國立臺灣大學理學院數學研究所

碩士論文

Department of Mathematics

College of Science

National Taiwan University

Master Thesis

有理數上的四元素環

Quaternion Algebra over Rational Number Field

林運翔

Yun-Xiang Lin

指導教授：陳其誠 博士

Advisor: Ki-Seng Tan, Ph. D.

中華民國 103 年 8 月

August 2014

國立臺灣大學碩士學位論文
口試委員會審定書

有理數上的四元素環
Quaternion Algebra over Rational Number Field

本論文係林運翔君（r01221021）在國立臺灣大學數學系完成之碩士學位論文，於民國一〇三年七月十七日承下列考試委員審查通過及口試及格，特此證明

口試委員：陳其誠（簽名）

（指導教授）

陳榮凱

謝銘倫

陳君明

系主任、所長 ____________（簽名）

（是否須簽章依各院系所規定）

致謝

能夠在數學研究所完成這份論文，並獲得這個學位，我真的感謝很多人在我這段時間給予我的幫助。首先，在精神以及物質的支持上，我最需要感謝的是我的家人，包括我的父母與我的未婚妻明娴，他們總是在我最需要的時候給我加油與打氣，並且幫助我完成了很多做學問時沒有辦法顧到的事情，此外我的指導教授陳其誠老師，其宏大的人生觀教導我對人生很多面向的思考，讓我的視野有不一樣的啟發。

而在學術上，我最感謝的人就是我的指導教授陳其誠老師，總是不厭其煩地為我講解我不甚了解的定理，以舉例的方式來幫助我釐清問題的本質，在他的指導之下，很多模糊的觀念得以明朗。也感謝老師在學生寫論文的期間，不斷幫助學生，提供學生更為清晰的思考方向，也提供學生其他的研究路徑，使用更為傳統和基本的方式完成這份論文。也感謝口試委員：陳君明教授，陳榮凱教授，謝銘倫教授，在學生口試時提供寶貴修改的意見，幫助學生糾正在文字使用上的瑕疵，讓這份論文能夠更加完整。

而在台大數學研究所的時間，我也要感謝余家富老師以及楊策仲助教，兩位願意花相當的時間幫我把代數數論的基本底子建立起來，才能夠進入這個殿堂，進而完成論文。另外也要感謝張鎮華老師以及陳聖華助教，讓我在圖論的課程上有獲得很多數學上的思考。而我也要感謝，陳君明老師的密碼學讓我了解如何把數學的代數和數論跟實際應用方面做結合。此外，蔡宜洵老師也曾幫助學生釐清一些現代數學的觀念和傳統數學差別的觀念，學生也非常感謝。還有要感謝李國瑋先生對學生在使用 LaTeX 完成論文方面的幫助。並且，學生也非常感謝中研院的黃振芳先生對學生的鼓勵。

最後，我也感謝之前跟我一起討論課業的學長同學們：昱丞，彥勝，禮中，治廣，宗驛...，還有我的同門師兄弟們：膺任，家成，健樺，宗堂，在我們 meeting 時給我的一些靈感。另外也要謝謝系辦的各位朋友給我的許多幫助。

摘要

本論文主要不只是探討四元素環在有理數上的分類情況，也描述由他們所形成的 Brauer 群結構。

有理數上的四元素環大致可分為 2 乘 2 矩陣與可除環情況，而我們可以用 quadratic form 討論其同構狀況。由於 2 乘 2 矩陣均同構，故只需考慮可除環的情況，其可更進一步分為不同的同構狀況。

在局部域的情況，可說明其可除環均同構，並使用希爾伯特符號來分類其為 2 乘 2 矩陣或是可除環。

最後我們使用 Brauer 群來描述其分類，並且闡述其群運算方式，透過 Hasse-Minkowski 定理我們可以觀察在不同的地方做四元素環局部域的分類，則可以完全決定其在有理數上的分類。

關鍵字：漢彌爾頓四元素環，希爾伯特符號，Brauer 群，Hasse-Minkowski 定理

Abstract

This thesis not only classify all quaternion algebras over rational number field but also describe the group structure of the Brauer group formed by them.

The quaternion algebra over rational number field can be roughly classified into two types: the 2 by 2 matrix algebra and division rings. Since all 2 by 2 matrices are isomorphic, we only need to classify division rings into non-isomorphic classes.

We study the group of norms and the local Hilbert symbols and show that there are exactly two isomorphic classes of quaternion algebras over the local field unless the field is complex number field.

Finally, we classify the quaternion algebras over rational number field and define explicitly the group operation of the Brauer group. By Hasse-Minkowski theorem, a quaternion algebra over the rational number field determines a set of local data and such data determines the quaternion algebra.

Key words and phrases: Hamiltonian quaternion, group of norms, Hilbert symbol, Brauer group, Hasse-Minkowski theorem

Contents

Chapter 1

Introduction

The Hamiltonian quaternion $\mathbb{H}$ was first introduced by the Irish mathematician William Rowan Hamilton in 1843. In modern language, $\mathbb{H}$ is a 4 dimensional $\mathbb{R}$-algebra, with an $\mathbb{R}$-basis $\{1, i, j, k\}$ such that $i^2 = j^2 = -1$, $ij = -ji = k$ (which implies $k^2 = -1$).

For a element $x = a1+bi+cj+dk \in \mathbb{H}$, $a, b, c, d \in \mathbb{R}$, denote $\bar{x} = a1-bi-cj-dk$. Then $\|x\| := x\bar{x} = \bar{x}x = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$. Thus, if $x \neq 0$, then $\frac{1}{\|x\|}\bar{x}$ is actually the inverse of x. In other words, $\mathbb{H}$ is a division ring.

The simplicity and beauty in the structure of $\mathbb{H}$ has been fascinating me, since the first time I learned it. That is why I chose to study in my thesis the corresponding objects over $\mathbb{Q}$, namely, the 4-dimensional $\mathbb{Q}$-algebra that is also a division ring. Soon, I learned that it is even better to consider all quaternion algebras (see Definition 2.2.2) over a fixed number field, because their isomorphic classes form a group, called the Brauer group of quaternions (see §4.2).

Most references I have found are on the general theory of finite dimensional central simple algebras (see Definition 2.2.1) including quaternion algebras as a special subset. It turned out that to describe the complete story on the classification of all all central simple algebras would take much more effort than what I was originally thought. "But, it might be possible to prove all the related theorems just for the quaternion algebras instead, because most arguments used can be simplified and there could be even better short cuts to take", suggested my advisor, Professor

Ki-Seng Tan. I took his advice, and the result is this thesis. In it I not only classify all quaternion algebras over $\mathbb{Q}$ but also describe the group structure of the Brauer group formed by them, by using the language and the results in the standard book on *algebraic number theory*.

In Chapter 2, I describe the general theory of quaternion algebra over a field of characteristic different from 2.

Then in Chapter 3, the field is required to be the completion of a number field at certain place. We study the group of norms and the local Hilbert symbols and show that there are exactly two isomorphic classes of quaternion algebras over the field, unless the field is $\mathbb{C}$, then there is only one classes. Finally, in Chapter 4, we classify the quaternion algebras over $\mathbb{Q}$ and define explicitly the group operation of the Brauer group. We consider Theorem 9 as the main result of this thesis.

As mentioned before, this thesis does not contain anything new other than some of the proofs formed by piecing together known material and old arguments, and I am indebted to Professor Tan for many arguments used.

Chapter 2

Quaternion Algebras over a Field of Characteristic $\neq 2$

In this chapter, K denotes a field of characteristic $\neq 2$. All results in this Chapter can be found in standard references on central simple algebra. For example, [Wel, §IX]

In general, we have the following lemma:

Lemma 2.0.1. *Suppose K is a field and D is a 4-dimensional K-algebra that is a division ring. Then either D is a field or D is noncommutative and K is the center of D.*

Proof. Let L denote the center of D. Then $K \subset L$ and D is an L-algebra. Therefore, if $[L : K] = l$ and $\dim_L D = d$, then $ld = 4$. Therefore, $l = 1$, 2, or 4. If $l = 4$, then D is a field. It is sufficient to show that if D is noncommutative, then $l \neq 2$.

Suppose $l = 2$. Let α be an element of D not contained in L. Then $L[\alpha]$ is a commutative integral domain which is a finite dimensional vector space over L, and hence $L[\alpha] = L(\alpha)$, a non-trivial field extension of L. The dimension counting shows $D = L(\alpha)$, a field. This is absurd.

□

2.1 The fundamental theorem

Definition 2.1.1. *A quaternion division ring over a field K is a 4-dimensional K-algebra that is a division ring with K as its center.*

Let D be a quaternion division ring over K and let α be an element of D not contained in K. By the argument similar to the one used in the proof of Lemma 2.0.1, we know that $K(\alpha) = K[\alpha]$ is a non-trivial field extension of K. Then by the dimension counting, we know that $K(\alpha)/K$ is actually a quadratic extension. By the assumption $char.(K) \neq 2$, there is some element i such that $K(i) = K(\alpha)$ such that $i^2 = a \in K$. It follows that a is not a square of elements of K.

Consider the map $\phi_i : D \longrightarrow D$ that sends x to the conjugate $i \cdot x \cdot i^{-1}$. It is a K-linear transformation with $\phi_i \circ \phi_i = id$, the identity map. Since ϕ_i satisfies the equation $T^2 - 1 = 0$, its minimal polynomial has no multiple roots, and hence D can be decomposed as the direct sum of D^+, the 1-eigenspace of ϕ_i, and D^-, the -1-eigenspace of ϕ_i. It is clear that $K(i) \subset D^+$. Now if there were some $\beta \in D^+$ not contained in $K(i)$, then $K(i, \beta)$ would be a non-trivial field extension, and hence must equal D, by dimension counting. But, this is absurd, since D is non-commutative. Thus, we have $D^+ = K(i)$ and D^- is of dimension 2 over K.

Suppose $j \in D^-$ is a non-zero element. Then $K(j)$ is a quadratic extension, and hence

$$j^2 = cj + b, \text{ for some } b, c \in K.$$

Since ϕ_i is a ring homomorphism, we have $\phi_i(j^2) = \phi_i(j)^2 = (-j)^2 = j^2$. Hence $j^2 \in D^+$. Since $b \in D^+$, we must have $cj \in D^+$. But $cj \in D^-$, too. Hence $cj = 0$, and $j^2 = b$. Denote $k = ij$. Then direct computation shows $k \in D^-$, and hence j and k span the 2-dimensional space D^-.

Definition 2.1.2. *Let a and b be two non-zero elements in K. The associated cyclic algebra $\mathbb{H}(a, b)$ over K is defined to be the 4-dimensional K-algebra spanned by the basis $\{1, i, j, k\}$, with the identity $i^2 = a$, $j^2 = b$, $ij = -ji = k$.*

Thus, $\mathbb{H}(a,b)$ is a special case of the cyclic algebra discussed in [Wel, §IX.4, Proposition 11]. The above discussion proves the following theorem.

Theorem 1. *If D is a quaternion division ring over K, then $D = \mathbb{H}(a,b)$ for some $a, b \in K^*$.*

Note that if k is as above, then $k^2 = -ab$.

2.2 Basic properties of the cyclic algebra $\mathbb{H}(a,b)$

Definition 2.2.1. *A finite dimensional K-algebra is a central simple algebra over K if it is a simple ring (no non-trivial two sided ideal) with center K.*

Proposition 2.2.1. *The cyclic algebra $\mathbb{H}(a,b)$ is a central simple algebra over K.*

Proof. For $x, y \in \mathbb{H}(a,b)$, define $[x,y] := xy - yx$ so that $[x,y] = 0$ if and only if $xy = yx$. Write $x = \alpha_0 + a_1 i + \alpha_2 j + \alpha_3 k$, $\alpha_0, \alpha_1, \alpha_2, a_3 \in K$. Then

$$[i,x] = 2a\alpha_3 j + 2\alpha_2 k,$$

$$[j,x] = -2\alpha_3 bi - 2\alpha_1 k,$$

and

$$[ij,x] = 2b\alpha_2 i - 2a\alpha_1 j.$$

Thus, x is contained in the center of $\mathbb{H}(a,b)$, if and only if $\alpha_1 = \alpha_2 = \alpha_3 = 0$, which means $x = \alpha_0 \in K$.

Let $I \neq 0$ be a non-zero two sided ideal of $\mathbb{H}(a,b)$. We need to show $I = \mathbb{H}(a,b)$. If $K \cap I$ contains a non-zero element, then $1 \in I$, and hence $I = \mathbb{H}(a,b)$ as desired. Otherwise, choose an $x \in I$, and $x \notin K$. This means at least one of α_1, α_2, and α_3 is non-zero. Consider $u_3 := [i,[ij,x]] = -4a\alpha_1 k$, $u_2 := [j,[i,x]] = -4b\alpha_2 i$, and $u_3 := [k,[j,x]] = 4ab\alpha_3 j$. Then u_λ, $\lambda = 1,2,3$, are contained in I, and u_λ is a unit of $\mathbb{H}(a,b)$ if and only if $\alpha_\lambda \neq 0$. This shows I contains a unit of $\mathbb{H}(a,b)$, and hence $I = \mathbb{H}(a,b)$. □

The following theorem is a consequence of the general theory of central simple algebra. For instance, see [Wel, §IX.1]. Here we give a direct proof of it.

Theorem 2. *A* 4*-dimensional central simple algebra* $\mathbb{A}$ *is either a division ring, and hence a quaternion division ring, or isomorphic to the matrix algebra* $\mathrm{M}(2, K)$.

Proof. There are basic useful facts we are going to use. First, every $x \in \mathbb{A}$ generates a finite dimensional subalgebra $K[x] \subset \mathbb{A}$. Thus, if $d := \dim K[x]$, then $1, x, ..., x^d$ are linearly dependent over K. This implies that x satisfied a polynomial equation over K. For instance, if $x = c \in K$, then x satisfies a linear equation $T - c = 0$, and *vice versa.* Let $f_x(T) \in K[T]$ denote the minimal polynomial, namely, the lowest degree monic polynomial that has x as its root. Let $a_x \in K$ denote the constant term of f_x.

Note that we can write $f_x(T) = T \cdot g(T) + a_x$. If $a_x \neq 0$, then

$$x \cdot \frac{-g(x)}{a_x} = \frac{-g(x)}{a_x} \cdot x = 1,$$

and hence $x \in \mathbb{A}^*$. On the other hand, if $a_x = 0$, then $x \cdot g(x) = g(x) \cdot x = 0$. This implies $x \notin \mathbb{A}^*$, for otherwise we would have $g(x) = g(x) \cdot x \cdot x^{-1} = 0$, which contradicts to the fact that f_x is the minimal polynomial.

For each $x \in \mathbb{A}$, we set the principal left ideal $M_x := \mathbb{A} \cdot x$. Suppose $M_x = \mathbb{A}$. Then there exists some $y \in \mathbb{A}$ such that $y \cdot x = 1$. In particular, we have $g(x) = y \cdot x \cdot g(x) = -y \cdot a_x$. But, since the degree of $g(T)$ is less than that of $f_x(T)$, we must have $g(x) \neq 0$. Therefore, $a_x \neq 0$, and hence $x \in \mathbb{A}^*$. Conversely, if $x \in \mathbb{A}^*$, then the composition $\mathbb{A} \longrightarrow \mathbb{A} \cdot x \longrightarrow \mathbb{A}$, where the first map sends m to $m \cdot x$, while the second $n \mapsto n \cdot x^{-1}$, is the identity map. Thus, $\dim_K M_x = 4$. Therefore, $M_x = \mathbb{A}$.

Suppose that $\mathbb{A}$ is not a division ring and choose a non-zero $x \in \mathbb{A}$, which is not a unit. Then M_x is non-zero and is of dimension less than 4.

In general, if $M \subset \mathbb{A}$ is a non-zero left ideal, then the assignment $x \mapsto \psi_x$, where $\psi_x : M \longrightarrow M$ is the K-linear transformation that sends $m \in M$ to $x \cdot m$, gives rise to a K-algebra homomorphism

$$\psi : \mathbb{A} \longrightarrow \mathrm{End}_K(M) \simeq \mathrm{M}(r, K),$$

where $r = \dim_K M$. Since $\psi(1) = id$, the kernel of ψ is a proper two-sided ideal of $\mathbb{A}$. Hence, by Proposition 2.2.1, the kernel is trivial and ψ is injective. This also shows that $r \neq 1$, for otherwise ψ would embed $\mathbb{A}$ into the one dimensional vector space $\mathrm{M}(1, K) = K$, which is impossible.

Now take $M = M_x$. We claim that $\dim_K M_x \leq 2$. Since $\dim_K M_x \neq 1$, it follows from the claim that $\dim_K M_x = 2$ and $\mathrm{End}_K(M_x) \simeq \mathrm{M}(2, K)$. By the dimension counting, ψ is a surjection, and hence an isomorphism. The lemma is proved.

To prove the claim, recall that $x \cdot g(x) = g(x) \cdot x = 0$, since x is not a unit. This implies that $M_x \cdot g(x) = 0$, and hence M_x is contained in the kernel of the surjective K-linear map $\varrho : \mathbb{A} \longrightarrow M_{g(x)}$, $y \mapsto y \cdot g(x)$. Since $M_{g(x)} \neq 0$, the above conclusion $r \neq 1$ (for $M = M_{g(x)}$) implies $\dim_K \ker(\varrho) \geq 2$. Hence the dimension counting implies $\dim_K M_x \leq 2$ as desired.

□

Definition 2.2.2. *A 4-dimensional K-algebra is called a quaternion algebra over K, if it is either a quaternion division ring over K or isomorphic to the matrix algebra* $\mathrm{M}(2, K)$.

By Proposition 2.2.1, every cyclic algebra $\mathbb{H}(a, b)$ is a central simple algebra, while Theorem 2 says that each central simple algebra is a quaternion algebra. Conversely, every quaternion algebra equals some $\mathbb{H}(a, b)$, in view of Theorem 1 and the fact that $\mathrm{M}(2, K) = \mathbb{H}(1, 1)$ by taking

$$i = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad j = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad k = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

The map sending each $x = \alpha_0 + a_1 i + \alpha_2 j + \alpha_3 k$ to $\bar{x} := \alpha_0 - a_1 i - \alpha_2 j - \alpha_3 k$ is an isomorphism of $\mathbb{H}(a, b)$ (and is an involution).

Definition 2.2.3. *Define the reduced trace and the reduced norm of an element $x \in \mathbb{H}(a,b)$ to be*

$$\mathrm{tr}(x) := x + \bar{x} \in K, \quad \textit{and} \quad |x| := x\bar{x} = \bar{x}x \in K.$$

Thus, every $x \in \mathbb{H}(a,b)$ satisfies the quadratic equation:

$$x^2 - \mathrm{tr}(x)x + |x| = 0. \tag{2.1}$$

Also, x is a unit of $\mathbb{H}(a,b)$ if and only if $|x| \neq 0$.

2.3 Isomorphic classes of cyclic algebras

Suppose $\varrho : \mathbb{H}(a,b) \longrightarrow \mathbb{H}(c,d)$ is an isomorphism of K-algebras and let $\{1, i'', j'', k''\}$ be the basis of $\mathbb{H}(c,d)$ with $i''i'' = c$, $j''j'' = d$, $i''j'' = -j''i'' = k''$. Put $i' = \varrho^{-1}(i'')$, $j' = \varrho^{-1}(j'')$, and $k' = \varrho^{-1}(k'')$. Then $\{1, i', j', k'\}$ forms a basis of $\mathbb{H}(a,b)$ with $i'i' = c$, $j'j' = d$, $i'j' = -j'i' = k'$. Thus, we can write $\mathbb{H}(a,b) = \mathbb{H}(c,d)$ instead. In this situation, the $\mathbb{H}(c,d)$ structure induces the corresponding reduced trace and reduced norm on $\mathbb{H}(a,b)$, which we denote by $\mathrm{tr}'(x)$ and $|x|'$. Namely, if $x = \beta_0 1 + \beta_1 i' + \beta_2 j' + \beta_3 k'$, then $\mathrm{tr}'(x) = 2\beta_0$ and $|x|' = \beta_0^2 - \beta_1^2 c - \beta_2^2 d + \beta_3^2 cd$.

Lemma 2.3.1. *If $\mathbb{H}(a,b) = \mathbb{H}(c,d)$, then $\mathrm{tr}'(x) = \mathrm{tr}(x)$ and $|x|' = |x|$ for every $x \in \mathbb{H}(a,b)$.*

Proof. By applying (2.1) both, we get

$$-(\mathrm{tr}'(x) - \mathrm{tr}(x))x + (|x|' - |x|) = 0 - 0 = 0.$$

Thus, if $\mathrm{tr}'(x) \neq \mathrm{tr}(x)$, then $x = \frac{|x|' - |x|}{\mathrm{tr}'(x) - \mathrm{tr}(x)} \in K$. This shows the first equality in the lemma, for $x \notin K$. Then the second follows from the above equation. If $x \in K$, then $\mathrm{tr}'(x) = 2x = \mathrm{tr}(x)$ and $|x|' = x^2 = |x|$. □

Definition 2.3.1. *For a given pair $(a,b) \in K^* \times K^*$, define*

$$Q_{(a,b)}(x,y,z) := ax^2 + by^2 - abz^2.$$

Suppose $\mathbb{H}(a,b) = \mathbb{H}(c,d)$. Then Lemma 2.3.1 implies

$$\mathbb{H}(a,b)^o := \text{Span}(i,j,k) = \{x \in H(a,b) \mid \text{tr}(x) = 0\} = \text{Span}(i',j',k').$$

If $x = x_1 i + x_2 j + x_3 k \in \mathbb{H}(a,b)^o$, then

$$-|x| = ax_1^2 + bx_2^2 - abx_3^2 = Q_{(a,b)}(x_1,x_2,x_3).$$

Similarly, using the expression $x = x_1' i' + x_2' j' + x_3' k'$, we have

$$-|x| = cx_1'^2 + dx_2'^2 - cdx_3'^2 = Q_{(c,d)}(x_1',x_2',x_3').$$

Recall that if $f = \sum_{i,j=1}^n a_{ij} x_i x_j$, where $a_{ij} = a_{ji} \in K$, is a quadratic form, then the symmetric matrix $A = (a_{ij})$, called the matrix of the quadratic form f, is uniquely determined by f, and vice versa. If $X = (x_1, x_2, ..., x_n)$, then

$$f(X) = XAX^t.$$

Two quadratic forms f and g are equivalent, denoted as $f \sim g$, if there is some $C \in \text{GL}(n,K)$ such that the matrix of g equals CAC^t.

Theorem 3. *Two cyclic algebras $\mathbb{H}(a,b)$ and $\mathbb{H}(c,d)$ are isomorphic if and only if the associated quadratic forms $Q_{(a,b)}$ and $Q_{(c,d)}$ are equivalent.*

Proof. Let A denote the matrix of $Q_{(a,b)}$. If $\mathbb{H}(a,b) = \mathbb{H}(c,d)$, then there exists $C \in \text{GL}(3,K)$ such that for $x_1 i + x_2 j + x_3 k = x = x_1' i' + x_2' j' + x_3' k'$ as before, we have $(x_1', x_2', x_3')\, C = (x_1, x_2, x_3)$. and hence

$$Q_{(c,d)}(x_1',x_2',x_3') = -|x| = (x_1',x_2',x_3')\, CAC^t\, (x_1',x_2',x_3')^t.$$

This means $Q_{(c,d)} \sim Q_{(a,b)}$.

Conversely, assume $Q_{(c,d)} \sim Q_{(a,b)}$ and let $C \in \text{GL}(3,K)$ be such that

$$Q_{(c,d)}(x_1',x_2',x_3') = (x_1',x_2',x_3')\, CAC^t\, (x_1',x_2',x_3')^t.$$

Let $(c_1^{(\lambda)}, c_2^{(\lambda)}, c_3^{(\lambda)})$ denote the λth row of the matrix C and set

$$i' = c_1^{(1)} i + c_2^{(1)} j + c_3^{(1)} k,$$
$$j' = c_1^{(2)} i + c_2^{(2)} j + c_3^{(2)} k.$$

Then $i'i' = -|i'| = Q_{(a,b)}(c_1^{(1)}, c_2^{(1)}, c_3^{(1)}) = Q_{(c,d)}(1,0,0) = c$, and similarly, $j'j' = Q_{(c,d)}(0,1,0) = d$. Then $(i'+j')(i'+j') = Q_{(c,d)}(1,1,0) = c+d$, and hence $i'j' = -j'i'$. Set $k' = i'j'$. Then the basis $\{1, i', j', k'\}$ gives rise to a $\mathbb{H}(c,d)$ structure of $\mathbb{H}(a,b)$. In other words, we have $\mathbb{H}(a,b) = \mathbb{H}(c,d)$.

□

2.4 Quadratic forms

In this section, we review the classical theory on Quadratic forms. Our reference is [Bor, page 390-396.]. See also, [Ser]

Definition 2.4.1. *Let f be a quadratic form and let A be its matrix. Then f is non-singular if and only if* $\det(f) := \det A \neq 0$.

Definition 2.4.2. *Let f be a quadratic form. We say that f represents an element $r \in K$, if there exist some $\alpha_1, \alpha_2, ..., \alpha_n \in K$, not all zero, such that $f(\alpha_1, \alpha_2, ..., \alpha_n) = r$.*

Definition 2.4.3. *Let f and g be quadratic forms in n and m variables respectively. We say a quadratic form h in $n+m$ variables is the direct sum of f and g and denote $h = f \oplus g$, if*

$$h(x_1, ..., x_{n+m}) = f(x_1, ..., x_n) + g(x_{n+1}, ..., x_{n+m}).$$

If $f \sim g$, then $f \oplus f_1 \sim g \oplus f_1$ for every f_1.

Lemma 2.4.1. *If quadratic forms $f \sim g$, then* $\det(f) = c^2 \det(g)$*, where $c \in K^*$.*

Proof. If A and $B = CAC^t$ are matrices of f and g, then $\det B = (\det C)^2 \det A$. □

Lemma 2.4.2. *If quadratic form f in n variable represents $r \neq 0$, then $f \sim rx_1^2 + g(x_2, ..., x_n)$.*

Proof. Let A denote the matrix of f. For two vectors $X, Y \in K^n$, define $\langle X, Y \rangle := XAY^t$ and denote

$$X^{\perp} := \{Z \in K^n \ \mid \ \langle Z, X \rangle = 0\}$$

which is a K-linear subspace of K^n of dimension at least $n-1$. Let $\alpha = (\alpha_1, ..., \alpha_n) \in V$ be such that

$$f(\alpha) = \langle \alpha, \alpha \rangle = r.$$

Then $\alpha \notin \alpha^{\perp}$. Write $\alpha^{(1)} = \alpha$ and extend it to a basis $\{\alpha^{(1)}, \alpha^{(2)}, ..., \alpha^{(n)}\}$ of K^n with $\alpha^{(2)}, ..., \alpha^{(n)} \in \alpha^{\perp}$. Let C be the matrix with $\alpha^{(\lambda)}$ as its λth row and let f' be the quadratic form with CAC^t as its matrix. Then $f \sim f'$ and $f'(x_1, ..., x_n) = rx_1^2 + g(x_2, ..., x_n)$ as desired.

□

Corollary 2.4.1. *Every quadratic form f in n variable is diagonalizable. Namely, $f \sim r_1x_1^2 + r_2x_2^2 + ... + r_nx_n^2$ for some $r_1, ..., r_n \in K$ which are representable by f.*

Proposition 2.4.1 (Witt's Theorem)**.** *Let f, g, h be non-singular quadratic forms. If $f \oplus g \sim f \oplus h$, then $g \sim h$.*

Proof. Let f_0 be a diagonal form equivalent to f. Since $f \oplus g \sim f_0 \oplus g$ and $f \oplus h \sim f_0 \oplus h$, we have $f_0 \oplus g \sim f_0 \oplus h$. Thus, we can assume f is diagonal. Then it suffices to consider the case where $f = ax^2, a \neq 0$. Let A and B denote the matrices of g and h. Since $ax^2 \oplus g \sim ax^2 \oplus h$, there exists a matrix $C = \begin{bmatrix} \gamma & S \\ T & Q \end{bmatrix}$ such that

$$\begin{bmatrix} \gamma & T^t \\ S^t & Q^t \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & A \end{bmatrix} \begin{bmatrix} \gamma & S \\ T & Q \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & B \end{bmatrix}.$$

Then, we obtain

$$\begin{aligned}\gamma^2 a + T^t A T &= a\\ \gamma a S + T^t A Q &= 0\\ S^t a S + Q' t A Q &= b\end{aligned}$$

Then we want to show that there exists a nonsingular matrix C_0 such that $C_0^t A C_0 = B$. The matrix C_0 will be found in the form $C_0 = Q + \xi T S$, where the element ξ is suitably chosen. By above equations we have

$$\begin{aligned}C_0^t A C_0 &= (Q^t + \xi S^t T^t) A (Q + \xi T S)\\ &= Q^t A Q + \xi S^t T^t A Q + \xi Q^t A T S + \xi^2 S^t T^t A T S\\ &= Q^t A Q + [(1-\gamma^2)\xi^2 - 2\gamma\xi] S^t S.\end{aligned}$$

Thus, if $(1-\gamma^2)\xi^2 - 2\gamma\xi = 1$, then we have $C_0^t A C_0 = B$. The equation can be written in the form $\xi^2 - (\gamma\xi + 1)^2 = 0$, there is always a solution $\xi \in K$ for any $\gamma \in K$. □

Lemma 2.4.3. *If a non-singular quadratic form f represents zero over field K, then f represents all number of K.*

Proof. Since equivalent forms represent the same field elements, it suffices to prove the theorem for a diagonal form $f = a_1 x_1^2 + ... + a_n x_n^2$. Let $a_1\alpha_1^2 + ... + a_n\alpha_n^2 = 0$ be a representation of zero, and let γ be any element of K. Without loss of generality, we can assume that $\alpha_1 \neq 0$. We express the variables $x_1, ..., x_n$ in terms of a new variable t:

$$\begin{aligned}x_1 &= \alpha_1(1+t),\\ x_k &= \alpha_k(1-t) \qquad (k = 2, ..., n).\end{aligned}$$

Substituting in the form f we obtain

$$f^* = f^*(t) = 2a_1\alpha_1^2 t - 2a_2\alpha_2^2 t - ... - 2a_n\alpha_n^2 t = 4a_1\alpha_1^2 t.$$

If we now set $t = \gamma/4a_1\alpha_1^2$, we obtain $f^* = \gamma$. □

Lemma 2.4.4. *A non-singular quadratic form f represents $\gamma \neq 0$ in K if and only if the form $-\gamma x_0^2 + f(x_1, ..., x_n)$ represents 0.*

Proof. If f represents r, then $f \sim rx_1^2 \oplus g$ by Lemma 2.4.2, and hence $-rx_0^2 \oplus f \sim -rx^0 + rx_1^2 \oplus g$, which represents zero. Since equivalent forms represents the same things, $-\gamma x_0^2 + f(x_1, ..., x_n) = 0$ represents 0. Conversely, if $-r\alpha_0^2 + f(\alpha_1, ..., \alpha_n) = 0$, then either $\alpha_0 = 0$, and hence f represents 0 and r (by Lemma 2.4.3), or $\alpha_0 \neq 0$, and hence $f(\frac{\alpha_1}{\alpha_0}, ..., \frac{\alpha_n}{\alpha_0}) = r$.

□

Lemma 2.4.5. *If a quadratic form f represents 0, then it is equivalent to a form of the type $y_1y_2 + g(y_3, ..., y_n)$.*

Proof. By Lemma 2.4.3, f represents 1, and hence by Lemma 2.4.2, is equivalent to $x_1^2 + f'(x_2, ..., x_n)$. By Lemma 2.4.4, f' represents -1, and hence by Lemma 2.4.2 again, is equivalent to $-x_2^2 + g(x_3, ..., x_n)$. Therefore, f is equivalent to $x_1^2 - x_2^2 + g(x_3, ..., x_n)$. Then take $y_1 = x_1 + x_2$, $y_2 = x_1 - x_2$, $y_3 = x_3$,..., $y_n = x_n$.

□

Corollary 2.4.2. *All nonsingular quadratic forms in two variables representing 0 in K are equivalent.*

Proof. They all equivalent to x_1x_2. □

Lemma 2.4.6. *A quadratic form f in two variables with $d = det(f) \neq 0$ represents 0 in K if and only if $-d$ is a square in K.*

Proof. We can write $f(x, y) = ax^2 + by^2$, by Corollary 2.4.1. □

Lemma 2.4.7. *Let f, g be two nonsingular quadratic forms in two variables. Then the following statements are equivalent:*

(a) *$f \sim g$.*

(b) *$det(f) = c^2 det(g)$, $c \in K$, and there exists some nonzero element $a \in K$ represented by both f and g.*

Proof. The implication (a)⇒(b) is clear. If (b) holds, then Corollary 2.4.1, we can write $f = ax^2 + by^2$ and $g = ax^2 + dy^2$. Then (a) follows.

□

2.5 The quadratic form $P_{(a,b)}(x, y, z)$

The quadratic form $P_{(a,b)}(x, y, z) := ax^2 + by^2 - z^2$ turns out to be useful for studying the quaternion algebra $\mathbb{H}(a, b)$.

Theorem 4. *The quaternion algebra $\mathbb{H}(a, b)$ is isomorphic to $\mathrm{M}(2, K)$ if and only if the quadratic form $P_{(a,b)}(x, y, z)$ represents zero in K.*

Proof. If $\mathbb{H}(a, b) = \mathrm{M}(2, K) = \mathbb{H}(1, 1)$, then by Theorem 3,

$$Q_{(a,b)}(x, y, u) \sim Q_{(1,1)}(x, y, u),$$

and hence

$$P_{(a,b)}(x, y, z) - abu^2 = Q_{(a,b)}(x, y, u) - z^2 \sim x^2 + y^2 - u^2 - z^2.$$

Since $y^2 - u^2 = (y + u)(y - u) \sim yu \sim (aby)u \sim ab(y^2 - u^2)$, the above relation implies

$$P_{(a,b)}(x, y, z) - abu^2 \sim x^2 + aby^2 - z^2 - abu^2.$$

Then by Proposition 2.4.1, $P_{(a,b)}(x, y, z) \sim x^2 + aby^2 - z^2$, which represents zero.

If $P_{(a,b)}(x, y, z)$ represents zero, then by Lemma 2.4.5, we have

$$P_{(a,b)}(x, y, z) \sim y_1 y_2 + cy_3^2 \sim x^2 - y^2 + cy_3^2,$$

where by Lemma 2.4, we can choose $c = ab$. Then

$$Q_{(a,b)}(x, y, u) - z^2 = P_{(a,b)}(x, y, z) - abu^2 \sim x^2 - y^2 + aby_3^2 - abu^2.$$

Again, since $aby_3^2 - abu^2 \sim wv \sim u^2 - z^2$, the above relation shows

$$Q_{(a,b)}(x, y, u) - z^2 \sim x^2 - y^2 + u^2 - z^2.$$

Hence, by Proposition 2.4.1,

$$Q_{(a,b)}(x, y, u) \sim x^2 + u^2 - y^2 = Q_{(1,1)}(x, u, y) \sim Q_{(1,1)}(x, y, u).$$

□

If $K(\sqrt{a})/K$ is a quadratic extension, let $\mathrm{N}_{(a)} := \mathrm{N}_{K(\sqrt{a})/K}(K(\sqrt{a})^*)$ denote the subgroup of norms. If a is a square in K^*, denote $\mathrm{N}_{(a)} := K^*$.

Lemma 2.5.1. *The following statements are equivalent:*

(a) $b \in \mathrm{N}_{(a)}$.

(b) $a \in \mathrm{N}_{(b)}$.

(c) *The quadratic form* $P_{(a,b)}$ *represents zero in* K.

Proof. Note that $P_{(b,a)} = P_{(a,b)}$. It is sufficient to show (a)⇔(c), because by interchanging a and b, we obtain (b)⇔(c) as well. If a is a quare in K, then both (a) and (c) holds. Suppose a is not a square in K. By Lemma 2.4.4, (c) holds if and only if the quadratic form $z^2 - ax^2$ represents b. But this means exactly $b \in \mathrm{N}_{(a)}$.

□

Chapter 3

Quaternion Algebras over Local Fields

In this chapter, K is the completion of a number field at certain place v. Our references are [Bor, Lan].

3.1 The group of local norms

Let L/K be a quadratic extension with $G := \mathrm{Gal}(L/K) = \{id, \sigma\}$.

Theorem 5. *The group $K^*/\mathrm{N}_{L/K}(L^*)$ is isomorphic to G.*

The theorem holds for any abelian extension of K and is one of the main theorem in the class field theory. In §3.5, a direct proof of Theorem 5 will be given. Basically, it is the same as the proof given in [Lan]. The theorem allows us to make use of the Hilbert Symbol defined in the next section.

3.2 The Hilbert symbols

We let $\frac{1}{2}\mathbb{Z}/\mathbb{Z} = \{0, \frac{1}{2}\}$ denote the cyclic group of order two.

Definition 3.2.1. *For $a, b \in K^*$, define the Hilbert Symbol*

$$\left(\frac{a,b}{K}\right) := \begin{cases} 0 \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}, & \textit{if } P_{(a,b)} \textit{ represents zero;} \\ \frac{1}{2} \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}, & \textit{otherwise.} \end{cases}$$

Some basic properties of the Hilbert Symbol are in order.

Lemma 3.2.1. *The Hilbert Symbol satisfied the following:*

(a) $\left(\frac{b,a}{K}\right) = \left(\frac{a,b}{K}\right)$

(b) *If a or b is a square in K^*, then $\left(\frac{a,b}{K}\right) = 0$.*

(c) *We always have $\left(\frac{a,-a}{K}\right) = 0$.*

Proof. Statements (a) and (b) follow directly from Lemma 2.5.1, while (c) is obvious, since $ax^2 - ay^2 - z^2$ represents zero. □

Proposition 3.2.1. *The map $K^* \times K^* \longrightarrow \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ sending (a, b) to $\left(\frac{a,b}{K}\right)$ is bi-linear in the sense that*

$$\left(\frac{a, bb'}{K}\right) = \left(\frac{a, b}{K}\right) + \left(\frac{a, b'}{K}\right),$$

and

$$\left(\frac{aa', b}{K}\right) = \left(\frac{a, b}{K}\right) + \left(\frac{a', b}{K}\right).$$

Furthermore, the left kernel and the right kernel of this bi-linear map are exactly $(K^*)^2$, the subgroup of the squares in K^*. Namely, we have

$$\{a \in K^* \mid \left(\frac{a, b}{K}\right) = 0, \text{ for all } b \in K^*\} = (K^*)^2,$$

and

$$\{b \in K^* \mid \left(\frac{a, b}{K}\right) = 0, \text{ for all } a \in K^*\} = (K^*)^2.$$

Proof. By Lemma 3.2.1, if $a \in (K^*)^2$, then the first equality holds trivially. Suppose $a \notin (K^*)^2$. By Theorem 5, $K^*/\mathrm{N}_{(a)} \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, and Lemma 2.5.1 says the composition of group homomorphisms

$$K^* \longrightarrow K^*/\mathrm{N}_{(a)} \xrightarrow{\sim} \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}\,,$$

where the left map is the quotient map, is the same as the map

$$\left(\frac{a, \bullet}{K}\right) : K^* \longrightarrow \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

that sends $b \in K^*$ to $\left(\frac{a,b}{K}\right)$. Thus, $\left(\frac{a,\bullet}{K}\right)$ is a group homomorphism and the first equality follows. The second equality is proved similarly.

If $a \in (K^*)^2$, then a is contained in the left kernel of the Hilbert Symbols. If $a \notin (K^*)^2$, then again $K^*/\mathrm{N}_{(a)} \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z}$. Hence there exists some $b \in K^*$, $b \notin \mathrm{N}_{(a)}$. For such b, we have $\left(\frac{a,b}{K}\right) \neq 0$. This shows a is not contained in the left kernel of the Hilbert Symbols. The same argument can be applied to the right kernel. □

3.3 Quaternion algebras over local fields

Recall that two quaternion algebras $\mathbb{H}(a,b)$ and $\mathbb{H}(c,d)$ are isomorphic if and only if the quadratic forms $Q_{(a,b)}$ and $Q_{(c,d)}$ are equivalent. Also, $\mathbb{H}(a,b)$ is a quaternion division ring if and only if $P_{(a,b)}$ does not represents zero in K, or equivalently, the Hilbert Symbol $\left(\frac{a,b}{K}\right) \neq 0$.

If $K \simeq \mathbb{R}$, then $(K^*)^2 = \mathbb{R}^+$ is a subgroup of index 2 in $\mathbb{R}^*$. If the place v is non-archimedean, then $K^* = \mathbb{Z} \times \mathcal{O}^*$, where $\mathcal{O}$ denotes the ring of integers of K, and hence $(K^*)^2 = 2\mathbb{Z} \times (\mathcal{O}^*)^2$, also a proper subgroup of K^*.

Theorem 6. *Suppose $K \not\simeq \mathbb{C}$. Then there is exactly one isomorphic class of quaternion division rings over K. Namely, every two quaternion division rings over K are isomorphic.*

Proof. First, for every non-square $a \in k^*$, Theorem 5 says there is $b \notin \mathrm{N}_{(a)}$. Hence, $P_{(a,b)}$ does not represent zero in K. This shows the isomorphic classes of quaternion division rings over K is not empty.

Let $\mathbb{H}(a,b)$ and $\mathbb{H}(c,d)$ are two quaternion division ring. First consider the case where $c \equiv a \pmod{(K^*)^2}$. Then $Q_{(c,d)} \sim Q_{(a,d)}$ and $\left(\frac{c,d}{K}\right) = \left(\frac{a,d}{K}\right)$. we need to show that $Q_{(a,d)} \sim Q_{(a,b)}$, which, by Proposition 2.4.1, is equivalent to

$$f := d(y^2 - az^2) = dy^2 - adz^2 \sim by^2 - abz^2 = b(y^2 - az^2) := g.$$

Since $\det(f) = -ad^2$, $\det(g) = -ab^2$, and f represents d in K, Lemma 2.4.7 says $f \sim g$ holds if and only if g represents d in K. The quadratic form $y^2 - az^2 =$

$(y+\sqrt{a})(y-\sqrt{a})$ represents all elements in $\mathrm{N}_{(a)}$. Therefore, g represents all elements in $b\mathrm{N}_{(a)}$. But, since $\left(\frac{a,b}{K}\right) = \left(\frac{a,d}{K}\right) = \frac{1}{2}$, Theorem 5 says $d\mathrm{N}_{(a)} = b\mathrm{N}_{(a)}$, and hence g represents d.

In general, we need to find some $e \in K^*$ to have $Q_{(a,b)} \sim Q_{(e,b')}$ and $Q_{(c,d)} \sim Q_{(e,d')}$, for some $b', d' \in K^*$. Then we can apply the above result to conclude $Q_{(a,b)} \sim Q_{(c,d)}$. To proceed, write $f = by^2 - abz^2$ and $g = cy^2 - cdz^2$. We claim to find an e representable by f and g. Then e is also representable by $Q_{(a,b)} = ax^2 \oplus f$ and $Q_{(c,d)} = cx^2 \oplus g$. By Lemma 2.4.2 and Corollary 2.4.1, we have $Q_{(a,b)} \sim ex^2 + b'y + b''z^2$, where by the computation of the related determinants, we can write $b'' = -eb'$. In other words, $Q_{(a,b)} \sim Q_{(e,b')}$. Similarly, $Q_{(c,d)} \sim Q_{(e,d')}$, as desired. By the argument used before, f represents all elements in $b\mathrm{N}_{(a)}$, and g all $d\mathrm{N}_{(c)}$. We need to show that $b\mathrm{N}_{(a)} \cap d\mathrm{N}_{(c)}$ is non-empty. But, since $b \notin \mathrm{N}_{(a)}$ and $d \notin \mathrm{N}_{(c)}$, we have

$$K^* = \mathrm{N}_{(a)} \sqcup b\mathrm{N}_{(a)} \text{ and } K^* = \mathrm{N}_{(c)} \sqcup d\mathrm{N}_{(c)},$$

where both $\mathrm{N}_{(a)}$ and $\mathrm{N}_{(c)}$ are subgroup, elementary group theory implies

$$\mathrm{N}_{(a)} \cup \mathrm{N}_{(c)} \subsetneq \mathrm{N}_{(a)} \cdot \mathrm{N}_{(c)}.$$

□

Thus, if $K = \mathbb{R}$, then the isomorphism class of quaternion division is represented by the Hamiltonian Quaternion $\mathbb{H}(-1,-1)$.

If $K \neq \mathbb{C}$, then there are two isomorphic classes of cyclic algebras. Hence, there are also two equivalent classes of quadratic forms of the type $Q_{(a,b)}$. It is worthwhile to mention that this does not mean there are only two equivalent classes of quadratic forms of type $P_{(a,b)}$. Indeed, $P_{(a,b)} \sim P_{(c,d)}$ if and only if $ax^2 + by^2 \sim cx^2 + dy^2$, by Witt's theorem. Write $ax^2 + by^2 = a(x^2 - b'y^2)$, $cx^2 + dy^2 = c(x^2 - d'y^2)$, with $b = -ab'$, $d = -cd'$. By Lemma 2.4.7, $P_{(a,b)} \sim P_{(c,d)}$ if and only if $b'/d' \in (K^*)^2$ and both $a(x^2 - b'y^2)$ and $c(x^2 - d'y^2)$ represent a same number. Then one sees there are actually more than two isomorphic classes.

3.4 The Herbrand quotient

Let L/K be a quadratic extension as before and denote $G := \mathrm{Gal}(L/K) = \{id, \sigma\}$. For each G-module M, set

$$M^G := \{m \in M \mid \sigma(m) = m\},$$

$$\mathrm{N}_G(M) := \{m + \sigma(m) \mid m \in M\},$$

$$\ker(\mathrm{N}_{G,M}) = \{m \in M \mid m + \sigma(m) = 0\},$$

$$(1-\sigma)M := \{m - \sigma(m) \mid m \in M\}.$$

Obviously, these are sub-modules of M, with

$$\mathrm{N}_G(M) \subset M^G \text{ and } (1-\sigma)M \subset \ker(\mathrm{N}_{G,M}).$$

Definition 3.4.1. *Define*

$$\mathrm{H}^e(G, M) := M^G/\mathrm{N}_G(M), \text{ and } \mathrm{H}^o(G, M) := \ker(\mathrm{N}_{G,M})/(1-\sigma)M.$$

If $\alpha : M_1 \longrightarrow M_2$ is a homomorphism of G-modules, then we have the induced homomorphism $\alpha_* : \mathrm{H}^\bullet(G, M_1) \longrightarrow \mathrm{H}^\bullet(G, M_2)$, for $\bullet = e$, or $\bullet = o$.

Definition 3.4.2. *If both $\mathrm{H}^e(G, M)$ and $\mathrm{H}^o(G, M)$ are finite groups, define the Herbrand quotient of the G-module M to be*

$$h(M) := \frac{|\mathrm{H}^e(G, M)|}{|\mathrm{H}^o(G, M)|}.$$

Lemma 3.4.1. *If M is a finite G-module, then $h(M) = 1$.*

Proof. We have the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M^G \arrow[r] & M \arrow[r, "1-\sigma"] & (1-\sigma)M \arrow[r] & 0 \end{tikzcd},$$

where the middle arrow is the map $m \mapsto m - \sigma(m)$. This implies

$$|M| = |M^G| \cdot |(1-\sigma)M|.$$

Also, the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker(\mathrm{N}_{G,M}) \arrow[r] & M \arrow[r, "1+\sigma"] & \mathrm{N}_G(M) \arrow[r] & 0 \end{tikzcd}$$

implies

$$|M| = |\ker(\mathrm{N}_{G,M})| \cdot |\mathrm{N}_G(M)|.$$

Then the lemmas follow from the above two equalities. □

Lemma 3.4.2. *Suppose we have the exact sequence of G-modules*

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\alpha"] & M_2 \arrow[r, "\beta"] & M_3 \arrow[r] & 0\ . \end{tikzcd} \tag{3.1}$$

If two of $h(M_1)$, $h(M_2)$, $h(M_3)$ are defined, then so is the third, and we have

$$h(M_2) = h(M_1) \cdot h(M_3).$$

Proof. We have the exact sequence (exact hexagon)

$$\begin{tikzcd} \mathrm{H}^e(M_1) \arrow[r, "\alpha_*"] & \mathrm{H}^e(M_2) \arrow[r, "\beta_*"] & \mathrm{H}^e(M_3) \arrow[d, "\delta_e"] \\ \mathrm{H}^o(M_3) \arrow[u, "\delta_o"] & \mathrm{H}^o(M_2) \arrow[l, "\beta_*"'] & \mathrm{H}^o(M_1). \arrow[l, "\alpha_*"'] \end{tikzcd} \tag{3.2}$$

Here the boundary homomorphisms δ_e and δ_o are as follow. By applying the snake lemma to the diagram

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\alpha"] \arrow[d, "1-\sigma"] & M_2 \arrow[r, "\beta"] \arrow[d, "1-\sigma"] & M_3 \arrow[r] \arrow[d, "1-\sigma"] & 0\ , \\ 0 \arrow[r] & M_1 \arrow[r, "\alpha"] & M_2 \arrow[r, "\beta"] & M_3 \arrow[r] & 0 \end{tikzcd}$$

we obtain the exact sequence

$$\begin{tikzcd} M_2^G \arrow[r] & M_3^G \arrow[r, "\delta^{(0)}"] & M_1/(1-\sigma)M_1 \arrow[r, "\alpha^{(1)}"] & M_2/(1-\sigma)M_2. \end{tikzcd} \tag{3.3}$$

Suppose $m_3 = \mathrm{N}_G(m_3')$, for some $m_3' \in M_3$ and by (3.1), let $m_2' \in M_2$ be such that $\beta(m_2') = m_3'$. Let $m_2 = \mathrm{N}_G(m_2')$. Then $m_3 = \beta(m_2)$. This shows that β

induces a surjection $\mathrm{N}_G(M_2) \twoheadrightarrow \mathrm{N}_G(M_3)$. Thus, the exact sequence (3.3) implies $\mathrm{N}_G(M_3) \subset \ker(\delta^{(0)})$, and hence $\delta^{(0)}$ factors through

$$\delta_e : \mathrm{H}^e(G, M_3) \longrightarrow M_1/(1-\sigma)M_1.$$

Now (3.3) also implies the image of δ_e equals the kernel of $\alpha^{(1)}$, which can be expressed as $(M_1 \cap (1-\sigma)M_2)/(1-\sigma)M_1$. Since $((1-\sigma)M_2) \subset \ker(\mathrm{N}_{G,M_2})$, $M_1 \cap (1-\sigma)M_2$ is contained in $\ker(\mathrm{N}_{G,M_1})$. Therefore, the image of δ_e is contained in $\mathrm{H}^0(G, M_1)$.

Also, by applying the snake lemma to the diagram

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r, "\alpha"] \arrow[d, "\mathrm{N}_G"] & M_2 \arrow[r, "\beta"] \arrow[d, "\mathrm{N}_G"] & M_3 \arrow[r] \arrow[d, "\mathrm{N}_G"] & 0 \ , \\
0 \arrow[r] & M_1 \arrow[r, "\alpha"] & M_2 \arrow[r, "\beta"] & M_3 \arrow[r] & 0
\end{tikzcd}$$

we obtain the exact sequence

$$\ker(\mathrm{N}_{G,M_2}) \longrightarrow \ker(\mathrm{N}_{G,M_3}) \xrightarrow{\delta^{(1)}} M_1/\mathrm{N}_G(M_1) \xrightarrow{\alpha^{(2)}} M_2/\mathrm{N}_G(M_2). \tag{3.4}$$

Similarly, (3.1) implies the surjection $(1-\sigma)M_2 \twoheadrightarrow (1-\sigma)M_3$, and hence $\delta^{(1)}$ factors through

$$\delta_o : \mathrm{H}^o(G, M_3) \longrightarrow M_1/\mathrm{N}_G(M_1).$$

then we apply the exact sequence (3.4) to show that the image of δ_o is contained in $\mathrm{H}^e(G, M_1)$. The boundary maps are defined. Then the exactness of (3.2) can be checked accordingly.

Suppose $h(M_1)$ and $h(M_2)$ are defined. Then by (3.2), both $\mathrm{H}^o(G, M_3)$ and $\mathrm{H}^e(G, M_3)$ are finite, and hence $h(M_3)$ is defined. Other cases can be treated by similar arguments. Finally, (3.2) shows

$$|\mathrm{H}^o(G, M_1)| \cdot |\mathrm{H}^o(G, M_3)| \cdot |\mathrm{H}^e(G, M_2)| = |\mathrm{H}^o(G, M_2)| \cdot |\mathrm{H}^e(G, M_1)| \cdot |\mathrm{H}^e(G, M_3)|$$

that implies $h(M_2) = h(M_1) \cdot h(M_3)$. □

Another proof of the above lemma can be found in [Lan, §IX.1].

Lemma 3.4.3. *If $h(M)$ is defined and the multiplication by 2 is invertible in M, then $h(M) = 1$.*

Proof. Then for every $m \in M$, there is a unique n such that $2n = m$. Hence $m = (n + \sigma(n)) + (n - \sigma(n))$. Then it follows that $M^G = \mathrm{N}_G(M)$ and $\ker(\mathrm{N}_{G,M}) = (1 - \sigma)M$. □

Lemma 3.4.4. *Suppose $M = \mathbb{Z}$, or $M = \mathbb{Z}_2$. If G acts trivially on M, then $h(M) = 2$. If σ acts as (-1) on M, then $h(M) = \frac{1}{2}$*

Proof. Direct computation. □

3.5 The proof of Theorem 5

Proof of Theorem 5. Suppose $K = \mathbb{R}$. Then $L = \mathbb{C}$ is the only quadratic extension, and hence $K * /\mathrm{N}_{L/K}(L^*) = \mathbb{R}^*/\mathbb{R}^+$, which is of order 2.

Suppose K is non-archimedean, let $\mathbb{F}_K$ denote the residue field of K, and let $\mathcal{O}_L$, $\mathbb{F}_L$ denote the ring of integers of L and the residue field.

Let π_K denote a prime element of K and π_L a prime element of L. Write $U_1 := 1 + \pi_L\mathcal{O}_L$. Let p denote the characteristic of $\mathbb{F}_K$. Then U_1 is a p-group. We have the exact sequences (all group written additively)

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{O}_L^* \arrow[r] & L^* \arrow[r] & \mathbb{Z} \arrow[r] & 0, \end{tikzcd} \tag{3.5}$$

and

$$\begin{tikzcd} 0 \arrow[r] & U_1 \arrow[r] & O_L^* \arrow[r] & \mathbb{F}_L^* \arrow[r] & 0. \end{tikzcd} \tag{3.6}$$

Consider the case where $p \neq 2$. Then multiplication by 2 is invertible in U_1. Hence, Lemma 3.4.3 implies $h(U_1) = 1$. Also, by Lemma 3.4.1, $h(\mathbb{F}_L^*)$ equals 1. Thus, Lemma 3.4.2, (3.5) and (3.6) together imply $h(L^*) = h(\mathbb{Z})$, which is 2 by Lemma 3.4.4. But Hilbert Theorem 90 says $\mathrm{H}^o(G, L^*) = 1$. Therefore, we have $|K^*/\mathrm{N}_{L/K}(L^*)| = |\mathrm{H}^e(G, L^*)| = 2$.

Suppose $p = 2$. We need to show that $h(U_1) = 1$. The the previous argument applies. Let F^+ (resp. F^-) denote the free $\mathbb{Z}_p$-module of rank 1 such that on it σ acts as 1 (resp. -1). The lemma below implies that $h(U_1) = h((F^+)^r \cdot h(F^-)^r = 1$. □

Lemma 3.5.1. *Suppose K/Q_p is a finite extension of degree r and L/K is a quadratic extension with $G := \mathrm{Gal}(L/K) = \{id, \sigma\}$. Then there exist G-modules U^+ and U^- satisfying the following:*

(a) *Both U^+ and U^- are free $\mathbb{Z}_p$-modules. On U^+, σ acts trivially, while σ acts as -1 on U^-.*

(b) *We have the exact sequence*

$$\begin{tikzcd} 0 \arrow[r] & U^+ \oplus U^- \arrow[r] & U_1 \arrow[r] & H \arrow[r] & 0 \end{tikzcd}$$

where H is a finite group.

Proof. Let π_K denote a prime element of K and put $U_{1,K} = 1 + \pi_K \mathcal{O}$. It is well known that $U_{1,K}$ (resp. U_1) is a finitely generated $\mathbb{Z}_p$-module of rank r (resp. $2r$), [Bor, §4.5, Theorem 3]. Thus, we can find some rank r free $\mathbb{Z}_p$-module $W^+ \subset U_{1,K}$ such that $U_{1,K}/W^+$ is a finite group. Clearly, G act trivially on W^+. Consider the exact sequence of G-modules (written additively)

$$\begin{tikzcd} 0 \arrow[r] & U_{1,K} \arrow[r] & U_1 \arrow[r, "1-\sigma"] & U_1 , \end{tikzcd}$$

where $1 - \sigma$ is the map sending ξ to $\xi \cdot \sigma(\xi)^{-1}$. Then its image Y is a G-module and its $\mathbb{Z}_p$ rank is r. Since $\sigma(1 - \sigma) = \sigma - 1$, σ acts on Y as -1. Let W^- be a rank r free $\mathbb{Z}_p$ submodule of Y. Then W and W^- generate a submodule W^+W^- of U_1 of $\mathbb{Z}_p$ rank $2r$, so that U_1/W^+W^- is finite. If $x \in W^+ \cap W^-$, then $x = \sigma(x) = \sigma(x)^{-1}$, and hence $x^2 = 1$. But since $W^+ \cap W^-$ is a free module over $\mathbb{Z}_p$, x must be 1. Take $U^+ = W^+$ and $U^- = W^-$. □

3.6 Non-archimedean places

Consider the case where v is a non-archimedean place. Then there is a unique unramified quadratic extension L/K. Let notation be as the previous sections. In particular, $\mathcal{O}$ denotes the ring of integers of K. We quote the following well known fact (see [Lan, §II.4, Corollary of Proposition 9]).

Proposition 3.6.1. *If L/K is a finite unramifed extension, then the group of norms $\mathrm{N}_{L/K}(L^*)$ contains $\mathcal{O}^*$.*

Corollary 3.6.1. *Suppose $p \neq 2$. If $a, b \in \mathcal{O}^*$, then $\left(\frac{a,b}{K}\right) = 0$.*

Proof. Since $K(\sqrt{a})/K$ is unramified and $b \in \mathcal{O}^*$. □

Lemma 3.6.1. *Suppose $p \neq 2$, a is a prime element of K and $b \in \mathcal{O}^*$. Then $\left(\frac{a,b}{K}\right) = 0$ if and only if the residue class of b is contained in $(\mathbb{F}_K^*)^2$.*

Proof. Since $\left(\frac{a,-a}{K}\right) = 0$ by Lemma 3.2.1 and a is a prime element, if $\left(\frac{a\,,\xi}{K}\right) = 0$ for all $\xi \in \mathcal{O}^*$, then $\left(\frac{a\,,\eta}{K}\right) = 0$ for all $\eta \in K^*$. But this is absurd. Since

$$\mathcal{O}^*/(\mathcal{O}^*)^2 \xrightarrow{\sim} \mathbb{F}_K^*/(\mathbb{F}_K^*)^2 \xrightarrow{\sim} \tfrac{1}{2}\mathbb{Z}/\mathbb{Z},$$

where the first arrow is induced by the reduction map, we see that $\left(\frac{a,b}{K}\right) = 0$ if and only if the reduction of b is a square.

□

Chapter 4

Quaternion Algebras over $\mathbb{Q}$

Although the "Hasse-Minkowski Theorem" holds for any number field K, here we only quote the $K = \mathbb{Q}$ case, because it is a classical result and the proof is relatively "elementary", part of the proof can be traced back to Legendre (in some what different terminology). See [Bor, §1.7] or [Ser] for details.

Theorem 7 (Hasse-Minkowski)**.** *A quadratic form with rational coefficients represents zero in $\mathbb{Q}$ if and only if it represents zero in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p.*

Another classical result is the summation formula: for every $a, b \in \mathbb{Q}^*$, then for p running through all places including the archimedean one,

$$\sum_p \left(\frac{a\,,\,b}{\mathbb{Q}_p} \right) = 0. \tag{4.1}$$

Note that by Corollary 3.6.1, the values of $\left(\frac{a\,,\,b}{\mathbb{Q}_p} \right)$ equal 0 for almost all p. Therefore, the summation is well-defined. The formula is basically an equivalence of Gauss' quadratic reciprocity formula. See [Bor, §1.7, p.66].

In Section §4.1, we apply Theorem 7 to the following:

Theorem 8. *Let $a, b, c, d \in \mathbb{Q}^*$. The following statements are equivalent:*

(a) *The quaternion algebra $\mathbb{H}(a, b)$ and $\mathbb{H}(c, d)$ are isomorphic over $\mathbb{Q}$.*

(b) *The quaternion algebra $\mathbb{H}(a, b)$ and $\mathbb{H}(c, d)$ are isomorphic over $\mathbb{Q}_p$, for all $p = \infty, 2, 3, \ldots.$*

(c) *We have* $\left(\frac{a\,,b}{\mathbb{Q}_p}\right) = \left(\frac{c\,,d}{\mathbb{Q}_p}\right)$, *for all* $p = \infty, 2, 3, ...$

Let $\mathrm{Br}_2(\mathbb{Q})$ denote the isomorphic classes of all quaternion over $\mathbb{Q}$. Then by Theorem 8, the map

$$\begin{array}{rcl} inv : \mathrm{Br}_2(\mathbb{Q}) & \longrightarrow & \bigoplus_{\text{all } p} \frac{1}{2}\mathbb{Z}/\mathbb{Z} \\ \mathbb{H}(a,b) & \mapsto & (\left(\frac{a\,,b}{\mathbb{Q}_p}\right))_p \end{array}$$

is injective. Here in the target of *inv*, the direct sum is taken over all places including the archimedean one. In view of the summation formula (4.1), we have the sequence

$$0 \longrightarrow \mathrm{Br}_2(\mathbb{Q}) \xrightarrow{inv} \bigoplus_{\text{all } p} \tfrac{1}{2}\mathbb{Z}/\mathbb{Z} \xrightarrow{\Sigma} \tfrac{1}{2}\mathbb{Z}/\mathbb{Z} \longrightarrow 0, \tag{4.2}$$

where Σ is the summation map. Finally, we have our main theorem.

Theorem 9. *We can endow* $\mathrm{Br}_2(\mathbb{Q})$ *an abelian group structure to make* (4.2) *an exact sequence of abelian groups.*

The proof of the theorem as well as an explicit description of the group operation on $\mathrm{Br}_2(\mathbb{Q})$ is given in §4.2.

4.1 The local-global relation

In this section we complete the proof of Theorem 8.

Proof of Theorem 8. Since over each $\mathbb{Q}_p$, $p = \infty, 2, 3, ...$, there are only two isomorphic classes of Quaternion and the value of Hilbert Symbol $\left(\frac{a\,,b}{\mathbb{Q}_p}\right)$ determines if $\mathbb{H}(a,b)$ is isomorphic to $\mathrm{M}(2,\mathbb{Q}_p)$ or not, we can conclude that (b)⇔(c). Also, the implication (a)⇒(b) is obvious. It remains to show (b)⇒(a).

Suppose (b) holds. Then $Q_{(a,b)}$ represents c in $\mathbb{Q}_p$ for all p. Therefore, by the Hasse-Minkowski theorem, $Q_{(a,b)}$ represents c in $\mathbb{Q}$. Hence, by Lemma 2.4.2, we have $Q_{(a,b)} \sim cx^2 + b'y^2 + b''z^2$. By computing the determinant, we see that b'' can be taken as $-cb'$, and hence $Q_{(a,b)} \sim Q_{(c,b')}$. Thus, it is sufficient to show that $f := b'y^2 - cbz^2$ and $g := dy^2 - cdz^2$ are equivalent over $\mathbb{Q}$. But the assumption of (b) implies that

$f \sim g$ over $\mathbb{Q}_p$ for all p. Since g represents d, f also represents d in all $\mathbb{Q}_p$. Then by Hass-Minkowski theorem, f represents d in $\mathbb{Q}$. Then again, by Lemma 2.4.2 and the determinant computation, we have $f \sim g$ as required. □

4.2 The Brauer group

Since the invariant map *inv* is injective, the group structure of $\mathrm{Br}_2(\mathbb{Q})$ is completely determined by that of $\bigoplus_{\text{all } p} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$. The point is for two pairs (a, b) and (c, d), we need to show there is the third (e, f) such that

$$inv(\mathbb{H}(e, f)) = inv(\mathbb{H}(a, b)) + inv(\mathbb{H}(c, d)). \tag{4.3}$$

One can prove this by first showing that the tensor product

$$\mathbb{H}(a, b) \otimes_{\mathbb{Q}} \mathbb{H}(c, d) = \mathrm{M}(2, \mathbb{H}(e, f)) \tag{4.4}$$

for some (e, f) that actually satisfies (4.3). This is the usual way to solve this problem, but it takes a long way to arrive at the end, one reason might be that (4.4) might not hold in for arbitrary field.

Fortunately, there is a direct way to do it. For a given pair (a, b), choose a finite set S of places of $\mathbb{Q}$ such that

$$\left(\frac{a\,,\,b}{\mathbb{Q}_p}\right) = 0 \text{ for every } p \notin S. \tag{4.5}$$

Write $\lambda_p = -1$, if $p = \infty$, and $\lambda_p = p$, otherwise.

Lemma 4.2.1. *Let the notation be as above. Then $Q_{(a,b)}$ represents the product $\lambda_S := \prod_{p \in S} \lambda_p$ in $\mathbb{Q}$.*

Proof. By the Hasse-Minkowski theorem, we need to show that $Q_{(a,b)}$ represents λ_S in all $\mathbb{Q}_p$. If $\left(\frac{a\,,\,b}{\mathbb{Q}_p}\right) = 0$, then $\mathbb{H}(a, b) = \mathrm{M}(2, \mathbb{Q}_p)$. Thus $Q_{(a,b)} \sim Q_{(1,1)}$ representing zero, and hence by Lemma 2.4.3, it represents λ_S.

Suppose $\left(\frac{a\,,\,b}{\mathbb{Q}_p}\right) = \frac{1}{2}$. Then $p \in S$. If $p = \infty$, then $\mathbb{H}(a, b) = \mathbb{H}(-1, -1)$ and λ_S is a negative in $\mathbb{Q}_p = \mathbb{R}$. Therefore, $\mathbb{H}(a, b)$ represents λ_S. If p is a finite prime number, then $\lambda_S = p{\cdot}u$, where $u \in \mathbb{Z}_p^*$. Choose $c \in \mathbb{Z}_p^*$ such that $\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p$ is unramified. By Proposition 3.6.1, u is contained in the group of norms $\mathrm{N}_{\mathbb{Q}_p(\sqrt{c})/\mathbb{Q}_p}(\mathbb{Q}_p(\sqrt{c})^*)$, while p is not. Thus, $\left(\frac{c\,,\lambda_S}{\mathbb{Q}_p}\right) = \frac{1}{2}$. Therefore $\left(\frac{a\,,b}{\mathbb{Q}_p}\right) = \left(\frac{c\,,\lambda_S}{\mathbb{Q}_p}\right)$, and hence $Q_{(a,b)} \sim Q_{(c,\lambda_S)}$, which represents λ_S. □

If the set S chosen satisfies (4.5) for (a, b) and S' contains S, then S' also satisfies (4.5) for (a, b). Thus, for two pairs (a, b) and (c, d), we can choose S to satisfies (4.5) for both (a, b) and (c, d). By Lemma 4.2.1, both $Q_{(a,b)}$ and $Q_{(c,d)}$ represent λ_S in $\mathbb{Q}$. Put $e = \lambda_S$. Then Lemma 2.4.2 and the computation of determinant imply that $Q_{(a,b)} \sim Q_{(e,b')}$ and $Q_{(c,d)} \sim Q_{(e,d')}$ for some b' and d'. In particular, $inv(\mathbb{H}(a, b)) = inv(\mathbb{H}(e, b'))$ and $inv(\mathbb{H}(c, d)) = inv(\mathbb{H}(e, d'))$, and hence

$$inv(\mathbb{H}(a, b)) + inv(\mathbb{H}(c, d)) = inv(\mathbb{H}(e, b')) + inv(\mathbb{H}(e, d')) = inv(\mathbb{H}(e, b'd')).$$

Put $f = b'd'$. Then (4.3) is satisfied. This defines the group structure on $\mathrm{Br}_2(\mathbb{Q})$, which we call the Brauer group of quaternions over $\mathbb{Q}$. Finally, we prove Theorem 9.

Proof of Theorem 9. We need to prove that every element $\xi = (\xi_p)_p \in \ker(\Sigma)$ can be written as $inv(\mathbb{H}(a, b))$ for some pair (a, b). Since now $\mathrm{Br}_2(\mathbb{Q})$ is a group and $\ker(\Sigma)$ is a vector space over $\mathbb{F}_2$, the field of order 2, it is sufficient to prove the statement for a basis of $\ker(\Sigma)$.

An obvious basis consists of E_q, $q = 2, 3, ...$, where the coordinate of E_q at $p = \infty$ and $p = q$ equals $\frac{1}{2}$ and other coordinates all equal 0. For instant, $E_2 = inv(\mathbb{H}(-1, -1))$. For each odd prime, consider $\mathbb{H}(-q, -q')$ where q' is another odd prime $\neq q$. Then $\left(\frac{-q,-q'}{\mathbb{R}}\right) = \left(\frac{-1,-1}{\mathbb{R}}\right) = \frac{1}{2}$. Also, if $p \neq 2, q, q'$, then $\left(\frac{-q,-q'}{\mathbb{Q}_p}\right) = 0$ by Corollary 3.6.1. Also, by Lemma 3.6.1, $\left(\frac{-q,-q'}{\mathbb{Q}_q}\right) = \frac{1}{2}$ if and only if

$$\text{“} -q' \;\; \textit{is not a quadratic residue modulo}\; q\text{”}, \tag{4.6}$$

while $\left(\frac{-q,-q'}{\mathbb{Q}_{q'}}\right) = 0$, if and only if

$$\text{“} -q \;\; \textit{is a quadratic residue modulo}\; q'\text{”}. \tag{4.7}$$

If $q \equiv 1 \pmod 4$, choose q' such that $q' \equiv 3 \pmod 4$ and q' not a quadratic residue modulo q, then by the quadratic reciprocity law, q is not a quadratic residue modulo q', and hence the above conditions (4.6) and (4.7) are satisfied. For such pair (q, q'), each coordinate of $inv(\mathbb{H}(q, q'))$ is the same as that of E_q except maybe the coordinate at $p = 2$. But, by (4.1), their coordinates at $p = 2$ also equal.

If $q \equiv 3 \pmod 4$, choose q' such that $q' \equiv 3 \pmod 4$ and q' a quadratic residue modulo q, then by the quadratic reciprocity law, q is not a quadratic residue modulo q', and hence the above conditions (4.6) and (4.7) are satisfied. Then we have $inv(\mathbb{H}(q, q')) = E_q$.

□

Bibliography

[Bor] Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Academic Press Inc, 1966.

[Lan] S. Lang, *Algebraic Number Theory*, second edition, Springer Verlag New York, 1994.

[Ser] J.-P. Serre, *A Course in Arithmetic*, Graduate texts in Mathematics, **7**, Springer Verlag New York, 1973.

[Wel] A, Weil, *Basic Number THeory*, Springer Verlag Berlin, Heidelberg, 1971.