พีชคณิตควอเทอร์เนียนเหนือภาคขยายของฟีลด์ของฟังก์ชัน

นายศิลิพงษ์ ทองมีปั่น

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2563

QUATERNION ALGEBRAS OVER SOME EXTENSIONS OF FUNCTION FIELDS

Mr. Silipong Thongmeepun

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2020

Thesis Title	QUATERNION ALGEBRAS OVER SOME EXTENSIONS OF FUNCTION FIELDS
By	Mr. Silipong Thongmeepun
Field of Study	Mathematics
Thesis Advisor	Nithi Rungtanapirom, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

. . . . Dean of the Faculty of Science

(Professor Polkit Sangvanich, Ph.D.)

THESIS COMMITTEE

Yotsanan Meemark

. . . . Chairman

(Professor Yotsanan Meemark, Ph.D.)

Nithi Rungn

. . . . Thesis Advisor

(Nithi Rungtanapirom, Ph.D.)

T. Chaichana

. . . . Examiner

(Associate Professor Tuangrat Chaichana, Ph.D.)

. . . . External Examiner

(Assistant Professor Detchat Samart, Ph.D.)

ศิลิพงษ์ ทองมีปั่น: พีชคณิตควอเทอร์เนียนเหนือภาคขยายของฟีลด์ของฟังก์ชัน. (QUATERNION ALGEBRAS OVER SOME EXTENSIONS OF FUNCTION FIELDS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : อ.ดร. นิธิ รุ่งธนาภิรมย์, 27 หน้า.

ในวิทยานิพนธ์นี้ เราศึกษาพีชคณิตควอเทอร์เนียนเหนือฟีลด์ของฟังก์ชันตรรกยะบนฟีลด์จำกัดที่มีขนาดเป็นจำนวนคี่ เป็นที่รู้จักกันดีว่าพีชคณิตควอเทอร์เนียนจะเป็นพีชคณิตของเมทริกซ์ขนาด 2×2 หรือพีชคณิตการหารอย่างใดอย่างหนึ่ง เราคำนวณหาเงื่อนไขที่ทำให้พีชคณิตควอเทอร์เนียนในรูป $\left(\frac{c, f(t)}{\mathbb{F}_q(t)}\right)$ เป็นพีชคณิตการหาร และหาเงื่อนไขที่ทำให้พีชคณิตควอเทอร์เนียนแตกตัวหลังจากขยายไปบนภาคขยายฟีลด์ค่าคงตัวระดับขั้นสอง

ภาควิชา	คณิตศาสตร์และ วิทยาการคอมพิวเตอร์	ลายมือชื่อนิสิต	ศิลิพงษ์ ทองมีปั่น
สาขาวิชา	คณิตศาสตร์	ลายมือชื่อ อ.ที่ปรึกษาหลัก	นิธิ รุ่งธนาภิรมย์
ปีการศึกษา	2563		

6270104023: MAJOR MATHEMATICS

KEYWORDS: QUATERNION ALGEBRA / FUNCTION FIELD / SPLITTING FIELD

SILIPONG THONGMEEPUN : QUATERNION ALGEBRAS OVER SOME EXTENSIONS OF FUNCTION FIELDS. ADVISOR : NITHI RUNGTANAPIROM, Ph.D., 27 pp.

In this thesis, we study quaternion algebras over rational function fields over finite fields of odd order. [It is known that a quaternion algebra is either the algebra of $2 \times 2-$matrices or a division algebra.] We determine conditions for quaternion algebras of the form $\left(\frac{c, f(t)}{\mathbb{F}_q(t)}\right)$ to be division algebras and conditions for quaternion algebras to split after the constant quadratic field extension.

Department:	Mathematics and Computer Science	Student's Signature	Silipong Thongmeepun
Field of Study:	Mathematics	Advisor's Signature	Nithi Rung
Academic Year:	2020		

Acknowledgements

I would like to express my sincere gratitude to my thesis advisor, Dr. Nithi Rungtanapirom for providing invaluable, guidance, comments, and suggestions throughout the course of this thesis. I could not have imagined having a better advisor and mentor for my thesis. Besides my advisor, I would like to express my special thanks to my project committee: Professor Dr. Yotsanan Meemark, Associate Professor Dr. Tuangrat Chaichana, and Assistant Professor Dr. Detchat Samart for their encouragement, insightful comments, and hard questions. Moreover, I feel very thankful to all of my teachers who have taught me abundant knowledge for supporting me a scholarship to do the project comfortably. Special thanks go to my friends for helping me to assemble the parts and give suggestion about my project. Last but not least, I would like to thank my family for supporting me spiritually throughout my life.

CONTENTS

Page

Chapter 1

INTRODUCTION

We begin by recalling basic facts about quaternion algebras and global fields. We assume that every ring is with unit and denote by $F^\times$ the set of units of a field F. An **algebra** B over a field F or an $F-$**algebra** is a vector space B over F together with a ring structure on B satisfying

$$(ax)(by) = (ab)(xy) \text{ for all } x, y \in B, a, b \in F,$$

or equivalently, a ring B together with a ring homomorphism from F to B whose image lies in its center. An algebra B is a **division algebra** if every nonzero element has a multiplicative inverse. Furthermore, an algebra is **central** if the image of its homomorphism is exactly its center, and is **simple** if it has no non-trivial ideals. For algebras A, B over a field F, an **algebra homomorphism** from A to B is a ring homomorphism from A to B which is also linear over F. It is an **isomorphism** if it is bijective. If there is an isomorphism from A to B, then we say that A is **isomorphic** to B and denote this by $A \simeq B$.

A **quaternion algebra** B over a field F is a central simple algebra of dimension 4 over F. If B is a quaternion algebra over a field F with $\operatorname{char} F \neq 2$, then there are $i, j \in B$, $a, b \in F^\times$ such that $\{1, i, j, ij\}$ is an $F-$basis for B and

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

In this case, B is denoted by $(\frac{a,b}{F})$.

Example 1.1. Let F be a field with $\operatorname{char} F \neq 2$. Recall that the algebra of $2 \times 2-$matrices over F is an $F-$algebra, denoted by $M_2(F)$. Additionally, it is a quaternion algebra over F, and $(\frac{1,1}{F}) \simeq M_2(F)$. In fact, an isomorphism is given by

$$i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let K be a field extension of F, and B be a quaternion algebra over F. We say that K is a **splitting field** for B, K **splits** B, or B is **split** by K if $B \otimes_F K \simeq M_2(K)$. Note that $(\frac{a,b}{F}) \otimes_F K \simeq (\frac{a,b}{K})$.

Theorem 1.2. (Voight, 2021, Theorem 5.4.4) *Let F be a field with* $\operatorname{char} F \neq 2$. *Let $B = (\frac{a,b}{F})$ be a quaternion algebra over F for some $a, b \in F^\times$. The followings are equivalent:*

(1) $B \simeq M_2(F)$,

(2) *B is not a division algebra,*

(3) $\exists x, y \in F : ax^2 + by^2 = 1$.

Several results are known so far about quaternion algebras over $\mathbb{Q}$ that are split by certain field extensions. For integers a, b and a natural number c, the notation $a \equiv b \pmod{c}$ means that $a - b$ is divisible by c. Now, we give some examples. Recall that if p is an odd prime number and d is an integer such that p does not divide d, then the **Legendre symbol** for d over p is given by

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & \text{if } \exists a \in \mathbb{Z} : d \equiv a^2 \pmod{p}, \\ -1 & \text{otherwise.} \end{cases}$$

Moreover, an important magnitude of a number field F is the **discriminant**, denoted by Δ_F (Neukirch, 1999, Remark, p.14). For example, if $F = \mathbb{Q}(\sqrt{d})$ for some square-free integer d, then

$$\Delta_F = \begin{cases} 4d & \text{if } d \equiv 2, 3 \pmod{4}, \\ d & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Conditions for quaternion division algebras over quadratic number fields are in terms of the Legendre symbol and the discriminant of that number field. The proofs of these theorems use some properties about the local Hilbert symbol. In Acciaro et al. (2019) and Acciaro et al. (2004), Acciaro et al. proved the following theorems, which are related to quadratic extensions and Galois extensions.

Theorem 1.3. (Acciaro et al., 2019, Proposition 5) *Let $F = \mathbb{Q}(\sqrt{d})$ with discriminant Δ_F, where $d \neq 1$ is a square-free integer. Let p be an odd prime integer with $p \equiv 3 \pmod 8$. Then $(\frac{p,2}{F})$ is a division algebra if and only if $(\frac{\Delta_F}{p}) = 1$ or $d \equiv 1 \pmod 8$.*

Theorem 1.4. (Acciaro et al., 2019, Proposition 6) *Let $F = \mathbb{Q}(\sqrt{d})$ with discriminant Δ_F, where $d \neq 1$ is a square-free integer. Let p, q be odd prime integers with $p \equiv q \equiv 3 \pmod 4$ and $(\frac{q}{p}) \neq 1$. Then $(\frac{p,q}{F})$ is a division algebra if and only if $(\frac{\Delta_F}{p}) = 1$ or $d \equiv 1 \pmod 8$.*

Theorem 1.5. (Acciaro et al., 2004, Theorem 3.9) *Let $F = \mathbb{Q}(\sqrt{d})$ with discriminant Δ_F, where $d \neq 1$ is a square-free integer. Let K be an extension of F which is Galois over $\mathbb{Q}$ with the dihedral group of degree 2ℓ for some odd prime number ℓ as Galois group. Let p, q be distinct prime integers. Then $(\frac{p,q}{K})$ is a division algebra if and only if one of the following conditions is satisfied:*

(1) *p or $q \equiv 1 \pmod 4$, $(\frac{p}{q}) = -1$, and $(\frac{\Delta_F}{p}) = 1$ or $(\frac{\Delta_F}{q}) = 1$;*

(2) *$p \equiv 3 \pmod 8$, and $(\frac{\Delta_F}{p}) = 1$ or $d \equiv 1 \pmod 8$;*

(3) *$p \equiv q \equiv 3 \pmod 4$, $(\frac{q}{p}) = -1$, and $(\frac{\Delta_F}{p}) = 1$ or $d \equiv 1 \pmod 8$.*

Consequently, in the situation of Theorem 1.5, if p, q are distinct prime integers such that $p \equiv q \equiv 3 \pmod 4$, and $(\frac{p}{q}) = -1$, then $(\frac{p,q}{F})$ is split by K if and only if $(\frac{p,q}{F})$ is the matrix algebra.

The proofs of these theorems rely on the local-global principle in the version of number fields, but we will introduce the general version in terms of global fields in next chapters, and our results over $\mathbb{F}_q(t)$ where q is an odd prime power will be discussed in the final chapter. Our approach is to find an explicit quaternion algebra which is ramified at the given places, which can be verified by the local Hilbert symbol.

Chapter 2

VALUATIONS

In this chapter, we introduce an approach for places of global fields. Let F be a field and $F^\times = F\setminus\{0\}$. A **valuation** or **absolute value** of F is a function $|\cdot| : F \to \mathbb{R}$ such that

(1) $|x| \geq 0$ for all $x \in F$,

(2) $|x| = 0 \Longleftrightarrow x = 0$ for all $x \in F$,

(3) $|x| \cdot |y| = |xy|$ for all $x \in F$,

(4) $|x + y| \leq |x| + |y|$ for all $x, y \in F$.

For example, the trivial valuation defined by

$$|0| = 0, |x| = 1 \text{ for all } x \in F^\times$$

is a valuation on F. We note that F with a valuation $|\cdot|$ induces a metric space by defining the distance to be

$$d(x, y) := |x - y| \text{ for all } x, y \in F,$$

hence also a topological space. Moreover, two valuations of a field F are **equivalent** if they induce the same topology on F. A valuation $|\cdot|$ of a field F is called **non-archimedean** if $|n|$ stays bounded for all $n \in \mathbb{N}$. Otherwise, it is called **archimedean**. Two valuations $|\cdot|_1, |\cdot|_2$ are **equivalent** if there is a positive real number s such that $|x|_1 = |x|_2^s$ for all $x \in F$.

Proposition 2.1. (Neukirch, 1999, Chapter 2, Proposition 3.6) *A valuation $|\cdot|$ of a field F is non-archimedean if and only if it satisfies for all $x, y \in F$*

$$|x + y| \leq \max\{|x|, |y|\}.$$

Moreover, $|x + y| = \max\{|x|, |y|\}$ *if* $|x| \neq |y|$.

We define an **exponential valuation** of F with respect to a non-archimedean valuation $|\cdot|$ to be the function

$$v : F \to \mathbb{R} \cup \{\infty\}, \quad v(x) = \begin{cases} -\log|x| & \text{if } x \neq 0, \\ \infty & \text{if } x = 0. \end{cases}$$

Moreover, the exponential valuation v satisfies for all $x, y \in F$:

(1) $v(x) = \infty \iff x = 0$,

(2) $v(xy) = v(x) + v(y)$,

(3) $v(x+y) \geq \min\{v(x), v(y)\}$,

(4) $v(x+y) = \min\{v(x), v(y)\}$ if $v(x) \neq v(y)$,

providing $a < \infty, a + \infty = \infty, \infty + \infty = \infty$ for all $a \in \mathbb{R}$. Two exponential valuations v_1, v_2 are **equivalent** if there is a positive real number s such that $v_1(x) = sv_2(x)$ for all $x \in F^\times$. Conversely, if we have a function $v : F \to \mathbb{R} \cup \{\infty\}$ satisfying above conditions, then we obtain a non-archimedean valuation defined by

$$|x| = q^{-v(x)} \text{ for all } x \in F,$$

for some fixed $q > 1$. Consequently, we obtain a one-to-one correspondence between the equivalence classes of non-archimedean valuations and the equivalence classes of exponential valuations. From now on, valuations refer to exponential valuations or non-archimedean valuations.

Proposition 2.2. (Neukirch, 1999, Chapter 2, Proposition 3.8) *Let F be a field with a valuation v. Then*

$$\mathcal{O}_v := \{x \in F \big| v(x) \geq 0\}$$

is a subring of F, and

$$\mathfrak{p}_v := \{x \in F \big| v(x) > 0\}$$

is the unique maximal ideal of $\mathcal{O}_v$.

Let v be a valuation of a field F. $\mathcal{O}_v$ is called a **valuation ring**, and $\mathcal{O}_v/\mathfrak{p}_v$ is called the **residue field** of v. v is **discrete** if $v(F^\times) = s\mathbb{Z}$ for some positive real number s, and v is a **normalized discrete valuation** if $s = 1$. In this case, there is $\pi \in \mathcal{O}_v$ such that $v(\pi) = 1$, and π is called a **uniformizer** of v. In addition, for all $x \in F^\times$, we can express $x = u\pi^{v(x)}$ for some $u \in \mathcal{O}_v \setminus \mathfrak{p}_v$ ($v(u) = 0$). For any $x, y \in F$ and a uniformizer π, we will write $x \equiv y \pmod{\pi}$ for $x - y \in \mathfrak{p}_v$.

Let F be a field with an absolute value $|\cdot|$. Let $(a_n)_{n\in\mathbb{N}}$ be a sequence in F. For an element $a \in F$, $(a_n)_{n\in\mathbb{N}}$ **converges** to a if it satisfies

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} \forall n \in \mathbb{N} : n \geq N \implies |a_n - a| < \varepsilon.$$

A sequence $(a_n)_{n\in\mathbb{N}}$ in F is said to be **convergent** if it converges to some element in F called **limit** of the sequence. Indeed, a convergent sequence has unique limit, and we denote the limit by $\lim\limits_{n\to\infty} a_n$. A sequence $(a_n)_{n\in\mathbb{N}}$ in F is a **Cauchy sequence** if it satisfies

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} \forall m, n \in \mathbb{N} : m, n \geq N \implies |a_n - a_m| < \varepsilon.$$

In particular, every convergent sequence is a Cauchy sequence, and F is said to be **complete** if every Cauchy sequence is convergent. The set of Cauchy sequences together with pointwise addition and multiplication form a ring. Moreover, the set of sequences converging to 0 is an ideal, and the quotient ring is a field, called the **completion** of F. If v is a valuation of F concerning to $|\cdot|$, then we denote F_v the completion of F with respect to v.

Recall that a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$ for a prime number p is called a **global field**, and its completion is called a **local field**. We will focus on the places of global function fields. Here a **place** of F is an equivalence class of valuations of F. The places of the rational function field over a finite field can be described by the below theorem.

Theorem 2.3. (Stichtenoth, 2009, Theorem 1.2.2) *Let q be a prime power. The places of $\mathbb{F}_q(t)$ are given by the following:*

(1) *The valuation v_f, where f is a monic irreducible polynomial over $\mathbb{F}_q$, is given by*

$$v_f\left(f^n \cdot \frac{g}{h}\right) = n \quad \text{for } g, h \in \mathbb{F}_q[t],\ g, h \neq 0, f \text{ does not divide both } g, h.$$

In this case, f is a uniformizer for v_f since $v_f(f) = 1$, and we define $\deg v_f = \deg f$.

(2) *The place at infinity with the valuation v_∞ is given by*

$$v_\infty\left(\frac{g}{h}\right) = \deg h - \deg g \quad \text{for } g, h \in \mathbb{F}_q[t],\ g, h \neq 0.$$

In this case, $\frac{1}{t}$ is a uniformizer for v_∞ since $v_\infty(\frac{1}{t}) = 1$, and we define $\deg v_\infty = 1$.

Now we can give an example of a completion of the rational function field:

Theorem 2.4. (Stichtenoth, 2009, Theorem 4.2.6) *Let $F = \mathbb{F}_q(t)$. Let v be a place of degree 1 with a uniformizer π. Then every $x \in F_v$ can be written as the unique form*

$$x = \sum_{i=n}^{\infty} a_i \pi^i \textit{ with } n \in \mathbb{Z}, a_i \in \mathbb{F}_q.$$

Moreover, for any sequence $(a_i)_{i \geq n}$ in $\mathbb{F}_q$ for some $n \in \mathbb{Z}$, the series $\sum_{i=n}^{\infty} a_i \pi^i$ converges in F_v and the valuation can be defined on F_v by

$$v\left(\sum_{i=n}^{\infty} a_i \pi^i\right) = \min\{i | a_i \neq 0\}.$$

The following theorem is an important result for local fields:

Theorem 2.5 (Hensel's Lemma)**.** (Voight, 2021, Theorem 12.2.17) *Let F be a nonarchimedean local field with valuation v, valuation ring $\mathcal{O}_v$, and maximal ideal $\mathfrak{p}$. Let $f(x) \in \mathcal{O}_v[x]$, and $a \in \mathcal{O}_v$ satisfy $m := v(f(a)) > 2v(f'(a))$. Then there exists $\widetilde{a} \in \mathcal{O}_v$ such that*

$$f(\widetilde{a}) = 0 \quad \textit{and} \quad \widetilde{a} \equiv a \pmod{\mathfrak{p}^m}.$$

Let K be a finite extension over a global function field F. Let v be a place of F, and w be a place of K. We say that w is an **extension** of v over K, w **lies over** v, or v **lies under** w if $v = e \cdot w$ for some positive integer e, where we, by abuse of notation, write v, w for the normalized discrete valuations associated to v, w, respectively. In this case, $e_{w|v} := e$ is called the **ramification index**. For the alternative definition of extension of v which appears in (Stichtenoth, 2009, Proposition 3.1.4), $\mathcal{O}_w/\mathfrak{p}_w$ is a vector space over $\mathcal{O}_v/\mathfrak{p}_v$, and its dimension is finite, denoted by $f_{w|v}$, which is called the **inertia degree**.

Theorem 2.6. (Stichtenoth, 2009, Theorem 3.1.11) *Let K be a finite extension over a function field F. Let v be a place of F, and $w_1, \ldots, w_g$ be all extensions of v over K where g is the number of the extensions of v over K. Then*

$$\sum_{i=1}^{g} e_{w_i|v} f_{w_i|v} = [K : F].$$

Chapter 3

QUATERNION ALGEBRAS OVER GLOBAL FIELDS

In this chapter, we introduce some facts about quaternion algebras over global fields or local fields. Let F be a global field, v be a place of F, and B be quaternion algebra over F. We denote $B \otimes_F F_v$ by B_v. The splitting condition for a quaternion algebra over F_v is then given by the local Hilbert symbol. Let $B = (\frac{a,b}{F})$, where $a, b \in F^\times$. The **local Hilbert symbol** is defined by

$$(a,b)_v = \begin{cases} 1 & \text{if } B_v \simeq M_2(F_v), \\ -1 & \text{if } B_v \text{ is a division algebra.} \end{cases}$$

Note that this is well-defined since B_v is again a quaternion algebra over F, hence by Theorem 1.2 either the matrix algebra $M_2(F_v)$ or a division algebra. We say that B is **split** or **unramified** at v if $(a,b)_v = 1$, and is **ramified** at v if $(a,b)_v = -1$. Let us give some basic properties of the local Hilbert symbol here:

Theorem 3.1. (Voight, 2021, Lemma 12.4.3) *Let F be a global field and v be a place of F. Let $a, b \in F^\times$. Then the following statements hold:*

(1) $(ac^2, bd^2)_v = (a,b)_v$ *for all* $c, d \in F^\times$.

(2) $(a,b)_v = (b,a)_v$.

(3) $(a,b)_v = (a,-ab)_v = (b,-ab)_v$.

(4) $(1,a)_v = (a,-a)_v = 1$.

(5) *If* $a \neq 1$, *then* $(a, 1-a)_v = 1$.

Theorem 3.2. (Voight, 2021, Lemma 12.4.6) *Let F be a global field and v be a place of F. Let $a, b, c \in F^\times$. Then* $(a, bc)_v = (a,b)_v(a,c)_v$ *and* $(ab, c)_v = (a,c)_v(b,c)_v$.

The computation of the local Hilbert symbol can be done as follows:

Definition 3.3. Let F be a field with a normalized discrete valuation v and a uniformizer $\pi \in F$ (i.e. $v(\pi) = 1$). For $d \in F$ such that $v(d) = 0$, we define the **Legendre symbol** for d over π by

$$\left(\frac{d}{\pi}\right) = \begin{cases} 1 & \text{if } \exists a \in F : d \equiv a^2 \pmod{\pi}, \\ -1 & \text{otherwise.} \end{cases}$$

Lemma 3.4. *Let q be an odd prime power and $c \in \mathbb{F}_q^\times$. Then $c^{\frac{q-1}{2}} = 1$ if $c \in (\mathbb{F}_q^\times)^2$ and $c^{\frac{q-1}{2}} = -1$ if $c \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$.*

Proof. Let ξ be a generator of $\mathbb{F}_q^\times$. If $c = d^2$ for some $d \in \mathbb{F}_q^\times$, then we get that $c^{\frac{q-1}{2}} = d^{q-1} = 1$. Assume c is not square. Since $q-1$ is even, we have $c = \xi^{2\ell+1}$ for some $\ell \in \mathbb{N}$. It follows that

$$c^{\frac{q-1}{2}} = \xi^{\ell(q-1)}\xi^{\frac{q-1}{2}} = \xi^{\frac{q-1}{2}} = -1. \qquad \square$$

Proposition 3.5. *Let F be a field with a normalized discrete valuation v and a uniformizer $\pi \in F$. Suppose that the residue field k has order q for some odd prime power q. Let $a, b \in F$ such that $v(a) = v(b) = 0$, then*

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

Proof. Consider for each $a, d \in F$ where $a \in \mathcal{O}_v \setminus \mathfrak{p}_v$ and $a - d^2 \in \mathfrak{p}_v$. Observe that $d^2 = a-(a-d^2) \in \mathcal{O}_v$. If $d \in F \setminus \mathcal{O}_v$, then $d^{-1} \in \mathcal{O}_v$, and it follows that $d = d^2 d^{-1} \in \mathcal{O}_v$. If $d \in \mathfrak{p}_v$, then $a = (a-d^2) + d^2 \in \mathfrak{p}_v$. Thus $d \in \mathcal{O}_v \setminus \mathfrak{p}_v$. Therefore we can conclude that for each $a \in \mathcal{O}_v \setminus \mathfrak{p}_v$, $(\frac{a}{\pi}) = 1$ if and only if $a + \mathfrak{p}_v$ is square in k.

Now let $a, b \in F$ such that $v(a) = v(b) = 0$. Let $x = a + \mathfrak{p}_v$ and $y = b + \mathfrak{p}_v$. Then we have

$$x^{\frac{q-1}{2}} y^{\frac{q-1}{2}} = (xy)^{\frac{q-1}{2}},$$

whence the desired equation follows from Lemma 3.4 immediately. $\square$

Theorem 3.6. *Let F be a non-archimedean local field with uniformizer π, valuation v with $v(\pi) = 1$, and residue field k. Let $q = |k|$, and suppose that q is odd. Let $a, b \in F^{\times}$, if we write $a = a_0\pi^{v(a)}$ and $b = b_0\pi^{v(b)}$ for some $a_0, b_0 \in F^{\times}$ with $v(a_0) = v(b_0) = 0$, then*

$$(a,b)_v = (-1)^{v(a)v(b)\frac{q-1}{2}} \left(\frac{a_0}{\pi}\right)^{v(b)} \left(\frac{b_0}{\pi}\right)^{v(a)}.$$

Proof. If we know that $(a_0, b_0)_v = 1$, $(a_0, \pi)_v = (\frac{a_0}{\pi})$, $(\pi, b_0)_v = (\frac{b_0}{\pi})$, and $(\pi,\pi)_v = (-1)^{\frac{q-1}{2}}$, then we can apply Theorem 3.2 to obtain the desired equation.

First, let $\mathcal{O}_v$ be the valuation ring of F. It is known from (O'Meara, 1973, Theorem 63:11a) that the equation $a_0x^2 + b_0y^2 = 1$ has a solution modulo π. Suppose that $x_0, y_0 \in \mathcal{O}_v$ are such that $a_0x_0^2 + b_0y_0^2 \equiv 1 \pmod{\pi}$. We may assume without loss of generality that $x_0 \not\equiv 0 \pmod{\pi}$, so $v(x_0) = 0$. Now consider the polynomial

$$f(x) := a_0x^2 + b_0y_0^2 - 1 \in \mathcal{O}_v[x].$$

Since q is odd, we have $1 \not\equiv -1 \pmod{\pi}$, so $v(2) = 0$. By observing that

$$v(a_0x_0^2 + b_0y_0^2 - 1) \geq 1 > 0 = v(2) + v(a_0) + v(x_0) = 2v(2a_0x_0),$$

we can apply Theorem 2.5 to obtain $\widetilde{x} \in \mathcal{O}_v$ such that $a_0\widetilde{x}^2 + b_0y_0^2 = 1$. By Theorem 1.2, we have $(a_0, b_0)_v = 1$.

Next, let $c \in \mathcal{O}_v^{\times}$. We will show that $(c,\pi)_v = (\frac{c}{\pi})$. Assume that $(\frac{c}{\pi}) = 1$. Then $x_0^2 - c \equiv 0 \pmod{\pi}$ for some $x_0 \in F$. More precisely, $x_0 \in \mathcal{O}_v^{\times}$ since $v(x_0^2) = v(c) = 0$. Then we can apply Theorem 2.5 to $x^2 - c \in \mathcal{O}_v[x]$ and x_0 because

$$v(x_0^2 - c) \geq 1 > 0 = 2v(2x_0),$$

so we obtain $\widetilde{x} \in \mathcal{O}_v$ such that $\widetilde{x}^2 = c$. It follows that $c(\frac{1}{\widetilde{x}})^2 + \pi(0)^2 = 1$. Conversely, assume that $cx^2 + \pi y^2 = 1$ for some $x, y \in F$. If $x = 0$, then we have $2v(y) = -1$ which is impossible, so $x \neq 0$. Since $2v(x) \neq 1 + 2v(y)$, we have

$$0 = v(cx^2 + \pi y^2) = \min\{2v(x), 1 + 2v(y)\},$$

which implies that $v(x), v(y) \geq 0$. Note that

$$v(x) = v\left(\frac{\pi y^2 - 1}{c}\right) = v(\pi y^2 - 1) - v(c) = 0 - 0 = 0.$$

Hence c is a square modulo π.

From the previous paragraph, we obtain $(a_0, \pi)_v = (\frac{a_0}{\pi})$. Hence by Theorem 3.1 and Lemma 3.4, we have $(\pi, b_0)_v = (\frac{b_0}{\pi})$, and

$$(\pi, \pi)_v = (\pi, -\pi^2)_v = (\pi, -1)_v = \left(\frac{-1}{\pi}\right) = (-1)^{\frac{q-1}{2}}$$

as desired. □

Corollary 3.7. *Let F be a non-archimedean local field with uniformizer π, valuation v with $v(\pi) = 1$, and residue field k. Let $q = |k|$, and suppose that q is odd. The following holds for $a, b \in F^\times$:*

(1) *If $v(a) = 0$, then $(a, b)_v = (\frac{a}{\pi})^{v(b)}$.*

(2) *If $v(a) = v(b) = 0$, then $(a, b)_v = 1$.*

Proof. (1) If $v(a) = 0$, we can write $a = a\pi^0$, i.e. $a_0 = a$. Hence by Theorem 3.6, we have

$$(a, b)_v = (-1)^0 \left(\frac{a_0}{\pi}\right)^{v(b)} \left(\frac{b_0}{\pi}\right)^0 = \left(\frac{a_0}{\pi}\right)^{v(b)}.$$

(2) This follows easily from (1) by substituting $v(b) = 0$. □

The quaternion algebras over a global field can be classified by the following theorem. Note that if K is a number field and v is an archimedean place of K, then v can be obtained from an embedding of K in $\mathbb{C}$. In this case, v is a real place if the image of the associated embedding is contained in $\mathbb{R}$ and complex otherwise.

Theorem 3.8. (Voight, 2021, Theorem 14.6.1) *Let F be a global field. The set of the ramified places of a given quaternion algebra over F contains only non-complex places and has a finite even cardinality. Conversely, for a given finite subset S of non-complex places of F of even cardinality, there is a unique quaternion algebra over F up to isomorphism which is ramified exactly at the places of S.*

Theorem 3.9 (Local-global principle)**.** (Voight, 2021, theorem 14.6.5) *Let B, B' be quaternion algebras over a global field F. Then $B \simeq B'$ if and only if $B_v \simeq B'_v$ for* *all places v of F. In particular, $B \simeq M_2(F)$ if and only if $B_v \simeq M_2(F_v)$ for all places v of F.*

Chapter 4

QUATERNION ALGEBRAS OVER FUNCTION FIELDS

Throughout this chapter, let q be an odd prime power. We determine conditions for quaternion algebra to split by the quadratic constant field extension $\mathbb{F}_{q^2}(t)$. The results are proved by investigating the local Hilbert symbol, and basic properties about finite fields. We denote by $(\mathbb{F}_q^\times)^2$ the set of elements in $\mathbb{F}_q^\times$ which are square.

Lemma 4.1. *Let $c \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$, and $f(t) \in \mathbb{F}_q[t]$ be a monic irreducible polynomial. Then $f(t)$ is a uniformizer of v_f, $v_f(c) = 0$, and*

$$\left(\frac{c}{f(t)}\right) = (-1)^{\deg f(t)}.$$

Proof. Let $d = \deg f(t)$. Recall that the residue field of v_f is $\mathcal{O}_{v_f}/\mathfrak{p}_{v_f} \simeq \mathbb{F}_q[t]/(f(t)) = \mathbb{F}_{q^d}$. By Lemma 3.4, we obtain $c^{\frac{q-1}{2}} = -1$. It follows that

$$c^{\frac{q^d-1}{2}} = c^{(\frac{q-1}{2})(q^{d-1}+\cdots+1)} = (-1)^{(q^{d-1}+\cdots+1)} = (-1)^d,$$

so we conclude that $\left(\frac{c}{f(t)}\right) = (-1)^d$ by Lemma 3.4 again. □

Theorem 4.2. *Let $F = \mathbb{F}_q(t)$, $f(t) \in \mathbb{F}_q[t] \setminus \{0\}$, $c \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$, and $B = (\frac{c,f(t)}{F})$. Suppose that $f(t) = af_1(t)^{\alpha_1} \cdots f_n(t)^{\alpha_n}$, where $f_i(t)$ is a monic irreducible polynomial over $\mathbb{F}_q$, $\alpha_i \in \mathbb{N}$, and $a \in \mathbb{F}_q^\times$ for all $i \in \{1, \ldots, n\}$ for some $n \in \mathbb{N}$. Then the set of places of F at which B is ramified is one of the following:*

(1) *The set of places corresponding to $f_i(t)$ for which $f_i(t)^{\alpha_i}$ has odd degree if $f(t)$ has even degree.*

(2) *The set of places corresponding to $f_i(t)$ for which $f_i(t)^{\alpha_i}$ has odd degree together with the place at infinity if $f(t)$ has odd degree.*

In particular, B is a division algebra if and only if $\deg f_i(t)$ *and α_i are both odd for some i.*

Proof. Let $d = \deg f(t)$, $d_i = \deg f_i(t)$, and v be a place of F. Then $v(c) = 0$ for any place v of F, and we can apply Corollary 3.7. We now distinguish the following cases.

Case 1: $v = v_{f_i(t)}$ for some $i = 1, \dots, n$. By Lemma 4.1, we have

$$(c, f(t))_v = \left(\frac{c}{f_i(t)}\right)^{\alpha_i} = (-1)^{d_i \alpha_i}.$$

Case 2: $v = v_\infty$. In this case, the residue field is $\mathbb{F}_q$ and c is not square in $\mathbb{F}_q$. Hence we can apply Corollary 3.7 to get

$$(c, f(t))_v = \left(\frac{c}{1/t}\right)^{-d} = \left(\frac{c}{1/t}\right)^{d} = (-1)^d.$$

Case 3: $v = v_g$ where $g(t)$ is a monic irreducible polynomial over $\mathbb{F}_q$ other than $f_1(t), \dots, f_n(t)$. It follows from Corollary 3.7 that $(c, f(t))_v = 1$.

Assume that d_i and α_i are odd for some i. Then $(c, f(t))_{v_{f_i}} = (-1)^{d_i \alpha_i} = -1$, i.e. B is ramified at v_{f_i}, in particular a division algebra. Otherwise, d_i or α_i is even for all i, which implies that $d = \alpha_1 d_1 + \cdots + \alpha_n d_n$ is also even. Thus $(c, f(t))_v = 1$ for all places v. Hence the proof is complete by local-global principle. □

Theorem 4.3. *Every quaternion algebra over $F = \mathbb{F}_q(t)$ whose all ramified places are of odd degree splits after a constant quadratic field extension $\mathbb{F}_{q^2}(t)$.*

Proof. Let B be a quaternion algebra over F whose all ramified places are of odd degree. Let S be the set of such places, so that $|S|$ is even by Theorem 3.8. Fix some $c \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$ and let $f(t)$ be the product of all monic irreducible polynomials corresponding to the places in S except v_∞ if $v_\infty \in S$. Note that this is 1 if $|S|$ is empty. We consider two cases.

Case 1: S contains only the places corresponding to irreducible polynomials. Since $|S|$ is even, we have $\deg f(t)$ is even, so $(c, f)_{v_\infty} = 1$. Since the irreducible factors of $f(t)$ have odd degree, it follows from Theorem 4.2 that $(\frac{c,f(t)}{F})$ ramifies exactly in the places of F.

Case 2: S contains the place at infinity v_∞.
Since $|S\backslash\{v_\infty\}|$ is odd, we have $\deg f(t)$ is odd, which implies that $(\frac{c,f(t)}{F})$ is ramified at v_∞. Similarly to Case 1, we obtain $(c, f(t))_v = -1$ if and only if $v \in S$.

From the both cases, we see that $B \simeq (\frac{c,f(t)}{F})$ for some $f(t) \in \mathbb{F}_q[t]$. But then

$$B \otimes_F \mathbb{F}_{q^2}(t) \simeq \left(\frac{c, f(t)}{\mathbb{F}_{q^2}(t)}\right) \simeq M_2(\mathbb{F}_{q^2}(t)).$$

By Lemma 3.4 twice, we have $c^{\frac{q-1}{2}} = -1$, and c is a square in $\mathbb{F}_{q^2}^\times$ because

$$c^{\frac{q^2-1}{2}} = c^{\frac{q-1}{2}(q+1)} = (-1)^{q+1} = 1,$$

so it yields the latter isomorphism. Therefore, $\mathbb{F}_{q^2}(t)$ splits B. □

Now we see that every quaternion algebra over $\mathbb{F}_q(t)$ which is ramified at a places of odd degree and is ramified at no places of even degree is a division algebra, but splits after the constant quadratic field extension $\mathbb{F}_{q^2}(t)$. What is about quaternion algebras over $\mathbb{F}_q(t)$ which is ramified at a place of even degree? We will discuss this problem in the following theorems.

Proposition 4.4. *Let $F = \mathbb{F}_q(t)$, $K = \mathbb{F}_{q^2}(t)$, v be a place of F of even degree. Then v splits completely in K, i.e. there are two valuations w_1, w_2 in K such that*

$$w_1|_F = w_2|_F = v, e_{w_1|v} = e_{w_2|v} = 1, f_{w_1|v} = f_{w_2|v} = 1.$$

Proof. Let $f(t)$ be the monic irreducible polynomial of degree $2d$ over $\mathbb{F}_q$ corresponding to v. Then there is an inclusion $\iota : \mathbb{F}_{q^2} \hookrightarrow \mathbb{F}_{q^{2d}} = \mathbb{F}_q[t] \,/\, (f(t))$. This can be extended to $\alpha : \mathbb{F}_{q^2}[t] \to \mathbb{F}_q[t] \,/\, (f(t))$ by sending t to $t + (f(t))$. It is easy to see that α is a surjective homomorphism. Hence by the first isomorphism theorem,

$$\mathbb{F}_{q^2}[t] \,/\, \ker\alpha \simeq \mathbb{F}_q[t] \,/\, (f(t)) = \mathbb{F}_{q^{2d}}.$$

Moreover, $\ker\alpha = (g(t))$ for some monic irreducible polynomial $g(t)$ of degree d over $\mathbb{F}_{q^2}$ since $\mathbb{F}_{q^2}[t]$ is a PID and $\ker\alpha$ is a prime ideal. Since $\alpha(f(t)) = f(t + (f(t))) = 0$, we have $(f(t)) \cdot \mathbb{F}_{q^2}[t] \subseteq \ker \alpha$, so that $g(t) \mid f(t)$. Let w_1 be the valuation in K corresponding to $g(t)$. Then $f_{w_1|v} = 1$ since

$$\mathbb{F}_{q^2}[t] \;/\; (g(t)) \simeq \mathbb{F}_q[t] \;/\; (f(t)).$$

Note that ramification index of a place of constant field extension is still 1 (Stichtenoth, 2009, Theorem 3.6.3), i.e. $e_{w_1|v} = 1$. By Theorem 2.6, we have another place w_2 of K lying over v which have the same ramification index and inertia degree as w_1. □

Lemma 4.5. *Let $F = \mathbb{F}_q(t)$, $K = \mathbb{F}_{q^2}(t)$, v be a place of F of even degree. Let B be a quaternion algebra over F, and w a place of K lying over v. Then B is ramified at v if and only if $B \otimes_F K$ is ramified at w.*

Proof. Let $B = (\frac{a,b}{F})$ for some $a, b \in F^\times$ and $2d$ be the degree of v. Write $a = a_0\pi^{v(a)}$ and $b = b_0\pi^{v(b)}$ for some uniformizer π. By Proposition 4.4, we get that $\pi = \pi_1\pi_2$ for some irreducible polynomials π_1, π_2 over $\mathbb{F}_{q^2}$, so w corresponds to π_1 without loss of generality. By Theorem 3.6, we obtain two equations:

$$(a,b)_v = (-1)^{v(a)v(b)\frac{q^{2d}-1}{2}} \left(\frac{a_0}{\pi}\right)^{v(b)} \left(\frac{b_0}{\pi}\right)^{v(a)}, \tag{4.1}$$

and

$$(a,b)_w = (-1)^{w(a)w(b)\frac{(q^2)^d-1}{2}} \left(\frac{a_0\pi_2^{w(a)}}{\pi_1}\right)^{w(b)} \left(\frac{b_0\pi_2^{w(b)}}{\pi_1}\right)^{w(a)}. \tag{4.2}$$

Now, we show that $(a,b)_v = (a,b)_w$ to complete the proof. Note that $w|_F = v$ because $e_{w|v} = 1$, and $(\frac{c}{\pi}) = (\frac{c}{\pi_1})$ for all $c \in F$ with $v(c) = 0$ because $f_{w_1|v} = 1$. By considering the parity of $v(a), v(b)$, we may distinguish the following:

Case 1: $v(a), v(b)$ are both even. It is clear.

Case 2: $v(a), v(b)$ are both odd. Then

$$\begin{aligned}\left(\frac{a_0}{\pi}\right)^{v(b)} \left(\frac{b_0}{\pi}\right)^{v(a)} &= \left(\frac{a_0}{\pi}\right)\left(\frac{b_0}{\pi}\right) = \left(\frac{a_0}{\pi}\right)\left(\frac{b_0}{\pi}\right)\left(\frac{\pi_2}{\pi_1}\right)^{w(b)+w(a)} \\ &= \left(\frac{a_0\pi_2^{w(a)}}{\pi_1}\right)\left(\frac{b_0\pi_2^{w(b)}}{\pi_1}\right) = \left(\frac{a_0\pi_2^{w(a)}}{\pi_1}\right)^{w(b)} \left(\frac{b_0\pi_2^{w(b)}}{\pi_1}\right)^{w(a)}.\end{aligned}$$

It follows that $(a,b)_v = (a,b)_w$.

Case 3: $v(a)$ is odd and $v(b)$ is even (or vice versa). Then it follows from the equation (4.1) and the equation (4.2) that

$$(a,b)_v = \left(\frac{b_0}{\pi}\right)^{v(a)} = \left(\frac{b_0}{\pi_1}\right)^{w(a)} \left(\frac{\pi_2}{\pi_1}\right)^{w(b)} = \left(\frac{b_0 \pi_2^{w(b)}}{\pi_1}\right)^{w(a)} = (a,b)_w. \qquad \square$$

Now we can conclude this chapter with the following main result:

Theorem 4.6. *Every quaternion algebra over $F = \mathbb{F}_q(t)$ which is ramified at a place of even degree is a division algebra, but its tensoring with the constant quadratic field extension $\mathbb{F}_{q^2}(t)$ is still a division algebra.*

Proof. Let $F = \mathbb{F}_q(t)$, and B be a quaternion algebra over F. Suppose that B is ramified at v for some place of even degree of F. The result follows from Lemma 4.5 automatically. □

REFERENCES

Acciaro, V., Savin, D., Taous, M., and Zekhnini, A. 2004. On quaternion algebras over some extensions of quadratic number fields [Online]. Available from: https://arxiv.org/abs/2004.01040 [2004,04].

Acciaro, V., Savin, D., Taous, M., and Zekhnini, A. 2019. On quaternion algebras that split over quadratic number fields [Online]. Available from: https://arxiv.org/abs/1906.11076 [2019,06].

Neukirch, J. 1999. Algebraic Number Theory, volume 322 of Grundlehren Math. Wiss. Springer-Verlag, Berlin.

O’Meara, T., O’.1973. Introduction to Quadratic Forms, volume 117 of Grundlehren Math. Wiss. Springer-Verlag, Berlin.

Stichtenoth, H. 2009. Algebraic Function Fields and Codes, volume 254 of Grad. Texts Math. Springer-Verlag, Berlin.

Voight, J. 2021. Quaternion Algebras, volume 288 of Grundlehren Math. Wiss. Springer International Publishing, Berlin.

VITA

Name : Silipong Thongmeepun

Date of Birth : 26 July 1996

Place of Birth : Bangkok Thailand

Education : B.Sc. (Mathematics), Chulalongkorn University, 2017

Scholarship : Graduate School, Chulalongkorn University