Some explicit constructions of integral structures in quaternion algebras

M. Ciavarella, L. Terracini

February 2, 2008

Abstract

Let $B$ be an undefined quaternion algebra over $\mathbb{Q}$. Following the explicit characterization of some Eichler orders in $B$ given by Hashimoto, we define explicit embeddings of these orders in some local rings of matrices; we describe the two natural inclusions of an Eichler order of level $Nq$ in an Eichler order of level $N$. Moreover we provide a basis for a chain of Eichler orders in $B$ and prove results about their intersection.

AMS Mathematics Subject Classification: 11R52

1 Introduction

The aim of this work is to give an explicit description of the quaternion algebras over $\mathbb{Q}$ and of some of their Eichler orders. Let $B$ be a quaternion algebra over $\mathbb{Q}$ of discriminant $\Delta$ and let $B_q = B \otimes_{\mathbb{Q}} \mathbb{Q}_q$ be its localization at the prime number $q$. It is well known that if $q$ is a unramified place, then there is an isomorphism between $B_q$ and $M_2(\mathbb{Q}_q)$; if $B$ is ramified at $q$ then $B_q$ can be represented as a subalgebra of $M_2(\mathbb{Q}_q^{2e})$, where $\mathbb{Q}_q^{2e}$ denotes the quadratic unramified extension of $\mathbb{Q}_q$, as described in [4]. In the general literature on quaternion algebras Eichler orders are defined by using these local isomorphisms. In [3] an explicit definition of an Eichler orders $R(N)$ of level $N$ is given. The author fixes a representation of the quaternion algebra $B$ as a pair $\{-\Delta N, p\}$ and gives a basis of the Eichler order $R(N)$ depending on this representation. This construction provides a very useful tool for working with Eichler orders. However, for our purposes, it has the limitation of not respecting the natural inclusion of an Eichler order of level $M$ in an Eichler order of level $N$ for $N$ dividing $M$. Starting from the
work of Hashimoto, we then provide an explicit description of Eichler orders $R(N)$ and $R(Nq)$, and of the two natural inclusion maps $R(Nq) \to R(N)$.

More precisely, for any prime number $q$, we will describe an isomorphisms $\varphi_q$ between $B_q$ and the corresponding matrix algebra and we will write the image of $R_q(N)$ under $\varphi_q$. We characterize two copies of $R(Nq)$ in $R(N)$ by using these local isomorphisms, and we define a basis for each of them in terms of a basis of $R(N)$.

As in [7] we will consider the quaternionic analogue of the congruence groups $\Phi(N)$; we will express them by using our characterization of Eichler orders and we will prove some initial results for these groups.

Our interest in Eichler orders and groups $\Phi(N)$, arises from a difficulty encountered in some previous work on Galois representations and Hecke algebras arising from quaternionic groups [7], [1]: an analogue for Shimura curves of Ihara's lemma (which holds for modular curves) is missing. We briefly give a sketch of this open problem; for a deep overview of the status of art see [2].

For any integer number $N$, $\Phi(N)$ is defined as $(GL_2^+(\mathbb{R}) \times (R(N) \otimes \hat{\mathbb{Z}})^*) \cap B^\times$. Let we consider the Shimura curves $X(N)$ and $X(Nq)$ coming from $\Phi(N)$ and $\Phi(Nq)$ respectively, where $q$ is a prime number such that $q \nmid \Delta$. There are two injective maps from $\Phi(Nq)$ in $\Phi(N)$: the natural inclusion and the conjugation by a certain element $\delta_q \in B^\times$. These maps naturally induce degeneracy maps on cohomology; their direct sum provides a map $\alpha : H^1(X(N))^2 \to H^1(X(Nq))$ where cohomology has coefficients in the ring of integers of a suitable finite extension of $\mathbb{Q}_\ell$ for a fixed prime $\ell$. The conjecture in [2] asserts that $\alpha$ is injective with cokernel torsion free.

2 Preliminaries and notations

Let $B$ be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant $\Delta = p_1...p_t$ with $t$ a even number. We will denote by $(\frac{\cdot}{p})$ the Legendre symbol and by $(\cdot,\cdot)_q$ the Hilbert symbol at $q$ [3]. Let $N$ be a positive integer prime to $\Delta$ and $p$ be a prime number such that:

- $p \equiv 1 \mod 4$ and $p \equiv \begin{cases} 5 \mod 8 & \text{if } 2|\Delta \\ 1 \mod 8 & \text{if } 2|N \end{cases}$;
- $\left(\frac{p}{p_i}\right) = -1$ for each $p_i \neq 2$;
- $\left(\frac{q}{q}\right) = 1$ for each odd prime factor $q$ of $N$. 

2
We observe that the last condition implies that $p$ is a square in $\mathbb{Z}_q$ for any $q$ prime factor of $N$; since $p$ is not a square in $\mathbb{Z}_p$, then $p$ does not divide $N$. Hashimoto \[3\] shows that then $B \simeq \{-\Delta N, p\}$ (with the notations of \[8\]). This means that $B$ can be expressed as $B(N, p) = \mathcal{Q} + \mathcal{Q}i + \mathcal{Q}j + \mathcal{Q}k$ where $i^2 = -\Delta N, j^2 = p, k = ij = -ji$. Moreover by Theorem 2.2 of \[3\], an Eichler order of level $N$ of $B$ can be expressed as the $\mathbb{Z}$-lattice $R(N) = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 + \mathbb{Z}e_4$ with

$$e_1 = 1, \ e_2 = \frac{1+j}{2}, \ e_3 = \frac{i+k}{2}, \ e_4 = \frac{a\Delta N j + k}{p}$$

where $a \in \mathbb{Z}$ satisfies $a^2\Delta N + 1 \equiv 0 \mod p$.

We observe that $i, j, k$ depend on the choice of $N$ and $p$; in the sequel, whenever will be necessary to express the dependence on $N$ we will write $i^N, j^N, k^N$ instead of $i, j, k$ and $e_1^N, e_2^N, e_3^N, e_4^N$ instead of $e_1, e_2, e_3, e_4$.

We consider $R = R(1)$; then $R$ is a maximal order in $B$. For any prime number $q$, let we denote $B_q = B \otimes \mathcal{Q} \mathbb{Q}_q$ and $R_q(N) = R(N) \otimes \mathbb{Z} \mathbb{Z}_q$.

We start with a simple lemma which will be useful in the sequel.

**Lemma 2.1** Let $K$ be a field and let $B_1$, $B_2$ be two quaternion algebras over $K$. If there exist a non-zero homomorphism $\varphi : B_1 \rightarrow B_2$ then $\varphi$ is an isomorphism.

**Proof**

Since $B_1$ is a central simple algebra, it does not have non-trivial bilateral ideals so that $\varphi$ is injective, Then the dimension $\dim_K(\varphi(B_1)) = 4$ and $\varphi$ is an isomorphism.

**Corollary 2.1** Let $K$ be a field and $B_1$, $B_2$ be two quaternion algebras over $K$. We represent $B_1$ as $B_1 = K + Ki + Kj + Kk$ with $i^2, j^2 \in K$ and $k = ij = -ji$. Let $\varphi : B_1 \rightarrow B_2$ be a $K$-linear map such that

$$\varphi(1) = 1, \ \varphi(i)^2 = i^2, \ \varphi(j)^2 = j^2, \ \varphi(k) = \varphi(i)\varphi(j) = -\varphi(j)\varphi(i).$$

Then $\varphi$ is an isomorphism of $K$-algebras.

We will work with $K = \mathcal{Q}$ or $K = \mathbb{Q}_q$ for any place $q$ including $\infty$. We observe that to define in an explicit way an isomorphism of $K$-algebras $\varphi : B_q^N \rightarrow B'$ it is enough to define the values $\varphi(i), \varphi(j)$ such that $\varphi(i)^2 = -\Delta N, \varphi(j)^2 = p$ and $\varphi(i)\varphi(j) = -\varphi(j)\varphi(i)$. If we put $\varphi(1) = 1, \varphi(k) = \varphi(i)\varphi(j)$ and if we extend the map by $K$-linearity, then by Corollary 2.1 $\varphi$ is a well defined isomorphism of $K$-algebras.
3 The case of $M_2(\mathbb{Q})$

If $\Delta = 1$ then $B$ can be represented as $B(N,1) = \{-N,1\}$ where $N$ is any positive integer. It is well known that there is an isomorphism $\varphi^N : B \to M_2(\mathbb{Q})$ such that the image of the maximal order $R$ is $M_2(\mathbb{Z})$. Let us explicitly describe such an isomorphism. We consider the $\mathbb{Q}$-linear map $\varphi^N$ defined as follows:

$$\varphi^N(i) = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \quad \text{and} \quad \varphi^N(j) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$ 

Then

$$\varphi^N(i)^2 = -NI \quad \varphi^N(j)^2 = I$$

where $I$ is the identity $2 \times 2$ matrix,

$$\varphi^N(k) = \varphi^N(i)\varphi^N(j) = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -N & 1 \end{pmatrix} = -\varphi^N(j)\varphi^N(i).$$

It results that for any element $x + yi + zj + tk \in B(N,1)$ with $x, y, z, t \in \mathbb{Q}$

$$\varphi^N(x + iy + jz + kt) = \begin{pmatrix} x - z & -y - t \\ N(y - t) & x + z \end{pmatrix}$$

and by Corollary 2.1 the map $\varphi^N : B(N,p) \to M_2(\mathbb{Q})$ is an isomorphism. The image of the basis of the Eichler order $R(N)$ is:

$$\varphi^N(e_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\varphi^N(e_2) = \varphi^N\left(\frac{1 + j}{2}\right) = \frac{1}{2} \left[ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\varphi^N(e_3) = \varphi^N\left(\frac{i + k}{2}\right) = \frac{1}{2} \left[ \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} + \begin{pmatrix} 0 & -1 \\ -N & 0 \end{pmatrix} \right] = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$$

$$\varphi^N(e_4) = \varphi^N(Nj + k) = \begin{pmatrix} -N & 0 \\ 0 & N \end{pmatrix} + \begin{pmatrix} 0 & -1 \\ -N & 0 \end{pmatrix} = \begin{pmatrix} -N & -1 \\ -N & N \end{pmatrix}$$

and for any element $xe_1 + ye_2 + ze_3 + te_4 \in R(N)$ with $x, y, z, t \in \mathbb{Z}$

$$\varphi^N(xe_1 + ye_2 + ze_3 + te_4) = \begin{pmatrix} x - Nt & -z - t \\ -Nt & x + y + Nt \end{pmatrix}.$$
We observe that if $N > 1$, the reduced discriminant
$$\sqrt{|\det(\text{tr}(\varphi^N(e_k)\varphi^N(e_h)))|}$$
for $h, k = 1, \ldots, 4$ of $\varphi^N(R(N))$ is $N$ so that the image of $R(N)$ via $\varphi^N$ is
$$\varphi^N(R(N)) = \left\{ \gamma \in M_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}.$$

If $N = 1$ then $R(1)$ is a maximal order of $B = B^1$, the reduced discriminant of $\varphi^1(R)$ is:
$$\sqrt{\det \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 4 \end{pmatrix}} = 1 \quad (1)$$
and its image via $\varphi^1$ is $M_2(\mathbb{Z})$.

### 3.1 An isomorphism between $B(N, 1)$ and $B(M, 1)$

Let $B$ be a quaternion algebra of discriminant 1 and let $B(N, 1) = Q + Qi^N + Qj^N + Qk^N$ and $B(M, 1) = Q + Qi^M + Qj^M + Qk^M$ be two representations of $B$ where $N$ and $M$ are as in Section 2. We will write an isomorphism $\Psi^M_N : B(N, 1) \to B(M, 1)$.

We define $\Psi^M_N$ as the composite $(\varphi^M)^{-1} \circ \varphi^N$:
$$\Psi^M_N(i^N) = i^M \left( \frac{M + N}{2M} \right) + k^M \left( \frac{M - N}{2M} \right)$$
$$\Psi^M_N(j^N) = j^M$$
$$\Psi^M_N(k^N) = i^M \left( \frac{M - N}{2M} \right) + k^M \left( \frac{M + N}{2M} \right)$$

**Proposition 3.1** If $M$ is an integer such that $M|N$, then $\Psi^M_N(R(N)) \subset R(M)$.

**Proof** Let $N = SM$ with $S \in \mathbb{N}$. Then $\Psi^M_N(e_1^N) = e_1^M$, $\Psi^M_N(e_2^N) = e_2^M$, $\Psi^M_N(e_3^N) = e_3^M$ and $\Psi^M_N(e_4^N) = -(1 - S)e_3^M + Se_4^M$.

### 4 The case of discriminant $> 1$

We fix a prime $p$ and a positive integer $N$ as in Section 2. We represent the quaternion algebra $B$ of discriminant $\Delta$ as $B(N, p) = \{-\Delta N, p\} = Q + Qi + Qj + Qk$. For each prime $q$ we want to identify $B_q$ to a ring
of matrices, in such a way that the integer structure is preserved. Let us denote by \( \mathcal{R}_q(N) \) the subring of \( M_2(\mathbb{Z}_q) \) containing all the matrices of the form \( \left( \begin{array}{cc} Z_q & Z_q \\ N Z_q & Z_q \end{array} \right) \). We observe that if \( q \nmid N \) then \( \mathcal{R}_q(N) = M_2(\mathbb{Z}_q) \).

We recall that every local Eichler orders of level \( N \) in \( M_2(\mathbb{Q}_q) \) is isomorphic to \( \mathcal{R}_q(N) \) and its reduced discriminant is equal to \( \Delta N \).

We will deal separately with the cases of unramified places and of ramified places.

4.1 The isomorphism at the non-Archimedean unramified places

In this section let \( q \) be a prime number such that \( q \nmid \Delta \); since at \( q \) the quaternion algebra \( B(N, p) \) is not ramified, the Hilbert symbol is

\[ 1 = (-\Delta N, p)_q. \]  

We shall define an isomorphism \( \varphi^{(N, p)}_q : B(N, p)_q \cong M_2(\mathbb{Q}_q) \) such that \( \varphi^{(N, p)}_q(\mathcal{R}_q(N)) = \mathcal{R}_q(N) \). To make easier the notation we will write \( \varphi^N_q \) instead of \( \varphi^{(N, p)}_q \).

4.1.1 The isomorphism at places \( q \) not dividing \( \Delta p \) such that \( p \) is not a square in \( \mathbb{Z}_q^\times \)

We consider the case \( q \nmid \Delta p \) such that \( \left( \frac{p}{q} \right) = -1 \) (we observe that the last condition excludes the cases \( q = 2 \) and \( q|N \)). This hypotheses on \( q \) assure that \( p \) is not a square in \( \mathbb{Z}_q^\times \), thus \( \mathbb{Q}_q(\sqrt{p}) \) is a quadratic extension of \( \mathbb{Q}_q \) and by the identity (2), the prime \( -\Delta N \) is the norm of a unit of \( \mathbb{Q}_q(\sqrt{p}) \).

We write \( -\Delta N = x^2 - py^2 \) with \( x, y \in \mathbb{Z}_q \) and we define \( \varphi^N_q \) as follows:

\[ \varphi^N_q(i) = \left( \begin{array}{cc} x & -py \\ y & -x \end{array} \right), \quad \varphi^N_q(j) = \left( \begin{array}{cc} 0 & p \\ 1 & 0 \end{array} \right). \]

Then

\[ \varphi^N_q(i)^2 = -\Delta N I, \quad \varphi^N_q(j)^2 = pI \]

\[ \varphi^N_q(k) = \varphi^N_q(i)\varphi^N_q(j) = \left( \begin{array}{cc} -py & px \\ -x & py \end{array} \right) = -\varphi^N_q(j)\varphi^N_q(i). \]

It results that for any \( h = \alpha + \beta i + \gamma j + \delta k \in B_q(N, p) \)

\[ \varphi^N_q(h) = \left( \begin{array}{cc} \alpha + \beta x - \delta py & -\beta py + \gamma p + \delta xp \\ \beta y + \gamma - \delta x & \alpha - \beta x + \delta py \end{array} \right). \]
and by Corollary 2.1, \( \varphi_q^N : B_q \rightarrow M_2(\mathbb{Q}_q) \) is an isomorphism. The image of the basis of the local Eichler order is:

\[
\varphi_q^N(e_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\]

\[
\varphi_q^N(e_2) = \frac{1}{2} \begin{pmatrix} 1 & p \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{Z}_q) \text{ since } q \neq 2
\]

\[
\varphi_q^N(e_3) = \frac{1}{2} \begin{pmatrix} x - py & p(y - x) \\ y - x & -x + py \end{pmatrix} \in M_2(\mathbb{Z}_q) \text{ since } q \neq 2
\]

\[
\varphi_q^N(e_4) = \begin{pmatrix} \frac{-y}{a \Delta N - x} & a \Delta N + x \\ y & \end{pmatrix} \in M_2(\mathbb{Z}_q) \text{ since } q \neq p.
\]

The reduced discriminant of \( \varphi_q^N(R_q(N)) \) is \( \Delta N \). So \( \varphi_q^N(R_q(N)) = M_2(\mathbb{Z}_q) \).

Any element \( g = \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4 \in R_q(N) \)

\[
\varphi_q^N(g) = \begin{pmatrix} \alpha + \frac{\beta}{2} + \frac{\gamma}{2} (x - py) - \delta y \\ \frac{\beta}{2} + \frac{\gamma}{2} (y - x) + \delta a \Delta N - x \\ \alpha + \frac{\beta}{2} + \frac{\gamma}{2} (py - x) + \delta y \end{pmatrix}
\]

(3)

4.1.2 The isomorphism at primes \( q \) such that \( p \) is a square in \( \mathbb{Z}_q^\times \)

We consider the primes \( q \nmid \Delta \) such that \( \left( \frac{q}{p} \right) = 1 \). We observe that this hypothesis excludes the case \( q \mid N \) and includes \( q \mid N \) and \( q = 2 \) (in fact if \( q = 2 \) then by hypothesis \( p \equiv 1 \pmod{8} \) and by (2), II, §3) \( p \) is a square in \( \mathbb{Z}_2^\times \). We define the \( \mathbb{Q}_q \)-linear map \( \varphi_q^N \) as follows:

\[
\varphi_q^N(i) = \begin{pmatrix} 0 & 1 \\ -\Delta N & 0 \end{pmatrix} \text{ and } \varphi_q^N(j) = \begin{pmatrix} -\sqrt{p} & 0 \\ 0 & \sqrt{p} \end{pmatrix}
\]

where \( \sqrt{p} \) is an element \( \omega \) in \( \mathbb{Z}_q^\times \) such that \( \omega^2 = p \). Then

\[
\varphi_q^N(i)^2 = -\Delta NI \quad \varphi_q^N(j)^2 = pI
\]

\[
\varphi_q^N(k) = \varphi_q^N(i) \varphi_q^N(j) = \begin{pmatrix} 0 & \sqrt{p} \\ \Delta N \sqrt{p} & 0 \end{pmatrix} = -\varphi_q^N(j) \varphi_q^N(i).
\]

It results that for any element \( \alpha + \beta i + \gamma j + \delta k \in B_q \)

\[
\varphi_q^N(\alpha + \beta i + \gamma j + \delta k) = \begin{pmatrix} \alpha - \gamma \sqrt{p} & \beta + \delta \sqrt{p} \\ \Delta N(-\beta + \delta \sqrt{p}) & \alpha + \gamma \sqrt{p} \end{pmatrix}
\]
and by Corollary 2.1 \( \varphi^N_q : B_q(N,p) \to M_2(\mathbb{Q}_q) \) is an isomorphism. The image of a basis of the local Eichler order \( R_q(N) \) is:

\[
\varphi^N_q(e_1) = I \\
\varphi^N_q(e_2) = \begin{pmatrix}
\frac{1-\sqrt{p}}{2} & 0 \\
0 & \frac{1+\sqrt{p}}{2}
\end{pmatrix} \in \mathcal{R}_q(N) \\
\varphi^N_q(e_3) = \begin{pmatrix}
0 & \frac{1+\sqrt{p}}{2} \\
\Delta N(\sqrt{p}-1) & 0
\end{pmatrix} \in \mathcal{R}_q(N) \\
\varphi^N_q(e_4) = \frac{1}{\sqrt{p}} \begin{pmatrix}
-a\Delta N & 1 \\
\Delta N & a\Delta N
\end{pmatrix} \in \mathcal{R}_q(N)
\]

The reduced discriminant of \( \varphi^N_q(R_q(N)) \) is \( \Delta N \), so \( \varphi^N_q(R_q(N)) = \mathcal{R}_q(N) \). Then, for any element \( g = \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4 \in R_q(N) \)

\[
\varphi^N_q(g) = \begin{pmatrix}
\alpha + \frac{(1-\sqrt{p})\beta}{2} - \frac{\delta a\Delta N}{\sqrt{p}} \\
\gamma \Delta N \sqrt{p-1} + \frac{\delta a\Delta N}{\sqrt{p}} & \alpha + \frac{(1+\sqrt{p})\beta}{2} + \frac{\delta a\Delta N}{\sqrt{p}}
\end{pmatrix}.
\] (4)

We observe that in this case we accept that \( 2|N \).

4.1.3 The isomorphism at \( p \)

If \( q = p \) then \( 1 = (-\Delta N, p)_p = \left( \frac{-\Delta N}{p} \right) \) (3, II, §3). So \( -\Delta N \) is a square in \( \mathbb{Z}_p^* \). We recall that \( a \in \mathbb{Z} \) was chosen in Section 2 in such a way that \( a^2\Delta N + 1 \equiv 0 \mod p \). Let we denote by \( \sqrt[4]{-\Delta N} \) the square root of \( -\Delta N \) in \( \mathbb{Z}_p^* \) such that \( a\sqrt[4]{-\Delta N} \equiv -1 \mod p \). Then the following identity holds:

\[
(a\Delta N - \sqrt{-\Delta N}) = \sqrt{-\Delta N}(a\sqrt{-\Delta N} - 1) \equiv 0 \mod p. \tag{5}
\]

We define the \( \mathbb{Q}_p \)-linear map \( \varphi^N_p \) as follows:

\[
\varphi^N_p(i) = \begin{pmatrix}
-\sqrt{-\Delta N} & 0 \\
0 & \sqrt{-\Delta N}
\end{pmatrix} \quad \text{and} \quad \varphi^N_p(j) = \begin{pmatrix}
0 & 1 \\
p & 0
\end{pmatrix}.
\]

Then

\[
\varphi^N_p(i)^2 = -\Delta NI \quad \varphi^N_p(j)^2 = pI \\
\varphi^N_p(k) = \varphi^N_p(i)\varphi^N_p(j) = \begin{pmatrix}
0 & -\sqrt{-\Delta N} \\
p\sqrt{-\Delta N} & 0
\end{pmatrix} = -\varphi^N_p(j)\varphi^N_p(i).
\]
It results that for any element \( \alpha + \beta i + \gamma j + \delta k \in B_p(N, p) \)
\[
\varphi_p^N(\alpha + \beta i + \gamma j + \delta k) = \begin{pmatrix} \alpha - \beta \sqrt{-\Delta N} & \gamma - \delta \sqrt{-\Delta N} \\ \gamma p + \delta p\sqrt{-\Delta N} & \alpha + \beta \sqrt{-\Delta N} \end{pmatrix}
\]
and by Corollary 2.1 \( \varphi_p^N : B(N, p)_p \to M_2(Q_p) \) is an isomorphism. It remains to show that integer structures are preserved. The image of the basis of the local Eichler order is:
\[
\varphi_p^N(e_1) = I
\]
\[
\varphi_p^N(e_2) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ p & 1 \end{pmatrix} \in M_2(Z_p)
\]
\[
\varphi_p^N(e_3) = \frac{1}{2} \begin{pmatrix} -\sqrt{-\Delta N} & -\sqrt{-\Delta N} \\ p\sqrt{-\Delta N} & \sqrt{-\Delta N} \end{pmatrix} \in M_2(Z_p)
\]
\[
\varphi_p^N(e_4) = \begin{pmatrix} 0 & a\Delta N - \sqrt{-\Delta N} \\ a\Delta N + \sqrt{-\Delta N} & p \end{pmatrix} \in M_2(Z_p).
\]
The reduced discriminant of \( \varphi_p^N(R_p(N)) \) is \( \Delta N \) so that \( \varphi_p^N(R_p(N)) = M_2(Z_p) \).

For any element \( \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4 \in R_p(N) \) the following identity holds:
\[
\varphi_p^N(\alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4) = \frac{1}{2} \begin{pmatrix} 2\alpha + \beta - \gamma \sqrt{-\Delta N} & \beta - \gamma \sqrt{-\Delta N} + \frac{2}{p}(a\Delta N - \sqrt{-\Delta N}) \\ p\beta + \gamma p\sqrt{-\Delta N} + 2\delta(a\Delta N + \sqrt{-\Delta N}) & 2\alpha + \beta + \gamma \sqrt{-\Delta N} \end{pmatrix}
\]

4.2 The isomorphism at the Archimedean place

Since \( B \) is an indefinite quaternion algebra over \( Q \), there exists an isomorphism \( B_\infty \simeq M_2(R) \). We define \( \varphi_\infty^N \) via
\[
i \mapsto \begin{pmatrix} 0 & 1 \\ -\Delta N & 0 \end{pmatrix} \quad j \mapsto \begin{pmatrix} \sqrt{p} & 0 \\ 0 & -\sqrt{p} \end{pmatrix}.
\]

Then
\[
\varphi_\infty^N(i)^2 = -\Delta NI \quad \varphi_\infty^N(j)^2 = pI
\]
\[
\varphi_\infty^N(k) = \varphi_\infty^N(i)\varphi_\infty^N(j) = \begin{pmatrix} 0 & -\sqrt{p} \\ -\sqrt{p}\Delta N & 0 \end{pmatrix} = -\varphi_\infty^N(j)\varphi_\infty^N(i)
\]
and by Corollary 2.1 the map \( \varphi_\infty^N : B_\infty \to M_2(R) \) is an isomorphism.
4.3 The isomorphism at the ramified places

For any prime number $q$ such that $q | \Delta$ we shall define, following [4], an isomorphism $\varphi^N_q : B_q(N, p) \cong \left\{ \left( \frac{\alpha}{q^2} \frac{\beta}{\alpha} \right) \mid \alpha, \beta \in \mathbb{Q}_q \right\}$ such that

$$\varphi^N_q(R_q(N)) = \varphi^N_q(R_q) = \left\{ \left( \frac{\alpha}{q^2} \frac{\beta}{\alpha} \right) \mid \alpha, \beta \in \mathbb{Z}_q \right\} :\mathbb{O}_q$$

where $\mathbb{Q}_{q^2}$ is the quadratic unramified extension of $\mathbb{Q}_q$, $\alpha \mapsto \bar{\alpha}$ is its non-trivial automorphism and $\mathbb{Z}_{q^2}$ is its ring of integers.

We have $-1 = (-\Delta N, p)_q = (-\Delta N, p)_q(q, p)_q$; since $\Delta$ is square free $(-\Delta N, p)_q = 1$ and $(q, p)_q = -1$. This means in particular that $p$ is not a square in $\mathbb{Q}_q$ and $-\Delta N$ is a norm of a unit of $\mathbb{Q}_q(\sqrt{p})$. Thus there exist $x, y \in \mathbb{Z}_q$ such that $-\Delta N = x^2 - py^2 = (x - \sqrt{py})(x + \sqrt{py})$. We can identify $\mathbb{Q}_{q^2} = \mathbb{Q}_q(\sqrt{p})$ and $\mathbb{Z}_{q^2} = \mathbb{Z}_q(\sqrt{p})$.

We define $\varphi^N_q$ as follows:

$$\varphi^N_q(i) = \begin{pmatrix} 0 & x - \sqrt{py} \\ q(x + \sqrt{py}) & 0 \end{pmatrix}$$

$$\varphi^N_q(j) = \begin{pmatrix} -\sqrt{p} & 0 \\ 0 & \sqrt{p} \end{pmatrix}.$$

Then

$$\varphi^N_q(i)^2 = \Delta NI \quad \varphi^N_q(j)^2 = pI$$

$$\varphi^N_q(k) = \varphi^N_q(i)\varphi^N_q(j) = \begin{pmatrix} 0 & \sqrt{p}(x - \sqrt{py}) \\ -\sqrt{pq}(x + \sqrt{py}) & 0 \end{pmatrix} = -\varphi^N_q(j)\varphi^N_q(i)$$

and for any element $\alpha + \beta i + \gamma j + \delta k$ of $B_q(N, p)$ with $\alpha, \beta, \gamma, \delta \in \mathbb{Q}_q$,

$$\varphi^N_q(\alpha + \beta i + \gamma j + \delta k) = \begin{pmatrix} \alpha - \gamma \sqrt{p}(x - \sqrt{py}) & (\beta + \delta \sqrt{p})(x - \sqrt{py}) \\ q(\beta - \delta \sqrt{p})(x + \sqrt{py}) & \alpha + \gamma \sqrt{p} \end{pmatrix}.$$

By Corollary 2.1, $\varphi^N_q$ is an isomorphism.

We compute the image of the local Eichler order $R_q(N)$:

$$\varphi^N_q(e_1) = I$$

$$\varphi^N_q(e_2) = \frac{1}{2} \begin{pmatrix} 1 - \sqrt{p} & 0 \\ 0 & 1 + \sqrt{p} \end{pmatrix} \in \mathbb{O}_q$$

$$\varphi_q(e_3) = \frac{1}{2} \begin{pmatrix} q(x + \sqrt{py})(1 - \sqrt{p}) & (x - \sqrt{py})(1 + \sqrt{p}) \\ q(x + \sqrt{py})(1 - \sqrt{p}) & 0 \end{pmatrix} \in \mathbb{O}_q$$
\[ \varphi_q(e_4) = \left( \begin{array}{cc} -\frac{a\Delta N}{p} \sqrt{p} & y + \frac{x}{p} \sqrt{p} \\ q \left( -y - \frac{x}{p} \sqrt{p} \right) & -\frac{a\Delta N}{p} \sqrt{p} \end{array} \right) \in O_q \]

and the reduced discriminant of \( \varphi^N_q(R_q(N)) \) is \( N\Delta \).

For any element \( \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4 \) of \( R_q(N) \)

\[ \varphi^N_q(\alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4) = \]

\[ \left( \begin{array}{cc} \alpha + \frac{\beta}{2} - \sqrt{p} \left( \frac{\beta}{2} + aN\Delta \frac{\delta}{p} \right) & (x - \sqrt{py}) \left[ \frac{\gamma}{2} + \sqrt{p} \left( \frac{\gamma}{2} + \frac{\delta}{p} \right) \right] \\ q(x + \sqrt{py}) \left[ \frac{\gamma}{2} - \sqrt{p} \left( \frac{\gamma}{2} + \frac{\delta}{p} \right) \right] & \alpha + \frac{\beta}{2} + \sqrt{p} \left( \frac{\beta}{2} + aN\Delta \frac{\delta}{p} \right) \end{array} \right) \].

5 Characterization of \( \Phi(N) \)

Let \( B \) be a quaternion algebra over \( Q \) of discriminant \( \Delta \) and let \( R(N) \) be an Eichler order of level \( N \) of \( B \). Then \( R(N)^* \times \hat{Z} \) is a compact open subgroup of the finite adelization \( B^*_{\Delta,\infty} \) and it is possible to associate to it a discrete subgroup \( \Phi(N) \) of \( SL_2(R) \) by

\[ \Phi(N) = (GL_2^+(R) \times (R(N)^* \times \hat{Z})) \cap B^* \]

It is known that \( \Phi(N) \) is a co-compact congruence subgroup of \( SL_2(R) \) \[^8\].

Lemma 5.1 If we denote by \( R(N)^{(1)} \) the group of reduced norm 1 elements of \( R(N) \), then the following identity holds: \( \Phi(N) = R(N)^{(1)} \).

Proof The inclusion \( \supseteq \) is trivial since \( R(N)^{(1)} \subseteq B^* \) and \( R(N)^{(1)} \subseteq GL_2^+(R) \times (R(N)^* \times \hat{Z}) \).

We prove the inclusion \( \subseteq \). Let \( \alpha \) be an element of \( \Phi(N) \); then:

a) \( \alpha \in GL_2^+(R) \times (R(N)^* \times \hat{Z}) \)

b) \( \alpha \in B^* \)

If we denote by \( n(\alpha) \) the reduced norm of \( \alpha \), then by b), \( n(\alpha) \) is a rational number, which, by a), is a \( p \)-adic unit for every prime \( p \), and positive. Thus \( n(\alpha) = 1 \) and \( \alpha \in R(N) \). \[\]
6 Explicit description of two conjugates to $R(Nq)$ in $B(N, p)$

In this section we will keep the usual notation and we will represent the quaternion algebra $B$ as $B(N, p) = \{-N\Delta, p\}$.

Let $q$ be a prime number such that $q \nmid \Delta$. It is well known that by definition

$$R(Nq) \simeq R(N) \cap (\varphi_q^N)^{-1}(R_q(qN)).$$

(7)

We shall identify $R(Nq)$ with this subgroup of $R(N)$. Let we consider the idèle $\eta_q$ in $B_A^\times$ defined by

$$\eta_q = \begin{cases} 
\eta_q, \nu = 1 & \text{if } \nu \neq q \\
\eta_q, q = (\varphi_q^N)^{-1} \begin{pmatrix} q & 0 \\
0 & 1 \end{pmatrix} & \text{if } \nu = q
\end{cases}$$

By strong approximation, write $\eta_q = \delta_q g_\infty u$, with $\delta_q \in B^\times$, $g_\infty \in GL_2^+(\mathbb{R})$ and $u \in (R(Nq) \otimes \mathbb{Z})^\times$.

We observe that

$$\eta_q R_q(Nq)\eta_q^{-1} = \delta_q R_q(Nq)\delta_q^{-1} = R_q(N) \cap (\varphi_q^N)^{-1} \begin{pmatrix} Z_q & qZ_q \\
NZ_q & Z_q \end{pmatrix}$$

and

$$\delta_q R(Nq)\delta_q^{-1} = R(N) \cap (\varphi_q^N)^{-1} \begin{pmatrix} Z_q & qZ_q \\
NZ_q & Z_q \end{pmatrix}.\quad (8)$$

We will give bases for $R(Nq)$ and $\delta_q R(Nq)\delta_q^{-1}$. We observe that the following theorems are direct applications of the construction in [5] §1.5, by considering the results in the previous sections and the image via the isomorphisms $\varphi_q^N$ of a generic element of $R_q(N)$.

**Proposition 6.1** Let $q$ be a prime number such that $q \nmid \Delta p$ and $p$ is not a square in $\mathbb{Z}_q^\times$. Let $-\Delta N = x^2 - py^2$ with $x, y \in \mathbb{Z}_q$. Let $c_1, c_2, c_3$ be integers such that

$$c_1 \equiv (y - x) \mod q$$
$$c_2 \equiv p^{-1} \mod q$$
$$c_3 \equiv x \mod q.$$

Then a basis of $R(Nq)$ in $R(N)$ is:

$$f_1 = e_1, \ f_2 = -c_1 e_2 + e_3, \ f_3 = -2c_2(a\Delta N - c_3)e_2 + e_4, \ f_4 = qe_2$$

and a basis of $\delta_q R(Nq)\delta_q^{-1}$ in $R(N)$ is:

$$g_1 = e_1, \ g_2 = c_1 e_2 + e_3, \ g_3 = -2c_2(a\Delta N + c_3)e_2 + e_4, \ g_4 = qe_2.$$
Proof By the results in Section 4.1.1 and by the equality (7), we see that \( f_1, f_2, f_3, f_4 \in R(Nq) \) and
\[
\begin{vmatrix}
1 & 0 & 0 & 0 \\
0 & -c_1 & -2c_2(a\Delta N - c_3) & q \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
\end{vmatrix} = q.
\]
By the results in Section 4.1.1 and by the equality (8) we see that \( g_1, g_2, g_3, g_4 \in \delta_q R(Nq)\delta_q^{-1} \) and
\[
\begin{vmatrix}
1 & 0 & 0 & 0 \\
0 & c_1 & -2c_2(a\Delta N + c_3) & q \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
\end{vmatrix} = q.
\]

Proposition 6.2 Let \( q \nmid \Delta \) be a prime number such that \( p \) is a square in \( \mathbb{Z}_q^\times \). A basis of \( R(qN) \) in \( R(N) \) is:
\[
f_1 = e_1, \quad f_2 = e_2, \quad f_3 = e_3 - ce_4, \quad f_4 = qe_4
\]
where \( \mathbb{Z} \ni c \equiv (p - \sqrt{p})2^{-1} \mod q \). A basis of \( \delta_q R(qN)\delta_q^{-1} \) in \( R(N) \) is:
\[
g_1 = e_1, \quad g_2 = e_2, \quad g_3 = e_3 - c'e_4, \quad g_4 = qe_4
\]
where \( \mathbb{Z} \ni c' \equiv (p + \sqrt{p})2^{-1} \mod q \).

Proof By the results in section 4.1.2 and by the equality (7), we observe that \( f_1, f_2, f_3, f_4 \in R(qN) \) and
\[
\begin{vmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & -c & q \\
\end{vmatrix} = q;
\]
by the equality (8), it is easy to verify that \( g_1, g_2, g_3, g_4 \in \delta_q R(qN)\delta_q^{-1} \) and
\[
\begin{vmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & -c' & q \\
\end{vmatrix} = q.
\]
Proposition 6.3 Let $\sqrt{-\Delta N}$ be the square root of $-\Delta N$ in $\mathbb{Q}_p$ such that $a\sqrt{-\Delta N} \equiv -1 \mod p$. A basis of $R(Np)$ in $R(N)$ is:

$$f_1 = e_1, \quad f_2 = -c_4e_2 + e_3, \quad f_3 = -2(a\Delta N + c_4)e_2 + pe_4, \quad f_4 = p(Ae_2 + Be_4)$$

and a basis of $\delta_p R(Np)\delta_p^{-1}$ in $R(N)$ is:

$$g_1 = e_1, \quad g_2 = c_4e_2 + e_3, \quad g_3 = -2\frac{a\Delta N - c_4}{p}e_2 + e_4 \quad g_4 = pe_2$$

where $\mathbb{Z} \ni c_4 \equiv \sqrt{-\Delta N} \mod p$, $a \in \mathbb{Z}$ is such that $a^2 \Delta N + 1 \equiv 0 \mod p$ and $A, B \in \mathbb{Z}$ are such that $Ap + 2B(a\Delta N + c_4) = 1$.

Proof We first observe that if we fix $\sqrt{-\Delta N}$ the square roots in $\mathbb{Q}_p$ such that $a\sqrt{-\Delta N} \equiv -1 \mod p$, then $p|(a\Delta N - c_4)$ and $p \not| (a\Delta N + c_4)$. Then the existence of $A, B \in \mathbb{Z}$ such that $Ap + 2B(a\Delta N + c_4) = 1$ is ensured.

By the results in Section 4.1.3 and by the equality (7), we observe that $f_1, f_2, f_3, f_4 \in R(Np)$ and

$$\det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -c_4 & -2(a\Delta N + c_4) & pA \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & pB \end{pmatrix} = p;$$

by the equality (8), we see that $g_1, g_{2,3}, g_4 \in \delta_p R(Np)\delta_p^{-1}$ and

$$\det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & c_4 & -2\frac{a\Delta N - c_4}{p} & p \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = p.$$ 

\[\blacksquare\]

7 Description of the isomorphism $\Psi^M_N$

Let we fix $\Delta$ as in Section 2 by the classification theorem, up to isomorphism there exists only one quaternion algebra $B$ over $\mathbb{Q}$ with discriminant $\Delta$. Let $B(M, p) = \{-\Delta M, p\}$ and $B(N, p) = \{-\Delta N, p\}$ be two representations of $B$, with $p, N, M$ as in Section 2. Then there is an isomorphism $\Psi^M_N : B(N, p) \to B(M, p)$. This implies that there exists an element $h \in B(M, p)$.
such that $h^2 = -N \Delta$; we observe that $h$ is of the form $h = i^M \beta + j^M \gamma + k^M \delta$ where $(\beta, \gamma, \delta) \in \mathbb{Q}^3$ is a solution of the equation

$$M \Delta \beta^2 - p \gamma^2 - p \Delta M \delta^2 = N \Delta.$$ 

**Lemma 7.1** Let $f$ be the quadratic form on $\mathbb{Q}$ defined as $f = M \beta^2 - pM \delta^2$; then $f$ represents $N$.

**Proof** By the Hasse-Minkowski theorem (see for example [6]), $f$ represents $N$ in $\mathbb{Q}$ if and only if $f$ represents $N$ in $\mathbb{Q}_\ell$ at any place $\ell$, that is $(N, p)_\ell = (M, p)_\ell$ for any prime number $\ell$.

We write: $N = \ell^a u$, $p = \ell^b v$, $\epsilon(\ell) \equiv \frac{\ell - 1}{2} \mod 2$.

If $\ell \neq 2$ then

$$(N, p)_\ell = (-1)^{abc(\ell)} \left( \frac{u}{\ell} \right)^b \left( \frac{v}{\ell} \right)^a$$

- If $\ell \nmid pN$ then $(N, p)_\ell = 1$.
- If $\ell = p$ then $\epsilon(p) = 0$, $v = 1$, $b = 1$ so $(N, p)_p = \left( \frac{u}{p} \right)^b \left( \frac{v}{p} \right)^a = \left( \frac{u}{p} \right)$.

By the hypothesis on the prime factors $q$ of $N$, by the law of reciprocity and since $p \equiv 1 \mod 4$,

$$\left( \frac{u}{p} \right) = \prod_{q \mid u} \left( \frac{q}{p} \right) = \prod_{q \mid u} \left( \frac{p}{q} \right) (-1)^{(q-1)(p-1)/4} = 1.$$ 

- If $\ell \mid N$ and $\ell \neq p$ then $b = 0, v = p$ so

$$(N, p)_\ell = \left( \frac{p}{\ell} \right)^a = 1$$

by the hypothesis on the prime factors of $N$.

If $\ell = 2$ then $b = 0$ and $v = p$; we know that

$$(N, p)_2 = (-1)^{\epsilon(v) = a \omega(p) + b \omega(u)}$$

where $\epsilon(v) = 0, \omega(p) \equiv \frac{p^2 - 1}{8} \mod 2$. So

$$(N, p)_2 = (-1)^{a \omega(p)}.$$ 

- if $a = 0$ then $(N, p)_2 = 1$;
- if $a \neq 0$ then $2 \mid N$ and $p \equiv 1 \mod 8$. So $\omega(p) = 0$ and $(N, p)_2 = 1$. 

15
Since $N$ and $M$ satisfy the same hypotheses, then $(N,p)\ell = (M,p)\ell = 1$ for any prime number $\ell$.

We define the $\mathbb{Q}$-linear map $\Psi^M_N : B(N,p) \rightarrow B(M,p)$ as:

$$\Psi^M_N(i^N) = h, \quad \Psi^M_N(j^N) = j^M$$

where $h = \beta i^M + \delta k^M$ with $(\beta, \gamma) \in \mathbb{Q}^2$ solution of $M\beta^2 - pM\delta^2 = N$ (by Lemma 7.1 such an element exists). Then $\Psi^M_N(i^N)^2 = -N\Delta$, $\Psi^M_N(j^N)^2 = p$ and

$$\Psi^M_N(i^N)\Psi^M_N(j^N) = hj^M = k^M \beta + i^M p\delta = -\Psi^M_N(j^N)\Psi^M_N(i^N).$$

By the Corollary 2.1 the map $\Psi^M_N$ is an isomorphism.

We observe that if $N = MS$ then

$$\beta^2 - p\delta^2 = S \quad (9)$$

so $S$ is the norm of an element $\beta + \sqrt{p}\delta$ of the ring of integer

$$\mathcal{O} = \left\{ \frac{1}{2}(a + \sqrt{p}b) : a, b \in \mathbb{Z} \text{ with the same parity} \right\}$$

of $\mathbb{Q}(\sqrt{p})$.

We denote by $a_M, a_N$ the integer numbers as in Section 2 such that $a_M^2 \Delta M + 1 \equiv 0 \mod p$ and $a_N^2 \Delta N + 1 \equiv 0 \mod p$.

**Lemma 7.2** If $N = MS \in \mathbb{N}$ then we can choose $\beta \in \mathbb{Z}\left[\frac{1}{2}\right]$ satisfying the identity (7) such that $a_M \equiv a_N \beta \mod p$.

**Proof** By definition of $a_N, a_M$, since $p \not| \Delta M$, we find that $a_N^2 S - a_M^2 \equiv 0 \mod p$, that is by (9) $a_N^2 \beta^2 - a_M^2 \equiv 0 \mod p$. In particular $a_N \beta - a_M \equiv 0 \mod p$ or $a_N \beta + a_M \equiv 0 \mod p$. If we are in the second situation, then we can take $-\beta$ instead of $\beta$, so we have that $a_M \equiv a_N \beta \mod p$.

In the sequel when $M|N$ we choose $a_M$ as in the above lemma.

**Proposition 7.1** Let $B(N,p)$ and $B(M,p)$ be two representations of the quaternion algebra $B$ defined over $\mathbb{Q}$ with discriminant $\Delta$. Let we consider the isomorphism $\Psi^M_N : B(N,p) \rightarrow B(M,p)$ defined above. If $M|N$ then $\Psi^M_N(R(N)) \subset R(M)$.

**Proof** Let $N = MS$ where $S \in \mathbb{N}$. We recall that $p \equiv 1 \mod 4$ and we verify that $\Psi^M_N(e^N_1) \in R(M)$ for $\ell = 1, 2, 3, 4$.

By definition of $\Psi^M_N$:

$$\Psi^M_N(e^N_1) = 1 = e^M_1$$

16
\[ \Psi_N^M(e^2) = \frac{1 + j^M}{2} = e^2 \]
\[ \Psi_N^M(e^3) = A_3e_1^M + B_3e_2^M + C_3e_3^M + D_3e_4^M \]
where \( A_3 = \frac{1}{2}\delta(1-p)a_M\Delta \in \mathbb{Z} \), \( B_3 = \delta(p-1)a_M\Delta \in \mathbb{Z} \), \( C_3 = \delta p + \beta \in \mathbb{Z} \) and \( D_3 = \delta p \frac{1-p}{2} \in \mathbb{Z} \).

\[ \Psi_N^M(e^4) = A_4e_1^M + B_4e_2^M + C_4e_3^M + D_4e_4^M \]
where \( B_4 = -2A_4 = \frac{2}{p}\delta M(a_N S - a_M^2 + p^2 a_M \beta) \), \( C_4 = 2\delta \in \mathbb{Z} \) and \( D_4 = \beta - p\delta \in \mathbb{Z} \). We observe that \( B_4 \in \mathbb{Z} \) (and \( A_4 \in \mathbb{Z} \)), in fact by Lemma 7.2:

\[ a_N S - a_M^2 \equiv a_N S - a_N \beta^2 \mod p \]
\[ \equiv a_N S - a_N(S + p^2) \mod p \]
\[ \equiv 0 \mod p \]

---

8 Some properties of the Eichler orders

By using the local isomorphisms given in Section 4, we will prove some new results for the Eichler orders. Let \( B \) be a quaternion algebra over \( \mathbb{Q} \) of fixed discriminant \( \Delta \).

Let \( B(N, p) = \{ -\Delta N, p \} = \mathbb{Q}[i^N] + \mathbb{Q}[j^N] + \mathbb{Q}[k^N] \) be a representation of \( B \); we will write \( R(N) \subset B(N, p) \) to denote the Eichler order of level \( N \) of Hashimoto [3]: \( R(N) = \mathbb{Z}[e_1^N] + \mathbb{Z}[e_2^N] + \mathbb{Z}[e_3^N] + \mathbb{Z}[e_4^N] \) with

\[ e_1^N = 1, \ e_2^N = \frac{1 + j^N}{2}, \ e_3^N = \frac{i^N + k^N}{2}, \ e_4^N = \frac{a\Delta N j^N + k^N}{p} \]

where \( a \in \mathbb{Z} \) satisfies \( a^2 \Delta N + 1 \equiv 0 \mod p \). By abuse of notation, in this section we will write \( R(M) \) instead of \( \Psi_N^M(R(M)) \). In this way, if \( N|M \) the inclusion \( R(M) \subset R(N) \) in \( B(N, p) \) is true.

**Lemma 8.1** Let \( B \) be a quaternion algebra over \( \mathbb{Q} \) of discriminant \( \Delta \); let \( N \) be a positive integer prime to \( \Delta \) and \( q \) be a prime number not dividing \( \Delta \). Then the \( \mathbb{Z} \)-rank of \( \bigcap_{n \in \mathbb{N}} R(Nq^n) \) is equal to the \( \mathbb{Z} \)-rank of \( \bigcap_{n \in \mathbb{N}} R(q^n) \).

**Proof** Let \( B(1, p) \) be a representation of \( B \) where \( p \) is as in Section 2. It is obvious that

\[ \bigcap_n R(Nq^n) = \bigcap_n R(q^n) \cap R(N) \subset R(1). \quad (10) \]
Since the rank is invariant by isomorphism and $R(N)$ has maximal rank over $\mathbb{Z}$, then
\[
\text{rk} \left( \bigcap_{n \in \mathbb{N}} R(Nq^n) \right) = \text{rk} \left( \bigcap_{n \in \mathbb{N}} R(q^n) \right).
\]

Let $B(1, p)$ be a representation of $B$ and let $q \nmid \Delta$ be a prime number; we consider the chain of Eichler orders...

\[ ... \subset R(q^n) \subset ... \subset R(q^2) \subset R(q) \subset R(1) \]
in $B(1, p)$. We will characterize the intersection $A_q = \bigcap_{n \in \mathbb{N}} R(q^n)$ as an $\mathbb{Z}$-lattice. Since
\[
R(q) \simeq R(1) \cap (\varphi_q^1)^{-1} \begin{pmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ q\mathbb{Z}_q & \mathbb{Z}_q \end{pmatrix}
\]
where $\varphi_q^1 : B(1, p)_q \rightarrow M_2(\mathbb{Q}_q)$ is a local isomorphism, then
\[
A_q \simeq R(1) \cap \left[ \bigcap_n (\varphi_q^1)^{-1} \begin{pmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ q\mathbb{Z}_q & \mathbb{Z}_q \end{pmatrix} \right] = R(1) \cap (\varphi_q^1)^{-1} \begin{pmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ 0 & \mathbb{Z}_q \end{pmatrix}. \quad (11)
\]

**Proposition 8.1** Let $B$ be a quaternion algebra over $\mathbb{Q}$ of discriminant $\Delta$; let we fix a prime number $q$ not dividing $\Delta$. The intersection
\[
A_q = \bigcap_{n \in \mathbb{N}} R(q^n)
\]
has rank 2 over $\mathbb{Z}$.

**Proof**
Let we fix a prime number $p$ is as in Section 2. We will distinguish the following cases:

1. $q \nmid \Delta p$ such that $\left( \frac{p}{q} \right) = -1$;

2. $q \nmid \Delta$ such that $\left( \frac{p}{q} \right) = 1$;

3. $q = p$.

1. Let $q \nmid \Delta$ be a prime number such that $\left( \frac{p}{q} \right) = -1$. Let $N$ be a positive integer prime to $\Delta$ such that $\left( \frac{p}{s} \right) = 1$ for all $s | N$ and $\left( \frac{-\Delta N}{q} \right) = 1$. This last condition on $N$ implies that there exists $x(N, q) \in \mathbb{Z}_q$ such that $-\Delta N = x(N, q)^2$. Let we represent $B$ as $B(N, p) = \{-\Delta N, p\}$. 

18
If \( q \) is such that \(-\Delta\) is a square in \( \mathbb{Z}_q \), then we can take \( N = 1 \) and \( \mathcal{A}_q \subset R(1) \) in \( B(1,p) \); if \( h \in \mathcal{A}_q \) then by (11) there exist \( \alpha, \beta, \gamma, \delta \in \mathbb{Z} \) such that \( h = \alpha e_1^4 + \beta e_2^4 + \gamma e_3^4 + \delta e_4^4 \) where \( \{e_1, e_2, e_3, e_4\}\) is the Hashimoto basis of \( R(1) \) in \( B(1,p) \). Moreover, by the identity (3)

\[
x(N, q) \left( \frac{-\gamma - \delta}{2} + \frac{\beta + \delta a\Delta}{p} \right) = 0.
\]

Then \( \mathcal{A}_q \subset R(1) \) can be expressed as the \( \mathbb{Z} \)-lattice \( \mathcal{A}_q = \mathbb{Z} e_1^4 + \mathbb{Z} e_3^4 \) where \( e_1^4 = -2a\Delta e_2^4 - 2e_3^4 + pe_4^4 \).

If \( q \) is such that \(-\Delta\) is not a square in \( \mathbb{Z}_q \), then we take \( N \) such that \( \left( \frac{N}{q} \right) = -1 \). If \( h \in \cap_n R(Nq^n) \simeq R(N) \cap (\varphi^N_q)^{-1} \left( \begin{array}{cc} \mathbb{Z}_q & \mathbb{Z}_q \\
0 & \mathbb{Z}_q \end{array} \right) \) in \( B(N,p) \)

then there exist \( \alpha, \beta, \gamma, \delta \in \mathbb{Z} \) such that \( h = \alpha e_1^N + \beta e_2^N + \gamma e_3^N + \delta e_4^N \) where \( \{e_1^N, e_2^N, e_3^N, e_4^N\}\) is the Hashimoto basis of \( R(N) \) in \( B(N,p) \). Moreover, by the identity (3)

\[
x(N, q) \left( \frac{-\gamma - \delta}{2} + \frac{\beta + \delta a\Delta N}{p} \right) = 0.
\]

Then \( \cap_n R(Nq^n) \subset R(N) \) can be expressed as the \( \mathbb{Z} \)-lattice \( \cap_n R(Nq^n) = \mathbb{Z} e_1^N + \mathbb{Z} e_3^N \) where \( e_1^N = -2a\Delta N e_2^N - 2e_3^N + pe_4^N \). By Lemma (8.1), \( \text{rk}(\cap_n R(q^n)) = \text{rk}(\cap_n R(Nq^n)) = 2 \).

2. Let \( q \not| \Delta \) be a prime number such that \( \left( \frac{q}{\Delta} \right) = 1 \); we represent the quaternion algebra \( B \) as \( B(1,p) = \{-\Delta, p\} \). If \( h \in \mathcal{A}_q \), then by (11) and by the identity (11), \( h = \alpha e_1^4 + \beta e_2^4 + \gamma e_3^4 + \delta e_4^4 \) where \( \alpha, \beta, \gamma, \delta \in \mathbb{Z} \) satisfy the equation

\[
\sqrt{p}(-\gamma) + (\gamma p + 2\delta) = 0. \tag{12}
\]

Then \( \gamma = \delta = 0 \) and \( \mathcal{A}_q \subset R(1) \) can be expressed as the \( \mathbb{Z} \)-lattice \( \mathcal{A}_q = \mathbb{Z} e_1^4 + \mathbb{Z} e_2^4 \).

3. Let \( q = p \); we represent the quaternion algebra \( B \) as \( B(1,p) = \{-\Delta, p\} \).

If \( h \in \mathcal{A}_p \), then by (11) and by the identity (11), \( h = \alpha e_1^4 + \beta e_2^4 + \gamma e_3^4 + \delta e_4^4 \) where \( \alpha, \beta, \gamma, \delta \in \mathbb{Z} \) satisfy the equation

\[
\sqrt{-\Delta}(\gamma p + 2\delta) + (\beta p + 2a\Delta \delta) = 0. \tag{13}
\]

Then \( \mathcal{A}_q \subset R(1) \) can be expressed as the \( \mathbb{Z} \)-lattice \( \mathcal{A}_p = \mathbb{Z} e_1^4 + \mathbb{Z} e \) where \( e = -2a\Delta e_2^4 - 2e_3^4 + pe_4^4 \).

**Proposition 8.2** Let \( B \) a quaternion algebra over \( \mathbb{Q} \) of discriminant \( \Delta \) and let \( B(1,p) \) be a representation of \( B \). Let \( q, s \not| \Delta p \) be two prime number such that \( \left( \frac{q}{\Delta} \right) = 1 \) and \( \left( \frac{q}{\Delta} \right) = -1 \). Then \( \mathcal{A}_q \cap \mathcal{A}_p = \mathcal{A}_s \cap \mathcal{A}_p = \mathcal{A}_q \cap \mathcal{A}_s = \mathbb{Z} \).
Proof Let \( \{e_1, e_2, e_3, e_4\} \) be the Hashimoto basis of \( R(1) \) in \( B(1, p) \).
If \( h \in A_q \cap A_p \) then \( h = \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4 \) where \( \alpha, \beta, \gamma, \delta \in \mathbb{Z} \) satisfy the equations (12) and (13). This imply that \( \beta = \gamma = \delta = 0 \).
If \( h \in A_s \cap A_p \) then \( h = \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4 \) where \( \alpha, \beta, \gamma, \delta \in \mathbb{Z} \) satisfy the equation (13) and by the identity (3)

\[
x \left[ -\frac{\gamma}{2} - \frac{\delta}{p} \right] + y \left[ \frac{\gamma}{2} \right] + \frac{\beta}{2} + \delta \frac{a\Delta}{p} = 0.
\] (14)

where \( x, y \in \mathbb{Z} \) are such that \(-\Delta = x^2 - py^2\). This imply that \( \beta = \gamma = \delta = 0 \).
If \( h \in A_q \cap A_s \) then \( h = \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4 \) where \( \alpha, \beta, \gamma, \delta \in \mathbb{Z} \) satisfy the equations (12) and (14). This imply that \( \beta = \gamma = \delta = 0 \).

Corollary 8.1 Let \( B \) a quaternion algebra over \( \mathbb{Q} \) of discriminant \( \Delta \); then

\[
A := \bigcap_N R(N) = \mathbb{Z}
\]

where \( N \) runs over the set of positive integer numbers primes to \( \Delta \).

As corollary, by Lemma 5.1, the following result holds:

Corollary 8.2 Let \( \Phi(N) \) be the group defined in Section 8 then:

\[
\bigcap_N \Phi(N) = \{\pm 1\}
\]

where \( N \) runs over the set of positive integer numbers primes to \( \Delta \).

9 Example

Using a mathematical problem-solving environment as Maple, wich work with \( p \)-adic numbers, it is possible to produce some examples.

Let we consider the quaternion algebra \( B \) over \( \mathbb{Q} \) with discriminant \( \Delta = 35 \); following Hashimoto we can represent it as \( B(3, 13) = \{-105, 13\} \). A basis over \( \mathbb{Z} \) of the Eichler order \( R(3) \) of \( B(3, 13) \) is

\[
e_1 = 1, \ e_2 = \frac{1 + j}{2}, \ e_3 = \frac{i + k}{2}, \ e_4 = \frac{525j + k}{13}.
\]
If we consider $q = 11$, then $q \nmid \Delta$ and $p = 13$ is not a square in $\mathbb{Z}_{11}^\times$; thus by Proposition 6.1 a basis of the Eichler order $R(33)$ in $B(3, 13)$ is:

$$f_1 = 1, \quad f_2 = -\frac{5}{2} + \frac{i}{2} - \frac{5}{2}j + \frac{k}{2}$$

$$f_3 = -3150 - \frac{40425}{13}j + \frac{1}{13}k, \quad f_4 = \frac{11}{2} + \frac{11}{2}j.$$

A basis of $\delta_{11}R(33)\delta_{11}^{-1}$ in $B(3, 13)$ is:

$$g_1 = 1, \quad g_2 = \frac{5}{2} + \frac{i}{2} + \frac{5}{2}j + \frac{k}{2}$$

$$g_3 = -3150 - \frac{40425}{13}j + \frac{1}{13}k, \quad g_4 = \frac{11}{2} + \frac{11}{2}j.$$

Moreover let $B(17, 13) = \{-595, 13\} = \mathbb{Q} + \mathbb{Q}i^{(17)} + \mathbb{Q}j^{(17)} + \mathbb{Q}k^{(17)}$ be the quaternion algebra over $\mathbb{Q}$ with discriminant 35 and $N = 17$; then $(i^{(17)})^2 = -595$ and $(j^{(17)})^2 = 13$. It is possible to write the isomorphism $\Psi_{3}^{17} : B(3, 13) \to B(17, 13)$ described in Section 7:

$$\Psi_{3}^{17}(j) = j^{(17)}, \quad \Psi_{3}^{17}(i) = \frac{8}{17}i^{(17)} + \frac{1}{17}k^{(17)}.$$

### References

[1] Ciavarella Miriam: Congruences between modular forms and related modules, arXiv:0710.4677v1 [math. NT] 25 Oct. 2007.

[2] Ciavarella Miriam and Terracini Lea: Analogue of Ihara`s lemma for Shimura Curves, Submitted paper, 2007.

[3] Hashimoto Ki-ichiro: Explicit form of Quaternion modular embeddings, Osaka J. Math., 32 n.3, 533-546, 1995.

[4] Pizer Arnold: On the arithmetic of quaternions algebras II, J. Math. Soc. Japan, 28, 676-688, 1976.

[5] Samuel Pierre: Théorie Algébrique des Nombres, Hermann Paris, 1971.

[6] Serre Jean-Pierre: Cours d’arithmétique, Presses Universitaires de France, 1970.

[7] Terracini Lea: A Taylor-Wiles system for quaternionic Hecke algebras, Compositio Mathematica, 137, 23-47, 2003.
[8] Vignéras, Marie-France, Arithmétique des algèbres de quaternions, Lecture Notes Math., 800, Springer, 1980.

Authors’ affiliation:

Miriam Ciavarella
Università degli Studi di Torino
Dipartimento di Matematica
Via Carlo Alberto,10
10123 Torino (Italy)
e-mail: miriam.ciavarella@unito.it

Lea Terracini
Università degli Studi di Torino
Dipartimento di Matematica
Via Carlo Alberto,10
10123 Torino (Italy)
e-mail: lea.terracini@unito.it