# 國立交通大學

## 應用數學系

## 碩士論文

# 四元素代數

# Quaternion Algebras

研究生：郭泓呈

指導老師：康明軒　教授

中華民國一百三年七月

# 四元素代數

# Quaternion Algebras

研 究 生：郭泓呈　　Student：Hung-Cheng Kuo

指導教授：康明軒　　Advisor：Ming-Hsuan Kang

國 立 交 通 大 學

應用數學系

碩 士 論 文

A Thesis

Submitted to Department of Applied Mathematics

College of Science

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master

In

Applied Mathematics

July 2014

Hsinchu, Taiwan, Republic of China

中 華 民 國 一 百 三 年 七 月

# 四元素代數

學生：郭泓呈　　指導老師：康明軒教授

國立交通大學應用數學系碩士班

## 摘　要

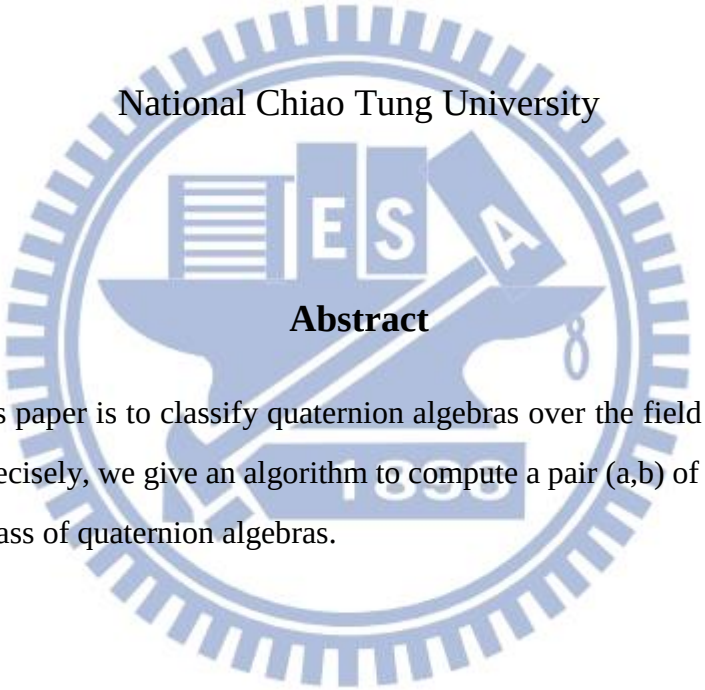
這篇論文主要是對四元素代數其係數為有理數作分類。更確切地說，我們提供一組演算法，對每一四元素代數的同構類利用此演算法計算一組非零整數(a,b)。

# Quaternion Algebras

Student: Hung-Cheng Kuo Advisor: Ming-Hsuan Kang

Department of Applied Mathematics

National Chiao Tung University



**Abstract**

The goal of this paper is to classify quaternion algebras over the field of rational numbers explicitly. More precisely, we give an algorithm to compute a pair (a,b) of nonzero integers for each isomorphic class of quaternion algebras.

# 目　　錄

In order to make the thesis self-contained, we only assume the readers are familiar with basic theory of groups, rings and fields and basic knowledge of metric spaces. The purpose of the article is to classify quaternion algebras over $\mathbb{Q}$ explicitly.

Here are some assumptions throughout the thesis: rings always have identities and ring homomorphisms always preserve identities and additive and multiplicative operations.

# 1 Preliminaries I

We shall recall some basic results about central simple algebras in order to introduce quaternion algebras in the next section. All the materials in the section could be found in [5].

**Definition.** *Let $K$ be a field. A $K$-algebra $A$ is a ring such that $A$ is a vector space over $K$ satisfying $a(xy) = (ax)y = x(ay)$ for any $x, y \in A$ and $a \in K$.*

Given a $K$-algebra $A$, the map $k \longrightarrow k1_A$ is a monomorphism from $K$ to $A$, where $1_A$ is the identity of $A$. We may assume the ground field $K$ is a subfield of $A$.

Recall that a group $G$ is simple if and only if $G$ has no nontrivial normal subgroup. Similarly, a simple ring is a ring which has no nontrivial ideal.

**Proposition 1.1.** *Let $D$ be a division ring.*

*(i) The center $Z(D)$ is a subfield of $D$ and any maximal subfield contains $Z(D)$.*

*(ii) There exists a maximal subfield.*

*(iii) Any division ring is a simple algebra over its center.*

**Definition.** *A central simple $K$-algebra $A$ is a simple $K$-algebra such that the center of $A$ is the field $K$.*

There is a classification theorem of central simple algebras.

**Theorem 1.2.** *(Artin-Wedderburn) Let $A$ be a finite dimensional central simple $K$-algebra. Then $A$ is $K$-algebra isomorphic to $M_{n\times n}(D)$ for some central division $K$-algebra $D$ (unique up to $K$-algebra isomorphism) and unique integer $n \geq 1$.*

Let $K$ be an algebraically closed field, e.g. $\mathbb{C}$. For any finite dimensional central division $K$-algebra $D$ and $d \in D$, $[D{:}K] < \infty$ implies that there exists a nonconstant polynomial $p \in K[x]$ with $p(d) = 0$. Since $K$ is algebraically closed, $d \in K$ and then $D = K$. Hence any finite dimensional central division

$K$-algebra is $K$. By Artin-Wedderburn theorem, any finite dimensional central simple $K$-algebras is a matrix algebra over $K$.

Before discussing central simple algebras over a finite field, we need the following theorem.

**Theorem 1.3.** *(Wedderburn) Every finite division ring is a field.*

Let $F_q$ be the finite field with $q$ elements. Combining two theorems above, any finite dimensional central division $F_q$-algebra is just the finite field $F_q$. Then any finite dimensional central simple $F_q$-algebra is a matrix algebra over $F_q$.

We shall introduce tensor products first before discussing further properties of division rings. Recall the multiplication of a ring $R$ follows the rules: $x(y+z) = xy + xz$, $(x+y)z = xz + yz$ for any $x, y, z \in R$. We hope there is a vector space in which one can take "products" xy of elements x in a vector space and y in another vector space and satisfying the two rules mentioned before.

Here is the construction of tensor products. Given two vector spaces $V$ and $W$ over a field $K$. Let $X$ be a vector space over $K$ with a basis $\{(v, w) | v \in V, w \in W\}$. Consider the subspace $Y$ of $X$ generated by

$$\begin{aligned}
&(v + v', w) - (v, w) - (v', w),\\
&(v, w + w') - (v, w) - (v, w'),\\
&(av, w) - a(v, w),\\
&(v, aw) - a(v, w),
\end{aligned}$$

for any $v, v' \in V$, $w, w' \in W$ and $a \in K$. Denote the quotient space $X/Y$ by $V \otimes_K W$ and $(v, w) + Y$ by $v \otimes w$. Then we have the following rules in $V \otimes_K W$: $(v + v') \otimes w = v \otimes w + v' \otimes w$, $v \otimes (w + w') = v \otimes w + v \otimes w'$ and $a(v \otimes w) = (av) \otimes w = v \otimes (aw)$. It can be shown that $v \otimes 0 = 0 \otimes w = 0$ for any $v, w$ and $\beta_1 \otimes \beta_2$ is a basis of $V \otimes_K W$ if $\beta_1$ and $\beta_2$ are basis of $V$ and $W$, respectively.

Given two $K$-algebras $A$ and $B$, choose two basis $\{x_\alpha\}$ and $\{y_\beta\}$ of $A$ and $B$, respectively. Define the multiplication on the basis $\{x_\alpha\} \otimes \{y_\beta\}$ by $(x_{\alpha_1} \otimes y_{\beta_1})(x_{\alpha_2} \otimes y_{\beta_2}) = x_{\alpha_1} x_{\alpha_2} \otimes y_{\beta_1} y_{\beta_2}$. Extend the multiplication linearly. In this way, $A \otimes_K B$ forms a $K$-algebra. The identity of $A \otimes_K B$ is $1 \otimes 1$. The multiplication we defined is independent of the choice of basis of $A$ and $B$. The maps $x \longrightarrow x \otimes 1$ and $y \longrightarrow 1 \otimes y$ are $K$-algebra monomorphisms. This means $A \otimes_K B$ is a $K$-algebra contains isomorphic copies of $A$ and $B$. If $F$ is an extension field of $K$ and $A$ is a vector space over $F$, $A \otimes_K B$ is an $F$-algebra with $\alpha(x \otimes y) = (\alpha x) \otimes y$, where $\alpha \in F$, $x \in A$ and $y \in B$. In particular, $F \otimes_K B$ is an $F$-algebra with $F$-basis $1 \otimes \{y_\beta\}$. This can be regarded as extending the coefficients of $B$ from $K$ to $F$. When $B$ is a central division $K$-algebra, there are more properties about $B$.

**Proposition 1.4.** *Let $D$ be a central division $K$-algebra, $F$ be a maximal subfield and $A$ be a $K$-algebra.*

*(i)* $[D{:}K]$ *is finite if and only if* $[F{:}K]$ *is finite.*

*(ii)* $F \otimes_K D \cong M_{n\times n}(F)$ *as $F$-algebras and* $[D{:}K]=[F{:}K]^2$ *if* $[D{:}K]<\infty$.

*(iii)* $F \otimes_K M_{n\times n}(A) \cong M_{n\times n}(F \otimes_K A)$ *as $F$-algebras for any* $n \geq 1$.

The proposition says if we extend the coefficients of a finite dimensional central division algebra from the ground field to its maximal subfield, the extended algebra is a matrix algebra over the maximal subfield.

Let $A$ be a finite dimensional central simple $K$-algebra. By Artin-Wedderburn theorem, $A \cong M_{n\times n}(D)$ for some central division algebra over $K$ and $n \geq 1$. Let $F$ be a maximal subfield of $D$ and $m{=}[F{:}K]$. Then $F \otimes_K A \cong M_{n\times n}(F \otimes_K D) \cong M_{n\times n}(M_{m\times m}(F)) \cong M_{nm\times nm}(F)$.

This means after extending the coefficients, the extended algebra may become a matrix algebra over a field.

**Definition.** *A finite dimensional central simple $K$-algebra $A$ splits over a field $F$ if $F$ is an extension field of $K$ satisfying $F \otimes_K A \cong M_{n\times n}(F)$ for some $n \geq 1$. In this case, $F$ is called a splitting field of $A$.*

For further properties of central simple algebras, see Section 8.

Recall that for any element $g$ of a group $G$, the map $x \longrightarrow gxg^{-1}$ is an automorphism of $G$, called an inner automorphism of $G$. Given a central simple $K$-algebra $A$, the maps of the form $x \longrightarrow axa^{-1}$, where $a \in A^{\times}$, are also automorphisms, inner automorphisms of $A$.

**Theorem 1.5.** *(Noether-Skolem) Let $A$ be a finite dimensional central simple $K$-algebra and $B_1$ and $B_2$ be two $K$-subalgebras of $A$. If $\phi : B_1 \longrightarrow B_2$ is a $K$-algebra isomorphism, there exists an inner automorphism $\Phi$ of $R$ such that $\Phi|_{B_1} = \phi$.*

As a corollary of Noether-Skolem theorem, every automorphism of a finite dimensional central simple algebra is an inner automorphism.

## 2 Basic Properties of Quaternion Algebras

For convenience, we assume the ground field $K$ is of characteristic not equalt to 2 when discussing quaternion algebras. Except for Theorem 2.12 and Corollary 2.13, the materials in this section come from [1].

**Definition.** *A quaternion algebra $H$ over $K$ is a $K$-algebra with a basis $\{1, i, j, ij\}$ satisfying $i^2 = a, j^2 = b$ and $ij = -ji$, where $a$ and $b$ are some nonzero elements of $K$. In this case, $\{1, i, j, ij\}$ is called a standard basis corresponding to $(a, b)$.*

**Lemma 2.1.** *Let $A$ be a $K$-algebra. If $i$ and $j$ are two elements of $A$ satisfying $i^2 = a \in K^\times, j^2 = b \in K^\times$ and $ij = -ji$, then $\{1, i, j, ij\}$ is linearly independent over $K$.*

*Proof.* Suppose $a_1+a_2i+a_3j+a_4ij = 0$. Since $K$ is of characteristic not equal to 2, we have $0 = i(a_1+a_2i+a_3j+a_4ij)i^{-1} = a_1+a_2i-a_3j-a_4ij$, $a_1+a_2i = 0$ and $a_3j + a_4ij = 0$. Since $j$ is a unit of $A$, we have $a_1 + a_2i = a_3 + a_4i = 0$. $ij = -ji$ and $j \in A^\times$ imply the equality $jij^{-1} = -i$. By the equality and $0 = j(a_1 + a_2i)j^{-1}$, we obtain $a_1 - a_2i = 0$ and then $a_1 = a_2 = 0$ since $K$ is of characteristic not equal to 2. Similarly, $a_3 = a_4 = 0$. Therefore $\{1, i, j, ij\}$ is linearly independent over $K$. □

From the proof of the lemma, if we replace the condition $j^2 = b \in K^\times$ by $j \in A^\times$, the lemma still holds.

Given a quaternion algebra $H$ with a standard basis $\{1, i, j, ij\}$ corresponding to $(a, b)$, the multiplication rules on $H$ are determined by the pair $(a, b)$. Hence we write $H = (\frac{a,b}{K})$ while the quaternion algebra $H$ over $K$ has a standard basis corresponding to $(a, b)$.

**Theorem 2.2.** *Let $a, b \in K^\times$. Then $(\frac{a,b}{K})$ exists.*

*Proof.* Let $\overline{K}$ be an algebraic closure of $K$. Choose $\alpha, \beta \in \overline{K}$ with $\alpha^2 = a$ and $\beta^2 = -b$. Put $i = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & -\alpha \end{smallmatrix}\right)$ and $j = \left(\begin{smallmatrix} 0 & \beta \\ -\beta & 0 \end{smallmatrix}\right)$. Then $i^2 = aI_2, j^2 = bI_2$ and $ij = -ij$. By Lemma 2.1, $\{1, i, j, ij\}$ is independent over $K$. Hence the 4-dimensional $K$-subspace generated by $\{1, i, j, ij\}$ is a quaternion algebra over $K$. □

It is possible that $(\frac{a,b}{K}) \cong (\frac{c,d}{K})$ for two different pairs $(a, b)$ and $(c, d)$. In other words, $(\frac{a,b}{K})$ may contain another standard basis $\{1, \hat{i}, \hat{j}, \hat{i}\hat{j}\}$ corresponding to $(c, d)$ for some $(c, d) \neq (a, b)$. It is easy to prove the following proposition.

**Proposition 2.3.** *Let $a, b, c \in K^\times$.*

*(i)* $(\frac{a,b}{K}) \cong (\frac{b,a}{K})$.

*(ii)* $(\frac{a,b}{K}) \cong (\frac{ac^2,bd^2}{K})$ *for any* $c, d \in K^\times$.

*(iii)* $M_{2\times2}(K) = (\frac{1,c}{K})$ *with* $i = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ *and* $j = \left(\begin{smallmatrix} 0 & c \\ 1 & 0 \end{smallmatrix}\right)$.

There is a characterization of quaternion algebras which we need in Section 8.

**Proposition 2.4.** *Every quaternion algebra over $K$ is a 4-dimensional central simple $K$-algebra, and vice versa.*

*Proof.* Let $H = (\frac{a,b}{K})$ be a quaternion algebra and $I$ be a proper ideal of $H$. Then $H/I$ is a $K$-algebra and, by Lemma 2.1, $\{1+I, i+I, j+I, ij+I\}$ is a $K$-basis of $H/I$. Thus I is a zero ideal and H is a simple ring. Let $x = a_1 + a_2 i + a_3 j + a_4 ij$ be an element in the center of $H$. Comparing the coefficients from $ix = xi$ and $jx = xj$, we have $a_2 = a_3 = a_4 = 0$ and $x = a_1 \in K$. Hence H is a 4-dimensional central simple $K$-algebra.

Conversely, let $A$ be a 4-dimensional central simple $K$-algebra. By Artin-Wedderburn theorem, $A$ is a 4-dimensional central division $K$-algebra or $A$ is isomorphic to $M_{2\times 2}(K)$. From Proposition 2.3, $M_{2\times 2}(K)$ is a quaternion algebra over $K$. We may assume that $A$ is a 4-dimensional central division $K$-algebra. Choose $\alpha \in A - K$. Since $K \subset K(\alpha) \subset A$ are division rings, we have $4 = [A : K] = [A : K(\alpha)][K(\alpha) : K]$. That A is noncommutative and $[K(\alpha) : K] > 1$ implies $[K(\alpha) : K] = 2$. Moreover, $K(\alpha) = K(\sqrt{a})$ for some $a \in K^\times$ since $K$ is of characteristic not equal to 2. Put $i = \sqrt{a}$. Since $i \in A - K$, $x^2 - 1$ is the minimal polynomial of $\phi$ over $K$, where $\phi$ is the inner automorphism $z \longrightarrow izi^{-1}$. Then $\phi$ has an eigenvector $j$ corresponding to $-1$, that is, $ij = -ji$. Since $i^2 = a \in K^\times, j \in A^\times$ and $ij = -ji$, it can be shown that $\{1, i, j, ij\}$ is independent over $K$ by the same argument of Lemma 2.1. It is easy to check that $j^2$ commutes all elements of the basis and thus $j^2 = b \in Z(A) = K$. Therefore $A = (\frac{a,b}{K})$. □

In order to determine whether $H$ is a division algebra or not, we need the concept of pure quaternions and norm maps to obtain some criteria.

**Definition.** *Let $H = (\frac{a,b}{K})$ be a quaternion algebra and $\{1, i, j, ij\}$ be a standard basis corresponding to $(a, b)$. The subsapce $H_0 = Ki \oplus Kj \oplus Kij$ is called the pure quaternion of $H$.*

By straightforward computation, we have the following proposition.

**Proposition 2.5.** *If $x \in H = (\frac{a,b}{K})$, then $x^2 \in K$ if and only if $x \in K$ or $x \in H_0$.*

The proposition above implies the pure quaternion is independent of the choice of standard basis. In other words, if a quaternion algebra $H$ contains two standard basis $\{1, i_1, j_1, i_1 j_1\}$ and $\{1, i_2, j_2, i_2 j_2\}$, the pure quaternion of $H$ is $Ki_1 \oplus Kj_1 \oplus Ki_1 j_1 = Ki_2 \oplus Kj_2 \oplus Ki_2 j_2$.

**Definition.** *Let $H$ be a quaternion algebra. For any $x = a + \alpha \in H$, $a \in K, \alpha \in H_0$, the element $\overline{x} = a - \alpha$ is called the conjugate of $x$.*

Recall the opposite ring $R^{op}$ of a ring $R$ is another ring with the same elements and addition operation, but the multiplication on $R^{op}$ is performed in the reverse order. It is clear that the opposite ring of a central simple $K$-algebra is still a central simple $K$-algebra.

It is easy to prove the following proposition if we write the conjugate map as linear combinations of a fixed standard basis.

**Proposition 2.6.** *Let $H$ be a quaternion algebra. The map $H \longrightarrow H^{op}$ by $x \longrightarrow \overline{x}$ is a $K$-algebra isomorphism, where $H^{op}$ is the opposite ring of $H$.*

The proposition above implies the corresponding class of a quaternion algebra in the Brauer group is of order 1 or 2. See Section 8.

For a quaternion algebra $H = (\frac{a,b}{K})$ and $a \notin (K^\times)^2$, $K \oplus Ki$ is a quadratic extension field of $K$. The Galois group is generated by the map $\sigma : i \longrightarrow -i$. Hence the conjugate map is an extension of $\sigma$.

Let $H$ be a quaternion algebra constructed in Theorem 2.2 and a matrix $x = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in H$. Then $\overline{x} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, i.e. the classical adjoint matrix of $x$. Moreover, we have $x\overline{x} = \det(x)I_2$ and $x + \overline{x} = \mathrm{tr}(x)I_2$.

**Definition.** *Let $H$ be a quaternion algebra. The map $N : H \longrightarrow H$ by $x \longrightarrow x\overline{x}$ is called the norm map and $T : H \longrightarrow H$ by $x \longrightarrow x + \overline{x}$ is called the trace map.*

From the definition the norm map and trace map are independent of the choice of standard basis. For each standard basis of a quaternion algebra, it is easy to write down the norm map and trace map explicitly.

**Proposition 2.7.** *Let $H = (\frac{a,b}{K})$ be a quaternion algebra. For $a, a_i \in K$, $\alpha \in H_0$ and $x, y \in H$,*

*(i)* $N(a_1 + a_2 i + a_3 j + a_4 ij) = a_1^2 - aa_2^2 - ba_3^2 + aba_4^2$;

*(ii)* $N(xy) = N(x)N(y)$ *and* $N(ax) = a^2 N(x)$;

*(iii)* $N(a + \alpha) = a^2 - \alpha^2$;

*(iv)* $T(a_1 + a_2 i + a_3 j + a_4 ij) = 2a_1$;

*(v)* $T(x + y) = T(x) + T(y)$ *and* $T(ax) = aT(x)$;

*(vi)* $H^\times = \{x \in H | N(x) \neq 0\}$ *and* $x^{-1} = \frac{\overline{x}}{N(x)}$;

*(vii) $H$ is a division algebra if and only if $N(x) \neq 0$ for any $x \neq 0 \in H$.*

For a quaternion algebra $H = (\frac{a,b}{K})$ and $a \notin (K^\times)^2$, the restriction of norm map and trace map on $F = K \oplus Ki$, which is the quadratic extension field of $K$, are the norm $N_{F/K}$ and trace $T_{F/K}$.

Since the norm map and trace map are independent of the choice of standard basis and any isomorphism of quaternion algebras preserves standard basis, the norm map and trace map are invariant under isomorphism.

**Proposition 2.8.** *Let $H_1$ and $H_2$ be two quaternion algebras over $K$. If $\phi : H_1 \longrightarrow H_2$ is a $K$-algebra isomorphism, $\phi(\overline{x}) = \overline{\phi(x)}$, $N(\phi(x)) = N(x)$ and $T(\phi(x)) = T(x)$ for all $x \in H_1$.*

Here is the first criterion for splitness.

**Theorem 2.9.** *Let $H = (\frac{a,b}{K})$ be a quaternion algebra. The following conditions are equivalent:*

*(i) $H$ splits over $K$.*

*(ii) There exists an $x \neq 0 \in H$ with $N(x) = 0$.*

*(iii) $b \in N_{F/K}(F^\times)$, where $F = K(\sqrt{a})$.*

*(iv) $a \in N_{F/K}(F^\times)$, where $F = K(\sqrt{b})$.*

*Proof.* (i)⇒(ii): Since $H$ splits over $K$ $H \cong M_{2\times 2}(K)$ which is not a division algebra, by (vii) in Proposition 2.7, there must exists a nonzero element $x$ such that $N(x) = 0$. (ii)⇒(iii): By hypothesis, $0 = a_1^2 - aa_2^2 - ba_3^2 + aba_4^2$ for some $(a_1, a_2, a_3, a_4) \neq (0, 0, 0, 0) \in K^4$. Then $a_1^2 - aa_2^2 = b(a_3^2 - aa_4^2)$. When $a$ is square, $b$ is in the image of norm. When $a$ is nonsquare, we have $a_1^2 - aa_2^2 = b(a_3^2 - aa_4^2) \neq 0$. Hence

$$b = \frac{a_1^2 - aa_2^2}{a_3^2 - aa_4^2} = \frac{N_{F/K}(a_1 + a_2\sqrt{a})}{N_{F/K}(a_3 + a_4\sqrt{a})} = N_{F/K}((a_1 + a_2\sqrt{a})(a_2 + a_4\sqrt{a})^{-1})$$

and $b$ is in the image of the norm. (iii)⇒(i): By Proposition 2.3, $H$ splits over $K$ if $a$ is square. For a nonsquare $a$, $b = x^2 - ay^2$ for some $(x, y) \neq (0, 0)$. $0 = x^2 - ay^2 - b = N(x + yi + j)$ and $x + yi + j \neq 0$. By Proposition 2.3 again, $H$ is not a division algebra. Hence $H$ splits over $K$. (ii)⇒(iv) and (iv)⇒(i) are proved in similar arguments. □

**Corollary 2.10.** *Let $a \in K^\times$. $(\frac{a,-a}{K}) \cong M_{2\times 2}(K)$.*

*Proof.* $\{1, i, j, ij\}$ is a standard basis corresponding to the pair $(a, -a)$. Since $N(i + j) = -a(1) - (-a)(1) = 0$, by Theorem 2.9, $(\frac{a,-a}{K}) \cong M_{2\times 2}(K)$. □

**Corollary 2.11.** *Let $p$ be a prime. The quaternion algebra $(\frac{-1,p}{\mathbb{Q}})$ splits over $\mathbb{Q}$ if and only if $p = 2$ or $p \equiv 1$ mod 4.*

*Proof.* By Theorem 2.9, $(\frac{-1,p}{\mathbb{Q}})$ splits over $\mathbb{Q}$ if and only if $p = x^2 + y^2$ some $(x, y) \neq (0, 0) \in \mathbb{Q}^2$. From elementary number theory, any positive integer $n$ is a sum of two square of integers if and only if all prime factors of $n$ of the form $4m + 3$ have even exponent in the prime factorization of $n$. Hence $(\frac{-1,p}{\mathbb{Q}})$ splits over $\mathbb{Q}$ if $p = 2$ or $p \equiv 1$ mod 4. Conversely, $p = (\frac{a}{b})^2 + (\frac{c}{d})^2$ for some $(\frac{a}{b}, \frac{c}{d}) \neq (0, 0) \in \mathbb{Q}^2$. $d^2 | b^2d^2p = a^2d^2 + c^2b^2$ implies $d|b$ since $c, d$ are relatively prime. Similarly, $b|d$ and thus $b = d$. Now, we have $b^2p = a^2 + c^2$, which implies all prime factors of $a^2 + c^2$ of the form $4m + 3$ have even exponent. Therefore $p = 2$ or $p \equiv 1$ mod 4. □

The key point in the proof of Proposition 2.4 is to prove the existness of element $z$ such that $iz = -zi$. Suppose $H = (\frac{a,b}{K})$ is a quaternion algebra containing an element $z$ such that $iz = -zi$ . Then $z = xj + yij$, where $(x, y) \neq (0, 0) \in K^2$. And $z^2 = (xj + yij)^2 = b(x^2 - ay^2)$. By Lemma 2.1, $\{1, i, z, iz\}$ is a standard basis corresponding to the pair $(a, b(x^2 - ay^2))$ if $z^2 \neq 0$. With the observation we can characterize some families of quaternion algebras in the following theorem.

**Theorem 2.12.** *Let $a, b, c \in K^\times$. Two quaternion algebras $(\frac{a,b}{K})$ and $(\frac{a,c}{K})$ are isomorphic if and only if $\overline{b} = \overline{c}$ in $K^\times/N_{F/K}(F^\times)$, where $F = K(\sqrt{a})$.*

*Proof.* If $a$ is square, both sides hold trivially. We may assume $a$ is non-square. Let $\{1, i, j, ij\}$ be the standard basis of $(\frac{a,b}{K})$ and suppose $\overline{b} = \overline{c}$. Then $c = b(x^2 - ay^2)$ for some $(x, y) \neq (0, 0)$. Put $j' = xj + yij$. Hence $j'^2 = b(x^2 - ay^2)$ and $ij' = -j'i$. By Lemma 2.1, $\{1, i, j', ij'\}$ is a standard basis of $(\frac{a,b}{K})$ corresponding to $(a, b(x^2 - ay^2) = (a, c)$ and thus $(\frac{a,b}{K}) \cong (\frac{a,c}{K})$.

Conversely, suppose $(\frac{a,b}{K})$ and $(\frac{a,c}{K})$ are isomorphic. By assumption, $(\frac{a,b}{K})$ contains a standard basis $\{1, \tilde{i}, \tilde{j}, \tilde{i}\tilde{j}\}$ corresponding to the pair $(c, d)$. Since $\phi : K \oplus K\tilde{i} \longrightarrow K \oplus Ki$ by $\tilde{i} \longrightarrow i$ is an isomorphism, by Noether-Skolem theorem, $\phi$ can be extended to an inner automorphism $\Phi$ of $(\frac{a,b}{K})$. Write $\Phi(\tilde{j}) = a_1 + a_2 i + a_3 j + a_4 ij$. Since $\tilde{i}\tilde{j} = -\tilde{j}\tilde{i}$ and $\Phi(\tilde{i}) = \phi(\tilde{i}) = i$, $a_1 = a_2 = 0$ and $\Phi(\tilde{j}) = a_3 j + a_4 ij$. Hence $c = (\Phi(\tilde{j}))^2 = (a_3 j + a_4 ij)^2 = b(a_3^2 - aa_4^2)$. □

**Corollary 2.13.** *For any two distinct odd primes $p, q \equiv 3$ mod 4, $(\frac{-1,p}{\mathbb{Q}})$ and $(\frac{-1,q}{\mathbb{Q}})$ are nonisomorphic division algebras.*

*Proof.* By Corollary 2.11 , $(\frac{-1,p}{\mathbb{Q}})$ is a division algebra for any odd prime $p \equiv 3$ mod 4. Suppose there are two distinct primes $p, q \equiv 3$ mod 4 with $(\frac{-1,p}{\mathbb{Q}}) \cong (\frac{-1,q}{\mathbb{Q}})$. From Theorem 2.12

$$p = q[(\frac{a}{b})^2 + (\frac{c}{d})^2] \tag{1}$$

for some $(\frac{a}{b}, \frac{c}{d}) \neq (0, 0) \in \mathbb{Q}^2$. Then $b^2d^2p = q[a^2d^2 + c^2b^2]$ and $q$ must divide $b$ or $d$. We may assume that $q|b$. We have $q^2|b^2d^2p = q[a^2d^2 + c^2b^2]$ and thus $q|a^2d^2 + c^2b^2$. Since $q|b$ and $q|a^2d^2 + c^2b^2$ , $q|a^2d^2$. If $q|a$, then $q|(a, b) = 1$, a contradiction. Hence $b$ and $d$ have a common prime factor $q$. Rewrite (1):

$$p = q[(\frac{a}{e})^2 + (\frac{c}{f})^2]\frac{1}{q^2} \tag{2}$$

, where $e = \frac{b}{q}, f = \frac{d}{q} \in \mathbb{N}$. By (2), we have $e^2f^2pq = a^2f^2 + c^2e^2$. All prime factors of $a^2f^2 + c^2e^2$ of the form $4m+3$ have even exponent. But the prime factor of $e^2f^2pq$ of $p$ has odd exponent, a contradiction. □

From the corollary, we know there are infinitely many nonisomorphic quaternion algebras over $\mathbb{Q}$.

# 3 Viewpoints from Quadratic Forms

We shall recall some basic results about symmetric bilinear forms and quadratic forms. Detailed proofs can be founded in [6],[8].

**Definition.** *Let $V$ be a vector space over $K$. The map $\phi : V \times V \longrightarrow K$ is a symmetric bilinear form if for each $x \in V$, $\phi(x, \ . \ )$ and $\phi(\ . \ , x)$ are linear maps from $V$ to $K$ and $\phi(x, y) = \phi(y, x)$ all $x, y \in V$. A vector space $V$ equipped a symmetric bilinear form $\phi$ is denoted by $(V, \phi)$.*

The easiest example of symmetric bilinear forms is the inner product on the Euclidean space $\mathbb{R}^n$.

**Definition.** *Let $V$ be a vector space over $K$. A symmetric bilinear form $\phi$ is nondegenerate if the map $x \longrightarrow \phi(x, \ . \ )$ is a monomorphism from from $V$ to its dual space $V^*$.*

It is clear that a symmetric bilinear form $\phi$ on a finite dimensional vector space $V$ is nondegenerate if and only if the map $x \longrightarrow \phi(x, \ . \ )$ is an isomorphism. Let $X = \{x_i\}$ be a basis and $x = \sum_i a_i x_i$, $y = \sum_i b_i x_i \in V$. Then $\phi(x, y) = [a_i]^t [\phi(x_i, x_j)][b_i]$. That means $\phi$ is determined by the matrix $[\phi(x_i, x_j)]$, denoted $[\phi]_X$. One can proved $\phi$ is nondegenerate if and only if $[\phi]_X$ is invertible. If $Y = \{y_i\}$ is also a basis, we have $[\phi]_X = P^t [\phi]_Y P$ for some invertible matrix $P$. Therefore $\phi$ is nondegenerate if and only if $[\phi]_X$ is invertible for any basis $X$ of $V$.

Now we are going to see what is a quadratic form. Consider a symmetric bilinear form $\phi$ on $K^n$ and $(a_{ij})$ be the matrix corresponding to the standard basis. Then $\phi((x_1, ..., x_n), (x_1, ..., x_n)) = \sum_{i,j} a_{ij} x_i x_j$. Hence we can associate a homogeneous polynomial of degree 2 in variables $x_1, ..., x_n$ with a symmetric bilinear form on a $n$-dimensional vector space if a basis is fixed.

**Definition.** *Let $V$ be a vector space over $K$. The map $Q : V \longrightarrow K$ is a quadratic form if the map $\phi(x, y) = \frac{1}{2}[Q(x+y) - Q(x) - Q(y)]$ is a symmetric bilinear form on $V$. A vector space $V$ equipped a quadratic form $Q$ is denoted by $(V, Q)$, which called a quadratic space.*

We shall point out the relationship among symmetric bilinear forms, quadratic forms and homogeneous polynomials of degree 2.

**Proposition 3.1.** *Let $V$ be a $n$-dimensional vector space over $K$ and $\{v_i\}$ be a basis of $V$.*

*(i) The map $\phi \longrightarrow Q$, where $Q$ is defined by $Q(x) = \phi(x, x)$, is a bijection between the set of symmetric bilinear forms and the set of quadratic forms.*

*(ii) The map* $\phi \longrightarrow \sum_{i,j} \phi(v_i, v_j)x_i x_j$ *is a bijection between the set of symmetric bilinear forms and the set of homogeneous polynomials of degree 2 in variables* $x_1, ..., x_n$.

**Definition.** *Let* $(V_i, Q_i)$ *be a quadratic space and* $\phi_i$ *be the corresponding symmetric bilinear form,* $i = 1, 2$. $Q_1$ *and* $Q_2$ *are equivalent, denoted* $(V_1, Q_1) \cong (V_2, Q_2)$, *if there is an isomorphism* $\Phi : V_1 \longrightarrow V_2$ *such that* $Q_2(\Phi(x)) = Q_1(x)$ *for any* $x \in V_1$. $\phi_1$ *and* $\phi_2$ *are equivalent, denoted* $(V_1, \phi_1) \cong (V_2, \phi_2)$, *if there is an isomorphism* $T : V_1 \longrightarrow V_2$ *such that* $\phi_2(Tx, Ty) = \phi_1(x, y)$ *for any* $x, y \in V_1$.

It is clear that two quadratic forms are equivalent if and only if the corresponding symmetric bilinear forms are equivalent.

Go back to quaternion algebras.

**Proposition 3.2.** *Let* $H$ *be a quaternion algebra. Then the norm map* $N$ *is a quadratic form on* $H_0$.

*Proof.* Suppose $H = (\frac{a,b}{K})$. Let $\{1, i, j, ij\}$ be a standard basis corresponding to $(a, b)$. For $x = a_1 i + a_2 j + a_3 ij$, $y = b_1 i + b_2 j + b_3 ij \in H_0$,

$$\phi(x, y) = \frac{1}{2}[N(x + y) - N(x) - N(y)] = -aa_1b_1 - ba_2b_2 + aba_3b_3. \quad (3)$$

It is easy to see that $\phi$ is a symmetric bilinear form on $H_0$ and then $N$ is a quadratic form. □

**Theorem 3.3.** *Let* $H_i$ *be a quaternion algebra with norm map* $N_i$ , $i = 1, 2$. *Then* $H_1 \cong H_2$ *if and only if* $((H_1)_0, N_1) \cong ((H_2)_0, N_2)$.

*Proof.* Suppose $\Phi : H_1 \longrightarrow H_2$ is an isomorphism. Let $x$ be an element of pure quaternion of $H_1$. By Proposition 2.5, $x \notin K$ and $x^2 \in K$ and then $\Phi(x) \notin K$ and $\Phi(x)^2 \in K$, i.e. $\Phi(x) \in (H_2)_0$. Since any isomorphism of quaternion algebras keeps the values of norm maps (Proposition 2.8), the restriction $\Phi$ is an isomorphism of two quadratic spaces $((H_i)_0, N_i)$, $i = 1, 2$. Conversely, let $\sigma : (H_1)_0 \longrightarrow (H_2)_0$ be an isomorphism of quadratic spaces and $\{1, i, j, ij\}$ be a standard basis of $H_1$. By (iii) in Proposition 2.7, the equivalence of the corresponding symmetric bilinear forms $\phi_i$ and the equality $\phi_i(x, y) = -\frac{1}{2}(xy + yx) \in K$ for elements $x$, $y$ in pure quaternions, one can show that $\{1, \sigma(i), \sigma(j), \sigma(i)\sigma(j)\}$ is a standard basis of $H_2$. Hence the isomorphism of vector spaces by $1 \longrightarrow 1$, $i \longrightarrow \sigma(i)$, $j \longrightarrow \sigma(j)$ and $ij \longrightarrow \sigma(i)\sigma(j)$ is a $K$-algebra isomorphism. □

# 4 Preliminaries II

We shall recall some results about the theory of valuations and local fields which we need in the next section. Detailed Proofs could be found in [5],[6].

In order to apply Theorem 2.9 and Theorem 2.12 in the next section, we shall find all the quadratic extension fields of $p$-adic fields and characterize the images of their norms.

**Definition.** *An absolute value on a field $K$ is a map $\| \ . \ \|: K \longrightarrow \mathbb{R}_{\geq 0}$ satisfying the following properties:*

*(i)* $\| x \| = 0$ *if and only if* $x = 0$.

*(ii)* $\| xy \| = \| x \| \| y \|$ *for any* $x, y \in K$.

*(iii)* $\| x + y \| \leq \| x \| + \| y \|$ *for any* $x, y \in K$.

*The group $\| K^{\times} \|$ is called the the value group of $K$ with respect to $\| \ . \ \|$. If an absolute value satisfies $\| x + y \| \leq \max(\| x \|, \| y \|)$ for all $x$, $y$, the absolute value is called nonarchimedean; Otherwise, it is called archimedean.*

The usual absolute value on $\mathbb{Q}$ is archimedean. For each prime $p$, the $p$-adic absolute value on $\mathbb{Q}$ is defined by $\| \frac{a}{b} \|_p = (\frac{1}{p})^{\mathrm{ord}_p(a) - \mathrm{ord}_p(b)}$, where $\mathrm{ord}_p(a)$ is the exponent of $p$ in the prime factorization of nonzero integer $a$. The $p$-adic absolute value is nonarchimedean.

**Definition.** *Let $K$ be a field with absolute values $\| \ . \ \|_1$ and $\| \ . \ \|_2$. $\| \ . \ \|_1$ and $\| \ . \ \|_2$ are equivalent if $\{x_n\}$ is a Cauchy sequence with respect to $\| \ . \ \|_1$ if and only if $\{x_n\}$ is a Cauchy sequence with respect to $\| \ . \ \|_2$.*

There are several characterizations of equivalence of absolute values. Let $\| \ . \ \|_1$ and $\| \ . \ \|_2$ be absolute values on a field. $\| \ . \ \|_1$ and $\| \ . \ \|_2$ are equivalent if and only if there is an $a > 0$ such that $\| \ . \ \|_2 = \| \ . \ \|_1^a$ if and only if the corresponding topologies are the same.

**Theorem 4.1.** *(Ostrowski) Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to the usual absolute value or the $p$-adic absolute value for some unique prime $p$.*

Ostrowski's theorem says all nontrivial absolute value on $\mathbb{Q}$ are the usual absolute value and $p$-adic absolute value for all primes $p$ up to equivalence.

**Definition.** *The usual absolute value on $\mathbb{Q}$ is called the infinite place, denoted by $\infty$ or -1. And $\mathbb{R}$ is denoted by $\mathbb{Q}_{\infty}$ or $\mathbb{Q}_{-1}$. For each prime $p$ the $p$-adic absolute value is called a finite place, denoted by $p$.*

Recall that a commutative ring $R$ is local if and only if there is a unique maximal ideal of $R$(or equivalently, $R - R^{\times}$ is an ideal).

**Proposition 4.2.** *Let $K$ be a field with a nonarchimedean absolute value $\| \ . \ \|$.*

*(i)* $\mathcal{O}_K = \{x \in K | \ \| x \| \leq 1\}$ *is a an integral domain with a unique maxiaml ideal $\mathcal{M}_K$ and the group of units is $\{x \in K | \ \| x \| = 1\}$.*

*(ii)* $\mathcal{O}_K$ *is a principal ideal domain with a unique maximal ideal* $(\pi)$*, where* $\| \pi \|$ *generates the value group, if the value group is cyclic of infinite order.*

**Definition.** *Let* $K$ *be a field with a nonarchimedean absolute value* $\| \cdot \|$*.* $\mathcal{O}_K$ *is called the valuation ring with respect to* $\| \cdot \|$*. The field* $\mathcal{O}_K/\mathcal{M}_K$ *is called the residue field. For the second case in the proposition above,* $\pi$ *is called a uniformizer which is unique up to units and* $\| \cdot \|$ *is called a discrete nonarchimedean absolute value.*

For the $p$-adic absolute value on $\mathbb{Q}$, $p$ is an uniformizer and the value group is $\langle \frac{1}{p} \rangle$, which is an infinite cyclic subgroup of $\mathbb{R}_{>0}$. The valuation ring is $\{ \frac{a}{b} \in \mathbb{Q} | b \notin p\mathbb{Z} \}$, which is the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$. The residue field is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ by $\frac{a}{b} \longrightarrow (a + p\mathbb{Z})(b + p\mathbb{Z})^{-1}$.

Since a field with an absolute value forms a metric space, we can discuss convergence, Cauchy sequences, completeness, denseness, *etc.*

**Theorem 4.3.** *Let* $K$ *be a field with an absolute value* $\| \cdot \|$*. There exists a field* $\hat{K}$*, which is complete with respect to an absolute value* $\| \cdot \|'$*, and a monomorphism* $\phi : K \longrightarrow \hat{K}$ *preserving absolute values such that* $K$ *is dense in* $\hat{K}$*.*

*Moreover,* $\hat{K}$ *is unique in the following sense: if* $\hat{K}_1$ *is a field, which is complete with respect to an absolute value* $\| \cdot \|_1$*, and a monomorphism* $\phi_1 : K \longrightarrow \hat{K}_1$ *preserving absolute values such that* $K$ *is dense in* $\hat{K}_1$*, then there is a unique isomorphism* $\Phi : \hat{K} \longrightarrow \hat{K}_1$ *preserving the absolute values and* $\Phi \circ \phi = \phi_1$*.*

The unique complete field is called the completion of $K$ with respect to $\| \cdot \|$. For convenience, we assume that any field with an absolute value is a subfield of its completion and use the same notation for the absolute values.

It is clear that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value. The completion of $\mathbb{Q}$ with respect to $p$-adic absolute value is called the $p$-adic field and denoted by $\mathbb{Q}_p$.

**Proposition 4.4.** *Let* $K$ *be a field with a nonarchimedean absolute value* $\| \cdot \|$*. The absolute value on the completion* $\hat{K}$ *is also nonarchimedean and the canonical map* $x + \mathcal{M}_K \longrightarrow x\mathcal{M}_{\hat{K}}$ *is an isomorphism of residue fields. If* $\| \cdot \|$ *on* $K$ *is discrete and nonarchimedean, then any uniformizer of* $K$ *is also a uniformizer of* $\hat{K}$*.*

The valuation ring of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$. From the proposition above and the discussion before we have $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$. A field that is complete with respect to a discrete nonarchimedean absolute value and the residue field is finite is called a nonarchimedean local field.

**Theorem 4.5.** *Let* $K$ *be a nonarchimedean local field with a uniformizer* $\pi$*. If* $S$ *is a set of representatives of residue field of* $K$ *containing 0, then any*

*element* $x \in K^\times$ *can be written as* $\sum_{i \geq n} a_i \pi^i$ *for* $a_i \in S$, $a_n \neq 0$ *and* $n \in \mathbb{Z}$ *uniquely. Moreover, the absolute value of the sum* $\sum_{i \geq n} a_i \pi^i$ *is* $\| \pi \|^n$.

Since $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ , $\{0, 1, ..., p-1\}$ is a set of representatives. Then

$$\mathbb{Q}_p = \{\sum_{i \geq n} a_i p^i | a_i = 0, 1, ..., p-1, n \in \mathbb{Z}\},$$
$$\mathbb{Z}_p = \{\sum_{i \geq 0} a_i p^i | a_i = 0, 1, ..., p-1\},$$
$$\mathbb{Z}_p^\times = \{\sum_{i \geq 0} a_i p^i | a_i = 0, 1, ..., p-1, a_0 \neq 0\}.$$

**Theorem 4.6.** *Let* $K$ *be a complete field with respect to an absolute value* $\| \, . \, \|$ *and* $F$ *be a finite extension field of* $K$. *The map* $\| \, . \, \|' \colon F \longrightarrow \mathbb{R}_{\geq 0}$ *by* $x \longrightarrow \| N_{F/K}(x) \|^{\frac{1}{[F:K]}}$ *is the unique absolute value on* $F$ *extending* $\| \, . \, \|$ *and* $F$ *is also complete with respect to* $\| \, . \, \|'$. $\| \, . \, \|'$ *is (discrete) nonarchimedean if* $\| \, . \, \|$ *is (discrete) nonarchimedean.*

Let $K$ be a nonarchimedean local field. For any finite extension field $F$ the value group of $K$ is a subgroup of the value group of $F$ and the canonical map $x + \mathcal{M}_K \longrightarrow x + \mathcal{M}_F$ is a monomorphism from the residue field of $K$ to the residue field of $F$.

**Definition.** *Let* $K$ *be a nonarchimedean local field. For any finite extention* $F$ *of* $K$, *the ramification index* $e$ *is defined as the index of the value group of* $K$ *in the value group of* $F$. *The residue degree* $f$ *is defined as the dimension of the residue field of* $F$ *over the residue field of* $K$. $F$ *is unramified over* $K$ *if and only if* $e=1$.

**Theorem 4.7.** *Let* $K$ *be a nonarchimedean local field. Then* $[F:K]=ef$ *for any finite extension field* $F$ *of* $K$, *where* $e$ *and* $f$ *are the ramification index and residue degree, respectively.*

Here is the idea of the proof of the theorem. $\| \overline{\pi} \|' = \| \pi \|^e$, where $\overline{\pi}$ and $\pi$ are uniformizers of $F$ and $K$, respectively, and $\{\overline{\pi}^i | i = 0, 1, ..., e-1\}$ is a set of representatives in the coset of value groups. $\{u_j | j = 1, ..., f\}$ is a subset of $\mathcal{O}_F$ such that $\{u_j + \mathcal{O}_F \overline{\pi}\}$ is a basis of the residue field of $F$ over the residue field of $K$. Then it can be proved that $\{\overline{\pi}^i u_j | i = 0, 1, ..., e-1, j = 1, ...f\}$ is a $K$-basis of $F$.

Before discussing unramified extension fields, we need the following theorem.

**Theorem 4.8.** *(Hensel's Lemma) Let* $K$ *be nonarchimedean local field and* $k$ *be the residue field of* $K$. *Let* $p$ *be a monic polynomial over the valuation ring*

$\mathcal{O}_K$. *If* $\overline{\pi}(p)$ *has a simple root* $\overline{r} \in k$, $p$ *has a unique root* $r \in \mathcal{O}_K$ *such that* $\pi(r) = \overline{r}$, *where* $\pi : \mathcal{O}_K \longrightarrow k$ *is the canonical map and* $\overline{\pi} : \mathcal{O}_K[x] \longrightarrow k[x]$ *is the map induced by* $\pi$.

**Theorem 4.9.** *Let* $K$ *be a nonarchimedean local field and* $F$ *be a finite extension field of* $K$. *Let* $f$ *be the corresponding residue degree. Then* $F$ *contains a unique maximal subfield* $W$ *such that* $W$ *is unramified over* $K$. *Moreover,* $W$ *is cyclic over* $K$ *of degree* $f$ *and* $W$ *is the cyclotomic extension field of* $K$ *of degree* $q^f - 1$, *where* $q$ *is the cardinality of the residue field of* $K$.

The main idea of the proof of the theorem is that the residue field of $F$ is the splitting field of $x^{q^f} - x$ over the residue field of $K$ and then, by Hensel's Lemma, there is a set $S$ of representatives of the residue field of $F$ consisting of all roots of $x^{q^f} - x$. Let $W$ be the splitting field of $x^{q^f} - x$ over $K$. Then one can show that $W$ is the desired one.

From the discussion above, it is easy to prove the uniqueness of unramified extension fields.

**Theorem 4.10.** *Let* $K$ *be a nonarchimedean local field and* $\overline{K}$ *be an algebraic closure of* $K$. *For each* $n \geq 1$, *there exists a unique umramified extension field of degree* $n$ *in* $\overline{K}$.

There is a characterization of the image of the norms of unramified extension fields.

**Theorem 4.11.** *Let* $K$ *be a nonarchimedean local field and* $F$ *be a unramified extension of* $K$ *with a uniformizer* $\pi$. *Let* $f$ *and* $k$ *be the residue fields of* $F$ *and* $K$, *respectively. Then*

*(i)* $F$ *is cyclic over* $K$ *of degree* $[F{:}K]$ *and the Galois group* $Gal(F/K)$ *is isomorphic to the Galois group* $Gal(f/k)$ *by* $\sigma \longrightarrow \overline{\sigma}$, *where* $\overline{\sigma}$ *is defined by* $\overline{\sigma}(x + \overline{\pi}\mathcal{O}_F) = \sigma(x) + \overline{\pi}\mathcal{O}_F$;

*(ii)* $N_{F/K}(F^\times) = \{u\pi^m | u \in \mathcal{O}_K^\times, m \in n\mathbb{Z}\}$ *and* $K^\times / N_{F/K}(F^\times)$ *is a cyclic group generated by* $\pi N_{F/K}(F^\times)$ *of order* $n$, *where* $n = [F{:}K]$.

Before discussing further properties of local fields, we shall see some explicit examples which we actually need in Section 5.

**Proposition 4.12.** *Let* $p$ *be an odd prime and* $\omega_p$ *be an element such that* $1 \leq \omega_p \leq p - 1$ *with the Legendre symbol* $(\frac{\omega_p}{p}) = -1$. *We have the following properties:*

*(i) For* $a = \sum_{i \geq 0} a_i p^i \in \mathbb{Z}_p^\times$, $a \in (\mathbb{Z}_p^\times)^2$ *if and only if* $(\frac{a_0}{p}) = 1$.

*(ii)* $\mathbb{Z}_p / (\mathbb{Z}_p^\times)^2 = \{\overline{1}, \overline{\omega_p}\}$.

*(iii)* *For* $a = \sum_{i \geq n} a_i p^i \in \mathbb{Q}_p^\times$, $a \in (\mathbb{Q}_p^\times)^2$ *if and only if* $n$ *is even and* $(\frac{a_n}{p}) = 1$.

*(iv)* $\mathbb{Q}_p/(\mathbb{Q}_p^\times)^2 = \{\overline{1}, \overline{\omega_p}, \overline{p}, \overline{p\omega_p}\}$.

One shall keep in mind that

$$\overline{p^n u} = \begin{cases} \overline{1} & \text{if n is even and } (\frac{a_0}{p}) = 1 \\ \overline{\omega_p} & \text{if n is even and } (\frac{a_0}{p}) = -1 \\ \overline{p} & \text{if n is odd and } (\frac{a_0}{p}) = 1 \\ \overline{p\omega_p} & \text{if n is odd and } (\frac{a_0}{p}) = -1 \end{cases}$$

, where $u = \sum_{i \geq 0} a_i p^i \in \mathbb{Z}_p^\times$.

**Proposition 4.13.** *We have the following properties for* $p = 2$*:*

*(i)* *For* $a = \sum_{i \geq 0} a_i 2^i \in \mathbb{Z}_2^\times$, $a \in (\mathbb{Z}_2^\times)^2$ *if and only if* $a \equiv 1 \bmod 8$.

*(ii)* $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \cong (\mathbb{Z}/8\mathbb{Z})^\times$ *by* $a \longrightarrow a \bmod 8$.

*(iii)* *For* $a = \sum_{i \geq n} a_i 2^i \in \mathbb{Q}_2^\times$, $a \in (\mathbb{Q}_2^\times)^2$ *if and only if* $n$ *is even and* $\frac{a}{2^n} \equiv 1 \bmod 8$.

*(iv)* $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{2}, \overline{6}, \overline{10}, \overline{14}\}$.

For the case $p = 2$, we have

$$\overline{2^n u} = \begin{cases} \overline{1} & \text{if n is even and } u \equiv 1 \bmod 8 \\ \overline{3} & \text{if n is even and } u \equiv 3 \bmod 8 \\ \overline{5} & \text{if n is even and } u \equiv 5 \bmod 8 \\ \overline{7} & \text{if n is even and } u \equiv 7 \bmod 8 \\ \overline{2} & \text{if n is odd and } u \equiv 1 \bmod 8 \\ \overline{6} & \text{if n is odd and } u \equiv 3 \bmod 8 \\ \overline{10} & \text{if n is odd and } u \equiv 5 \bmod 8 \\ \overline{14} & \text{if n is odd and } u \equiv 7 \bmod 8 \end{cases}$$

, where $u \in \mathbb{Z}_2^\times$.

Recall that for any field $K$ of characteristic $\neq 2$, the map $\overline{a} \longrightarrow K(\sqrt{a})$ is a bijection between the set of nontrivial representatives of $K^\times/(K^\times)^2$ and the set of all distinct quadratic extension fields of $K$. Hence there are 3 distinct quadratic extension fields of $\mathbb{Q}_p$ for any odd prime $p$ and 7 distinct quadratic extension fields of $\mathbb{Q}_2$.

**Corollary 4.14.** *Let $\omega_p$ be a nonzero element such that $(\frac{\omega_p}{p}) = -1$ for any odd prime $p$ and $\omega_2 \equiv 5$ mod 8. Then $\mathbb{Q}_p(\sqrt{\omega_p})$ is the unique quadratic unramified extension field of $\mathbb{Q}_p$ for any prime $p$.*

There is a result from local class field theory: $[F : K] = [F^\times : N_{F/K}(F^\times)]$ for any finite abelian extension $F$ of a nonarchimedean local field $K$. Hence $[N_{F/K}(F^\times) : (K^\times)^2] = 4$ for any quadratic extension $F$ of a nonarchimedean local field $K$. We can write down the representatives in $N_{F/\mathbb{Q}_p}(F^\times)/(\mathbb{Q}_p^\times)^2$ explicitly without knowledge of class field theory, where $F$ is a quadratic extension field of $\mathbb{Q}_p$. Here we only treats the case of $\mathbb{Q}_2$, which is much tedious than the cases of odd primes. One can use similar process to find the corresponding representatives for each odd prime $p$.

**Proposition 4.15.**

*(i)* $F = \mathbb{Q}_2(\sqrt{3})$, $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2 = \{\overline{1}, \overline{5}, \overline{6}, \overline{14}\}$.

*(ii)* $F = \mathbb{Q}_2(\sqrt{5})$, $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2 = \{\overline{1}, \overline{3}, \overline{5}, 7\}$.

*(iii)* $F = \mathbb{Q}_2(\sqrt{7})$, $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2 = \{\overline{1}, \overline{5}, \overline{2}, \overline{10}\}$.

*(iv)* $F = \mathbb{Q}_2(\sqrt{2})$, $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2 = \{\overline{1}, \overline{7}, \overline{2}, \overline{14}\}$.

*(v)* $F = \mathbb{Q}_2(\sqrt{6})$, $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2 = \{\overline{1}, \overline{3}, \overline{10}, \overline{14}\}$.

*(vi)* $F = \mathbb{Q}_2(\sqrt{10})$, $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2 = \{\overline{1}, \overline{7}, \overline{6}, \overline{10}\}$.

*(vii)* $F = \mathbb{Q}_2(\sqrt{14})$, $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2 = \{\overline{1}, \overline{3}, \overline{2}, \overline{6}\}$.

*Proof.* Let $F$ be a quadratic extension field of $\mathbb{Q}_2$. By Proposition 4.13, $8 = [\mathbb{Q}_2^\times : (\mathbb{Q}_2^\times)^2]$ and thus $[N_{F/\mathbb{Q}_2}(F^\times) : (\mathbb{Q}_2^\times)^2]$=1, 2, 4, 8.

(i): Put $F = \mathbb{Q}_2(\sqrt{3})$. Since $1^2 - 3(1)^2 = -2$ and $1^2 - 3(2)^2 = -11$, we have $\overline{-2} = \overline{14}$, $\overline{-11} = \overline{5} \in N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2$. Since $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2$ is a group, $\overline{5} \times \overline{14} = \overline{6} \in N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2$. Then $\{\overline{1}, \overline{5}, \overline{6}, \overline{14}\}$ is a subset of $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2$ and thus $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2$ is a group of order 4 or 8. Observe that $x^2 - 3y^2 \equiv 0, 1, 4, 5, 6$ mod 8 for any $x, y \in \mathbb{Z}_2$. Thus $2 \neq x^2 - 3y^2 = N_{F/\mathbb{Q}_2}(x + y\sqrt{3})$ for any $x, y \in \mathbb{Z}_2$. It suffices to show that $2 \notin N_{F/\mathbb{Q}_2}(F^\times)$. Suppose $2 = a^2 - 3b^2$ for some $(a, b) \neq (0, 0) \in \mathbb{Q}_2^2$. By the equality $2 = a^2 - 3b^2$, we have $\| a^2 \|_2 \leq max\{\frac{1}{2}, \| b^2 \|_2\}$ and $\| b^2 \|_2 \leq max\{\frac{1}{2}, \| a^2 \|_2\}$. Then $\| a \|_2 \leq 1$ if and only if $\| b \|_2 \leq 1$. Since $2 \neq x^2 - 3y^2$ for any $x, y \in \mathbb{Z}_2$ and $2 = a^2 - 3b^2$, where $(a, b) \neq (0, 0) \in \mathbb{Q}_2^2$, $\| a \|_2 = \| b \|_2 > 1$. Write $a = 2^k u$ and $b = 2^k v$, $k < 0$ and $u, v \in \mathbb{Z}_2^\times$. Then $2 = a^2 - 3b^2 = 2^{2k}(u^2 - 3v^2)$ and $u^2 - 3v^2 = 2^{1-2k} \equiv 0$ mod 8 since $1 - 2k \geq 3$. We have $u^2 \equiv 3v^2$ mod 8 and $(\frac{u}{v})^2 \equiv 3$ mod 8, which means 3 is square in $\mathbb{Z}/8\mathbb{Z}$, a contradiction. Therefore $\overline{2} \notin N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2$ and $N_{F/\mathbb{Q}_2}(F^\times)/(\mathbb{Q}_2^\times)^2 = \{\overline{1}, \overline{5}, \overline{6}, \overline{14}\}$.

One can prove the rest of cases by similar arguments. □

# 5 Quaternion Algebras over Local Fields

Except some additional materials, the treatments here mainly from [1].

**Theorem 5.1.** *Let $a, b \in \mathbb{R}^\times$. Hamilton quaternion $\mathbb{H} = (\frac{-1,-1}{\mathbb{R}})$ is the unique quaternion division algebra over $\mathbb{R}$. $(\frac{a,b}{\mathbb{R}}) \cong \mathbb{H}$ if and only if $a, b < 0$.*

*Proof.* Since any positive real number has a unique positive square root in $\mathbb{R}$ and Proposition 2.3, $(\frac{a,b}{\mathbb{R}})$ splits over $\mathbb{R}$ if $a, b > 0$ , $(\frac{a,b}{\mathbb{R}})$ splits over $\mathbb{R}$ if $ab < 0$ and $(\frac{a,b}{\mathbb{R}}) \cong \mathbb{H}$ if $a, b < 0$. It is clear that $-1 \notin N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times)$. By Theorem 2.9, $\mathbb{H}$ is a division algebra. □

Now we are going to deal with the cases of $\mathbb{Q}_p$. We shall note that the following theorems and propositions hold for any nonarchimedean local field $K$, i.e. $K$ has a nonarchimedean absolute value whose value group is infinite cyclic and is complete with respect to the absolute value.

**Proposition 5.2.** *Let $H$ be a quaternion division algebra over $\mathbb{Q}_p$. Define $\| \, . \, \| : H \longrightarrow \mathbb{R}$ by $x \longrightarrow \| N(x) \|_p^{1/2}$. $H$ has the following properties:*

*(i)* $\| \, . \, \|$ *is a non-archimedean absolute value on $H$.*

*(ii) The restriction of* $\| \, . \, \|$ *on $F$ is the unique absolute value extending* $\| \, . \, \|_p$ *for any quadratic extension field $F$ of $\mathbb{Q}_p$ in $H$.*

*(iii)* $\| \, . \, \|$ *is the unique absolute value extending* $\| \, . \, \|_p$ *such that $H$ is complete with respect to* $\| \, . \, \|$.

*(iv)* $\| H^\times \|$ *is an infinite cyclic group generated by* $\| \pi \|$ *for some $\pi \in H^\times$ and* $\| \pi \| = \| p \|_p^e$ *for e=1 or 2.*

*(v) $\mathcal{O}_H = \{x \in H | \, \| x \| \leq 1\}$ is a subring containing $\mathbb{Z}_p$.*

*(vi) $\mathcal{O}_H^\times = \{x \in H | \, \| x \| = 1\}$.*

*(vii) Any nonzero ideal $I$ of $H$ is of the form $\mathcal{O}_H \pi^n = \pi^n \mathcal{O}_H$ for some $n \geq 0$ and $\mathcal{O}_H - \mathcal{O}_H^\times = \mathcal{O}_H \pi = \pi \mathcal{O}_H$ is the unique maximal ideal.*

*(viii) $N(\mathcal{O}_H) \subseteq \mathbb{Z}_p$ and $N(\pi \mathcal{O}_H) \subseteq p\mathbb{Z}_p$.*

*Proof.* (i),(ii): It is easy to verify that $\| x \| = 0$ if and only if $x = 0$ , $\| xy \| = \| x \| \| y \| = 0$ and $\| \, . \, \| = \| \, . \, \|_p$ on $\mathbb{Q}_p$. For any quadratic extension field $F$ of $\mathbb{Q}_p$ in $H$, $F = \mathbb{Q}_p(\sqrt{a})$ for some nonsquare $a \in \mathbb{Q}_p^\times$. Put $i = \sqrt{a}$. From the proof of Proposition 2.4, there exists a $j \in H$ such that $ij = -ji$ and $j^2 = b \in K^\times$. Hence $\{i, i, j, ij\}$ is a standard basis corresponding to $(a, b)$ and $F = \mathbb{Q}_p(\sqrt{a}) = \mathbb{Q}_p \oplus \mathbb{Q}_p i$. Since the norm map on $F$ is the norm of $F$ over $\mathbb{Q}_p$, the restriction of $\| \, . \, \|$ on $F$ is the unique absolute value extending $\| \, . \, \|_p$. $\| x + y \| \leq \max(\| x \|, \| y \|)$ holds trivially if $x = 0, y = 0$

or $x+y=0$. For $x,y,x+y\neq 0$, $\|\ .\ \|_p$. $\|\ 1+\frac{x}{y}\ \|\leq \max(\|\ 1\ \|,\|\ \frac{x}{y}\ \|)$ if $\frac{x}{y}\in\mathbb{Q}_p$. The inequality also holds for $\frac{x}{y}\notin\mathbb{Q}_p$ since $\mathbb{Q}_p(\frac{x}{y})$ is a quadratic extension of $\mathbb{Q}_p$. (iii): It is proved by the same argument for proving unique absolute value extending an absolute value on a complete field. (iv): It is easy to see that $\langle\frac{1}{p}\rangle\subseteq\|\ H^\times\ \|\subseteq\langle\frac{1}{\sqrt{p}}\rangle$. (v),(vi),(vii),(viii): These are done by routine checks. □

Before discussing further properties of $\mathcal{O}_H$, we shall recall some basic results for the readers who are not familiar with module theory.

Roughly speaking, a module is a "vector space" over a ring. The formal definition of modules is as follows: for a given ring $R$, $M$ is an $R$-module if $M$ is an additive group and there is a scalar product satisfying the following conditions: for any $r,s\in R$ and $x,y\in M$,

(i) $rx\in M$;

(ii) $1x=x$;

(iii) $r(x+y)=rx+ry$;

(iv) $(r+s)x=rx+sx$;

(v) $(rs)x=r(sx)$.

We shall know that for any additive group $M$, $Hom(M,M)$, the set of all group homomorphism from $M$ to $M$, is a ring with identity. And $M$ has a $R$-module structure if and only if there exists a ring homomorphism $R\longrightarrow Hom(M,M)$.

Here are some terminologies we need to know. Let $R$ be a ring and $M$ be a $R$-module. $N$ is a submodule of $M$ if $N$ is an additive subgroup of $M$ and closed under scalar product. A subset $X$ of $M$ is linearly independent over $R$ if $\sum_i r_i x_i=0$ implies $r_i=0$ for all $i$, where $r_i\in R$ and $x_i\in M$, and generates $M$ if any element $x$ of $M$ is a linear combination of $X$. $X$ is called a basis of $M$ if $X$ is linearly independent over $R$ and generates $M$. $M$ is a free $R$-module if $M$ contains a basis.

There are two nontrivial results we shall keep in mind: any two basis of a free $R$-module have the same cardinality if $R$ is commutative; any submodule of a free $R$-module is free if $R$ is a principle ideal domain. The rank of a free module over a commutative ring is defined as the cardinality of a basis.

Now, we can continue discussing the properties of $\mathcal{O}_H$.

**Proposition 5.3.** *$\mathcal{O}_H$ is a free $\mathbb{Z}_p$-module of rank 4.*

*Proof.* Clearly, $H$ is a $\mathbb{Z}_p$-module. Since $\|\ x\ \|_p\leq 1$ for any $x\in\mathbb{Z}_p$, $\mathcal{O}_H$ is a $\mathbb{Z}_p$-submodule. Observe that for each $x\in H$, $\|\ \pi^n x\ \|\leq 1$ if $n$ sufficiently

large. We can choose a $\mathbb{Q}_p$-basis $\{x_i\}$ of $H$ such that $x_i \in \mathcal{O}_H$. From (3) in the proof of Proposition 3.2,

$$[\phi]_X = \begin{pmatrix} 1 & & & \\ & -a & & \\ & & -b & \\ & & & ab \end{pmatrix}$$

, where $\phi$ is the corresponding symmetric bilinear form and $X$ is a standard basis corresponding to $(a, b)$, and then $\phi$ is nondegenerate. Hence $\{\phi(x_i, .)\}$ is a $\mathbb{Q}_p$-basis of the dual space $H^*$. Let $\{f_{x_i}\}$ be the dual basis of $\{x_i\}$. Then $f_{x_j} = \sum_i a_{ij}\phi(x_i, )$ for all $j$ and $(a_{ij}) \in GL_4(\mathbb{Q}_p)$. Put $y_j = \sum_i a_{ij}x_i$. $\{y_i\}$ is a $\mathbb{Q}_p$-basis such that $\phi(y_j, x_i) = \delta_{ij}$(Kronecker delta). Let $x = \sum_i b_i y_i \in \mathcal{O}_H$. Then

$$b_{i'} = \phi(\sum_i b_i y_i, x_{i'}) = \frac{1}{2}[N(x + x_i) - N(x) - N(x_i)] \in \frac{1}{2}\mathbb{Z}_p.$$

We have $\mathcal{O}_H$ is a free $\mathbb{Z}_p$-submodule of $\oplus_i \mathbb{Z}_p \frac{1}{2} y_i$ since $\mathbb{Z}_p$ is a principal ideal domain. It is clear that $\{x_i\}$ is an independent subset of $\mathcal{O}_H$ over $\mathbb{Z}_p$. Therefore $\mathcal{O}_H$ is a free $\mathbb{Z}_p$-module of rank 4. □

**Proposition 5.4.** *$\mathcal{O}_H/\pi\mathcal{O}_H$ is a finite field containing $\mathbb{Z}_p/p\mathbb{Z}_p$ with a canonical embedding.*

*Proof.* Since $\mathbb{Z}_p \subseteq \mathcal{O}_H$, $p\mathbb{Z}_p \subseteq \pi\mathcal{O}_H$ and $\pi\mathcal{O}_H$ is a maximal ideal of $\mathcal{O}_H$, $\mathcal{O}_H/\pi\mathcal{O}_H$ is a division ring and $x+p\mathbb{Z}_p \longrightarrow x+\pi\mathcal{O}_H$ is a monomorphismfrom $\mathbb{Z}_p/p\mathbb{Z}_p$ to $\mathcal{O}_H/\pi\mathcal{O}_H$. It is clear that any $\mathbb{Z}_p$-basis $\{x_i\}$ of $\mathcal{O}_H$, $\{x_i + \pi\mathcal{O}_H\}$ generates $\mathcal{O}_H/\pi\mathcal{O}_H$ as a $\mathbb{Z}_p/p\mathbb{Z}_p$-module. With the observation and Proposition 5.3, $\mathcal{O}_H/\pi\mathcal{O}_H$ is a division ring and a finite dimensional over the finite field $\mathbb{Z}_p/p\mathbb{Z}_p$. By Wedderburn's theorem, $\mathcal{O}_H/\pi\mathcal{O}_H$ must be a finite field. □

For any finite extension $F$ of a nonarchimedean local field $K$ , [F:K]=$ef$, where $e$ is the ramification index and $f$ is the residue degree. The result still holds for the case of quaternion division algebras over nonarchimedean local fields.

**Theorem 5.5.** *Let $H$ be a quaternion division algebra over $\mathbb{Q}_p$. Let e be the index of $\| \mathbb{Q}_p^\times \|_p$ in $\| H^\times \|$ and $f$ be the dimension of $\mathcal{O}_H/\mathcal{O}_H - \mathcal{O}_H^\times$ over $\mathbb{Z}_p/p\mathbb{Z}_p$. Then $e = f = 2$ and $H$ contains a quadratic unramified extension field of $\mathbb{Q}_p$.*

*Proof.* One can prove that $4 = ef$ by the same argument for the case of fields. By Proposition 5.2, $(e, f) = (1, 4), (2, 2)$. Since $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ and Proposition 5.4, $\mathcal{O}_H/\pi\mathcal{O}_H$ is the extension field $\mathbb{Z}_p/\pi\mathcal{O}_H(\xi + \pi\mathcal{O}_H)$, where $\xi + \pi\mathcal{O}_H$ is a primitive $(p^f - 1)th$ root of unity. $\xi \in \mathcal{O}_H - \mathbb{Z}_p$ since $f \geq 2$. Moreover, $\xi \notin \mathbb{Q}_p$ and $\mathbb{Q}_p(\xi)$ is a quadratic extension field of $\mathbb{Q}_p$

in $H$. Put $F = \mathbb{Q}_p(\xi)$. By Proposition 5.2, the restriction of the absolute value on $F$ is the unique absolute value extending $p$-adic absolute value and thus $\mathbb{Z}_p \subseteq \mathcal{O}_F \subseteq \mathcal{O}_H$. Since $\mathcal{O}_H/\pi\mathcal{O}_H = \mathbb{Z}_p/\pi\mathcal{O}_H(\xi + \pi\mathcal{O}_H)$ and $\xi \in F$, $\mathbb{Z}_p/\pi\mathcal{O}_H \subseteq \mathcal{O}_F/\pi\mathcal{O}_H = \mathcal{O}_H/\pi\mathcal{O}_H$ and then

$$2 \leq f = [\mathcal{O}_H/\pi\mathcal{O}_H : \mathbb{Z}_p/\pi\mathcal{O}_H] = [\mathcal{O}_F/\pi\mathcal{O}_H : \mathbb{Z}_p/\pi\mathcal{O}_H] \leq [F : K] = 2.$$

We have $e = f = 2$. Since $F = \mathbb{Q}_p(\xi)$ and $\xi + \pi\mathcal{O}_H$ is a primitive $(p^f - 1)th$ root of unity, $F$ is the unique quadratic unramified extension of $\mathbb{Q}_p$ □

From Corollary 4.14, we know $\mathbb{Q}_p(\sqrt{\omega_p})$ is the unique quadratic unramified extension fied of $\mathbb{Q}_p$, where $\omega_p$ is an integer such that $0 < \omega_p < p$ and the Legendre symbol $(\frac{\omega_p}{p}) = -1$ for any odd prime $p$ and $\omega_2 = 5$.

**Theorem 5.6.** *Let $p$ be a prime. Then $(\frac{\omega_p, p}{\mathbb{Q}_p})$ is the unique quaternion division algebra over $\mathbb{Q}_p$.*

*Proof.* Put $F = \mathbb{Q}_p(\sqrt{\omega_p})$. Since $F$ is unramified over $\mathbb{Q}_p$, by Theorem 4.11, $N_{F/\mathbb{Q}_p}(F^\times) = \{up^n | u \in \mathbb{Z}_p^\times, n \in 2\mathbb{Z}\}$ and $\mathbb{Q}_p^\times/N_{F/\mathbb{Q}_p}(F^\times) = \langle\overline{p}\rangle$ which is a cyclic group of order 2. By Theorem 2.12, $(\frac{\omega_p, p}{\mathbb{Q}_p})$ and $(\frac{\omega_p, 1}{\mathbb{Q}_p}) = M_{2\times 2}(\mathbb{Q}_p)$ are nonisomorphic and thus $(\frac{\omega_p, p}{\mathbb{Q}_p})$ is a division algebra.

Now for uniqueness. Let $H$ be a quaternion division algebra over $\mathbb{Q}_p$. From Theorem 5.5, $H$ contains a quadratic unramified extension field of $\mathbb{Q}_p$. By the uniqueness of unramified extension fields, $\mathbb{Q}_p(\sqrt{\omega_p}) \subseteq H$. Put $i = \sqrt{\omega_p}$. From the proof in Proposition 2.4, there exists an element $j$ such that $\{1, i, j, ij\}$ is a standard basis. Then $H = (\frac{\omega_p, j^2}{\mathbb{Q}_p})$. Write $j^2 = vp^{2k+r}$ for $v \in \mathbb{Z}_p^\times$, $k \in \mathbb{Z}$ and $r = 0, 1$. $H = (\frac{\omega_p, vp^{2k+r}}{\mathbb{Q}_p}) \cong (\frac{\omega_p, vp^r}{\mathbb{Q}_p})$. In $\mathbb{Q}_p^\times/N_{F/\mathbb{Q}_p}(F^\times)$, $\overline{vp} = \overline{p}$ and $\overline{v} = \overline{1}$. By Theorem 2.12, $r = 1$ and

$$H = (\frac{\omega_p, vp^{2k+r}}{\mathbb{Q}_p}) \cong (\frac{\omega_p, vp}{\mathbb{Q}_p}) \cong (\frac{\omega_p, p}{\mathbb{Q}_p}).$$

□

**Corollary 5.7.** *Let $p$ be an odd prime such that $p \equiv 1$ mod 4. Let $a, b \neq 0 \in \mathbb{Z}_p$.*

*(i) For $a, b \in \mathbb{Z}_p^\times$, $(\frac{a,b}{\mathbb{Q}_p})$ splits over $\mathbb{Q}_p$.*

*(ii) For $a \in \mathbb{Z}_p^\times$ and $b \in p\mathbb{Z}_p - p^2\mathbb{Z}_p$, $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{\omega_p, p}{\mathbb{Q}_p})$ if and only if $a \notin (\mathbb{Z}_p^\times)^2$.*

*(iii) For $a, b \in p\mathbb{Z}_p - p^2\mathbb{Z}_p$, $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{\omega_p, p}{\mathbb{Q}_p})$ if and only if exactly one of $\frac{a}{p}$ and $\frac{b}{p}$ is square.*

*Proof.* Put $F_1 = \mathbb{Q}_p(\sqrt{\omega_p})$, $F_2 = \mathbb{Q}_p(\sqrt{p})$ and $F_3 = \mathbb{Q}_p(\sqrt{p\omega_p})$. (i): If $a \in (\mathbb{Z}_p^\times)^2$, $(\frac{\sqrt{a}^2,b}{\mathbb{Q}_p}) \cong (\frac{1,b}{\mathbb{Q}_p})$. For $a \notin (\mathbb{Z}_p^\times)^2$, $a = \omega_p u^2$ for some $u \in \mathbb{Z}_p^\times$ by Proposition 4.12. Then $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{\omega_p,b}{\mathbb{Q}_p})$. By Theorem 4.11 and Theorem 2.9, $b \in N_{F_1/\mathbb{Q}_p}(F_1^\times)$ and thus $(\frac{a,b}{\mathbb{Q}_p})$ splits over $\mathbb{Q}_p$.

(ii): $(\frac{a,b}{\mathbb{Q}_p})$ splits over $\mathbb{Q}_p$ if $a \in (\mathbb{Z}_p^\times)^2$. For $a \notin (\mathbb{Z}_p^\times)^2$, $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{\omega_p,b}{\mathbb{Q}_p})$. By Theorem 4.11 and Theorem 2.9, $b \notin N_{F_1/\mathbb{Q}_p}(F_1^\times)$ and thus $(\frac{\omega_p,b}{\mathbb{Q}_p})$ is a division algebra. By Theorem 5.6, $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{\omega_p,p}{\mathbb{Q}_p})$.

(iii): Write $a = pu$ and $b = pv$, where $u, v \in \mathbb{Z}_p^\times$.

Case 1: $u, v \in (\mathbb{Z}_p^\times)^2$.

Then $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{p,p}{\mathbb{Q}_p})$. Since $\overline{p} = \overline{-1}$ in $\mathbb{Q}_p^\times / N_{F_2/\mathbb{Q}_p}(F_2^\times)$, by Theorem 2.12, $(\frac{p,p}{\mathbb{Q}_p}) \cong (\frac{p,-1}{\mathbb{Q}_p})$. Since $p \equiv 1 \bmod 4$, by Proposition 4.12, $-1 \in (\mathbb{Z}_p^\times)^2$ and thus $(\frac{p,-1}{\mathbb{Q}_p})$ splits over $\mathbb{Q}_p$. Hence $(\frac{a,b}{\mathbb{Q}_p})$ splits over $\mathbb{Q}_p$.

Case 2: $u \notin (\mathbb{Z}_p^\times)^2, v \in (\mathbb{Z}_p^\times)^2$.

Then $a = p\omega_p u_1^2$ and $b = pv_1^2$, where $u_1, v_1 \in \mathbb{Z}_p^\times$, and $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{p\omega_p,p}{\mathbb{Q}_p})$. Since $-1 \in (\mathbb{Z}_p^\times)^2$ and $\frac{-1}{p} \in N_{F_2/\mathbb{Q}_p}(F_2^\times)$, $\frac{1}{p} \in N_{F_2/\mathbb{Q}_p}(F_2^\times)$. By Theorem 2.12, $(\frac{p\omega_p,p}{\mathbb{Q}_p}) \cong (\frac{\frac{p\omega_p}{p},p}{\mathbb{Q}_p}) = (\frac{\omega_p,p}{\mathbb{Q}_p})$. Hence $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{\omega_p,p}{\mathbb{Q}_p})$.

Case 3: $u, v \notin (\mathbb{Z}_p^\times)^2$.

Then $a = p\omega_p u_1^2$ and $b = p\omega_p v_1^2$, where $u_1, v_1 \in \mathbb{Z}_p^\times$, and $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{p\omega_p,p\omega_p}{\mathbb{Q}_p})$. Since $-1 \in (\mathbb{Z}_p^\times)^2$ and $\frac{-1}{p\omega_p} \in N_{F_3/\mathbb{Q}_p}(F_3^\times)$, $\frac{1}{p\omega_p} \in N_{F_3/\mathbb{Q}_p}(F_3^\times)$. By Theorem 2.12, $(\frac{p\omega_p,p\omega_p}{\mathbb{Q}_p}) \cong (\frac{p\omega_p,1}{\mathbb{Q}_p})$. Hence $(\frac{a,b}{\mathbb{Q}_p})$ splits over $\mathbb{Q}_p$. □

**Corollary 5.8.** *Let $p$ be an odd prime such that $p \equiv 3$ mod 4. Let $a, b \neq 0 \in \mathbb{Z}_p$.*

*(i) For $a, b \in \mathbb{Z}_p^\times$, $(\frac{a,b}{\mathbb{Q}_p})$ splits over $\mathbb{Q}_p$.*

*(ii) For $a \in \mathbb{Z}_p^\times$ and $b \in p\mathbb{Z}_p - p^2\mathbb{Z}_p$, $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{\omega_p,p}{\mathbb{Q}_p})$ if and only if $a \notin (\mathbb{Z}_p^\times)^2$.*

*(iii) For $a, b \in p\mathbb{Z}_p - p^2\mathbb{Z}_p$, $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{\omega_p,p}{\mathbb{Q}_p})$ if and only if $\frac{a}{p}$ and $\frac{b}{p}$ are both square or both nonsquare.*

*Proof.* (i) and (ii) have proved in Corollary 5.7. (iii): Put $F_1 = \mathbb{Q}_p(\sqrt{\omega_p})$, $F_2 = \mathbb{Q}_p(\sqrt{p})$ and $F_3 = \mathbb{Q}_p(\sqrt{p\omega_p})$. Write $a = pu$ and $b = pv$, where $u, v \in \mathbb{Z}_p^\times$.

Case 1: $u, v \in (\mathbb{Z}_p^\times)^2$.

As in Corollary 5.7, $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{p,-1}{\mathbb{Q}_p})$. Since $p \equiv 3 \bmod 4$, by Proposition 4.12 and Theorem 2.9, $-1 \notin (\mathbb{Z}_p^\times)^2$ and thus $(\frac{p,-1}{\mathbb{Q}_p})$ is a division algebra. By Theorem 5.6, $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{\omega_p,p}{\mathbb{Q}_p})$.

Case 2: $u \notin (\mathbb{Z}_p^\times)^2, v \in (\mathbb{Z}_p^\times)^2$.

As in Corollary 5.7, $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{p\omega_p,p}{\mathbb{Q}_p})$. Since $\frac{-1}{p} \in N_{F_2/\mathbb{Q}_p}(F_2^\times)$, by Theorem 2.12, $(\frac{p\omega_p,p}{\mathbb{Q}_p}) \cong (\frac{-\frac{p\omega_p}{p},p}{\mathbb{Q}_p}) = (\frac{-\omega_p,p}{\mathbb{Q}_p})$. By Proposition 4.12 , $\overline{-1} = \overline{\omega_p}$ and thus $-\omega_p \in (\mathbb{Z}_p^\times)^2$. Hence $(\frac{a,b}{\mathbb{Q}_p})$ splits over $\mathbb{Q}_p$.

Case 3: $u, v \notin (\mathbb{Z}_p^\times)^2$.

As in Corollary 5.7, $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{p\omega_p,p\omega_p}{\mathbb{Q}_p})$. Since $\frac{-1}{p\omega_p} \in N_{F_3/\mathbb{Q}_p}(F_3^\times)$, by Theorem 2.12, $(\frac{p\omega_p,p\omega_p}{\mathbb{Q}_p}) \cong (\frac{p\omega_p,-1}{\mathbb{Q}_p})$. By Proposition 4.12, $\overline{-1} = \overline{\omega_p}$ in $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ and thus $(\frac{p\omega_p,-1}{\mathbb{Q}_p}) \cong (\frac{p\omega_p,\omega_p}{\mathbb{Q}_p})$. By Theorem 4.11, $p\omega_p \notin N_{F_1/K}(F_1^\times)$ and thus $(\frac{a,b}{\mathbb{Q}_p})$ is a division algebra. Hence $(\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{\omega_p,p}{\mathbb{Q}_p})$. □

**Definition.** *Let $H$ be a quaternion algebra over $\mathbb{Q}$. The ramified places of $H$ consists of places $v$ such that $\mathbb{Q}_v \otimes_{\mathbb{Q}} H$ is the quaternion division algebra over $\mathbb{Q}_v$, where $\mathbb{Q}_{-1} = \mathbb{R}$.*

We will see that there is a stronger statement about quaternion algebras over $\mathbb{Q}$ than the following corollary after introducing Hilbert symbol in Section 7.

**Corollary 5.9.** *Let $H$ be a quaternion algebra over $\mathbb{Q}$. Then the set of ramified places of $H$ is a finite set.*

*Proof.* Let $H = (\frac{a,b}{\mathbb{Q}})$ be a quaternion algebra. Since (ii) in Proposition 2.3, we may assume $a, b \in \mathbb{Z}$. It is clear that the number of odd prime(s) $p$ such that $p|a$ or $p|b$ is finite. This means $a, b \in \mathbb{Z}_p^\times$ for all but finitely many odd prime(s) $p$. By Corollary 5.7 and Corollary 5.8, the set of ramified places contains only finitely many odd prime(s). Hence the set of ramified places of $H$ is a finite set. □

Now, we are going to deal with the case of $\mathbb{Q}_2$. Using the results in Proposition 4.15, Theorem 2.9 and Theorem 5.6, it is easy to prove the following corollary.

**Corollary 5.10.** *Let $a, b \neq 0 \in \mathbb{Z}_2$. $(\frac{a,b}{\mathbb{Q}_2}) \cong (\frac{5,2}{\mathbb{Q}_2})$ if and only if $(\overline{a}, \overline{b})$ is one of the following pairs:*

$$
\begin{gathered}
(\overline{3},\overline{3}), (\overline{3},\overline{7}), (\overline{3},\overline{2}), (\overline{3},\overline{10}),\\
(\overline{5},\overline{2}), (\overline{5},\overline{6}), (\overline{5},\overline{10}), (\overline{5},\overline{14}),\\
(\overline{7},\overline{3}), (\overline{7},\overline{7}), (\overline{7},\overline{6}), (\overline{7},\overline{14}),\\
(\overline{2},\overline{3}), (\overline{2},\overline{5}), (\overline{2},\overline{6}), (\overline{2},\overline{10}),\\
(\overline{6},\overline{5}), (\overline{6},\overline{7}), (\overline{6},\overline{2}), (\overline{6},\overline{6}),\\
(\overline{10},\overline{3}), (\overline{10},\overline{5}), (\overline{10},\overline{2}), (\overline{10},\overline{14}),\\
(\overline{14},\overline{5}), (\overline{14},\overline{7}), (\overline{14},\overline{10}), (\overline{14},\overline{14}).
\end{gathered}
$$

Using Corollary 5.7, Corollary 5.8 and Corollary 5.10, we can find the ramified places of quaternion algebras $(\frac{a,b}{\mathbb{Q}})$ for $a, b = \pm 1, \pm p$, where $p$ is a prime. Let $p, q$ be distinct odd primes. Here are the results. In the following two tables, $\overline{a}$ is the congruence class modulo 4 and $\hat{a}$ is the congruence class modulo 8.

| Ramified Places of $(\frac{a,b}{\mathbb{Q}})$ | -1 | 2 | -2 | $p$ | -$p$ |
|---|---|---|---|---|---|
| -1 | $\{-1, 2\}$ | $\phi$ | $\{-1, 2\}$ | $\phi$ if $\overline{p} = \overline{1}$. $\{2, p\}$ if $\overline{p} = \overline{3}$. | $\{-1, 2\}$ if $\overline{p} = \overline{1}$. $\{-1, p\}$ if $\overline{p} = \overline{3}$. |
| 2 | | $\phi$ | $\phi$ | $\phi$ if $\hat{p} = \hat{1}, \hat{7}$. $\{2, p\}$ if $\hat{p} = \hat{3}, \hat{5}$. | $\phi$ if $\hat{p} = \hat{1}, \hat{7}$. $\{2, p\}$ if $\hat{p} = \hat{3}, \hat{5}$. |
| -2 | | | $\{-1, 2\}$ | $\phi$ if $\hat{p} = \hat{1}, \hat{3}$. $\{2, p\}$ if $\hat{p} = \hat{5}, \hat{7}$. | $\{-1, 2\}$ if $\hat{p} = \hat{1}, \hat{3}$. $\{-1, p\}$ if $\hat{p} = \hat{5}, \hat{7}$. |
| $p$ | | | | $\phi$ if $\overline{p} = \overline{1}$. $\{2, p\}$ if $\overline{p} = \overline{3}$. | $\phi$ |
| -$p$ | | | | | $\{-1, 2\}$ if $\overline{p} = \overline{1}$. $\{-1, p\}$ if $\overline{p} = \overline{3}$. |

| Ramified Places of $(\frac{\pm p,\pm q}{\mathbb{Q}})$ | $q$ | -$q$ |
|---|---|---|
| $p$ | $(\overline{p},\overline{q}) \neq (\overline{3},\overline{3})$:<br>$\phi$ if $(\frac{p}{q}) = 1$.<br>$\{p, q\}$ if $(\frac{p}{q}) = -1$.<br><br>$(\overline{p},\overline{q}) = (\overline{3},\overline{3})$:<br>$\{2, p\}$ if $(\frac{p}{q}) = 1$.<br>$\{2, q\}$ if $(\frac{p}{q}) = -1$. | $(\overline{p},\overline{q}) \neq (\overline{3},\overline{1})$:<br>$\phi$ if $(\frac{p}{q}) = 1$.<br>$\{p, q\}$ if $(\frac{p}{q}) = -1$.<br><br>$(\overline{p},\overline{q}) = (\overline{3},\overline{1})$:<br>$\{2, p\}$ if $(\frac{p}{q}) = 1$.<br>$\{2, q\}$ if $(\frac{p}{q}) = -1$. |
| -$p$ | | $(\overline{p},\overline{q}) = (\overline{1},\overline{1})$:<br>$\{-1, 2\}$ if $(\frac{p}{q}) = 1$.<br>$\{-1, 2, p, q\}$ if $(\frac{p}{q}) = -1$.<br><br>$(\overline{p},\overline{q}) \neq (\overline{1},\overline{1})$:<br>$\{-1, q\}$ if $(\frac{p}{q}) = 1$.<br>$\{-1, p\}$ if $(\frac{p}{q}) = -1$. |

We will see that the ramified places of a quaternion algebra over $\mathbb{Q}$ is of even cardinality in the next section and two quaternion algebras over $\mathbb{Q}$ are isomorphic if and only if they have the same ramified places. With these in mind and from the two tables above, we have some suggestions about the choice of quaternion algebras over $\mathbb{Q}$ for a given places of the form $\{-1, p\}$ and $\{2, p\}$.

| Ramified Places | Choice of Quaternion Algebras |
|---|---|
| $\{-1, 2\}$ | $(\frac{-1,-1}{\mathbb{Q}})$ |
| $\{-1, p\}$, $p \equiv 1 \bmod 4$ | $(\frac{-p,-q}{\mathbb{Q}})$, where $q$ is an odd prime such that $q \equiv 3 \bmod 4$ and the Legendre symbol $(\frac{q}{p}) = -1$ |
| $\{-1, p\}$, $p \equiv 3 \bmod 4$ | $(\frac{-1,-p}{\mathbb{Q}})$ |
| $\{2, p\}$, $p \equiv 1 \bmod 8$ | $(\frac{-p,q}{\mathbb{Q}})$, where $q$ is an odd prime such that $q \equiv 3 \bmod 4$ and the Legendre symbol $(\frac{q}{p}) = -1$ |
| $\{2, p\}$, $p \equiv 5 \bmod 8$ | $(\frac{2,\pm p}{\mathbb{Q}})$ |
| $\{2, p\}$, $p \equiv 3 \bmod 4$ | $(\frac{-1,-p}{\mathbb{Q}})$ |

# 6 Preliminaries III

In previous section we have shown that the the set of places in which a quaternion algebra over $\mathbb{Q}$ ramifies is finite. In fact, the set is of even cardinality. In order to prove the property, we shall recall Hilbert symbol and some results which are from [8].

**Definition.** *Let $K$ be a field and $a, b \in K^\times$. Define $(a,b)_K = 1$ if the polynomial $z^2 - ax^2 - by^2$ has a nontrivial solution in $K^3$; Otherwise, $(a,b)_K = -1$. The number $(a,b)_K$ is called the Hilbert symbol of $a$ and $b$ relative to $K$.*

For simplicity, $(\ ,\ )_{\mathbb{R}}$ and $(\ ,\ )_{\mathbb{Q}_p}$ are denoted by $(\ ,\ )_{-1}$ and $(\ ,\ )_p$, respectively. We shall recall some basic properties of the Hilbert symbol and then focus on $\mathbb{R}$ and $p$-adic fields $\mathbb{Q}_p$.

**Proposition 6.1.** *Let $K$ be a field and $a, b \in K^\times$.*

*(i)* $(a,b)_K = (b,a)_K$.

*(ii)* $(au^2, bv^2)_K = (a,b)_K$ *for any* $u, v \in K^\times$.

*(iii)* $(a,b)_K = 1$ *if and only if* $b \in N_{F/K}(F^\times)$, *where* $F = K(\sqrt{a})$.

By (ii) of the proposition above and Theorem 2.9, the quaternion algebra $(\frac{a,b}{K})$ is a division algebra if and only if $(a,b)_K = -1$.

The following theorem rephrases Corollary 5.7, Corollary 5.8 and Corollary 5.10.

**Theorem 6.2.**

*(i)* $(a,b)_{-1} = -1$ *iff* $a < 0$ *and* $b < 0$.

*(ii) Let $p$ be an odd prime. $(p^n u, p^m v)_p = (-1)^{nm\frac{p-1}{2}} (\frac{a_0}{p})^m (\frac{b_0}{p})^n$, where $n, m \in \mathbb{Z}$, $u = \sum_{\geq 0} a_i p^i, v = \sum_{\geq 0} b_i p^i \in \mathbb{Z}_p^\times$ and $(\frac{\cdot}{\cdot})$ is the Legendre symbol.*

*(iii)* $(2^n u, 2^m v)_2 = (-1)^{(\frac{u-1}{2} \bmod 2)(\frac{v-1}{2} \bmod 2) + m(\frac{u^2-1}{8} \bmod 2) + n(\frac{v^2-1}{8} \bmod 2)}$, *where $n, m \in \mathbb{Z}$ and $u, v \in \mathbb{Z}_2^\times$.*

Recall that we choose $\omega_p$ as an integer such that $1 \leq \omega_p \leq p-1$ with the Legendre symbol $(\frac{\omega_p}{p}) = -1$ for any odd prime $p$ and $\omega_2 = 5$. By the formulas above, $(\omega_p, p)_p = -1$ for all primes $p$.

By the formulas in Theorem 6.2, one can show the following proposition.

**Proposition 6.3.** $(ab, c)_K = (a,c)_K (b,c)_K$ *for any* $a, b, c \in K$, *where* $K = \mathbb{R}$ *or* $\mathbb{Q}_p$.

**Theorem 6.4.** *(Hilbert reciprocity) Let $V$ be the set of all primes $p$ together with -1. Let $a, b \in \mathbb{Q}$. Then $(a,b)_v = 1$ for all but finitely many $v \in V$ and $\prod_{v \in V} (a,b)_v = 1$.*

The reason $(a,b)_v = 1$ for almost all $v \in V$ is that $a$ and $b$ are both units of $p$-adic integers for all but finitely many odd primes $p$. The last equality is proved by checking $\prod_{v \in V} (a,b)_v$ for all $a, b \in V$ and using Proposition 6.3.

**Corollary 6.5.** *Let $H$ be a quaternion algebra over $\mathbb{Q}$. The set of ramified places of $H$ is finite and of even cardinality.*

Let $(V, Q)$ be a $n$-dimensional quadratic space over a field $K$ with a basis $\beta$ and $F$ be an extension field of $K$. Then $F \otimes_{\mathbb{Q}} V$ is a vector space over $F$ with a basis $1 \otimes \beta$. By Proposition 3.1, $Q$ is associated with a unique homogenous polynomial $p$ of $n$ variable over $K$and there is a unique quadratic form $Q_F$ on $F \otimes_K V$ associated with the polynomial $p$ under the basis $1 \otimes \beta$. Hence we associate the quadratic space $(V, Q)$ with a quadratic space $(F \otimes_K V, Q_F)$ over $F$.

In fact, the association is coordinate-free. For any quadratic space $(V, Q)$ over a field $K$, one can show that the map $\Phi : F \otimes_K V \times F \otimes_K V \longrightarrow F$ by $(\sum_i \alpha_i \otimes v_i, \sum_j \beta_j \otimes w_j) \longrightarrow \sum_{i,j} \alpha_i \beta_j \phi(v_i, w_j)$ is a symmetric bilinear form on $F \otimes_K V$, where $\phi$ is the corresponding symmetric bilinear form of $Q$. Let $Q_F$ be the corresponding quadratic form of $\Phi$. Then $Q_F(\alpha \otimes v) = \alpha^2 Q(v)$ and the association coincides with the association in the above paragraph. The quadratic space $(F \otimes_K V, Q_F)$ is denoted by $(V, Q)_F$. For simplicity, we write $(V, Q)_{-1}$ and $(V, Q)_p$ instead of $(V, Q)_{\mathbb{R}}$ and $(V, Q)_{\mathbb{Q}_p}$, respectively.

# 7 Quaternion Algebras over Global Fields

In this section we will show two quaternion algebras over $\mathbb{Q}$ are isomorphic if and only if they are isomorphic locally, which is equivalent to that their ramified places are the same. On the other hand, we have discussed some families of quaternion algebras in the end of Section 5. We will give an unified method to find a pair $(a, b)$ for a given finite set of places with even cardinality in which the quaternion algebra $(\frac{a,b}{\mathbb{Q}})$ is ramified.

**Theorem 7.1.** *(Hasse-Minkowski) Let $(V_i, \phi_i)$ be a quadratic space over $\mathbb{Q}$, $i = 1, 2$. Then $(V_1, \phi_1) \cong (V_2, \phi_2)$ if and only if $(V_1, \phi_1)_v \cong (V_2, \phi_2)_v$ for all places $v$.*

For detailed proof of Hasse-Minkowski theorem, see [8].

**Theorem 7.2.** *Let $H$ and $H'$ be two quaternion algebras over $\mathbb{Q}$ Then $H$ and $H'$ are isomorphic if and only if the ramified places of $H$ and $H'$ are the same.*

*Proof.* It is clear that the ramified places of $H$ and $H'$ are the same if $H$ and $H'$ are isomorphic. Suppose $H$ and $H'$ have the same ramified places. Then $H_v = \mathbb{Q}_v \otimes_{\mathbb{Q}} H$ and $H'_v = \mathbb{Q}_v \otimes_{\mathbb{Q}} H'$ are isomorphic for all places $v$ of $\mathbb{Q}$. Let $N$ and $N'$ be the corresponding quadratic forms of $H$ and $H'$, respectively. By Theorem 3.3, $(H_0, N)_v$ and $(H'_0, N')_v$ are isomorphic all places $v$ of $\mathbb{Q}$. By Hasse-Minkowski theorem, $(H_0, N)$ and $(H'_0, N')$ are isomorphic and then $H$ and $H'$ are isomorphic by Theorem 3.3. □

**Theorem 7.3.** *Let $R$ be a finite subset of places with even cardinality. Then there is a quaternion algebra $H$ over $\mathbb{Q}$ such that $R$ is the set of ramified places of $H$.*

*Proof.* Set $a = \prod_{v \in R} v$. By Chinese Remainder Theorem and Dirichlet's theorem on arithmetic progressions, there exists an odd prime or a negative odd prime $b \notin R$ satisfying the congruence equations $(\frac{b}{v}) = -1$ for all $v \neq 2 \in R$ and $b \equiv 5 \bmod 8$. Here $(\frac{\cdot}{v})$ is the Kronecker symbol such that when $v$ is an odd prime, it is equal to Legendre symbol; when $v = 2$, $(\frac{b}{v}) = -1$ if and only if $b \equiv \pm 3 \mod 8$; when $v = -1$, $(\frac{b}{v}) = -1$ if and only if $b < 0$. From the discussion in quaternion algebras over local fields in Section 5, we see that the quaternion $H = (\frac{a,b}{\mathbb{Q}})$ is ramified at all places in $R$ and except for $R$, it may only be ramified at the place $b$. Since $H$ is ramified at even number of places, we conclude that it is ramified exactly at all places of $R$. □

Serre also gave an explicit construction of quaternion algebras over $\mathbb{Q}$ in [8, p.24], which is more complicated. In general, both method can not provide the smallest pair $(a, b)$ (in the sense that $|ab|$ is minimal). However, they do give an upper bound for the exhaustive method. In following table, for given two places, we compare the pair $(a, b)$ given by three distinct algorithms: Serre's algorithm (in the first row), our algorithm (in the second row) and Magma (in the last row of each cell).

| | 2 | 3 | 5 | 7 | 11 |
|---|---|---|---|---|---|
| -1 | (-3,-14)<br>**(-2,-3)**<br>(-1,-1) | (-19,-219)<br>**(-3,-19)**<br>(-3,-1) | (-3,-35)<br>**(-5,-3)**<br>(-5,-2) | (-11,-259)<br>**(-7,-11)**<br>(-7,-1) | (-3,-77)<br>**(-11,-3)**<br>(-11,-1) |
| 2 | | (5,66)<br>**(6,5)**<br>(3,-1) | (-3,70)<br>**(10,-3)**<br>(10,-3) | (-11,42)<br>**(14,5)**<br>(7,-2) | (-3,154)<br>**(22,-3)**<br>(22,-3) |
| 3 | | | (-43,1515)<br>**(15,-43)**<br>(15,2) | (5,231)<br>**(21,5)**<br>(21,-1) | (29,4917)<br>**(33,29)**<br>(33,-1) |
| 5 | | | | (13,2135)<br>**(35,13)**<br>(35,-2) | (-3,385)<br>**(55,-3)**<br>(55,2) |
| 7 | | | | | (13,7931)<br>**(77,13)**<br>(77,-1) |

# 8 Viewpoints from Brauer Groups

In this section we introduce the Brauer groups and Galois cohomology. We will see that the classes of quaternion algebras in the Brauer group over

$\mathbb{Q}$ forms a 2-subgroup. As in previous sections, we always assume that the ground field $K$ is of characteristic not equal to 2 when discussing quaternion algebras. All materials in this section could found in [3],[4],[5],[9].

First, let us recall some properties about central simple algebras without giving the proof.

**Theorem 8.1.** *The tensor product of two central simple $K$-algebras over $K$ is also a central simple $K$-algebra.*

**Proposition 8.2.**

*(i)* $M_{n\times n}(A)^{op} \cong M_{n\times n}(A^{op})$ *for any $K$-algebra $A$ and $n \geq 1$.*

*(ii)* $(A \otimes_K B)^{op} \cong A^{op} \otimes_K B^{op}$ *for any $K$-algebras $A$ and $B$.*

**Definition.** *Let $A$ and $B$ be finite dimensional central simple $K$-algebras. $A$ and $B$ are equivalent, denoted by $A \sim B$, if $A \cong M_{n\times n}(D_1)$, $B \cong M_{m\times m}(D_2)$ and $D_1 \cong D_2$.*

**Proposition 8.3.** *$\sim$ is an equivalent relation on the set of finite dimensional central simple $K$-algebras.*

**Proposition 8.4.** *Let $A_i$ and $B_i$ be a finite dimensional central simple $K$-algebras, $i = 1, 2$.*

*(i)* $A_1 \sim A_2$ *and* $B_1 \sim B_2$ *imply* $A_1 \otimes_K B_1 \sim A_2 \otimes_K B_2$

*(ii)* $A_1 \otimes_K M_{n\times n}(K) \sim A_1 \otimes_K M_{m\times m}(K)$ *for any $n, m \geq 1$.*

*(iii)* $A_1 \otimes_K B_1 \sim B_1 \otimes_K A_1$.

*(iv)* $A_1 \otimes_K A_1^{op} \cong A_1^{op} \otimes_K A_1$.

**Definition.** *The Brauer group of $K$, denoted by $Br(K)$, is the set of equivalent classes under the relation $\sim$. Define $[A][B] = [A \otimes_K B]$ for all $[A], [B] \in Br(K)$.*

Roughly speaking, the set of elements of $Br(K)$ is the representatives of nonisomorphic finite dimensional division $K$-algebras.

Using Proposition 8.4, it is easy to prove:

**Proposition 8.5.** *The multiplication on the set $Br(K)$ is well defined and the Brauer group $Br(K)$ forms an abelian group.*

Let $H$ be a quaternion algebra over $K$. By Proposition 2.4, $[H] \in Br(K)$. Since $[H]^{-1} = [H^{op}]$ and $H \cong H^{op}$, $[H]$ is of order 2 in $Br(K)$. One may ask if every element of order 2 in the Brauer group is a class of quaternion. Brauer himself indeed gave an counterexample that there exists an element of order 2 in the Brauer group which is not a class of quaternion algebra.

On the other hand, since $Br(K)$ is abelian, all elements of order 2 form a subgroup of $Br(K)$ and we can know more about the role of quaternion algebras in this subgroup by theorems of Albert and Merkurjev.

Let $H_i$ be a quaternion algebra over $K$ with the norm map $N_i$, $i = 1, 2$. One can show there is a unique linear map $\sigma$ on the biquaternion $H_1 \otimes_K H_2$ such that $x \otimes y \longrightarrow \overline{x} \otimes \overline{y}$ for any $x \in H_1$ and $y \in H_2$. In fact, the map $\sigma$ is an involution on the biquaternion $H_1 \otimes_K H_2$ and is a $K$-algebra isomorphism between $H_1 \otimes_K H_2$ and $(H_1 \otimes_K H_2)^{op}$. Set $V = \{v \in H_1 \otimes_K H_2 | \sigma(v) = -v\}$. Then $V$ is a $K$-subspace and $\{i \otimes 1, j \otimes 1, ij \otimes 1, 1 \otimes \tilde{i}, 1 \otimes \tilde{j}, 1 \otimes \tilde{i}\tilde{j}\}$ is a basis of $V$, where $\{1, i, j, ij\}$ and $\{1, \tilde{i}, \tilde{j}, \tilde{i}\tilde{j}\}$ are standard basis of $H_1$ and $H_2$, respectively. Note that any $v \in V, v = x \otimes 1 + 1 \otimes y$ for $x \in (H_1)_0$ and $y \in (H_2)_0$ uniquely. Define $\tilde{N} : V \longrightarrow K$ by $x \otimes 1 + 1 \otimes y \longrightarrow N_1(x) - N_2(y)$. Then $\tilde{N}$ is a quadratic form on the 6-dimensional vector space $V$. The quadratic form $\tilde{N}$ is called the Albert form for $H_1$ and $H_2$.

**Theorem 8.6.** *(Albert) Let $H_i$ be a quaternion algebra over $K$. The following conditions are equivalent:*

*(i) The biquaternion $H_1 \otimes_K H_2$ is not a division algebra.*

*(ii) There exists $a, b, c \in K^\times$ such that $H_1 \cong (\frac{a,b}{K})$ and $H_2 \cong (\frac{a,c}{K})$.*

*(iii) The Albert form for $H_1$ and $H_2$ has a nontrivial zero.*

By Artin-Wedderburn theorem, $H_1 \otimes_K H_2 \cong M_{n \times n}(D)$ for some unique central division $K$-algebra and $n \geq 1$. Since $H_1 \otimes_K H_2$ is of 16-dimensional, $n = 1, 2, 4$. Then $n = 1$ if and only if $H_1 \otimes_K H_2 \cong D$; $n = 2$ if and only if $D$ is a quaternion division algebra over $K$; $n = 4$ if and only if $H_1 \otimes_K H_2 \cong D$ splits over $K$. Hence the classes of quaternion algebras over $K$ forms a subgroup of the Brauer group of $K$ if and only if any biquaternion algebra over $K$is not a division algebra, by Albert's theorem, if and only if any Albert form has a nontrivial zero. By the fact that any quadratic forms of degree 6 over $\mathbb{Q}$ has a nontrivial zero, the classes of quaternion algebras over $\mathbb{Q}$ form a subgroup of $Br(\mathbb{Q})$.

Furthermore, there is a characterization of the elements of order 2 in Brauer groups.

**Theorem 8.7.** *(Merkurjev) Let $D$ be a central division $K$-algebra such that $[D]$ is of order 2 in the Brauer group of $K$. There exist positive integers $n_1, n_2, m$ and quaternion algebras $H_1, ..., H_m$ such that*

$$D \otimes_K M_{n_1 \times n_1}(K) \cong H_1 \otimes_K ... \otimes_K H_m \otimes_K M_{n_2 \times n_2}(K).$$

Merkurjev's theorem says the elements of order 2 in the Brauer group are products of the classes of quaternion algebras.

Combining Albert's and Merjurjev's theorems, we conclude that

**Theorem 8.8.** *Every element of order 2 in $Br(\mathbb{Q})$ is a class of quaternion algebra.*

Let $F$ be an algebraically closed field or a finite field. We already know that any finite dimensional central simple $F$-algebra is a matrix algebra over $F$. Thus $Br(F)$ is a trivial group.

**Proposition 8.9.** *The Brauer groups over algebraically closed fields and finite fields are trivial groups.*

We shall continue the discussion of the splitness of central simple algebras in Section 1. Here are some basic properties about the splitness.

**Proposition 8.10.** *Let $A$ and $B$ be two finite dimensional central simple $K$-algebras.*

*(i) If $F$ is a splitting field of $A$ and $B$, $F$ is also a splitting field of $A \otimes_K B$.*

*(ii) If $F$ is a splitting field of $A$, $F$ is also a splitting field of the opposite ring $A^{op}$.*

*(iii) If $A \cong M_{n\times n}(D)$, where $D$ is the unique central division $K$-algebra, $A$ splits over $F$ if and only if $D$ splits over $F$.*

Let $F$ be an extension field of $K$. The first property in the proposition above implies the set of the classes of central simple $K$-algebras which split over $F$ forms a subgroup of $Br(K)$. And the subgroup is denoted by $Br(F/K)$.

Due to the third property in the proposition above, if we would like to study the splitness of central simple algebras, then we only need to study the splitness of division algebras.

**Theorem 8.11.** *Let $D$ be a central division $K$-algebra. Then there is a finite Galois extension field $F$ of $K$ such $F$ is a splitting field of $D$.*

By the theorem above, we have $Br(K) = \cup_\alpha Br(F_\alpha/K)$, where $\{F_\alpha\}$ is the collection of finite Galois extension fields of $K$.

Now, we are in the position for introducing Galois (group) cohomology.

**Definition.** *Let $G$ be a group. $A$ is a $G$-module if $A$ is an additive group and $G$ acts on $A$ such that $g(a+b) = ga + gb$ for all $g \in G$ and $a, b \in A$.*

There are also treatments of non-abelian $G$-module. See [7] for more details. Here we only consider the abelian case.

Here are characterizations of $G$-modules.

**Proposition 8.12.** *Let $G$ be a group and $A$ be an additive group. The following conditions are equivalent:*

(i) *$A$ is a $G$-module.*

(ii) *$A$ is a $\mathbb{Z}[G]$-module, where $\mathbb{Z}[G]$ is the group ring of $G$ over $\mathbb{Z}$.*

(iii) *There is a ring homomorphism $\phi : \mathbb{Z}[G] \longrightarrow End_{\mathbb{Z}}(A)$, where $End_{\mathbb{Z}}(A)$ is the ring of endomorphisms on $A$.*

(iv) *There is a ring homomorphism $\varphi : G \longrightarrow End_{\mathbb{Z}}(A)^{\times}$.*

**Definition.** *Let $G$ be a group and $A$ be a $G$-module. For $n \geq 0$, the group of $n$-cochains of $G$ with coefficients in $A$ is the set of functions from $G^n$ to $A$, denoted by $C^n(G, A)$. The $n$th differential $\partial^n$ is the map from $C^n(G, A)$ to $C^{n+1}(G, A)$ defined by*

$$\begin{aligned}\partial^n(f)(g_0, .., g_n) =& g_0 f(g_1, ..., g_n) \\ &+ \sum_{i=1}^{n} (-1)^i f(g_0, ..., g_{i-1}g_i, ..., g_n) \\ &+ (-1)^{n+1} f(g_0, ..., g_{n-1}).\end{aligned}$$

**Proposition 8.13.** *Let $G$ be a group and $A$ be a $G$-module. The differentials are group homomorphisms and $\partial^{n+1} \circ \partial^n$ is the zero map for any $n \geq 0$.*

By the proposition above, we know that $im\partial^{n-1} \subset ker\partial^n$ are subgroups of the group of $n$-cochains. Then $ker\partial^n / im\partial^{n-1}$ forms a group since the group of $n$-cochains is abelian.

**Definition.** *Let $G$ be a group and $A$ be a $G$-module. The group $ker\partial^n / im\partial^{n-1}$ is called the $n$th cohomology group of $G$ with coefficients in $A$, denoted by $H^n(G, A)$. Any $f \in ker\partial^n$ is called a $n$-cocycle. And any $g \in im\partial^{n-1}$ is called a $n$-coboundary.*

Let $f$ be a 2-cocycle. Define the map $h : G \longrightarrow A$ by $g \longrightarrow f(e, e)$ for all $g \in G$, where $e$ is the identity of $G$. Set $f_1 = f - \partial^1 h$. One can show that $f_1$ is a 2-cocycle such that $f_1(g, e) = f(e, g) = 0$ for any $g \in G$. $f_1$ is called a normalized 2-cocycle.

**Theorem 8.14.** *Let $F$ be a finite Galois extension field of $K$. For any normalized 2-cocycle $f$, there is a central simple $K$-algebra $A_f$ satisfying the following properties:*

(i) *$A_f$ has a $F$-basis $\{u_\sigma | \sigma \in Gal(F/K)\}$ with the same cardinality of the Galois group $Gal(F/K)$.*

(ii) *$[A_f : K] = [F : K]^2$.*

(iii) *$F$ is a splitting field of $A_f$.*

*More precisely, the multiplication of $A_f$ is as follows:*

$$(\sum_{\sigma} \alpha_\sigma u_\sigma)(\sum_{\tau} \beta_\tau v_\tau) = \sum_{\sigma,\tau} \alpha_\sigma \sigma(\beta_\tau) f(\sigma,\tau) u_{\sigma\tau}$$

*, where $\alpha_\sigma, \beta_\tau \in F$.*

**Definition.** *The algebra $A_f$ constructed in Theorem 8.14 is called the crossed product algebra associated with $f$.*

**Proposition 8.15.** *Let $A_f$ and $A_g$ be two crossed product algebras associated with the normalized 2-cocyles $f$ and $g$, respectively. In the Brauer group $Br(K)$, $[A_f] = [A_g]$ if these two cocycles $f$,$g$ are in the same class in the 2nd cohomology group; $[A_f \otimes_K A_g] = [A_{fg}]$.*

**Theorem 8.16.** *Let $F$ be a finite Galois extension field of $K$. Then the cohomology group $H^2(Gal(F/K), F^\times)$ is isomorphic to the relative Brauer group $Br(F/K)$.*

Recall that we prove Theorem 2.12 using an algebraic approach. One can prove Theorem 2.12 by a cohomological approach.

**Corollary 8.17.** *Let $F$ be a quadratic extension field of $K$. Let $a$ be a number such that $F = K(\sqrt{a})$.*

*(i) The crossed product algebra $A_f$ associated with $f$ is isomorphic to the quaternion algebra $(\frac{a,f(\sigma,\sigma)}{K})$ for any normalized 2-cocycle $f$.*

*(ii) $H^2(Gal(F/K), F^\times) \cong K^\times / N_{F/K}(F^\times)$ by $[f] \longrightarrow f(\sigma,\sigma)$.*

# Appendix

We list two MATLAB codes for Theorem 7.3. The first is a simplified vision which based on the method in [8, p.24]. The second is the algorithm in the proof of Theorem 7.3. In our MATLAB codes, `f_primefactors` is a user-defined function which find the prime factors of a given nonzero integer; `f_findplace` is a user-defined function by the formulas in Theorem 6.2.

```
clc; clear;
RAM=[  ]   %the ramified places
           %  ramifies at inifinite place iff -1 appears
FP=primes(1000000); % to check the prime factors for large numbers
%%
%functions will appear in the algorithm:
%f_primefactors: to find prime factors of a given integer
%f_findplace:    to find the ramified places of a given quaternion (a,b)

%%
```

```
if isempty(RAM)==0 % if RAM is nonempty
    RAModd=setdiff(RAM,[-1, 2]); % the set of odd prime p in RAM
    temppa=5;
    tempna=-3;
    %%
    if isempty(RAModd)==0            % RAM contains an odd prime
        Legp=ones(1,length(RAModd));
        % to record the value of Legendre symbol for choosing temppa
        Legn=ones(1,length(RAModd));
        % to record the value of Legendre symbol for choosing tempna
        prodramodd=prod(RAModd);
        %%
        if ismember(-1,RAM)==0 % -1 is not in RAM
            % to choose temppa>0 such that a is nonquare in Z/pZ for all
            % odd primes p in RAModd and a=5 mod 8
            if gcd(temppa,prodramodd)==1
                %to avoid the situation that the input of
                %Legendre symbol ( /p) is not relatively prime to p
                for i=1:length(RAModd)
              Legp(i)=feval(symengine,'numlib::legendre',temppa,RAModd(i));
                end
            end
            while  (ismember(1,Legp)==1)| (gcd(temppa,prodramodd)~=1)
                % the last condition is to avoid the situation that
                %the input of Legendre symbol ( /p) is not
                %relatively prime to p
                temppa=temppa+8;
                if gcd(temppa,prodramodd)==1
                    for i=1:length(RAModd)
                Legp(i)=feval(symengine,'numlib::legendre',temppa,RAModd(i));
                    end
                end
            end
            %%
            % to find tempna<0 such that a is nonquare in Z/pZ for all
            %odd primes p in RAModd and a=5 mod 8
            if gcd(tempna,prodramodd)==1
                %to avoid the situation that the input of
                %Legendre symbol ( /p) is not relatively prime to p
                for i=1:length(RAModd)
              Legn(i)=feval(symengine,'numlib::legendre',tempna,RAModd(i));
                end
            end
            while  (ismember(1,Legn)==1)| (gcd(tempna,prodramodd)~=1)
                % the last condition is to avoid the situation that
                %the input of Legendre symbol ( /p) is not
                %relatively prime to p
                tempna=tempna-8;
                if gcd(tempna,prodramodd)==1
                    for i=1:length(RAModd)
              Legn(i)=feval(symengine,'numlib::legendre',tempna,RAModd(i));
                    end
                end
            end
```

```
    else  %-1 is in RAM
        %%
        % to choose tempna<0 such that a is nonquare in Z/pZ for all
        %odd primes p in RAModd and a=5 mod 8
        if gcd(tempna,prodramodd)==1
            %to avoid the situation that the input of
            %Legendre symbol ( /p) is not relatively prime to p
            for i=1:length(RAModd)
         Legn(i)=feval(symengine,'numlib::legendre',tempna ,RAModd(i));
            end
        end
        while  (ismember(1,Legn)==1)| (gcd(tempna,prodramodd)~=1)
            % the last condition is to avoid the situation that
            %the input of Legendre symbol ( /p) is not
            %relatively prime to p
            tempna=tempna-8;
            if gcd(tempna,prodramodd)==1
                for i=1:length(RAModd)
         Legn(i)=feval(symengine,'numlib::legendre',tempna ,RAModd(i));
                end
            end
        end
    end
end

%%
P=f_primefactors(temppa,FP); % the set of prime factors of temppa
N=f_primefactors(tempna,FP); % the set of prime factors of tempna
c=prod(RAM);
temppd=prod(P);
tempnd=prod(N);
%%
if ismember(-1,RAM)==0 %-1 is not in RAM
    i=2;
    j=2;
    %find a prime p= mod c (Dirichlet's Thm)
    while (mod(FP(i)-c,temppd)~=0) | (ismember(FP(i),union(RAM,P))==1)
        i=i+1;
    end
     %find a prime p=c mod tempnd (Dirichlet's Thm)
    while (mod(FP(j)-c,tempnd)~=0) | (ismember(FP(j),union(RAM,N))==1)
        j=j+1;
    end
    if abs(temppa*FP(i))<=abs(tempna*FP(j))
        PAIR=[temppa c*FP(i)];
    else
        PAIR=[tempna c*FP(j)];
    end
    %%
    RAMPAIR=f_findplace(PAIR,FP);
     % to check the ramified places of PAIR is the set RAM
    if isempty(union(setdiff(RAMPAIR,RAM),setdiff(RAM,RAMPAIR)))==1
        PAIR
    else
```

```
            disp('errors in the Rrocess')
        end
    else %-1 is in RAM
        %%
        j=2;
        %find a prime p=c mod tempnd (Dirichlet's Thm)
        while (mod(FP(j)-c,tempnd)~=0) | (ismember(FP(j),union(RAM,N))==1)
            j=j+1;
        end
        %%
        PAIR=[tempna c*FP(j)];
        RAMPAIR=f_findplace(PAIR,FP);
        % to check the ramified places of PAIR is the set RAM
        if isempty(union(setdiff(RAMPAIR,RAM),setdiff(RAM,RAMPAIR)))==1
            PAIR
        else
            disp('errors in the Rrocess')
        end
    end
else
    PAIR=[1 1]
end
```

Here is the second code.

```
clc; clear;
RAM=[  ]  % the ramified places
          % ramifies at infinite place iff -1 appears
FP=primes(1000000); % to check the prime factors for large numbers
%%
%functions will be applied in the algorithm:
%f_primefactors: to find finding prime factors of a given integer
%f_findplace: to find the ramified places for a given quaternion (a,b)

%%
if isempty(RAM)==0
    a=prod(RAM);
    RAModd=setdiff(RAM,[-1, 2]); % the set of odd prime p in RAM
    % -1 not in RAM:
    %to choose a odd prime p* not in RAM such that
    % p* is nonsquare in Z/pZ all p in RAModd and p*=5 mod 8
    % or  -p* is nonsquare in Z/pZ all p in RAModd and -p*=5 mod 8

    % -1 in RAM:
    %to choose a odd prime p* not in RAM such that
    % -p* is nonsquare in nonsquare in Z/pZ all p in RAModd and -p*=5 mod 8
    %%
    if ismember(-1,RAM)==0 % -1 not in RAM
        i=2;
        j=2;
        if isempty(RAModd)==0   % RAM contains an odd prime
            Legp=ones(1,length(RAModd));
            Legn=ones(1,length(RAModd));
```

```
        %%
        if ismember(FP(i),RAM)~=1
            for k=1:length(RAModd)
           Legp(k)=feval(symengine,'numlib::legendre',FP(i),RAModd(k));
            end
        end

        while (ismember(FP(i),RAM)==1)|( (mod(FP(i),8)~=5)|
            (ismember(1,Legp)==1) )
            i=i+1;
            if ismember(FP(i),RAM)~=1
                for k=1:length(RAModd)
           Legp(k)=feval(symengine,'numlib::legendre',FP(i),RAModd(k));
                end
            end
        end
        bp=FP(i);
        %%
        if ismember(FP(j),RAM)~=1
            for k=1:length(RAModd)
         Legn(k)=feval(symengine,'numlib::legendre',-FP(j),RAModd(k));
            end
        end

        while (ismember(FP(j),RAM)==1)|( (mod(-FP(j),8)~=5)|
                                                (ismember(1,Legn)==1))
            j=j+1;
            if ismember(FP(j),RAM)~=1
                for k=1:length(RAModd)
         Legn(k)=feval(symengine,'numlib::legendre',-FP(j),RAModd(k));
                end
            end
        end
        bn=-FP(j);
        %%
        if bp<=abs(bn)
            b=bp;
        else
            b=bn;
        end
%%
    else % RAM contains no odd primes
        while (ismember(FP(i),RAM)==1)| (mod(FP(i),8)~=5)
            i=i+1;
        end
        bp=FP(i);
        while (ismember(FP(j),RAM)==1)| (mod(-FP(j),8)~=5)
            j=j+1;
        end
        bn=-FP(j);

        if bp<=abs(bn)
            b=bp;
        else
```

```
                b=bn;
            end
        end
    %%
    else % -1 in RAM
        i=2;
        if isempty(RAModd)==0    % RAM contains an odd prime
            Leg=ones(1,length(RAModd));
            if ismember(FP(i),RAM)~=1
                for j=1:length(RAModd)
                Leg(j)=feval(symengine,'numlib::legendre',-FP(i),RAModd(j));
                end
            end
            while (ismember(FP(i),RAM)==1)|( (mod(FP(i),8)~=3)|
                                                (ismember(1,Leg)==1) )
                i=i+1;
                if ismember(FP(i),RAM)~=1
                    for j=1:length(RAModd)
                Leg(j)=feval(symengine,'numlib::legendre',-FP(i),RAModd(j));
                    end
                end
            end
            b=-FP(i);
%%
        else % RAM contains no odd primes
            while (ismember(FP(i),RAM)==1)| (mod(FP(i),8)~=3)
                i=i+1;
            end
            b=-FP(i);
        end
    end
 %%
    PAIR=[a b];
    RAMPAIR=f_findplace(PAIR,FP);
    if isempty(union(setdiff(RAMPAIR,RAM),setdiff(RAM,RAMPAIR)))==1
        PAIR
    else
        disp('errors in the process')
    end
else
    PAIR=[1 1]
end
```

# References


[1] W. K. Chan, *Arithmetic of Quaternion Algebras*, online notes.

[2] D. S. Dummit and R.M. Foote, *Abstract Algebra*, 3rd. ed., Wiley, 2003.

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

[4] I. N. Herstein, *Noncommutaive Rings*, the Mathematical Association of America, 1973.

[5] N. Jacobson, *Basic Algebra II*, 2nd. ed., Dover, 2009.

[6] S. Lang, *Algebra*, Rev. 3rd. ed., Springer-Verlag, New York, 2005.

[7] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number fields*, 2nd. ed., Springer-Verlag, New York, 2008.

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

[9] R. T. Sharifi, *Group Cohomology*, online notes.