QUATERNION ORDERS OVER QUADRATIC INTEGER RINGS FROM ARITHMETIC FUCHSIAN GROUPS

Edson Donizete de Carvalho¹, Antonio Aparecido de Andrade² §, Reginaldo Palazzo Jr.³

¹Department of Mathematics
São Paulo State University at Ilha Solteira
Ilha Solteira - SP, BRAZIL
e-mail: edson@mat.feis.unesp.br

²Department of Mathematics
São Paulo State University at São José do Rio Preto
São José do Rio Preto - SP, BRAZIL
e-mail: andrade@ibilce.unesp.br

³Department of Telematics
Campinas State University
Campinas - SP, BRAZIL
e-mail: palazzo@dt.fee.unicamp.br

Abstract: In this paper we show that the quaternion orders \( O_{\mathbb{Z}[\sqrt{2}]} \cong (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]} \) and \( O_{\mathbb{Z}[\sqrt{3}]} \cong (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]} \), appearing in problems related to the coding theory [4], [3], are not maximal orders in the quaternion algebras \( \mathcal{A}_{\mathbb{Q}(\sqrt{2})} \cong (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})} \) and \( \mathcal{A}_{\mathbb{Q}(\sqrt{3})} \cong (3 + 2\sqrt{3}, -1)_{\mathbb{Q}(\sqrt{3})} \), respectively. Furthermore, we identify the maximal orders containing these orders.

AMS Subject Classification: 18B35, 94A15

Key Words: Hilbert symbol, arithmetic Fuchsian group, quaternion order, coding theory

Received: April 11, 2012 © 2012 Academic Publications

§Correspondence author
1. Introduction

A Fuchsian group is defined as a discrete subgroup of the projective special linear group $\text{PSL}(2, \mathbb{R})$. Geometrically, the group $\text{PSL}(2, \mathbb{R})$ can be viewed as isometries which act by homeomorphisms on the upper-half plane $\mathbb{H}^2 = \{ z \in \mathbb{C} : \text{Im}(z) > 0 \}$ (Euclidean model of hyperbolic plane), where each isometry is given by a Möbius transformation $T : \mathbb{C} \to \mathbb{C}$ defined as $T(z) = \frac{az + b}{cz + d}$, where $a, b, c, d \in \mathbb{R}$ and $ad - bc = 1$, [9]. In this paper, we are interested in the special class of Fuchsian group called arithmetic Fuchsian group which is obtained by embedding $\rho_1$ of the group of units of an order $\mathcal{O}^1$ belonging to a quaternion algebra $\mathcal{A}$ over a totally real number field into a subgroup of the group $\text{PSL}(2, \mathbb{R})$ of real matrices with determinant equal to 1.

Recently, in [4] and [3] several lattice identifications in the hyperbolic plane have been realized in the context of coding and communication theory. These lattices are described by $\mathbb{Z}$-modules (quaternion orders) consisting of hyperbolic points as the barycenter of the fundamental regular polygons belonging to the hyperbolic tessellation $\{4g, 4g\}$, where $g \geq 2$ denotes the genus of the oriented and compact surface. In [4] and [3] the authors proposed an arithmetic procedure for the identification of the elements of the arithmetic Fuchsian groups $\Gamma_8$ and $\Gamma_{12}$ by the elements of the quaternion orders $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]} \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ and $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]} \simeq (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$, respectively. The arithmetic Fuchsian groups $\Gamma_8$ and $\Gamma_{12}$ consist of the corresponding Möbius transformations associated with the normal form type of edge-pairings [1] with respect to the fundamental regular polygons with 8 and 12 edges.

We develop an arithmetic procedure for the determination of the places at which these quaternion orders ramify. This procedure gives a criterion for checking if these quaternion order are maximal in the corresponding quaternion algebra. We will see that $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ and $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$ are not maximal orders. At the same time, we identify the maximal orders $\mathcal{M}$ containing the quaternion orders $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ and $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$.

Thus, the study of maximal orders has its motivation based on the importance that geometrically uniform codes (GUCs) and space-time block codes (SBTCs) have in the design of new efficient digital communication systems. In the context of GUCs, Cavalcante and Palazzo [8], show that the error-probability of signal sets $\Lambda$ depends on the curvature $t$ associated with homogeneous spaces $\mathbb{E}$, or equivalently, on the genus of a surface, and that the best performance is achieved when we consider surfaces with constant negative curvature (hyperbolic space).
Silva et al. [5] have shown how relevant is the design of hyperbolic signal sets (quotient of a maximal order by a non-trivial ideal) with respect to the performance of the system. In the context of STBCs, Luzzi et al. [7] propose a new method called algebraic reduction for $2 \times 2$ STBCs based on maximal orders from the quaternion algebra $\mathcal{O}$ (identified by the symmetric group which in turn are associated with a fundamental region in the hyperbolic plane).

2. Basic Algebraic Results

In this section we review basic results on valuations over a number field of characteristic different from 2 and $\mathcal{P}$-completion and quaternion algebra which are relevant to the development of this paper. In this regard, we refer the reader to [2].

Let $\mathbb{F}$ be any number field. A valuation $\upsilon$ on $\mathbb{F}$ is a mapping $\upsilon : \mathbb{F} \to \mathbb{R}^+$, satisfying the following properties:

1. $\upsilon(x) \geq 0$ for all $x \in \mathbb{F}$ and $\upsilon(x) = 0$ if and only if $x = 0$.
2. $\upsilon(xy) = \upsilon(x)\upsilon(y)$ for all $x, y \in \mathbb{F}$.
3. $\upsilon(x + y) \leq \upsilon(x) + \upsilon(y)$ for all $x, y \in \mathbb{F}$.
4. $\upsilon(x + y) \leq \max\{\upsilon(x) + \upsilon(y)\}$ for all $x, y \in \mathbb{F}$.

If the valuation $\upsilon$ also satisfies property 4, then $\upsilon$ is called non-Archimedean valuation. If the valuation $\upsilon$ does not satisfy property 4, then we say $\upsilon$ is an Archimedean valuation. Two valuations $\upsilon$ and $\upsilon_1$ in $\mathbb{F}$ are equivalent if there exists $l \in \mathbb{R}^+$ such that $\upsilon(x) = [\upsilon_1(x)]^l$ for $x \in \mathbb{F}$. This equivalence of valuations, also defines equivalence between topological spaces. An equivalence class of valuations is called a place, a prime or a prime spot of $\mathbb{F}$. The field $\mathbb{F}$ is said to be complete at $\upsilon$ if every Cauchy sequence in $\mathbb{F}$ converges to an element of $\mathbb{F}$. If the number field $\mathbb{F}$ is not complete with a valuation, it is always possible to construct a field $\mathbb{F}_\upsilon$ such that $\mathbb{F}_\upsilon$ is an extension of $\mathbb{F}$, and in addition $\mathbb{F}_\upsilon$ is complete with respect to this extended valuation. These fields are called completions of $\mathbb{F}$.

For the cases where $\mathbb{F}$ is complete with an Archimedean valuation, then $\mathbb{F}$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ and the valuation is equivalent to the usual absolute value. The classes of non-Archimedean valuations are known as the finite places or finite primes and these are in one-to-one correspondence with the prime ideals of the integer ring $\mathcal{O}_\mathbb{F}$ of the number field $\mathbb{F}$. For these cases, we also denote
\( \nu = \mathcal{P} = \langle \beta \rangle \). If \( \beta \in \mathcal{O}_F \) and \( \beta \neq 0 \), let \( \nu_\mathcal{P}(\beta) \) be the order of \( \beta \) at \( \mathcal{P} \), that is, the power of \( \mathcal{P} \) in the factorization of the fractional ideal \( \beta \mathcal{P} \). Define \( \nu_\mathcal{P}(0) \) to be 1. The symbol \( \mathbb{F}_\mathcal{P} \) denotes the completion of \( \mathbb{F} \) with respect to the \( \mathcal{P} \)-adic valuation (this field is also called \( \mathcal{P} \)-adic field), \( \mathcal{R}_\mathcal{P} = \{ x \in \mathbb{F}_\nu : \nu_\mathcal{P}(x) \geq 0 \} \) the ring of \( \mathcal{P} \)-adic integers and the maximal ideal in \( \mathcal{P} \) is given by \( \mathcal{P} = \{ x \in \mathbb{F}_\nu : \nu_\mathcal{P}(x) > 0 \} \). Thus, \( \mathbb{F}_\mathcal{P} = \{ \sum_{j=n}^\infty a_j \beta^j : a_j \in \mathcal{O}_F \} \), where \( n \) satisfies the condition \( \nu_\mathcal{P}(x) = \nu_\mathcal{P}(\beta^n) \). The \( \mathcal{P} \)-adic field \( \mathbb{F}_\mathcal{P} \) is called dyadic if \( N(\mathcal{P}) \) is a power of 2, otherwise non-dyadic.

**Theorem 1.** (Hensel’s Lemma) Let \( \mathcal{R}_\mathcal{P} \) be a ring of \( \mathcal{P} \)-adic integers and let \( \mathbb{F} \) denotes the residue field. Let \( f(x) \) be a monic polynomial in \( \mathcal{R}_\mathcal{P} \) such that \( f(x) = \bar{g}(x)\bar{h}(x) \), where \( \bar{g}(x), \bar{h}(x) \in \mathbb{F}[x] \) are relatively prime polynomials. Then there exists polynomials \( g, h \in \mathcal{R}_\mathcal{P}[x] \), where \( g \) and \( h \) reduce mod \( \mathcal{P} \) to \( \bar{g} \) and \( \bar{h} \), with \( \deg(g) = \deg(\bar{g}), \; \deg(h) = \deg(\bar{h}) \) and \( f(x) = g(x)h(x) \).

### 2.1. Quaternion Algebra and Hilbert Symbol

A quaternion algebra \( \mathcal{A} = (\frac{t,s}{F}) \) is defined as a 4-dimensional vector space over a field \( \mathbb{F} \), with basis \( \{1, i, j, ij\} \), satisfying the conditions \( i^2 = t, \; j^2 = s, \; ij = -ji \) and \( (ij)^2 = -ts \), where \( t, s \in \mathbb{F} = \mathbb{F} - \{0\} \). The algebra \( \mathcal{A} = (\frac{t,s}{F}) \) can be embedded in \( M(2, \mathbb{F}(\sqrt{t})) \) (the set of all \( 2 \times 2 \) matrices with elements over \( \mathbb{F}(\sqrt{t}) \)), i.e., there is a linear map such that

\[
\begin{align*}
i &\mapsto \begin{pmatrix} \sqrt{t} & 0 \\ 0 & -\sqrt{t} \end{pmatrix} \quad \text{and} \quad j &\mapsto \begin{pmatrix} 0 & r_1 \\ r_2 & 0 \end{pmatrix},
\end{align*}
\]

where \( s = r_1r_2 \). There exist \( \mathbb{R} \)-isomorphisms \( \rho_i \) given by \( \rho_1 : \mathcal{A}^\mathbb{Q} \otimes \mathbb{R} \to M(2, \mathbb{R}) \) and \( \rho_i : \mathcal{A}^\mathbb{Q} \otimes \mathbb{R} \to H_i \), for \( i = 2, 3, \cdots, n \), where \( \mathcal{A} \) is non-ramified at the place \( \rho_1 \) (we also say \( \mathcal{A} \) splits at the place \( \rho_1 \)) and ramified at the remaining places \( \rho_i \)'s, with \( H_i = (\frac{-1,-1}{\mathbb{R}}) \) denoting the Hamilton quaternion. The Hamilton quaternion is a division algebra, that is, for every nonzero element there is a multiplicative inverse.

The element \( \mathcal{T} = x_0 - x_1i - x_2j - x_3ij \in \mathcal{A} \) is called conjugate of the element \( x = x_0 + x_1i + x_2j + x_3ij \in \mathcal{A} \). The reduced trace and the reduced norm of an element \( x \in \mathcal{A} \) are defined by \( \text{Trd}(x) = x + \mathcal{T} \) and \( \text{Nrd}(x) = x\mathcal{T} = x_0^2 - tx_1^2 - sx_2^2 + txs_3^2 \). Notice, \( \text{Nrd}(x) \) is a quadratic form over \( \mathbb{F} \) in the four variables \( x_0, x_1, x_2, x_3 \).

**Theorem 2.** If \( t, s \in \frac{\mathbb{F}}{\mathbb{F}} \) then, for \( \mathcal{A} = (\frac{t,s}{F}) \), the following facts are equivalent:
1. $A \cong \left( \frac{-1}{\mathbb{F}} \right)$ or $M(2, \mathbb{F})$.

2. The quadratic form $A$ is not a division algebra.

3. There is $x \in \mathbb{F}^4$, where $x = (x_0, x_1, x_2, x_3) \neq (0, 0, 0, 0)$ such that $\text{Nrd}(x) = x_0^2 - tx_1^2 - sx_2^2 + txs x_3^2 = 0$.

4. The quadratic form $tx_1^2 + sx_2^2 = 1$ has a solution with $(x, y) \in \mathbb{F} \times \mathbb{F}$.

5. If $E = \mathbb{F}(\sqrt{t})$ then $s \in N_{E|\mathbb{F}}(E)$.

The Hilbert symbol for the elements $t, s \in \hat{\mathbb{F}}$ is defined by

$$(t, s) = \begin{cases} 1, & \text{if } tx_1^2 + sx_2^2 = 1 \text{ has nonzero solution in } \mathbb{F} \times \mathbb{F} \\ -1, & \text{if not.} \end{cases}$$

Note that the Hilbert symbol $(t, s)$ denotes the same result as established in items (2) and (3) of Theorem 2.

In order to get control over different isomorphism classes of the quaternion algebras over $\mathbb{F}$, one considers the completions $A_\nu \cong A \otimes \mathbb{F} F_\nu$. It is well-known that for every $A_\nu$ there is only two possibilities: $A_\nu \cong M_2(F_\nu)$ ($A$ splits at $\nu$) or $A_\nu \cong H_\nu$ ($A$ is ramified at $\nu$), where $H_\nu$ is a division algebra over $\mathbb{F}_\nu$. In order to decide if $(t, s)_{F_\nu}$ is ramified when $\nu = P$ is a prime ideal, it is convenient to use the Hilbert symbol. A quaternion algebra $A = (t, s)_F$ is called ramified at $P$ if and only if $(\frac{Ls}{P}) = -1$.

**Theorem 3.** (Hilbert Reciprocity Law, see [2]) Let $\mathbb{F}$ be a number field and $t, s \in \mathbb{F} - \{0\}$. Then the set of places $\{ \nu | (t, s) = -1 \text{ in } \mathbb{F}_\nu \}$ is finite and of even cardinality.

Another important result for the determination whether the quaternion algebra $A = (t, s)_P$ splits over the $P$-adic field $\mathbb{F}_P$ is given next.

**Theorem 4.** (see [2]) Let $\mathbb{F}_P$ be a non-archimedean $P$-adic field, with ring $p$-adic integer $R$ and maximal ideal $P$. Let $A = (\frac{t}{P})_P$, where $t, s \in R$.

- If $t, s \not\in P$, then $A$ splits.
- If $t \not\in P, s \in P$, then $A$ splits if and only if $t$ is a square mod $P$.
- If $t, s \in P - P^2$, then $A$ splits if and only if $-t^{-1}s$ is a square mod $P$. 
We conclude, from Theorem 4, that the quaternion algebra \( \mathcal{A} = \left( \frac{t,s}{\mathbb{F}} \right) \) splits if only if \(-t^{-1}s\) is a square in \( R_{\mathcal{P}}^* \). However, an element \( a \in R_{\mathcal{P}}^* \) is a square if only if its image \( \bar{a} \) is a square in the residue field. As a natural consequence of the Hensel’s Lemma (Theorem 1), it follows that the polynomial \( x^2 - a = 0 \) factorizes in \( R_{\mathcal{P}}^*[x] \) if only if the polynomial \( \bar{x}^2 - \bar{a} = \bar{0} \) factorizes in the residue field into relatively prime factors.

**Remark 1.** Let \( \mathbb{F} \) be a totally real number field and \( t, s \in \bar{\mathbb{F}} \) and \( \mathcal{P} \) a prime ideal of \( \mathbb{F} \), with \( N(\mathcal{P}) = q \). In order to decide whether \((t, s)_{\mathbb{F}} \) is ramified at the prime ideal \( \mathcal{P} \) it is equivalent to showing that \( \bar{a} \) is not a square in \( \bar{\mathbb{F}} \). Without loss of generality, we take \( G = \{1, -1\} \). From this, we conclude that \( \bar{a} = -(-1t) = -\bar{1} \). Therefore, we need to show that either \(-1 \not\in \mathbb{L}^2 \) or \((\frac{-1}{q}) = -1 \).

Now we consider a number field \( \mathbb{F} \) of degree \( n \) over \( \mathbb{Q} \). Then there are \( n \) Galois embedding of \( \mathbb{F} \) into \( \mathbb{C} \) with \( n = r_1 + 2r_2 \), where \( r_1 \) is the number of real embedding \( \sigma(\mathbb{F}) \subset \mathbb{R} \) and \( r_2 \) is the number of pairs of \((\sigma, \bar{\sigma})\) such that \( \sigma(\mathbb{F}) \not\subset \mathbb{R} \). If \( \mathbb{F} \subset \mathbb{K} \), where \( \mathbb{K} \) is an extension field of \( \mathbb{F} \), then \((\frac{t,s}{\mathbb{F}}) \otimes _{\mathbb{F}} K \cong (\frac{t,s}{\mathbb{K}}) \).

**Definition 1.** If \( \sigma: \mathbb{F} \longrightarrow \mathbb{R} \) is a real embedding of a number field \( \mathbb{F} \), then \((\frac{t,s}{\mathbb{F}}) \) is said to be ramified at \( \sigma \) if \((\frac{\sigma(t),\sigma(s)}{\mathbb{R}}) \cong \mathcal{H} \) or \( M(2, \mathbb{R}) \).

For a real embedding \( \sigma \) of the number field \( \mathbb{F} \), it follows that \((\frac{t,s}{\mathbb{F}}) \otimes _{\sigma} \mathbb{R} \cong (\frac{\sigma(t),\sigma(s)}{\mathbb{R}}) \cong \mathcal{H} \) or \( M(2, \mathbb{R}) \).

**Remark 2.** We known that every positive real number is a square in \( \mathbb{R} \). As a consequence, the Hilbert symbol associated with \((\frac{1,1}{\mathbb{R}})\) and \((\frac{1,-1}{\mathbb{R}})\) is equal to 1 and the Hilbert symbol associated with \((\frac{-1,-1}{\mathbb{R}})\) is equal to \(-1\). Therefore, the quaternion algebra over \( \mathbb{R} \) given by \((\frac{1,1}{\mathbb{R}})\) and \((\frac{1,-1}{\mathbb{R}})\) are isomorphic to \( M(2, \mathbb{R}) \) and for the case \((\frac{-1,-1}{\mathbb{R}})\) it is isomorphic to the Hamilton quaternion \( \mathcal{H} \).
Theorem 5. (see [2]) A quaternion algebra \((t,s)\) is isomorphic to exactly one of \(H\) or \(M(2,\mathbb{R})\), according to whether both \(t\) and \(s\) are negative or not.

Theorem 6. (see [2]) Let \(\mathcal{A}\) be a quaternion algebra over a number field \(\mathbb{F}\). Then \(\mathcal{A}\) splits over \(\mathbb{F}\) if and only if \(\mathcal{A} \otimes_{\mathbb{F}} \mathbb{F}_\nu\) splits over \(\mathbb{F}_\nu\) at all places.

Note that the finiteness of the set of places at which \(tx^2 + sy^2 = 1\) fails to have a solution, given in Hilbert Reciprocity Law, followed from Theorem 4. For any \(t\) and \(s\), which we can assume lie in \(\mathcal{O}_\mathbb{F}\), there are only finitely many prime ideals so that \(t\) or \(s\) \(\in\) \(\mathcal{P}\). Thus \((t,s)\) splits at all but a finite number of \(\mathcal{P}\)-places. As there are only finitely many Archimedean places and finitely many \(\mathcal{P}\)-places (with characteristic different from 2), then \((t,s)\) splits at all but finite number of places [2].

Theorem 7. (see [2]) Let \(\mathcal{A}\) be a quaternion algebra over a number field \(\mathbb{F}\). The number of places \(\nu\) on \(\mathbb{F}\) such that \(\mathcal{A}\) is ramified at \(\nu\) is of even cardinality.

Definition 2. The finite set of places at which \(\mathcal{A}\) is ramified will be denoted by \(\text{Ram}(\mathcal{A})\), the subset of Archimedean ones by \(\text{Ram}_\infty(\mathcal{A})\) and the non-Archimedean ones by \(\text{Ram}_f(\mathcal{A})\). The places \(\nu \in \text{Ram}_\infty(\mathcal{A})\) correspond to prime ideals \(\mathcal{P}\) and the reduced discriminant of \(\mathcal{A}, \Delta(\mathcal{A})\), is the ideal defined by

\[
\Delta(\mathcal{A}) = \prod_{\mathcal{P} \in \text{Ram}_f(\mathcal{A})} \mathcal{P}.
\]  

The discriminant \(\Delta(\mathcal{A})\) of \(\mathcal{A}\) is defined as the product of the prime ideals at which \(\mathcal{A}\) is ramified.

2.2. Quaternion Order

An order \(\mathcal{O}\) in \(\mathcal{A}\) over \(\mathbb{F}\) is a subring of \(\mathcal{A}\) containing \(\mathbb{Z}[\theta]\), which is finitely generated as a \(\mathcal{O}_{\mathbb{F}}\)-module containing 1 with rank equal to \(4n\), such that \(\mathbb{F}\mathcal{O} = \mathcal{A}\).

Example 1. (see [4], [3]) Let \(\mathbb{Z}[\sqrt{2}]\) be the integers ring of the number field \(\mathbb{Q}(\sqrt{2})\). The \(\mathbb{Z}[\sqrt{2}]\)-module given by \(\mathcal{O}_{\mathbb{Z}[\sqrt{2}]} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]} = \{x_0 + x_1i + x_2j + x_3ij | x_0, x_1, x_2, x_3 \in \mathbb{Z}[\sqrt{2}]\}\) (where \(i^2 = \sqrt{2}\) and \(j^2 = -1\)) is a quaternion order of the quaternion algebra \(\mathcal{A}\) over \(\mathbb{Q}(\sqrt{2})\). The elements of this quaternion order can be seen as elements of an arithmetic Fuchsian group.
Γ₈ associated with the fundamental polygon P₈ of the hyperbolic tessellation {8,8} from the normal form type of edge-pairings identification. Now, let \( \mathbb{Z}[\sqrt{3}] \) be the integers ring of the number field \( \mathbb{Q}(\sqrt{3}) \). The \( \mathbb{Z}[\sqrt{3}] \)-module given by \( \mathcal{O}_{\mathbb{Z}[\sqrt{3}]} = (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]} = \{x_0 + x_1i + x_2j + x_3ij | x_0, x_1, x_2, x_3 \in \mathbb{Z}[\sqrt{3}] \} \) (where \( i^2 = 3 + 2\sqrt{3} \) and \( j^2 = -1 \)) is a quaternion order of the quaternion algebra \( A \) over \( \mathbb{Q}(\sqrt{3}) \). The elements of this quaternion order can be seen as elements of an arithmetic Fuchsian group \( \Gamma_{12} \) associated with the fundamental polygon \( P_{12} \) of the hyperbolic tessellation \( \{12,12\} \) from the normal form type of edge-pairings identification.

3. Maximal Order

If \( \mathcal{O} \) is an order in \( A \), then the discriminant \( \Delta(\mathcal{O}) \) is defined as the square root of the \( \mathbb{Z}[\theta] \)-ideal generated by \( \det(Tr(x_i \bar{x}_j)) \), where \( \mathbb{Z}[\theta] \) is integer ring of number field \( \mathbb{F} \) and \( \{x_1, x_2, x_3, x_4\} \) is a \( \mathbb{Z}[\theta] \)-basis of the quaternion order \( \mathcal{O} \). An order \( \mathcal{M} \) in a quaternion algebra \( A \) is called maximal if \( \mathcal{M} \) is not contained in any other order in \( A \). If \( \mathcal{M} \) is a maximal order in \( A \) containing another order \( \mathcal{O} \), then the discriminant satisfies the following condition, \( \Delta(\mathcal{O}) = \Delta(\mathcal{M})|\mathcal{M} : \mathcal{O}| \) and \( \Delta(\mathcal{M}) = \Delta(\mathcal{A}) \). Conversely, if \( \Delta(\mathcal{O}) = \Delta(\mathcal{A}) \), then \( \mathcal{O} \) is a maximal order in \( A \).

**Proposition 1.** (see [3]) If \( \mathcal{O}_{\mathbb{Z}[\theta]} = (t,s)_{\mathbb{Z}[\theta]} \) is a quaternion order of a quaternion algebra \( A = (t,s)_{\mathbb{F}} \) over a field \( \mathbb{F} \) then the discriminant is given by \( \Delta(\mathcal{O}_{\mathbb{Z}[\theta]}) = 4ts \).

**Example 2.** Applying Proposition 1 to the quaternion order \( \mathcal{O}_{\mathbb{Z}[\sqrt{2}]} \cong (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]} \) and \( \mathcal{O}_{\mathbb{Z}[\sqrt{3}]} \cong (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]} \), we obtain \( \Delta(\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}) = -4\sqrt{2} = -\sqrt{2}^5 \) and \( \Delta(\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}) = -4(3 + 2\sqrt{3}) \), respectively.

**Proposition 2.** If \( A = (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})} \) is a quaternion algebra over \( \mathbb{Q}(\sqrt{2}) \), then \( A \) is ramified at one real place \( \sigma_2 \in Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \). If \( A = (3 + 2\sqrt{3}, -1)_{\mathbb{Q}(\sqrt{3})} \) is a quaternion algebra over \( \mathbb{Q}(\sqrt{3}) \), then \( A \) is ramified at one real place \( \sigma_2 \in Gal(\mathbb{Q}(\sqrt{3})|\mathbb{Q}) \).

**Proof.** When we applied the non-identity homomorphism \( \sigma_2 \) over \( \sqrt{2} \), we
obtain $\sigma_2(\sqrt{2}) = -\sqrt{2} < 0$. From Equation (2.1), we obtain $(\frac{\sqrt{2} - 1}{Q(\sqrt{2})}) \otimes_{\sigma} \sigma(Q(\sqrt{2})) \cong (\frac{\sigma_2(\sqrt{2}) - 1}{\sigma(Q(\sqrt{2}))})$. As a consequence of Definition 1 and Theorem 5, it follows that $\mathcal{A} = (-\sqrt{2}, -1)_{Q(\sqrt{2})} \cong H$ and $\mathcal{A}$ is ramified at the real place $\sigma_2$. Now, when we applied the non-identity homomorphism $\sigma_2$ over $3 + 2\sqrt{3}$, we obtain $\sigma_2(3 + 2\sqrt{3}) = 3 - 2\sqrt{3} < 0$. From Equation (2.1), we obtain $(3 + 2\sqrt{3}, -1)_{Q(\sqrt{3})} \cong (\sigma_2(3 + 2\sqrt{3}) - 1)_{\sigma(Q(\sqrt{3}))}$. As a consequence of Definition 1 and Theorem 5, it follows that $\mathcal{A} = (3 - 2\sqrt{3}, -1)_{Q(\sqrt{3})} \cong H$ and $\mathcal{A}$ is ramified at the real place $\sigma_2$.

Notice that the place $\sigma_2$ non-identity homomorphism belonging to the Galois Group $Gal(F|Q)$ for the cases $F = Q(\sqrt{2})$ or $Q(\sqrt{3})$ corresponds to the Archimedean valuation, and we obtain $\mathbb{R}$ as completion of the field $F$ with this valuation.

**Proposition 3.** Let $O_{Z[\sqrt{2}]} \cong (\sqrt{2}, -1)_{Z[\sqrt{2}]}$ be a quaternion order of the quaternion algebra $A_{Q(\sqrt{2})} \cong (\sqrt{2}, -1)_{Q(\sqrt{2})}$. Then, we obtain the following results:

1. $\mathcal{P}_1 = \langle \sqrt{2} \rangle$ is the unique prime ideal, such that, the quaternion algebra $A_{Q(\sqrt{2})}$ is ramified.

2. The quaternion order $O_{Z[\sqrt{2}]}$ is not maximal order in the quaternion algebra $A_{Q(\sqrt{2})}$.

**Proof.** 1) Notice that $\Delta(A_{Q(\sqrt{2})})$ divides $\Delta(O_{Z[\sqrt{2}]}) = -4\sqrt{2} = -(\sqrt{2})^5$. We know the relative norm $N_{Q(\sqrt{2})|Q}$ over the element $z = x + y\sqrt{2} \in Z[\sqrt{2}]$ is given by $N_{Q(\sqrt{2})|Q}(z) = x^2 - 2y^2$. Then, when we applied the relative norm $N_{Q(\sqrt{2})|Q}$ over $\sqrt{2}$, we obtain $N_{Q(\sqrt{2})|Q}(\sqrt{2}) = -2$. Therefore, we conclude the prime ideal $\mathcal{P}_1 = \langle \sqrt{2} \rangle$, it is the only possibility of the prime ideal, such that, the quaternion $\mathcal{A}$ is ramify. For 2), as a consequence of item 1), we obtain $\Delta(A) = \sqrt{2}$. Then, we conclude $\Delta(A) \neq \Delta(O)$. Therefore $O$ is not a maximal order in $A$. \qed

**Proposition 4.** Let $O_{Z[\sqrt{3}]} \cong (3 + 2\sqrt{3}, -1)_{Z[\sqrt{3}]}$ be a quaternion order of the quaternion algebra $A_{Q(\sqrt{2})} \cong (\sqrt{2}, -1)_{Q(\sqrt{2})}$. Then, we obtain the followings results:
1. \( P_1 = \langle 3 + 2\sqrt{3} \rangle \) is the unique prime ideal such that the quaternion algebra \( A \) is ramified.

2. The quaternion order \( O_{\mathbb{Z}[\sqrt{3}]} \) is not maximal order in the quaternion algebra \( A_{\mathbb{Q}(\sqrt{3})} \).

**Proof.** Notice that \( \Delta(A_{\mathbb{Q}(\sqrt{3})}) \) divides \( \Delta(O_{\mathbb{Z}[\sqrt{3}]}) = -4(3 + 2\sqrt{3}) \). We know the relative norm \( N_{\mathbb{Q}(\sqrt{3})}^{\mathbb{Q}} \) over the element \( z = x + y\sqrt{3} \in \mathbb{Z}[\sqrt{3}] \) is given by \( N_{\mathbb{Q}(\sqrt{3})}^{\mathbb{Q}}(z) = x^2 - 3y^2 \). We can write \(-2\) as \(-2 = (1 + \sqrt{3})(1 - \sqrt{3})\). Then, when we applied the relative norm \( N_{\mathbb{Q}(\sqrt{3})}^{\mathbb{Q}} \) over \( 3 + 2\sqrt{3} \), \( 1 + \sqrt{3} \) and \( 1 - \sqrt{3} \), we obtain \( N_{\mathbb{Q}(\sqrt{3})}^{\mathbb{Q}}(3 + 2\sqrt{3}) = -3 \) and \( N_{\mathbb{Q}(\sqrt{3})}^{\mathbb{Q}}(1 + \sqrt{3}) = N_{\mathbb{Q}(\sqrt{3})}^{\mathbb{Q}}(1 - \sqrt{3}) = -2 \). Therefore, \( 3 + 2\sqrt{3}, 1 + \sqrt{3} \) and \( 1 - \sqrt{3} \) are prime elements in integer ring \( \mathbb{Z}[\sqrt{3}] \). Then, we conclude \( \Delta(O_{\mathbb{Z}[\sqrt{3}]}) \) divides \( \Delta(\mathbb{Q}(\sqrt{3})) \). Now, we take \( P_1 = \langle 3 + 2\sqrt{3} \rangle, P_2 = \langle 1 + \sqrt{3} \rangle \) and \( P_3 = \langle 1 - \sqrt{3} \rangle \). Then \( \Delta(O_{\mathbb{Z}[\sqrt{3}]}) = P_1 P_2^2 P_3^2 \). However, it is possible to write \( 1 + \sqrt{3} \) as \( 1 + \sqrt{3} = (1 - \sqrt{3})(-2 - \sqrt{3}) \), where and \( N_{\mathbb{Q}(\sqrt{3})}^{\mathbb{Q}}(-2 - \sqrt{3}) = 1 \). Then, we conclude \( \langle -2 - \sqrt{3} \rangle \) is invertible element of \( \mathbb{Z}[\sqrt{3}] \). Therefore, the prime ideals generated by \( \langle 1 + \sqrt{3} \rangle \) and \( \langle 1 - \sqrt{3} \rangle \) are conjugate. Without loss of generality, we take \( P_2 = \langle 1 + \sqrt{3} \rangle \). Then, we conclude the \( P_1 = \langle 3 + 2\sqrt{3} \rangle, P_2 = \langle 1 + \sqrt{3} \rangle \) are only the possibilities of prime ideals, such that, \( A \) is ramified. It is easy to verify \(-1 \not\in \mathbb{L} \) and \( \mathbb{L} = \mathbb{F}^* = \mathbb{F} = \mathbb{F} - \{0\} \) (with \( \mathbb{F} \) finite field of cardinality 3), or as, \( (\frac{-1}{3}) = -1 \). We saw in item 2) of Proposition 2 that \( A \) is ramified one real places. However, we saw in Theorem 7 that \( A \) are ramified on even places. Therefore, we conclude \( P_1 = \langle 3 + 2\sqrt{3} \rangle \), it is only prime ideal in \( \mathbb{Z}[\sqrt{3}] \), such that, \( A \) is ramified. \( \mathbb{L} = \mathbb{F}^* \).

For (2) as a consequence of item (1), we obtain \( \Delta(A) = 3 + 2\sqrt{3} \). Then, we conclude \( \Delta(A) \neq \Delta(\mathcal{O}) \). Therefore \( \mathcal{O} \) is not a maximal order in \( A \).

Notice that if \( O_{\mathbb{Z}[\sqrt{2}]} \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]} \), then a \( \mathbb{Z}[\sqrt{2}] \)-basis for \( O_{\mathbb{Z}[\sqrt{2}]} \) is given by \( \{1, i, j, ij\} \), where \( i = \sqrt{2}, j = l, ij = \sqrt{2}l, l^2 = -1 \) and \( ij = -ji \).

From Proposition 3 it follows that the order \( O_{\mathbb{Z}[\sqrt{2}]} \) is not maximal. However, \( \{1, \frac{i}{2} = \frac{\sqrt{2}}{2}, j = l, \frac{i}{2}j = -j\frac{i}{2} \} \) is another \( \mathbb{Z}[\sqrt{2}] \)-basis for \( O_{\mathbb{Z}[\sqrt{2}]} \) and so, there is a new quaternion order \( \mathcal{M}_{\mathbb{Z}[\sqrt{2}]} \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]} \) containing \( (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]} \), where \( \Delta(\mathcal{M}_{\mathbb{Z}[\sqrt{2}]} = \sqrt{2} \). Therefore, \( \Delta(\mathcal{M}) = d(\mathcal{A}) \) and \( \mathcal{M}_{\mathbb{Z}[\sqrt{2}]} \) is a maximal order in \( A_{\mathbb{Z}[\sqrt{2}]} \). Similarly, if \( O_{\mathbb{Z}[\sqrt{3}]} \simeq (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]} \), then a \( \mathbb{Z}[\sqrt{3}] \)-basis for \( O_{\mathbb{Z}[\sqrt{3}]} \) is given by \( \{1, i, j, ij\} \), where \( i = \sqrt{2 + 3\sqrt{3}}, j = l, l^2 = -1 \) and \( ij = -ji \). From Proposition 4 it follows that the order \( O_{\mathbb{Z}[\sqrt{3}]} \) is not maximal.
However, $\{1, \frac{i}{2} = \sqrt{\frac{3+2\sqrt{3}}{2}}, j, \frac{j}{2} = -\frac{j}{2}i\}$ is another $\mathbb{Z}[^3]{\sqrt{3}}$-basis for $\mathcal{O}_{\mathbb{Z}[^3]{\sqrt{3}}}$ and so there is a new quaternion order $\mathcal{M}_{\mathbb{Z}[^3]{\sqrt{3}}} \simeq \langle \frac{3+2\sqrt{3}}{2}, -1 \rangle_{\mathbb{Z}[^3]{\sqrt{3}}}$ containing $(3 + 2\sqrt{3}, -1)_{\mathbb{Z}[^3]{\sqrt{3}}}$, where $\Delta(\mathcal{M}_{\mathbb{Z}[^3]{\sqrt{3}}}) = \sqrt{3}$. Therefore, $\Delta(\mathcal{M}) = \Delta(\mathcal{A})$ and $\mathcal{M}_{\mathbb{Z}[^3]{\sqrt{3}}}$ is a maximal order in $\mathcal{A}_{\mathbb{Z}[^3]{\sqrt{3}}}$. \hfill $\square$

Acknowledgments

The authors would like to thank the financial support received by FAPESP under Grant 2007/56052-8.

References


