CAUCHY –Jurnal Matematika Murni dan Aplikasi
Volume 8(2) (2023), Pages 142-156
p-ISSN: 2086-0382; e-ISSN: 2477-3344

Existence of Split Property in Quaternion Algebra Over Composite of Quadratic Fields

Muhammad Faldiyan*, Ema Carnia, Asep K. Supriatna

Department of Mathematics, Faculty of Mathematics and Natural Sciences, Padjadjaran University, Indonesia

Email: faldiyan18001@mail.unpad.ac.id

ABSTRACT

Quaternions are extensions of complex numbers that are four-dimensional objects. Quaternion consists of one real number and three complex numbers, commonly denoted by the standard vectors i, j, and k. Quaternion algebra over the field is an algebra in which the multiplication between standard vectors is non-commutative and the multiplication of standard vector with itself is a member of the field. The field considered in this study is the quadratic field and its extensions are biquadratic and composite. There have been many studies done to show the existence of split properties in quaternion algebras over quadratic fields. The purpose of this research is to prove a theorem about the existence of split properties on three field structures, namely quaternion algebras over quadratic fields, biquadratic fields, and composite of n quadratic fields. We propose two theorems about biquadratic fields and composite of n quadratic fields refer to theorems about the properties of the split on quadratic fields. The result of this research is a theorem proof of three theorems with different field structures that shows the different conditions of the three field structures. The conclusion is that the split property on quaternion algebras over fields exists if certain conditions can be met.

Keywords: quaternion algebra; quadratic field; biquadratic field; composite; split;

INTRODUCTION

Quaternions are a useful tool for comprehending a variety of physics and kinematic concepts. Quaternion are frequently employed to address optimization issues involving predicting rigid body transformations, particularly in the disciplines of computer vision, computer graphics, and animation [1]. Quaternions are extensions of complex numbers. Complex numbers denoted by $\mathbb{C}$ are a subset of quaternion numbers with the notation $\mathbb{H}$. Quaternion numbers are also called hypercomplex numbers because they are a generalization of the complex number system. Quaternion numbers are applied in various applications such as color image filtering, segmentation, and 3-dimensional impulse response filter design [2]. Quaternion numbers have four components, namely one real number and three imaginary numbers that have the form: $q = a + bi + cj + dk$, where a, b, c, and d are real numbers and i, j, and k are imaginary numbers [3].

Submitted: July 14, 2023 Reviewed: August 15, 2023 Accepted: September 12, 2023
DOI: http://dx.doi.org/10.18860/ca.v8i2.22881

Quaternion algebra is a generalization of vector algebra. Quaternion algebra was first presented by Hamilton more than a hundred years ago but has only been practically applied recently, especially in the industrial field. A four-dimensional vector can be used to symbolize quaternion algebra [4]. A vector space V over a field F with a bilinear mapping makes up a quaternion algebra. An algebra A is said to be a division algebra if for every $a, b \in A$, with $a \cdot b = 0$ implies $a = 0$ or $b = 0$. In other words, there are no zero divisors in division algebra. Any field $\mathbb{F}$ can be used to generalize quaternion algebra in place of the real number field $\mathbb{F}$. A quaternion algebraic system is a non-commutative algebraic system defined the multiplication of its imaginary vectors, i.e., $i^2 = a, j^2 = b, k^2 = -ab$, and $ij = -ji = k$, where $a, b \in \mathbb{F}$ [5].

A quadratic field is a two-degree field over a rational number $\mathbb{Q}$. A quadratic field has the form $a + b\sqrt{d}$, where $a, b \in \mathbb{Q}$ and d is a square-free integer. An integer that has no repeating elements in its prime decomposition is said to be square-free. The symbol for a quadratic field is $\mathbb{Q}(\sqrt{d})$. A biquadratic field is a quadratic field that contains two different square-free integer elements. Suppose $\mathbb{Q}$ is a rational number and m, p are distinct square-free integers; the field formed by $\sqrt{m}$ and $\sqrt{p}$ to $\mathbb{Q}$ is denoted by $\mathbb{Q}(\sqrt{m}, \sqrt{p})$. The notation $\mathbb{Q}(\sqrt{m}, \sqrt{p})$ can be defined as a quadratic field over rational numbers $\mathbb{Q}$ if $\mathbb{Q}(\sqrt{m}, \sqrt{p}) = \mathbb{Q}(\sqrt{m} + \sqrt{p})$ and $\sqrt{m} + \sqrt{p}$ has unique minimal polynomial $x^4 - 2(m+p)x^2 + (m+p)^2$. The term "integer of the field $\mathbb{Q}(\sqrt{m}, \sqrt{p})$" refers to any element in $\mathbb{Q}(\sqrt{m}, \sqrt{p})$ that has a monic equation of degree ≥ 1 with rational integral coefficients [6]. A composite number is a natural number greater than one and is the inverse of a prime number. The composite of n quadratic fields is the quadratic field of number n and is denoted by $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ [7].

A lot of research has been done to study quaternion algebras over a field. Research [8] discusses the characteristics of quaternion numbers. This research studies the properties of quaternion numbers in general but has not studied them further in the field. Research [9] discusses the split quaternion algebra over a certain field. This research further studies the split properties of quaternion algebras over certain fields. The second research [10] discusses the class of quaternion algebra in the field. This research studies the special properties of division algebra in quaternion algebra. The characteristics of quaternion algebras over quadratic fields are covered in research [11]. This study explores the properties of quaternion algebras over quadratic fields as well as the prerequisites and requirements for using quaternion algebras over quadratic fields as division algebras. Research [7] discusses the development of previous research, namely the characteristics of the quaternion algebra over the composite of n quadratic fields. This research reveals the characteristics of quaternion algebra and its application to Fibonacci numbers. Based on this research, a study is formed that discusses the characteristics of the quaternion algebra over the composite of n quadratic fields in a division algebra.

From these studies, we found a research gap that needs to be developed further. We will develop a theorem on split existence for a wider field, namely quaternion algebra over the composite of n quadratic fields. The purpose of this research is to prove the theorem about split existence on three algebraic structures over the field, namely a quadratic field, a biquadratic field, and a composite of n quadratic field. Since split properties on quaternion algebras over quadratic fields have already been theorized, this study will focus on split properties on quaternion algebras over biquadratic fields and composites of n quadratic fields, two areas of unexplored research. A theorem on the split properties of quaternion algebras over quadratic fields was described by Acciaro and

Savin in 2018 [12]. Two theorems regarding the split properties on biquadratic fields and a composite of n quadratic fields that are related to theorems about the split properties on quadratic fields are proposed. The results of this study will show the existence of split properties that always exist in quaternion algebras under certain conditions. In addition, the results of this study show the different conditions required for quaternion algebras to be split. Larger fields tend to require more conditions for the split existence theorem on quaternion algebras to hold. This research can be useful for the advancement of algebraic science studies, especially in the field of algebra over the field.

METHODS

This section describes the definitions, theorems, lemmas, and propositions used in this research to answer the main research problem, namely answering the characteristics through theorem proving of the quaternion algebra over the composite of n quadratic fields that have split properties. The method used in answering this main problem is a literature study that focuses on the material of quaternion algebra over the composite of n quadratic fields and its properties. First, we will prove the theorem about the sufficient condition of quaternion algebra over quadratic fields having split properties. Then, the research will be extended by proving the theorem about the sufficient condition that the quaternion algebra over the biquadratic fields has split properties. Finally, the research will be extended again by proving the theorem about the sufficient condition of quaternion algebra over the composite of n quadratic fields that also has the split property. The following is a definition that becomes the theoretical basis for answering research problems about quaternion algebra.

Definition 1. (See [13]) **(Quaternion)**

Quaternions are an extension of complex numbers. Quaternions have number elements consisting of one real number and three imaginary numbers. Quaternions mathematically, can be written as follows:

$$\mathbb{H} = \{a + bi + cj + dk;\ \forall a, b, c, d \in \mathbb{R}\};$$

where the following multiplication rule conditions apply:

1. $i^2 = j^2 = k^2 = -1$;
2. $ij = k,\ jk = i,\ ki = j, ik = -j,\ kj = -i,\ ji = -k$;
3. Each $a \in \mathbb{R}$ is commutative with i, j, and k.

Definition 2. (See [14]) **(Quaternion from complex number)**

Suppose $A = a + bi$ and $C = c + di$ are two complex numbers. Construct the number $q = A + Cj$ and define $k = ij$, so as to produce a number in a four-dimensional vector space denoted by $\mathbb{H}$.

$$q = a + bi + cj + dk \in \mathbb{H};$$

where $\{a, b, c, d\} \in \mathbb{R}$, and $\{i, j, k\}$ are three imaginary numbers defined as follows

$$i^2 = j^2 = k^2 = -1;$$

As a result, the following equation may be deduced:

$$ij = -ji = k,\ \ jk = -kj = i,\ \ ki = -ik = j.$$

Definition 3. (See [15]) **(Algebra over field)**

Assume that K is a field and that A is a vector space over K with an addition operation in binary form from $A \times A$ to A. Vector space A is an algebra over a field K if it satisfies the following axioms:

$$(\lambda a)b = a(\lambda b) = \lambda(ab), \;\; \forall \lambda \in K \; and \; \forall a, b \in A.$$

Definition 4. (See [16]) **(Quaternion Algebra)**

A quaternion algebra is an algebra A over a field F if there exist $i, j \in A$ such that $1, i, ij$ is a basis for algebra A and holds:

$$i^2 = a, \qquad j^2 = b, \qquad k^2 = -ab, and \; ji = -ij = k;$$

For every $a, b \in F$.

Definition 5. (See [17]) **(Conjugate)**

Consider $q = a + bi + cj + dk$ to be a quaternion number. The conjugate of quaternion can be defined as follows:

$$q^* = (a + bi + cj + dk)^* = a - bi - cj - dk.$$

Definition 6. (See [17]) **(Norm)**

Consider $q = a + bi + cj + dk$ to be a quaternion number. The norm of quaternion can be defined as follows:

$$N(q) = qq^* = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2.$$

Definition 7. (See [17]) **(Inverse)**

Consider $q = a + bi + cj + dk$ to be a quaternion number. The multiplication inverse of quaternion denoted by q^{-1} may be defined as follows:

$$q^{-1} = \frac{q^*}{N(q)};$$

and the multiplication of the inverse holds $qq^{-1} = 1 = q^{-1}q$. The inverse operation contains the properties of the inverse of multiplication, namely: $(q^{-1})^{-1} = q$ and $(pq)^{-1} = q^{-1}p^{-1}$, where p is a quaternion number.

Definition 8. (See [18]) **(Field Extension)**

Suppose E and F are fields. If and only if F is a subfield of E, then field E is an extension of F. Field E is a vector space over a field F denoted by E/F and its dimension is denoted by $[E: F]$.

Definition 9. (See [19]) **(Quadratic Field)**

The field of rational numbers $\mathbb{Q}$ of degree two extends into the quadratic field. The quadratic field has the form $a + b\sqrt{d}$, where d is a square-free integer represented by $\mathbb{Q}(\sqrt{d})$ in the form of a quadratic field. If $d > 0$, the field is referred to as a real quadratic field. If $d < 0$, it is referred to as an imaginary quadratic field.

Definition 10. (See [20]) **(Square-free)**

A number is said to be squarefree if its prime decomposition does not contain repeated factors. Therefore, all prime numbers are squarefree.

Definition 11. (See [11]) **(Division Algebra)**

Associative algebra A is a kind of algebra. A over a field F is a division algebra if and only if it has a multiplication identity element of $1 \neq 0$ and a left and right multiplication inverse for each non-zero element in A. If A is a finite-dimensional algebra, it is a division algebra if and only if it has no zero divisors.

Definition 12. (See [16]) **(Division Ring)**

Division algebra is an algebra over the division ring K (every nonzero element has an inverse).

Definition 13. (See [6]) **(Biquadratic Field)**

Let $\mathbb{Q}$ indicate the rational number field. $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ denotes the field produced by $\sqrt{m}$ and $\sqrt{n}$ to $\mathbb{Q}$ if $\sqrt{m}$ and $\sqrt{n}$ are separate square-free integers. $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n})$, and $\sqrt{m} + \sqrt{n}$ has a unique minimum polynomial $x^4 - 2(m+n)x^2 + (m+n)^2$, implying that $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is a biquadratic field over $\mathbb{Q}$. Members of the field $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ have the following formula: $a_0 + a_1\sqrt{m} + a_2\sqrt{n} + a_3\sqrt{mn}$, where $a_0, a_1, a_2, a_3 \in \mathbb{Q}$.

Definition 14. (See [21]) **(Discriminant)**

Suppose K to be a field of degree n with complex insertions $\sigma_1, \dots, \sigma_n$ and let $\alpha_1, \dots, \alpha_n \in K$. The discriminant $\Delta(\alpha_1, \dots, \alpha_n)$ of these n-tuples is defined as the square of the determinant of an $n \times n$ matrix.

$$\left(\sigma_i(\alpha_j)\right)$$

Definition 15. (See [22]) **(Legendre Symbol)**

Assume that p is an odd prime integer and that $a \in \mathbb{Z}$. This is how the legendre symbol $\left(\frac{a}{p}\right)$ is defined:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & if\ x^2 \equiv a\ (mod\ p)\ has\ solution \\ 0, & if\ p|a \\ -1, & else \end{cases}$$

If p is prime and $a \in \mathbb{Z}$ satisfies $\left(\frac{a}{p}\right) = 1$ then a is a quadratic residue, while if $\left(\frac{a}{p}\right) = -1$ [11]then a is a non-quadratic residue.

Definition 16. (See [11]) **(Quadratic Residue Symbol)**

Suppose $\mathcal{P}$ is a prime ideal of the ring O_K. If α is quadratic in K, then its quadratic residue symbol is

$$\left(\frac{\alpha}{\mathcal{P}}\right) = \begin{cases} 1, & if\ \mathcal{P}\ split\ in\ K(\sqrt{\alpha}) \\ -1, & if\ \mathcal{P}\ inert\ in\ K(\sqrt{\alpha}) \\ 0, & if\ \mathcal{P}\ ramified\ in\ K(\sqrt{\alpha}) \end{cases}$$

Definition 17. (See [23]) **(Hilbert Equation)**

For the field $\mathbb{F}$ and $a, b \in \mathbb{F}^* = \mathbb{F}\backslash\{0\}$. We state that

$$aX^2 + bY^2 = Z^2$$

is a Hilbert Equation and the solution $(x, y, z) \in \mathbb{F}^3$ is trivial if and only if $x = y = z = 0$, otherwise it is nontrivial.

Definition 18. (See [23]) **(Hilbert Symbol)**

Suppose F is a field and $R \subseteq F$ is a subring. Define the mapping that resolves a quadratic diagonal equation in three variables with coefficients in F and is nontrivial R solvable:

$$h_{R,F}(\cdot,\cdot) : F^* \times F^* \to \{-1,1\}$$
$$(a,b) \longmapsto \begin{cases} 1, & if\ \exists(x,y,z) \in R^3\backslash\{0\} : ax^2 + by^2 = z^2 \\ & -1,\ otherwise \end{cases}$$

If $R = F$, then write $h_F(\cdot,\cdot) := h_{F,F}(\cdot,\cdot)$.

Proposition 19. (See [24]) **(Discriminant of quadratic field)**

Let Δ_K be the discriminant of a square-free integer d in the quadratic field $K = \mathbb{Q}(\sqrt{d})$. The following conditions hold:

1. If $d = 2{,}3\ (mod\ 4)$ then $\Delta_K = 4d$;
2. If $d = 1\ (mod\ 4)$ then $\Delta_K = d$.

Theorem 20. (See [6]) **(Discriminant of biquadratic field)**

Assume that $l = (m, n)$ is a Hilbert Symbol, $m = lm_1$, and that $n = ln_1$, and that $(m_1, n_1) = 1$. $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ has the following discriminant:

1. $l^2 m_1^2 n_1^2$, if $(m, n) = (1,1)(mod\ 4)$;
2. $16 l^2 m_1^2 n_1^2$, if $(m, n) = (1,2)\ or\ (3,3)(mod\ 4)$;
3. $64 l^2 m_1^2 n_1^2$, if $(m, n) = (2,3)(mod\ 4)$.

Theorem 21. (See [25]) **(Split Properties)**

Suppose K is an extension quadratic field of $\mathbb{F}$ and $H_{\mathbb{F}}$ is a quaternion algebra over $\mathbb{F}$. If no ramified prime of $\mathbb{F}$ in $H_{\mathbb{F}}$ is split in K, then there is an insertion of K into $H_{\mathbb{F}}$.

Theorem 22. (See [12]) **(Prime decomposition in the quadratic field)**

Suppose $d \neq 0{,}1$ is an integer with no squares (square-free integer). Suppose Δ_K is the discriminant of K and $\mathcal{O}_K$ is the integer ring of the quadratic field $K = \mathbb{Q}(\sqrt{d})$. Assume that p is an odd prime number. Next, we have:

a. If and only if $p | \Delta_K$, p is ramified in $\mathcal{O}_K$. Therefore, $p\mathcal{O}_K = (p, \sqrt{d})^2$;

b. If $\left(\frac{\Delta_K}{p}\right) = 1$, then and only if p is split in $\mathcal{O}_K$. If P_1 and P_2 are different prime ideals in $\mathcal{O}_K$, then $p\mathcal{O}_K = P_1 \cdot P_2$.

c. If $\left(\frac{\Delta_K}{p}\right) = -1$, then and only if, p is inert in $\mathcal{O}_K$;

d. If and only if $d \equiv 2\ (mod\ 4)$ or $d \equiv 3\ (mod\ 4)$ are true, the prime number 2 is ramified in $\mathcal{O}_K$. $2\mathcal{O}_K = (2, \sqrt{d})^2$ in the first instance and $2\mathcal{O}_K = (2{,}1 + \sqrt{d})^2$ in the second;

e. If and only if $d \equiv 1\ (mod\ 8)$ exists, the prime 2 is split in $\mathcal{O}_K$. Given that $P_1 = \left(2, \frac{1+\sqrt{d}}{2}\right)$, P_2 is a separate prime ideal in $\mathcal{O}_K$, and $2\mathcal{O}_K = P_1 \cdot P_2$;

f. If and only if $d \equiv 5\ (mod\ 8)$, the prime 2 is inert in $\mathcal{O}_K$.

Theorem 23. (See [12]) **(Split properties of prime numbers in a biquadratic field)**

Suppose d_1 and d_2 are two distinct square-free integers not equal to one, and suppose $d_3 = \frac{lcm(d_1,d_2)}{\gcd(d_1,d_2)}$. Suppose $\mathcal{O}_K$ is the integer ring of the quadratic field K and $\mathcal{O}_{K_i}$ is the integer ring of the quadratic subfield $K_i = \mathbb{Q}(\sqrt{d_i})$, where $i = 1,2,3$. Let's assume p is a prime number. When p is split in every $\mathcal{O}_{K_i}$, where $i = 1,2,3$, then and only then p is split in $\mathcal{O}_K$.

Theorem 24. (See [12]) **(Split for composite field)**

Suppose p is a prime of $\mathbb{Q}$ that is split in every field $F_1, F_2, \dots, F_n$. Then p is split in the composite field $F_1F_2 \dots F_n$.

Lemma 25. (See [12]) **(Discriminant of prime number)**

Suppose p and q are prime numbers, and $H_{\mathbb{Q}(\sqrt{d})}(p,q)$ is quaternion algebra with discriminant Δ_H.

a. If $p \equiv q \equiv 3 \ (mod\ 4)$ and $\left(\frac{q}{p}\right) \neq 1$, then $\Delta_H = 2p$;

b. If $q = 2$ and $p \equiv 3 \ (mod\ 8)$, then $\Delta_H = pq = 2p$;

c. If $p \equiv 1 \ (mod\ 4)$ or $q \equiv 1 \ (mod\ 4)$ with $p \neq q$ and $\left(\frac{p}{q}\right) = -1$, then $\Delta_H = pq$.

RESULTS AND DISCUSSION

A development of complex algebra known as quaternion algebra may be created in a number of areas of mathematics, including algebra, analysis, geometry, and arithmetic. In the field of algebra, quaternion algebra can be developed based on algebraic properties, namely split, inert, and ramified. Split quaternion algebras tend to be easier to decompose into simpler algebras. Therefore, a sufficient condition is needed so that a quaternion algebra is said to be a split algebra. First, what will be reviewed in this result and discussion is the existence of split properties on quaternion algebras over quadratic fields have been proved by Acciaro and Savin [12]. Then proceed to prove the split properties for a wider field, namely the biquadratic field and the composite of n quadratic fields. The theorem on the split properties of the quaternion algebra over the quadratic field is shown as follows:

Theorem 26 (See [12])

Suppose $d \neq 0,1$ are square-free integers, $d \not\equiv 1 \ (mod\ 8)$, and p, q are prime integers, with $q \geq 3, p \neq q$. Let Δ_K is the discriminant of K and $\mathcal{O}_K$ is the ring of integers for the quadratic field $K = \mathbb{Q}(\sqrt{d})$. Then:

a. If $p \geq 3$ and the legendre symbol $\left(\frac{\Delta_K}{p}\right) \neq 1$, $\left(\frac{\Delta_K}{q}\right) \neq 1$, then $H_{\mathbb{Q}(\sqrt{d})}(p,q)$ is split;

b. If $p = 2$ and legendre symbol $\left(\frac{\Delta_K}{q}\right) \neq 1$, then $H_{\mathbb{Q}(\sqrt{d})}(2,q)$ is split;

Proof:

a. According to Proposition 19, $\Delta_K = d$ (if $d \equiv 1 \ (mod\ 4)$) or $\Delta_K = 4d$ (if $d \equiv 2,3 \ (mod\ 4)$). Because $\left(\frac{\Delta_K}{p}\right) \neq 1$ and $\left(\frac{\Delta_K}{q}\right) \neq 1$, by Definition 15, $\left(\frac{\Delta_K}{p}\right) = -1$ or 0 and $\left(\frac{\Delta_K}{q}\right) = -1$ or 0. According to Definition 16, p and q are both ramified in $\mathcal{O}_K$ or inert in $\mathcal{O}_K$, therefore p and q are not split in the quadratic field K.

Suppose Δ is the discriminant of the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(p,q)$.
A prime positive integer p' is known to be ramified in $H_{\mathbb{Q}(\sqrt{d})}(p,q)$ if $p'|2\Delta$, indicating that $p'|2pq$.
Since $d \not\equiv 1\ (mod\ 8)$ and the decomposition of 2 in ring $\mathcal{O}_K$ yield that 2 is not split in K. Applying Theorem 21, there is no ramified prime such that $H_{\mathbb{Q}(\sqrt{d})}(p,q)$ is split. Based on the above proof, it can be concluded that the quaternion algebra is split under this condition.

b. According to Proposition 19, $\Delta_K = d$ (if $d \equiv 1\ (mod\ 4)$) or $\Delta_K = 4d$ (if $d \equiv 2,3\ (mod\ 4)$). Because $\left(\frac{\Delta_K}{q}\right) \neq 1$ then by Definition 15, $\left(\frac{\Delta_K}{q}\right) = -1$ or 0. According to Definition 16, q is ramified or inert in $\mathcal{O}_K$ so q is not split in the quadratic field K.
Suppose Δ is the discriminant of the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(2,q)$ and a prime positive integer p' is known to be ramified in $H_{\mathbb{Q}(\sqrt{d})}(2,q)$ if $p'|2\Delta$, indicating that $p'|2q$.
Since $d \not\equiv 1\ (mod\ 8)$ and the decomposition of 2 in ring $\mathcal{O}_K$ yield that 2 is not split in K. Applying Theorem 21, no prime is ramified, so $H_{\mathbb{Q}(\sqrt{d})}(2,q)$ is split. Based on the above proof, it can be concluded that the quaternion algebra is split with this condition.

So, the sufficient condition for quaternion algebra to be split is when $p \geq 3, \left(\frac{\Delta_K}{p}\right) \neq 1, \left(\frac{\Delta_K}{q}\right) \neq 1$ or when $p = 2$ and $\left(\frac{\Delta_K}{q}\right) \neq 1$.

Furthermore, a new theorem is given that will be proved about the split properties of quaternion algebras over biquadratic fields. The biquadratic field is wider and more complicated than the quadratic field, so it requires some additional conditions on this theorem compared to the previous theorem. The theorem on the split property of a biquadratic field is a research novelty formed from Theorem 26. The establishment of this theorem is done to guarantee the existence of sufficient conditions that make a quaternion algebra over biquadratic field is split. The following is the content and proof of the theorem on the existence of split properties on quaternion algebras over biquadratic fields.

Theorem 27

Suppose $d_1, d_2 \neq 0,1$ are square-free integers, where $d_1, d_2 \not\equiv 1\ (mod\ 8)$ and $d_3 = \frac{lcm(d_1,d_2)}{gcd(d_1,d_2)}$. Suppose p, q are prime integers, with $q \geq 3, p \neq q$. Suppose $\mathcal{O}_K$ is the ring of integers for the biquadratic field $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ and that $\mathcal{O}_{K_i}$ is the ring of integers for the quadratic subfield $K_i = \mathbb{Q}(\sqrt{d_i})$, where $i = 1,2,3$, with discriminant Δ_{K_i}. Then:

a. If $p \geq 3$ and legendre symbol $\left(\frac{\Delta_{K_i}}{p}\right) \neq 1$, $\left(\frac{\Delta_{K_i}}{q}\right) \neq 1$, then $H_{\mathbb{Q}(\sqrt{d_1},\sqrt{d_2})}(p,q)$ is split in $\mathcal{O}_{K_i}$;

b. If $p = 2$ and legendre symbol $\left(\frac{\Delta_{K_i}}{q}\right) \neq 1$, then $H_{\mathbb{Q}(\sqrt{d_1},\sqrt{d_2})}(2,q)$ is split in $\mathcal{O}_{K_i}$.

Proof:

a. According to Theorem 23, a prime p' split in $\mathcal{O}_K$ only if p' split in $\mathcal{O}_{K_i}$, where $i = 1,2$, and 3. We will prove that both prime p and q split in $\mathcal{O}_{K_1}, \mathcal{O}_{K_2}$, and $\mathcal{O}_{K_3}$.

First case for $\mathcal{O}_{K_1}$:
By Proposition 19, it is known that the discriminant of Δ_{K_1} is d_1 (if $d_1 \equiv 1\ (mod\ 4)$) or $4d_1$ (if $d_1 \equiv 2,3\ (mod\ 4)$). Since in the theorem it is known that $\left(\frac{\Delta_{K_1}}{p}\right) \neq 1$ and $\left(\frac{\Delta_{K_2}}{q}\right) \neq 1$, then by Definition 15, the quadratic residue symbol $\left(\frac{\Delta_{K_1}}{p}\right) = -1$ or 0 as well as the quadratic residue symbol $\left(\frac{\Delta_{K_1}}{q}\right) = -1$ or 0. Based on Definition 16, the primes p and q are ramified or inert in $\mathcal{O}_{K_1}$ so they are not split in the quadratic subfield K_1.
In Theorem 22, it is known that p is ramified in $\mathcal{O}_{K_1}$ if and only if $p|\Delta_{K_1}$. By Lemma 25 points (a) and (c), the discriminant of the quadratic subfield K_1 is $\Delta_{K_1}= 2p$ or pq. Since $p|2p$ or $p|pq, p$ is ramified in $\mathcal{O}_{K_1}$. It is also true for q which is also ramified in $\mathcal{O}_{K_1}$.
Since $d_1 \not\equiv 1\ (mod\ 8)$ and the decomposition of primes p, q imply that p, q are not split in K_1. By Theorem 21, it is clear that there are no ramified primes such that $H_{\mathbb{Q}(\sqrt{d_1})}(p, q)$ is split.

Second case for $\mathcal{O}_{K_2}$:
The proof is the same as in the first case (for $\mathcal{O}_{K_1}$) by replacing K_1 with K_2 and d_1 with d_2. This happens because the criteria for the reviewed square-free integers d_1 and d_2 are the same.

Third case for $\mathcal{O}_{K_3}$:
By Proposition 19, it is known that the discriminant of Δ_{K_1} is d_1 (if $d_1 \equiv 1\ (mod\ 4)$) or $4d_1$ (if $d_1 \equiv 2,3\ (mod\ 4)$) and the discriminant of Δ_{K_2} is d_2 (if $d_2 \equiv 1\ (mod\ 4)$) or $4d_2$ (if $d_2 \equiv 2,3\ (mod\ 4)$). Lemma 25 explains that the discriminant of a quadratic field is $2p$ (if $p \equiv q \equiv 3\ (mod\ 4)$ and $\left(\frac{q}{p}\right) \neq 1$) or pq (if $p \equiv 1\ (mod\ 4)$ or $q \equiv 1\ (mod\ 4)$ with $p \neq q$ and $\left(\frac{p}{q}\right) = -1$). From Proposition 19 and Lemma 25, the relation of the discriminant of the quadratic field is $d_1 = 2p$ or $d_1 = pq$ or $4d_1 = 2p$ or $4d_1 = pq$, and the same is true for d_2. Since d_1, d_2 are square-free integers, the relationship $d_1 = \frac{2p}{4}$ or $d_1 = \frac{pq}{4}$ does not hold, and neither does d_2. It follows that $d_1 \equiv 1\ (mod\ 4)$ and $d_2 \equiv 1\ (mod\ 4)$.
It is known in the theorem that $d_3 = \frac{lcm(d_1,d_2)}{gcd(d_1,d_2)}$.

1. Consider the cases $d_1 = 2p$ and $d_2 = 2p'$ so that
$$d_3 = \frac{lcm(d_1, d_2)}{gcd(d_1, d_2)} = \frac{lcm(2p, 2p')}{gcd(2p, 2p')} = \frac{2pp'}{2} = pp'$$
2. Consider the cases $d_1 = 2p$ and $d_2 = p'q'$ so that
$$d_3 = \frac{lcm(d_1, d_2)}{gcd(d_1, d_2)} = \frac{lcm(2p, p'q')}{gcd(2p, p'q')} = \frac{2pp'q'}{1} = 2pp'q'$$
3. Consider the cases $d_1 = pq$ and $d_2 = 2p'$ so that
$$d_3 = \frac{lcm(d_1, d_2)}{gcd(d_1, d_2)} = \frac{lcm(pq, 2p')}{gcd(pq, 2p')} = \frac{pq2p'}{1} = 2pp'q$$
4. Consider the cases $d_1 = pq$ and $d_2 = p'q'$ so that
$$d_3 = \frac{lcm(d_1, d_2)}{gcd(d_1, d_2)} = \frac{lcm(pq, p'q')}{gcd(pq, p'q')} = \frac{pqp'q'}{1} = pp'qq'$$

From these four cases, it can be concluded that d_3 is the product of two or more primes once, so that the prime decomposition is not repeated. Therefore, d_3 is also a square-free integer.
In the theorem, it was mentioned that $\left(\frac{\Delta_{K_3}}{p}\right) \neq 1$ and $\left(\frac{\Delta_{K_3}}{q}\right) \neq 1$, so by Definition 15, the quadratic residue symbol $\left(\frac{\Delta_{K_3}}{p}\right) = -1$ or 0 as well as the quadratic residue symbol $\left(\frac{\Delta_{K_3}}{q}\right) = -1$ or 0. By Definition 16, the primes p and q are ramified or inert in $\mathcal{O}_{K_3}$ so they are not split in the quadratic subfield of K_3.
In Theorem 22, it is known that p is ramified in $\mathcal{O}_{K_3}$ if and only if $p|\Delta_{K_3}$. The discriminant of the quadratic subfield of K_3 is pp', $2pp'q'$, or $pp'qq'$. Since $p|pp'$ or $p|2pp'q'$ or $p|pp'qq'$ so p is ramified in $\mathcal{O}_{K_3}$. The same holds for q which is also ramified in $\mathcal{O}_{K_3}$. Since $d_1, d_2 \not\equiv 1\ (mod\ 8)$ then $d_3 \not\equiv 1\ (mod\ 8)$.
Since $d_3 \not\equiv 1\ (mod\ 8)$ and the decomposition of primes p and q imply that p and q are not split in K_3. Based on Theorem 21, it is clear that there are no ramified primes such that $H_{\mathbb{Q}(\sqrt{d_3})}(p, q)$ is split.

From these three cases, it can be concluded that the primes p and q split in the ring of integers $\mathcal{O}_{K_1}, \mathcal{O}_{K_2}$, and $\mathcal{O}_{K_3}$. Since primes p and q split in every $\mathcal{O}_{K_i}$ $(i = 1,2,3)$, then by Theorem 23 it can be said that primes p and q split in $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. So, it is proved that quaternion algebra over biquadratic field is split.

b. According to Theorem 23, a prime p' split in $\mathcal{O}_K$ only if p' split in $\mathcal{O}_{K_i}$, where $i = 1,2$, and 3. We will prove that prime q is split in $\mathcal{O}_{K_1}, \mathcal{O}_{K_2}$, and $\mathcal{O}_{K_3}$.

First case for $\mathcal{O}_{K_1}$:
By Proposition 15, it is known that the discriminant of Δ_{K_1} is d_1 (if $d_1 \equiv 1\ (mod\ 4)$) or $4d_1$ (if $d_1 \equiv 2,3\ (mod\ 4)$). Since in the theorem it is known that $\left(\frac{\Delta_{K_1}}{q}\right) \neq 1$, then by Definition 17, the quadratic residue symbol $\left(\frac{\Delta_{K_1}}{q}\right) = -1$ or 0. Based on definition 18, the prime q is ramified or inert in $\mathcal{O}_{K_1}$ so it is not split in the quadratic subfield K_1.
In Theorem 22, it is known that q is ramified in $\mathcal{O}_{K_1}$ if and only if $q|\Delta_{K_1}$. By Lemma 24 point (b), the discriminant of the quadratic subfield K_1 is $\Delta_{K_1} = 2q$. Since $q|2q$, then q is ramified in $\mathcal{O}_{K_1}$.
Since $d_1 \not\equiv 1\ (mod\ 8)$ and the decomposition of prime q imply that q is not split in K_1. By Theorem 21, it is clear that there are no ramified primes such that $H_{\mathbb{Q}(\sqrt{d_1})}(2, q)$ is split.

Second case for $\mathcal{O}_{K_2}$:
The proof is the same as in the first case (for $\mathcal{O}_{K_1}$) by replacing K_1 with K_2 and d_1 with d_2. This happens because the criteria for the reviewed square-free integers d_1 and d_2 are the same.

Third case for $\mathcal{O}_{K_3}$:
By Proposition 15, it is known that the discriminant of Δ_{K_1} is d_1 (if $d_1 \equiv 1\ (mod\ 4)$)

or $4d_1$ (if $d_1 \equiv 2,3\ (mod\ 4)$) and the discriminant of Δ_{K_2} is d_2 (if $d_2 \equiv 1\ (mod\ 4)$) or $4d_2$ (if $d_2 \equiv 2,3\ (mod\ 4)$). Lemma 19 explains that the discriminant of a quadratic field is $2q$ (if $p = 2$ and $q \equiv 3\ (mod\ 8)$). From proposition 15 and Lemma 19, the relation of the discriminant of the quadratic field is $d_1 = 2q$ or $4d_1 = 2q$ and $d_2 = 2q$ or $4d_2 = 2q$. Since d_1, d_2 are square-free integers, the relationship $d_1 = \frac{2q}{4}$ and $d_2 = \frac{2q}{4}$ does not hold. It follows that $d_1 \equiv 1\ (mod\ 4)$ and $d_2 \equiv 1\ (mod\ 4)$.

It is known in the theorem that $d_3 = \frac{lcm(d_1,d_2)}{gcd(d_1,d_2)}$ so that

$$d_3 = \frac{lcm(d_1,d_2)}{gcd(d_1,d_2)} = \frac{lcm(2q,2q')}{gcd(2q,2q')} = \frac{2qq'}{2} = qq'$$

Discriminant d_3 is the product of two distinct primes, such that its prime decomposition does not repeat. Since the prime decomposition is non-repeating, d_3 is a square-free integer.

In the theorem, it was mentioned that $\left(\frac{\Delta_{K_3}}{q}\right) \neq 1$, so by definition 17, the quadratic residue symbol $\left(\frac{\Delta_{K_3}}{q}\right) = -1$ or 0. By definition 18, the prime q is ramified or inert in $\mathcal{O}_{K_3}$ so it is not split in the quadratic subfield of K_3.

In theorem 22, it is known that q is ramified in $\mathcal{O}_{K_3}$ if and only if $q|\Delta_{K_3}$. The discriminant of the quadratic subfield of K_3 is qq'. Since $q|qq'$, so that q is ramified in $\mathcal{O}_{K_3}$. Since $d_1, d_2 \not\equiv 1\ (mod\ 8)$ then $d_3 \not\equiv 1\ (mod\ 8)$.

Since $d_3 \not\equiv 1\ (mod\ 8)$ and the decomposition of prime q imply that q is not split in K_3. Based on theorem 21, it is clear that there are no ramified primes such that $H_{\mathbb{Q}(\sqrt{d_3})}(2,q)$ is split.

From these three cases, it can be concluded that the primes 2 and q split in the ring of integers $\mathcal{O}_{K_1}, \mathcal{O}_{K_2}$, and $\mathcal{O}_{K_3}$. Since primes 2 and q split in every $\mathcal{O}_{K_i}$ ($i = 1,2,3$), then by Theorem 23 it can be said that primes 2 and q split in $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. So, it is proved that quaternion algebra over biquadratic field is split.

Quaternion algebras over quadratic fields and biquadratic fields can be split under certain conditions, as has been demonstrated in the previous theorem. After that, it will be demonstrated that splitting the quaternion algebra over the composite of n quadratic fields is adequate. The goal of this theorem's proof to establish the prerequisites for splitting the quaternion algebra over the composite of n quadratic fields. This theorem is a new statement that builds on Theorem 26 by studying the split properties of composites fields. The following is the content of the theorem and its proof of existence of split on quaternion algebra over the composite of n quadratic fields.

Theorem 28

Suppose $d_1, d_2, \dots, d_n$ be separate square-free numbers that are not equal to zero or one, where $d_1, d_2, \dots, d_n \not\equiv 1\ (mod\ 8)$. Suppose p, q are distinct prime integers, with $q \geq 3, p \neq q$. Prime p and q does not divide d_i, for $i = 1,2, \dots, n$. Suppose $\mathcal{O}_K$ is the ring of integers for the composite of n quadratic field $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ and $\mathcal{O}_{K_i}$ is the ring of integers for the quadratic subfield $K_i = \mathbb{Q}(\sqrt{d_i})$, where $i = 1,2, \dots, n$, with discriminant Δ_{K_i}. Then:

a. If $p \geq 3$ and legendre symbol $\left(\frac{\Delta_{K_i}}{p}\right) \neq 1$, $\left(\frac{\Delta_{K_i}}{q}\right) \neq 1$, then $H_{\mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\dots,\sqrt{d_n})}(p,q)$ is split in $\mathcal{O}_{K_i}$;

b. If $p = 2$ and legendre symbol $\left(\frac{\Delta_{K_i}}{q}\right) \neq 1$, then $H_{\mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\dots,\sqrt{d_n})}(2, q)$ is split in $\mathcal{O}_{K_i}$.

Proof:

a. To respond to this theorem's proof, use mathematical induction.

1. <u>Establish the validity of the statement for $n = 1$</u>

   Suppose $n = 1$, in which case the quadratic field's form is
   $$K = \mathbb{Q}(\sqrt{d_1})$$
   The form of the field is a quadratic field. In Theorem 26, it has been proved that the split property of quaternion algebra over quadratic fields holds under these conditions.

   So, the theorem is proved true for $n = 1$.

2. <u>Assume that the theorem is valid or accurate for $n = k$</u>

   Suppose $n = k$, in which case the composite of quadratic field's form is
   $$K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_k})$$
   This theorem is assumed to be true for $n = k$.

3. <u>Prove that the theorem also holds true for $n = k + 1$</u>

   Suppose $n = k + 1$, in which case the composite of quadratic field's form is
   $$K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_k}, \sqrt{d_{k+1}})$$
   Based on Definition 13, the form of the composite of quadratic field is obtained:
   $$\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_k}, \sqrt{d_{k+1}}) = \mathbb{Q}\left((\sqrt{d_1} + \sqrt{d_2} + \dots + \sqrt{d_k}), \sqrt{d_{k+1}}\right)$$
   Then, from the composite of the quadratic field, the form of the biquadratic field is obtained. According to Theorem 23, prime p' splits in $\mathcal{O}_K$ only if prime p' splits in $\mathcal{O}_{K_i}$.

   Suppose $\mathcal{O}_L$ is the ring of integers for the biquadratic field $L = \mathbb{Q}(\sqrt{d}, \sqrt{d_{k+1}})$, where $\sqrt{d} = \sqrt{d_1} + \sqrt{d_2} + \dots + \sqrt{d_k}$, $\mathcal{O}_{L_1}$ is the ring for integers of the quadratic subfield $L_1 = \mathbb{Q}(\sqrt{d})$, and $\mathcal{O}_{L_2}$ is the ring of integers for the quadratic subfield $L_2 = \mathbb{Q}(\sqrt{d_{k+1}})$. We will prove that primes p and q are split in quadratic subfield L_1 and L_2.

   First case for $\mathcal{O}_{L_1}$:

   We know that the quadratic subfield of L_1 is
   $$L_1 = \mathbb{Q}(\sqrt{d})$$
   $$L_1 = \mathbb{Q}(\sqrt{d_1} + \sqrt{d_2} + \dots + \sqrt{d_k})$$
   Based on Definition 13, we know that the quadratic subfield is
   $$L_1 = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_k})$$
   Mathematical induction assumes that it is true that primes p and q are split in $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_k})$ so it is proved that primes p and q are split in the quadratic subfield L_1.

   Second case for $\mathcal{O}_{L_2}$:

   We know that the quadratic subfield of L_2 is
   $$L_2 = \mathbb{Q}(\sqrt{d_{k+1}})$$
   Where $k \in \mathbb{Z}$. Then $k + 1$ is also an integer $(k + 1) \in \mathbb{Z}$.

Since $k+1$ is an integer and $\mathbb{Q}(\sqrt{d_{k+1}})$ is a quadratic subfield, applying Theorem 26, we find that primes p and q are split in $\mathcal{O}_{L_2=\mathbb{Q}(\sqrt{d_{k+1}})}(p,q)$.

Since it is proven that primes p and q are split in L_1 and L_2, Theorem 23 implies that primes p and q are also split in L, where $L=\mathbb{Q}(\sqrt{d},\sqrt{d_{k+1}})=\mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\dots,\sqrt{d_k},\sqrt{d_{k+1}})$.
So, the theorem proves true for $n=k+1$.

So, mathematical induction proves that the split property theorem holds for composite of n quadratic fields.

b. The proof is the same as that of part (a). It is only necessary to substitute $p=2$ and apply Theorems 26 and 27 of part (b) to answer the proof of Theorem 28.

So, the theorem proves that quaternion algebra over composite of n quadratic field is split to be true under these conditions.

Theorems 26, 27, and 28 have differences in the fields, namely the quadratic field in Theorem 26, the biquadratic field in Theorem 27, and the composite of n quadratic fields in Theorem 28. It can be seen that the wider field considered in these theorems to be split, the more additional conditions are required. Theorem 26 applies according to the conditions mentioned in the theorem. Theorem 27 adds additional conditions from theorem 26, namely $d_3=\frac{lcm(d_1,d_2)}{gcd(d_1,d_2)}$ and a quadratic subfield. Theorem 28 adds an additional condition from Theorem 26 and 27, namely, that primes p and q do not divide the square-free integer d_i. Thus, the split property will apply more easily to quadratic fields than to biquadratic fields and composite of n quadratic fields.

CONCLUSIONS

The conclusion of this research is that the split property of quaternion algebra will apply more easily to smaller fields. The larger the field under review, the more condition will be needed so that the quaternion algebra over the field is split. The Legendre symbol of the field determinant of prime numbers generally must not equal one in order for a quaternion algebra to be split.

ACKNOWLEDGEMENTS

The author would like to thank to the Indonesian Ministry of Education, Culture, Research, and Technology for partially funding this research under Master Thesis Research Project in 2022 entitled “Aljabar Quaternion Atas Komposit Lapangan Kuadratik”, grant number 1318/UN6.3.1/PT.00/2022 and thank to the Directorate of Research and Community Service (DRPM) of Padjadjaran University for partially funding this research under Academic Leadership Grant (ALG) in 2023, grant number 1549/UN6.3.1/PT.00/2023.

REFERENCES

[1] M. Jafari, "On The Properties Of Quasi-Quaternion Algebra," *Communications*, vol. 63, no. 1, pp. 1–10, Jan. 2014.

[2] H.-T. Chang, C. J. Kuo, N.-W. Lo, and W.-Z. Lv, "DNA Sequence Representation and Comparison Based on Quaternion Number System," in *International Journal of Advanced Computer Science and Applications (IJACSA)*, 2012. [Online]. Available: www.ijacsa.thesai.org

[3] P. Bas, N. Le Bihan, and J.-M. Chassery, "Color Image Watermarking Using Quaternion Fourier Transform," in *International Conference on Acoustics, Speech, and Signal Processing*, May 2003. [Online]. Available: https://hal.archives-ouvertes.fr/hal-00166555

[4] K. W. Spring, "Euler Parameters And The Use Of Quaternion Algebra In The Manipulation Of Finite Rotations: A Review," vol. 21, no. 5, pp. 365–373, 1986, doi: https://doi.org/10.1016/0094-114X(86)90084-4.

[5] E. Malekian, A. Zakerolhosseini, and A. Mashatan, "QTRU: A Lattice Attack Resistant Version of NTRU PKCS Based on Quaternion Algebra," 2009.

[6] K. S. Williams, "Integers of Biquadratic Fields," *Canadian Mathematical Bulletin*, vol. 13, no. 4, pp. 519–526, Dec. 1970, doi: 10.4153/cmb-1970-094-8.

[7] V. Acciaro, D. Savin, M. Taous, and A. Zekhnini, "On Quaternion Algebras Over The Composite Of Quadratic Number Fields," *Glas Mat*, vol. 56, no. 1, pp. 63–78, Jun. 2021.

[8] M. Tărnăuceanu, "A characterization of the quaternion group," *Analele Stiintifice ale Universitatii Ovidius Constanta, Seria Matematica*, vol. 21, no. 1, pp. 209–213, 2013, doi: 10.2478/auom-2013-0013.

[9] D. Savin, "About some split central simple algebras," Mar. 2014, [Online]. Available: http://arxiv.org/abs/1403.3443

[10] D. Savin, "About division quaternion algebras and division symbol algebras," Nov. 2014, [Online]. Available: http://arxiv.org/abs/1411.2145

[11] V. Acciaro, D. Savin, M. Taous, and A. Zekhnini, "On quaternion algebras that split over specific quadratic number fields," *Italian Journal Of Pure And Applied Mathematics-N*, vol. 47, no. 2022, pp. 91–107, 2019.

[12] V. Acciaro and D. Savin, "On quaternion algebra over the composite of quadratic number fields and over some dihedral fields," Feb. 2018, [Online]. Available: http://arxiv.org/abs/1802.08185

[13] K. Conrad, "QUATERNION ALGEBRAS," Storrs, 2018.

[14] J. Solà, "Quaternion kinematics for the error-state Kalman filter," Nov. 2017, [Online]. Available: http://arxiv.org/abs/1711.02508

[15] M. Hazewinkel, N. Gubareni, and V. V. Kirichenko, *Algebras, Rings and Modules*, vol. 1. Springer, 2004.

[16] J. Voight, *Quaternion Algebras*. Springer, 2021. [Online]. Available: http://www.springer.com/series/136

[17] D. Eberly, "Quaternion Algebra and Calculus," *Magic Software Inc*, Sep. 2002, [Online]. Available: http://www.geometrictools.com

[18] C. Schwarzweller, "Field Extensions and Kronecker's Construction," *Formalized Mathematics*, vol. 27, no. 3, pp. 229–235, Oct. 2019, doi: 10.2478/forma-2019-0022.

[19] H. Chatland, "On The Euclidean Algorithm In Quadratic Number Fields," *Bulletin of the American Mathematical Society*, vol. 55, no. 10, pp. 948–953, Oct. 1949, [Online]. Available: https://www.ams.org/journal-terms-of-use

[20] D. Shanks, *Solved and unsolved problems in number theory.* Spartan Books, 1962.

[21] T. Weston, "Algebraic Number Theory," Amherst, 1999.

[22] S. Galbraith, *MATHEMATICS OF PUBLIC KEY CRYPTOGRAPHY*. Auckland, New Zealand: Cambridge University Press, 2012.

[23] L. A. Wallenborn, "Berechnung des Hilbert Symbols, quadratische Form-¨ Aquivalenz und Faktorisierung ganzer Zahlen (Computing the Hilbert symbol, quadratic form equivalence and integer factoring)," 2013.

[24] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed. Springer, 1982.

[25] D. Savin, "About split quaternion algebras over quadratic fields and symbol algebras of degree n," *Bulletin mathématique de la Société des Sciences Mathématiques de Roumanie Nouvelle Série*, vol. 60, no. 108, pp. 307–312, Nov. 2017, [Online]. Available: http://arxiv.org/abs/1511.07509