UNIVERSITAT DE BARCELONA

Treball Final del Màster de Matemàtica Avançada
Facultat de Matemàtiques i Informàtica

Families of Orders of Quaternion Algebras over $\mathbb{Q}$

Alejandro de Miquel Bleier

Director: Dr. Artur Travesa Grau
Departament de Matemàtiques i Informàtica

Barcelona, 28 de juny de 2017

Abstract

Every quaternion algebra contains a set of orders, whose understanding would be helping for the Shimura curves theory development. In this master's thesis, certain parametric families of orders of quaternion algebras over $\mathbb{Q}$ have been defined, and their relationships with Eichler orders have been studied. In particular, for some given quaternion algebras over $\mathbb{Q}$, we have defined and studied three families of orders $\mathcal{O}$, $\mathcal{O}'$ and $\mathcal{O}''$, together with a maximal order $\mathcal{O}^{max}$ belonging to all of the families. As a main result, given a square-free integer N coprime with the discriminant of the quaternion algebra given, it is possible to find an Eichler order of level N belonging to the family $\mathcal{O}'$ and satisfying

$$\mathcal{O}^{max} \supset \mathcal{O}' \supset \mathcal{O}'' \supset \mathcal{O} = \mathbb{Z} + N\mathcal{O}^{max},$$

in a way that every quotient is isomorphic to $\mathbb{Z}/N\mathbb{Z}$ as abelian groups, this is,

$$\mathcal{O}/\mathcal{O}' \cong \mathcal{O}'/\mathcal{O}'' \cong \mathcal{O}''/\mathcal{O} \cong \mathbb{Z}/N\mathbb{Z}.$$

Introduction

The article [2] studies a certain family of orders of the matrix algebra $\mathbf{M}(2,\mathbb{Q})$. Their unit groups can be related to congruence groups of $\mathbf{SL}(2,\mathbb{Z})$, and therefore act in the Poincaré half-plane. The idea of this master's thesis is to make a similar study, but considering families of orders of quaternion algebras over $\mathbb{Q}$, rather than of $\mathbf{M}(2,\mathbb{Q})$. The groups of units of the orders of quaternion algebras also act on the Poincaré half-plane, via some suitable embeddings in $\mathbf{PSL}(2,\mathbb{R})$, and each one of them is associated to a Shimura curve. Thus, a good understanding of the quaternion algebras, and in particular of their orders and corresponding unit groups, would be helpful for the understanding of the Shimura curves. In this work we focus on the orders.

In [4], a solid background on the arithmetic of quaternion algebras and their orders is given, and in [1] the focus is put on applying this background to quaternion algebras over $\mathbb{Q}$ and their use in the Shimura curves theory. We use some of the results therein presented to analyse the orders that are meaningful to our study. In fact, the first chapter of this work is basically composed of results extracted from these references. Once the necessary background and tools have been introduced, we present the results of our research in the second chapter. We consider two types of quaternion algebras over $\mathbb{Q}$ and study three different families of orders for each of them. These families have been chosen for having the most interesting properties amongst all of the families that have been considered during the research. The meaningfulness of the families of orders is shown along the work. The relation they have with each other and their relation with Eichler orders is particularly relevant. It is to be remarked that the study has led to very similar results in both cases, even if the calculations were different. A summary of the main results and conclusions, common for all the quaternion algebras studied, follows.

For both types of quaternion algebras, three different families of tri-parametric orders have been defined, $\mathcal{O}(m,n,d)$, $\mathcal{O}'(m,n,d)$ and $\mathcal{O}''(m,n,d)$, and a maximal order belonging to all of the families has been found, called $\mathcal{O}^{max}$. The family $\mathcal{O}'(m,n,d)$ contains an Eichler order of level N for every N square-free and coprime with the discriminant of the quaternion algebra. The order is such that level N coincides with the value of the first parameter. For every such Eichler order, there also exist orders belonging to the families $\mathcal{O}(m,n,d)$ and $\mathcal{O}''(m,n,d)$ such that

$$\mathcal{O}^{max} \supset \mathcal{O}'(N,n,d) \supset \mathcal{O}''(N,n,N) \supset \mathcal{O}(N,N,N) = \mathbb{Z} + N\mathcal{O}^{max}.$$

Moreover, if $N > 1$, these inclusions are always strict, and every quotient is isomorphic to $\mathbb{Z}/N\mathbb{Z}$ as abelian groups, this is,

$$\mathcal{O}^{max}/\mathcal{O}'(N,n,d) \cong \mathcal{O}'(N,n,d)/\mathcal{O}''(N,n,N) \cong \mathcal{O}''(N,n,N)/\mathcal{O}(N,N,N) \cong \mathbb{Z}/N\mathbb{Z}.$$

Acknowledgements

First of all, I would like to thank my master's thesis director, Dr. Artur Travesa Grau, for all the time he has spent guiding me and advising me to help me solving the different problems I have faced for completing this master's thesis. I would also like to thank my parents and my sister for their support during this master's degree. Finally, I want to thank all the friends that have made these two years of hard work easier; in particular, Edu, for the time spent discussing with me several mathematics problems of all kinds, and Alex, Victòria, Cardús and Adrià, for all the good moments we have shared.

Contents

Chapter 1

Quaternion Algebras and their Orders

In order to introduce some basic concepts about quaternion algebras, we are first going to introduce them in a general way. This will allow us to have a general insight on the behaviour of quaternion algebras and to introduce some important properties that will later apply to our particular case, the quaternion algebras over $\mathbb{Q}$. The definitions and results shown in this first chapter can be found either in [1], in [2] or in [4]. Some of them will be referred more precisely throughout the chapter.

1.1. Quaternion Algebras

Definition 1.1. Let K be a field. A quaternion K-algebra H is a central simple K-algebra, associative and with unit element, of dimension 4 over K.

If the characteristic of K is different from 2, there exist two nonzero elements $a, b \in K$ such that there exists a basis $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ of H with $\mathbf{1}$ being the neutral element for the multiplication and satisfying the relations

$$\mathbf{i}^2 = a, \quad \mathbf{j}^2 = b, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}. \tag{1.1}$$

In fact, these relations define the algebra. Consequently, we will express a quaternion algebra H over a field K defined by a and b as $\left(\frac{a,b}{K}\right)$. If the characteristic of K is equal to 2, there also exists a couple (a, b) defining the operations of the quaternion algebra. However, these operations are characterised by the relations

$$\mathbf{i}^2 + \mathbf{i} = a, \quad \mathbf{j}^2 = b, \quad \mathbf{ij} = \mathbf{j}(\mathbf{i} + \mathbf{1}), \tag{1.2}$$

which yields a different structure than for the rest of characteristics.

In the following, we are only going to consider fields of characteristic different from 2. Note that from the relations (1.1), the following multiplication table follows:

$\cdot$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	a	$\mathbf{k}$	$a\mathbf{j}$
$\mathbf{j}$	$-\mathbf{k}$	b	$-b\mathbf{i}$
$\mathbf{k}$	$-a\mathbf{j}$	$b\mathbf{i}$	$-ab$

Definition 1.2. Let $H = \left(\frac{a,b}{K}\right)$ be a quaternion algebra, and consider the element $\alpha = x + y\mathbf{i} + z\mathbf{j} + t\mathbf{k} \in H$, with $x, y, z, t \in K$.

- The quaternion α is called **pure** if $x = 0$.
- The **conjugate** of α is $\overline{\alpha} = x - y\mathbf{i} - z\mathbf{j} - t\mathbf{k}$.
- The **reduced trace** of α is $tr(\alpha) = \alpha + \overline{\alpha} = 2x$.
- The **reduced norm** of α is $n(\alpha) = \alpha\overline{\alpha} = x^2 - ay^2 - bz^2 + abt^2$.

If the elements $\alpha \in H$ are expressed as $\alpha = x+y\mathbf{i}+z\mathbf{j}+t\mathbf{k}$, with $x, y, z, t \in K$, like in the previous definition (note that we omit the specification of the $\mathbf{1}$ dimension), we will use the notation $\alpha_{\mathbf{1}}, \alpha_{\mathbf{i}}, \alpha_{\mathbf{j}}$ and $\alpha_{\mathbf{k}}$ to refer to the coefficient of each of the 4 dimensions of the quaternion. In this case, for example, we would have that $\alpha_{\mathbf{1}} = x, \alpha_{\mathbf{i}} = y, \alpha_{\mathbf{j}} = z$ and $\alpha_{\mathbf{k}} = t$.

Proposition 1.3. [4] *A quaternion algebra $\left(\frac{a,b}{K}\right)$ is isomorphic to*

$$\left\{ \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix} | x, y, z, t \in K \right\} \subseteq \mathbf{M}\left(2, K(\sqrt{a})\right), \tag{1.3}$$

where $\sqrt{a}$ is a square root of a in a fixed separable closure of K.

Proof. Just note that the matrices

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{-a} \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}, \quad IJ = \begin{pmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{pmatrix}$$

satisfy the relations (1.1). □

Example 1.4 (The Hamilton quaternions)**.** The quaternion algebra $\left(\frac{-1,-1}{\mathbb{R}}\right)$ is also known as the Hamilton quaternions. This quaternion algebra is the most known one, due to the big amount of applications it has been found useful for. As an example, its strong relationship with the group of rotations $SO(3)$ ($\left(\frac{-1,-1}{\mathbb{R}}\right)^*$ is a double covering of the group $SO(3)$) is currently used for computing the position of autonomous vehicles when interpreting data acquired by gyroscopes.

Definition 1.5. Let $K = \mathbb{Q}$, and consider the set of embeddings $i : K \to L$ into a local field (i.e. a finite extension of $\mathbb{R}$, $\mathbb{Q}_p$ of $\mathbb{F}_p[[x]]$) such that $i(K)$ is dense in L. We say that two such embeddings i, i' are equivalent if $i' = fi$ for some isomorphism $f : L \to L'$. An equivalence class is called a **place** of K, and we note it as v. We will note as K_v the representants of the local fields such that $i_v : K \to K_v$ is an embedding for a place v.

Definition 1.6. Let H be a quaternion algebra over K. A place **ramifies** in H if the extended quaternion algebra $H_v = H \otimes K_v$ is a division algebra.

Lemma 1.7. [4] *The number of places of K that ramify in H is finite.*

Let R be an integral domain, and let K be its field of fractions.

Definition 1.8. The **reduced discriminant** D_H of a quaternion K-algebra H is the integral ideal of R equal to the product of prime ideals of R that ramify in H.

Since R is a principal ideal domain, we can identify the ideals of R with their generators. Hence, in the quaternion $\mathbb{Q}$-algebras, we can identify the reduced discriminants with integers.

Proposition 1.9. *Two quaternion K-algebras are isomorphic if and only if they have the same reduced discriminant.*

1.1.1. Quaternion Algebras over $\mathbb{Q}$

So far we have given some basic definitions about quaternion algebras that will be useful to us. For the case of the quaternion algebras over $\mathbb{Q}$, which is the one we are particularly interested in, one can obtain more specific results. The following theorem characterises many of the quaternion algebras over $\mathbb{Q}$, and will determine the quaternion algebras we will be working with in the next chapter.

Theorem 1.10. [1] *Let $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a quaternion algebra such that its discriminant D_H either is equal to one or can be expressed as the product of two primes. Then,*

(I) *If $D_H = 1$, then $H \cong \mathbf{M}(2,\mathbb{Q}) \cong \left(\frac{1,-1}{\mathbb{Q}}\right)$.*

(II) *If $D_H = 2p$, with p prime and $p \equiv 3 \mod 4$, then $H \cong \left(\frac{p,-1}{\mathbb{Q}}\right)$.*

(III) *If $D_H = pq$, with p, q prime numbers such that $q \equiv 1 \mod 4$ and $\left(\frac{p}{q}\right) = -1$, where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol, then $H \cong \left(\frac{p,q}{\mathbb{Q}}\right)$.*

If a and b are prime numbers, then H satisfies one, and only one, of these three statements.

We denote by $H_A(p)$ and $H_B(p,q)$ the quaternion algebras like the ones specified in (II) and (III), respectively.

Definition 1.11. The quaternion $\mathbb{Q}$-algebras having discriminant equal to the product of two distinct prime numbers are called **small ramified $\mathbb{Q}$-algebras**. We say that a small ramified $\mathbb{Q}$-algebra is of **type A** if it is isomorphic to $H_A(p)$ for some prime p satisfying $p \equiv 3 \mod 4$, and we say that it is of **type B** if it is isomorphic to $H_B(p,q)$ for some primes p, q satisfying $q \equiv 1 \mod 4$ and $\left(\frac{p}{q}\right) = -1$.

In what follows, we are going to work on quaternion algebras up to isomorphism. Thus, we will call the algebras of the form $H_A(p)$ type A algebras, and we will call the algebras of the form $H_B(p,q)$ type B algebras; in both cases, p and q satisfying the required conditions.

1.2. Quaternion Orders

Our main object of study are the orders of quaternion algebras. This section introduces them and states their main properties, to be used in the next chapter.

Let R be a principal ideal domain, K its field of fractions and H a quaternion algebra over K.

Definition 1.12. An element $\alpha \in H$ is called **integral** over K if $tr(\alpha), n(\alpha) \in R$.

Example 1.13. In the case of a quaternion algebra H over $\mathbb{Q}$, an element $\alpha \in H$ is integral if $tr(\alpha), n(\alpha) \in \mathbb{Z}$.

Definition 1.14. Let V be a K-vector space. An R-**lattice** of V is a finitely generated R-module contained in V. If L is an R-lattice of V, we say that L is **full** if $K \otimes_R L \simeq V$.

Definition 1.15. An **ideal** of a quaternion algebra H is a full R-lattice.

Definition 1.16. An **order** $\mathcal{O}$ of H is a ring of integral elements containing R such that $K\mathcal{O} = H$. An order is called **maximal** if it is not strictly contained inside any other order. An order is called **Eichler order** if it is the intersection of two maximal orders.

Remark 1.17. Equivalently, an order could also have been defined as an ideal which is also a ring.

Definition 1.18. Let $\mathcal{O}$ be an R-order in H. The **different** $\mathcal{D}_\mathcal{O}$ of $\mathcal{O}$ is the bilateral R-ideal of $\mathcal{O}$ computed as the inverse of the dual of $\mathcal{O}$ by the bilinear form given by the reduced trace. This is, $\alpha \in \mathcal{D}_\mathcal{O}^{-1}$ if and only if $tr(\alpha\mathcal{O}) \subseteq R$. Its reduced norm, $D_\mathcal{O} = n(\mathcal{D}_\mathcal{O})$, is then the **reduced discriminant** of $\mathcal{O}$.

Proposition 1.19. *Let $\mathcal{O}$ be an R-order in H. Then,*

- *$D_\mathcal{O}^2$ is the ideal of R generated by $\{\det(tr(w_i w_j)) : 1 \leq i, j \leq 4, w_i, w_j \in \mathcal{O}\}$;*
- *if $\{v_1, \dots v_4\}$ is an R-basis of $\mathcal{O}$, then $D_\mathcal{O}^2 = R \det(tr(v_i v_j))$;*
- *if $\mathcal{O}'$ is an order in H such that $\mathcal{O} \subset \mathcal{O}'$, then $D_{\mathcal{O}'}$ divides $D_\mathcal{O}$, and $D_{\mathcal{O}'} = D_\mathcal{O}$ only if $\mathcal{O} = \mathcal{O}'$.*

Corollary 1.20. *Let $\mathcal{O}$ be an order of the quaternion algebra $H = \left(\frac{a,b}{\mathbb{Q}}\right)$, with $a, b \in \mathbb{Z}$. Let P be the matrix of change of basis from a fixed $\mathbb{Z}$-basis of $\mathcal{O}$ to the basis $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Then, $D_\mathcal{O} = |4ab \det P|$.*

Proposition 1.21. *All the maximal orders of a quaternion algebra over $\mathbb{Q}$ belong to the same conjugacy class.*

Definition 1.22. Let v be a place of K, and let $\mathcal{O}_v$ be an Eichler order in a quaternion K_v-algebra H_v. Then, the **level** of $\mathcal{O}_v$ is the ideal

$$N_{\mathcal{O}_v} = \begin{cases} R_v, & \text{if } H_v \text{ is a division algebra,} \\ N_{\varphi(\mathcal{O}_v)}, & \text{where } \varphi : H_v \to \mathbf{M}(2, K_v) \text{ is an isomorphism.} \end{cases}$$

Definition 1.23. The **level** $N_{\mathcal{O}}$ of an Eichler order $\mathcal{O}$ is the unique integral ideal NR in R such that N_v is the level of each $\mathcal{O}_v$ at each finite place v of K. Thus, $N_{\mathcal{O}} = \prod_v N_{\mathcal{O}_v}$.

Proposition 1.24. [1] *Let $\mathcal{O}$ be an order in a quaternion $\mathbb{Q}$-algebra H of discriminant D_H.*

(I) *If $\mathcal{O}$ is an Eichler order, then $D_{\mathcal{O}} = D_H N_{\mathcal{O}}$ and $\gcd(D_H, N_{\mathcal{O}}) = 1$.*

(II) *If $D_{\mathcal{O}} = D_H N$ is a square-free integer, then $\mathcal{O}$ is an Eichler order of level N.*

(III) *Let $\mathcal{O}$ and $\mathcal{O}'$ be conjugate $\mathbb{Z}$-orders in H. Then, $\mathcal{O}$ is an Eichler order of level N if and only if $\mathcal{O}'$ is an Eichler order of level N.*

Remark 1.25. An Eichler order has level 1 if and only if it is a maximal order.

Proposition 1.26. [1] *Let H be a quaternion $\mathbb{Q}$-algebra of discriminant D. Then, for each integer N such that $\gcd(N, D) = 1$, there exist Eichler orders of level N.*

1.3. Parametric Families of Orders: A First Example

In this section we are going to state the main results shown in [2]. In the cited article, a parametric family of orders over the matrix algebra $\mathbf{M}(2, \mathbb{Q})$ is considered and studied. This will serve us as a motivating example for us to define the families of orders of quaternions over $\mathbb{Q}$.

Definition 1.27. For every $m, n \geq 1$ integers and for every divisor $d \geq 1$ of mn, we define the family of orders

$$\mathcal{O}(m, n, d) = \left\{ \begin{pmatrix} x & ym \\ zn & x + td \end{pmatrix} \mid x, y, z, t \in \mathbb{Z} \right\} \subseteq \mathbf{M}(2, \mathbb{Z}).$$

Indeed, it is not hard to show that the condition $d|mn$ is enough for each of the defined sets to be an order. In particular, $\mathcal{O}(1, 1, 1) = \mathbf{M}(2, \mathbb{Z})$ is a maximal order. Even though it is not true that every order of $\mathbf{M}(2, \mathbb{Q})$ belongs to the family of orders $\mathcal{O}(m, n, d)$, every order of $\mathbf{M}(2, \mathbb{Q})$ is included in a maximal order. Moreover, since $\mathbb{Z}$ is principal, two maximal orders of $\mathbf{M}(2, \mathbb{Q})$ are always conjugate.

Not every order $\mathcal{O}$ contained in $\mathbf{M}(2, \mathbb{Z})$ belongs to the family $\mathcal{O}(m, n, d)$. However, it is always such that $\mathcal{O}(m', n', d') \subset \mathcal{O} \subset \mathcal{O}(m'', n'', d'')$ for some integers $m', n', d', m'', n'', d''$. Hence, every order of $\mathbf{M}(2, \mathbb{Q})$ is isomorphic (via conjugation) to an order lying between two orders of the family $\mathcal{O}(m, n, d)$. Thus, it is possible to study only the orders of the family $\mathcal{O}(m, n, d)$ to obtain the properties of many orders of $\mathbf{M}(2, \mathbb{Q})$ up to isomorphism.

Observe also that it makes sense to define parametric families of orders with three parameters. Since $\mathbb{Z}$ has always to be included in the order (we associate an element $x \in \mathbb{Z}$ to the diagonal matrix $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$), we can impose 1 to be an element of any basis, and have a parameter for each of the other 3 dimensions.

One particularity of this family of orders is that

$$\mathcal{O}(1,1,1) \supset \mathcal{O}(1,N,1) \supset \mathcal{O}(1,N,N) \supset \mathcal{O}(N,N,N) = \mathbb{Z} + N\mathcal{O}(1,1,1),$$

and these orders are such that, as abelian groups,

$$\mathcal{O}(1,1,1)/\mathcal{O}(1,N,1) \cong \mathcal{O}(1,N,1)/\mathcal{O}(1,N,N) \cong \mathcal{O}(1,N,N)/\mathcal{O}(N,N,N) \cong \mathbb{Z}/N\mathbb{Z}.$$

Moreover, these orders have a strong relationship with the congruence groups of $\mathbf{SL}(2,\mathbb{Z})$. For example, $\Gamma_0(N)$ is the group of units of $\mathcal{O}(1,N,1)$, $\Gamma_1(N)$ generates $\mathcal{O}(1,N,N)$, and $\Gamma(N)$ generates $\mathcal{O}(N,N,N)$ if N is odd and $\mathcal{O}(N,N,2N)$ is N is even.

In the case of the quaternion algebras, it is possible to find similar relations if we consider different families of orders, as we will see in the next chapter.

Chapter 2

Orders of Quaternion Algebras over $\mathbb{Q}$

In this chapter, we are going to study some families of orders of quaternion algebras over $\mathbb{Q}$. This chapter is separated in two main sections, each one of them dedicated to one of the two types of quaternion algebras over $\mathbb{Q}$ defined previously. This is because each type of quaternion algebra has certain particular properties that affect directly the structure of the orders. We will first state a result of [1] that gives some examples of Eichler orders of quaternion algebras over $\mathbb{Q}$.

Lemma 2.1. *Let p, q be different primes. Then,*

(I) $\mathcal{O}_M(1,N) := \mathbb{Z}\left[\mathbf{1}, \frac{\mathbf{j}+\mathbf{k}}{2}, N\frac{-\mathbf{j}+\mathbf{k}}{2}, \frac{\mathbf{1}-\mathbf{i}}{2}\right]$ *is an Eichler order of level N in the matrix algebra $\left(\frac{1,-1}{\mathbb{Q}}\right)$ for every $N \geq 1$ square-free.*

(II) $\mathcal{O}_A(2p,N) := \mathbb{Z}\left[\mathbf{1}, \mathbf{i}, N\mathbf{j}, \frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}\right]$ *is an Eichler order of level N in the quaternion algebra $H_A(p)$, for $N|\frac{p-1}{2}$, N square-free.*

(III) $\mathcal{O}_B(pq,N) := \mathbb{Z}\left[\mathbf{1}, N\mathbf{i}, \frac{\mathbf{1}+\mathbf{j}}{2}, \frac{\mathbf{i}+\mathbf{k}}{2}\right]$ *is an Eichler order of level N, in the quaternion algebra $H_B(p,q)$, for $N|\frac{q-1}{4}$, $\gcd(N,p)=1$, N square-free.*

Proof. In all the cases, it is not difficult to check that the lattices are orders, and in every case the conditions on N make it coprime with the discriminant of the algebra. One can easily check the levels of the orders computing their discriminant using proposition 1.19, and deduce that all of them are Eichler orders using proposition 1.24. □

The two sections that follow have a pretty similar structure. First, we define some parametric families of lattices, deducing the conditions to be satisfied by the parameters for the lattices to be orders. A maximal order common to all quaternion algebras of the considered type is also computed. Finally, we get to see some interesting relations between the orders that have been found. Considering the structural similarity of both chapters, one might think that it could be more handy to merge them in order not to repeat statements and calculations. However, this separation is needed, because even though the final results obtained are pretty similar, the intermediate calculations differ considerably. In fact, the fact that we obtain such similar results for both A and B type quaternion algebras is remarkable itself.

2.1. Type A Quaternion Algebras

Recall that for us the type A quaternion algebras are the ones of the form $H_A(p) = \left(\frac{p,-1}{\mathbb{Q}}\right)$ such that $p \equiv 3 \mod 4$. In this whole section, we are only going to consider orders over such quaternion algebras. With the purpose of studying these orders, we will start considering the lattice $\mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \mathbf{j}, \frac{\mathbf{1+i+j+k}}{2}\right]$.

Proposition 2.2. *All the elements of the lattice $\mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \mathbf{j}, \frac{\mathbf{1+i+j+k}}{2}\right]$ are integral.*

Proof. Let $\alpha \in \mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \mathbf{j}, \frac{\mathbf{1+i+j+k}}{2}\right]$. Then, it is of the form

$$\alpha = \left(x + \frac{t}{2}\right) + \left(y + \frac{t}{2}\right)\mathbf{i} + \left(z + \frac{t}{2}\right)\mathbf{j} + \frac{t}{2}\mathbf{k}, \quad x, y, z, t \in \mathbb{Z}.$$

This element is integral, since $tr(\alpha) = 2x + t$ and

$$\begin{aligned} n(\alpha) &= \left(x + \frac{t}{2}\right)^2 - p\left(y + \frac{t}{2}\right)^2 + \left(z + \frac{t}{2}\right)^2 - p\frac{t^2}{4} \\ &= x^2 + xt - py^2 - pyt + z^2 + zt - \frac{p-1}{2}t^2. \end{aligned}$$

□

Definition 2.3. For every $m, n, d \in \mathbb{Z}$, we define the three following families of lattices:

- $\mathcal{O}_A(m,n,d) := \mathbb{Z}\left[\mathbf{1}, m\mathbf{i}, n\mathbf{j}, d\frac{\mathbf{1+i+j+k}}{2}\right]$;
- $\mathcal{O}'_A(m,n,d) := \mathbb{Z}\left[\mathbf{1}, m\mathbf{i}, n\mathbf{i}+\mathbf{j}, d\mathbf{i} + \frac{\mathbf{1+i+j+k}}{2}\right]$;
- $\mathcal{O}''_A(m,n,d) := \mathbb{Z}\left[\mathbf{1}, m\mathbf{i}, n\mathbf{i}+\mathbf{j}, d\frac{\mathbf{1+i+j+k}}{2}\right]$.

Remark 2.4. It is not claimed that $\mathcal{O}_A(m,n,d)$, $\mathcal{O}'_A(m,n,d)$ and $\mathcal{O}''_A(m,n,d)$ are orders for every m, n and d. In fact, it is not true. However, it is true for some of them; we will see later in which cases this happens.

Remark 2.5.

$$\mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \mathbf{j}, \frac{\mathbf{1+i+j+k}}{2}\right] = \mathcal{O}_A(1,1,1) = \mathcal{O}'_A(1,0,0) = \mathcal{O}''_A(1,0,1). \tag{2.1}$$

Remark 2.6. Note that since all the elements of $\mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \mathbf{j}, \frac{\mathbf{1+i+j+k}}{2}\right]$ are integral, every element of $\mathcal{O}_A(m,n,d)$, $\mathcal{O}'_A(m,n,d)$ and $\mathcal{O}''_A(m,n,d)$ is integral too, independently of the choice of m, n and d.

Proposition 2.7. *$O_A(m,n,d)$ is an order of $H_A(p)$ if and only if $m|nd$, $n|md\frac{p-1}{2}$ and $d|2mn$.*

Proof. In order to prove this, we only need to show that $O_A(m,n,d)$ is a ring, because we have already seen that every element is integral, and it is clear that it is a full lattice. For doing this, the only non-trivial thing to check is whether the product is internal or not (remember that $\mathbb{Z} \subseteq \mathcal{O}_A(m,n,d)$). Let us see under which conditions the product between elements of the lattice's basis belongs again to the lattice. Let $e_0 = \mathbf{1}, e_1 = m\mathbf{i}, e_2 = n\mathbf{j}$ and $e_3 = d\frac{\mathbf{1+i+j+k}}{2}$. Then:

- $e_0e_i = e_ie_0 = e_i$ for $i = 0, 1, 2, 3$.
- $e_0^2, e_1^2, e_2^2 \in \mathbb{Z}$.
- $e_3^2 = \frac{d^2}{4}(\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k})^2 = \frac{d^2}{4}(2p+2\mathbf{i}+2\mathbf{j}+2\mathbf{k}) = de_3 + d^2\frac{p-1}{2}e_0$.
- $e_1e_2 = -e_2e_1 = mn\mathbf{k} = \frac{2mn}{d}e_3 - mne_0 - ne_1 - me_2$. Hence, we need $d|2mn$.
- $e_1e_3 = \frac{md}{2}(\mathbf{i}+p+\mathbf{k}+p\mathbf{j}) = me_3 + \frac{p-1}{2}mde_0 + \frac{(p-1)}{2}\frac{md}{n}e_2$. Hence, we need $n|md\frac{p-1}{2}$.
- $e_3e_1 = \frac{md}{2}(\mathbf{i}+p-\mathbf{k}-p\mathbf{j}) = -e_3e_1 + pmde_0 + de_1$.
- $e_2e_3 = \frac{nd}{2}(\mathbf{j}-\mathbf{k}-\mathbf{1}+\mathbf{i}) = -ne_3 + de_2 + \frac{dn}{m}e_1$. Hence, we need $m|dn$.
- $e_3e_2 = \frac{nd}{2}(\mathbf{j}+\mathbf{k}-\mathbf{1}-\mathbf{i}) = -e_2e_3 - nde_0 + de_2$.

□

Let us briefly analyse what the conditions $m|nd$, $n|md\frac{p-1}{2}$ and $d|2mn$ mean. Let us first suppose that we have the (more restrictive) conditions $m|nd$, $n|md$ and $d|mn$, and let P be a prime number dividing m. Then, since $n|md$ and $d|mn$, either $P|n$ or $P|d$ (or both). Basically, this tells us that each prime factor has to divide at least two of the parameters. More precisely, if $P^r|m$, and $P^{r+1} \nmid n$ and $P^{r+1} \nmid d$, then $P^r|nd$. Going back to the conditions $m|nd$, $n|md\frac{p-1}{2}$ and $d|2mn$, we see that they mean the same, but with the additional allowance that d can have an additional factor 2, and n can have an additional factor x, with x a divisor of $\frac{p-1}{2}$.

Corollary 2.8. *$\mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \mathbf{j}, \frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}\right]$ is a maximal order for every type A quaternion algebra. We will call it $\mathcal{O}_A^{max}$.*

Proof. The fact that it is an order follows from the previous proposition. It is maximal because its discriminant coincides with the discriminant of the quaternion algebra, which is $2p$. One can check it using proposition 1.19, for example. □

Remark 2.9. Note that this was already stated in lemma 2.1.

Remark 2.10. Every maximal quaternion order of $H_A(p)$ is a conjugate of $\mathcal{O}_A^{max}$, as follows from proposition 1.21.

We have just seen in which cases $\mathcal{O}_A(m, n, d)$ is an order. For seeing in which cases $\mathcal{O}'_A(m, n, d)$ and $\mathcal{O}''_A(m, n, d)$ are orders, the proofs are quite similar to the previous one. Thus, we will only state the theorems, in order to avoid unnecessarily repetitive calculations and reasonings. Their proofs can be found in the appendix (propositions A.1 and A.2).

Proposition 2.11. *$\mathcal{O}'_A(m, n, d)$ is an order of $H_A(p)$ if and only if m is such that divides $2d^2 - 2dn + 2d - \frac{p-1}{2}n^2 - n + 1$.*

Proposition 2.12. *$\mathcal{O}''_A(m, n, d)$ is an order of $H_A(p)$ if and only if d divides $2m$ and m divides $d\left(\frac{p-1}{2}n^2 + n - 1\right)$.*

One question that now rises is which of the orders that we have found is an Eichler order. We know that there exist Eichler orders of level N for each N with $\gcd(N, D) = 1$, where D is the discriminant of the quaternion algebra (proposition 1.26). Hence, every order satisfying this property is a candidate for being an Eichler order. However, it is not easy to check if an order is the intersection of two maximal orders, following the definition of Eichler order. Instead, proposition 1.24 gives us a more useful tool for us to find Eichler orders belonging to our families of orders. If we find an order whose discriminant is square-free and not divisible by the discriminant of the quaternion algebra, it will be an Eichler order. For this purpose, recall that the discriminant of the quaternion algebra $H_A(p)$ equals $2p$.

Proposition 2.13. *If $\mathcal{O}_A(m, n, d)$, $\mathcal{O}'_A(m', n', d')$ and $\mathcal{O}''_A(m'', n'', d'')$ are orders, then their discriminants equal $2pmnd, 2pm'$ and $2pm''d''$, respectively.*

Proof. Using the second item of proposition 1.19 for instance, one can compute the discriminant of the orders $\mathcal{O}_A(m, n, d)$, $\mathcal{O}'_A(m', n', d')$ and $\mathcal{O}''_A(m'', n'', d'')$ to find that they are $2pmnd$ and $2pm'$ and $2pm''d''$, respectively. □

Proposition 2.14. *Consider the quaternion algebra $H_A(p)$. For every $m \in \mathbb{Z}$ square-free and such that $\gcd(2p, m) = 1$, there exist $n, d \in \mathbb{Z}$ such that $\mathcal{O}'_A(m, n, d)$ is an Eichler order.*

Proof. Recall that the condition to be satisfied for $\mathcal{O}'_A(m, n, d)$ to be an order is that m has to divide $2d^2 - 2dn + 2d - \frac{p-1}{2}n^2 - n + 1$. Hence, we only need to prove that for every m square-free and coprime with $2p$, there exist $n, d \in \mathbb{Z}$ making this divisibility condition hold. First, observe that, since $\gcd(m, 2) = 1$, our problem is equivalent to proving that there exist n, d satisfying the congruence

$$4d^2 - 4dn + 4d - pn^2 + n^2 - 2n + 2 \equiv 0 \mod m.$$

It is not difficult to check that the equality

$$(2d - n + 1)^2 - pn^2 + 1 = 4d^2 - 4dn + 4d - pn^2 + n^2 - 2n + 2$$

holds. Let us now suppose that m is prime, and let.

$$\mathcal{A} = \left\{x \in \mathbb{Z}/m\mathbb{Z} \mid x \equiv -pn^2 + 1 \mod m \quad \text{for some } n \in \mathbb{Z}\right\},$$
$$\mathcal{B}_n = \left\{x \in \mathbb{Z}/m\mathbb{Z} \mid x \equiv (2d - n + 1)^2 \mod m \quad \text{for some } d \in \mathbb{Z}\right\}.$$

Then, since $\gcd(p, m) = 1$, $\#\mathcal{A} = \frac{m+1}{2}$. Also, for some fixed n, and since m and 2 are coprime, $\#\mathcal{B}_n = \frac{m+1}{2}$. Actually, the set $\mathcal{B}_n$ is independent of n. Note that since m is prime, every element of $(\mathbb{Z}/m\mathbb{Z}) \setminus \{0\}$ is a unit of the finite field $(\mathbb{Z}/m\mathbb{Z})^*$. Suppose that there is no element in $\mathcal{A}$ such that its invere is in $\mathcal{B}_n$. This can only happen if $0 \in \mathcal{A} = \mathcal{B}_n$, and there exist n, d such that

$$(2d - n + 1)^2 - pn^2 + 1 \equiv 0 \mod m.$$

If some element of $\mathcal{A}$ has its inverse in $\mathcal{B}_n$, then there also clearly exist n, d satisfying the desired congruence.

Suppose now that m is a square-free integer. Then, the theorem follows from the Chinese remainder theorem. □

Corollary 2.15. *Consider the quaternion algebra $H_A(p)$. For every $m \in \mathbb{Z}$ square-free and coprime with p there exists an Eichler order of level m belonging to the family $\mathcal{O}'_A$.*

Proof. Follows from the previous proposition, proposition 1.24 and the fact that the discriminant of $\mathcal{O}'_A(m,n,d)$ equals $2mp$. □

Remark 2.16. We do not claim that every Eichler order belongs to this family. Also, if we check proposition 1.26, we see that we are not considering the Eichler orders whose level is divisible by a square.

Remark 2.17. Consider the quaternion algebra $H_A(p)$, and let m be a square-free integer coprime with $2p$. We have seen that if $\mathcal{O}'_A(m,n,d)$ is an Eichler order, its level equals m. From proposition 1.24, we deduce that each Eichler order of level m is a conjugate of $\mathcal{O}'_A(m,n,d)$.

Proposition 2.18. *The order $\mathcal{O}_A(m,m,m)$ is an order contained in $\mathcal{O}'_A(m,n,d)$.*

Proof. Proposition 2.7 tells us that $\mathcal{O}_A(m,m,m)$ is an order, and the inclusion follows from the fact that

$$m\mathbf{j} = m\cdot(n\mathbf{i}+\mathbf{j}) - n\cdot\mathbf{i},$$
$$m\frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} = m\cdot\left(d\mathbf{i}+\frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}\right) - d\cdot m\mathbf{i}.$$

□

Proposition 2.19. *Let $n \geq 1$ be an integer. Then, $\mathbb{Z} + n\mathcal{O}_A^{max} = \mathcal{O}_A(n,n,n)$.*

Proof. Just observe that the sets

$$\left\{\left(v+n\left(x+\frac{t}{2}\right)\right)+n\left(y+\frac{t}{2}\right)\mathbf{i}+n\left(z+\frac{t}{2}\right)\mathbf{j}+n\frac{t}{2}\mathbf{k} \;:\; x,y,z,t,v\in\mathbb{Z}\right\},$$
$$\left\{\left(x+n\frac{t}{2}\right)+\left(ny+n\frac{t}{2}\right)\mathbf{i}+\left(nz+n\frac{t}{2}\right)\mathbf{j}+n\frac{t}{2}\mathbf{k} \;:\; x,y,z,t\in\mathbb{Z}\right\}$$

are equal, because $\{v+nx \;:\; v,x\in\mathbb{Z}\} = \mathbb{Z}$. □

Proposition 2.20. *Let $\mathcal{O}'_A(m,n,d)$ be an order of a quaternion algebra $H_A(p)$. Then, $\mathcal{O}''_A(m,n',m)$ is an order such that*

$$\mathcal{O}_A^{max} \supset \mathcal{O}'_A(m,n,d) \supset \mathcal{O}''_A(m,n',m) \supset \mathcal{O}_A(m,m,m) = \mathbb{Z} + m\mathcal{O}_A^{max} \tag{2.2}$$

for every $n' \in \mathbb{Z}$.

Proof. Note first that, indeed, $\mathcal{O}''_A(m,n',m)$ is an order for every $n' \in \mathbb{Z}$. The inclusions of (2.2) are clear, since

$$m\frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} = m\cdot\left(d\mathbf{i}+\frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}\right) - d\cdot m\mathbf{i},$$
$$m\mathbf{j} = m\cdot(n'\mathbf{i}+\mathbf{j}) - n'\cdot m\mathbf{i}.$$

□

Proposition 2.21. *The following isomorphisms as abelian groups hold:*

(I) $\mathcal{O}_A^{max}/\mathcal{O}'_A(m,n,d) \cong \mathbb{Z}/m\mathbb{Z}$

(II) $\mathcal{O}'_A(m,n,d)/\mathcal{O}''_A(m,n,m) \cong \mathbb{Z}/m\mathbb{Z}$

(III) $\mathcal{O}''_A(m,n,m)/\mathcal{O}_A(m,m,m) \cong \mathbb{Z}/m\mathbb{Z}$

(IV) $\mathcal{O}_A^{max}/\mathcal{O}_A(m,n,d) \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z}$

Proof. Follows from the definitions of the orders. □

2.2. Type B Quaternion Algebras

In this section, we are going to proceed like in the previous one. In this case, however, we are going to consider B type quaternion algebras instead of A type quaternion algebras. This has a direct impact in the families of orders to be considered. Recall that B type quaternion algebras are of the form $H_B(p,q) = \left(\frac{p,q}{\mathbb{Q}}\right)$, with p,q primes such that $q \equiv 1 \mod 4$ and $\left(\frac{p}{q}\right) = -1$.

At first, one might be tempted to start with the lattice $\mathbb{Z}\left[\mathbf{1},\mathbf{i},\mathbf{j},\frac{\mathbf{1+i+j+k}}{2}\right]$, like in the previous section. However,

$$i \cdot \frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} = \frac{1}{2}(\mathbf{i}+p+\mathbf{k}+p\mathbf{j}) = \frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} + \frac{p-1}{2}(\mathbf{1}+\mathbf{j}).$$

Since in this case p might not be odd, this last equality means that the lattice is not necessarily a ring, and consequently not an order. Instead, we are going to start considering the lattice $\mathbb{Z}\left[\mathbf{1},\mathbf{i},\frac{\mathbf{1+j}}{2},\frac{\mathbf{i+k}}{2}\right]$.

Proposition 2.22. *Every element of the lattice* $\mathbb{Z}\left[\mathbf{1},\mathbf{i},\frac{\mathbf{1+j}}{2},\frac{\mathbf{i+k}}{2}\right]$ *is integral.*

Proof. Let $\alpha \in \mathbb{Z}\left[\mathbf{1},\mathbf{i},\frac{\mathbf{1+j}}{2},\frac{\mathbf{i+k}}{2}\right]$. Then, it is of the form

$$\alpha = \left(x+\frac{z}{2}\right) + \left(y+\frac{t}{2}\right)\mathbf{i} + \frac{z}{2}\mathbf{j} + \frac{t}{2}\mathbf{k}, \quad x,y,z,t \in \mathbb{Z}.$$

This means that $tr(\alpha) = 2x+z$ and

$$\begin{aligned} n(\alpha) &= \left(x+\frac{z}{2}\right)^2 - p\left(y+\frac{t}{2}\right)^2 - q\frac{z^2}{4} + pq\frac{t^2}{4} \\ &= x^2 + xz - py^2 - pyt + \frac{(q-1)}{4}(pt^2 - z^2). \end{aligned}$$

Hence, α is integral. □

Definition 2.23. For every $m,n,d \in \mathbb{Z}$, we consider the lattices

- $\mathcal{O}_B(m,n,d) := \mathbb{Z}\left[\mathbf{1}, m\mathbf{i}, n\frac{\mathbf{1+j}}{2}, d\frac{\mathbf{i+k}}{2}\right]$;
- $\mathcal{O}'_B(m,n,d) := \mathbb{Z}\left[\mathbf{1}, m\mathbf{i}, n\mathbf{i}+\frac{\mathbf{1+j}}{2}, d\mathbf{i}+\frac{\mathbf{i+k}}{2}\right]$;

- $\mathcal{O}''_B(m,n,d) := \mathbb{Z}\left[\mathbf{1}, m\mathbf{i}, n\mathbf{i} + \frac{\mathbf{i}+\mathbf{j}}{2}, d\frac{\mathbf{i}+\mathbf{k}}{2}\right]$.

Remark 2.24. Again, it is not claimed that the lattices $\mathcal{O}_B(m,n,d)$, $\mathcal{O}''_B(m,n,d)$ and $\mathcal{O}'_B(m,n,d)$ are orders for every m,n and d. It is true for some of them though.

Remark 2.25.

$$\mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \frac{\mathbf{1}+\mathbf{j}}{2}, \frac{\mathbf{i}+\mathbf{k}}{2}\right] = \mathcal{O}_B(1,1,1) = \mathcal{O}'_B(1,0,0) = \mathcal{O}''_B(1,0,1) \tag{2.3}$$

Remark 2.26. Every element of $\mathcal{O}_B(m,n,d)$, $\mathcal{O}''_B(m,n,d)$ and $\mathcal{O}'_B(m,n,d)$ is integral for every m, n and d, as all of these lattices are sublattices of $\mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \frac{\mathbf{1}+\mathbf{j}}{2}, \frac{\mathbf{i}+\mathbf{k}}{2}\right]$.

Let us proceed to state in which cases the lattices defined in 2.23 are orders. As has already been done in the previous chapter, the proofs are now omitted, but can be found in the appendix (A.3, A.4, A.5).

Proposition 2.27. *$\mathcal{O}_B(m,n,d)$ is an order of $H_B(p,q)$ if and only if $m|nd^{\frac{q-1}{4}}$, $n|md$ and $d|mn$.*

Corollary 2.28. *$\mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \frac{\mathbf{1}+\mathbf{j}}{2}, \frac{\mathbf{i}+\mathbf{k}}{2}\right]$ is a maximal order for every type B quaternion algebra. We will call it $\mathcal{O}_B^{max}$.*

Proof. Follows from the previous proposition and the fact that the discriminant of the order coincides with the discriminant of the algebra. □

Remark 2.29. $\mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \frac{\mathbf{1}+\mathbf{j}}{2}, \frac{\mathbf{i}+\mathbf{k}}{2}\right]$ is not an order in any A type quaternion algebra, because

$$\frac{\mathbf{1}+\mathbf{j}}{2} \cdot \frac{\mathbf{i}+\mathbf{k}}{2} = \frac{\mathbf{i}+\mathbf{k}-\mathbf{k}+\mathbf{i}}{4} = \frac{\mathbf{i}}{2} \notin \mathbb{Z}\left[\mathbf{1}, \mathbf{i}, \frac{\mathbf{1}+\mathbf{j}}{2}, \frac{\mathbf{i}+\mathbf{k}}{2}\right].$$

Remark 2.30. Note that for both A and B types of quaternion algebras, if our maximal orders have been defined as $\mathbb{Z}[\mathbf{1}, e_1, e_2, e_3]$, then for $\mathbb{Z}[\mathbf{1}, me_1, ne_2, de_3]$ to be an order we have obtained very similar divisibility conditions. In particular, the cases in which $m|nd, n|md$ and $d|mn$ yield orders in both cases.

Proposition 2.31. *$\mathcal{O}'_B(m,n,d)$ is an order of $H_B(p,q)$ if and only if m is such that divides $\frac{q-1}{4} + pn^2 - d^2 - d$.*

Proposition 2.32. *$\mathcal{O}''_B(m,n,d)$ is an order of $H_B(p,q)$ if and only if d divides m and m divides $n^2p + \frac{q-1}{4}$.*

Recall that the discriminant of the B type quaternion algebras $H_B(p,q)$ equals pq. Similarly as in the previous section, we obtain the following proposition.

Proposition 2.33. *If $\mathcal{O}_B(m,n,d)$, $\mathcal{O}'_B(m',n',d')$ and $\mathcal{O}''_B(m'',n'',d'')$ are orders, then their discriminants equal $pqmnd, pqm'$ and $pqm''d''$, respectively.*

Proof. Using the second item of proposition 1.19 for instance, one can compute the discriminant of the orders $\mathcal{O}_B(m,n,d)$, $\mathcal{O}'_B(m',n',d')$ and $\mathcal{O}''_B(m'',n'',d'')$ to find that they are $pqmnd$ and pqm' and $pqm''d''$, respectively. □

As in the previous section, we are interested in finding Eichler orders among the orders of our families. Analysing the orders of the family $\mathcal{O}'_B$, we get the same result as for the type A quaternion algebras:

Proposition 2.34. *Consider the quaternion algebra $H_B(p,q)$. For every $m \in \mathbb{Z}$ square-free and such that $\gcd(pq,m)=1$, there exist $n,d \in \mathbb{Z}$ such that $\mathcal{O}'_B(m,n,d)$ is an Eichler order.*

Proof. The statement is equivalent to proving that for every m square-free and coprime with pq, there exist $n,d \in \mathbb{Z}$ such that the congruence

$$\frac{q-1}{4} + pn^2 - d^2 - d \equiv 0 \mod m \tag{2.4}$$

holds. Let m be a prime number such that $\gcd(m,pq)=1$, and consider the sets

$$\mathcal{A} = \left\{ x \in \mathbb{Z}/m\mathbb{Z} \mid x \equiv \frac{q-1}{4} + pn^2 \mod m \quad \text{for some } n \in \mathbb{Z} \right\}$$
$$\mathcal{B} = \left\{ x \in \mathbb{Z}/m\mathbb{Z} \mid x \equiv d^2 + d \mod m \quad \text{for some } d \in \mathbb{Z} \right\}$$

If $m=2$, then $\mathcal{A} = \mathbb{Z}/m\mathbb{Z}$. If m is an odd prime, then $\#\mathcal{A} = \frac{m+1}{2}$, because m and p are coprime. For proving that $\#\mathcal{B} = \frac{p+1}{2}$, just note that if $x,y \in \mathbb{Z}/m\mathbb{Z}$ are such that $x^2+x = y^2+y$, then $(x+y+1)(x-y)=0$, meaning that either $x=y$ or $x=-y-1$. Hence, with the same reasoning used in proposition 2.14, we deduce that there exist n,d such that equation (2.4) holds. The statement for a non-prime m follows now from the Chinese remainder theorem. □

Corollary 2.35. *Consider the quaternion algebra $H_B(p,q)$. For every $m \in \mathbb{Z}$ square-free and coprime with pq there exists an Eichler order of level m belonging to the family $\mathcal{O}'_B$.*

Proof. Follows from the previous proposition, proposition 1.24 and the fact that the discriminant of the order $\mathcal{O}'_B(m,n,d)$ equals mpq. □

Proposition 2.36. *$\mathcal{O}_B(m,m,m)$ is an order contained in $\mathcal{O}'_B(m,n,d)$.*

Proof. Just note that $\mathcal{O}_B(m,m,m)$ is an order (proposition 2.27) and that

$$m\frac{\mathbf{1}+\mathbf{j}}{2} = m \cdot \left(n\mathbf{i} + \frac{\mathbf{1}+\mathbf{j}}{2} \right) - n \cdot m\mathbf{i},$$
$$m\frac{\mathbf{i}+\mathbf{k}}{2} = m \cdot \left(d\mathbf{i} + \frac{\mathbf{i}+\mathbf{k}}{2} \right) - d \cdot m\mathbf{i}.$$

□

Proposition 2.37. *Let $n \geq 1$ be an integer. Then, $\mathbb{Z} + n\mathcal{O}_B^{max} = \mathcal{O}_B(n,n,n)$.*

Proof. Similarly as in the previous chapter, it is enough to observe that the sets

$$\left\{ \left(v + n\left(x + \frac{z}{2} \right) \right) + n\left(y + \frac{t}{2} \right)\mathbf{i} + n\frac{z}{2}\mathbf{j} + n\frac{t}{2}\mathbf{k} \ : \ x,y,z,t,v \in \mathbb{Z} \right\},$$
$$\left\{ \left(x + n\frac{z}{2} \right) + \left(ny + n\frac{t}{2} \right)\mathbf{i} + n\frac{z}{2}\mathbf{j} + n\frac{t}{2}\mathbf{k} \ : \ x,y,z,t \in \mathbb{Z} \right\}$$

are equal. □

Proposition 2.38. *Let $\mathcal{O}'_B(m,n,d)$ be an Eichler order. For every $n' \in \mathbb{Z}$, the lattice $\mathcal{O}''_B(m,n',m)$ is an order such that*

$$\mathcal{O}_B^{max} \supset \mathcal{O}'_B(m,n,d) \supset \mathcal{O}''_B(m,n',m) \supset \mathcal{O}_B(m,m,m) = \mathbb{Z} + m\mathcal{O}_B^{max}. \tag{2.5}$$

Proof. The inclusions are clear, since

$$m\frac{\mathbf{i}+\mathbf{k}}{2} = m \cdot \left(d\mathbf{i} + \frac{\mathbf{i}+\mathbf{k}}{2} \right) - d \cdot m\mathbf{i}$$

and

$$m\frac{\mathbf{1}+\mathbf{j}}{2} = m \cdot \left(n'\mathbf{i} + \frac{\mathbf{1}+\mathbf{j}}{2} \right) - n' \cdot m\mathbf{i}.$$

The fact that $\mathcal{O}''_B(m,n',m)$ is an order for every n' is also clear. □

Proposition 2.39. *The following isomorphisms as additive groups hold:*

(I) $\mathcal{O}_B^{max}/\mathcal{O}'_B(m,n,d) \cong \mathbb{Z}/m\mathbb{Z}$

(II) $\mathcal{O}'_B(m,n,d)/\mathcal{O}''_B(m,n,m) \cong \mathbb{Z}/m\mathbb{Z}$

(III) $\mathcal{O}''_B(m,n,m)/\mathcal{O}_B(m,m,m) \cong \mathbb{Z}/m\mathbb{Z}$

(IV) $\mathcal{O}_B^{max}/\mathcal{O}_B(m,n,d) \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z}$

Proof. Follows directly from the definition of the orders. □

Appendix A

Proving that some Lattices are Orders

This appendix contains some of the proofs that have been omitted in sections 2.1 and 2.2. They have been omitted in order to avoid repetition of arguments, since all of them are very similar proofs to proposition 2.7's proof. Some of the calculations needed for these proofs follow.

Proposition A.1. *$\mathcal{O}'_A(m,n,d)$ is an order of $H_A(p)$ if and only if m is such that divides $2d^2-2dn+2d-\frac{p-1}{2}n^2-n+1$.*

Proof. We just need to check that the multiplication is an internal operation, because we know that the elements of $\mathcal{O}'_A(m,n,d)$ are integral. Let us check that the multiplication between elements of the basis lies again in $\mathcal{O}'_A(m,n,d)$. Let $e_0=\mathbf{1}$, $e_1=m\mathbf{i}$, $e_2=n\mathbf{i}+\mathbf{j}$ and $e_3=d\mathbf{i}+\frac{\mathbf{1+i+j+k}}{2}$. Then:

- $e_0e_i=e_ie_0=e_i$ for $i=0,1,2,3$.
- $e_1^2=m^2pe_0$.
- $e_2^2=n^2p+n\mathbf{k}-n\mathbf{k}-1=(n^2p-1)e_0$.
- $e_3^2=d^2p+\frac{d}{2}(\mathbf{i}+p+\mathbf{k}+p\mathbf{j})+\frac{d}{2}(\mathbf{i}+p-\mathbf{k}-p\mathbf{j})+\frac{(\mathbf{1+i+j+k})^2}{4}=d^2p+d(p+\mathbf{i})+\frac{p+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}$ $=e_3+\left(\frac{p-1}{2}+pd(d+1)\right)e_0$.
- $e_1e_2=mnp+m\mathbf{k}=mnpe_0+2me_3-me_0-(2d+1)e_1-me_2+ne_1$.
- $e_2e_1=mnp-m\mathbf{k}=m(np+1)e_0-2me_3+me_2-(n-2d-1)e_1$.
- $e_1e_3=mdp+\frac{m}{2}(\mathbf{i}+p+\mathbf{k}+p\mathbf{j})=me_3+m(dp+\frac{p-1}{2})e_0+m\frac{p-1}{2}e_2-\left(n\frac{p-1}{2}+d\right)e_1$.
- $e_3e_1=mdp+\frac{m}{2}(\mathbf{i}+p-\mathbf{k}-p\mathbf{j})=-e_1e_3+2mdpe_0+mpe_0+m\mathbf{i}$.
- $e_2e_3=ndpe_0+\frac{n}{2}(\mathbf{i}+p+\mathbf{k}+p\mathbf{j})-d\mathbf{k}+\frac{1}{2}(\mathbf{j}-\mathbf{k}-\mathbf{1}+\mathbf{i})$, with
  - $\frac{n}{2}(\mathbf{i}+p+\mathbf{k}+p\mathbf{j})=ne_3+\frac{p-1}{2}ne_0+\frac{p-1}{2}ne_2-\frac{n^2}{m}\frac{p-1}{2}e_1-\frac{nd}{m}e_1$;
  - $d\mathbf{k}=2de_3-de_0-de_2+\frac{dn}{m}e_1-\frac{2d^2+d}{m}e_1$;
  - $\frac{1}{2}(\mathbf{j}-\mathbf{k}-\mathbf{1}+\mathbf{i})=-e_3+e_2-\frac{n}{m}e_1+\frac{d+1}{m}e_1$.

Adding all the terms, $e_2e_3 = X + \frac{1}{m}\left(\frac{p-1}{2}n^2 - 2dn + 2d^2 + 2d + 1 - n\right)$, with X belonging to the lattice. Hence, we need m to divide $2d^2 - 2dn + 2d - \frac{p-1}{2}n^2 - n + 1$.

- $e_3e_2 = dnp + d\mathbf{k} + \frac{n}{2}(\mathbf{i} + p - \mathbf{k} - p\mathbf{j})\frac{1}{2}(\mathbf{j} + \mathbf{k} - \mathbf{1} - \mathbf{i})$. Note that this is equal to $-e_2e_3 + 2dnpe_0 + n(p + \mathbf{i}) + (\mathbf{j} - \mathbf{1})$, with $n(\mathbf{i} + p) = npe_0 + \frac{n}{m}e_1$ and $\mathbf{j} - \mathbf{1} = -e_0 + e_2 - \frac{n}{m}e_1$.

□

Proposition A.2. *$\mathcal{O}''_A(m, n, d)$ is an order of $H_A(p)$ if and only if $d|2m$ and m is such that divides $d\left(\frac{p-1}{2}n^2 + n - 1\right)$.*

Proof. We just need to check that the multiplication is an internal operation, because we know that the elements of $\mathcal{O}''_A(m, n, d)$ are integral. Let us check that the multiplication between elements of the basis lies again in $\mathcal{O}''_A(m, n, d)$. Let $e_0 = \mathbf{1}$, $e_1 = m\mathbf{i}$, $e_2 = n\mathbf{i} + \mathbf{j}$ and $e_3 = d\frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}$. Then:

- $e_0e_i = e_ie_0 = e_i$ for $i = 0, 1, 2, 3$.
- $e_1^2 = m^2pe_0$.
- $e_2^2 = (n^2p - 1)e_0$, as seen in proposition A.1's proof.
- $e_3^2 = de_3 + d^2\frac{p-1}{2}e_0$, as seen in proposition 2.7's proof.
- $e_1e_2 = mnp + m\mathbf{k} = mnpe_0 + \frac{2m}{d}e_3 - me_0 - (me_2 - ne_1) - e_1$. Thus, we need d to divide $2m$.
- $e_2e_1 = mnp - m\mathbf{k} = -e_1e_2 + 2mnpe_0$.
- $e_1e_3 = \frac{md}{2}(\mathbf{i} + p + \mathbf{k} + p\mathbf{j}) = me_3 + m\frac{p-1}{2}e_0 + m\frac{p-1}{2}e_2 - n\frac{p-1}{2}e_1$.
- $e_3e_1 = \frac{md}{2}(\mathbf{i} + p - \mathbf{k} - p\mathbf{j}) = -e_1e - 3 + mde_0 + de_1$.
- $e_2e_3 = \frac{nd}{2}(\mathbf{i} + p + \mathbf{k} + p\mathbf{j}) + \frac{d}{2}(\mathbf{j} - \mathbf{k} - \mathbf{1} + \mathbf{i})$, with
  - $\frac{nd}{2}(\mathbf{i} + p + \mathbf{k} + p\mathbf{j}) = ne_3 + nd\frac{p-1}{2}e_0 + nd\frac{p-1}{2}e_2 - \frac{n^2d}{m}\frac{p-1}{2}e_1$,
  - $\frac{d}{2}(\mathbf{j} - \mathbf{k} - \mathbf{1} + \mathbf{i}) = -e_3 + \frac{d}{m}e_1 + de_2 - \frac{nd}{m}e_1$.

  If we now add both terms, we see that m has to divide $d\left(n^2\frac{p-1}{2} + n - 1\right)$.
- $e_3e_2 = \frac{nd}{2}(\mathbf{i} + p - \mathbf{k} - p\mathbf{j}) + \frac{d}{2}(\mathbf{j} + \mathbf{k} - \mathbf{1} - \mathbf{i}) = -e_2e_3 + d(n\mathbf{i} + np + \mathbf{j} - \mathbf{1})$, where $n\mathbf{i} = \frac{n}{m}e_1$ and $\mathbf{j} = e_2 - \frac{n}{m}e_1$ (recall that m divides d).

□

Proposition A.3. *$\mathcal{O}_B(m, n, d)$ is an order of $H_B(p, q)$ if and only if $m|nd\frac{q-1}{4}$, $n|md$ and $d|mn$.*

Proof. We just need to check that the multiplication is an internal operation, because we know that the elements of $\mathcal{O}_B(m, n, d)$ are integral. Let us check that the multiplication between elements of the basis lies again in $\mathcal{O}_B(m, n, d)$. Let $e_0 = \mathbf{1}$, $e_1 = m\mathbf{i}$, $e_2 = n\frac{\mathbf{1}+\mathbf{j}}{2}$ and $e_3 = d\frac{\mathbf{i}+\mathbf{k}}{2}$. Then:

- $e_0e_i = e_ie_0 = e_i$ for $i = 0, 1, 2, 3$.
- $e_1^2 = m^2pe_0$.
- $e_2^2 = \frac{n^2}{4}(\mathbf{1} + 2\mathbf{j} + q) = n^2\frac{q-1}{4}e_0 + ne_2$.
- $e_3^2 = \frac{d^2}{4}(p + p\mathbf{j} - p\mathbf{j} - pq) = -pd^2\frac{q-1}{4}e_0$.
- $e_1e_2 = \frac{mn}{2}(\mathbf{i} + \mathbf{k}) = \frac{mn}{d}e_3$. Hence, we need d to divide mn.
- $e_2e_1 = \frac{mn}{2}(-\mathbf{k} + \mathbf{i}) = -e_1e_2 + ne_1$.
- $e_1e_3 = \frac{md}{2}p(\mathbf{1} + \mathbf{j}) = \frac{md}{n}pe_2$. Hence, we need n to divide md.
- $e_3e_1 = \frac{md}{2}p(\mathbf{1} - \mathbf{j}) = -e_1e_3 + pmde_0$.
- $e_2e_3 = \frac{nd}{4}(\mathbf{i} + \mathbf{k} - \mathbf{k} - q\mathbf{i}) = \frac{1-q}{4}\frac{nd}{m}e_1$. Hence, we need m to divide $\frac{q-1}{4}nd$.
- $e_3e_2 = \frac{nd}{4}(\mathbf{i} + \mathbf{k} + \mathbf{k} + q\mathbf{i}) = -e_2e_3 + ne_3$.

□

Proposition A.4. *$\mathcal{O}'_B(m, n, d)$ is an order of $H_B(p, q)$ if and only if m is such that divides $\frac{q-1}{4} + pn^2 - d^2 - d$.*

Proof. We just need to check that the multiplication is an internal operation, because we know that the elements of $\mathcal{O}'_B(m, n, d)$ are integral. Let us check that the multiplication between elements of the basis lies again in $\mathcal{O}'_B(m, n, d)$. Let $e_0 = \mathbf{1}$, $e_1 = m\mathbf{i}$, $e_2 = n\mathbf{i} + \frac{\mathbf{1}+\mathbf{j}}{2}$ and $e_3 = d\mathbf{i} + \frac{\mathbf{i}+\mathbf{k}}{2}$. Then:

- $e_0e_i = e_ie_0 = e_i$ for $i = 0, 1, 2, 3$.
- $e_1^2 = m^2pe_0$.
- $e_2^2 = n^2p + n\frac{\mathbf{i}+\mathbf{k}}{2} + n\frac{\mathbf{i}-\mathbf{k}}{2} + \frac{1+2\mathbf{j}+q}{4} = \frac{q-1}{4}e_0 + e_2$.
- $e_3^2 = d^2p + d\frac{p+p\mathbf{j}}{2} + d\frac{p-p\mathbf{j}}{2} + \frac{p+p\mathbf{j}-p\mathbf{j}-pq}{4} \in \mathbb{Z}$.
- $e_1e_2 = mnp + m\frac{\mathbf{i}+\mathbf{k}}{2} = mnpe_0 + me_3 - de_1$.
- $e_2e_1 = mnp + m\frac{\mathbf{i}-\mathbf{k}}{2} = -e_1e_2 + 2mnpe_0 + e_1$.
- $e_1e_3 = mdp + \frac{p+p\mathbf{j}}{2} = mdpe_0 + mpe_2 - ne_1$.
- $e_3e_1 = mdp + \frac{p-p\mathbf{j}}{2} = -e_1e_3 + 2mdpe_0 + mpe_0$.
- $e_2e_3 = ndp + np\frac{\mathbf{1}+\mathbf{j}}{2} + d\frac{\mathbf{i}-\mathbf{k}}{2} + \frac{\mathbf{i}+\mathbf{k}-\mathbf{k}-q\mathbf{i}}{4}$, where
  - $np\frac{\mathbf{1}+\mathbf{j}}{2} = npe_2 - \frac{pn^2}{m}e_1$,
  - $d\frac{\mathbf{i}-\mathbf{k}}{2} = -de_3 + \frac{d}{m}e_1 + \frac{d^2}{m}e_1$,
  - $\frac{\mathbf{i}-q\mathbf{i}}{4} = -\frac{1}{m}\frac{q-1}{4}e_1$.

If we add everything, we get that m has to divide $\frac{q-1}{4} + pn^2 - d^2 - d$.

- $e_3e_2 = ndp + d\frac{\mathbf{i}+\mathbf{k}}{2} + np\frac{\mathbf{1}-\mathbf{j}}{2} + \frac{\mathbf{i}+\mathbf{k}+\mathbf{k}+q\mathbf{i}}{4} = -e_2e_3 + 2ndpe_0 + npe_0 + e_3$.

□

Proposition A.5. *$\mathcal{O}''_B(m,n,d)$ is an order of $H_B(p,q)$ if and only if the divisibility conditions $d|m$ and $m|d\left(n^2p + \frac{q-1}{4}\right)$ hold.*

Proof. Since all the elements of $\mathcal{O}''_B(m,n,d)$ are integral, we just need to see that the multiplication is an internal operation, checking that the multiplication between elements of the basis lies again in $\mathcal{O}''_B(m,n,d)$. Let $e_0 = \mathbf{1}$, $e_1 = m\mathbf{i}$, $e_2 = n\mathbf{i} + \frac{\mathbf{1}+\mathbf{j}}{2}$ and $e_3 = d\frac{\mathbf{i}+\mathbf{k}}{2}$.

- $e_0e_i = e_ie_0 = e_i$ for $i = 0,1,2,3$.
- $e_1^2 = m^2pe_0$.
- $e_2^2 = \frac{q-1}{4}e_0 + e_2$, as has been seen in proposition A.4's proof.
- $e_3^2 \in \mathbb{Z}$, as has been seen in proposition A.3's proof.
- $e_1e_2 = mnp + m\frac{\mathbf{i}+\mathbf{k}}{2} = mnpe_0 + \frac{m}{d}e_3$. Hence, we need d to divide m.
- $e_2e_1 = mnp + m\frac{\mathbf{i}-\mathbf{k}}{2} = -e_1e_2 + 2mnpe_0 + e_1$.
- $e_1e_3 = mdp\frac{\mathbf{1}+\mathbf{j}}{2} = mdpe_2 - ndpe_1$.
- $e_3e_1 = mdp\frac{\mathbf{1}-\mathbf{j}}{2} = -e_1e_3 + mdpe_0$.
- $e_2e_3 = ndp\frac{\mathbf{1}+\mathbf{j}}{2} + d\frac{\mathbf{i}+\mathbf{k}-\mathbf{k}-q\mathbf{i}}{4} = ndpe_2 - \frac{n^2dp}{m}e_1 - \frac{q-1}{4}\frac{d}{m}e_1$. Hence, we need m to divide $d\left(n^2p + \frac{q-1}{4}\right)$.
- $e_3e_2 = ndp\frac{\mathbf{1}-\mathbf{j}}{2} + d\frac{\mathbf{i}+\mathbf{k}+\mathbf{k}+q\mathbf{i}}{4} = -e_2e_3 + ndpe_0 + e_3$.

□

Bibliography

[1] Alsina, M., Bayer, P.: *Quaternion Orders, Quadratic Forms, and Shimura Curves*. CRM Monograph Series, Volume 22. American Mathematical Society, 2004.

[2] Bayer, P., Travesa, A.: *Órdenes Matriciales Generados por Grupos de Congruencia*. Rev.R.Acad.Cienc.Exact.Gís.Nat, Vol. 94, N.3, pp 339-346, 2000.

[3] Deuring, M.: *Algebren. Zweite Auflage*. Springer-Verlag, 1968.

[4] Vignéras, M-F.: *Arithmétique des Algèbres de Quaternions*. Springer-Verlag, 1980.