Quaternion Algebras

A Thesis Submitted in Fulfillment of the Requirement for the Award of the Degree of

MASTER OF SCIENCE

in Mathematics and Computing

Submitted By

Swati Bansal

(302303016)

Under Supervision of

Dr. Yashpreet Kaur

Assistant Professor

Department of Mathematics

Department of Mathematics

THAPAR INSTITUTE OF ENGINEERING & TECHNOLOGY, PATIALA, PUNJAB

July, 2025

DECLARATION

I, Swati Bansal, hereby declare that the work presented in this thesis entitled ***Quaternion Algebras*** in fulfillment of the requirement for the award of the degree of Master of Science, submitted at Department of Mathematics, Thapar Institute of Engineering and Technology, Patiala, is an authentic record of work carried out under the supervision of Dr.Yashpreet Kaur, Assistant Professor, Department of Mathematics, Thapar Institute of Engineering and Technology from January 2025 to July 2025. The matter presented in this thesis has not been submitted either in part or full to any other university or institute for the award of any other degree.

Date: 31 July, 2025

Swati Bansal

(**Swati Bansal**)
(302303016)

CERTIFICATE

It is certified that the work contained in the thesis titled ***Quaternion Algebras*** by Swati Bansal (302303016) has been carried out under my supervision and that this work has not been submitted elsewhere for any other degree.

Dr.Yashpreet Kaur
(Assistant Professor)
Department of Mathematics
Thapar Institute of Engineering and Technology

Date: 31 July, 2025

To my supervisor, for her guidance;

to my parents, for their endless support;

to Sir William Rowan Hamilton - for carving not only equations but a path for all of us to follow;

and above all,
TO THE ALMIGHTY!

ACKNOWLEDGEMENT

I would like to express my gratitude to everyone who helped with this dissertation.
First, I would like to express my gratitude to God for giving me the perseverance to finish the work within the allotted time.
Next, I would like to express my gratitude to my research supervisor, Dr.Yashpreet Kaur, for her guidance. She always encouraged me, which helped me work better. She always waited patiently while I was trying to prove the results. I could not have imagined having a better mentor for my dissertation.
I also want to thank Dr. Mahesh Kumar Sharma, Head of the Mathematics Department, TIET, Patiala, for providing a research environment.
Above all, I want to express my gratitude to my family for providing me with their most needed support. Their assistance was also crucial in the completion of this work.
I also want to express my gratitude to my friends for their assistance and late-night conversations.

ABSTRACT

In this dissertation, we present an analysis of quaternion algebras. We provide a concise overview of the classical theory of quaternion algebras, and move on to study of quaternion algebras along with an additional differential structure. We discuss the classification of first and second order derivations on quaternion algebras and briefly mention the higher order derivations. Furthermore, we discuss about the splitting of differential quaternion algebras and extend these results to quaternion algebras with higher-order ordinary derivations. In the end, we provide an application of quaternion algebras to Number Theory by proving the Lagrange's four square theorem exploiting Hurwitz factorization within the quaternion ring.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

16 October 1843 was a significant day in the history of mathematics, especially in the field of algebra. On this day, an Irish Mathematician, **Sir William Rowan Hamilton**, came up with the concept of quaternions, which is an extension of complex numbers. He carved the multiplication formulae:

$$i^2 = -1, \quad j^2 = -1, \quad ij = -ji$$

on the stone of Broomebridge in Dublin. Broomebridge is the birthplace of non-commutative algebra, and it has been visited by many mathematicians and, particularly, algebraists. It is even regarded as a pilgrimage by many mathematicians. Hamilton's discovery led to the introduction of new algebraic structures where basic properties of associativity and commutativity were set aside [8]. Quaternions have had many applications not only in mathematics but also in physics.

We first provide a brief overview of the classical theory of quaternion algebras. For more detailed knowledge of quaternions, we refer the readers to see [2]. We provide a few examples of quaternion algebras, namely the algebra of Hamilton quaternions and matrix algebras.

We then move on to the study of quaternion algebras along with an additional differential structure. For this, we first discuss the definitions and properties of derivations and differential structures. In [1], the author classified the derivations on central simple algebras, precisely for matrix algebras. He showed that any derivation on a matrix algebra is the sum of coordinate-wise derivation and inner derivation with respect to a trace-zero matrix. Similarly, in [7], the authors classified the derivations on a quaternion algebra. The authors defined a standard derivation that depends on the generators of quaternion algebra and showed that for every derivation, there exists a pure quaternion v such that the derivation is the sum of a standard derivation and an inner derivation with respect to pure quaternion v. We further classify the second-order derivation of quaternion algebras.

Another crucial aspect of quaternion algebras is their splitting fields. In classical theory, every quaternion algebra over F splits over some quadratic extension of the field F. However, this is not true in the case of quaternion algebras along with a differential structure. In [7], it is shown that the splitting fields of differential quaternion algebras need not be algebraic. The definition of splitting fields of differential quaternion algebras is due to [5]. It is observed in [7] that the splitting of algebras is directly related to isomorphism of differential matrix algebras. The authors in [5] provided a necessary and sufficient condition for isomorphism of differential

matrix algebras. These results are reproduced in this dissertation. We further prove that the splitting of the quaternion algebra naturally extends to the quaternion algebras with ordinary higher derivations.

We end the dissertation by discussing an application of quaternions in Number Theory. The renowned result, Lagrange's four square theorem, holds an important role. The theorem states that every natural number is the sum of at most four integer squares. Though it has been observed that Diophantus of Alexandria was aware of this result in the 1600s, Lagrange was the first to prove it in 1770. We prove the theorem with the help of Hurwitz quaternions, which are the analog of integers for quaternions.

The dissertation is organized into three chapters.

Chapter 2: We introduce quaternion algebras and derivations and discuss the properties of quaternion algebras in the classical and differential sense.

Chapter 3: Several results on the splitting of differential quaternion algebras are discussed.

Chapter 4: We provide an application of quaternions to Number Theory. We prove Lagrange's four square theorem using Hurwitz quaternions.

CHAPTER 2

QUATERNION ALGEBRAS AND DERIVATIONS

We first define the algebras and their properties, which we will be dealing with throughout the upcoming chapters. We will also discuss a few important results associated with these, which will build our foundation for further study.

2.1 Basic Properties

Throughout, we fix F to be a field with char$(F) = 0$. We first begin with the definition and basic properties of quaternion algebras [2].

Definition 2.1.1. *Let α, β be elements in $F^\times$. The **quaternion algebra** $Q := (\alpha, \beta)$ is a four-dimensional F-algebra with the basis $\{1, x, y, xy\}$ such that*

$$x^2 = \alpha, \quad y^2 = \beta, \quad xy = -yx.$$

The basis $\{1, x, y, xy\}$ is known as the quaternion basis of Q. Thus, any element q in (α, β) can be represented as

$$q = a + bx + cy + dxy\,,$$

where $a, b, c, d \in F$.

Example 2.1.2. *For $\alpha = \beta = -1$, the basis elements x, y, xy are called **Hamilton quaternions** and the algebra $(-1, -1)$ is called the algebra of Hamilton quaternions.*

The Hamilton quaternions have a wide range of applications in geometry, physics, and number theory. We will discuss an application of Hamilton quaternions at a later stage.

Definition 2.1.3. *Let $q = a + bx + cy + dxy \in Q$, then the **conjugate** of q, represented by $\overline{q}$, is*

$$\overline{q} = a - bx - cy - dxy\,.$$

*The **norm** of q, denoted by $\|q\|$, is defined as the product of q and its conjugate. That is,*

$$\|q\| = q.\overline{q} = a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2\,.$$

It is clear that if $\|q\| \neq 0$, then inverse of q exists and is given by $\dfrac{\overline{q}}{\|q\|}$.

Definition 2.1.4. *An element $q \in Q$ such that $q^2 \in F$ and $q \notin F$, is called a **pure quaternion**. In other words, $q = a+bx+cy+dxy$ is a pure quaternion iff $a = 0$. The set of pure quaternions is represented as Q^0.*

Remark 2.1.5. *Let $\alpha, \beta \in F^\times \setminus F^{\times 2}$ and $u, v \in F^\times$. Consider a map $\phi : (\alpha, \beta) \to (u^2\alpha, v^2\beta)$ defined as $\phi(x) = ux$, $\phi(y) = vy$, $\phi(a) = a$ for all $a \in F$. Then ϕ is an isomorphism. Hence,*

$$(\alpha, \beta) \simeq (u^2\alpha, v^2\beta).$$

Thus, the isomorphism class of (α, β) depends only on α and β.
Further, consider $\phi : (\alpha, \beta) \to (\beta, \alpha)$ defined as $\phi(x) = \alpha\beta y$, $\phi(y) = \alpha\beta x$, $\phi(a) = a$ for all $a \in F$. Then ϕ is an isomorphism. Hence,

$$(\alpha, \beta) \simeq (\beta, \alpha)$$

Definition 2.1.6. *The set of 2×2 matrices with each entry from a field F forms an algebra over F, called the **matrix algebra** and is denoted by $M_2(F)$.*

The F-algebra $M_2(F)$ of 2×2 matrices is another example of quaternion algebras. Consider a map $\phi : (1, \beta) \to M_2(F)$ defined as

$$\phi(x) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = X \quad \text{(say)},$$
$$\phi(y) = \begin{bmatrix} 0 & \beta \\ 1 & 0 \end{bmatrix} = Y \quad \text{(say)},$$
$$\phi(a) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \quad \text{for all} \quad a \in F.$$

Then ϕ is an isomorphism. Moreover,

$$X^2 = \mathrm{I}, \quad Y^2 = \beta\mathrm{I}, \quad XY = -YX$$

implies $\{I, X, Y, XY\}$ is basis of $M_2(F)$.
We now proceed with the topic of derivations in a purely algebraic sense [10].

Definition 2.1.7. *Let A be a ring (need not be commutative). A map $d : A \to A$ that satisfies*

$$d(a + b) = d(a) + d(b)\,,$$
$$d(ab) = ad(b) + d(a)b\,,$$

*for all $a, b \in A$ is called a **derivation** on A.*
*A ring A together with a derivation d is called **differential ring**, and is denoted by (A, d). If A is a field, then (A, d) is called **differential field**.*

Let (F, δ) be a differential field and A be an algebra over (F, δ), then d is a derivation on F-algebra A if $d(a) = \delta(a)$ for all $a \in F$.

Proposition 2.1.8. *Let (A, d) be a differential ring and A contains unity 1. Then*

(a) $d(1) = 0$.

(b) $d(a^{-1}) = -a^{-1}d(a)a^{-1}$ *for any invertible element* $a \in A$.

Proof. (a). Since

$$1 = 1.1\,.$$

Applying derivation both sides

$$d(1) = d(1.1)\,.$$

On applying Leibniz rule, we get

$$\begin{aligned} d(1) &= 1.d(1) + d(1).1\,, \\ d(1) &= 2.d(1)\,, \\ \text{Thus,}\quad d(1) &= 0\,. \end{aligned}$$

(b). Consider

$$aa^{-1} = 1\,.$$

Applying derivation both sides

$$d(aa^{-1}) = d(1)\,.$$

From part(a), $d(1) = 0$ and applying Leibnitz rule we get,

$$\begin{aligned} d(a)a^{-1} + ad(a^{-1}) &= 0\,, \\ a^{-1}d(a)a^{-1} + d(a^{-1}) &= 0\,, \\ \Rightarrow d(a^{-1}) &= -a^{-1}d(a)a^{-1}\,. \end{aligned}$$

□

2.2 Classification of Derivations

Since $d(1) = 0$, it is clear that $d(\mathbb{Q}) = 0$. That is, the only possible derivation of the field of rationals $\mathbb{Q}$ is the zero map. However, there are many possibilities of a derivation on a ring; we specifically discuss a few here.

Definition 2.2.1. *A derivation is called* ***zero derivation*** *if* $d(a) = 0$ *for all* $a \in A$.
For any element $u \in A$ *,we define a map* $\delta_u : A \to A$ *by*

$$\delta_u(a) = au - ua$$

for all $a \in A$. *This map* δ_u *satisfies the properties of a derivation and is referred to as* ***inner derivation*** *on* A.

In [1], the author provided a classification of derivations on matrix algebras.

Definition 2.2.2. *Let d be derivation on field F. The map $\delta^c : M_2(F) \to M_2(F)$, given by*

$$\delta^c(a_{ij}) = (d(a_{ij}))$$

*defines a derivation on matrix algebra $M_2(F)$, known as the **coordinate wise derivation**.*

Theorem 2.2.3. *[1] Any derivation over matrix algebra $M_2(F)$ can be expressed as*

$$d_P = \delta^c + \partial_P,$$

where δ^c is coordinate-wise derivation and ∂_P is an inner derivation w.r.t trace zero matrix P .

The classification of derivations on a quaternion algebra is due to Kulshrestha and Srinivasan [7]. We mention the result here.

Theorem 2.2.4. *[7] Let δ be a derivation on F and $Q = (\alpha, \beta)$ be a quaternion algebra over F.*

(a) A map $d : Q \to Q$ is a derivation on Q provided there exist elements $a_2, a_3, b_1, b_3 \in F$ such that

$$d(x) = \frac{\delta(\alpha)}{2\alpha}x + a_2 y + a_3 xy\,, \quad d(y) = b_1 x + \frac{\delta(\beta)}{2\beta}y + b_3 xy$$

where $a_2\beta = -b_1\alpha$.

(b) Let d_s be a derivation on Q defined by $d_s(x) = \frac{\delta(\alpha)}{2\alpha}x$ and $d_s(y) = \frac{\delta(\beta)}{2\beta}y$. Then for any derivation d on Q over (F, δ), there exists a unique pure quaternion $v \in Q^0$ such that $d = d_s + \partial_v$, where ∂_v denotes the inner derivation associated with v.

Proof. (a). Let $a_i, b_i \in F$ be such that

$$d(x) = a_0 + a_1 x + a_2 y + a_3 xy\,, \quad d(y) = b_0 + b_1 x + b_2 y + b_3 xy\,.$$

Since $x^2 = \alpha$, $d(x^2) = d(\alpha)$ and on applying the Leibniz rule, we get

$$d(x)x + xd(x) = \delta(\alpha).$$

Putting the value of $d(x)$ here, and using the facts $xy = -yx$, $x^2 = \alpha$, we get.

$$a_0 x + a_1\alpha + a_0 x + a_1\alpha = \delta(\alpha)$$

Since $\delta(\alpha) \in F$ and $x \notin F$, so coefficient of x must be 0. Thus,

$$a_1 = \frac{\delta(\alpha)}{2\alpha} \quad \text{and} \quad a_0 = 0.$$

Similarly from $y^2 = \beta$, we get

$$b_1 = \frac{\delta(\beta)}{2\beta} \quad \text{and} \quad b_0 = 0.$$

Further, on applying derivation on both sides of $xy = -yx$, then putting the value of $d(x)$ and $d(y)$, we get $a_2\beta = -b_1\alpha$.
(b). Let d be derivation on Q over (F, δ) as determined in part(a). Then

$$(d - d_s)(x) = a_2y + a_3xy \quad \text{and} \quad (d - d_s)(y) = b_1x + b_3xy\,. \tag{2.1}$$

Let $v = v_0 + v_1x + v_2y + v_3xy \in Q$ then

$$\partial_v(x) = 2v_2xy + 2v_3\alpha y \quad \text{and} \quad \partial_v(y) = -2v_1xy - 2v_3x\beta\,. \tag{2.2}$$

From Equations (2.1) and (2.2), we get that $d - d_s = \partial_v$ if

$$v_1 = \frac{-b_3}{2}\,, \quad v_2 = \frac{a_3}{2}\,, \quad v_3 = \frac{a_2}{2\alpha} = \frac{-b_1}{2\beta}.$$

For uniqueness of v, we consider $v_0 = 0$. Thus, the unique pure quaternion v is given by

$$v = \frac{-b_3}{2}x + \frac{a_3}{2}y + \frac{a_2}{2\alpha}xy\,.$$

□

2.3 Second Order Derivations

In this section, we introduce ordinary higher derivations, in particular second order derivations. Throughout, we fix F to be a field with derivation δ.

Definition 2.3.1. *[9, 11] Let A be a F-algebra with derivation d. A sequence of additive maps $\{d_n\}$ is known as **higher derivation** on A if*

$$d_m(ab) = \sum_{i=0}^{m} {}^mC_i\; d_i(a)d_{m-i}(b)\,,$$

for all $a, b \in A$, $1 \leq m \leq n$, where d_0 denotes identity on A and $d_1 = d$.
*If $d_n = d^n$ (n times composition of d) then $\{d_n\}$ is called **ordinary higher derivation**.*

Note that for any m, $d_m(a) = \delta^m(a)$ for all $a \in F$. In the next result, we classify second order derivations on quaternion algebras.

Theorem 2.3.2. *Consider a differential field (F, δ). Let $Q = (\alpha, \beta)$ be a quaternion algebra over F.*

(a) A map $d_2 : Q \to Q$ is second order derivation on Q over (F, δ) if there are elements $u_{01}, u_{11}, v_{10}, v_{11}, a_2, a_3, b_1, b_3 \in F$ such that

$$d_2(x) = \left(\frac{\delta^2(\alpha)}{2\alpha} - \left(\frac{\delta(\alpha)}{2\alpha}\right)^2 - \frac{a_2^2\beta}{\alpha} + a_3^2\beta\right)x + u_{01}y + u_{11}xy\,,$$
$$d_2(y) = v_{10}x + \left(\frac{\delta^2(\beta)}{2\beta} - \left(\frac{\delta(\beta)}{2\beta}\right)^2 - \frac{b_1^2\alpha}{\beta} + b_3^2\alpha\right)y + v_{11}xy\,,$$

where $v_{10}\alpha + u_{01}\beta + \delta(\alpha)b_1 + \delta(\beta)a_2 - 2a_3b_3\alpha\beta = 0$.

(b) For every second order derivation d_2 *on* Q*, there are elements* $u, v \in Q^0$ *such that*

$$d_2 = d_s^2 + \partial_u - 2v\partial_v - 2\partial_v(d_s).$$

Proof. (a). Let $u_0, v_0, u_{ij}, v_{ij} \in F$ be such that

$$d_2(x) = u_0 + u_{10}x + u_{01}y + u_{11}xy \quad \text{and} \quad d_2(y) = v_0 + v_{10}x + v_{01}y + v_{11}xy\,.$$

Since $x^2 = \alpha$, using the definition of higher derivation, we get

$$d_0(x)d_2(x) + 2d_1(x)d_1(x) + d_2(x)d_0(x) = \delta^2(\alpha).$$

Substituting $d_2(x)$ and using the fact that $d_0(x) = x$, we get

$$2xu_0 + 2u_{10}\alpha + 2d_1(x)d_1(x) = \delta^2(\alpha)\,. \tag{2.3}$$

From Theorem (2.2.4), we have $d_1(x) = \frac{\delta(\alpha)}{2\alpha}x + a_2y + a_3xy$ and $(d_1(x))^2 = \left(\frac{\delta(\alpha)}{2\alpha}\right)^2\alpha + a_2^2\beta - a_3^2\alpha\beta$. Thus, we rewrite Equation (2.3) as

$$2xu_0 + 2u_{10}\alpha + 2\left(\frac{\delta(\alpha)}{2\alpha}\right)^2\alpha + 2a_2^2\beta - 2a_3^2\alpha\beta = \delta^2(\alpha)$$

Since $x \notin F$, so coefficient of x must be 0. Therefore,

$$u_0 = 0 \quad \text{and} \quad u_{10} = \frac{\delta^2(\alpha)}{2\alpha} - \left(\frac{\delta(\alpha)}{2\alpha}\right)^2 - \frac{a_2^2\beta}{\alpha} + a_3^2\beta\,.$$

Similarly, since $y^2 = \beta$, we get

$$d_2(y)d_0(y) + 2d_1(y)d_1(y) + d_0(y)d_2(y) = \delta^2(\beta)$$

Substituting $d_2(y)$ and using the fact that $d_0(y) = y$, we get

$$2v_0y + 2v_{01}\beta + 2(d_1(y))^2 = \delta^2(\beta) \tag{2.4}$$

From Theorem (2.2.4), we have $d_1(y) = b_1x + \frac{\delta(\beta)}{2\beta}y + b_3xy$ and $(d_1(y))^2 = b_1^2\alpha + \left(\frac{\delta(\beta)}{2\beta}\right)^2\beta - b_3^2\alpha\beta$. Thus, we rewrite Equation (2.4) as

$$2v_0y + 2v_{01}\beta + 2b_1^2\alpha + 2\left(\frac{\delta(\beta)}{2\beta}\right)^2\beta - 2b_3^2\alpha\beta = \delta^2(\beta)\,.$$

Since $y \notin F$, so coefficient of y must be 0. Therefore,

$$v_0 = 0 \quad \text{and} \quad v_{01} = \frac{\delta^2(\beta)}{2\beta} - \left(\frac{\delta(\beta)}{2\beta}\right)^2 - \frac{b_1^2\alpha}{\beta} + b_3^2\alpha\,.$$

Further $xy = -yx$ implies

$$d_2(x)y + xd_2(y) + 2d_1(x)d_1(y) = -d_2(y)x - yd_2(x) - 2d_1(y)d_1(x)\,.$$

Substituting $d_1(x), d_1(y), d_2(x)$ and $d_2(y)$, and on solving we get

$$v_{10}\alpha + u_{01}\beta + b_1\delta(\alpha) + a_2\delta(\beta) - 2a_3b_3\alpha\beta = 0.$$

(b). Since $d_2(x) = \left(\frac{\delta^2(\alpha)}{2\alpha} - \left(\frac{\delta(\alpha)}{2\alpha}\right)^2 - \frac{a_2^2\beta}{\alpha} + a_3^2\beta\right)x + u_{01}y + u_{11}xy$

$$\begin{aligned}
\text{and} \qquad d_s^2(x) &= d_s\left(\frac{\delta(\alpha)}{2\alpha}x\right) \\
&= d_s\left(\frac{\delta(\alpha)}{2\alpha}\right)x + \frac{\delta(\alpha)}{2\alpha}d_s(x) \\
&= \frac{\alpha\delta^2(\alpha)x}{2\alpha^2} - \frac{2\delta(\alpha)d_s(\alpha)x}{4\alpha^2} + \left(\frac{\delta(\alpha)}{2\alpha}\right)\left(\frac{\delta(\alpha)}{2\alpha}\right)x \\
&= \frac{\delta^2(\alpha)x}{2\alpha} - \left(\frac{\delta(\alpha)}{2\alpha}\right)^2 x\,.
\end{aligned}$$

From Theorem (2.2.4), we know $v = \frac{-b_3x}{2} + \frac{a_3y}{2} + \frac{a_2xy}{2\alpha}$. Thus,

$$\begin{aligned}
2v\partial_v(x) &= 2\left(\frac{-b_3x}{2} + \frac{a_3y}{2} + \frac{a_2xy}{2\alpha}\right)(a_2y + a_3xy) \\
&= \left(-a_2b_3xy - a_3b_3\alpha y + a_2a_3\beta - a_3^2\beta x + \frac{a_2^2\beta x}{\alpha} - a_2a_3\beta\right) \\
&= \left(\frac{a_2^2\beta}{\alpha} - a_3^2\beta\right)x - a_3b_3\alpha y - a_2b_3xy.
\end{aligned}$$

$$\text{Further,} \qquad 2\partial_v(d_s(x)) = 2\partial_v\left(\frac{\delta(\alpha)x}{2\alpha}\right) = \frac{\delta(\alpha)}{\alpha}\partial_v(x) = \frac{\delta(\alpha)}{\alpha}(a_2y + a_3xy)\,.$$

Thus,

$$(d_2 - d_s^2 + 2v\partial_v + 2\partial_v(d_s))(x) = \left(u_{01} - a_3b_3\alpha + \frac{\delta(\alpha)a_2}{\alpha}\right)y + \left(u_{11} - a_2b_3 + \frac{\delta(\alpha)a_3}{\alpha}\right)xy\,. \tag{2.5}$$

Using the condition $a_2\beta = -b_1\alpha$ from the Theorem (2.2.4), we can similarly deduce that,

$$(d_2 - d_s^2 + 2v\partial_v + 2\partial_v(d_s))(y) = \left(v_{10} - a_3b_3\beta + \frac{\delta(\alpha)b_1}{\beta}\right)x + \left(v_{11} - b_1a_3 + \frac{\delta(\beta)b_3}{\beta}\right)xy\,. \tag{2.6}$$

Hence, for the pure quaternion $u = u_1x + u_2y + u_3xy$, where

$$u_1 = -\frac{v_{11}}{2} + \frac{a_3b_1}{2} - \frac{\delta(\beta)b_3}{2\beta}, \quad u_2 = \frac{u_{11}}{2} - \frac{a_2b_3}{2} + \frac{a_3\delta(\alpha)}{2\alpha}$$
$$u_3 = \frac{u_{01}}{2\alpha} - \frac{a_3b_3}{2} + \frac{a_2\delta(\alpha)}{2\alpha^2} = \frac{-v_{10}}{2\beta} + \frac{a_3b_3}{2} - \frac{a_2\delta(\beta)}{2\beta\alpha},$$

we have $d_2 - d_s^2 + 2v\partial_v + 2\partial_v(d_s) = \partial_u$. □

Next, we will be discussing a result on higher-order derivations.

Theorem 2.3.3. *Let A be a ring and $\{d_n\}$ be higher derivations on A. Then the matrix representation of higher derivation is given by*

$$D_n = \begin{bmatrix} d_0 & \binom{n}{1}d_1 & \cdots & \binom{n}{n-1}d_{n-1} & d_n \\ 0 & d_0 & \cdots & \binom{n-1}{n-2}d_{n-2} & d_{n-1} \\ 0 & 0 & \cdots & \binom{n-2}{n-3}d_{n-3} & d_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & d_0 & d_1 \\ 0 & 0 & \cdots & 0 & d_0 \end{bmatrix}$$

Proof. Let us consider a truncated polynomial ring:

$$A[t]/(t^{n+1}),$$

which consists of polynomials of the form:

$$v = \sum_{i=0}^{n} v_i t^i, \quad \text{where } v_i \in A.$$

We can express v as a column vector:

$$v = [v_0, v_1t, \cdots, v_nt^n]^T,$$

with respect to the basis $\{1, t, t^2, \ldots, t^n\}$.
Now, we apply a higher derivation δ to each term of v using the Leibniz rule so, we get:

$$\delta(v_it^i) = \sum_{m=0}^{i} \binom{i}{m} d_m(v_i)\, \delta(t^{i-m}).$$

Since t is treated as a fixed formal variable (i.e., $\delta(t) = t$), it follows that:

$$\delta(t^{i-m}) = t^{i-m}.$$

Therefore, the expression becomes:

$$\delta(v_i t^i) = \sum_{m=0}^{i} \binom{i}{m} d_m(v_i) t^{i-m}. \tag{2.7}$$

Now, let us determine the entries of the matrix D_n that represents this higher derivation. The matrix entry $D_n[i, j]$ (row i, column j) corresponds to the coefficient of t^j in the expansion of $\delta(v_i t^i)$.

Case 1: $j = i$

From Equation (2.7), the term contributing to $t^j = t^i$ arises only when $m = 0$:

$$\delta(v_i t^i) = \binom{i}{0} d_0(v_i) t^i.$$

Hence, the coefficient of t^i is $d_0(v_i)$, and:

$$D_n[i, i] = d_0.$$

Case 2: $j > i$

All powers of t in Equation (2.7) are of the form t^{i-m}, and since m ranges from 0 to i, the highest power of t is t^i. Thus, any t^j with $j > i$ cannot appear in the expansion. Therefore,

$$D_n[i, j] = 0 \quad \text{for } j > i.$$

Case 3: $j < i$

We are looking for the coefficient of t^j in the expansion of $\delta(v_i t^i)$. To do this, we solve for m such that

$$i - m = j \quad \Rightarrow \quad m = i - j.$$

This value of m lies within the summation index range $0 \leq m \leq i$, so the term exists in the sum. Therefore, the coefficient of t^j is

$$\binom{i}{i-j} d_{i-j}(v_i)\,.$$

Hence,

$$D_n[i, j] = \binom{i}{i-j} d_{i-j} \quad \text{for } j < i.$$

Thus, we summarize the entries of the matrix D_n as:

$$D_n[i, j] = \begin{cases} 0, & \text{if } j > i, \\ d_0, & \text{if } j = i, \\ \binom{i}{i-j} d_{i-j}, & \text{if } j < i. \end{cases}$$

This completes the derivation of the matrix form of higher derivations using a truncated polynomial ring. □

CHAPTER 3

SPLITTING FIELDS OF QUATERNION ALGEBRAS

Wedderburn's Structure Theorem [2] states that a central simple algebra over a field F, that is, an algebra over F with no two sided ideal and whose center is F, is isomorphic to a matrix algebra over a division algebra. This naturally leads to the question that under what conditions a given algebra is isomorphic to a matrix algebra over some field extension. This question introduced the concept of splitting. The quaternion algebras are one of the example of central simple algebras. In this chapter, we discuss the splitting of quaternion algebras in classical and differential sense.

3.1 Splitting in Classical Sense

Definition 3.1.1. *[2] Let Q be a quaternion algebra over F. Then Q is called **split algebra** if there is an F-isomorphism from Q to $M_2(F)$.*
*If Q is not split over F, but for a field extension E of F we have $Q \otimes E \simeq M_2(E)$ then we say Q **splits** over E and E is the **splitting field** of Q.*

Theorem 3.1.2. *[2] Let Q be a quaternion algebra over F. Then Q splits over an quadratic field extension of F.*

Proof. Let $\alpha, \beta \in F$ such that $Q = (\alpha, \beta)_k$ with basis $\{1, x, y, xy\}$, i.e.

$$x^2 = \alpha, \quad y^2 = \beta, \quad xy = -yx.$$

Consider $L := F(\sqrt{\alpha})$. Since $\mathrm{char}(F) \neq 2$ and $\sqrt{\alpha}$ is not contained in F, then $[L : F] = 2$.
We now consider the scalar extension of Q to L:

$$Q \otimes_F L = (\alpha, \beta)_F \otimes_F L.$$

We claim that $Q \otimes_F L \cong M_2(L)$, i.e., the quaternion algebra splits over L.
To construct such an isomorphism, define a L-algebra homomorphism $\varphi : Q \otimes_k L \to M_2(L)$ by mapping the generators x and y as follows:

$$\varphi(x) = \begin{bmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{bmatrix}, \qquad \varphi(y) = \begin{bmatrix} 0 & \beta \\ 1 & 0 \end{bmatrix}.$$

Then

$$\varphi^2(x) = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} = \alpha I,$$
$$\varphi^2(y) = \begin{bmatrix} 0 & \beta \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} \beta & 0 \\ 0 & \beta \end{bmatrix} = \beta I,$$
$$\varphi(x)\varphi(y) = \begin{bmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{bmatrix} \begin{bmatrix} 0 & \beta \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \beta\sqrt{\alpha} \\ -\sqrt{\alpha} & 0 \end{bmatrix},$$
$$\varphi(y)\varphi(x) = \begin{bmatrix} 0 & \beta \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{bmatrix} = \begin{bmatrix} 0 & -\beta\sqrt{\alpha} \\ \sqrt{\alpha} & 0 \end{bmatrix},$$

so that $\varphi(x)\varphi(y) = -\varphi(y)\varphi(x)$, as required.
Since $Q \otimes_k L$ is a 4-dimensional L-algebra and $M_2(L)$ is also 4-dimensional over L, and φ preserves the defining relations, it follows that φ is an isomorphism.
Therefore, Q splits over $L = F(\sqrt{\alpha})$.

□

3.2 Splitting in Differential Sense

Definition 3.2.1. *[3] The two differential F-algebras (A_1, d_1) and (A_2, d_2) are called **differential isomorphic** if there exists*

$$\psi : A_1 \to A_2$$

such that ψ is an F-isomorphism and

$$\psi \circ d_1 = d_2 \circ \psi.$$

*In this case, ψ is known as **differential isomorphism**.*

Definition 3.2.2. *[5] Let F be a field with derivation d. A differential quaternion algebra (Q, d) over (F, δ) is said to be **split** if it is differential isomorphic to the matrix algebra with coordinate wise derivation $(M_2(F), \delta^c)$.*

Although every quaternion algebra splits over some quadratic extension, this does not necessarily hold for differential quaternion algebras. From [3] and [7], it is evident that a differential quaternion algebra need not be split over quadratic extensions. Furthermore, there exist cases where quaternion algebras with derivation fail to have an algebraic splitting field and thus, transcendental extensions come into picture. We reproduce a few examples here.

Proposition 3.2.3. *[7] Let F be a field with zero derivation δ. Let (Q, d) be differential quaternion algebra such that Q is not split over F and d is non-zero derivation. Then (Q, d) splits over a transcendental extension of (F, δ).*

Proof. Let K be an algebraic extension of F such that (Q, d) differentially splits over (K, δ_K), that is, there is a differential isomorphism $\phi : (Q, d) \to (M_2(K), \delta^c)$. Since K is algebraic

over F. Let $a \in K$ ($\notin F$) be any element. Then the derivation on a, $\delta_K(a)$ is determined by the characteristic polynomial of a over F. Let $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_0$ be characteristic polynomial of a then

$$\delta_K(a) = \frac{\delta(f_{n-1})x^{n-1} + \cdots + \delta(f_0)}{nx^{n-1} + f_{n-1}(n-1)x^{n-2} + \cdots + f_1}\,.$$

Since the derivation δ is identically zero, we have $\delta_K(a) = 0$. Thus, only possible derivation on K is zero derivation. Therefore, the coordinate wise derivation δ^c over $M_2(K)$ is also zero derivation. Hence, $\delta^c \circ \phi$ is zero map. Since the derivation d is non-zero, there is a $\gamma \in Q$ with $d(\gamma) \neq 0$ and $\phi \circ d(\gamma) \neq 0$. This implies $\delta^c \circ \phi \neq \phi \circ d$. Therefore, the splitting field of the quaternion algebra (Q, d) cannot be algebraic over F. □

In [3], authors proved that for any differential quaternion algebra, the transcendence degree of splitting field is at most 3. However, the question of determining exact transcendence degree still remains open.

In [7], the authors provided a method of determining the splitting field of a quaternion algebra with derivation. From Theorem (3.1.2), $Q = (\alpha, \beta)$ splits over $F(\sqrt{\alpha})$. Let $\eta := \sqrt{\alpha}$ then $Q \otimes F(\eta) \simeq M_2(F(\eta))$. Let d_P be the derivation on $M_2(k(\eta))$ for which $(Q \otimes F(\eta), d)$ is differentially isomorphic to $(M_2(F(\eta)), d_P)$. Then the problem remains in finding a field extension L of $(F(\eta))$ for which $(M_2(L), d_P)$ is differentially isomorphic to $(M_2(L), \delta^c)$. Thus, the problem of finding splitting fields for quaternion algebras reduces to find field extensions for which two differential matrix algebras are differential isomorphic.

3.3 Differential Matrix Algebras

Recall that every derivation on $M_2(F)$ is of the form $d_P = \delta^c + \partial_P$, where δ^c denotes coordinate wise derivation and ∂_P denotes inner derivation w.r.t. trace zero matrix P.

Theorem 3.3.1. *[5] The differential matrix algebras $(M_2(F), d_P)$ and $(M_2(F), d_Q)$ are isomorphic iff there exists a matrix $M \in \mathrm{GL}_2(F)$ such that*

$$M^{-1}\delta^c(M) + M^{-1}QM = P\,.$$

Proof. Suppose that $\phi : (M_2(F), d_P) \to (M_2(F), d_Q)$ is a differential F-algebra isomorphism. Hence, ϕ is an inner automorphism and there exists $M \in GL_2(F)$ such that $\phi(X) = MXM^{-1}$. Since M is determined up to a multiplication by a non-zero scalar, without loss of generality we may assume that $\det(M) = 1$. Now,

$$\begin{aligned}\phi(d_P(X)) &= \phi(\delta^c(X) + PX - XP)\\ &= M(\delta^c(X) + PX - XP)M^{-1}\\ &= M\delta^c(X)M^{-1} + MPXM^{-1} - MXPM^{-1}\,.\end{aligned}$$

$$\begin{aligned} d_Q(\phi(X)) &= d_Q(MXM^{-1}) \\ &= \delta^c(MXM^{-1}) + Q(MXM^{-1}) - (MXM^{-1})Q \\ &= \delta^c(M)XM^{-1} + M\delta^c(X)M^{-1} + MX\delta^c(M^{-1}) \\ &+ Q(MXM^{-1}) - (MXM^{-1})Q\,. \end{aligned}$$

Note that

$$\begin{aligned} MM^{-1} &= I \\ \text{Taking derivative both sides,} \qquad \delta^c(MM^{-1}) &= 0 \\ M'M^{-1} + M\delta^c(M^{-1}) &= 0 \\ \delta^c(M^{-1}) &= -M^{-1}\delta^c(M)M^{-1}\,. \end{aligned}$$

Thus,

$$\begin{aligned} d_Q(\phi(X)) = \delta^c(M)XM^{-1} + M\delta^c(X)M^{-1} - MXM^{-1}\delta^c(M)M^{-1} \\ + Q(MXM^{-1}) - (MXM^{-1})Q\,. \end{aligned}$$

Since $\phi(d_P(X)) = d_Q(\phi(X)$, we get

$$\begin{aligned} MPXM^{-1} - MXPM^{-1} = \delta^c(M)XM^{-1} - MXM^{-1}\delta^c(M)M^{-1} \\ + QMXM^{-1} - MXM^{-1}Q\,. \end{aligned}$$

Apply left multiplication by M^{-1} and right multiplication by M, we get

$$\begin{aligned} PX - XP &= M^{-1}\delta^c(M)X - XM^{-1}\delta^c(M) + M^{-1}QMX - XM^{-1}QM\,. \\ \text{Thus,} \qquad (P - M^{-1}\delta^c(M) - M^{-1}QM)X - X(P - M^{-1}\delta^c(M) - M^{-1}QM) &= 0\,. \end{aligned}$$

Since $P - M^{-1}\delta^c(M) - M^{-1}QM$ commutes with X, it is in the center of $M_2(F)$. Thus, it is a scalar matrix aI_2, where $a \in F$. That is,

$$P - M^{-1}\delta^c(M) - M^{-1}QM = aI_2\,.$$

Taking trace on both sides, we get

$$\begin{aligned} \mathrm{tr}(P - M^{-1}\delta^c(M) - M^{-1}QM) &= \mathrm{tr}(aI_2) \\ \mathrm{tr}(P) - \mathrm{tr}(M^{-1}\delta^c(M)) - \mathrm{tr}(M^{-1}QM) &= 2a\,. \end{aligned}$$

Also $\mathrm{tr}(MQM^{-1}) = \mathrm{tr}(Q) = 0$ and $\mathrm{tr}(P) = 0$. Therefore,

$$\mathrm{tr}(M^{-1}\delta^c(M)) = -2a\,.$$

Now, $\mathrm{tr}(M^{-1}\delta^c(M))$ is the logarithmic derivative of $\det(M)$, i.e.,

$$\mathrm{tr}(M^{-1}\delta^c(M)) = \frac{d(\det(M))}{\det(M)}\,.$$

Since $\det(M) = 1$, $2a = 0$. Thus,

$$\begin{aligned} P - M^{-1}\delta^c(M) - M^{-1}QM &= 0 \\ M^{-1}\delta^c(M) + M^{-1}QM &= P\,. \end{aligned}$$

Conversely, let $M \in GL_2(F)$ such that

$$M^{-1}\delta^c(M) + M^{-1}QM = P\,.$$

Consider $\Phi : (M_2(F), d_P) \to (M_2(F), d_Q)$ defined as $\Phi(X) = MXM^{-1}$. Clearly it is an isomorphism. Furthermore,

$$\begin{aligned} \Phi(d_P(X)) &= \Phi(\delta^c(X) + PX - XP) \\ &= M\delta^c(X)M^{-1} + MPXM^{-1} - MXPM^{-1} \\ &= M\delta^c(X)M^{-1} + M(M^{-1}\delta^c(M) + M^{-1}QM)XM^{-1} \\ &- MX(M^{-1}\delta^c(M) + M^{-1}QM)M^{-1} \\ &= M\delta^c(X)M^{-1} + \delta^c(M)XM^{-1} + QMXM^{-1} - MXM^{-1}\delta^c(M)M^{-1} \\ &- MXM^{-1}Q \\ &= \delta^c(MXM^{-1}) + \partial_Q(MXM^{-1}) \\ &= d_Q(MXM^{-1}) = d_Q(\Phi(X))\,. \end{aligned}$$

Hence, Φ is a differential isomorphism. □

With the help of differential matrix algebras, one can determine the splitting field for a quaternion algebra.

3.4 Splitting of Algebras with Higher Derivations

We now show that differential isomorphism at first-order extends naturally to ordinary higher-order derivations.(E, δ_E) be a differential field extension of (F, δ) We say a quaternion algebra with higher derivation (Q, d_n) splits over (E, δ_E) if $(Q \otimes E, d_n)$ is differentially isomorphic to $(M_2(E), (\delta^c)^n)$.

Theorem 3.4.1. *Let (F, δ) be a differential field and (Q, d) be quaternion algebra over (F, δ). Let (E, δ_E) be a splitting field of (Q, d). Then the quaternion algebra with ordinary higher derivation (Q, d^n) also splits over E.*

Proof. Let $\phi : (Q, d) \to (M_2(E), \delta^c)$ such that

$$\phi \circ d = \delta^c \circ \phi.$$

For $u \in Q$, consider

$$\begin{aligned}
\phi \circ d^n(u) &= \phi(d^n(u)) \\
&= \phi(d(d^{n-1}(u))) \\
&= \delta^c(\phi(d^{n-1}(u))) \quad \text{(as } \phi \circ d = \delta^c \circ \phi) \\
&= \delta^c(\phi(d(d^{n-2}(u))) \\
&= (\delta^c)^2(\phi(d^{n-2}(u)) \\
&\vdots \\
&= (\delta^c)^n \circ \phi(u)\,.
\end{aligned}$$

Thus, $(Q \otimes E, d_n)$ is differentially isomorphic to $(M_2(E), (\delta^c)^n)$, where E is splitting field of (Q, d^n). □

However, the question of splitting of a general quaternion algebra with higher derivation still remains unanswered.

CHAPTER 4

AN APPLICATION TO NUMBER THEORY: LAGRANGE'S FOUR SQUARE THEOREM

In this chapter, we establish Lagrange's Four Square Theorem through the framework of quaternion algebra, demonstrating a profound connection between number theory and the algebraic structure of quaternions.

4.1 Hurwitz Integers

Definition 4.1.1. *[4] The **Hurwitz integers** are a set of quaternions consisting of all integer linear combinations of the elements*

$$\frac{1+u+v+uv}{2},\ u,\ v,\ uv\,,$$

where $u^2 = v^2 = -1$ and $vu = -uv$. This set is denoted by $\mathbb{Z}[h, u, v, uv]$, where

$$h = \frac{1+u+v+uv}{2}.$$

It contains the subring $\mathbb{Z}[u, v, uv] = \{a + bu + cv + duv \mid a, b, c, d \in \mathbb{Z}\}$.

Definition 4.1.2. *[4] An element $p \in \mathbb{Z}[h, u, v, uv]$ is said to be **Hurwitz prime** if its only divisors are the units of $\mathbb{Z}[h, u, v, uv]$ and their multiples by p.*

We provide a key lemma of the real Hurwitz prime that helps to establish a divisibility criterion in the context of Hurwitz prime.

Lemma 4.1.3. *[4] Let p be an irreducible real Hurwitz prime such that p divides mn for Hurwitz integers m and n. Then either p divides m or p divides n.*

Proof. Let $p \nmid m$.
Since $\gcd(p, m) = 1$, there exist Hurwitz integers μ, ν such that

$$1 = \mu p + \nu m\,. \tag{4.1}$$

Post-multiply by n both sides in Equation (4.1)

$$n = \mu pn + \nu mn \tag{4.2}$$

Since p is left and right divisor of whichever number it divides, a real number commutes with quaternions. Therefore,

$$p \mid \mu pn \quad , \quad p \mid \nu mn \, .$$

Thus,

$$p \mid \mu pn + \nu mn \, .$$

Using Equation 4.2, we get that $p \mid n$.

□

With this divisibility criterion in hand, we now turn our attention to another important lemma which lays the foundation for factorization in the quaternion ring.

Lemma 4.1.4. *[4] Let $p = 2m + 1$ be an odd prime. Then there are integers f, g such that*

$$1 + f^2 + g^2 \equiv 0 \pmod{p} \, .$$

Proof. Let $a, b \in \{0, 1, \ldots, m\}$ such that

$$\begin{aligned} & a^2 \equiv b^2 \pmod{p} \\ & a^2 - b^2 \equiv \overline{0} \\ & (a - b)(a + b) \equiv \overline{0} \\ & \text{either} \quad a + b \equiv \overline{0} \quad \text{or} \quad a - b \equiv \overline{0}. \end{aligned}$$

If $a + b \equiv \overline{0}$ then $p \mid a + b$. But since $0 < a, b < m$, we have $0 < a + b < 2m < p$. Thus, $p \nmid a + b$.
Let $a - b \equiv \overline{0}$. Without loss of generality, assume $a > b$. Then $a - b < m < p$ and hence, $p \nmid a - b$.
Thus, there are $m+1$ distinct numbers from 0 to m and it gives rise to $m+1$ incongruent value of $f^2 \pmod{p}$.
Similarly, there are $m + 1$ incongruent values of $g^2 \pmod{p}$ and hence of, $-1 - g^2 \pmod{p}$ where $g = 0, 1, \ldots, m$.
Therefore, we get $2m + 2$ incongruent values. However, we have only $2m + 1$ incongruent values. Thus, by pigeon hole principle, for some f and g, we have

$$\begin{aligned} & f^2 \equiv -1 - g^2 \pmod{p} \\ \text{i.e.,} \quad & 1 + f^2 + g^2 \equiv 0 \pmod{p} \\ \text{Thus,} \quad & p \mid 1 + f^2 + g^2 \, . \end{aligned}$$

□

4.2 Four Square Theorem

With all the necessary tools in place, we are now prepared to present a conditional proof of the Four Square Theorem.

Theorem 4.2.1 (Conditional four square theorem)**.** *[4] Every real prime p that is not a Hurwitz prime is a sum of four integer squares.*

Proof. Assume p factors non-trivially into Hurwitz integers

$$p = \mu\nu\,, \tag{4.3}$$

where $\mu, \nu \in \mathbb{Z}[h, u, v, uv]$. Let

$$\mu = a + bu + cv + duv.$$

Then

$$\begin{aligned}
\overline{p} &= \overline{\mu\nu} \\
\overline{p} &= \overline{(a + bu + cv + duv)\nu} \\
\overline{p} &= \overline{\nu}(a - bu - cv - duv)\,.
\end{aligned}$$

Since p is ordinary prime, $\overline{p} = p$. Thus,

$$p = \overline{\nu}(a - bu - cv - duv) \tag{4.4}$$

Multiplying Equation (4.3) and Equation (4.4), we get

$$\begin{aligned}
p^2 &= (a + bu + cv + duv)\nu\overline{\nu}(a - bu - cv - duv) \\
&= (a + bu + cv + duv)(a - bu - cv - duv)\nu\overline{\nu} \\
&= (a^2 + b^2 + c^2 + d^2)|\nu|^2\,,
\end{aligned}$$

where both $a^2 + b^2 + c^2 + d^2, |\nu|^2 \in \mathbb{Z}$ and are greater than 1.
Since prime factorization is unique and $p^2 = p.p$, we have

$$\begin{aligned}
p &= a^2 + b^2 + c^2 + d^2 \\
&= (a + bu + cv + duv)(a - bu - cv - duv)\,.
\end{aligned}$$

If $\mu = a + bu + cv + duv \in \mathbb{Z}[u, v, uv]$ then it is clear that p is sum of at most four integer squares.
Now, let $\mu = a + bu + cv + duv$ has half-integer coefficients.
Consider

$$\omega = \frac{\pm 1 \pm u \pm v \pm uv}{2},$$

which has norm 1, that is, $\omega\overline{\omega} = 1$. By choosing appropriate signs in ω, μ can be rewritten as

$$\mu = \omega + a_1 + b_1 u + c_1 v + d_1 uv,$$

where $a_1, b_1, c_1, d_1 \in \mathbb{Z}$ are even integers. Therefore,

$$\begin{aligned}
p &= (a + bu + cv + duv)(a - bu - cv - duv) \\
&= (\omega + a_1 + b_1u + c_1v + d_1uv)(\overline{\omega} + a_1 - b_1u - c_1v - d_1uv) \\
&= (\omega + a_1 + b_1u + c_1v + d_1uv) \cdot 1 \cdot (\overline{\omega} + a_1 - b_1u - c_1v - d_1uv) \\
&= (\omega + a_1 + b_1u + c_1v + d_1uv) \cdot \overline{\omega}\omega \cdot (\overline{\omega} + a_1 - b_1u - c_1v - d_1uv) \\
&= ((\omega + a_1 + b_1u + c_1v + d_1uv) \cdot \overline{\omega})(\omega \cdot (\overline{\omega} + a_1 - b_1u - c_1v - d_1uv)) \,.
\end{aligned}$$

On solving it further, we get

$$\begin{aligned}
p = 1 &+ \omega a_1 - \omega b_1u - \omega c_1v + a_1\overline{\omega} + (a_1)^2 - \omega d_1uv + b_1u\overline{\omega} + (b_1)^2 \\
&+ a_1v\overline{\omega} + (a_1)^2 + d_1uv\overline{\omega} + (d_1)^2.
\end{aligned}$$

Let

$$\begin{aligned}
\omega &= \omega_0 + \omega_1u + \omega_2v + \omega_3uv \\
\overline{\omega} &= \omega_0 - \omega_1u - \omega_2v - \omega_3uv \,.
\end{aligned}$$

Substituting these values above and on solving, we get

$$p = 1 + 2a_1w_0 + 2b_1w_1 + 2c_1w_2 + 2d_1w_3 + (a_1)^2 + (b_1)^2 + (c_1)^2 + (d_1)^2. \tag{4.5}$$

We know $\omega\overline{\omega} = 1$. Also,

$$\begin{aligned}
\omega\overline{\omega} &= (\omega_0 + \omega_1x + \omega_2y + \omega_3xy)(\omega_0 - \omega_1x - \omega_2y - \omega_3xy) \\
\omega\overline{\omega} &= \omega_0^2 + \omega_1^2 + \omega_2^2 + \omega_3^2 \\
\text{Thus,} \qquad 1 &= \omega_0^2 + \omega_1^2 + \omega_2^2 + \omega_3^2 \,.
\end{aligned}$$

Putting this value of 1 in Equation (4.5), we get

$$\begin{aligned}
p &= \omega_0^2 + \omega_1^2 + \omega_2^2 + \omega_3^2 + 2a_1w_0 + 2b_1w_1 + 2c_1w_2 + 2d_1w_3 + (a_1)^2 + (b_1)^2 + (c_1)^2 + (d_1)^2 \\
&= (\omega_0^2 + a_1^2 + 2a_1w_0) + (\omega_1^2 + b_1^2 + 2b_1w_1) + (\omega_2^2 + c_1^2 + 2c_1w_2) + (\omega_3^2 + d_1^2 + 2d_1w_3) \\
&= (\omega_0 + a_1)^2 + (\omega_1 + b_1)^2 + (\omega_2 + c_1)^2 + (\omega_3 + d_1)^2 \,.
\end{aligned}$$

Hence, p is sum of four integer squares. □

Having established the required lemmas and the conditional theorem, we now bring them together to complete the proof of Lagrange's Four Square Theorem.

Theorem 4.2.2 (Lagrange's Four Square Theorem)**.** *[4] Every natural number is the sum of four integer squares.*

Proof. We know

$$\begin{aligned}
1 &= 1^2 + 0^2 + 0^2 + 0^2 \\
2 &= 0^2 + 0^2 + 1^2 + 1^2
\end{aligned}$$

Since these are the trivial cases, we focus only on odd primes.

Let p be an odd prime, then according to Lemma (4.1.4), there exist $f, g \in \mathbb{Z}$ such that $p \mid 1 + f^2 + g^2$. On factorizing, we get

$$1 + f^2 + g^2 = (1 + fu + gv)(1 - fu - gv).$$

Let p be a Hurwitz prime, then according to Lemma (4.1.3), it must divide either $1 + fu + gv$ or $1 - fu - gv$. But none of the case is possible as

$$\frac{1}{p} + \frac{fu}{p} + \frac{gv}{p} \quad \text{and} \quad \frac{1}{p} - \frac{fu}{p} - \frac{gv}{p}$$

are not Hurwitz integers. Thus, p is not a Hurwitz prime.
Hence, using Theorem (4.2.1), we conclude that p is the sum of four integer squares. □

A natural question arises that if we can express numbers as sums of four squares individually, what can we say about their product? The answer to this question is given with the help of norm.

Theorem 4.2.3 (Four square Identity)**.** *[4] Let m, n be two numbers that are expressible as the sum of four integer squares, then the product mn is also a sum of four integer squares.*

Proof. Let m, n be two numbers such that

$$\begin{aligned} m &= m_0^2 + m_1^2 + m_2^2 + m_3^2 = ||m_0 + m_1 u + m_2 v + m_3 uv||^2 = ||h_1||^2 \quad \text{(say)} \\ n &= n_0^2 + n_1^2 + n_2^2 + n_3^2 = ||n_0 + n_1 u + n_2 v + n_3 uv||^2 = ||h_2||^2 \quad \text{(say)}\,, \end{aligned}$$

where m_0, m_1, m_2, m_3 and n_0, n_1, n_2, n_3 are integers. Using the multiplicative property of norms, we get

$$\begin{aligned} mn &= ||h_1||^2 ||h_2||^2 = ||h_1 h_2||^2 \\ &= ||(m_0 + m_1 u + m_2 v + m_3 uv)(n_0 + n_1 u + n_2 v + n_3 uv)||^2 \\ &= (m_0 n_0 - m_1 n_1 - m_2 n_2 - m_3 n_3)^2 + (m_0 n_1 + m_1 n_0 + m_2 n_3 - m_3 n_2)^2 \\ &\quad + (m_0 n_2 + m_2 n_0 - m_1 n_3 + m_3 n_1)^2 + (m_0 n_3 + m_3 n_0 + m_1 n_2 - m_2 n_1)^2\,. \end{aligned}$$

Since m_i, n_i are integers, it follows that the product mn is also expressible as the sum of four integer integer squares.

□

With this identity the picture is completed. We conclude that every prime is a sum of four squares and product of primes also satisfies the same. Hence, every positive integer can be written as the sum of four integer squares.

BIBLIOGRAPHY

[1] Amitsur, S. A. (1957). *Derivations in simple rings*. Proceedings of the London Mathematical Society, 3(1), 87-112.

[2] Gille, P., & Szamuely, T. (2017). *Central simple algebras and Galois cohomology* (Vol. 165). Cambridge University Press.

[3] Gupta, P., Kaur, Y., & Singh, A. (2023). *Splitting of differential quaternion algebras*. Journal of Algebra, 633, 43-55.

[4] Hong, J. & Ng, R. (2008). *Quaternions and the four square theorem*. Summer VIGRE REU.

[5] Juan, L., & Magid, A. (2008). *Differential central simple algebras and Picard Vessiot representations*. Proceedings of the American Mathematical Society, 136(6), 1911-1918.

[6] Kolchin, E. R. (1973). *Differential Algebra and Algebraic Groups*. Academic Press.

[7] Kulshrestha, A., & Srinivasan, V. R. (2022). *Quaternion algebras with derivations*. Journal of Pure and Applied Algebra, 226(2), 106805.

[8] Lewis, D. (2006). *Quaternion Algebras and the Algebraic Legacy of Hamilton's Quaternions*. Irish Mathematical Society Bulletin, 57.

[9] Mirzavaziri M,. (2010). *Characterization of higher derivations on algebras*. Communications in Algebra. 38:3, 981-987.

[10] Ritt, J. F. (1950). *Differential Algebra*. American Mathematical Society Colloquium Publications, Vol. 33.

[11] Roy, A., Sridharan, R. (1968). *Higher derivations and central simple algebras*. Nagoya Math. J. 32, 21-30.

[12] Voight, J. (2021). *Quaternion Algebras*. Graduate Texts in Mathematics, Springer Cham.