

$$s(-dQ) \backsim s(Q) \otimes (-d,-d)$$

and it follows that $s(-dQ) \backsim s(-dQ')$, so it suffices to prove the result for Q and Q' of discriminant -1. Then we can assume that

$$Q = aX_1^2 + bX_2^2 - abX_3^2 \text{ and } Q' = a'X_1^2 + b'X_2^2 - a'b'X_3^2.$$

The Hasse invariant $s(Q) = (a,b)(a,-ab)(b,-ab) \backsim (a,b)(ab,-ab) \backsim (a,b)$ using Proposition 5.2.4 (2) and bilinearity of Hilbert symbol. Similarly, $s(Q') \backsim (a',b')$. As $s(Q) \backsim s(Q')$, then $(a,b) \cong (a',b')$. Considering Remark 4.1.10, since Q and Q' are the negatives of the norm form on $(a,b)_0$ and $(a',b')_0$ respectively, it follows that Q and Q' are equivalent. $\square$

Proposition 6.1.2. *Let k be a field such that every quadratic form on a five-dimensional vector space over k is isotropic. Then any two non-degenerate quadratic forms on a vector space V over k are equivalent if and only if they have same discriminant and Hasse invariant.*

Proof. ($\Rightarrow$) The necessity of the condition is clear.

($\Leftarrow$) Let $\dim Q = n$. The sufficiency holds by Proposition 6.1.1 above if $n \leq 3$. Now assume $n \geq 4$. The hypotheses implies that any non-degenerate quadratic form P on a four dimensional vector space U over k is universal. If $a \neq 0$, we can form $U \oplus kx$ where $x \neq 0$, and define a quadratic form R on $U \oplus kx$ by

$$R(u + \alpha x) = P(u) - \alpha^2 a \qquad \text{for } u \in U, \alpha \in k$$

The fact that R is isotropic implies that we have $u + \alpha x \neq 0$ such that $P(u) = \alpha^2 a$. If $\alpha = 0$ then $u \neq 0$, so P is a isotropic and hence P is universal. If $\alpha \neq 0$, then $P(\alpha^{-1}u) = a$. Thus P is universal. The universality of non-degenerate quadratic form on an four-dimensional spaces implies that Q is a non-degenerate quadratic forms on an n-dimensional vector space V, $n \geq 4$, then we have an orthogonal base $(v_1, ..., v_n)$ with $Q(v_i) = 1$ for $i > 3$. If R denotes the restriction of Q to $kv_1 + kv_2 + kv_3$, then the definitions and the formula $(1, a) = 1$ show that Q and R have the same discriminant and Hasse invariant. If Q' is a second non-degenerate quadratic form on an n-dimensional vector space, then we have an orthogonal base $(v_1', ..., v_n')$ with $Q(v_i') = 1$ for $i > 3$. The that $s(Q) = s(Q')$ and Q and Q' have the same discriminant implies the same conditions on the restriction of Q and Q' to $kv_1 + kv_2 + kv_3$ and $kv_1' + kv_2' + kv_3'$. Hence these restriction are equivalent and so Q and Q' are equivalent. □

Definition 6.1.3. *A quaternion algebra A over k is split if $A \cong M_2(k)$. A field K containing k is a* splitting field *for A if $A \otimes_k K$ is split.*

Proposition 6.1.4. *The quadratic form $Q = a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^4$ with $d = a_1a_2a_3a_4 \neq 0$ is isotropic if and only if $k(\sqrt{d})$ is a splitting field for $(-a_3a_4, -a_2a_4)$*

Proof. Let $a = -a_3a_4$, $b = -a_2a_4$, $c = a_2a_3a_4$. Now cQ is equivalent to $dX_1^2 - aX_2^2 - bX_3^2 + abX_4^2$. We have $-aX_2^2 - bX_3^2 + abX_4^2$ is the norm form on $(a, b)_0 = (-a_3a_4, -a_2a_4)_0$. Suppose $\sqrt{d} \in k$, then $k(\sqrt{d}) = k$. In this case, cQ is equivalent to $X_1^2 - aX_2^2 - bX_3^2 + abX_4^2$, which is the norm form of (a, b). Now $(a, b) \backsim 1$ if and only if the norm form is isotropic. This implies k is a splitting field of $(a, b) = (-a_3a_4, -a_2a_4)$ if and only if Q is isotropic. Now suppose $\sqrt{d} \notin k$, then $k(\sqrt{d})$ is a splitting field of (a, b) if and only if $k(\sqrt{d})$ is a subfield of (a, b). This occurs if and only if $(a, b)_0$ contains element u such that $u^2 = d$, and this is true if and only if cQ, and therefore Q, is isotropic. □

Lemma 6.1.5. *Suppose A is a quaternion algebra over field k, let $W \subseteq A$ be a subfield with degree 2 over A, then W splits A over k.*

Proof. Let $W = k(\sqrt{d})$. Consider the map

$$W \otimes W \hookrightarrow W \otimes A$$

Consider the elements $d \otimes 1, \sqrt{d} \otimes \sqrt{d} \in W \otimes W$. As

$$\begin{aligned}
&(d \otimes 1 + \sqrt{d} \otimes \sqrt{d})(d \otimes 1 - \sqrt{d} \otimes \sqrt{d}) \\
&= d^2 \otimes 1 - d \otimes d \\
&= d^2 \otimes 1 - d^2 \otimes 1 \\
&= 0
\end{aligned}$$

This implies there exists non-trivial element in $x, y \in W \otimes A$ such $xy = 0$. It follows that $W \otimes A$ is not a division algebra, hence W splits A over k. □

The following two propositions are from Jacobson [9], however as we are working over $\mathbb{Q}_p$ instead of an arbitrary local field, we will use a different approach to prove these propositions. The proof in Jacobson [9] requires knowledge of residue field and cyclic algebras, which is not covered in this thesis.

Proposition 6.1.6. *Let $k = \mathbb{Q}_p$ where $p \neq 2$ and let A be a quaternion division algebra over k. Then any quadratic extension field K/k is a splitting field for A.*

Proof. Let $A = (a, p) = k\langle\sqrt{a}, \sqrt{p}\rangle$ be a quaternion division algebra. This implies that a, p are not squares in k. Consider the two case for the extension field $k(\sqrt{a_i p^i + ...})$:

In the first case suppose i is even. We can remove all the squares and hence $k(\sqrt{a_i p^i + ...}) = k(\sqrt{a_i + ...})$. If we have $a_0 + a_1 p + ...$,

$$a_0 + a_1 p + ... = a_0^{-1}(1 + b_1 p + ...)$$

By Theorem 5.2.11 we have $(1 + b_1 p + ...) \in k^{*2}$ and hence

$$a_0 + a_1 p + ... = a_0^{-1} c^2$$

Therefore $a_0 \times (a_0 + a_1 p....) = c^2$. Hence we can write $k(\sqrt{a_i + ...}) = k(\sqrt{a_i})$.

If a_i is a square, then we are done. Suppose a_i is not a square, then as a is also not a square, we have aa_i^{-1} is a square. We can see this from bilinearity of Legendre symbol. First note that by definition

$$\left(\frac{a_i^{-1}}{p}\right) = \left(\frac{a_i}{p}\right)^{-1} = -1 \qquad \left(\frac{a}{p}\right) = -1$$

then

$$\left(\frac{aa_i^{-1}}{p}\right) = \left(\frac{a_i^{-1}}{p}\right)\left(\frac{a}{p}\right) = 1$$

Hence, we can write $k(\sqrt{a_i}) = k(\sqrt{a_i \times aa_i^{-1}}) = k(\sqrt{a})$ which is subfield of (a, p).

In the second case suppose i is odd. We have $k(\sqrt{a_i p^i + ...})$ and similar to above, we can write it as $k(\sqrt{a_i p})$. If $a_i \in \mathbb{Q}_p^{*2}$, then we are done as the extension

field becomes $k(\sqrt{p})$ which is a subfield of $(a,p) = k\langle\sqrt{a},\sqrt{p}\rangle$. If $a_i \notin \mathbb{Q}_p^{*2}$, then as $a_i a^{-1}$ is a square $k(\sqrt{a_i p}) = k(\sqrt{ap})$ which is also a subfield of (a,p).

Hence, all extension field is a subfield with degree 2 over A. Following Lemma 6.1.5 from above, we can conclude that any quadratic field K/k is a splitting field for A. □

Proposition 6.1.7. *We have $(-1,-1)_p = 1$ over $\mathbb{Q}_p$ where $p \neq 2$.*

Proof. We first want to show that

$$(a, \pm p) = \begin{cases} 1 & \text{if } a \in \mathbb{Q}_p^{*2} \\ -1 & \text{if } a \notin \mathbb{Q}_p^{*2} \end{cases} \tag{6.1.1}$$

If $a \in \mathbb{Q}_p^{*2}$, this is clear by Proposition 5.2.4. Suppose $a \notin \mathbb{Q}_p^{*2}$, then for a contradiction assume $(a, \pm p) = 1$. This implies that there exists non-trivial solution (z,x,y) to $X_1^2 - aX_2^2 \pm pX_3^2 = 0$ where $z, x \in \mathbb{U}_p$ is invertible and $y \in \mathbb{Z}_p$ by Lemma 5.2.12, then

$$z^2 - ax^2 \pm py^2 = 0$$

and

$$z^2 - ax^2 = 0 \bmod p$$

Hence it follows that $a = (\frac{z}{x})^2$ is a square which is a contradiction. Thus, the proposition follows from (6.1.1) above that

$$(-1,-1) = (-1,p)(-1,-p)^{-1} = 1$$

as required. □

Proposition 6.1.8. *Any non-degenerate quadratic form Q on a five-dimensional vector space over $\mathbb{Q}_p$ is isotropic.*

Proof. Suppose $Q = \sum_{i=1}^5 a_i X_i^2$ and assume if we multiple Q by $\prod_{i=1}^5 a_i$ we may assume that $\prod_{i=1}^5 a_i$ is a square. Suppose Q is not isotropic, then $\sum_{i=1}^4 a_j X_j$ is not isotropic. Otherwise, if $\sum_{i=1}^4 a_j X_j$ is isotropic, $\sum_{i=1}^5 a_j X_j$ is isotropic. This is because if there is non-trivial solution $(x_1, ..., x_4)$ such that $a_1x_1^2 + ... + a_4x_4^2 = 0$, then $a_1x_1^2 + ... + a_4x_4^2 + a_5(0)^2 = 0$ and $(x_1, ..., x_4, 0)$ is non-trivial.

Now since Q is not isotropic, by Proposition 6.1.4, $k(\sqrt{a_1a_2a_3a_4})$ is not a splitting field for $(-a_3a_4, -a_2a_4)$. Then $(-a_3a_4, -a_2a_4) \not\sim 1$. By Proposition 6.1.6, it follows that $a_1a_2a_3a_4$ is a square. Hence a_5 is a square as we assume $\prod_{i=1}^5 a_i$ is a square. Similarly, we can also show that every a_i is a square and hence we can write $Q = \sum_{i=1}^5 X_i^2$. Hence $(-1,-1) \not\sim 1$ by Proposition 6.1.4. This contradicts Proposition 6.1.7 if $p \neq 2$. Now suppose this is $p = 2$. We know that $\mathbb{Q}_2$ contains $\sqrt{-7}$. Note that by Hensel's lemma, $x^2 + x + 2$ is reducible in $\mathbb{Q}_2$. $\mathbb{Q}_2$ contains $\frac{1}{2}(-1 \pm \sqrt{-7})$ and hence $\mathbb{Q}_2$ contains $\sqrt{-7}$. Then $1^1 + 1^1 + 1^1 + 2^2 + (\sqrt{-7})^2 = 0$. This implies that $\sum_{i=1}^5 a_j X_j$ is isotropic in $\mathbb{Q}_2$. Hence we have Q is isotropic over all $\mathbb{Q}_p$ we required. □

By Proposition 6.1.2 and Proposition 6.1.8, we have the following important theorem which classifies all quadratic forms over $\mathbb{Q}_p$.

Theorem 6.1.9. *Any two non-degenerate quadratic forms Q, Q' on a n-dimensional vector space over $\mathbb{Q}_p$ are equivalent if and only if they have the same discriminant and Hasse invariant.*

This theorem gives us equivalence of quadratic over $\mathbb{Q}_p$ by dimension, discriminant and Hasse-invariant. One question which we might want to to know is over which $\mathbb{Q}_p$ are two quadratic forms equivalent. We will show the power of Theorem 6.1.9 with an example, but first we will introduce a lemma for easy calculation of Hasse-Witt invariant.

Lemma 6.1.10. *If $a, b \in \mathbb{Z}_p^*$ (i.e. $p \nmid a$ and $p \nmid b$), then $(a,b)_p = 1$ for $p \neq 2$ and $(a,b)_p = (-1)^{\epsilon(u)\epsilon(v)}$ for $p = 2$.*

Proof. Clear from the formulas for the Hilbert Symbol in Proposition 5.2.15 since we have $\alpha = \beta = 0$. □

The following example is from [12] Lam's book on p.167, we will however use a different approach from the book to prove or disprove equivalence. We will use the previous Theorem.

Example 6.1.11. *Consider two quadratic form*

$$Q = X_1^2 - 6X_2^2 + 15X_3^2 \quad \textit{and} \quad Q' = 3X_1^2 - 10X_2^2 + 3X_2^3$$

we wish to see over which $\mathbb{Q}_p$ is Q equivalent to Q'. First note that they both have same dimension and same discriminant since the product of the coefficient for both quadratic forms are $-2 \times 3^2 \times 5$. Hence, by the previous Theorem, we need their Hasse invariants to be equal if Q is equivalent to Q' over $\mathbb{Q}_p$.

For $p \nmid 2, 3, 5$, both Q and Q' has the same Hasse invariant equals 1 over $\mathbb{Q}_p$, which is clear following Lemma 6.1.10. Hence Q and Q' are equivalent over $\mathbb{Q}_p$ for all $p \nmid 2, 3, 5$.

Consider the quadratic forms over $\mathbb{Q}_2$. It is clear from Proposition 5.2.15 and Lemma 6.1.10 that

$$s(Q) = (1,-6)_2(1,15)_2(-6,15)_2 = 1$$

$$s(Q') = (3,-10)_2(3,3)_2(-10,3)_2 = -1$$

Hence Q and Q' are not equivalent over $\mathbb{Q}_2$. We can calculate $s(Q)$ using the fact that $(a, c^2) = 1$ and Hilbert symbol is symmetric.

Over $\mathbb{Q}_3$

$$s(Q) = (1,-6)_3(1,15)_3(-6,15)_3 = 1$$

$$s(Q') = (3,-10)_3(3,3)_3(-10,3)_3 = -1$$

Hence Q and Q' are not equivalent over $\mathbb{Q}_3$.

Over $\mathbb{Q}_5$

$$s(Q) = (1,-6)_5(1,15)_5(-6,15)_5 = 1$$

$$s(Q') = (3,-10)_5(3,3)_5(-10,3)_5 = 1$$

Hence Q and Q' are equivalent over $\mathbb{Q}_5$.

Now, I will give an interesting remark of what I have noticed about equivalence of quadratic over $\mathbb{R}$. First recall that from Sylvester's law of inertia, two quadratic forms over $\mathbb{R}$ are equivalent if and only if they have the same dimension and signature (r, s).

Remark 6.1.12. *The Hasse-Witt invariant over $\mathbb{R}$ depends mainly on the sign of the coefficients, which is similar to signature. Observe that Hasse-Witt invariant over $\mathbb{R}$ does not give as much information than the signature (r, s). Consider Proposition 5.2.15, the Hasse-Witt invariant over $\mathbb{R}$ only depends on the number of negative coefficients s. We have for the Hasse-Witt invariant $s(Q)$ over $\mathbb{R}$,*

$$s(Q) = \begin{cases} 1 & s(s-1)/2 \text{ is even} \\ -1 & s(s-1)/2 \text{ is odd} \end{cases}.$$

While dimension, discriminant and Hasse-Witt invariant classify quadratic form over $\mathbb{Q}_p$, this does not hold for $\mathbb{Q}_\infty := \mathbb{R}$. Clearly two quadratic form over $\mathbb{R}$ with two different signature $(5, 3), (1, 7)$ are not equivalent. However both have dimension $= 8$, discriminant $= -1 \in \mathbb{R}^*/\mathbb{R}^{*2}$ and Hasse-Witt invariant $= -1$.

6.2 Equivalence over $\mathbb{Q}$

After seeing the equivalence of quadratic form over $\mathbb{Q}_p$ in previous section, we are now ready to look at the equivalence over $\mathbb{Q}$. The main theorem in this section is the Hasse-Minkowski theorem which relates isotropy of quadratic forms over $\mathbb{Q}_p$ to forms over $\mathbb{Q}$. There are several ways to prove Hasse-Minkowski theorem, some proofs require basic class theory and other require Legendre theorem in number theory. We will use Legendre theorem to prove Hasse-Minkowski theorem. The Legendre theorem gives a condition of when a ternary quadratic form will have non-trivial solution.

The main reference for this section is Voight's incomplete book [19]. I will provide more details with the proofs which require a few more lemmas and corollary which are not in the book.

Theorem 6.2.1. *(Legendre) Let $a, b, c \in \mathbb{Z}$ be non-zero, square-free integers that are relatively prime in pairs. Then the quadratic form*

$$aX^2 + bY^2 + cZ^2 = 0$$

has non-trivial solution if and only if $-ab, -bc, -ac$ are quadratic residues modulo $|c|, |a|, |b|$ respectively.

Proof. ($\Leftarrow$) The condition for have non-trivial solution are indeed necessary. The condition on signs is necessary for a solution in $\mathbb{R}$. If $ax^2+by^2+cz^2 = 0$ with $x, y, z \in \mathbb{Q}$ not all zero, then scaling we may assume that $x, y, z \in \mathbb{Z}$ satisfy $\gcd(x, y, z) = 1$. If $p \mid c$ then $p \nmid y$, otherwise we have $p \mid x$ and $p \mid z$ and $\gcd(x, y, z) \neq 1$ which is a contradiction to $\gcd(x, y, z) = 1$. So

$$\left(\frac{x}{y}\right)^2 \equiv \left(\frac{-b}{a}\right) \bmod |c|$$

so $-ba$ is a quadratic residue module $|c|$. Similarly, the other conditions also holds by symmetry.

($\Rightarrow$) So suppose the conditions hold. We can multiply and rescale by squares, so we can assume that a and b are square free integers and $c = -1$. We have have $aX^2 + bY^2 = Z^2$ and wish to want to look for non-trivial solution. If $a \in \mathbb{Q}^{*2}$, then we have solution $(x, y, z) = (1, 0, \sqrt{a})$. Now, suppose $a \notin \mathbb{Q}^{*2}$, we need to solve

$$\frac{z^2 - ax^2}{y^2} = b = N_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}\left(\frac{z + x\sqrt{a}}{y}\right)$$

for $x, y, z \in \mathbb{Q}$ and $y \neq 0$. Hence we only need to show that b is a norm from $\mathbb{Q}(\sqrt{a})$. By our assumption a, b are not both negative and

$$b \text{ is a square module } |a| \qquad a \text{ is a square module } |b|$$

Also assume that $|a| \leq |b|$. Using induction on $m = |a| + |b|$. If $m = 2$, we have

$$\pm x^2 \pm y^2 = z^2$$

where have solution unless both signs are negative.

Now suppose $m > 2$, which implies $|b| \geq 2$. By assumption a is a square mod $|b|$, there exists t, b' such that

$$t^2 = a + bb'$$

Note that b' is also a square module $|a|$ and a is also a square module $|b'|$. We can choose t such that $|t| \leq \frac{|b|}{2}$. The formula

$$bb' = t^2 - a = N_{k(\sqrt{a})/k}(t + \sqrt{a})$$

shows that bb' is a norm of the extension $k(\sqrt{a})/k$ where $k = \mathbb{Q}$ or $\mathbb{Q}_v$. So b is a norm if and only if b' is a norm. But we have:

$$|b'| = \left|\frac{t^2 - a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|$$

Write $b' = b''u^2$ where $u \in \mathbb{Z}$ and b'' square free. Then $|b''| \leq |b'| < |b|$ and b'' is a norm if and only if b' is a norm. As b' is also a square module $|a|$ and a is also a square module $|b'|$. This implies that

$$b'' \text{ is a square module } |a| \qquad a \text{ is a square module } |b|$$

since $b' = b''u^2$. The induction hypothesis applies to the equation $ax^2 + b''y^2 = z^2$. Hence b'' is a norm, which implies b' is norm. This also implies b is a norm. Hence we have non-trivial solution to $aX^2 + bY^2 = Z^2$, completing the proof. □

To prove Hasse-Minkowski theorem, we will need the following corollary from Legendre theorem. This corollary give condition of when Q is isotropic over $\mathbb{Q}$.

Corollary 6.2.2. *Let Q be a non-degenerate ternary quadratic form $aX^2 + bY^2 + cZ^2$. Then Q is isotropic over $\mathbb{Q}$ if and only if Q is isotropic over $\mathbb{Q}_v$ for all (but one places) v.*

Proof. Clearly if Q is isotropic over $\mathbb{Q}$, then Q is isotropic over $\mathbb{Q}_p$. Conversely, assume that Q is isotropic over all $\mathbb{Q}_p$ for all p. Similar to the proof for Legendre theorem, we can rescale such that we have $Q = aX^2+bY^2-Z^2$. Since Q is isotropic over $\mathbb{R}$, it follows that a, b cannot both be negative. Now suppose p is an odd prime and $p \mid a$. If $\mathbb{Q}_p$ is isotropic then $(a, b)_p = \left(\frac{b}{p}\right) = 1$ as b has to be a square modulo p. Since this is true for all p where $p \mid a$, then we can conclude that b is square modulo $|a|$. By symmetry, the same holds so a is square modulo $|b|$. Using Legendre theorem above, it follows that Q is isotropic over $\mathbb{Q}$. □

The proof of the following two lemmas, which are needed to prove Hasse-Minkowski theoream, were omitted from Voight's incomplete book [19]. I altered the proof of Proposition 2.1.11 to prove the following lemma.

Lemma 6.2.3. *Let $Q = P \perp R$ be an orthogonal sum of two non-degenerate quadratic forms over a field k. The quadratic form Q is isotropic if and only if there exists $c \in k$ that is represented by both P and R.*

Proof. ($\Leftarrow$) This is clear.

($\Rightarrow$) A non-trivial solution of Q can be written in the from (x, y) where $Q(x, y) = P(x) - R(y) = 0$. That is $P(x) = R(y)$. If $c = P(x) = R(y)$ is non-zero, that we are done. Suppose $c = 0$, then at least one of x, y is non-trivial zero of P and R respectively. Without loss of generality, assume y is non-trivial zero of R. The following argument is similar to the one we used in Proposition 2.1.11. Since R is non-degenerate, there exist z such that $\beta_R(y, z) = 1$. Then the element $w = z - R(z)y$ is also an isotropic element so $R(w) = 0$. Now, for all $a \in k$, R represent a with $R(y+aw)$. Hence if $c = 0$, then R is isotropic and hence represents all element of k, in particularly all non-zero values represent by P. □

The proof of the following lemma was done with my supervisor.

Lemma 6.2.4. *Given $t_p \in \mathbb{Q}_p^*$ and $d = p_1^{n_1}p_2^{n_2}....p_s^{n_s}$, there exists $t \in \mathbb{Q}^*$ such that*

1. *$t \in t_p\mathbb{Q}_p^{*2}$ for all primes $p \mid d$*
2. *t and t_∞ have the same sign*
3. *$p \nmid t$ for all primes $p \nmid d$ except for possibly one prime $q \nmid d$*

Proof. Since $t_p \in \mathbb{Q}_p^*$, multiplying by a square, we can assume that $t_p = a_0+a_1p_1+...$ where a_o, a_1 cannot both be zero. Then for some $r, s \in \mathbb{N}$ we have congruence

$$\begin{aligned} t_{p_1} &= b_1 \bmod p_1 \\ &... \\ t_{p_r} &= b_r \bmod p_r \\ t_{p_{r+1}} &= b_{r+1}p_{r+1} \bmod p_{r+1}^2 \\ &... \\ t_{p_s} &= b_sp_s \bmod p_s^2 \end{aligned}$$

We want to find $b \bmod p_1...p_s$ such that

$$b \equiv \begin{cases} b_i(p_{r+1}...p_s)^{-1} \bmod p_i & \text{if } i \leq r \\ b_i(p_{r+1}...\hat{p_i}...p_s)^{-1} \bmod p_i & \text{if } i > r \end{cases}$$

By Chinese remainder theorem, we have unique solution of $b \bmod p_1p_2....p_s$ which satisfies the above congruences. Using Dirichlet's theorem on arithmetic progressions, we have infinite primes in the set

$$\{b + (p_1p_2....p_s), b + 2(p_1p_2....p_s), ..., b + k(p_1p_2....p_s), ...\}$$

Then we can choose one such that $q \in \{b + k(p_1p_2....p_s) | k \in \mathbb{N}\}$ such that $p \nmid q$ for all $p \nmid d$. We let $t = qp_{i+1}...p_s$ and we have the properties that stated above for this lemma. As

$$\begin{aligned} t &= t_{p_1} \bmod p_1 \\ &... \\ t &= t_{p_r} \bmod p_r \\ t &= t_{p_{r+1}} \bmod p_{r+1}^2 \\ &... \\ t &= t_{p_s} \bmod p_s^2 \end{aligned}$$

Note that $p \nmid t$ for all primes $p \nmid d$except for one prime $q \nmid d$. Then second properties is easy to satisfy by choosing t such that has the same sign as t_∞.

□

We can now state and prove the main theorem of this chapter, Hasse-Minkowski theorem.

Theorem 6.2.5. *(Hasse-Minkowski theorem) A quadratic form Q over $\mathbb{Q}$ is isotropic if and only if Q_v is isotropic over $\mathbb{Q}_v$ for all v.*

Proof. We may assume that Q is non-degenerate in $n \geq 1$ variables. Firstly, ($\Rightarrow$) is trivial. Now, we only need to consider ($\Leftarrow$).

1. Suppose $n = 1$, there is no non-trivial solution in any field.
2. Suppose $n = 2$, the we can rescale and assume that $Q = x^2 - ay^2$ where $a \in \mathbb{Q}^*$. We can write $a = \prod_p p^{\nu_p(a)}$. Since Q_p is isotropic for all primes p, then
$$a = \left(\frac{x}{y}\right)^2$$
and hence $a \in \mathbb{Q}_p^{*2}$. Hence $\nu_p(a)$ is even for all primes p. Since Q is isotropic in $\mathbb{Q}_\infty$, we have $a > 0$. Thus by unique factorisation, as all p has even power, we have $a \in \mathbb{Q}^2$. It follows that Q is isotropic over $\mathbb{Q}$.
3. Proven in Corollary 6.2.2 for ternary quadratic forms.

4. $n \geq 4$ We write

$$Q = \langle a, b \rangle \perp Q'$$

where $Q' = \langle c_1, ..., c_{n-2} \rangle$ and $a, b, c_i \in \mathbb{Z}$ for all i. Let $d = 2ab(c_1....c_{n-2}) \neq 0$. For each prime $p \mid d$, since Q is isotropic, then there exists $t_p \in \mathbb{Q}_p^*$ represented by $\langle a, b \rangle$ and Q' from Lemma 6.2.3. Similarly, there exist $t_\infty \in \mathbb{R}^*$ represented by these forms in $\mathbb{R}$. By Lemma 6.2.4, there exists $t \in \mathbb{Q}^*$ such that the quadratic form $\langle a, b, -t \rangle$ isotropic for all $p \mid d$ and at ∞ by construction and at all primes $p \nmid d$ except $p = q$ as $p \nmid abt$. Therefore, by using Corollary 6.2.2, the form $\langle a, b, -t \rangle$ is isotropic.
It remains to prove that $Q'' = \langle -t \rangle \perp Q'$ is isotropic on $\mathbb{Q}$. If $n = 4$, then $Q'' = \langle c_1, c_2, -t \rangle$ is also isotropic by same argument. Suppose $n \geq 5$, we will use induction on n. Since we have Q''_v is isotropic at $v = \infty$ and all $v = p \mid d$ by construction, and all for $v = p \nmid d$ the completion Q''_p is non-degenerate form in ≥ 3 variables over $\mathbb{Z}/p\mathbb{Z}$ and so is isotropic by the Lemma 5.2.14. We can use Hensel's lemma to lift a solution in $\mathbb{Z}_p$. Then as Q''_v is isotropic over all v except for possibly one place q, by the induction hypothesis, we have that Q'' is isotropic over $\mathbb{Q}$.
Hence, we have shown that $\langle a, b \rangle$ represents $t \in \mathbb{Q}^*$ and Q' represents $t \in \mathbb{Q}^*$. Then by Lemma 6.2.4, $Q = \langle a, b \rangle \perp Q'$ is isotropic over $\mathbb{Q}$. Hence Q is isotropic over $\mathbb{Q}$.

□

We now have this corollary for representation of elements.

Corollary 6.2.6. *Let Q be a quadratic form $\mathbb{Q}$ and let $u \in \mathbb{Q}^*$. Then Q represents u over $\mathbb{Q}$ if and only if Q represents u over $\mathbb{Q}_v$ for all v.*

Proof. Consider the quadratic form $Q \perp \langle -u \rangle$. This is isotropic over $\mathbb{Q}$ if and only it is isotropic over $\mathbb{Q}_v$ by Theorem 6.2.5 (Hasse-Minkowski theorem). With Proposition 2.1.11, this implies Q represents u over $\mathbb{Q}$ if and only if Q represents u in all $\mathbb{Q}_v$. □

Now we have classification over $\mathbb{Q}$ with a corollary from the Hasse-Minkowski theorem.

Corollary 6.2.7. *Two quadratic forms over $\mathbb{Q}$ are equivalent if and only if they are equivalent over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all p.*

Proof. Firstly, ($\Rightarrow$) is clear. If $Q \cong Q'$ over $\mathbb{Q}$, then $Q \cong Q'$ over $\mathbb{Q}_v$ for all v (including ∞). Now, we only need to consider ($\Leftarrow$). We will prove this by induction on number of variables. Assume Q, Q' are non-degenerate and $Q_v \cong Q'_v$ for all v by Corollary 6.2.6. Let $u \in \mathbb{Q}^*$ be represented by Q, then Q_v represents u for all v by Corollary 6.2.6. As $Q_v \cong Q'_v$, it follows that Q'_v represent u for all v. Hence Q' represents u by Corollary 6.2.6. Thus we can write $Q \cong \langle u \rangle \perp Q_1$ and $Q' \cong \langle u \rangle \perp Q'_1$. Hence by Witt cancellation (Theorem 2.2.5) as $Q_v \cong Q'_v$, we have $(Q_1)_v \cong (Q'_1)_v$ for all v. By induction hypothesis, we have $Q_1 \cong Q'_1$. Thus, it follows that $Q \cong Q'$. □

Using the above theorem and the classification of quadratic forms over $\mathbb{Q}_v$ and $\mathbb{R}$, we obtain a complete set of invariants for quadratic forms over $\mathbb{Q}$.

Theorem 6.2.8. *Two quadratic forms over $\mathbb{Q}$ are equivalent if and only if they have the same dimension, discriminant, signature (as forms over $\mathbb{R}$) and Hasse-Witt invariant (over all $\mathbb{Q}_p$).*

These invariants allow us to distinguish whether two quadratic form are equivalent over the field $\mathbb{Q}$. Consider the example below.

Example 6.2.9. *The quadratic forms*

$$Q = 5X_1^2 + 11X_2^2 - 13X_3^2 \text{ and } Q' = 5X_1^2 - 11X_2^2 + 13X_3^2$$

are equivalent over $\mathbb{R}$, $\mathbb{Q}_3$, $\mathbb{Q}_5$ and $\mathbb{Q}_{13}$, but not over $\mathbb{Q}_{11}$. Hence they are not equivalent over $\mathbb{Q}$ by Theorem 6.2.5 (Hasse-Minkowski theorem).

Proof. The two quadratic forms have same dimension = 3 and both quadratic forms have same signature over $\mathbb{R}$. Hence they are equivalent over $\mathbb{R}$. The two quadratic forms have same discriminant d as the product of coefficients of these two quadratic forms equal to -715.

We shall look at the Hasse-Witt invariant over $\mathbb{Q}_3$, it is clear from Lemma 6.1.10 that as $3 \nmid 5, 11, 13$ then all the Hilbert symbols equal to 1 hence

$$s(Q) = 1 = s(Q')$$

Hence the two quadratic form are also equivalent over $\mathbb{Q}_3$.

Now, looking over $\mathbb{Q}_5$, we use Proposition 5.2.15 to calculate the Hasse-Witt invariant.

$$s(Q) = (5,11)_5(5,-13)_5(11,-13)_5 = \left(\frac{11}{5}\right)\left(\frac{-13}{5}\right) = \left(\frac{1^2}{5}\right)\left(\frac{2}{5}\right) = -1$$

$$s(Q') = (5,-11)_5(5,13)_5(-11,13)_5 = \left(\frac{-11}{5}\right)\left(\frac{13}{5}\right) = \left(\frac{2^2}{5}\right)\left(\frac{3}{5}\right) = -1$$

Hence the two quadratic form are also equivalent over $\mathbb{Q}_5$.

Over $\mathbb{Q}_{13}$, the Hasse Witt invariants over $\mathbb{Q}_{13}$ are

$$s(Q) = (5,11)_{13}(5,-13)_{13}(11,-13)_{13} = \left(\frac{5}{13}\right)\left(\frac{11}{13}\right) = -1 \times -1 = 1$$

$$s(Q') = (5,-11)_{13}(5,13)_{13}(-7,13)_{13} = \left(\frac{5}{13}\right)\left(\frac{-11}{13}\right) = -1 \times -1 = 1$$

Thus the two quadratic forms are equivalent over $\mathbb{Q}_{13}$ because they have same Hasse-Witt invariant.

However, over $\mathbb{Q}_{11}$, the Hasse Witt invariant over $\mathbb{Q}_{11}$

$$s(Q) = (5,11)_{11}(5,-13)_{11}(11,-13)_{11} = \left(\frac{5}{11}\right)\left(\frac{-13}{11}\right) = \left(\frac{4^2}{11}\right)\left(\frac{3^2}{5}\right) = 1$$

$$s(Q') = (5,-11)_{11}(5,13)_{11}(-7,13)_{11} = \left(\frac{5}{11}\right)\left(\frac{13}{11}\right) = \left(\frac{4^2}{5}\right)\left(\frac{2}{11}\right) = -1$$

Hence the two quadratic spaces are not equivalent over $\mathbb{Q}_{11}$ because they have different Hasse-Witt invariant. This also implies that they are not equivalent over $\mathbb{Q}$. □

The following is an original corollary from the previous theorem (Theorem 6.2.8) which consider a special case of binary quadratic forms. We obtain a criteria for equivalence of binary quadratic forms which are easier to check.

Corollary 6.2.10. *Suppose we have two binary quadratic forms*

$$Q = aX_1^2 + bX_2^2 \text{ and } Q' = abX_1^2 + X_2^2$$

where a, b are positive square free integers and $\gcd(a,b) = 1$. The two quadratic forms Q, Q' are equivalent if and only if b is a square modulo a and a is a square modulo b.

Proof. Clearly, dimension, signature and discriminant of Q and Q' are the same. We will look at their Hasse invariant. By Theorem 6.2.8, these two quadratic forms are equivalent if their Hasse invariants are equal over $\mathbb{Q}_v$ for all v. We can write a and b as product of distinct primes, so $a = p_1....p_r$ and $b = q_1...q_s$. Over $\mathbb{Q}_{p_i}$ where $1 \leq i \leq r$, we have by Proposition 5.2.15,

$$s(Q) = (a,b)_{p_i} = \left(\frac{b}{p_i}\right)$$

$$s(Q') = (ab,1)_{p_i} = 1$$

and over $\mathbb{Q}_{q_j}$ where $1 \leq j \leq s$, we have

$$s(Q) = (a,b)_{q_i} = \left(\frac{a}{q_i}\right)$$

$$s(Q') = (ab,1)_{q_i} = 1.$$

Hence for $Q \cong Q'$, we need

$$\left(\frac{b}{p_i}\right) = 1 \text{ and } \left(\frac{a}{q_i}\right) = 1$$

for all $1 \leq i \leq r$ and $1 \leq j \leq s$. This implies $Q \cong Q'$ if and only if a is a square modulo b and b is a square modulo a. □

Chapter 7

Clifford modules and applications

Clifford algebras have very interesting properties and there are many applications of Clifford algebras besides classification of quadratic form. One such application is using Clifford modules to look at vector fields on spheres. In this section, the main reference is Husemoller's Fibre Bundle [7] chapter on vector fields on sphere as well as Hanh's book [6] on application of Clifford modules.

7.1 Clifford modules

Let k be a field and let D be a finite dimensional division algebra over k. Let V be the quadratic space over k and let $C(V)$ be its associated Clifford algebra. Let W be a finite dimensional vector space over D, then the homomorphism as D-algebras

$$\rho : C(V) \to End_D(W)$$

is called a *representation* of $C(V)$.

We will look at the dimension of Clifford modules using periodicity of Clifford algebras. This will give insight to the formula for calculating the Radon-Hurwitz numbers (in the next section). Let $Q_k = -X_1^2 - ... - X_k^2$ be the negative definite quadratic form on $\mathbb{R}^k$. We will denote $Cl_k = C(Q_k)$ to be the Clifford algebra generated by Q_k and let $Cl'_k = C(-Q_k)$ be the Clifford algebra generated by $-Q_k$.

Proposition 7.1.1. *As algebra over $\mathbb{R}$, we have $Cl_1 \cong \mathbb{C}$, $Cl_2 \cong \mathbb{H}$, and $Cl'_1 \cong \mathbb{R} \oplus \mathbb{R}$ and $Cl'_2 \cong M_2(\mathbb{R})$.*

Proof. First Cl_1 is two-dimensional over $\mathbb{R}$ with basis element 1 and e, where $e^2 = -1$. Hence $Cl_1 \cong \mathbb{C}$ by map $e \to i$ which is an isomorphism. Also Cl_2 is four dimensional with basis element $1, e_1, e_2, e_1e_2$, where $e_1^2 = e_2^2 = -1$ and $e_1e_2 = e_2e_1$. Mapping $1 \to 1$, $e_1 \to i$, $e_2 \to j$ and $e_1e_2 \to k$, we get an algebra isomorphism $Cl_2 \to \mathbb{H}$.

For Cl'_1, there are two basis elements 1 and e, where $e^2 = 1$. Now we map $1 \to (1, 1)$ and $e \to (1, -1)$, we get an algebra isomorphism $Cl'_1 \to \mathbb{R} \oplus \mathbb{R}$. For Cl'_2, there are four basis elements $1, e_1, e_2, e_1e_2$, where $e_1^2 = e_2^2 = 1$ and $e_1e_2 = -e_2e_1$. If we map

$$e_1 \to \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad e_2 \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

then we get algebra isomorphism $Cl'_2 \to \mathrm{M}_2(\mathbb{R})$. □

Theorem 7.1.2.

$$Cl_{k+2} \cong Cl'_k \otimes Cl_2 \cong Cl'_k \otimes \mathbb{H}$$
$$Cl'_{k+2} \cong Cl_k \otimes Cl'_2 \cong Cl_k \otimes M_2(\mathbb{R})$$

Proof. Let $e_1, ..., e_k$ and $e'_1, ..., e'_k$ be the generators of Cl_k and Cl'_k respectively. First, we define $u' : \mathbb{R}^{k+2} \to Cl_k \otimes Cl_2$ by

$$u'(e_i) = \begin{cases} 1 \otimes e_i & \text{for } 1 \leq i \leq 2 \\ e'_{i-2} \otimes e_1 e_2 & \text{for } 3 \leq i \leq k+2r \end{cases}$$

Then, we have for $i \leq 2$, $u'(e_i)^2 = (1 \otimes e_i)(1 \otimes e_i) = 1 \otimes e_i^2 = u'(e_i)^2 = 1 \otimes e_i^2 = -1$. For $i \geq 2$, $u'(e_i)^2 = e'^2_{i-1} \otimes e_1 e_2 e_1 e_2 = 1 \otimes 1(-1) = -1$. Note that $u'(e_i)u'(e_j + u'(e_j)u'(e_i) = 0$ for $i \neq j$. Therefore u' gives the map to $u : Cl_{k+2} \to Cl'_k \otimes Cl_2$. Since u carries distinct basis element into distinct basis elements, u is injective. Since the dimension is the same, this means that it is an isomorphism. For v, we need

$$v'(e_i) = \begin{cases} 1 \otimes e'_i & \text{for } 1 \leq i \leq 2 \\ e'_{i-2} \otimes e'_1 e'_2 & \text{for } 3 \leq i \leq k+2r \end{cases}$$

Then similar to above, we can show that v is an isomorphism and hence this completes the proof. □

Use the previous theorem twice and note that $Cl_4 \cong Cl'_4 \cong Cl_2 \otimes Cl'_2 \cong M_2(\mathbb{H})$, we have the corollary below.

Corollary 7.1.3.

$$Cl_{k+4} \cong Cl_k \otimes Cl_4 \cong Cl_k \otimes M_2(\mathbb{H})$$
$$Cl'_{k+4} \cong Cl'_k \otimes Cl'_4 \cong Cl'_k \otimes M_2(\mathbb{H})$$

Similarly, by the above corollary and noting that fact that $M_2(\mathbb{H}) \otimes M_2(\mathbb{H}) \cong M_{16}(\mathbb{R})$, we also have the following corollary.

Corollary 7.1.4.

$$Cl_{k+8} \cong Cl_k \otimes Cl_8 \cong Cl_k \otimes M_{16}(\mathbb{R})$$
$$Cl'_{k+8} \cong Cl'_k \otimes Cl'_8 \cong Cl'_k \otimes M_{16}(\mathbb{R})$$

Using the above corollary, we can obtain the table below, where b_k is the minimum dimension n such that $\mathbb{R}^n$ has the structure of Cl_{k-1}-module.

k	1	2	3	4	5	6	7	8	9
Cl_{k-1}	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$	$\mathbb{H} \oplus \mathbb{H}$	$M_2(\mathbb{H})$	$M_4(\mathbb{C})$	$M_8(\mathbb{R})$	$M_8(\mathbb{R}) \oplus M_8(\mathbb{R})$	$M_{16}(\mathbb{R})$
b_k	1	2	4	4	8	8	8	8	16

7.2 Vector field on sphere

In this section, we will finally see how Clifford algebras and modules are involved in finding linearly independent tangent field on vector fields on sphere. There are at least $\rho(n)$ linearity independent tangent vector field on the sphere S^{n-1}, where $\rho(n)$

is the Radon-Hurwtiz numbers. This number relates to Bott Periodicty of Clifford algebras.

The base field here is $\mathbb{R}$. Consider $\mathbb{R}^n$ and let $S^{n-1} = \{x \in \mathbb{R}^n | \, \|x\| = 1\}$ be the $n-1$-sphere.

Definition 7.2.1. *A* tangent vector field *on S^{n-1} is a continuous function $v : S^{n-1} \to \mathbb{R}^n$ such that $v(x) \perp x$ for all $x \in S^{n-1}$.*

Definition 7.2.2. *Let $v_1, ..., v_{n-1}$ be tangent vector field on S^{n-1}. They are said to be* point-wise linearly independent *if $\{v_1, ..., v_{n-1}\}$ is an independent set of vectors in $\mathbb{R}^n$ for all $x \in S^{n-1}$.*

To look at the lower bound on the number of linearly independent tangent vector field on sphere, we have the following theorem.

Theorem 7.2.3. *Suppose $\mathbb{R}^n$ is a Cl_k-module then there exists k point-wise linearly independent tangent vector fields on S^{n-1}. Or in another words, if $\mathbb{R}^n$ admits the structure of a Cl_k-module, then S^{n-1} admits k orthonormal vector fields.*

Proof. Since $\mathbb{R}^n$ is a Cl_k-module, we have a ring homomorphism $\rho : Cl_k \to M_n(\mathbb{R})$. Let $u_i = \rho(e_i)$. Then we have $u_1, ..., u_k$ are linear transformation of $\mathbb{R}^n$ into itself such that $u_i^2 = -1$ and $u_i u_j + u_j u_i = 0$ for $i \neq j$. There is an inner product $\langle x, y \rangle$ such that $\langle u_i(x), u_i(u) \rangle = \langle x, y \rangle$ for each $x, y \in \mathbb{R}^n$. Let $\Gamma = \langle u_1, ..., u_k \rangle$ be the group generated by $\{u_1, ..., u_k\}$. Let $(-,-)$ be any inner product of $\mathbb{R}^n$, then we can define an new inner product on $\mathbb{R}^n$ where

$$\langle x, y \rangle := \frac{1}{|\Gamma|} \sum_{\sigma \in \Gamma} (\sigma(x), \sigma(y))$$

and we have $\langle u_i(x), u_i(y) \rangle = \langle x, y \rangle$.

Now, we can show that $\{x, u_1(x), ..., u_k(x)\}$ are mutually orthogonal. Note that $\langle u_i(x), u_i(y) \rangle = \langle x, y \rangle$ and $u_i^2 = -1$. Then, we have

$$\begin{aligned} \langle u_i(x), x \rangle &= \langle u_i^2(x), u_i(x) \rangle \\ &= \langle -x, u_i(x) \rangle \\ &= -\langle u_i(x), x \rangle. \end{aligned}$$

This implies that $\langle u_i(x), x \rangle = 0$. Similar, note that $u_i u_j = -u_j u_i$ and $u_i^2 = -1$, we have

$$\begin{aligned} \langle u_i(x), u_j(x) \rangle &= \langle -x, u_i u_j(x) \rangle \\ &= \langle x, u_j u_i(x) \rangle \\ &= \langle u_j(x), -u_i(x) \rangle \\ &= -\langle u_i(x), u_j(x) \rangle \end{aligned}$$

for all $i \neq j$. This implies that $\langle u_i(x), u_j(x) \rangle = 0$. Thus $\{u_1, ..., u_k\}$ forms k vector fields on S^{n-1}.

□

Theorem 7.2.4. *For a given n, define $\rho(n)$ to be largest k such that $\mathbb{R}^n$ is a module over Cl_k. For $n = 16^a 2^b m$ with m odd and $0 \leq b \leq 3$ we have*

$$\rho(n) = 8a + 2^b$$

The $\rho(n)$ called the Radon-Hurwitz numbers.

Proof. The formula holds by inspection for $1 \leq n \leq 8$ from table in Section 7.1. For $n \geq 8$, we use the fact that $b_{k+8} = 16b_k$, which follows from $Cl_{k+8} = Cl_k \otimes \mathrm{M}_{16}(\mathbb{R})$ by Corollary 7.1.4. □

Example 7.2.5. $\mathbb{R}^4$ *admits Cl_4-module. This is since $4 = 2^2$, hence $\rho(n) = 8 \times 0 + 2^2 = 4$.*

Combining Theorem 7.2.3 and Theorem 7.2.4 above, we have obtain the lower bound of number of linearity independent tangent vector fields.

Theorem 7.2.6. *On the sphere S^{n-1}, there exists $\rho(n)$ point-wise linearly independent tangent vector fields.*

However, it can be shown that this lower bound is also the upper bound by Theorem 7.2.7 below, giving the number of linearly independent tangent vector field to be exactly $\rho(n)$. However the proof of Theorem 7.2.7 will be omitted in this thesis as it requires K-theory.

Theorem 7.2.7. *(Adams) The maximal number of vectors fields on S^{n-1} is precisely $\rho(n)$.*

Proof. Chapter 16 of Fibre Bundle [7]. □

Chapter 8

Conclusion

In this thesis, we have seen interesting relations between quadratic forms and Clifford algebras. In particular, we look at classifying quadratic forms over $\mathbb{Q}_p$ and $\mathbb{Q}$ using invariants. There are other ways to show classification of quadratic forms over $\mathbb{Q}_p$ and $\mathbb{Q}$ without involvement of Clifford algebra. We can see this in Serre's book [18], where he uses primarily number theory method to show the classification. However, the involvement of Clifford algebras is important as we are able to see the structure of the invariants and how they behave. This is particularly important when we want to generalize this to arbitrary field.

The classification of quadratic form can be extended to *arbitrary field* k (of the characteristic not 2). First, we say that two quadratic spaces V and V' are *Witt equivalent* if isotropic part of the quadratic form Q and Q' are equivalent. This forms an additive group the *Witt ring* with tensor product operation. The equivalence class of even-dimensional spaces gives the fundamental ideal $I(k)$ of $W(k)$. If we have V and V' be two quadratic spaces, then $V \cong V'$ if and only if $\dim V = \dim V'$ and $[V] = [V']$ in $W(k)$. Quadratic forms can be classified using cohomological invariants. For example, the *dimension* mod 2 induces an isomorphism $e_0 : W(k)/I(k) \to \mathbb{Z}/2\mathbb{Z}$. The discriminant induces an isomorphism $e_1 : I(k)/I^2(k) \to k^*/k^{*2}$. The Hasse-Witt invariant also gives a isomorphism $e_2 : I^2(k)/I^3(k) \to Br_2(k)$. In 1970 paper, Milnor conjectured that for every positive integer n, there exists a well-defined isomorphism

$$e_n : I^n(k)/I^{n+1}(k) \to H^n(k, \mathbb{Z}/2\mathbb{Z})$$

where $H^n(k, \mathbb{Z}/2\mathbb{Z})$ is a Galois cohomology group. This was proven in 2001 by Voevodsky and he was awarded the Fields Medal at the International Congress of Mathematicians in Beijing in 2002 for this his achievement. This gives us classification of quadratic form via "secondary invariants" over any field k where $char(k) \neq 2$. However, the question of whether it is possible to find a complete set of invariants defined on $W(k)$ is still unknown. See [5] and [1] for more details.

In this thesis and most of the literature on classifying quadratic forms, the field with characteristic 2 is avoided. The case where characteristic is 2 needed to be treated differently. However, with a theorem from Arf, we can also classify quadratic forms over such field given the field has the following property that every completely regular quadratic space of dimension > 4 is isotropic. Then every completely regular quadratic space V is uniquely determined (up to isomorphism) by its dimension, the Brauer class of its Clifford algebra and its Arf invariant. See [14] for more details.

References

[1] Bayer-Fluckiger, E. Book Review: Introduction to quadratic forms over fields. *Bulletin of the American Mathematical Society* **45**(3) (2008), 479

[2] Conrad, K. *Hensel's lemma*, Expository papers. www.math.uconn.edu/∽kconrad/blurbs/gradnumthy/hensel.pdf

[3] Dudley, U. *Elemetary number theory*, Second edition, W.H.Freeman and Company, San Francisco, 1969.

[4] Gille, P, and Szamuely, T. *Central simple algebras and Galois cohomology.* Vol. 101. Cambridge University Press, 2006

[5] Hahn, A. J. The Clifford Algebra in the Theory of Algebras, Quadratic Forms, and Classical Groups. In *Clifford Algebras* (2004) pp. 305-322. Birkhuser Boston.

[6] Hahn, A.J. *Quadratic algebra, Clifford algebras and Arithmetic Witt groups*, Springer-Verlag, Berlin and New York, 1994.

[7] Husemoller, D. *Fibre Bundle*, 3rd ed, New York: Springer-Verlag, 1994.

[8] Jacobson, N. *Basic Algebra I*, W. H. Freeman and Company, San Francisco, 1974.

[9] Jacobson, N. *Basic Algebra II*, W. H. Freeman and Company, San Francisco, 1989.

[10] Kitaoka,Y. *Arithmetic of quadratic forms*, Cambridge University Press, Cambridge, 1993.

[11] Krus, M.A. *Quadratic and Hermitian Forms over Rings*, Springer-Verlag, Berlin, 1991.

[12] Lam, T.Y. *Introduction to quadratic forms over fields.* American Mathematical Soc., 2005.

[13] Lerner, B. *The Brauer-Manin Obstruction to the Hasse Principle* , Honours thesis, UNSW, 2007.

[14] Lorenz ,F.(Munster) and P. Roquette ,P. (Heidelberg), *On the Arf invariant in historical perspective*, 2010. www.rzuser.uni-heidelberg.de/∽ci3/arf.pdf.

[15] Palais, R.S.,The Classification of Real Division Algebras, *The American Mathematical Monthly*, **75** (4) (1968), pp. 366-368.

[16] Reich, E. *Clifford Algebras and Isomorphisms*, Seminar Handout, www-math.mit.edu/∽dav/clifford.pdf.

[17] Schweber, N. *Brauer algebra and the Brauer group*, Expository papers, https://math.berkeley.edu/∽schweber/.

[18] Serre, J.P. *A Course in Arithmetic*, Springer-Verlag, New York, 1973

[19] Voight, J. *The arithmetic of quaternion algebras*, Incomplete book, 2012.

[20] Wadsworth A.R. Book review of A.J.Hahn's Quadratic algebras, Clifford algebras and arithmetic Witt groups, *Bulletin (New Series) of the American Mathematical Society*, **33**(4) (1996).