MASTER COURSE:

Quaternion algebras and Quadratic forms towards Shimura curves

Prof. Montserrat Alsina
Universitat Politècnica de Catalunya - BarcelonaTech
EPSEM Manresa

September 2013

Contents

Chapter 1

Introduction to quaternion algebras

In this chapter we review basics for quaternion algebras and their orders and consider small ramified quaternion algebras, under a classification in type A and B, where explicit results will be given.

1.1 Notation. Let us consider K a field of $\mathrm{char}(K) \neq 2$.
For characteristic 2, some arrangements need to be done.
As usual, we denote $\mathrm{M}(n, R)$ the ring of $n \times n$ matrices with entries in a ring R;

1.1 Basics on quaternion algebras

1.2 ***Classical definition.***
Given $a, b \in K^* = K\backslash\{0\}$, the quaternion K-algebra $H = \left(\frac{a,b}{K}\right)$ is the K-algebra with K-basis $\{1, i, j, k\}$ with the rules: $\quad i^2 = a,\ j^2 = b, ij = -ji = k.$

$\{1, i, j, ij\}$ *is called the canonical, or standard, basis. By construction,* $\dim_K H = 4$.

Thus, we can see a quaternion algebra as a K vectorial space of dimension 4 over K, with the natural definitions of addition and scalar multiplication, made into a ring by defining multiplication by the rules stated above.

An element $\omega \in H$ is $\omega = x + yi + zj + tk$, where $x, y, z, t \in K$
The product of two elements in H is computed from the following table (plus the associative property):

xy	1	i	j	k
1	1	i	j	k
i	i	a	k	aj
j	j	$-k$	b	$-bi$
k	k	$-aj$	bi	$-ab$

As usual, $H^* = \{u \in H : \exists v \in H,\ uv = vu = 1\}$.

1.3 Example. The most wellknown exemple is obtained by $K = \mathbb{R}$ and $a = b = -1$.
Then $\mathbb{H} = \left(\dfrac{-1,-1}{\mathbb{R}}\right)$ is the Hamilton quaternion algebra (H is for Hamilton!).

In fact, next October will be the 170th anniversary of Hamilton's idea (16th October 1843). He carved the multiplication formulae with a knife on the stone of a bridge in Dublin. It is considered as the birthplace of noncommutative algebra, because it was the precursor to a wide range of new kinds of algebraic structures (not assuming commutativity, or associativity, ...). There is a nice paper with Hamilton's results (On quaternions, or on a new system of imaginaries in algebra, W. Hamilton, *Philosophical Magazine* (1844-1850), D. Wilkins (ed.) 2000) and another one from a talk given at the Irish Mathematical Society at 2005 (Quaternion Algebras and the Algebraic Legacy of Hamilton's Quaternions, by D. Lewis, *Irish Math. Soc. Bulletin* **57** (2006) 41-64).

There is another similar birth happened in the same century, worth to be mentioned now: noneuclidean geometry. Actually, in this setting for modular and Shimura curves, hyperbolic geometry (a noneuclidean one!) will be used too.

1.4 Example. Let us consider $K = \mathbb{Q}$. This is the main case to keep in mind for this course. Any choice of a, b, different from 0 will give a quaternion $\mathbb{Q}$-algebra (but perhaps not so different!).

- $a = 1, \quad b = -1 \quad \to \left(\dfrac{1,-1}{\mathbb{Q}}\right)$.
- $a = 1, \quad b \quad \to \left(\dfrac{1,b}{\mathbb{Q}}\right)$.
- $a, \quad b = -a \quad \to \left(\dfrac{a,-a}{\mathbb{Q}}\right)$.

This was the classical definition, but there are other equivalent definitions.

1.5 Equivalent construction of quaternion algebras.
From Hamilton's algebra, comparing with complex numbers, we can guess another way to construct quaternion algebras in two steps (specially if we have field extensions in mind).

Consider a field K (for example $\mathbb{Q}$).
First step. Add to K a new element i such that $i^2 = a \in \mathbb{Q}^*$ (ex: $i = \sqrt{3}$ or $i = \sqrt{-3} \notin \mathbb{Q}$), so we get a new field $F = \mathbb{Q}(i) = Q[x]/(x^2 - a)$ which is commutative; it is called quadratic field, ... (For example: $\mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$, $\mathbb{Q}(\sqrt{-3}) \subset \mathbb{C}$...).
There is a nontrivial K-automorphism in $F = \mathbb{Q}(i)$ given by: $\alpha = x + yi \mapsto \alpha' = x - yi$, called conjugation.

Second step. Choose $b \in K^*$ and denote j a new element such that (by definition):
$j^2 = b$ and $j{\cdot}\alpha = \alpha'{\cdot}j$, for all $\alpha \in F$, α' the conjugate of α in $F = \mathbb{Q}(i)$.
Then, put $H = F + Fj$, and it is clear we get the quaternion algebra $\left(\dfrac{a,b}{K}\right)$.

This is the definition used, for example, at M-F. Vigneras book *Arithmétique des Algèbres de Quaternions*, LN 800, ed. Springer, 1980, one of the basic references for quaternion algebras (actually the "first" book devoted fully to quaternion algebras).

1.6 ***Equivalent definition of quaternion algebra.***
A quaternion K-algebra H is a central simple K-algebra of dimension 4 over K.

Next we recall the concepts used in above definition.

A K-algebra A (associative and with unity) is a K-vector space with ring structure and with unity, 1_A, in such a way that $k(uv) = (ku)v = u(kv)$, $u, v \in A$, $k \in K$.

The center of an algebra A is the subset of all those elements that commute with all other elements in A, $Z(A) = \{z \in A \mid za = az, \forall a \in A\}$. Note that elements $\{k \cdot 1_A \mid k \in K\}$ are central; that is, $K \subseteq Z(A)$, the center of A. A K-algebra A is called central if $Z(A) = K$.

A K-algebra is called simple if it has no non-trivial bilateral ideals.

An homomorphism of K-algebras $\varphi : A \to B$ is a K-linear homomorphism of rings.

1.7 Example. An excellent, and fundamental, example is the ring of matrices $\mathrm{M}(2, K)$.

It is easy to check that $H = \mathrm{M}(2, K)$ is a central simple K-algebra.

To check it is central, consider $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(H)$. Put $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then:

$$0 = A \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} A = \begin{pmatrix} -c & a-d \\ 0 & c \end{pmatrix},$$

$$0 = A \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} A = \begin{pmatrix} b & 0 \\ -a+d & -b \end{pmatrix}.$$

Thus $a = d$, $b = c = 0$, that is $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI$ and $Z(H) \simeq K$.

To check $H = \mathrm{M}(2, K)$ is simple, consider J a non trivial bilateral ideal in H, and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in J$. Then:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} A \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in J,$$

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} A \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \in J.$$

Then the sum $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI$ is a unit in the ideal J, so $J = H$.

1.2 Main known results

Next we will remind main results about quaternion algebras, without formal proofs, but trying to be constructive and deducing some results applying nice ideas.

Skolem-Noether theorem: the K-automorphisms of a quaternion K-algebra H are the inner automorphisms, namely, the conjugations $\omega \mapsto \sigma^{-1}\omega\sigma$, where $\sigma \in H^*$.

Wedderburn Theorem: any central simple K-algebra A is isomorphic to an algebra $\mathrm{M}(n, D)$ for some $n \in \mathbb{N}$ and some division algebra D. In particular, $\dim_K A = n^2 \dim_K D$.

Let us apply Wedderburn theorem to a quaternion algebra.
From $H \simeq \mathrm{M}(n, D)$, we get $4 = \dim_K H = n^2 \dim_K D$ which gives only two possibilities:

- $n = 1$, so $H \simeq D$ is a division algebra,
- $n = 2$ and $D = K$, so $H \simeq \mathrm{M}(2, K)$ is a matrix algebra (algebra **split**).

Thus, there are only two possibilities for quaternion K-algebras:
to be a division K-algebra or to be the ring of 2×2 matrices over K.
In fact this can be also proved without Wedderburn theorem, using other arguments.

1.8 Exercise. What about examples in 1.4? Are they division or matrix algebras?

1.9 Proposition. *Given a quaternion K-algebra $H = \left(\dfrac{a, b}{K}\right)$,*
the map $\phi : H \hookrightarrow \mathrm{M}(2, K(\sqrt{a}))$ defined by

$$\phi(x + yi + zj + tij) = \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix}.$$

is a monomorphism.

Proof: It is easy to check that this map is a morphism of quaternion algebras:

$$\phi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \phi(i) = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \quad \phi(j) = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix},$$

$$\phi(i)\phi(j) = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{pmatrix} = \phi(ij).$$

It is a monomorphism:

$$\phi(\omega_1) = \phi(\omega_2) \Rightarrow \mathrm{tr}(\omega_1) = \mathrm{tr}(\omega_2), \text{ so } x_1 = x_2, \text{ then } y_1 = y_2 \ldots$$

□

1.10 Corollary. *If $\sqrt{a} \in K$, then $H \simeq \mathrm{M}(2, K)$.*
Thus, If K is algebraically closed, we only obtain matrix algebras.
In particular $\mathrm{M}(2, \mathbb{C})$ is the unique quaternion algebra over $\mathbb{C}$.

But be aware that if $\sqrt{a} \notin K$, then still we have the two possibilities (a division algebra or the matrix ring), so more results are needed.

Coming back to example 1.4, applying the corollary we can be sure: $\left(\dfrac{1, -1}{\mathbb{Q}}\right) \simeq \left(\dfrac{1, b}{\mathbb{Q}}\right) \simeq \mathrm{M}(2, \mathbb{Q})$.

Before to move on, let us summarize some properties.

1.11 Properties. (i) *If K is algebraically closed, we only obtain matrix algebras. In particular* $\mathrm{M}(2,\mathbb{C})$ *is the unique quaternion algebra over* $\mathbb{C}$.

(ii) *If K is a finite field, we only obtain matrix algebras.*

(iii) *If K is a local field ($\neq \mathbb{C}$), there exists a unique division quaternion K-algebra up to isomorphism. If $K = \mathbb{R}$, we get the Hamilton quaternion algebra $\mathbb{H}$.*

What can be used to study the remaining case in the example 1.4?

This would be the "excuse" today to introduce some very important definitions and results about quaternion algebras, related to quadratic forms.

1.3 Reduced trace and norm

1.12 Definitions. There is a (unique) involutive antiautomorphism in H called conjugation, denoted by $\omega \mapsto \overline{\omega}$.
For $\omega = x + yi + zj + tij \in \left(\frac{a,b}{K}\right)$, $\overline{\omega} = x - yi - zj - tij$.

Then we define:

$$\begin{array}{ll} \text{reduced trace} & \mathrm{tr}(\omega) = \omega + \overline{\omega} \in K \\ \text{reduced norm} & \mathrm{n}(\omega) = \omega\overline{\omega} \in K \end{array}$$

Thus $\mathrm{tr}(\omega) = 2x$ and $\mathrm{n}(\omega) = x^2 - ay^2 - bz^2 + abt^2$.

If $H = \mathrm{M}(2,K)$, then the conjugation is defined by:

$$\omega = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in H \quad \mapsto \quad \overline{\omega} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}.$$

In this case, reduced trace is $\mathrm{tr}(\omega) = (\alpha + \delta)I$ and reduced norm is $\mathrm{n}(\omega) = (\alpha\delta - \beta\gamma)I$, so they can be identified with the trace and the determinant of ω as a matrix.

1.13 Definition. A quaternion $\omega = x + yi + zj + tij$ in H is called pure if $x = 0$.
Let H_0 denote the K-vector space of pure quaternions. Then $H = K \oplus H_0$.

In fact, this concept is independent of the basis $\{1, i, j, ij\}$ as
$H_0 = \{\omega \in H \mid \omega^2 \in K,\, \omega \notin K\} = \{\omega \in H \mid \overline{\omega} = -\omega\} = \{\omega \in H \mid \mathrm{tr}(\omega) = 0\}$.

Also we denote $H^* = \{\omega \in H \mid \mathrm{n}(\omega) \neq 0\}$.

1.14 Properties. *The reduced norm defines a quadratic form on the subjacent K-vector space V in H.*

1.15 Lemma. *Let $\psi : H \longrightarrow H'$ be an isomorphism of quaternion K-algebras. Consider $H = \left(\frac{a,b}{K}\right)$ endowed with the canonical basis $\{1, i, j, ij\}$. The following properties hold:*

(i) $\psi(i)^2 = a, \quad \psi(j)^2 = b.$

(ii) $\forall \omega \in H$, $\psi(\overline{\omega}) = \overline{\psi(\omega)}$, $\mathrm{n}(\psi(\omega)) = \mathrm{n}(\omega)$, $\mathrm{tr}(\psi(\omega)) = \mathrm{tr}(\omega)$.

(iii) $\psi(H_0) = H'_0$.

In fact, $H \simeq H'$ if and only if V and V' are isometrics, as quadratic spaces.

The norm is going to be helpful to prove if a quaternion algebra is a division algebra or a matrix ring, as we can see answering the following question.

1.16 Question. Why is the Hamilton quaternion algebra a division algebra?

ANSWER: It is easy to prove that $\mathbb{H}^* = \mathbb{H}\backslash\{0\}$, as for every $\omega \in \mathbb{H}$, $\omega \neq 0$,

$$\omega^{-1} = \frac{\overline{\omega}}{n(\omega)}$$

because $n(\omega) = x^2 + y^2 + z^2 + t^2 = 0$ if and only if $x = y = z = t = 0$.

1.17 Question. What about $H = \left(\frac{a, -a}{\mathbb{Q}}\right)$?

ANSWER: Use the norm form to get zero divisors.
It is clear that $x^2 - ay^2 + az^2 - a^2t^t = 0$ has non trivial solutions ($x = at$). Then H contains non invertible elements, so it can not be a division algebra. Thus $\left(\frac{a, -a}{\mathbb{Q}}\right) \simeq \mathrm{M}(2, \mathbb{Q})$.

Thus a key point to distinguish between the two possibilities is:
does the normic form represent 0 or it doesn't?
A quadratic form that represents 0 is called isotropic. Otherwise, anisotropic. Thus to decide which quaternion algebras are matrix rings, we need to study which norm forms are isotropic.

As it is common in the theory of quadratic forms a question on a global field K can be studied going to the local cases K_v, for the places v of K.

For simplicity, from now on, we will restrict to $K = \mathbb{Q}$. There we will consider the associated local fields:
• the real field $\mathbb{R} =: \mathbb{Q}_\infty$, completion of Q with respect the usual absolute value
• the p-adic fields $\mathbb{Q}_p$, completions of Q with respect the p-adic absolute value ($|\alpha|_p = p^{-\mathrm{ord}_p(\alpha)}$.).
Analogous results can be stated for K a number field, considering the local fields K_v, for each place v of K.

1.18 Definition. Given a quaternion K-algebra $H = \left(\frac{a, b}{\mathbb{Q}}\right)$, consider the quaternion algebras $H_p := H \times_{\mathbb{Q}} \mathbb{Q}_p$ and $H_\infty := H \times_{\mathbb{Q}} \mathbb{R}$. Let v any p prime or ∞.
The Hasse invariant at v is defined as

$$\varepsilon(H) = \varepsilon\left(\frac{a, b}{\mathbb{Q}}\right)_v = \begin{cases} -1, & \text{if } H_v \text{ is a division algebra,} \\ & \text{then } H \text{ is said to be ramified at } v \text{ or } v \text{ ramifies in } H \\ 1, & \text{if } H_v \text{ is a matrix algebra,} \\ & \text{then } H \text{ is said to be non-ramified at } v \text{ or } v \text{ does not ramify in } H. \end{cases}$$

By using normic forms it can be proved that the Hasse invariant coincides with the Hilbert Symbol, that is

$$\varepsilon\left(\frac{a,b}{\mathbb{Q}}\right)_v = (a,b)_v$$

where

$$(a,b)_v := \begin{cases} -1, & \text{if } ax^2+b^2=z^2 \text{ only has the trivial solution } x=y=z=0 \text{ in } H_v \\ 1, & \text{if } ax^2+b^2=z^2 \text{ has non trivial solutions in } H_v. \end{cases}$$

In fact Hilbert Symbol can be computed by using Legendre-Jacobi symbols, and it has very nice properties.

1.19 Definition. The reduced discriminant D_H of a quaternion $\mathbb{Q}$-algebra H is the integral ideal of $\mathbb{Z}$ equal to the product of prime ideals of $\mathbb{Z}$ that ramify in H. It can be identified with an integer number (because $\mathbb{Z}$ is a principal ideal domain).

The following classification theorem is well known.

1.20 Theorem. *Consider a quaternion $\mathbb{Q}$-algebra H.*

(i) *H is ramified at a finite even number of places.*

(ii) *Given an even number of non complex places of $\mathbb{Q}$, there exists a quaternion $\mathbb{Q}$-algebra that ramifies exactly at these places.*

(iii) *Two quaternion $\mathbb{Q}$-algebras are isomorphic if and only if they are ramified at the same places, that is they have the same reduced discriminant.*
In particular, H is a matrix $\mathbb{Q}$-algebra if and only if $D_H = 1$.

The isomorphism class of the matrix $\mathbb{Q}$-algebra $\mathrm{M}(2,\mathbb{Q})$ is characterized by $D_H = 1$.

1.21 Example. By using general properties of the Hilbert symbol, the following isomorphisms are obtained:

$$\mathrm{M}(2,\mathbb{Q}) \simeq \left(\frac{1,-1}{\mathbb{Q}}\right) \simeq \left(\frac{1,b}{\mathbb{Q}}\right) \simeq \left(\frac{a,-a}{\mathbb{Q}}\right) \simeq \left(\frac{a,1-a}{\mathbb{Q}}\right),\ a,b \in \mathbb{Q}^*,\ a \neq 1.$$

The explicit isomorphism from $\mathrm{M}(2,\mathbb{Q})$ to $\left(\frac{1,b}{\mathbb{Q}}\right)$, for example, can be seen as a particular example of the morphism defined at 1.9 for $a = 1$:

$$\begin{array}{ccc} \mathrm{M}(2,\mathbb{Q}) & \xrightarrow{\psi} & \left(\frac{1,b}{\mathbb{Q}}\right) \\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} & \rightarrow & \frac{1}{2}((\alpha+\delta)+(\alpha-\delta)i+(\beta+b^{-1}\gamma)j+(\beta-b^{-1}\gamma)ij), \\ \begin{pmatrix} x+y & z+t \\ b(z-t) & x-y \end{pmatrix} & \leftarrow & x+yi+zj+tij, \end{array}$$

The canonical/standard basis $\{i, i, j, ij\}$ of $\left(\frac{1, b}{\mathbb{Q}}\right)$ is mapped to the following basis of $\mathrm{M}(2, \mathbb{Q})$, different from the usual at $\mathrm{M}(2, \mathbb{Q})$, as vectorial space:

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\}.$$

1.22 Definition. A quaternion $\mathbb{Q}$-algebra H is called definite or indefinite according H ramifies or not at infinity.

The definite or indefinite character can be read off from the discriminant.

1.23 Proposition. *Consider* $H = \left(\frac{a, b}{\mathbb{Q}}\right)$. *Then*

(i) *H is definite $\Leftrightarrow$ D_H has an odd number of factors $\Leftrightarrow$ $a < 0$ and $b < 0$.*

(ii) *H is indefinite $\Leftrightarrow$ D_H has an even number of factors $\Leftrightarrow$ $a > 0$ or $b > 0$.*

Note that the embedding defined in 1.9 gives an explicit embedding of H in $\mathrm{M}(2, \mathbb{R})$ in the indefinite case, as we can assume $a > 0$.

1.4 Classification of non-ramified and small ramified quaternion $\mathbb{Q}$-algebras

Let p, q be rational primes. Consider the indefinite quaternion $\mathbb{Q}$-algebras $H = \left(\frac{p, q}{\mathbb{Q}}\right)$.

Denote by $\left(\frac{\cdot}{\cdot}\right)$ the multiplicative symbol of quadratic residues in a wide sense.

For a quaternion $\mathbb{Q}$-algebra $H = \left(\frac{p, q}{\mathbb{Q}}\right)$, we characterize the case of division $\mathbb{Q}$-algebras and we calculate the discriminants, depending on p and q.

Thus, we state the following theorem classifying quaternion algebras $H = \left(\frac{p, q}{\mathbb{Q}}\right)$.

1.24 Theorem. *Let* $H = \left(\frac{p, q}{\mathbb{Q}}\right)$ *be a quaternion algebra. Then, H satisfies one, and only one, of the following statements, interchanging p and q if necessary.*

(i) *$D_H = 1$, and* $H \simeq \mathrm{M}(2, \mathbb{Q}) \simeq \left(\frac{1, -1}{\mathbb{Q}}\right)$.

(ii) *$D_H = 2p$, p prime and $p \equiv 3 \mod 4$, and* $H \simeq \left(\frac{p, -1}{\mathbb{Q}}\right) =: H_A(p)$.

(iii) $D_H = pq$, p, q *primes*, $q \equiv 1 \mod 4$, $\left(\frac{p}{q}\right) = -1$, *and* $H \simeq \left(\frac{p,q}{\mathbb{Q}}\right) =: H_B(p,q)$.

Proof is straightforward using properties of Hilbert symbol. It can be done proving the items in next proposition.

1.25 Proposition. *Let* $H = \left(\frac{p,q}{\mathbb{Q}}\right)$, p, q *primes.*

(i) $D_H = 1$ *if and only if one of the following conditions are satisfied:* $p = q = 2$; $p = q \equiv 1 \mod 4$; $q = 2$ *and* $p \equiv \pm 1 \mod 8$; $p \neq q$, $p \neq 2$, $q \neq 2$, $\left(\frac{q}{p}\right) = 1$, *and either* p *or* q *is congruent to* $1 \mod 4$.

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

(iii) *If* $q = 2$, $p \equiv 3 \mod 8$, *then* $D_H = pq = 2p$.

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

1.26 Definition. According to the definition 1.18, we call *non-ramified* $\mathbb{Q}$*-algebras* the quaternion $\mathbb{Q}$-algebras having discriminant 1; that is, the algebras isomorphic to $\mathrm{M}(2,\mathbb{Q})$. We call *small ramified* $\mathbb{Q}$*-algebras* the quaternion $\mathbb{Q}$-algebras having discriminant equal to the product of two distinct prime numbers.
We say that a small ramified $\mathbb{Q}$-algebra is of type A if it is isomorphic to $H_A(p)$, and that it is of type B if it is isomorphic to $H_B(p,q)$, for some primes p,q.

We complete theorem 1.24 by giving a representative for each isomorphism class of small ramified $\mathbb{Q}$-algebras.

1.27 Proposition. *Let* H *be a quaternion* $\mathbb{Q}$*-algebra of discriminant* $D_H = pq$, p *and* q *two different prime numbers.*

(i) *If* $p \equiv 3 \mod 4$ *and* $q = 2$, *then* $H \simeq \left(\frac{p,-1}{\mathbb{Q}}\right)$.

(ii) *If* $p \equiv 5 \mod 8$ *and* $q = 2$, *the* $H \simeq \left(\frac{p,2}{\mathbb{Q}}\right)$.

(iii) *If* $p \equiv 1 \mod 8$ *and* $q = 2$, *then* $H \simeq \left(\frac{2p,-r}{\mathbb{Q}}\right)$, *where* r *is a prime number such that* $\left(\frac{r}{p}\right) = \left(\frac{r}{2}\right) = -1$.

(iv) *If* p *or* $q \equiv 1 \mod 4$ *and* $\left(\frac{q}{p}\right) \neq 1$, *then* $H \simeq \left(\frac{p,q}{\mathbb{Q}}\right)$.

(v) *If* p *or* $q \equiv 1 \mod 4$ *and* $\left(\frac{q}{p}\right) = 1$*, then* $H \simeq \left(\frac{pq, -r}{\mathbb{Q}}\right)$*, where* r *is a prime number such that* $\left(\frac{r}{s}\right) = \pm 1$ *according to* $s \equiv \mp 1 \mod 4$*, respectively, for* $s = p, q$*; moreover, if* p *or* $q \equiv 3 \mod 4$*, necessarily* $r \equiv 3 \mod 4$*.*

(vi) *If* $p \equiv q \equiv 3 \mod 4$*, then* $H \simeq \left(\frac{pq, -1}{\mathbb{Q}}\right)$*.*

PROOF: (The conditions over the primes p and q cover all the possibilities. Thus, it is only necessary to check the discriminant in each case.

Statements in (i) and (iv) come from previous lemmas.

Note that $(2, p)_p = (2, p)_2 = -1$ if and only if $p \equiv \pm 5 \mod 8$, and the case $p \equiv 3 \mod 8$ is included in (i). This proves (ii).

For (iii), let us see that there always exists at least one prime r verifying those conditions. The condition $\left(\frac{r}{2}\right) = -1$ is equivalent to $r \equiv \pm 5 \mod 8$; fix for example the positive sign. To satisfy the other condition, fix $b \in \mathbb{Z}$ such that $\left(\frac{b}{p}\right) = -1$. We want to look for primes r satisfying $r \equiv b \mod p$. Since $(8, p) = 1$, by Chinese remainder theorem, the system of congruences $x \equiv 5 \mod 8$, $x \equiv b \mod p$ has a solution: $x \equiv x_0 \mod 8p$. The solutions in $\mathbb{Z}$ form the arithmetic progression $\{x_0, x_0 + 8p, x_0 + 2 \cdot 8p, \ldots\}$, and by Dirichlet theorem, assuming $(x_0, 8p) = 1$, there are infinitely many primes r. Actually, we have $2 \nmid x_0$ since $x_0 \equiv 5 \mod 8$, and $p \nmid x_0$ since $x_0 \equiv b \mod p$ and $b \neq 0$. It just remains to check the discriminant of the quaternion algebra in (iii) is $pq = 2p$. Computations with the Hilbert symbol give $\varepsilon_v := (2p, -r)_v = (2, -1)_v(2, r)_v(p, -1)_v(p, r)_v = (2, r)_v(p, r)_v$. In particular, $\varepsilon_p = \left(\frac{r}{p}\right)$, $\varepsilon_2 = \left(\frac{r}{2}\right)$ and $\varepsilon_p = -\left(\frac{p}{r}\right)$. The conditions in (iii) for r are equivalent to asking $\varepsilon_p = \varepsilon_2 = -1$. Now the quadratic reciprocity law gives $\varepsilon_r = 1$.

Analogous arguments work for (v). In this case, to find the discriminant, we have $\varepsilon_v = (pq, -r)_v = (p, -1)_v(p, r)_v(q, -1)_v(q, r)_v$. Assume $p \equiv 1 \mod 4$; otherwise, replace p with q. Then, $\varepsilon_p = (p, -1)_p(p, r)_p = \left(\frac{r}{p}\right) = -1$. If $q \equiv 1 \mod 4$, then $\left(\frac{r}{q}\right) = -1$; so, $\varepsilon_q = (q, -1)_q(q, r)_q = -1$ and $\varepsilon_r = (p, r)_r(q, r)_r = 1$; thus the discriminant is pq. If $q \equiv 3 \mod 4$, we have $\left(\frac{r}{q}\right) = 1$; so, $\varepsilon_q = (q, -1)_q(q, r)_q = -1$, and $\varepsilon_r = (p, r)_r(q, r)_r = 1$, since $r \equiv 3 \mod 4$; thus, the discriminant is also pq. The condition over $\left(\frac{r}{q}\right)$ is equivalent to $\varepsilon_q = -1$. Note, that for $\varepsilon_q = -\varepsilon_r$ to be satisfied, it is necessary to exclude the case $q \equiv 3 \mod 4$, $r \equiv 1 \mod 4$.

Finally, it is clear that the quaternion algebra in (vi) has discriminant pq. □

1.5 Quaternion orders

Let H be a quaternion $\mathbb{Q}$-algebra, $H = \left(\frac{a,b}{\mathbb{Q}}\right)$. Assume $a, b \in \mathbb{Z}$ square free.

1.28 Definition. An element $\alpha \in H$ is said to be integral over $\mathbb{Q}$ if $\mathrm{n}(\alpha)$ and $\mathrm{tr}(\alpha)$ are in $\mathbb{Z}$. In general, the set of all integral elements in a quaternion algebra is not a ring.

1.29 Definition. An $\mathbb{Z}$-order $\mathcal{O}$ of H is a subring of H, whose elements are integral, that contains $\mathbb{Z}$ and $\mathbb{Q} \otimes \mathcal{O} = H$.

For example $Z[1, i, i, ij]$ is an order. Note that to prove $R = Z[v_1, v_2, v_3, v_4]$ is an order it is enough to prove:
- it contains the unit 1 and it is closed for the product,
- $\mathrm{n}(v_i), \mathrm{tr}(v_i), \mathrm{n}(v_i + v_j), \mathrm{tr}(v_i v_j) \in Z$.

1.30 Definition. Every $\mathbb{Z}$-order $\mathcal{O}$ has associated an ideal $D_{\mathcal{O}}$ called reduced discriminant, defined by certain technical conditions, and computable by using next proposition. Over $\mathbb{Z}$ it can be identified with an integer.
$D_{\mathcal{O}}$ is defined as the reduced norm of the bilateral $\mathbb{Z}$-ideal $\mathcal{D}(\mathcal{O})$, computed as the inverse of the dual of $\mathcal{O}$ by the bilinear form given by the reduced trace. Thus, $\alpha \in \mathcal{D}(\mathcal{O})^{-1}$ if and only if $\mathrm{tr}(\alpha\mathcal{O}) \subseteq \mathbb{Z}$ and $D_{\mathcal{O}} = n(\mathcal{D}(\mathcal{O}))$.

1.31 Proposition. *The reduced discriminant $D_{\mathcal{O}}$ of a $\mathbb{Z}$-order $\mathcal{O}$ satisfies:*

(i) *$D_{\mathcal{O}}^2$ is equal to the ideal generated by $\{\det(\mathrm{tr}(\omega_i \omega_j)) \mid 1 \le i, j \le 4, \omega_i, \omega_j \in \mathcal{O}\}$.*

(ii) *If $\{v_1, \dots, v_4\}$ is an R-basis of the order $\mathcal{O}$, then $D_{\mathcal{O}}^2 = \det(\mathrm{tr}(v_i v_j))$.*

(iii) *$\mathcal{O} \subseteq \mathcal{O}'$ be $\mathbb{Z}$-orders in $H \Rightarrow D_{\mathcal{O}'} \mid D_{\mathcal{O}}$.*
$D_{\mathcal{O}'} = D_{\mathcal{O}} \Rightarrow \mathcal{O} = \mathcal{O}'$ the two are equal if and only if $\mathcal{O} = \mathcal{O}'$.

1.32 Corollary. *Let $\mathcal{O} \subseteq \left(\frac{a,b}{\mathbb{Q}}\right)$ be an order given by a $\mathbb{Z}$-basis $\mathcal{B}$.*
Let P be the matrix of the change of basis from the $\mathcal{B}$-coordinates to the canonical coordinates. Then, $D_{\mathcal{O}} = |4ab \det P|$.

PROOF: By the above proposition, $D_{\mathcal{O}}^2 = |\det(\mathrm{tr}(v_i v_j))|$ for $\mathcal{B} = \{v_1, v_2, v_3, v_4\}$. We refer by M to the matrix of the bilinear form defined by the trace with respect to the canonical basis. By properties of change of basis, we have $D_{\mathcal{O}}^2 = |\det M|(\det P)^2 = 16a^2b^2(\det P)^2$.
□

1.33 Exercise. Consider the quaternion order $Z[1, i, i, ij]$. Compute its discriminant.

1.34 Lemma. (i) *Each order is contained in a maximal order.*

(ii) *$\mathcal{O}$ is maximal if and only if $\mathcal{O}_v$ is maximal, for every finite place v.*

(iii) *$\mathcal{O}$ is a maximal R-order if and only if $D_{\mathcal{O}} = D_H$.*
In particular, all maximal orders have the same discriminant.

This result is useful for recognizing maximal orders.
For example, $\mathrm{M}(2, R)$ is a maximal R-order of $\mathrm{M}(2, K)$, since it has reduced discriminant equal to R.

1.35 Exercise. Consider the quaternion order $\mathcal{O} = Z[1, i, i, ij]$ in the small ramified quaternion algebra of type A $H_A(3) = \left(\frac{3, -1}{\mathbb{Q}}\right)$. Is $\mathcal{O}$ a maximal order?

In the construction of Shimura curves, we need orders derived from maximal orders.

1.36 Definition. An Eichler order in a quaternion algebra is the intersection of two maximal orders.

The following proposition gives characterizations of Eichler orders.

1.37 Proposition. *Let $\mathcal{O}$ be an order in a quaternion $\mathbb{Q}$-algebra H of discriminant D. Let $N \subset \mathbb{Z}$ be coprime to D. Then, the following conditions are equivalent:*

(a) *$\mathcal{O}$ is an Eichler order of level N.*

(b) *For every prime $p \in \mathbb{Z}$, $\mathcal{O}$ satisfies: if $p \nmid N$, the local $\mathbb{Z}_p$-order $\mathcal{O}_p$ is maximal, and if $p | N$, $\mathcal{O}_p$ is isomorphic to the order $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ N\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.*

(c) *For every prime $p \in \mathbb{Z}$, $\mathcal{O}$ satisfies: if $p | D$, the local $\mathbb{Z}_p$-order $\mathcal{O}_p$ is maximal, and if $p \nmid D$, $\mathcal{O}_p$ is isomorphic to the order $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ N\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.*

We will denote by $\mathcal{O}(D, N)$ an Eichler order of level N in a quaternion algebra of discriminant D.

Unlike the case of maximal orders (cf. 1.34), there is no explicit characterization of Eichler orders in terms of their discriminant, but the following properties allow us to determine some Eichler orders.

1.38 Proposition. *Let H be a quaternion $\mathbb{Q}$-algebra of discriminant D.*

(i) *For each integer N such that $\gcd(D, N) = 1$, there exist Eichler orders of level N.*

(ii) *Let $\mathcal{O}(D, N) \subseteq \mathcal{O}(D, 1)$. Then, the index as $\mathbb{Z}$-modules is $[\mathcal{O}(D, 1) : \mathcal{O}(D, N)] = N$.*

(iii) *For $\mathcal{O} = \mathcal{O}(D, N)$, $\quad D_{\mathcal{O}} = DN$.*

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

1.39 Theorem. (cf. [Vig80]) *Let K be a totally real number field, and let H be an indefinite quaternion K-algebra. If the ideal class number of K is odd, there is only one conjugacy class of Eichler orders having the same level.*

In particular for indefinite quaternion rational algebras, all Eicher orders having the same level are conjugated.

1.6 Special basis for orders in quaternion algebras

In what follows, we consider the case $K = \mathbb{Q}$ and determine bases with special conditions.

1.40 Definition. Let $\mathcal{B} = \{v_1, v_2, v_3, v_4\}$ be a $\mathbb{Q}$-basis of H. We define the character $\chi(\mathcal{B})$ of the basis $\mathcal{B}$ by the 1×4 matrix over $\mathbb{Q}$ associated with the trace linear form: $\chi(\mathcal{B}) = (\mathrm{tr}(v_1), \mathrm{tr}(v_2), \mathrm{tr}(v_3), \mathrm{tr}(v_4))$.

1.41 Definition. Let $\mathcal{B} = \{v_1, v_2, v_3, v_4\}$ be a $\mathbb{Q}$-basis of H. We say that $\mathcal{B}$ is a normalized basis if $v_1 = 1$ and its character is $\chi(\mathcal{B}) = (2, 0, 0, 1)$ or $(2, 0, 0, 0)$; that is, $v_1 = 1$, $v_2, v_3 \in H_0$ and $\mathrm{tr}(v_4) \in \{0, 1\}$. We say that $\mathcal{B}$ is an even normalized basis in the first case, and an odd normalized basis in the second one.

1.42 Lemma. *Let $\mathcal{O}$ be an order in a quaternion $\mathbb{Q}$-algebra H.*

(i) *There exist normalized $\mathbb{Z}$-bases in $\mathcal{O}$. Its character is an invariant of the order, denoted by $\chi(\mathcal{O})$.*

(ii) *Let $Q \in \mathrm{GL}(4, \mathbb{Z})$. Then Q is the matrix of a change of basis between two normalized $\mathbb{Z}$-bases in $\mathcal{O}$ if and only if $\chi(\mathcal{O})$ is a left eigenvector corresponding to the eigenvalue 1 of Q.*

Proof: Let us construct a normalized $\mathbb{Z}$-basis of $\mathcal{O}$. The order $\mathcal{O}$ admits a $\mathbb{Z}$-basis of the form $\{1, u_2, u_3, u_4\}$, cf. [God78]. Put $u_i' = u_i - [\frac{\mathrm{tr}(u_i)}{2}]$, for $i = 2, 3, 4$. If $u_i' \in H_0$, for every i, we are done. Otherwise, up to permutation, we can assume $\mathrm{tr}(u_4') = 1$. Then, by putting $v_4 = u_4'$ and $v_i = u_i' - \mathrm{tr}(u_i')u_4'$ for $i = 2, 3$, we obtain a normalized basis $\{1, v_2, v_3, v_4\}$. Note that if $\mathrm{tr}(v_4) = 0$, then every element in $\mathcal{O}$ has even trace. The converse is also true. Hence, $\mathrm{tr}(v_4) = 1$ if and only if there exists an element in $\mathcal{O}$ with odd trace. Thus, any normalized basis in $\mathcal{O}$ has the same character.

The condition in (ii) simply means $\chi(\mathcal{O}) = \chi(\mathcal{O})Q$, which follows from (i) by the change of basis relation. □

Next, we introduce the concept of denominator of a $\mathbb{Z}$-order.

1.43 Definition. Let $\mathcal{O}$ be an order in a quaternion $\mathbb{Q}$-algebra H. We define the denominator $m_{\mathcal{O}}$ of $\mathcal{O}$ as the minimal positive integer such that $m_{\mathcal{O}} \cdot \mathcal{O} \subseteq \mathbb{Z}[1, i, j, ij]$. Then the ideal $(m_{\mathcal{O}})$ is the conductor of $\mathcal{O}$ in $\mathbb{Z}[1, i, j, ij]$.

1.44 Lemma. *Let $\mathcal{O}$ be an order in a quaternion $\mathbb{Q}$-algebra H. Fix a basis $\mathcal{B}$ of $\mathcal{O}$ and the canonical basis $\mathcal{C} = \{1, i, j, ij\}$ of H. Let P be the matrix of change of basis from the $\mathcal{B}$-coordinates to the $\mathcal{C}$-coordinates. Then $m_{\mathcal{O}}$ is the minimal positive integer such that the matrix $m_{\mathcal{O}}P$ has entries in $\mathbb{Z}$. Moreover, if $\mathcal{O} \subseteq \mathcal{O}'$, then $m_{\mathcal{O}} | m'_{\mathcal{O}}$.*

1.45 Remark. *Consider the order* $\mathrm{M}(2, \mathbb{Z})$ *in the quaternion algebra* $H = \mathrm{M}(2, \mathbb{Q})$. *Consider the following bases of* H:

$$\mathcal{C} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\},$$
$$\mathcal{B} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\},$$
$$\mathcal{B}' = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

The canonical basis $\mathcal{C}$ of H, given by the isomorphism in 1.21, is not a $\mathbb{Z}$-basis of the order $\mathrm{M}(2, \mathbb{Z})$, *in spite of having integral entries in all the matrices. Both $\mathcal{B}$ and $\mathcal{B}'$ are bases of* $\mathrm{M}(2, \mathbb{Z})$. *Although $\mathcal{B}$ is the usual one, only $\mathcal{B}'$ is normalized.*

The denominator of $\mathrm{M}(2, \mathbb{Z})$ *is* 2.

1.7 More on Eichler orders

Suppose that K is a number field with ring of integers R. For a finite place v, consider the local field K_v, the ring of integers R_v and π an uniformizer of R_v.

For H is a quaternion K-algebra consider the quaternion K_v-algebra $H_v = K_v \otimes H$.

For an R-order $\mathcal{O}$, put $\mathcal{O}_v := R_v \otimes \mathcal{O}$.
If v is a finite place, $\mathcal{O}_v$ is a local R_v-order; if v is an infinite place, consider $R_v = K_v$ and $\mathcal{O}_v = H_v$.
Then $\mathcal{O} = H \cap (\prod_v \mathcal{O}_v)$ and $(D_{\mathcal{O}})_v = D_{\mathcal{O}_v}$.

1.46 Lemma. (i) *Each order is contained in a maximal order.*

(ii) *$\mathcal{O}$ is maximal if and only if $\mathcal{O}_v$ is maximal, for every finite place v.*

(iii) *$\mathcal{O}$ is a maximal R-order if and only if $D_{\mathcal{O}} = D_H$.*
In particular, all maximal orders have the same discriminant.

This result is useful for recognizing maximal orders.
For example, $\mathrm{M}(2, R)$ is a maximal R-order of $\mathrm{M}(2, K)$, since it has reduced discriminant equal to R.

In the construction of Shimura curves, we need orders derived from maximal orders.

1.47 Definition. An Eichler order in a quaternion algebra is the intersection of two maximal orders.

1.48 Proposition. *$\mathcal{O}$ is an Eichler order if and only if $\mathcal{O}_v$ is an Eichler R_v-order for every finite place v.*

We recall that H_v is either a division algebra or a matrix algebra.

1.49 Lemma. *Let H_v be a local division K_v-algebra. Then $\mathcal{O}_v = \{h \in H_v : n(h) \in R_v\}$ is the unique maximal R_v-order, hence the unique Eichler R_v-order in H_v.*

PROOF: (Assume that H_v is a division algebra. Let v be a discrete valuation of K_v. Then for $h \in H_v$, $\widetilde{v}(h) := v(\mathrm{n}(h))$ defines a discrete valuation in H_v.

The valuation ring of $\widetilde{v}$ is $\mathcal{O}_v = \{h \in H_v : \widetilde{v}(h) \in R_v\} \subseteq H_v$, cf. [Vig80]. For every local field F_v, with $K_v \subseteq F_v \subseteq H_v$, the restriction of $\widetilde{v}$ to F_v is also a discrete valuation having valuation ring $\mathcal{O}_v \cap F_v$ equal to the ring of integers in F_v. Hence all the elements in $\mathcal{O}_v$ are integral over R_v and $\mathcal{O}_v$ is an order. Since it contains all the integral elements of H_v, it is a maximal order, the unique one.) $\square$

1.50 Lemma. *Let $H_v = \mathrm{M}(2, K_v)$. Then the maximal R_v-orders in H_v are the $\mathrm{GL}(2, K_v)$-conjugate orders of $\mathcal{O}_v = \mathrm{M}(2, R_v)$.*

1.51 Proposition. *Let $\mathcal{O}_v \subseteq \mathrm{M}(2, K_v)$ be an R_v-order. The following conditions are equivalent:*

(a) *$\mathcal{O}_v$ is an Eichler order.*

(b) *There exists a unique pair $\{\mathcal{O}_1, \mathcal{O}_2\}$ of maximal orders of $\mathrm{M}(2, K_v)$ such that $\mathcal{O}_v = \mathcal{O}_1 \cap \mathcal{O}_2$.*

(c) *There exists a unique $n \in \mathbb{N} \cup \{0\}$ such that the order $\mathcal{O}_v$ is conjugate to the order*

$$\mathcal{O}_{\underline{n}} := \begin{pmatrix} R_v & R_v \\ \pi^n R_v & R_v \end{pmatrix} = \mathrm{M}(2, R_v) \cap \begin{pmatrix} R_v & \pi^{-n} R_v \\ \pi^n R_v & R_v \end{pmatrix},$$

which is an Eichler R_v-order, called the canonical Eichler order of level $\pi^n R_v$.

The ideal $N_{\mathcal{O}_v} := \pi^n R_v$, determined in statement (c)*, is called the level of $\mathcal{O}_v \subseteq \mathrm{M}(2, K_v)$.*

Condition (c) tells us that all the local Eichler orders of the same level are conjugate. Actually the local rings of integers R_v are principal. When the global ring of integers R is also principal and the quaternion algebra is indefinite, then the global Eichler orders are also conjugate, by the Eichler result (cf. 1.57).

The following definition makes precise the concept of level for any local Eichler order $\mathcal{O}_v$.

1.52 Definition. Let $\mathcal{O}_v$ be an Eichler order in a quaternion K_v-algebra H_v. The level of $\mathcal{O}_v$ is the ideal

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

1.53 Remark. *For the canonical Eichler order $\mathcal{O}_{\underline{n}} \in \mathrm{M}(2, K_v)$, it is easy to check that $D_{\mathcal{O}_{\underline{n}}} = \pi^n R_v$. Since the discriminant is preserved by isomorphisms, for any Eichler order $\mathcal{O}_v \subseteq H_v \simeq \mathrm{M}(2, K_v)$ the discriminant and the level coincide: $D_{\mathcal{O}_v} = N_{\mathcal{O}_v}$*

1.54 Definition. The level $N_{\mathcal{O}}$ of a global Eichler order $\mathcal{O}$ is the unique integral ideal N in R such that N_v is the level of each $\mathcal{O}_v$ at each finite place v of K. Thus, $N_{\mathcal{O}} := \prod_v N_{\mathcal{O}_v}$.

We will denote by $\mathcal{O}(D, N)$ an Eichler order of level N in a quaternion algebra of discriminant D.

The following proposition, stated in the case $K = \mathbb{Q}$, gives characterizations of Eichler orders.

1.55 Proposition. *Let $\mathcal{O}$ be an order in a quaternion $\mathbb{Q}$-algebra H of discriminant D. Let $N \subset \mathbb{Z}$ be coprime to D. Then, the following conditions are equivalent:*

(a) *$\mathcal{O}$ is an Eichler order of level N.*

(b) *For every prime $p \in \mathbb{Z}$, $\mathcal{O}$ satisfies: if $p \nmid N$, the local $\mathbb{Z}_p$-order $\mathcal{O}_p$ is maximal, and if $p|N$, $\mathcal{O}_p$ is isomorphic to the order $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ N\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.*

(c) *For every prime $p \in \mathbb{Z}$, $\mathcal{O}$ satisfies: if $p|D$, the local $\mathbb{Z}_p$-order $\mathcal{O}_p$ is maximal, and if $p \nmid D$, $\mathcal{O}_p$ is isomorphic to the order $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ N\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.*

Unlike the case of maximal orders (cf. 1.34), there is no explicit characterization of Eichler orders in terms of their discriminant, but the following properties allow us to determine some Eichler orders.

1.56 Proposition. *Let H be a quaternion $\mathbb{Q}$-algebra of discriminant D.*

(i) *For each integer N such that $\gcd(D, N) = 1$, there exist Eichler orders of level N.*

(ii) *Let $\mathcal{O}(D, N) \subseteq \mathcal{O}(D, 1)$. Then, the index as $\mathbb{Z}$-modules is $[\mathcal{O}(D, 1) : \mathcal{O}(D, N)] = N$.*

(iii) *For $\mathcal{O} = \mathcal{O}(D, N)$, $D_{\mathcal{O}} = DN$.*

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

Eichler orders of the same level are locally conjugate. The following result proved by Eichler states a global conjugation. In particular, it ensures that Eichler orders with the same level in indefinite quaternion $\mathbb{Q}$-algebras are also globally conjugate.

1.57 Theorem. (cf. [Vig80]) *Let K be a totally real number field, and let H be an indefinite quaternion K-algebra. If the ideal class number of K is odd, there is only one conjugacy class of Eichler orders having the same level.*

1.8 Eichler orders in non-ramified and small ramified $\mathbb{Q}$-algebras

In the following proposition we provide explicit Eichler orders in non-ramified and small ramified quaternion $\mathbb{Q}$-algebras. In the particular case $N = 1$, they are maximal orders.

1.58 Proposition. *Let $N \geq 1$, and p, q different primes.*

(i) $\mathcal{O}_0(1,N) := \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} : a,b,c,d \in \mathbb{Z} \right\}$ *is an Eichler order of level N in the matrix algebra* $\mathrm{M}(2,\mathbb{Q})$.
$\mathcal{O}_M(1,N) := \mathbb{Z}\left[1, \frac{j+ij}{2}, N\frac{(-j+ij)}{2}, \frac{1-i}{2}\right]$ *is an Eichler order of level N in the matrix algebra* $\left(\frac{1,-1}{\mathbb{Q}}\right)$.

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

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

(iv) $\mathbb{Z}\left[1, i, j, \frac{1+i+j+ij}{2}\right]$ *is an Eichler order of H of level q in the $\mathbb{Q}$-algebra $H = \left(\frac{p,q}{\mathbb{Q}}\right)$ of type A, with $q \equiv 3 \mod 4$ and $D_H = 2p$.*

Proof: (Firstly, we need to ensure that the given $\mathbb{Z}$-module $\mathcal{O}$ is an order in the corresponding quaternion algebra. Secondly, we compute the discriminant $D_{\mathcal{O}}$ of the order and use the fact that $D_{\mathcal{O}} = D_H N$ is an square-free integer. Then $\mathcal{O}$ will be an Eichler order of level N.

The case (i) is clear.

Let us prove (ii). The condition $N | \frac{p-1}{2}$ ensures us that $\mathcal{O}_A(2p,N)$ is a $\mathbb{Z}$-order in $H_A(p)$. We compute $D_{\mathcal{O}_A(2p,N)} = 2pN$ and compare with $D_{H_A(p)} = 2p$, cf. 1.25. Putting together the conditions over N and p, note that N and $2p$ are coprime. Then, $\mathcal{O}_A(2p,N)$ is an Eichler order of level N.

Let us prove (iii). The condition $N | \frac{q-1}{4}$ ensures us that $\mathcal{O}_B(pq,N)$ is a $\mathbb{Z}$-order in $H_B(p,q)$. Its discriminant is $D_{\mathcal{O}_B(pq,N)} = pqN$. In this case, $D_{H_B(p,q)} = pq$, and automatically $\gcd(N,q) = 1$. Restrict ourselves to N and p coprime, then $\mathcal{O}_B(pq,N)$ is an Eichler order of level N.

In case (iv), the condition on the discriminant implies $p \equiv 3 \mod 4$. It is easy to check that $\mathbb{Z}\left[1, i, j, \frac{1+i+j+ij}{2}\right]$ is a $\mathbb{Z}$-order of discriminant $2pq$. We thus obtain that the given order is an Eichler order of level q.) $\square$

We also are able to construct Eichler orders for other levels. We computed tables with explicit $\mathbb{Z}$-bases for representative orders of the conjugacy classes of Eichler orders of consecutive levels N in the small ramified algebras $H_A(3)$, $H_B(2,5)$, $H_A(7)$ and $H_B(3,5)$.

Chapter 2

Introduction to Fuchsian groups

The goal of this chapter is to introduce Fuchsian groups and describe its action on the Poincaré half plane.

A full chapter could be devoted to describe the hyperbolic structure of the Poincaré half plane, but we will state only main definitions and results.

Let $\tilde{\mathbb{C}}$ denote $\mathbb{C} \cup \{\infty\}$ the complex plane with a point at infinity, also known as the Riemann sphere.

The Poincaré half plane is the complex upper half plane $\mathcal{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ endowed with the structure given by the hyperbolic metric.

2.1 Linear fractional transformations

In this section, we describe the transformations acting on $\tilde{\mathbb{C}}$, and specially on the Poincaré half plane. We classify them by their Jordan matrix and by their associated binary quadratic form. General definitions and known results can be found in [Poi1887], [Shi71] and [Sie71] and Koblitz book.

A linear fractional transformation (or homographic transformation, or Moebius transformation) $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{R})$ on $\tilde{\mathbb{C}}$ is defined by

$$\gamma(z) := \frac{az+b}{cz+d}, \forall z \in \mathbb{C} \quad \gamma(\infty) := \frac{a}{c} = lim_{z\to\infty}\gamma(z).$$

Thus, $\gamma(-d/c) = \infty$ and if $c = 0$ $\gamma(\infty) = \infty$.

Note that for $\gamma = -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, we have $\gamma(z) = z$.

Actually, $\pm I$ are the only matrices which act trivially on $\tilde{\mathbb{C}}$. We can see it as

$$z = \gamma(z) = (az+b)/(cz+d), \forall z \Leftrightarrow cz^2 + (d-a)z - b = 0 \, \forall z$$

implies that $c = b = 0$ and $d = a$, that is $\gamma = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. But since $\det\gamma = 1$, we get $\gamma = \pm I$. Thus the set of these transformations is a group isomorphic to $\mathrm{PSL}(2,\mathbb{R}) = \mathrm{SL}(2,\mathbb{R})/(\pm\,\mathrm{Id})$, which acts faithfully on $\mathbb{C}$, that is, each element other than identity acts nontrivially.

Note that any $\gamma \in \mathrm{SL}(2,\mathbb{R})$ preserves the upper half-plane $\mathcal{H}$, as $\mathrm{Im}(z) > 0$ implies $\mathrm{Im}(\gamma(z)) > 0$. This is because

$$\mathrm{Im}\,\gamma(z) = \mathrm{Im}\,\frac{az+b}{cz+d} = \mathrm{Im}\,\frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = |cz+d|^{-2}\,\mathrm{Im}(adz+bc\overline{z}).$$

But $\mathrm{Im}(adz+bc\overline{z}) = (ad-bc)\,\mathrm{Im}\,z = \mathrm{Im}\,z$. Thus

$$\mathrm{Im}\,\gamma(z) = |cz+d|^{-2}\,\mathrm{Im}\,z.$$

The subgroup of $\mathrm{SL}(2,\mathbb{R})$ consisting of matrices with integer entries is $\mathrm{SL}(2,\mathbb{Z})$, and it is called the full modular group.

Important subgroups are

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \mod N \right\}.$$

2.2 Classification of homographies

To compute the fixed points of $\gamma \in \mathrm{SL}(2,\mathbb{R})$ acting on $\mathbb{C} \cup \{\infty\}$, it is necessary to solve the quadratic equation $cz^2 + (d-a)z - b = 0$. This leads to the following well-known equivalent definitions.

2.1 Definition. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$. Assume that γ defines a transformation of $\mathbb{C}$ different from $\pm\,\mathrm{Id}$.

(a) We call γ an hyperbolic transformation if it has two different fixed points in $\mathbb{R}\cup\{\infty\}$; equivalently, if $(a+d)^2 > 4$; or if $|\operatorname{tr}(\gamma)| > 2$.

(b) We call γ an elliptic transformation if it has a fixed point $z \in \mathcal{H}$ and the other fixed point is $\overline{z}$; equivalently, if $(a+d)^2 < 4$; or if $|\operatorname{tr}(\gamma)| < 2$.

(c) We call γ a parabolic transformation if it has a unique fixed point in $\mathbb{R} \cup \{\infty\}$; equivalently, if $(a+d)^2 = 4$; or if $|\operatorname{tr}(\gamma)| = 2$.

Let us see the possible Jordan forms.

Each matrix $\gamma \in \mathrm{SL}(2,\mathbb{R})$, $\gamma \neq \pm\,\mathrm{Id}$, is conjugate over $\mathbb{C}$ to one of the following canonical Jordan forms:

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \text{ with } \lambda \in \mathbb{C}^*,\ \lambda \neq \pm 1, \quad \text{or} \quad \begin{pmatrix} \pm 1 & 0 \\ 1 & \pm 1 \end{pmatrix}.$$

The parabolic, hyperbolic or elliptic condition of a transformation can be read from the eigenvalues of its matrix, as we can see in the following lemma.

2.2 Lemma. *Given a transformation $\gamma \in \mathrm{SL}(2,\mathbb{R})$, let λ, λ^{-1} denote its complex eigenvalues and put $\mu := \dfrac{\lambda}{\lambda^{-1}} = \lambda^2$. Then,*

(i) *γ is hyperbolic if and only if $\mu \in \mathbb{R}^+$ and $\mu \neq 1$. In particular, if γ is hyperbolic, then the two eigenvalues are different and γ is diagonalizable.*

(ii) *γ is elliptic if and only if $\mu = e^{\iota\theta}$ and $0 < \theta < 2\pi$; in this case $\lambda + \lambda^{-1} = 2\cos\theta$. In particular, if γ is elliptic, then the two eigenvalues are different and γ is diagonalizable.*

(iii) *γ is parabolic if and only if $\mu = 1$. In particular, if γ is parabolic, it only has one eigenvalue but the eigenspace has dimension 1, thus γ is not diagonalizable.*

In the non parabolic cases, the value μ is called the multiplicator of γ. It has the following geometric interpretation. Consider the transformation γ given by some matrix M, and consider the change of variables transforming M in the corresponding Jordan matrix. If γ is hyperbolic or elliptic, this change of variables maps the two fixed points to 0 and infinity, respectively. Then the transformation is geometrically an homothety of ratio μ with center in the origin in the hyperbolic case, and a rotation of angle θ equal to the argument of μ around the origin in the elliptic case. In the case of a parabolic transformation, the change of variables maps its unique fixed point to infinity and geometrically it is a translation.

Elliptic transformations such that $\theta = r\pi$, with $r \in \mathbb{Q}^*$, have finite order. Parabolic transformations have infinite order.

2.3 Lemma. *Let $\gamma \in \Gamma \subseteq \mathrm{SL}(2,\mathbb{R})$ define an elliptic transformation in the group $\mathrm{PSL}(2,\mathbb{R})$. If $\mathrm{tr}(\gamma) = 0$, then γ has order 2 or 4 in $\mathrm{PSL}(2,\mathbb{R})$, depending on $-\mathrm{Id} \in \Gamma$ or $-\mathrm{Id} \notin \Gamma$, respectively. If $\mathrm{tr}(\gamma) = 1$, then γ has order 3 or 6 in $\mathrm{PSL}(2,\mathbb{R})$, depending on $-\mathrm{Id} \in \Gamma$ or $-\mathrm{Id} \notin \Gamma$, respectively. These are the two only possibilities for the elliptic transformations with integral traces.*

The classification of the transformations and their fixed points can be also interpreted in terms of suitable binary quadratic forms and their associated points.

2.4 Definitions. Given a matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}(2,\mathbb{R})$, the binary quadratic form associated with it is $f_\gamma(X,Y) := cX^2 + (d-a)XY - bY^2$.

The geometric interpretation given in the following proposition justifies the names of the transformations.

2.5 Proposition. *Let $\gamma \in \mathrm{SL}(2,\mathbb{R})$ and consider the associated binary form f_γ. Let $\kappa \in \mathbb{R}$, $\kappa \neq 0$. Then:*

(i) *γ is hyperbolic if and only if the conic $f_\gamma = \kappa$ is a hyperbola.*

(ii) *γ is elliptic if and only if the conic $f_\gamma = \kappa$ is an ellipse.*

(iii) *γ is parabolic if and only if the conic $f_\gamma = \kappa$ is a parabola.*

PROOF: Consider the binary quadratic form f_γ attached to γ. On the one hand, we have $\det_1(f_\gamma) = -bc - \frac{1}{4}(d-a)^2) = 1 - \frac{(a+d)^2}{4}$, since $\det\gamma = 1$. Hence, according to its sign, the quadratic form f_γ is indefinite, definite or degenerate according to whether $(a+d)^2$ is greater, lesser or equal to 4, respectively. This condition is precisely equivalent to the fact that the transformation is hyperbolic, elliptic or parabolic, respectively. On the other hand, it is clear that the indefinite, definite or degenerate condition of f_γ determine the fact that the conic $f_\gamma = \kappa$ is a hyperbola, an ellipse or a parabola, respectively. □

In particular, if z is a real fixed point of γ, then f_γ is isotropic over $\mathbb{R}$, since $f_\gamma(z,1) = 0$. The elliptic case corresponds to the quadratic form f_γ being anisotropic over $\mathbb{R}$.

2.6 Definition. Let $\Gamma \subseteq \mathrm{SL}(2,\mathbb{R})$ be a subgroup acting on the Poincaré half plane $\mathcal{H}$. The action of Γ is proper and discontinuous if there exist a point z_0 and a real number $\varepsilon > 0$ such that, for all $\gamma \in \Gamma$, $\gamma \neq \pm\,\mathrm{Id}$, the condition $|\gamma(z_0) - z_0| > \varepsilon$ is satisfied. In this case, z_0 is called a standard point with respect to Γ.

The definition of proper and discontinuous action is equivalent to the fact that Γ is a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$.

2.7 Definition. The action of Γ in $\mathcal{H}$ gives an equivalence relation between the points: two points $z, z' \in \mathcal{H}$ are called equivalent with respect to Γ if and only if $z' = \gamma(z)$ for some $\gamma \in \Gamma$.

2.8 Definitions. A point $x \in \mathbb{R} \cup \{\infty\}$ is called parabolic (or hyperbolic) with respect to Γ if there exists a transformation $\gamma \in \Gamma$ which is parabolic (or hyperbolic) and such that $\gamma(x) = x$.
A point $z \in \mathcal{H}$ is called elliptic with respect to Γ if there exists an elliptic transformation $\gamma \in \Gamma$, $\gamma \neq \pm\,\mathrm{Id}$, such that $\gamma(z) = z$.

2.9 Definition. The isotropy group of a point z with respect to Γ is the group $\Gamma_z = \{\gamma \in \Gamma \mid \gamma(z) = z\}$.

2.10 Remark. *If Γ is a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$, the isotropy group of an elliptic point is finite and cyclic. The matrices of order 2 lead to the involutions.*

2.11 Definition. The order of an elliptic point $z \in \mathcal{H}$ with respect to Γ is the order of its isotropy group with respect to $\overline{\Gamma}$ in $\mathrm{PSL}(2,\mathbb{R})$. That is, the order of an elliptic point z is $|\Gamma_z|$ if $-\mathrm{Id} \notin \Gamma$, or $\frac{1}{2}|\Gamma_z|$ if $-\mathrm{Id} \in \Gamma$.

2.12 Remark. *If z is an elliptic point with respect to Γ, then $\gamma(z)$ is also an elliptic point with respect to Γ, for any $\gamma \in \Gamma$. Moreover, equivalent elliptic points have the same order, since their isotropy groups are conjugate: $\Gamma_{\gamma(z)} = \gamma\Gamma_z\gamma^{-1}$.*

2.13 Definition. A connected closed polygon $\mathcal{D} \subseteq \mathcal{H} \cup \mathbb{R} \cup \{\infty\}$ is a fundamental domain for the action of Γ in $\mathcal{H}$ if any two points in the interior of $\mathcal{D}$ are not Γ-equivalent and if each point in $\mathcal{H}$ is Γ-equivalent to some point in $\mathcal{D}$. Obviously the fundamental domain for a group Γ is not unique.

2.14 Definition. A cycle of a fundamental domain is an orbit of vertices under the Γ-action.
A cycle is called elliptic of order k if it consists of elliptic vertices of order k.
A cycle is called parabolic if it is formed by parabolic vertices; then by convention its order is $k = \infty$.
The number of vertices in a cycle is called the length of the cycle.

2.3 The non ramified case

Let us consider the non ramified quaternion algebra over Q, $\mathrm{M}(2,\mathbb{Q})$, to see how the full modular group $\Gamma = \mathrm{SL}(2,\mathbb{Z})$, can be obtained.

Let us consider the maximal order $\mathrm{M}(2,\mathbb{Z})$. Restrict to the units, $\mathrm{GL}(2,\mathbb{Z})$, and consider only those with positive norm. Thus we get $\Gamma = \mathrm{SL}(2,\mathbb{Z})$.

We can also apply that to Eichler orders.

We make explicit the groups of transformations coming from Eichler orders in the non-ramified quaternion algebra.

2.15 *Non-ramified case. Consider $H = \mathrm{M}(2,\mathbb{Q})$. In this case, Φ is the canonical embedding $\mathrm{M}(2,\mathbb{Q}) \hookrightarrow \mathrm{M}(2,\mathbb{R})$. For every N, consider the Eichler order of level N*

$$\mathcal{O}_0(1,N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \,:\, a,b,c,d \in \mathbb{Z} \right\}.$$

Then, $\Gamma(1,N) = \mathcal{O}(1,N)^*_+$ is the congruence group denoted usually by $\Gamma_0(N)$.

If we consider the non-ramified quaternion algebra $H' = \left(\frac{1,-1}{\mathbb{Q}}\right)$ and the Eichler order $\mathcal{O}_M(1,N) = \mathbb{Z}\left[1, \frac{j+ij}{2}, N\frac{(-j+ij)}{2}, \frac{1-i}{2}\right]$, we also obtain $\Gamma(1,N) = \Phi(\mathcal{O}_M(1,N)^*_+) = \Gamma_0(N)$.

FUNDAMENTAL DOMAIN FOR $\Gamma = \mathrm{SL}(2,\mathbb{Z})$

2.4 Groups of quaternion transformations

Let $D, N \geq 1$ be natural numbers such that $\gcd(D,N) = 1$.

Consider a quaternion $\mathbb{Q}$-algebra H of discriminant D, which is determined up to isomorphism. Let $\mathcal{O}(D,N)$ be an Eichler order in H of level N. Consider the group of quaternion units with positive norm equal to 1:

$$\mathcal{O}(D,N)^*_+ := \{\alpha \in \mathcal{O}(D,N)^* : n(\alpha) = 1\}.$$

As a consequence of Eichler's results [Eic38], the group of quaternion units $\mathcal{O}(D,N)^*_+$ has the following properties.

2.16 Theorem. *Let $\mathcal{O}(D,N)$ be an Eichler order in a quaternion $\mathbb{Q}$-algebra H. Then:*

(i) *If H is indefinite, then $\mathcal{O}(D,N)$ has units of reduced norm -1. Therefore, $\mathcal{O}(D,N)^*_+$ has index 2 in $\mathcal{O}(D,N)^*$.*

(ii) *If H is definite, then there is no element in $\mathcal{O}(D,N)$ of reduced norm -1; thus, $\mathcal{O}(D,N)^*_+ = \mathcal{O}(D,N)^*$. Moreover, $\mathcal{O}(D,1)^*$ is a cyclic group of order 2, 4 or 6, except for the following cases:*

(a) $H = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, *with* $D_H = 2$. *In this case,* $\mathcal{O}(D,1)^*$ *is isomorphic to* $E_{24} := \left\{\pm1, \pm i, \pm j, \pm ij, \frac{\pm 1 \pm i \pm j \pm ij}{2}\right\}$, *the tetrahedral binary group, and hence it has order 24.*

(b) $H = \left(\frac{-1,-3}{\mathbb{Q}}\right)$, *with* $D_H = 3$. *In this case,* $\mathcal{O}(D,1)^* \simeq \langle s_6, j\rangle \simeq C_6 \times C_2$, *a bicyclic group, with* $s_6 = \cos 2\pi/6 + \iota \sin 2\pi/6$, *and hence it has order 12.*

Since $\mathcal{O}(D,N)^*_+$ is finite when H is definite, we restrict ourselves to the case where H is an indefinite quaternion algebra.

2.17 Remark. *All the groups $\Gamma(D,N)$ of quaternion transformations satisfy the hypothesis of lemma* **??**. *Thus, we have symmetry conditions for the elliptic points and the $\Gamma(D,N)$-equivalent points in $\mathcal{H}$.*

It is also true that all the groups $\Gamma(D,N)$ of quaternion transformations always contain $-\mathrm{Id}$, since the element -1 is always a unit in the order $\mathcal{O}(D,N)$ and $\Phi(-1) = -\mathrm{Id}$. Hence, by 2.3, the elliptic transformations defined by elements in $\Gamma(D,N)$ are of order 2 or 3.

Chapter 3

Introduction to Shimura curves

The goal of this chapter is to introduce Shimura curves $X(D,N)$ attached to Fuchsian groups defined from Eichler orders $\mathcal{O}(D,N)$ in quaternion $\mathbb{Q}$-algebras.

First, we consider the arithmetic Fuchsian groups $\Gamma(D,N)$ coming from Eichler orders in indefinite ramified quaternion algebras. We calculate them in the non-ramified and small ramified cases of type A or B. The moduli point of view of Shimura and the main facts concerning the canonical models are summarized in section 4.1. A compilation of known results allows us to implement instructions in the `Poincare` package in order to compute the constants associated to the Shimura curves $X(D,N)$ and to present them in tables collected in chapter **??**.

3.1 Quaternion fuchsian groups

Thus, assume D is the product of an even number of different primes and take an isomorphism $\Phi : \mathbb{R} \otimes H \to \mathrm{M}(2,\mathbb{R})$. Then, by 1.57, $\mathcal{O}(D,N)^*_+$ only depends on D and N, up to conjugation.

We will fix the monomorphism Φ given by proposition 1.9. Thus, for an indefinite quaternion algebra $H = \left(\dfrac{a,b}{\mathbb{Q}}\right)$, assume $a > 0$ and consider $\Phi : H \hookrightarrow \mathrm{M}(2,\mathbb{R})$ given by

$$\Phi(x + y\sqrt{a} + z\sqrt{b} + t\sqrt{a}\sqrt{b}) = \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix}.$$

Consider the discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$ defined by

$$\Gamma(D,N) := \Phi(\mathcal{O}(D,N)^*_+).$$

The group $\Gamma(D,N)$ acts on the Poincaré half plane. Its elements will be called quaternion transformations.

Therefore,

$$\Gamma(D,N) \subseteq \left\{ \begin{pmatrix} \alpha & \beta \\ b\beta' & \alpha' \end{pmatrix} : \alpha, \beta \in \mathbb{Q}(\sqrt{a}) \right\} \subseteq \mathrm{SL}(2, \mathbb{Q}(\sqrt{a})),$$

where $\alpha \mapsto \alpha'$ denotes the Galois conjugation in $\mathbb{Q}(\sqrt{a})$. The case $a = 1$ corresponds necessarily to a non-ramified quaternion algebra; that is, $D = 1$. In this case, $\Gamma(1, N) \subseteq \mathrm{SL}(2, \mathbb{Q})$.

We make explicit the groups of quaternion transformations for the non-ramified and small ramified quaternion algebras given in chapter 1.

3.1 *Non-ramified case. Consider $H = \mathrm{M}(2, \mathbb{Q})$. In this case, Φ is the canonical embedding $\mathrm{M}(2, \mathbb{Q}) \hookrightarrow \mathrm{M}(2, \mathbb{R})$. For every N, consider the Eichler order of level N*

$$\mathcal{O}_0(1, N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \; : \; a, b, c, d \in \mathbb{Z} \right\}.$$

Then, $\Gamma(1, N) = \mathcal{O}(1, N)^*_+$ is the congruence group denoted usually by $\Gamma_0(N)$.

If we consider the non-ramified quaternion algebra $H' = \left(\frac{1, -1}{\mathbb{Q}}\right)$ and the Eichler order $\mathcal{O}_M(1, N) = \mathbb{Z}\left[1, \frac{j + ij}{2}, N\frac{(-j + ij)}{2}, \frac{1 - i}{2}\right]$, we also obtain $\Gamma(1, N) = \Phi(\mathcal{O}_M(1, N)^*_+) = \Gamma_0(N)$.

3.2 *Small ramified case of type A. Consider the quaternion algebra $H_A(p) = \left(\frac{p, -1}{\mathbb{Q}}\right)$ and the Eichler order $\mathcal{O}_A(2p, N) = \mathbb{Z}\left[1, i, Nj, \frac{1 + i + j + ij}{2}\right]$, $N|\frac{p-1}{2}$ square-free. Then we obtain the following equivalent descriptions for the group $\Gamma(2p, N)$:*

(i) *The matrix $\gamma = \frac{1}{2}\begin{pmatrix} (2x + t) + (2y + t)\sqrt{p} & (2Nz + t) + t\sqrt{p} \\ -(2Nz + t) + t\sqrt{p} & (2x + t) - (2y + t)\sqrt{p} \end{pmatrix}$ lies in the group $\Gamma(2p, N)$ if and only if $x, y, z, t \in \mathbb{Z}$ and $\det(\gamma) = 1$.*

(ii) *The matrix $\gamma = \frac{1}{2}\begin{pmatrix} a + b\sqrt{p} & c + d\sqrt{p} \\ -c + d\sqrt{p} & a - b\sqrt{p} \end{pmatrix}$ lies in the group $\Gamma(2p, N)$ if and only if a, b, c, d are integers, $a \equiv b \equiv c \equiv d \mod 2$, $N|(c - d)$ and $\det(\gamma) = 1$.*

(iii) *The matrix $\gamma = \frac{1}{2}\begin{pmatrix} \alpha & \beta \\ -\beta' & \alpha' \end{pmatrix}$ lies in the group $\Gamma(2p, N)$ if and only if $\alpha, \beta \in \mathbb{Z}[\sqrt{p}]$, $\alpha \equiv \beta \equiv \alpha\sqrt{p} \mod 2$, $N \Big| \left(\mathrm{tr}(\beta) - \frac{\beta - \beta'}{\sqrt{p}}\right)$, $\det(\gamma) = 1$.*

3.3 *Small ramified case of type B. Consider the quaternion algebra $H_B(p, q) = \left(\frac{p, q}{\mathbb{Q}}\right)$ and the Eichler order $\mathcal{O}_B(pq, N) = \mathbb{Z}\left[1, Ni, \frac{1 + j}{2}, \frac{i + ij}{2}\right]$, N square-free, $N|\frac{q-1}{4}$, $\gcd(N, p) = 1$. Then, we obtain the following equivalent descriptions for the group $\Gamma(pq, N)$:*

(i) *The matrix $\gamma = \frac{1}{2}\begin{pmatrix} (2x + z) + (2Ny + t)\sqrt{p} & z + t\sqrt{p} \\ q(z + t\sqrt{p}) & (2x + z) - (2Ny + t)\sqrt{p} \end{pmatrix}$ lies in the group $\Gamma(pq, N)$ if and only if $x, y, z, t \in \mathbb{Z}$ and $\det(\gamma) = 1$.*

(ii) *The matrix* $\gamma = \frac{1}{2}\begin{pmatrix} a+b\sqrt{p} & c+d\sqrt{p} \\ q(c-d\sqrt{p}) & a-b\sqrt{p} \end{pmatrix}$ *lies in the group* $\Gamma(pq,N)$ *if and only if* $a,b,c,d \in \mathbb{Z}$, $a \equiv c \mod 2$, $b \equiv d \mod 2$, $2N \,|(b-d)$ *and* $\det(\gamma) = 1$.

(iii) *The matrix* $\gamma = \frac{1}{2}\begin{pmatrix} \alpha & \beta \\ q\beta' & \alpha' \end{pmatrix}$ *lies in the group* $\Gamma(pq,N)$ *if and only if* $\alpha, \beta \in \mathbb{Z}[\sqrt{p}]$, $\alpha \equiv \beta \mod 2$, $2N|\left(\frac{\alpha-\alpha'-\beta+\beta'}{2\sqrt{p}}\right)$ *and* $\det(\gamma) = 1$.

3.4 Remark. *All the groups* $\Gamma(D,N)$ *of quaternion transformations satisfy the hypothesis of lemma* **??**. *Thus, we have symmetry conditions for the elliptic points and the* $\Gamma(D,N)$*-equivalent points in* $\mathcal{H}$.

It is also true that all the groups $\Gamma(D,N)$ *of quaternion transformations always contain* $-\operatorname{Id}$, *since the element* -1 *is always a unit in the order* $\mathcal{O}(D,N)$ *and* $\Phi(-1) = -\operatorname{Id}$. *Hence, by 2.3, the elliptic transformations defined by elements in* $\Gamma(D,N)$ *are of order 2 or 3.*

3.2 The Shimura curves $X(D,N)$

Let D, N be natural numbers. Assume that D is a product of an even number of different primes and that $N \geq 1$ is a natural number such that $\gcd(D,N) = 1$.

Fix the following objects: an indefinite quaternion $\mathbb{Q}$-algebra H of discriminant $D_H = D$; an Eichler order $\mathcal{O}(D,N)$ of level N in H, and a monomorphism $\Phi : H \hookrightarrow \mathrm{M}(2,\mathbb{R})$. Consider the group of quaternion transformations $\Gamma(D,N)$ associated with the order $\mathcal{O}(D,N)$ and Φ.

The group $\Gamma(D,N) \subseteq \mathrm{SL}(2,\mathbb{R})$ is a Fuchsian group of the first kind acting on the Poincaré half plane. The quotient $\Gamma(D,N) \setminus \mathcal{H}$ is a Riemann surface.

The theory of Shimura provides a canonical model $X(D,N)$ for $\Gamma(D,N)\setminus\mathcal{H}$ and a modular interpretation.

The canonical model $X(D,N)$ has the following properties:

(i) $X(D,N)$ is a projective curve defined over $\mathbb{Q}$.

(ii) There exists a map $j_{D,N} : \mathcal{H} \to X(D,N)(\mathbb{C})$ that factorizes in an isomorphism between the analytic space $\Gamma(D,N) \setminus \mathcal{H}$ and a Zariski open set in $X(D,N)(\mathbb{C})$.

(iii) Let $F = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field splitting the algebra H. Let φ be an embedding of F into H, and $z \in \mathcal{H}$ the unique common fixed point of all the elements in $\Phi(\varphi(F^*))$. Then the coordinates of the point $j_{D,N}(z)$ are algebraic, more specifically, $j_{D,N}(z) \in X(D,N)(F_{\mathrm{ab}})$, where $F_{\mathrm{ab}} \subseteq \mathbb{C}$ denotes the maximal abelian extension of F.

$X(D,N)$ is called the Shimura curve associated with the subgroup $\Gamma(D,N)$.

The case $D = 1$ corresponds to a non-ramified quaternion algebra $H \simeq \mathrm{M}(2, \mathbb{Q})$. In this case, $\Gamma(1, N) \setminus \mathcal{H}$ is a non-compact Riemann surface, with finite volume. From the explicit expressions given for the groups $\Gamma(1, N)$, it is clear that the corresponding compact Shimura curve $X(1, N)$ is precisely the modular curve $X_0(N)$.

If $D > 1$, the quaternion algebra H is ramified. In this case, the Riemann surface $\Gamma(D, N) \setminus \mathcal{H}$ is already compact. In chapter 4 we give a very simple proof of this fact.

The modular interpretation of $X(D, N)$ runs as follows. A point in $X(D, N)(\mathbb{C})$ corresponds to an isomorphism class of triples (A, i, G), where A is an polarized abelian surface, $i : H \hookrightarrow \mathbb{Q} \underset{\mathbb{Z}}{\otimes} \mathrm{End}(A)$ is a monomorphism such that $i(\mathcal{O}(D, 1)) \subseteq \mathrm{End}(A)$, and G is a subgroup of the group of N-torsion points $A[N]$ of A which is a cyclic $\mathcal{O}(D, N)$-module.

We now present some results about the computation of certain constants attached to Shimura curves. Some computations can be done in a general way for the ramified and non-ramified cases.

3.5 Notation. Given a Shimura curve $X(D, N)$ and a fundamental domain for $\Gamma(D, N)$, we consider the following invariants: $V_h(D, N)$ the hyperbolic volume; $e_i(D, N)$ the number of elliptic cycles of order i, and $g(D, N)$ the genus. We also consider a normalization of the hyperbolic measure, given by $\dfrac{\mathrm{d}x\mathrm{d}y}{2\pi y^2}$, and we denote by $V(D, N)$ the volume computed with this normalized measure. It can be proved that $V(D, N) = \dfrac{1}{2\pi} V_h(R)$ is a rational number.

The following propositions provide an arithmetical way to compute these constants. They can be found in [Shi71] and [Vig80].

3.6 Proposition. *Consider a Shimura curve $X(D, N)$. The elliptic cycles are of order 2 or 3. The number of elliptic cycles, volume and genus are given by:*

$$e_2(D, N) = \prod_{p|D} \left(1 - \left(\frac{-4}{p}\right)\right) \prod_{p|N} \left(1 + \left(\frac{-4}{p}\right)\right) \text{ if } 4 \nmid N,\ e_2(D, N) = 0 \text{ if } 4 \mid N.$$

$$e_3(D, N) = \prod_{p|D} \left(1 - \left(\frac{-3}{p}\right)\right) \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) \text{ if } 9 \nmid N,\ e_3(D, N) = 0 \text{ if } 9 \mid N,$$

$$V(D, N) = \tfrac{N}{6} \textstyle\prod_{p|D} (p - 1) \prod_{p|N} (1 + \frac{1}{p}),$$

$$2 - 2g(D, N) = -V(D, N) + \tfrac{1}{2} e_2(D, N) + \tfrac{2}{3} e_3(D, N) + e_\infty(D, N).$$

For the Shimura curves corresponding to the small ramified quaternion algebras of type A and of type B, we deduce the following results.

3.7 Corollary. *Let $X(2p, 1)$ be the Shimura curve associated with a maximal order of a* *small ramified quaternion algebra of type A of discriminant 2p. Then,*

$$e_2(2p,1) = 2, \quad e_3(2p,1) = \begin{cases} 4 & \text{if } p \equiv 11 \mod 12, \\ 2 & \text{if } p = 3, \\ 0 & \text{if } p \equiv 7 \mod 12. \end{cases}$$

3.8 Corollary. *Let $X(pq,1)$ be the Shimura curve associated with a maximal order of a small ramified quaternion algebra of type B of discriminant pq. Then,*

$$e_2(pq,1) = 0, \quad e_3(pq,1) = \begin{cases} 4 & \text{if } p \equiv 2 \mod 3 \text{ and } q \equiv 5 \mod 12, \\ 2 & \text{if } p = 3, \\ 0 & \text{otherwise.} \end{cases}$$

From the relation between these constants, we can deduce some properties about the possible fundamental domains for the Shimura curve $X(D,N)$.

3.9 Proposition. *Let $X(D,N)$ be a Shimura curve with $D > 1$. Assume $X(D,N)$ has a fundamental domain such that all the vertices are elliptic. Then, the number of vertices of this fundamental domain is*

$$n_e(D,N) = 2 + 2V(D,N) + e_2(D,N) + \frac{2}{3}e_3(D,N).$$

If $N = 1$, then

$$n_e(D,1) = 2 + \frac{1}{3}\prod_{p|D}(p-1) + \prod_{p|D}(1 - \left(\frac{-4}{p}\right)) + \frac{2}{3}\prod_{p|D}\left(1 - \left(\frac{-3}{p}\right)\right).$$

Proof: Assume we have a fundamental domain for $X(D,N)$ such that all the vertices are elliptic and let $n_e(D,N)$ be the number of those vertices. Then, the hyperbolic volume $V_h(D,N)$ is $V_h(D,N) = (n_e(D,N)-2)\pi - (\theta_1 + \cdots + \theta_n)$, where $\theta_1, \ldots, \theta_n$ are the angles in the vertices.

In general, we do not know the angles in the vertices. Assuming all the vertices are elliptic points, we can determine the sum from the number of elliptic cycles of order 2 and 3, since the sum of the angles of a cycle of order q is exactly $2\pi/q$. Thus, we have $2\pi V(D,N) = (n_e(D,N)-2)\pi - (\pi e_2(D,N) + \frac{2\pi}{3}e_3(D,N))$ and we deduce the expression for $n_e(D,N)$ given in the statement. □

In chapter **??** we present several tables with numerical data about Shimura curves. The table 2.1 lists the constants V, e_2, e_3 and g for the Shimura curves corresponding to small ramified case with $D < 200$ and $N = 1$; cf. [Vig80], for first cases. The tables 2.2 – 2.5 contain constants attached to the Shimura curves $X(6,N)$, $X(10,N)$, $X(14,N)$ and $X(15,N)$, corresponding to the small ramified quaternion algebras of type A and small ramified quaternion algebras of type B mentioned in the previous chapter. The constants attached to Shimura curves of discriminant equal to the product of four primes can be found in the table 2.6, for $D < 1000$ and $N = 1$.

Table 2.7 lists known equations for Shimura curves obtained previously by Ihara, Kurihara [Kur79], Jordan-Livnè [Jor81] and Michon [Mic81a]. Table 2.8 lists all the values $D > 1$ and N such that $X(D,N)$ is a hyperelliptic Shimura curve, with the hyperelliptic involution w calculated by Ogg [Ogg83].

Chapter 4

Hyperbolic fundamental domains for Shimura curves

Let us consider the Shimura curves $X(D,N)$ attached to Fuchsian groups defined from Eichler orders $\mathcal{O}(D,N)$ in quaternion $\mathbb{Q}$-algebras.

We apply the results for embeddings and quadratic forms in chapter **??** to obtain elements in the group $\Gamma(D,N)$ and points in the curve $X(D,N)$ with the goal of constructing explicit fundamental domains.

4.1 Groups of quaternion transformations and the Shimura curves $X(D,N)$

Let $D,N \geq 1$ in $\mathbb{N}$, such that $\gcd(D,N)=1$ and D is the product of an even number of different primes. Let $\mathcal{H}$ be the Poincaré half plane.

Consider:

$H = \left(\frac{a,b}{\mathbb{Q}}\right)$, an indefinite quaternion algebra of discriminant D (H determined up to isomorphism).
$\mathcal{O}(D,N)$, an Eichler order in H of level N (determined up to conjugation).
$\mathcal{O}(D,N)^*_+ := \{\alpha \in \mathcal{O}(D,N)^* : n(\alpha) = 1\}$, the group of quaternion units with positive norm equal to 1, which only depends on D and N, up to conjugation (by 1.57).

Fix a monomorphism $\Phi : H \hookrightarrow \mathrm{M}(2,\mathbb{R})$,

$\Gamma(D,N) \subseteq \mathrm{SL}(2,\mathbb{R})$ is a Fuchsian group of the first kind acting on $\mathcal{H}$.
Its elements will be called quaternion transformations.

The quotient $\Gamma(D,N) \setminus \mathcal{H}$ is a Riemann surface.

The Riemann surface $\Gamma(D,N) \setminus \mathcal{H}$ is already compact if and only if $D > 1$.
We will give a very simple proof of this fact, by using quadratic forms.

The theory of Shimura provides a canonical model $X(D,N)$ for $\Gamma(D,N)\setminus\mathcal{H}$ and a modular interpretation. $X(D,N)$ is called the Shimura curve associated with the subgroup $\Gamma(D,N)$.

4.1 Theorem. *(The canonical model $X(D,N)$ has the following properties:*

(i) *$X(D,N)$ is a projective curve defined over $\mathbb{Q}$.*

(ii) *There exists a map $j_{D,N}:\mathcal{H}\to X(D,N)(\mathbb{C})$ that factorizes in an isomorphism between the analytic space $\Gamma(D,N)\setminus\mathcal{H}$ and a Zariski open set in $X(D,N)(\mathbb{C})$.*

(iii) *Let $F=\mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field splitting the algebra H. Let φ be an embedding of F into H, and $z\in\mathcal{H}$ the unique common fixed point of all the elements in $\Phi(\varphi(F^*))$. Then the coordinates of the point $j_{D,N}(z)$ are algebraic, more specifically, $j_{D,N}(z)\in X(D,N)(F_{\mathrm{ab}})$, where $F_{\mathrm{ab}}\subseteq\mathbb{C}$ denotes the maximal abelian extension of F.*

The modular interpretation of $X(D,N)$ runs as follows. A point in $X(D,N)(\mathbb{C})$ corresponds to an isomorphism class of triples (A,i,G), where A is an polarized abelian surface, $i:H\hookrightarrow \mathbb{Q}\underset{\mathbb{Z}}{\otimes}\mathrm{End}(A)$ is a monomorphism such that $i(\mathcal{O}(D,1))\subseteq\mathrm{End}(A)$, and G is a subgroup of the group of N-torsion points $A[N]$ of A which is a cyclic $\mathcal{O}(D,N)$-module.)

We make explicit the groups of quaternion transformations for the non-ramified and small ramified quaternion algebras given in chapter 1, when we assume $a>0$, and fix the monomorphism $\Phi:H\hookrightarrow\mathrm{M}(2,\mathbb{R})$ (cf. proposition 1.9) given by

$$\Phi(x+y\sqrt{a}+z\sqrt{b}+t\sqrt{a}\sqrt{b})=\begin{pmatrix} x+y\sqrt{a} & z+t\sqrt{a}\\ b(z-t\sqrt{a}) & x-y\sqrt{a}\end{pmatrix}.$$

4.2 *Non-ramified case.*
Consider $D=1$ and $H=\mathrm{M}(2,\mathbb{Q})\hookrightarrow\mathrm{M}(2,\mathbb{R})$, and the Eichler order of level N

$$\mathcal{O}_0(1,N)=\left\{\begin{pmatrix} a & b\\ cN & d\end{pmatrix} : a,b,c,d\in\mathbb{Z}\right\}.$$

In this case, $\Gamma(1,N)=\mathcal{O}(1,N)^*_+=\Gamma_0(N)$, the usual congruence group.
Thus, the Shimura curve is the usual modular curve, $X(1,N)=X_0(N)$.

4.3 *Small ramified case of type A.* $H_A(p)=\left(\dfrac{p,-1}{\mathbb{Q}}\right)$, $D=2p$,
$\mathcal{O}_A(2p,N)=\mathbb{Z}\left[1,i,Nj,\frac{1+i+j+ij}{2}\right]$, $N|\frac{p-1}{2}$ square-free.

Then, $\gamma=\dfrac{1}{2}\begin{pmatrix} a+b\sqrt{p} & c+d\sqrt{p}\\ -c+d\sqrt{p} & a-b\sqrt{p}\end{pmatrix}$ *lies in the group $\Gamma(2p,N)$ if and only if a,b,c,d are integers, $a\equiv b\equiv c\equiv d \mod 2$, $N|(c-d)$ and $\det(\gamma)=1$.*

4.4 ***Small ramified case of type B.*** $H_B(p,q) = \left(\frac{p,q}{\mathbb{Q}}\right)$, $D = pq$,
$\mathcal{O}_B(pq,N) = \mathbb{Z}\left[1, Ni, \frac{1+j}{2}, \frac{i+ij}{2}\right]$, *$N$ square-free,* $N|\frac{q-1}{4}$, $\gcd(N,p) = 1$.
Then, $\gamma = \frac{1}{2}\begin{pmatrix} a+b\sqrt{p} & c+d\sqrt{p} \\ q(c-d\sqrt{p}) & a-b\sqrt{p} \end{pmatrix}$ *lies in the group* $\Gamma(pq,N)$ *if and only if*
$a,b,c,d \in \mathbb{Z}$, $a \equiv c \mod 2$, $b \equiv d \mod 2$, $2N\,|(b-d)$ *and* $\det(\gamma) = 1$.

We now present some results about the computation of certain constants attached to Shimura curves. Some computations can be done in a general way for the ramified and non-ramified cases.

4.5 Notation. Given a Shimura curve $X(D,N)$ and a fundamental domain for $\Gamma(D,N)$, we consider the following invariants:
$V(D,N) \in \mathbb{Q}$ the normalized hyperbolic volume ($V(D,N) = \frac{1}{2\pi}V_h(D,N)$, mesure $\frac{\mathrm{d}x\mathrm{d}y}{2\pi y^2}$),
$e_i(D,N)$ the number of elliptic cycles of order i,
$g(D,N)$ the genus.

The following proposition provides an arithmetical way to compute these constants (cf. [Shi71] and [Vig80]).

4.6 Proposition. *Consider a Shimura curve $X(D,N)$. The elliptic cycles are of order 2 or 3. The number of elliptic cycles, volume and genus are given by:*

$$e_2(D,N) = \prod_{p|D}\left(1 - \left(\frac{-4}{p}\right)\right)\prod_{p|N}\left(1 + \left(\frac{-4}{p}\right)\right) \text{ if } 4 \nmid N,\ e_2(D,N) = 0 \text{ if } 4 \mid N.$$

$$e_3(D,N) = \prod_{p|D}\left(1 - \left(\frac{-3}{p}\right)\right)\prod_{p|N}\left(1 + \left(\frac{-3}{p}\right)\right) \text{ if } 9 \nmid N,\ e_3(D,N) = 0 \text{ if } 9 \mid N,$$

$$V(D,N) = \tfrac{N}{6}\textstyle\prod_{p|D}(p-1)\prod_{p|N}(1+\frac{1}{p}),$$

$$2 - 2g(D,N) = -V(D,N) + \tfrac{1}{2}e_2(D,N) + \tfrac{2}{3}e_3(D,N) + e_\infty(D,N).$$

For the Shimura curves corresponding to the small ramified quaternion algebras of type A and of type B, we deduce the following results.

4.7 Corollary. *Let $X(2p,1)$ be the Shimura curve associated with a maximal order of a small ramified quaternion algebra of type A of discriminant $2p$. Then,*

$$e_2(2p,1) = 2, \quad e_3(2p,1) = \begin{cases} 4 & \text{if } p \equiv 11 \mod 12, \\ 2 & \text{if } p = 3, \\ 0 & \text{if } p \equiv 7 \mod 12. \end{cases}$$

4.8 Corollary. *Let $X(pq,1)$ be the Shimura curve associated with a maximal order of a small ramified quaternion algebra of type B of discriminant pq. Then,*

$$e_2(pq,1) = 0, \quad e_3(pq,1) = \begin{cases} 4 & \text{if } p \equiv 2 \mod 3 \text{ and } q \equiv 5 \mod 12, \\ 2 & \text{if } p = 3, \\ 0 & \text{otherwise.} \end{cases}$$

From the relation between these constants, we can deduce some properties about the possible fundamental domains for the Shimura curve $X(D, N)$.

4.9 Proposition. *Let $X(D, N)$ be a Shimura curve with $D > 1$. Assume $X(D, N)$ has a fundamental domain such that all the vertices are elliptic. Then, the number of vertices of this fundamental domain is*

$$n_e(D, N) = 2 + 2V(D, N) + e_2(D, N) + \frac{2}{3}e_3(D, N).$$

If $N = 1$, then

$$n_e(D, 1) = 2 + \frac{1}{3}\prod_{p|D}(p-1) + \prod_{p|D}(1 - \left(\frac{-4}{p}\right)) + \frac{2}{3}\prod_{p|D}\left(1 - \left(\frac{-3}{p}\right)\right).$$

PROOF: (Assume we have a fundamental domain for $X(D, N)$ such that all the vertices are elliptic and let $n_e(D, N)$ be the number of those vertices. Then, the hyperbolic volume $V_h(D, N)$ is $V_h(D, N) = (n_e(D, N) - 2)\pi - (\theta_1 + \cdots + \theta_n)$, where $\theta_1, \ldots, \theta_n$ are the angles in the vertices.

In general, we do not know the angles in the vertices. Assuming all the vertices are elliptic points, we can determine the sum from the number of elliptic cycles of order 2 and 3, since the sum of the angles of a cycle of order q is exactly $2\pi/q$. Thus, we have $2\pi V(D, N) = (n_e(D, N) - 2)\pi - (\pi e_2(D, N) + \frac{2\pi}{3}e_3(D, N))$ and we deduce the expression for $n_e(D, N)$ given in the statement.) □

We can show several tables with numerical data about Shimura curves.

The table 2.1 lists the constants V, e_2, e_3 and g for the Shimura curves corresponding to small ramified case with $D < 200$ and $N = 1$. The tables 2.2 – 2.5 contain constants attached to the Shimura curves $X(6, N)$, $X(10, N)$, $X(14, N)$ and $X(15, N)$, corresponding to the small ramified quaternion algebras of type A and small ramified quaternion algebras of type B mentioned in the previous chapter. The constants attached to Shimura curves of discriminant equal to the product of four primes can be found in the table 2.6, for $D < 1000$ and $N = 1$.

4.2 Transformations, embeddings and forms

We denote by $\iota \in \mathbb{C}$ the imaginary complex number such that $\iota^2 = -1$ and by $\mathrm{Re}(z)$ and $\mathrm{Im}(z)$ the real and the imaginary part of a complex number $z = \mathrm{Re}(z) + \mathrm{Im}(z)\iota$. The Poincaré half plane is the complex upper half plane $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ endowed with the structure given by the hyperbolic metric.

Firstly, we describe the transformations acting on the Poincaré half plane and classify them by using their associated binary quadratic form.

General definitions and known results can be found in [Poi1887], [Shi71] and [Sie71].

A linear fractional transformation (or homographic transformation) $\gamma : \mathcal{H} \to \mathcal{H}$ is defined by

$$\gamma(z) = \frac{az + b}{cz + d}, \qquad \text{where } a, b, c, d \in \mathbb{R},\ ad - bc = 1.$$

4.10 Definition. Given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$ such that $c \neq 0$, the circle $C_\gamma := \{z \in \mathbb{C} : |cz + d| = 1\}$ is called isometric circle of γ.
We denote by r_γ and o_γ its radius and center, respectively.

The classification of the transformations and their fixed points can be also interpreted in terms of suitable binary quadratic forms and their associated points.

4.11 Definition. For $f(X,Y) = AX^2 + BXY + CY^2$ a binary quadratic form with coefficients in $\mathbb{R}$, consider

$$\mathcal{P}(f) = \{z : Az^2 + Bz + C = 0,\ \mathrm{Im}(z) \geq 0\}.$$

We have $\mathcal{P}(f) \cap \mathcal{H} = \emptyset$ or $\mathcal{P}(f)$ contains only one point, denoted by $\tau(f)$.

4.12 Definition. Given a matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}(2,\mathbb{R})$, the binary quadratic form associated with it is $f_\gamma(X,Y) := cX^2 + (d-a)XY - bY^2$.

By using this nice association a theory of binary quadratic forms associated to quaternion orders is developped. It leads to a classificaction of this forms, which generalize the usual one for binary integer forms (cf. [AlBa04] and [**?**]). These forms can also be used in the following theorems to play a similar role as the representations by ternary forms.

4.13 Properties. *Let* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$. *Let* $\kappa \in \mathbb{R}$, $\kappa \neq 0$.
Assume that γ *defines a transformation of* $\mathbb{C}$ *different from* $\pm\,\mathrm{Id}$.

(a) γ *is an hyperbolic transformation* $\Leftrightarrow$ γ *has two different fixed points in* $\mathbb{R} \cup \{\infty\} \Leftrightarrow (a+d)^2 > 4 \Leftrightarrow |\,\mathrm{tr}(\gamma)| > 2 \Leftrightarrow f_\gamma = \kappa$ *is a hyperbola.*

(b) γ *is an elliptic transformation* $\Leftrightarrow$ γ *has as fixed points* $z \in \mathcal{H}$ *and* $\overline{z} \Leftrightarrow (a+d)^2 < 4 \Leftrightarrow |\,\mathrm{tr}(\gamma)| < 2 \Leftrightarrow f_\gamma = \kappa$ *is an ellipse.*

(c) γ *is a parabolic transformation* $\Leftrightarrow$ γ *has a unique fixed point in* $\mathbb{R} \cup \{\infty\} \Leftrightarrow (a+d)^2 = 4 \Leftrightarrow |\,\mathrm{tr}(\gamma)| = 2 \Leftrightarrow f_\gamma = \kappa$ *is a parabola.*

Using the normic forms attached to the quaternion algebra, we obtain a direct proof of the well-known fact that the Riemann surface $\Gamma(D,N)\backslash\mathcal{H}$ is compact for $D > 1$.

4.14 Proposition. *If* $D > 1$, *then the Shimura curve* $X(D,N)$ *has no parabolic points.*

PROOF: Fix a quaternion algebra $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ of discriminant D. Assume that there exists $\omega = x + yi + zj + tk \in H$ such that $n(\omega) = 1$ and the matrix $\Phi(\omega)$ is parabolic. As $\mathrm{tr}(\omega) = \pm 2$, then we have $x = \pm 1$ and $-ay^2 - bz^2 + abt^2 = 0$. Thus, the ternary normic form $n_{H,3}(Y,Z,T) = -aY^2 - bZ^2 + abT^2$ represents 0 over $\mathbb{Q}$ and hence it represents 0 over $\mathbb{Q}_p$, for every p. By using properties of quadratic forms it means $(a,b)_p = 1$ for all p. Hence $D = 1$, which gives a contradiction.

In particular, all groups of quaternion transformations $\Gamma(D,N) \subseteq \Phi(H)$, $D > 1$, lack parabolic elements. □

From now on, consider quadratic orders $\Lambda(d,m) \subseteq \mathbb{Q}(\sqrt{d})$ such that $\mathcal{E}(\mathcal{O}(D,N),\Lambda(d,m)) \neq \emptyset$.
In next results, by using these embeddings and units in $\Lambda(d,m)$, we obtain quaternion transformations in the group $\Gamma(D,N)$.

4.15 Remark. *Let ε be a fundamental unit in the quadratic order $\Lambda(d,m)$. Put $\xi := \varepsilon$ if $\mathrm{n}(\varepsilon) = 1$ and $\xi := \varepsilon^2$ if $\mathrm{n}(\varepsilon) = -1$.*

$$\varphi \in \mathcal{E}(\mathcal{O}(D,N),\Lambda(d,m)) \Rightarrow \Phi(\varphi(\xi^n)) \in \Gamma(D,N), \quad \textit{for any} n \in \mathbb{Z}.$$

Conversely, every quaternion transformation can be obtained from embeddings of quadratic orders in the quaternion order as above.

4.16 Theorem. *Let $\gamma \in \Gamma(D,N)$, $D > 1$. Then:*

(i) *There exists a quadratic order $\Lambda(d,m)$, a number $n \in \mathbb{Z} - \{0\}$ and an optimal embedding $\varphi \in \mathcal{E}^*(\mathcal{O}(D,N),\Lambda(d,m))$ such that $\Phi(\varphi(\varepsilon^n)) = \gamma$, where ε is the fundamental unit of $\Lambda(d,m)$.*

(ii) *elliptic transformations come from imaginary quadratic fields, that is*
γ elliptic $\Leftrightarrow d < 0$.

(iii) *hyperbolic transformations come from real quadratic fields, that is*
γ hyperbolic $\Leftrightarrow d > 0$.

PROOF: Consider $\gamma \in \Gamma(D,N)$. By construction, there exists a quaternion $\omega \in \mathcal{O}(D,N)^*_+$ such that $\gamma = \Phi(\omega)$, $\mathrm{n}(\omega) = 1$.

Consider the polynomial $p_\omega(X) = X^2 - \mathrm{tr}(\omega)X + 1 \in \mathbb{Q}(X)$, which defines the quadratic field $F_\omega = \mathbb{Q}(\sqrt{d})$, with $d = \mathrm{tr}(\omega)^2 - 4$. The element $\alpha = \frac{\mathrm{tr}(\omega)}{2} + \frac{1}{2}\sqrt{d} \in F_\omega$ satisfies $\mathrm{tr}(\alpha) = \mathrm{tr}(\omega)$ and $\mathrm{n}(\alpha) = \mathrm{n}(\omega) = 1$. Therefore, $\varphi(\alpha) := \omega$ defines an embedding $\varphi \in \mathcal{E}(H, F_\omega)$.

To obtain an optimal embedding, take the quadratic order $\varphi^{-1}(\mathcal{O}(D,N)) \cap F_\omega$, which equals to $\Lambda(d,m)$, for some m. Then $\varphi \in \mathcal{E}^*(\mathcal{O}(D,N),\Lambda(d,m))$.

As α is a unit in $\Lambda(d,m)$, there exists $n \in \mathbb{Z} - \{0\}$ such that $\alpha = \varepsilon^n$, where ε is the fundamental unit; note that n must be even if $\mathrm{n}(\varepsilon) = -1$. This proves (i).

To prove (ii) and (iii), let us look to $F_\omega = \mathbb{Q}\left(\sqrt{\mathrm{tr}(\omega)^2 - 4}\right)$. It is clear that F_ω is an imaginary quadratic field if and only if $|\,\mathrm{tr}(\omega)| < 2$; this is equivalent to the fact that γ is elliptic. Since there are no parabolic transformations, (iii) is also proved. □

4.2.1 Elliptic points of $X(D,N)$

By theorem 4.16, the elliptic transformations in the group $\Gamma(D,N)$ are obtained from units of imaginary quadratic orders by means of embeddings of these orders into the quaternion order $\mathcal{O}(D,N)$. Using the results about the equivalence between embeddings and representations of ternary quadratic forms, we can reduce the problem of finding explicit elliptic elements of $\Gamma(D,N)$ and explicit elliptic points of the Shimura curve $X(D,N)$ to the study of integral representations of integers by ternary quadratic forms. We will also obtain analogous results by interpreting the elliptic points as the associated points to binary quadratic forms.

4.17 Lemma. *Let $\gamma \in \Gamma(D,N)$ define an elliptic transformation such that $\gamma = \Phi(\omega)$, for $\omega \in \mathcal{O}_+^*(D,N)$. Then:*

(i) *γ is elliptic of order 2 $\Longleftrightarrow F_\omega = \mathbb{Q}(\sqrt{-1})$.*

(ii) *γ is elliptic of order 3 $\Longleftrightarrow F_\omega = \mathbb{Q}(\sqrt{-3})$.*

(iii) *The order of γ can only be 2 or 3.*

Proof: By 4.16, every element $\gamma \in \Gamma(D,N)$ is $\gamma = \Phi(\omega)$ for some ω associated to a fundamental unit in the quadratic field F_ω, and F_ω is an imaginary field since γ is elliptic. The unique imaginary quadratic fields containing non-trivial units are $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. In fact, these are the two only possibilities for the field $F_\omega = \mathbb{Q}(\sqrt{\operatorname{tr}(\gamma)^2 - 4})$, taking into account that, for an elliptic transformation γ with integer trace, $|\operatorname{tr}(\gamma)|$ only takes the values 0 and 1, and that determines the order of the transformation. Note also that $\Phi(-1) = -\operatorname{Id} \in \Gamma(D,N)$. This proves (i) and (ii).

Since there are no other possibilities for the trace, (iii) is also proved. □

4.18 Remark. *By theorem 4.16, we have that the elliptic transformations are determined from embeddings of units of the quadratic orders contained in the fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ into quaternion orders.*

As the units $\neq \pm 1$ in the quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ belong to the quadratic maximal orders only, we only need to take in account optimal embeddings.

Thus, the existence of elliptic points of order 2 in the curve $X(D,N)$ is equivalent to the existence of optimal embeddings of the ring of integers of $\mathbb{Q}(\sqrt{-1})$ in $\mathcal{O}(D,N)$.
Analogously, in the case of order 3, we consider the units in $F = \mathbb{Q}(\sqrt{-3})$.
*Note the analogy between the explicit formulas which characterize both facts (cf. 4.6, **??**).*

Next, we characterize the quaternion elliptic transformations in terms of representations by ternary normic forms.

4.19 Theorem. *Consider the group $\Gamma(D,N)$ defined by the Eichler order $\mathcal{O}(D,N)$. Consider the associated ternary normic form $n_{\mathbb{Z}+2\mathcal{O}(D,N),3}$ ($\mathcal{B} = \{v_1, v_2, v_3, v_4\}$ a normalized basisfor $\mathcal{O}(D,N)$). Let $\gamma \in \Gamma(D,N)$. Then:*

(i) γ *is an elliptic transformation of order* 2 *if and only if there exists* (x, y, z) *in* $\mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O}(D,N),3}, 4; \mathbb{Z})$ *such that*

$$\gamma = \Phi\left(-\frac{z\,\mathrm{tr}(v_4)}{2}, x, y, z\right)_{\mathcal{B}}.$$

(ii) γ *is an elliptic transformation of order* 3 *if and only if there exists* (x, y, z) *in* $\mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O}(D,N),3}, 3; \mathbb{Z})$ *such that either*

$$\gamma = \Phi\left(\frac{1-z}{2}, x, y, z\right)_{\mathcal{B}} \quad \text{or} \quad \gamma = \Phi\left(\frac{-1-z\,\mathrm{tr}(v_4)}{2}, x, y, z\right)_{\mathcal{B}}.$$

PROOF: By theorem 4.16 and lemma 4.17, every elliptic transformation comes from a unit in an imaginary quadratic field. We use the bijection between the embeddings and the representations of ternary quadratic forms given in **??** and the explicit expression given in **??**.

By lemma 4.17 and theorem 4.16, we have that an elliptic transformation γ of order 2 must be $\gamma = \Phi(\varphi(u))$, where u is a non-trivial unit in a quadratic order $\Lambda(-1, m)$ and $\varphi \in \mathcal{E}(\mathcal{O}(D, N), \Lambda(-1, m))$. Now, the non-trivial units of the quadratic field $F = \mathbb{Q}(\sqrt{-1})$ are $\pm\iota$, both belonging to the quadratic maximal order $\Lambda_F = \Lambda(-1, 1)$. Thus the set of embeddings $\mathcal{E}(\mathcal{O}(D, N), \Lambda_F)$, which is equal to $\mathcal{E}^*(\mathcal{O}(D, N), \Lambda_F)$ in this case, is in one to one correspondence with the set of representations $\mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O}(D,N),3}, 4; \mathbb{Z})$, with $D_{\Lambda_F} = -4$. The corollary **??** gives explicit expressions of the embeddings in terms of these sets of representations. Note that the two units ι and $-\iota$ give the same transformation. Thus, we obtain $\varphi(\iota) = \left(-\frac{z}{2}, x, y, z\right)_{\mathcal{B}}$, for some representation $(x, y, z) \in \mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O}(D,N),3}, 4; \mathbb{Z})$.

Analogously, in the case of order 3, we consider the units of the quadratic field $F = \mathbb{Q}(\sqrt{-3})$. The units are 1, ε, ε^2, -1, $-\varepsilon$ and $-\varepsilon^2$, where $\varepsilon = \frac{1+\sqrt{-3}}{2}$, and they are contained in the maximal quadratic order $\Lambda_F = \Lambda(-3, 1)$. To obtain transformations it is enough to consider the units ε and ε^2.

Therefore, a transformation $\gamma \in \Gamma_3(D, N)$ is $\gamma = \Phi(\varphi(\varepsilon))$ or $\gamma = \Phi(\varphi(\varepsilon^2))$, $\varphi \in \mathcal{E}^*(\mathcal{O}(D, N), \Lambda_F)$, again by 4.16 and 4.17. The corollary **??** gives the explicit expression of $\varphi(\sqrt{-3})$ in terms of $(x, y, z) \in \mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O}(D,N),3}, 3; \mathbb{Z})$. From this expression we obtain the following results, which complete the proof of (ii):

$$\varphi(\varepsilon) = \left(\frac{1-z}{2}, x, y, z\right)_{\mathcal{B}}, \qquad \varphi(\varepsilon^2) = \left(\frac{-1-z}{2}, x, y, z\right)_{\mathcal{B}}.$$

□

4.20 Corollary. *Let* $X(D, N)$ *be the Shimura curve attached to the group* $\Gamma(D, N)$. *Then, the sets of elliptic points* $\mathrm{P}_2(D, N)$ *and* $\mathrm{P}_3(D, N)$ *are determined from the sets of representations* $\mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O}(D,N),3}, 4; \mathbb{Z})$ *and* $\mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O}(D,N),3}, 3; \mathbb{Z})$*, respectively.*

4.21 Remark. *From theorem 4.19, given* $(x, y, z) \in \mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O},3}, 3; \mathbb{Z})$*, we have two possible elliptic transformations of order 3:* $\sigma_1 = \varphi(\varepsilon)$ *and* $\sigma_2 = \varphi(\varepsilon^2) = (\varphi(\varepsilon))^2 = \sigma_1^2$*. But, if* $\tau \in \mathcal{H}$ *is the elliptic point corresponding to* σ_1*, it is clear that* τ *is also a fixed point of* σ_1^2*. Hence, these two elliptic transformations give the same elliptic point.*

4.22 Remark. *Using the class number of optimal embeddings of the rings of integers of $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ into $\mathcal{O}(D,N)$, we reobtain the formulas for the number of elliptic points of order 2 and 3 of the Shimura curves $X(D,N)$ given in chapter 4. This is a particular case of a more general result which will be obtained for the complex multiplication points in* **??**.

For every Shimura curve $X(D,N)$, by using the explicit order $\mathcal{O}(D,N)$ and theorem 4.19, we can compute the elliptic transformations and elliptic points explicitly. In particular, this process can be applied to the orders computed in the tables 1.4-1.7, and the corresponding normic forms, contained in the tables 4.1-4.4.

4.23 Theorem. *Let $X(2p,N)$ be a Shimura curve for $p \equiv 3 \mod 4$, $N|\frac{p-1}{2}$ square-free. Fix the quaternion algebra $H_A(p)$, the Eichler order $\mathcal{O}_A(2p,N)=\mathbb{Z}[1,i,Nj,\frac{1+i+j+ij}{2}]$, and the group of quaternion transformations $\Gamma(2p,N)$ defining $X(2p,N)$. Then:*

(i) $\left\{\tau = \dfrac{(2x+z)\sqrt{p}\pm 2\iota}{-(2Ny+z)+z\sqrt{p}} \in \mathcal{H} : (x,y,z)\in\mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O},3},4;\mathbb{Z})\right\}$ *quotient by* $\Gamma(2p,N)$ *is the set of elliptic points of order* 2 *of* $X(2p,N)$.

(ii) $\left\{\nu = \dfrac{(2x+z)\sqrt{p}\pm \sqrt{3}\iota}{-(2Ny+z)+z\sqrt{p}} \in \mathcal{H} : (x,y,z)\in\mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O},3},3;\mathbb{Z})\right\}$ *quotient by* $\Gamma(2p,N)$ *is the set of elliptic points of order* 3 *of* $X(2p,N)$.

(iii) *The sets of corresponding elliptic transformations are*

$$\Gamma_2(2p,N)=\{\gamma_\tau : \tau\in \textit{(i)}\} \text{ and } \Gamma_3(2p,N)=\{\gamma_\nu : \nu\in\textit{(ii)}\},$$

where $\gamma_\tau = \dfrac{1}{2}\begin{pmatrix}(2x+z)\sqrt{p} & (2Ny+z)+z\sqrt{p}\\ -(2Ny+z)+z\sqrt{p} & -(2x+z)\sqrt{p}\end{pmatrix}$ *and* $\gamma_\nu=\gamma_\tau\pm\mathrm{Id}$.

Proof: We determine the elliptic transformations from theorem 4.19.

Let γ define an elliptic transformation of order 2. Then, there exists a representation $(x,y,z)\in\mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O}_A(2p,N),3},4;\mathbb{Z})$ which determines an embedding $\varphi\in\mathcal{E}(\mathcal{O}_A(2p,N),\Lambda(-1,1))$, in such a way that $\gamma=\Phi(\varphi(\iota))$. If we apply 4.19 (i), we explicitly obtain $\gamma=\Phi(\frac{1}{2}((2x+z)i+(2Ny+z)j+zij))$; that is,

$$\gamma=\frac{1}{2}\begin{pmatrix}(2x+z)\sqrt{p} & (2Ny+z)+z\sqrt{p}\\ -(2Ny+z)+z\sqrt{p} & -(2x+z)\sqrt{p}\end{pmatrix}.$$

Thus, the fixed points of γ are the elliptic points $\dfrac{(2x+z)\sqrt{p}\pm 2\iota}{-(2Ny+z)+z\sqrt{p}}$.

For the elliptic points of order 3 of $X(2p,N)$, the proof is analogous, using 4.19(ii). Given γ an elliptic transformation of order 3, we have $\gamma=\Phi(\varphi(\varepsilon))$ or $\gamma=\Phi(\varphi(\varepsilon^2))$, where $\varepsilon=\frac{1+\sqrt{3}}{2}$. Now

$$\begin{aligned}\varphi(\varepsilon) &= \tfrac{1}{2}(1+(2x+z)i+(2Ny+z)j+zij),\\ \varphi(\varepsilon^2) &= \tfrac{1}{2}(-1+(2x+z)i+(2Ny+z)j+zij),\end{aligned}$$

for some representation $(x, y, z) \in \mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O},3}, 3; \mathbb{Z})$. If we apply Φ to these equalities, we obtain the expressions of the transformations and the corresponding elliptic points given in the statement. □

Using other arguments, we obtain the following equivalent description, depending on the ternary normic form associated to the quaternion algebra. This generalizes the result in [Als97].

4.24 Theorem. *Let $\Gamma(2p, N)$ be the group of transformations defined from the Eichler order $\mathcal{O}_A(2p, N) = \mathbb{Z}\left[1, i, Nj, \frac{1+i+j+ij}{2}\right]$ in the quaternion algebra $H_A(p)$, $N|\frac{p-1}{2}$ square-free. Then, the sets of elliptic points of order $k = 2, 3$ in the associated Shimura curve $X(2p, N)$ are the sets*

$$\left\{ \frac{b\sqrt{p} \pm 2\iota}{-c + d\sqrt{p}} \in \mathcal{H} : (b, c, d) \in \mathcal{R}(n_{H,3}, 4; \mathbb{Z}), b, c, d \text{ even, } 2N|c - d \right\},$$

$$\left\{ \frac{b\sqrt{p} \pm \sqrt{3}\iota}{-c + d\sqrt{p}} \in \mathcal{H} : (b, c, d) \in \mathcal{R}(n_{H,3}, 3; \mathbb{Z}), b, c, d \text{ odd, } 2N|c - d \right\},$$

quotient by $\Gamma(2p, N)$.

For an elliptic point $\tau = \tau(b, c, d)$ given as above, the corresponding elliptic transformation is

$$\gamma_\tau = \frac{1}{2} \begin{pmatrix} a + b\sqrt{p} & c + d\sqrt{p} \\ -c + d\sqrt{p} & a - b\sqrt{p} \end{pmatrix},$$

where $a = 0$ if $\tau \in \widetilde{\mathcal{P}}_2(2p, N)$ and $a = 1$ if $\tau \in \widetilde{\mathcal{P}}_3(2p, N)$.

PROOF: Let $\gamma \in \Gamma_e(2p, N)$ define an elliptic transformation. From the explicit description of the group $\Gamma(2p, N)$, cf. 4.3, we have $\gamma = \frac{1}{2} \begin{pmatrix} a + b\sqrt{p} & c + d\sqrt{p} \\ -c + d\sqrt{p} & a - b\sqrt{p} \end{pmatrix}$, where a, b, c are integers, $a \equiv b \equiv c \equiv d \mod 2$, $2N \mid c - d$, $\det(\gamma) = 1$ and $|a| < 2$. Thus, the elliptic points are $\tau = \dfrac{b\sqrt{p} \pm \sqrt{a^2 - 4}}{-c + d\sqrt{p}}$, where $a = 0, 1, -1$. In fact, it is enough to consider the cases $a = 0$ and $a = 1$. If $a = 0$, then the elliptic points are the points $\tau = \dfrac{b\sqrt{p} \pm 2\iota}{-c + d\sqrt{p}} \in \mathbb{C}$, where b, c, d are integral solutions of the equation $-pb^2 + c^2 - pd^2 = 4$, with $b \equiv c \equiv d \equiv 0 \mod 2$ and $2N|c - d$; in particular, b, c, d even. If $a = 1$, the elliptic points are the points $\tau = \dfrac{b\sqrt{p} \pm \sqrt{3}\iota}{-c + d\sqrt{p}} \in \mathbb{C}$, where b, c, d are integral solutions of the equation $-pb^2 + c^2 - pd^2 = 3$, with $b \equiv c \equiv d \equiv 1 \mod 2$ and $2N|c-d$; in particular, b, c, d are odd. The above quadratic equation is equivalent to considering the ternary normic form associated to the quaternion algebra $n_{H,3}(Y, Z, T) = -pY^2 + Z^2 - pT^2$; thus, it is necessary to study the set of representations of 3 and 4 by $n_{H,3}$ over $\mathbb{Z}$, depending on p, with the above conditions of parity and divisibility. □

4.25 Remark. *The elliptic points belong to the straight lines in $\mathbb{C}$ with slopes $\pm\dfrac{2}{b\sqrt{p}}$ or $\pm\dfrac{\sqrt{3}}{b\sqrt{p}}$, depending on whether they are elliptic of order 2 or of order 3, respectively.*

The following results for small ramified algebras of type B are obtained analogously.

4.26 Theorem. *Let $X(pq,N)$ be a Shimura curve, $q \equiv 1 \mod 4$, $\left(\frac{p}{q}\right) = -1$, $N|\frac{q-1}{4}$ square-free, and $\gcd(p,N) = 1$. Fix the quaternion algebra $H_B(p,q)$, the Eichler order $\mathcal{O}_B(pq,N) = \mathbb{Z}[1, Ni, \frac{1+j}{2}, \frac{i+ij}{2}]$ of level N, and the corresponding group of quaternion transformations $\Gamma(pq,N)$ defining $X(pq,N)$. Then, every elliptic point of $X(pq,N)$ has order 3 and*

$$\left\{\nu = \frac{(2Nx+y)\sqrt{p} \pm \sqrt{3}\iota}{q(z-y\sqrt{p})} \in \mathcal{H} : (x,y,z) \in \mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O}(pq,N),3}, 3; \mathbb{Z})\right\}.$$

quotient by $\Gamma(pq,N)$
is the set of elliptic points of order 3 of $X(pq,N)$.

The elliptic transformation γ_ν associated to an elliptic point ν as above is

$$\gamma_\nu = \frac{1}{2}\begin{pmatrix} \pm 1 + (2Nx+y)\sqrt{p} & z + y\sqrt{p} \\ q(z-y\sqrt{p}) & \pm 1 - (2Nx+y)\sqrt{p} \end{pmatrix}.$$

PROOF: Let us see that there are no elliptic points of order 2. First, we obtain that there are no embeddings of $\mathbb{Q}(\sqrt{-1})$ into $H_B(p,q)$. Namely, we have that $\left(\frac{-1}{q}\right) = 1$, since $q \equiv 1 \mod 4$, hence the prime q splits in the quadratic field $\mathbb{Q}(\sqrt{-1})$. Further, the discriminant of the algebra $H_B(p,q)$ is pq. Thus, if we apply criterion **??**, it follows that $\mathcal{E}(H_B(p,q), \mathbb{Q}(\sqrt{-1})) = \emptyset$. Note that this agrees with the formulas given in section 4.1. Now, by 4.16 and 4.17, we deduce that $\Gamma_2(pq,N) = \emptyset$ and $\mathcal{P}_2(pq,N) = \emptyset$.

We now deal with the elliptic transformations of order 3. Let $\gamma \in \Gamma_3(pq,N)$. There exist representations $(x,y,z) \in \mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O}_B(pq,N),3}, 3; \mathbb{Z})$ which determine an embedding $\varphi \in \mathcal{E}^*(\mathcal{O}_B(pq,N), \Lambda(-3,1))$, in such a way that $\gamma = \Phi(\varphi(u))$, where u is a unit of $\Lambda(-3,1))$. Applying directly theorem 4.19 (ii) to the order $\mathcal{O}_B(pq,N)$, with the normalized basis $\mathcal{B} = \{1, Ni, \frac{i+ij}{2}, \frac{1+j}{2}\}$, we obtain

$$\gamma = \frac{1}{2}\Phi(1 + (2Nx+y)i + zj + yi)) \quad \text{or} \quad \gamma = \frac{1}{2}\Phi(-1 + (2Nx+y)i + zj + yij).$$

Thus, the transformations $\gamma \in \Gamma_3(pq,N)$ are given by:

$$\gamma = \frac{1}{2}\begin{pmatrix} \pm 1 + (2Nx+y)\sqrt{p} & z + y\sqrt{p} \\ q(z-y\sqrt{p}) & \pm 1 - (2Nx+y)\sqrt{p} \end{pmatrix},$$

from which we obtain the elliptic points $\dfrac{(2Nx+y)\sqrt{p} \pm \sqrt{3}\iota}{q(z-y\sqrt{p})}$. □

As in theorem 4.24, we have the following result in the case of type B, which characterizes the elliptic points from the ternary normic form of the algebra.

4.27 Theorem. *Let $\Gamma(pq,N)$ be the group of matrices defined from the Eichler order $\mathcal{O}_B(pq,N) = \mathbb{Z}\{1, Ni, \frac{1+j}{2}, \frac{i+ij}{2}\} \subseteq H_B(p,q)$, where N is square-free, $N|\frac{q-1}{2}$, and*

$\gcd(p, N) = 1$. *Then, all the elliptic points of* $X(pq, N)$ *have order* 3 *and belong to the straight lines of* $\mathbb{C}$ *of slope* $\pm\frac{\sqrt{3}}{b\sqrt{p}}$. *Explicitly,* $\widetilde{\mathcal{P}}_3(pq, N)$ *is the set*

$$\left\{ \frac{b\sqrt{p} \pm \sqrt{3}\iota}{q(c - d\sqrt{p})} \in \mathcal{H} : (b, c, d) \in \mathcal{R}(n_{H,3}, 3; \mathbb{Z}),\ c \text{ odd},\ 2N | b - d \right\}.$$

quotient by $\Gamma(pq, N)$.

For an elliptic point $\tau = \tau(b, c, d)$ *as above, the corresponding elliptic transformation is*

$$\gamma_\tau = \frac{1}{2} \begin{pmatrix} 1 + b\sqrt{p} & c + d\sqrt{p} \\ q(c - d\sqrt{p}) & 1 - b\sqrt{p} \end{pmatrix}.$$

4.3 Local conditions at infinity

4.3.1 Principal homotheties of $\Gamma(D, N)$ for $D > 1$

By theorem 4.16, all the hyperbolic transformations in the group $\Gamma(D, N)$ are obtained via optimal embeddings of orders of real quadratic fields into the order $\mathcal{O}(D, N)$, by means of quadratic units. Some of these quadratic orders play a special role.

Since $D > 1$, we can assume $H = \left(\frac{a, b}{\mathbb{Q}}\right)$ is a quaternion algebra with $a > 1$, a squarefree. Once and for all, we fix the embedding $\Phi : H \hookrightarrow \mathrm{M}(2, \mathbb{Q}(\sqrt{a})) \subseteq \mathrm{M}(2, \mathbb{R})$, given in 1.9. The units of the real quadratic field $\mathbb{Q}(\sqrt{a})$ will be very important, especially the fundamental unit which will yield special hyperbolic transformations.

4.28 Notation. Let a be a square-free positive integer. Let ε be the fundamental unit of $\mathbb{Q}(\sqrt{a})$. Put $\xi = \varepsilon$ if $\mathrm{n}(\varepsilon) = 1$ and $\xi = \varepsilon^2$ if $\mathrm{n}(\varepsilon) = -1$. Then, let us denote by h the hyperbolic transformation obtained from ξ; that is,

$$h = \begin{pmatrix} \xi & 0 \\ 0 & \xi' \end{pmatrix},$$

where ξ' denotes the Galois conjugate of ξ in $\mathbb{Q}(\sqrt{a})$.

Note that the action of h is given by $h(z) = \xi^2 z$, where $\xi^2 \in \mathbb{R}$. This leads to geometric interpretation of h.

4.29 Lemma. *The hyperbolic transformation* h *is an homothety with center* 0 *and ratio* ξ^2. *Their two fixed real points are* 0 *and* ∞.

4.30 Lemma. *Let* D, N *be natural numbers such that* $\gcd(D, N) = 1$ *and assume that* D *is equal to the product of an even number of different primes. We consider the group* $\Gamma(D, N) \subseteq \mathrm{SL}(2, \mathbb{R})$ *defined by an Eichler order* $\mathcal{O}(D, N)$. *Then, there exists exactly one* $s \in \mathbb{N}$ *such that*

(a) $h^s \in \Gamma(D, N)$.

(b) *If* $h^{s'} \in \Gamma(D,N)$, *then* $s|s'$.

In particular, if $N=1$, *then* $s=1$.

Proof: Fix a quaternion algebra $H = \left(\dfrac{a,b}{\mathbb{Q}}\right)$ of discriminant D and an Eichler order $\mathcal{O}(D,N) \subseteq H$ of level N. Consider the natural embedding $\varphi : \mathbb{Q}(\sqrt{a}) \hookrightarrow H$, given by $\varphi(\alpha) := \alpha$, in such a way that $h = \Phi(\varphi(\xi))$. Consider the quadratic order $\Lambda := (\varphi^{-1}(\mathcal{O}(D,N))) \cap \mathbb{Q}(\sqrt{a})$ in $\mathbb{Q}(\sqrt{a})$. There exists a unique $k \in \mathbb{N}$ such that ε^k is the fundamental unit of the order Λ. If k is even and $\mathrm{n}(\varepsilon) = -1$, then $\mathrm{n}(\varepsilon^k) = \mathrm{n}(\xi^{k/2}) = 1$ and take $s = k/2$. Otherwise, take $s = k$. Thus, $\mathrm{n}(\xi^s) = 1$ and $\varphi(\xi) \in \mathcal{O}(D,N)^*{}_+$. Therefore, $h^s = \Phi(\varphi(\xi^s)) \in \Gamma(D,N)$. It is clear that this s satisfies the properties (a) and (b) in the statement.

In particular, for the maximal order $\mathcal{O}(D,1)$ it is clear that $s=1$, since in this case the quadratic order Λ is the ring of integers of $\mathbb{Q}(\sqrt{a})$. □

4.31 Definition. Fix the group $\Gamma(D,N)$. The hyperbolic transformation h^s determined in lemma 4.30 will be called the principal homothety of $\Gamma(D,N)$.

4.32 Lemma. *Let* h^s *be the principal homothety of* $\Gamma(D,N)$.

(i) *The points* z *and* $\varepsilon^{2sn}z$ *are* $\Gamma(D,N)$*-equivalent, for all* $n \in \mathbb{Z}$.

(ii) *Let* $\gamma \in \Gamma(D,N)_z$. *Then,* $\gamma^{h^{-sn}} := h^{sn}\gamma h^{-sn} \in \Gamma(D,N)_{\varepsilon^{2sn}z}$, *for all* $n \in \mathbb{Z}$.

Proof: We have $h^{sn} = \begin{pmatrix} \varepsilon^{sn} & 0 \\ 0 & (\varepsilon^{sn})' \end{pmatrix}$. Thus, $h^{sn}(z) = \varepsilon^{2sn}z$, for $z \in \mathcal{H}$, since $\mathrm{n}(\varepsilon)^s = 1$. Since s satisfies (a), we deduce (i).

Assume $\gamma \in \Gamma(D,N)$ is a matrix with z as a fixed point. Hence, applying the above computation, we obtain $h^{sn}\gamma h^{-sn}(\xi^{2sn}z) = \varepsilon^{2sn}z$, which proves (ii). □

4.33 Remark. *Given a quaternion algebra* H, *there are also other real quadratic fields* $F \neq \mathbb{Q}(\sqrt{a})$ *such that* $\mathcal{E}^*(H,F) \neq \emptyset$. *For example,* $\mathbb{Q}(\sqrt{D})$. *For any such* F, *by fixing a suitable embedding of* H *into* $\mathrm{M}(2,F)$, *any* $\varphi \in \mathcal{E}^*(H,F)$ *would yield another hyperbolic transformation, which could be considered as a principal homothety.*

4.3.2 Construction of a fundamental domain at infinity

We determine the subgroup $\Gamma(D,N)_\infty$ of the transformations in $\Gamma(D,N)$ fixing infinity, and we construct a fundamental domain.

Let $H = \left(\dfrac{a,b}{\mathbb{Q}}\right)$ be an indefinite quaternion algebra of discriminant $D > 1$. Assume $a > 0$ and fix the monomorphism $\Phi : H \hookrightarrow M(2,\mathbb{R})$ given in 1.9, which determines an embedding of H into $M(2,\mathbb{Q}(\sqrt{a}))$. Let ε be the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{a})$. Recall that we put $\xi = \varepsilon$ if $\mathrm{n}(\varepsilon) = 1$, and $\xi = \varepsilon^2$ if $\mathrm{n}(\varepsilon) = -1$.

4.34 Notation. Given two numbers $r_1, r_2 \in \mathbb{R}^+$, let $S(r_1, r_2)$ denote the hyperbolic strip defined by

$$S(r_1, r_2) := \{z \in \mathcal{H} : r_1 \leq |z| \leq r_2\} .$$

4.35 Proposition. *Let r be any positive real number. Let h^s be the principal homothety of $\Gamma(D,N)$. Then, $\Gamma(D,N)_\infty = \langle h^s \rangle$ and $S(r, \xi^{2s} r)$ is a fundamental domain in $\mathcal{H}$ for the action of $\Gamma(D,N)_\infty$; that is,*

$$\mathcal{D}_r(\Gamma(D,N)_\infty) = \left\{z \in \mathcal{H} : r \leq |z| \leq \xi^{2s} r\right\} .$$

Proof: Let $\gamma \in \Gamma(D,N)_\infty$. Let $\mathcal{O}(D,N)$ be a quaternion order such that $\Gamma(D,N) = \Phi(\mathcal{O}(D,N)^*_+)$. Using the generic expression of the integral elements of $\Phi(H)$, we get:

$$\Phi(x + yi + zj + tij) = \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ b\beta' & \alpha' \end{pmatrix} .$$

Since $\gamma(\infty) = \infty$, we have $\beta' = z - t\sqrt{a} = 0$, hence $z = t = 0$ and $\beta = 0$, because $a \neq 1$. Then

$$\gamma = \begin{pmatrix} u & 0 \\ 0 & u' \end{pmatrix}, \text{ with } u \in \mathbb{Q}(\sqrt{a}).$$

Since $\gamma \in \Gamma(D,N)$, we deduce that $\mathrm{tr}(u) \in \mathbb{Z}$, $\mathrm{n}(u) = 1$; hence u is a unit in the ring of integers of $\mathbb{Q}(\sqrt{a})$ and there exists $m \in \mathbb{Z}$ such that $u = \xi^m$, ξ defined from the fundamental unit. Therefore $\gamma = h^m$. Now, if we apply 4.30, we have that $s|m$ and $\gamma = h^m = (h^s)^n$ for some $n \in \mathbb{Z}$, $s = s(D,N)$. Since $h^s \in \Gamma(D,N)_\infty$, we deduce $\Gamma(D,N)_\infty$ is the infinite cyclic group generated by h^s; namely,

$$\Gamma(D,N)_\infty = \{h^{sn} : n \in \mathbb{Z}\} .$$

By using the geometric interpretation of h, it is clear that h^s is an homothety of center $(0,0)$ and ratio ξ^{2s}. Thus, a fundamental domain for $\Gamma(D,N)_\infty = \langle h^s \rangle$ is the hyperbolic strip between two circles, centered at 0 and of radius r, $\xi^{2s} r$, denoted by $S(r, \xi^{2s} r)$, for any r. □

We observe that, for a fixed hyperbolic strip $S = S(r, \xi^{2s} r)$, their images under the group $\Gamma(D,N)_\infty$ cover the Poincaré half plane.

4.36 Remark. *Proposition 4.35 generalizes a well-known fact in the non-ramified case, taking the algebra $\mathrm{M}(2,\mathbb{Q})$ and the Eichler order $\mathcal{O}_0(1,N) \subseteq \mathrm{M}(2,\mathbb{Z})$. In fact, the argument of the above proof also works for the non-ramified algebra $H = \left(\frac{1,-1}{\mathbb{Q}}\right)$ and the Eichler order $\mathcal{O}_M(1,N) = \mathbb{Z}\left[1, \frac{j+ij}{2}, N\frac{(-j+ij)}{2}, \frac{1-i}{2}\right] \subseteq H$. Then we have $a = 1$, the embedding Φ also makes sense and we obtain that the group $\Gamma(D,N)_\infty$ is generated by a translation.*

4.37 Remark. *In analogy to the modular case, the idea would be to choose a basic hyperbolic strip $S(r_1, r_2)$, playing the same role as the strip $\{z \in \mathcal{H} : |\,\mathrm{Re}(z)| \leq 1/2\}$ in the non-ramified case. In the modular case, the usual fundamental domain is invariant* *by the symmetry with respect to the hyperbolic line determined by the imaginary axis. In this context, for the non-modular fundamental domains it makes sense to determine a hyperbolic line, which will be a semicircle with center 0, in such a way that $\mathcal{D}(\Gamma(D,N)_\infty)$ turns out to be invariant by the hyperbolic symmetry with respect to this line. The key point is to choose this special hyperbolic line.*

4.38 Lemma. *Let $r \in \mathbb{R}^+$. The fundamental domain $\mathcal{D}_r(\Gamma(D,N)_\infty) = S(r, \xi^{2s}r)$ is invariant with respect to the hyperbolic symmetry given by the hyperbolic line $C = C(0, r\xi^s)$.*

Proof: Consider $\mathcal{D}_r(\Gamma(D,1)_\infty) = S(r, \xi^{2s}r)$ and let denote by $C_1 = C(0,r)$ and $C_2 = C((0,0), \xi^{2s}r)$ the hyperbolic lines in its boundary. The middle point between the points $r\iota$ and the $\xi^{2s}r\iota$, according to the hyperbolic distance δ defined in section **??**, is $(0,y)$ such that $\delta(r,y) = \left|\log\left|\frac{y}{r}\right|\right| = \left|\log\left|\frac{\xi^{2s}r}{y}\right|\right| = \delta(y, \xi^{2s}r)$; that is, $y = \xi^s r$. Note that there are infinitely many hyperbolic lines that pass through the point $\xi^s r\iota$ and have no intersection with the hyperbolic lines C_1 and C_2. Fix the line $C = C(0, \xi^s r)$ and let f be the hyperbolic symmetry with respect to this line. To see that the hyperbolic strip $S(r, \xi^{2s}r)$ is invariant under f, we prove that $f(C_1) = C_2$. Writing f in terms of the center and the radius of C, we have $f(z) = \frac{(\xi^s r)^2}{\overline{z}}$, cf. **??**. In particular, $f(r) = \xi^{2s}r$ and $f(r\iota) = \xi^{2s}r\iota$; since f maps lines to lines, we have $f(C_1) = C_2$. □

4.39 Remark. *As a consequence of lemma 4.38, for a quaternion group $\Gamma(D,N)$ and for a fixed hyperbolic line $C = C(0,r)$, we have three special fundamental domains for $\Gamma(D,N)_\infty$ with good properties with respect to C:*

(a) $S(r, \xi^{2s}r)$, having C as the inferior edge.

(b) $S(\xi^{-2s}r, r)$, having C as the superior edge.

(c) $S(\xi^{-s}r, \xi^s r)$, which is invariant by the symmetry with respect to C.

In the modular case, we can fix the imaginary positive axis as a special hyperbolic line C. Then, among the above three fundamental domains with good properties with respect to C, the usual fundamental domain for $\Gamma(D1,N)_\infty$ corresponds to case (c). For $N = 1$, this choice is the only one that yields to a fundamental domain satisfying the condition that in each parabolic cycle there is a unique vertex. But in the case $D > 1$, we do not have parabolic points; thus this can not be applied to a distinguish a fundamental domain.

Another option, for example, can be to fix a hyperbolic line C containing elliptic points, if they exist. Moreover, we can apply conditions about the symmetry of the elliptic points with respect to the imaginary axis, cf. **??**. *Thus, at least C contains two elliptic points, equivalent or not. Then, since the elliptic points cannot be in the interior of the fundamental domain, this leads us to a fundamental domain satisfying (a) or (b) with respect to C.*

4.4 Principal symmetries of $\Gamma(D, N)$

Besides the principal homothety, there are other elements acting on the Poincaré half plane with a special meaning in the construction of fundamental domains. We will use the isometric circles defined in section 2.1 to focus on some transformations given by elements of $\mathrm{SL}(2,\mathbb{R})$.

From the results in **??** about optimal embeddings, we easily obtain the lemma below.

4.40 Lemma. *Let $\mathcal{O}(D, N)$ be a quaternion order. Assume N is square-free. Then there exists $\omega \in \mathcal{O}(D, N)$ such that $\mathrm{n}(\omega) = DN$ and $\mathrm{tr}(\omega) = 0$.*

Proof: The quadratic order $\Lambda(-DN, 1)$ satisfies $\mathcal{E}^*(\mathcal{O}(D, N), \Lambda(-DN, 1)) \neq \emptyset$. Actually, by applying **??**, $\nu(D, N, -DN, 1; \mathcal{O}(D, N)^*) = h(-DN, 1)$. For any embedding $\varphi \in \mathcal{E}^*(\mathcal{O}(D, N), \Lambda(-DN, 1))$, put $\omega = \varphi(\sqrt{-DN})$. We have $\mathrm{n}(\omega) = DN$ and $\mathrm{tr}(\omega) = 0$ and $\omega \in \mathcal{O}(D, N)$, since $\sqrt{-DN} \in \Lambda(-DN, 1)$. □

4.41 Remark. *If $-DN \equiv 1 \mod 4$, we can also consider the set of optimal embeddings $\mathcal{E}^*(\mathcal{O}(D, N), \Lambda(-DN, 2))$ to obtain elements of $\mathcal{O}(D, N)$ with norm DN and trace 0, since $\sqrt{-DN} \in \Lambda(-DN, 2)$.*

The existence of embeddings allow us to make the following construction. For every embedding $\varphi \in \mathcal{E}^*(\mathcal{O}(D, N), \Lambda(-DN, 1))$, put $\omega = \varphi(\sqrt{-DN})$. We have $\mathrm{n}(\omega) = DN$ and $\mathrm{tr}(\omega) = 0$ and $\omega \in \mathcal{O}(D, N)$, since $\sqrt{-DN} \in \Lambda(-DN, 1)$. Thus, considering the map $\widetilde{\Phi}$ defined in **??**, we have a transformation $\eta := \widetilde{\Phi}(\omega) \in \mathrm{SL}(2,\mathbb{R})$.

4.42 Definition. Take any $\omega \in \mathcal{O}(D, N)$ such that $\mathrm{n}(\omega) = DN$ and $\mathrm{tr}(\omega) = 0$. By considering the map $\widetilde{\Phi}$ defined in **??** extended to H^*, we have a transformation $\eta := \widetilde{\Phi}(\omega) \in \mathrm{SL}(2,\mathbb{R})$. Assume that η does not fix infinity. Then, we say that the isometric circle C_η attached to η is a principal hyperbolic line for the group $\Gamma(D, N)$.

4.43 Definition. A hyperbolic symmetry is called principal with respect to $\Gamma(D, N)$ if it is the symmetry with respect to a principal hyperbolic line for $\Gamma(D, N)$.

4.44 Remark. *In the same way, we may consider elements with norm d, for any $d \mid DN$, coming from the quadratic orders $\Lambda(-d, 1)$ by means of embeddings, to obtain distinguished hyperbolic lines.*

Note that the explicit computations of principal lines and principal symmetries are done via explicit computations of embeddings using quadratic forms.

Next we look for properties of transformations of this kind.

4.45 Lemma. *Let $\eta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a transformation such that the isometric circle C_η is principal. Then η is an elliptic transformation of order 2 and L_η is the line $x = a/c$.*

PROOF: Since C_η is principal we have $\mathrm{tr}(\eta)=0$, thus η is elliptic of order 2. Hence $d=-a$. Let z_1, z_2 be the fixed points z_1, z_2 of η, that satisfy the equation $cZ^2-2aZ-b=0$. By properties of the isometric circles (cf. section 2.1), the line L_η is $x=\frac{z_1+z_2}{2}$ and $\frac{z_1+z_2}{2}=a/c$ which coincides with the center of the isometric circle. □

We are going to use these principal hyperbolic lines to get some symmetrical conditions on the fundamental domains. In particular, comparing with the modular case, we are especially interested in the cases where L_η is the imaginary axis. By lemma 4.45, this is achieved if and only if the transformation η has zeros at the diagonal.

4.46 *Small ramified case of type A. Let $\mathcal{O}(2p,1)\subseteq H_A(p)$ be the maximal order corresponding to the group $\Gamma(2p,1)$. As an example, we fix $p=3$ and consider $\omega=-3j+ij$; it satisfies $\mathrm{n}(\omega)=6$ and $\mathrm{tr}(\omega)=0$. Then,*

$$\eta=\widetilde{\Phi}(\omega)=\frac{1}{\sqrt{6}}\begin{pmatrix}0 & -3+\sqrt{3}\\ 3+\sqrt{3} & 0\end{pmatrix},\quad C_\eta=C\left(0,\frac{\sqrt{2}}{1+\sqrt{3}}\right).$$

The isometric circle C_η is a principal hyperbolic line and L_η is the imaginary axis. If we put $\omega'=i+3j$, it also satisfies $\mathrm{n}(\omega')=6$ and $\mathrm{tr}(\omega')=0$. Therefore, we have

$$\eta'=\widetilde{\Phi}(\omega')=\frac{1}{\sqrt{6}}\begin{pmatrix}\sqrt{3} & 3\\ -3 & -\sqrt{3}\end{pmatrix},\quad C_{\eta'}=C(-1/\sqrt{3},\sqrt{2}/\sqrt{3}).$$

The isometric circle $C_{\eta'}$ is a principal hyperbolic line and $L_{\eta'}$ is the line $x=-1/\sqrt{3}$.

4.47 *Small ramified case of type B. Let $\mathcal{O}_B(pq,1)\subseteq H_B(p,q)$ be the maximal order corresponding to the group of quaternion transformations $\Gamma(pq,1)$. In this case, we give the expression of a principal line of $\Gamma(pq,1)$ in terms of q. Consider $\omega=-ij$, since $\mathrm{n}(-ij)=pq$ and $\mathrm{tr}(-ij)=0$. Then,*

$$\eta=\widetilde{\Phi}(-ij)=\frac{1}{\sqrt{q}}\begin{pmatrix}0 & -1\\ q & 0\end{pmatrix},\quad C_\eta=C(0,1/\sqrt{q}).$$

The isometric circle C_η is a principal hyperbolic line and L_η is the imaginary axis. Namely, $\eta=\widetilde{\Phi}(-ij)$, $\mathrm{n}(-ij)=pq$, $\mathrm{tr}(-ij)=0$.

4.48 Remark. *Note the parallelism with the non-ramified case, $\Gamma(1,N)=\Gamma_0(N)$. Consider*

$$\omega=\begin{pmatrix}0 & -1\\ N & 0\end{pmatrix}\in\mathcal{O}_0(1,N),\quad \mathrm{n}(\omega)=N,\ \mathrm{tr}(\omega)=0.$$

Then we obtain

$$\eta=\widetilde{\Phi}(\omega)=\frac{1}{\sqrt{N}}\begin{pmatrix}0 & -1\\ N & 0\end{pmatrix},\quad C_\eta=C(0,1/\sqrt{N}).$$

The isometric circle C_η is a principal hyperbolic line and L_η is the imaginary axis.

If N is odd, we can also consider

$$\omega'=\begin{pmatrix}N & -\frac{N+1}{2}\\ 2N & -N\end{pmatrix}\in\mathcal{O}_0(1,N),\quad \mathrm{n}(\omega)=N,\mathrm{tr}(\omega)=0.$$

Then we obtain

$$\eta' = \widetilde{\Phi}(\omega) = \frac{1}{\sqrt{N}} \begin{pmatrix} N & -\frac{N+1}{2} \\ 2N & -N \end{pmatrix}, \quad C_{\eta'} = C(1/2, 1/2\sqrt{N}).$$

The isometric circle $C_{\eta'}$ *is a principal hyperbolic line and* $L_{\eta'}$ *is the line* $x = 1/2$*. Changing the signs of the matrix, we obtain* η'' *with isometric circle* $C_{\eta'} = C(-1/2, 1/2\sqrt{N})$ *and* $L_{\eta'}$ *the line* $x = -1/2$*.*

4.5 Construction of fundamental domains $(D > 1)$

4.5.1 General comments

In this section, we perform effective constructions of fundamental domains using results from previous sections. The graphical representations and the tables of constants can be found at the end of this chapter.

Consider the Shimura curve $X(D, N)$, $D > 1$, attached to the group $\Gamma(D, N)$. Assume that the set of elliptic points is not empty, that is, at least one of the values $e_2(D, N)$ and $e_3(D, N)$ is nonzero. We want to find a fundamental domain for $X(D, N)$ which is a hyperbolic polygon having elliptic points as vertices in order to get a fundamental domain for setting the comments in subsection 4.3.2 above. Moreover we can apply 4.9 to know in advance the number of vertices.

Using the formulas in section 4.1, we compute the constants attached to the Shimura curve $X(D, N)$: $e_2(D, N)$, $e_3(D, N)$, $g(D, N)$ and $V(D, N)$. Then we look for a hyperbolic polygon with exactly $n_e(D, N)$ elliptic vertices (cf. 4.9) and with those constants.

To compute elliptic points explicitly, we use the results for the Eichler orders $\mathcal{O}(D, N)$ given in chapter 1 and the group of quaternion transformations $\Gamma(D, N)$ given in 4.1 for the small ramified algebras of type A or B. We consider the normic forms attached to $\mathcal{O}(D, N)$ and $\mathbb{Z} + 2\mathcal{O}(D, N)$ and study their representations, which allow us to make an effective determination of elliptic transformations, cf. 4.2. To choose a suitable set of elliptic points, we look for $\Gamma(D, N)$-equivalences.

First of all, we make an attempt to determine a hyperbolic polygon with $n_e(D, N)$ elliptic vertices, with the suitable number of cycles according to $e_2(D, N)$, $e_3(D, N)$, the edges identified pairwise, and the suitable genus. After choosing a possible hyperbolic polygon, we check if the hyperbolic volume is correct. If this is the case, the polygon is a fundamental domain for the Shimura curve $X(D, N)$. In fact, the polygon is a fundamental domain for a subgroup of $\Gamma(D, N)$ with the same invariants as $\Gamma(D, N)$. Therefore, the subgroup has to be equal to $\Gamma(D, N)$, by Hurwitz's theorem. Moreover, the paired edges in a fundamental domain provide an explicit presentation of the group $\Gamma(D, N)$.

The process to obtain a fundamental domain involves laborious computations, such as the search for representations of integers by normic forms, formulas related to embeddings, etc. In the package `Poincare` we implemented instructions to make the computations more simply.

4.5.2 Fundamental domain for $X(6,1)$

The following theorem yields a fundamental domain for the Shimura curve $X(6,1)$ with the property that all the vertices are elliptic. It also contains the values of the constants, and the equivalence relations between the vertices. Its graphical representation can be found in figure 8.1.

4.49 Theorem. *Consider the Shimura curve $X(6,1)$. Then the hyperbolic hexagon of vertices $(v_1, v_2, v_3, v_4, v_5, v_6)$,*

$$v_1 = \frac{-\sqrt{3}+\iota}{2}, \qquad v_2 = \frac{-1+\iota}{1+\sqrt{3}}, \qquad v_3 = (2-\sqrt{3})\iota,$$
$$v_4 = \frac{1+\iota}{1+\sqrt{3}}, \qquad v_5 = \frac{\sqrt{3}+\iota}{2}, \qquad v_6 = \iota,$$

is a fundamental domain for the Shimura curve $X(6,1)$ in the Poincaré half plane, which we denote by $\mathcal{D}(6,1)$. It has the following properties.

(i) *All the vertices are elliptic and the corresponding elliptic transformations fixing them are:*

$$\gamma_{v_1} = \begin{pmatrix} \sqrt{3} & 2 \\ -2 & -\sqrt{3} \end{pmatrix}, \qquad \gamma_{v_2} = \tfrac{1}{2}\begin{pmatrix} 1+\sqrt{3} & 3-\sqrt{3} \\ -3-\sqrt{3} & 1-\sqrt{3} \end{pmatrix},$$

$$\gamma_{v_3} = \begin{pmatrix} 0 & -2+\sqrt{3} \\ 2+\sqrt{3} & 0 \end{pmatrix}, \quad \gamma_{v_4} = \tfrac{1}{2}\begin{pmatrix} 1+\sqrt{3} & -3+\sqrt{3} \\ 3+\sqrt{3} & 1-\sqrt{3} \end{pmatrix},$$

$$\gamma_{v_5} = \begin{pmatrix} \sqrt{3} & -2 \\ 2 & -\sqrt{3} \end{pmatrix}, \qquad \gamma_{v_6} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(ii) *The hyperbolic volume of $\mathcal{D}(6,1)$ is $V_h(6,1) = \frac{2\pi}{3}$ and the genus of the curve $X(6,1)$ is $g(6,1) = 0$.*

(iii) *The number of elliptic vertices of order 2 is $n_2(6,1) = 4$. There are $e_2(6,1) = 2$ elliptic cycles of order 2, namely $\{v_6\}$ and $\{v_1, v_3, v_5\}$. The relations between these vertices are $\gamma_{v_2}(v_3) = v_1$ and $\gamma_{v_4}(v_3) = v_5$.*

(iv) *The number of elliptic vertices of order 3 is $n_3(6,1) = 2$. There are $e_3(6,1) = 2$ elliptic cycles of order 3: $\{v_2\}$ and $\{v_4\}$.*

(v) *The principal homothety of $\Gamma(6,1)$ is*

$$h = \begin{pmatrix} 2+\sqrt{3} & 0 \\ 0 & 2-\sqrt{3} \end{pmatrix}.$$

(vi) *The pairing of the edges is:*

(v_2v_3, v_2v_1) *by the transformation* γ_{v_2},
(v_3v_4, v_5v_4) *by the transformation* γ_{v_4},
(v_5v_6, v_1v_6) *by the transformation* γ_{v_6}.

(vii) *We have the following presentation of the group* $\Gamma(6,1)/\pm\mathrm{Id}$:

$$\langle \gamma_{v_2}, \gamma_{v_4}, \gamma_{v_6} : \gamma_{v_2}^3 = \gamma_{v_4}^3 = \gamma_{v_6}^2 = (\gamma_{v_2}^{-1}\gamma_{v_6}\gamma_{v_4})^2 = 1\rangle.$$

(viii) *Put* $r_1 = 7-4\sqrt{3}$, $r_2 = 2-\sqrt{3}$, $r_3 = 1$, $r_4 = 2+\sqrt{3}$. $\mathcal{D}(6,1)$ *is included in the hyperbolic strips* $S(r_1,r_3)$ *and* $S(r_2,r_4)$, *which are two fundamental domains by the action of* $\Gamma(6,1)_\infty$. *These hyperbolic strips are symmetric with respect to the principal hyperbolic lines* $C(0,r_2)$ *and* $C(0,r_3)$, *respectively.*

(ix) *The edges* v_5v_6 *and* v_6v_1 *are segments of the isometric circle of* γ_{v_6}.

(x) $\mathcal{D}(6,1)$ *is symmetric with respect to the imaginary axis.*

PROOF: The constants attached to the Shimura curve $X(6,1)$ are $e_2(6,1) = 2$, $e_3(6,1) = 2$, $g(6,1) = 0$ and $V_h(6,1) = \frac{2\pi}{3}$, cf. 4.1. Moreover, if it exists, a fundamental domain for $X(6,1)$ in $\mathcal{H}$ whose vertices are all elliptic ones must have $n_e(6,1) = 6$ vertices.

Applying results 4.23 and 4.24, from representations by normic forms, we find elliptic points with the corresponding elliptic transformations fixing them. For example, we have the following elliptic points of order 2:

$$A_1 = \iota, \qquad \gamma_{A_1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$A_2 = (2-\sqrt{3})\iota, \qquad \gamma_{A_2} = \begin{pmatrix} 0 & -2+\sqrt{3} \\ 2+\sqrt{3} & 0 \end{pmatrix},$$

$$A_3 = \frac{-\sqrt{3}+\iota}{2}, \qquad \gamma_{A_3} = \begin{pmatrix} \sqrt{3} & 2 \\ -2 & -\sqrt{3} \end{pmatrix},$$

$$A_4 = \frac{\sqrt{3}+\iota}{2}, \qquad \gamma_{A_4} = \begin{pmatrix} \sqrt{3} & -2 \\ 2 & -\sqrt{3} \end{pmatrix},$$

$$A_5 = \frac{-\sqrt{3}+\iota}{4+2\sqrt{3}}, \qquad \gamma_{A_5} = \begin{pmatrix} \sqrt{3} & 4-2\sqrt{3} \\ -4-2\sqrt{3} & -\sqrt{3} \end{pmatrix},$$

$$A_6 = \frac{\sqrt{3}+\iota}{4+2\sqrt{3}}, \qquad \gamma_{A_6} = \begin{pmatrix} \sqrt{3} & -4+2\sqrt{3} \\ 4+2\sqrt{3} & -\sqrt{3} \end{pmatrix}.$$

The following points are elliptic of order 3:

$$B_1 = \frac{-1+\iota}{1+\sqrt{3}}, \qquad \gamma_{B_1} = \frac{1}{2}\begin{pmatrix} 1+\sqrt{3} & 3-\sqrt{3} \\ -3-\sqrt{3} & 1-\sqrt{3} \end{pmatrix},$$
$$B_2 = \frac{1+\iota}{1+\sqrt{3}}, \qquad \gamma_{B_2} = \frac{1}{2}\begin{pmatrix} 1+\sqrt{3} & -3+\sqrt{3} \\ 3+\sqrt{3} & 1-\sqrt{3} \end{pmatrix}.$$

The previous elliptic transformations give us some relations between these points:

$$\gamma_{A_1}(A_1) = A_1, \qquad \gamma_{A_1}(A_4) = A_3,$$
$$\gamma_{B_1}(B_1) = B_1, \qquad \gamma_{B_1}(A_2) = A_3,$$
$$\gamma_{B_2}(B_2) = B_2, \qquad \gamma_{B_2}(A_2) = A_4.$$

We will prove that the polygon with vertices $(A_3, B_1, A_2, B_2, A_4, A_1)$, which we denote by $(v_1, v_2, v_3, v_4, v_5, v_6)$, satisfies the desired conditions.

First, check that the two elliptic vertices of order 3, v_2 and v_4, are not $\Gamma(6,1)$-equivalent; thus, we have two cycles of order 3. Note that the angle of the fixed hyperbolic polygon in each of its vertices is $\frac{2\pi}{3}$; hence, each one is a cycle. In the same way, $\{v_1, v_3, v_5\}$ and $\{v_6\}$ are two cycles of order 2; the angles between these vertices also satisfy the condition for the sum in each cycle.

The hyperbolic volume of this polygon is $\frac{2\pi}{3}$, which coincides with the hyperbolic volume of $\Gamma(6,1)\backslash\mathcal{H}$. Therefore, this hyperbolic polygon is a fundamental domain $\mathcal{D}(6,1)$ for the Shimura curve $X(6,1)$.

The above relations between the vertices give the pairing of the edges. Thus, we have that the transformation γ_{v_2} maps the edge v_1v_2 to v_1v_6; the transformation γ_{v_4} maps the edge v_3v_4 to v_5v_4 and the transformation γ_{v_6} maps the edge v_2v_3 to v_6v_5. From the pairing of the edges, we see that the genus is 0 and we obtain the presentation of the group given in the statement.

By using the isometric circles, it is clear that the edges v_5v_6 and v_6v_1 are segments of the isometric circle $C_{\gamma_{v_6}}$.

Consider $\varepsilon = 2+\sqrt{3}$, the fundamental unit of $\mathbb{Q}(\sqrt{3})$. Then the hyperbolic strip $S(r, \varepsilon^2 r)$ is a fundamental domain for $\Gamma(6,1)_\infty$.

For $r_3 = |v_6| = 1 = \varepsilon^2 r$, we have $r = r_1 = 7 - 4\sqrt{3}$. For $r = r_2 = |v_3| = 2 - \sqrt{3}$, we have $r_4 = \varepsilon^2 r = 2 + \sqrt{3}$. Now the symmetry conditions follow from 4.38. Moreover $C(0, r_2) = C_{\gamma_{v_3}}$ and $C(0, r_3) = C_{\gamma_{v_6}}$, hence they are principal hyperbolic lines.

Finally, it is clear that $\mathcal{D}(6,1)$ is symmetric with respect to the imaginary axis, which coincides with $L_{\gamma_{v_3}}$ and $L_{\gamma_{v_6}}$. □

4.5.3 Fundamental domain for $X(10,1)$

4.50 Theorem. *Consider the Shimura curve $X(10,1)$. Then the hyperbolic hexagon of vertices $(v_1, v_2, v_3, v_4, v_5, v_6)$,*

$$v_1 = \frac{-\sqrt{2}+\sqrt{3}\iota}{5(-1+\sqrt{2})}, \qquad v_2 = \frac{-\sqrt{2}+\sqrt{3}\iota}{5(1+\sqrt{2})}, \qquad v_3 = \frac{-\sqrt{2}+\sqrt{3}\iota}{5(7+5\sqrt{2})},$$
$$v_4 = \frac{\sqrt{2}+\sqrt{3}\iota}{5(7+5\sqrt{2})}, \qquad v_5 = \frac{\sqrt{2}+\sqrt{3}\iota}{5(1+\sqrt{2})}, \qquad v_6 = \frac{\sqrt{2}+\sqrt{3}\iota}{5(-1+\sqrt{2})},$$

is a fundamental domain for the Shimura curve $X(10,1)$ in the Poincaré half plane, which we denote by $\mathcal{D}(10,1)$. It has the following properties.

(i) *All the vertices are elliptic of order 3 and the corresponding elliptic transformations* *fixing them are:*

$$\gamma_{v_1} = \tfrac{1}{2}\begin{pmatrix} 1+\sqrt{2} & 1+\sqrt{2} \\ 5(1-\sqrt{2}) & 1-\sqrt{2} \end{pmatrix}, \qquad \gamma_{v_2} = \tfrac{1}{2}\begin{pmatrix} 1+\sqrt{2} & -1+\sqrt{2} \\ -5(1+\sqrt{2}) & 1-\sqrt{2} \end{pmatrix},$$

$$\gamma_{v_3} = \tfrac{1}{2}\begin{pmatrix} 1+\sqrt{2} & -7+5\sqrt{2} \\ -5(7+5\sqrt{2}) & 1-\sqrt{2} \end{pmatrix}, \quad \gamma_{v_4} = \tfrac{1}{2}\begin{pmatrix} 1+\sqrt{2} & 7-5\sqrt{2} \\ 5(7+5\sqrt{2}) & 1-\sqrt{2} \end{pmatrix},$$

$$\gamma_{v_5} = \tfrac{1}{2}\begin{pmatrix} 1+\sqrt{2} & 1-\sqrt{2} \\ 5(1+\sqrt{2}) & 1-\sqrt{2} \end{pmatrix}, \qquad \gamma_{v_6} = \tfrac{1}{2}\begin{pmatrix} 1+\sqrt{2} & -1-\sqrt{2} \\ 5(-1+\sqrt{2}) & 1-\sqrt{2} \end{pmatrix}.$$

(ii) *The hyperbolic volume of* $\mathcal{D}(10,1)$ *is* $V_h(10,1) = \dfrac{4}{3}\pi$ *and the genus of the curve* $X(10,1)$ *is* $g(10,1) = 0$.

(iii) *The number of elliptic vertices of order 3 is* $n_3(10,1) = 6$. *There are* $e_3(10,1) = 4$ *elliptic cycles of order 3, namely* $\{v_1, v_3\}$, $\{v_4, v_6\}$, $\{v_2\}$ *and* $\{v_5\}$. *The relations between the vertices are* $\gamma_{v_2}(v_3) = v_1$ *and* $\gamma_{v_5}(v_4) = v_6$.

(iv) *The principal homothety of* $\Gamma(10,1)$ *is*

$$h = \begin{pmatrix} 3+2\sqrt{2} & 0 \\ 0 & 3-2\sqrt{2} \end{pmatrix}.$$

(v) *The pairing of the edges is:*

$$\begin{array}{ll} (v_2v_3, v_2v_1) & \text{by the transformation } \gamma_{v_2}, \\ (v_3v_4, v_1v_6) & \text{by the transformation } h, \\ (v_4v_5, v_6v_5) & \text{by the transformation } \gamma_{v_5}. \end{array}$$

(vi) *We have the following presentation of the group* $\Gamma(10,1)/\pm\mathrm{Id}$:

$$\langle h, \gamma_{v_2}, \gamma_{v_5} : \gamma_{v_2}^3 = \gamma_{v_5}^3 = (h^{-1}\gamma_{v_2})^3 = (h^{-1}\gamma_{v_5})^3 = 1\rangle.$$

(vii) *The edges* v_3v_4 *and* v_1v_6 *determine a hyperbolic strip* $S(r_1, r_3)$, $r_1 = |v_3|$, $r_3 = |v_1|$ *which is a fundamental domain by the action of* $\Gamma(10,1)_\infty$.

(viii) *The other edges correspond to segments of isometric circles in the following way:* $v_1v_2 \subseteq C_{\gamma_{v_1}^{-1}}$, $v_2v_3 \subseteq C_{\gamma_{v_2}^{-1}}$, $v_4v_5 \subseteq C_{\gamma_{v_5}^{-1}}$ *and* $v_5v_6 \subseteq C_{\gamma_{v_6}^{-1}}$.

(ix) $\mathcal{D}(10,1)$ *is invariant with respect to*

$$w = \frac{1}{\sqrt{5}}\begin{pmatrix} 0 & 1-\sqrt{2} \\ 5(1+\sqrt{2}) & 0 \end{pmatrix},$$

and it is symmetric with respect to the imaginary axis and the hyperbolic line $C_w = C\left(0, \dfrac{1}{\sqrt{5}(1+\sqrt{2})}\right)$.

4.51 Remark. *The above fundamental domain $\mathcal{D}(10,1)$ is the intersection of the hyperbolic strip $S(r_1,r_3)$ given in (vii) and the exterior of the isometric circles given in (viii).*

PROOF: The constants attached to the Shimura curve $X(10,1)$ are $e_2(10,1)=0$, $e_3(10,1)=4$, $g(10,1)=0$ and $V_h(10,1)=\frac{4}{3}\pi$.

By 4.9, in a fundamental domain such that all vertex are elliptic there must be $n_e(10,1)=6$ vertices. Let us look for elliptic points of order 3, according to the descriptions given in 4.26 or 4.27. For example, we obtain the points and the corresponding transformations below. Note that, taking into account the change of the sign, we obtain groups of 4 solutions. Moreover, the points are symmetric with respect to the imaginary axis.

$$B_1=\frac{-\sqrt{2}+\sqrt{3}\iota}{5(-1+\sqrt{2})},\qquad \gamma_{B_1}=\tfrac{1}{2}\begin{pmatrix}1+\sqrt{2} & 1+\sqrt{2}\\ 5(1-\sqrt{2}) & 1-\sqrt{2}\end{pmatrix},$$

$$B_2=\frac{-\sqrt{2}+\sqrt{3}\iota}{5(1+\sqrt{2})},\qquad \gamma_{B_2}=\tfrac{1}{2}\begin{pmatrix}1+\sqrt{2} & -1+\sqrt{2}\\ -5(1+\sqrt{2}) & 1-\sqrt{2}\end{pmatrix},$$

$$B_3=\frac{\sqrt{2}+\sqrt{3}\iota}{5(1+\sqrt{2})},\qquad \gamma_{B_3}=\tfrac{1}{2}\begin{pmatrix}1+\sqrt{2} & 1-\sqrt{2}\\ 5(1+\sqrt{2}) & 1-\sqrt{2}\end{pmatrix},$$

$$B_4=\frac{\sqrt{2}+\sqrt{3}\iota}{5(-1+\sqrt{2})},\qquad \gamma_{B_4}=\tfrac{1}{2}\begin{pmatrix}1+\sqrt{2} & -1-\sqrt{2}\\ 5(-1+\sqrt{2}) & 1-\sqrt{2}\end{pmatrix},$$

$$B_5=\frac{-\sqrt{2}+\sqrt{3}\iota}{5(-7+5\sqrt{2})},\qquad \gamma_{B_5}=\tfrac{1}{2}\begin{pmatrix}1+\sqrt{2} & 7+5\sqrt{2}\\ 5(7-5\sqrt{2}) & 1-\sqrt{2}\end{pmatrix},$$

$$B_6=\frac{-\sqrt{2}+\sqrt{3}\iota}{5(7+5\sqrt{2})},\qquad \gamma_{B_6}=\tfrac{1}{2}\begin{pmatrix}1+\sqrt{2} & -7+5\sqrt{2}\\ -5(7+5\sqrt{2}) & 1-\sqrt{2}\end{pmatrix},$$

$$B_7=\frac{\sqrt{2}+\sqrt{3}\iota}{5(7+5\sqrt{2})},\qquad \gamma_{B_7}=\tfrac{1}{2}\begin{pmatrix}1+\sqrt{2} & 7-5\sqrt{2}\\ 5(7+5\sqrt{2}) & 1-\sqrt{2}\end{pmatrix},$$

$$B_8=\frac{\sqrt{2}+\sqrt{3}\iota}{5(-7+5\sqrt{2})},\qquad \gamma_{B_8}=\tfrac{1}{2}\begin{pmatrix}1+\sqrt{2} & -7-5\sqrt{2}\\ 5(-7+5\sqrt{2}) & 1-\sqrt{2}\end{pmatrix}.$$

We look for relations between these elliptic points, using the elliptic transformations. We select the following ones:

$$\gamma_{B_2}(B_2)=B_2,\quad \gamma_{B_2}(B_6)=B_1,$$
$$\gamma_{B_3}(B_3)=B_3,\quad \gamma_{B_4}(B_7)=B_4.$$

The hyperbolic transformation fixing the infinity is

$$h=\begin{pmatrix}3+2\sqrt{2} & 0\\ 0 & 3-2\sqrt{2}\end{pmatrix}$$ and satisfies $h(B_6)=B_1$, $h(B_7)=B_4$.

Hence, we have the sets of equivalent vertices: $\{B_1, B_6\}$, $\{B_4, B_7\}$, $\{B_2\}$ and $\{B_3\}$. We check that the vertices of two different sets are not equivalent; hence we already have 6 elliptic points of order 3 in 4 cycles.

Consider the hyperbolic polygon with vertices:

$$(B_1, B_2, B_6, B_7, B_3, B_4).$$

Now we perform a change of notation and write $(v_1, v_2, v_3, v_4, v_5, v_6)$ to denote the vertices of this hyperbolic polygon. It is easy to check that the above relations give the pairing of the edges stated in (v). The hyperbolic volume is $\frac{4}{3}\pi$. Thus, effectively this hyperbolic polygon is a fundamental domain $\mathcal{D}(10,1)$ for the Shimura curve $X(10,1)$. In figure 8.3 there is its graphical representation, with the pairing of the edges.

From the pairing of the edges we check that the genus is 0. Moreover, we obtain the following presentation of the group $\Gamma(10,1)/\pm \mathrm{Id}$:

$$\langle h, \gamma_{v_2}, \gamma_{v_5} : \gamma_{v_2}^3 = 1, \gamma_{v_5}^3 = 1, (h^{-1}\gamma_{v_2})^3 = 1, (h^{-1}\gamma_{v_5})^3 = 1\rangle.$$

We note that most of the edges are segments of isometric circles, as described in statement (viii). The edges v_3v_4 and v_1v_6 are contained in the two circles $C(0, r_1)$ and $C(0, r_3)$, where $r_1 = |v_3|$ and $r_3 = |v_1|$. These circles determine the hyperbolic strip $S(r_1, r_3)$ which is a fundamental domain for $\Gamma(10,1)_\infty$, since the transformation h relates these two edges. Let ε_2 the fundamental unit of $\mathbb{Q}(\sqrt{2})$. Check that $\varepsilon_3 r_1 = r_2$ and $\varepsilon_2 r_2 = r_3$, hence, using 4.38, we have that the hyperbolic strip $S(r_1, r_3)$ is symmetric with respect to $C(0, r_2)$, $r_2 = |v_2|$.

The symmetry of $\mathcal{D}(10,1)$ with respect to the imaginary axis is evident. Moreover, it is easy to check that $\mathcal{D}(10,1)$ is invariant with respect to the transformation w and by the hyperbolic symmetry with respect to C_w. Note that these three facts are related, since the transformation w is the product of the two symmetries, and L_w is the imaginary axis. □

4.5.4 Fundamental domain for $X(15,1)$

4.52 Theorem. *Consider the Shimura curve $X(15,1)$. The hyperbolic polygon of vertices $(v_1, v_2, v_3, v_4, v_5, v_6)$,*

$$v_1 = \frac{-2+\iota}{5(2-\sqrt{3})}, \qquad v_2 = \frac{-2+\iota}{5(2+\sqrt{3})}, \qquad v_3 = \frac{2+\iota}{5(2+\sqrt{3})},$$
$$v_4 = \frac{8+\iota}{5(4+\sqrt{3})}, \qquad v_5 = \frac{8+\iota}{5(4-\sqrt{3})}, \qquad v_6 = \frac{2+\iota}{5(2-\sqrt{3})},$$

is a fundamental domain for the Shimura curve $X(15,1)$ in the Poincaré half plane, which we denote by $\mathcal{D}(15,1)$. It has the following properties.

(i) *All the vertices are elliptic of order 3 and the corresponding elliptic transformations* *fixing them are* $\gamma_{v_i} = \frac{1}{2} g_{v_i}$, *where*

$$g_{v_1} = \begin{pmatrix} 1+2\sqrt{3} & 3+2\sqrt{3} \\ 5(3-2\sqrt{3}) & 1-2\sqrt{3} \end{pmatrix}, \qquad g_{v_2} = \begin{pmatrix} 1+2\sqrt{3} & -3+2\sqrt{3} \\ 5(-3-2\sqrt{3}) & 1-2\sqrt{3} \end{pmatrix},$$

$$g_{v_3} = \begin{pmatrix} 1+2\sqrt{3} & 3-2\sqrt{3} \\ 5(3+2\sqrt{3}) & 1-2\sqrt{3} \end{pmatrix}, \qquad g_{v_4} = \begin{pmatrix} 1+8\sqrt{3} & 3-4\sqrt{3} \\ 5(3+4\sqrt{3}) & 1-8\sqrt{3} \end{pmatrix},$$

$$g_{v_5} = \begin{pmatrix} 1+8\sqrt{3} & -3-4\sqrt{3} \\ 5(-3+4\sqrt{3}) & 1-8\sqrt{3} \end{pmatrix}, \quad g_{v_6} = \begin{pmatrix} 1+2\sqrt{3} & -3-2\sqrt{3} \\ 5(-3+2\sqrt{3}) & 1-2\sqrt{3} \end{pmatrix}.$$

(ii) *The hyperbolic volume of* $\mathcal{D}(15,1)$ *is* $V_h(15,1) = \dfrac{8}{3}\pi$ *and the genus of the curve* $X(15,1)$ *is* $g(15,1) = 1$.

(iii) *The principal homothety of* $\Gamma(15,1)$ *is*

$$h = \begin{pmatrix} 2+\sqrt{3} & 0 \\ 0 & 2-\sqrt{3} \end{pmatrix}.$$

(iv) *We have* $n_3(15,1) = 6$ *elliptic vertices of order* 3. *There are* $e_3(15,1) = 2$ *elliptic cycles of order* 3, *namely* $\{v_1, v_2, v_4, v_5\}$ *and* $\{v_3, v_6\}$. *The relations between these vertices are*

$$\begin{array}{ll} h(v_2) = v_1 & h(v_3) = v_6, \\ \beta(v_1) = v_5, & \beta(v_2) = v_4, \\ \gamma(v_6) = v_3, & \gamma(v_5) = v_4, \end{array}$$

where

$$\beta = \frac{1}{2}\begin{pmatrix} 3 & 1 \\ 5 & 3 \end{pmatrix}, \quad \gamma = \frac{1}{2}\begin{pmatrix} -4+3\sqrt{3} & -\sqrt{3} \\ 5(\sqrt{3}) & -4-3\sqrt{3} \end{pmatrix}.$$

(v) *The pairing of the edges is:*

$$\begin{array}{ll} (v_1v_2, v_5v_4) & \text{by the transformation } \beta, \\ (v_2v_3, v_1v_6) & \text{by the transformation } h, \\ (v_3v_4, v_6v_5) & \text{by the transformation } \gamma^{-1}. \end{array}$$

(vi) $\Gamma(15,1)/\pm \mathrm{Id} = \langle h, \beta, \gamma : (\gamma h)^3 = (h\beta^{-1}\gamma\beta)^3 = 1 \rangle$.

(vii) *Put* $r_1 = \sqrt{5}(2-\sqrt{3})/5$, $r_2 = \sqrt{5}/5$ *and* $r_3 = \sqrt{5}(2+\sqrt{3})/5$. $\mathcal{D}(15,1)$ *is included in the hyperbolic strip* $S(r_1, r_3)$, *which is a fundamental domain by the action of* $\Gamma(15,1)_\infty$, *symmetric with respect to the principal hyperbolic line* $C(0, r_2)$. *The edges* v_2v_3 *and* v_1v_6 *are on the hyperbolic lines determined by* $S(r_1, r_3)$, *which are, moreover, principal lines.*

(viii) *The other edges correspond to segments of isometric circles in the following way:* $v_1v_2 \subseteq C_{\gamma_{v_1}}$, $v_3v_4 \subseteq C_{\gamma_{v_2}}$, $v_4v_5 \subseteq C_{\gamma_{v_5}}$ *and* $v_5v_6 \subseteq C_{\gamma_{v_6}}$. *Moreover* $\mathcal{D}(15,1)$ *is the intersection between* $S(r_1, r_3)$ *and the exterior of these isometric circles.*

(ix) $\mathcal{D}(15,1)$ *is symmetric with respect to the principal hyperbolic line given by* $C(0, \sqrt{5}/5)$.

PROOF: The constants attached to the Shimura curve $X(15,1)$ are $e_2(15,1)=0$, $e_3(15,1)=2$, $g(15,1)=1$ and $V_h(15,1)=\frac{8}{3}\pi$.

In a fundamental domain such that all the vertices are elliptic, there must be $n_e(15,1)=6$ vertices, by 4.9. We look for elliptic points of order 3, according to the descriptions given in 4.26 or 4.27. For example, we obtain the points and the corresponding transformations below. Note that the points are placed symmetricly with respect to the imaginary axis.

$$B_1=\frac{-2+\iota}{5(2-\sqrt{3})},\qquad \gamma_{B_1}=\tfrac{1}{2}\begin{pmatrix}1+2\sqrt{3} & 3+2\sqrt{3}\\ 5(3-2\sqrt{3}) & 1-2\sqrt{3}\end{pmatrix},$$

$$B_2=\frac{-2+\iota}{5(2+\sqrt{3})},\qquad \gamma_{B_2}=\tfrac{1}{2}\begin{pmatrix}1+2\sqrt{3} & -3+2\sqrt{3}\\ 5(-3-2\sqrt{3}) & 1-2\sqrt{3}\end{pmatrix},$$

$$B_3=\frac{2+\iota}{5(2+\sqrt{3})},\qquad \gamma_{B_3}=\tfrac{1}{2}\begin{pmatrix}1+2\sqrt{3} & 3-2\sqrt{3}\\ 5(3+2\sqrt{3}) & 1-2\sqrt{3}\end{pmatrix},$$

$$B_4=\frac{2+\iota}{5(2-\sqrt{3})},\qquad \gamma_{B_4}=\tfrac{1}{2}\begin{pmatrix}1+2\sqrt{3} & -3-2\sqrt{3}\\ 5(-3+2\sqrt{3}) & 1-2\sqrt{3}\end{pmatrix},$$

$$B_5=\frac{-8+\iota}{5(4-\sqrt{3})},\qquad \gamma_{B_5}=\tfrac{1}{2}\begin{pmatrix}1+8\sqrt{3} & 3+4\sqrt{3}\\ 5(3-4\sqrt{3} & 1-8\sqrt{3}\end{pmatrix},$$

$$B_6=\frac{-8+\iota}{5(4+\sqrt{3})},\qquad \gamma_{B_6}=\tfrac{1}{2}\begin{pmatrix}1+8\sqrt{3} & -3+4\sqrt{3}\\ 5(-3-4\sqrt{3} & 1-8\sqrt{3}\end{pmatrix},$$

$$B_7=\frac{8+\iota}{5(4+\sqrt{3})},\qquad \gamma_{B_7}=\tfrac{1}{2}\begin{pmatrix}1+8\sqrt{3} & 3-4\sqrt{3}\\ 5(3+4\sqrt{3} & 1-8\sqrt{3}\end{pmatrix},$$

$$B_8=\frac{8+\iota}{5(4-\sqrt{3})},\qquad \gamma_{B_8}=\tfrac{1}{2}\begin{pmatrix}1+8\sqrt{3} & -3-4\sqrt{3}\\ 5(-3+4\sqrt{3} & 1-8\sqrt{3}\end{pmatrix}.$$

We look for relations between these elliptic points. In this case, the elliptic transformations do not give any relation. If we consider the principal homothety h, we have

$$h=\begin{pmatrix}2+\sqrt{3} & 0\\ 0 & 2-\sqrt{3}\end{pmatrix},\quad h(B_1)=B_2,\ h(B_3)=B_4.$$

To find other relations we look for new hyperbolic transformations, applying the results of embeddings of fundamental units of real quadratic orders. Consider the quadratic field $\mathbb{Q}(\sqrt{5})$, splitting $H_B(3,5)$. The fundamental unit of the ring of integers is $\varepsilon_5=\frac{1+\sqrt{5}}{2}$, of norm $\mathrm{n}(\varepsilon_5)=-1$. Fixing an embedding φ of the ring of integers of $\mathbb{Q}(\sqrt{5})$ in $\mathcal{O}(15,1)$, we obtain the transformation

$$\beta=\Phi(\varphi(\varepsilon_5^2))=\frac{1}{2}\begin{pmatrix}3 & 1\\ 5 & 3\end{pmatrix},\qquad \text{satisfying } \beta(B_2)=B_8 \text{ and } \beta(B_1)=B_7.$$

We look directly for relations between the vertices. We find:

$$\gamma = \frac{1}{2}\begin{pmatrix} -4+3\sqrt{3} & -\sqrt{3} \\ 5(\sqrt{3}) & -4-3\sqrt{3} \end{pmatrix}, \qquad \text{satisfying } \gamma(B_4) = B_3 \text{ and } \gamma(B_8) = B_7.$$

Thus, we have the sets of equivalent vertices $\{B_1, B_2, B_5, B_6\}$ and $\{B_3, B_4\}$. After checking that the vertices of two different sets are not equivalent, we have 6 elliptic points of order 3 in 2 cycles.

Consider the hyperbolic polygon formed by the 6 elliptic points:

$$(B_1, B_2, B_3, B_7, B_8, B_4).$$

We change the notation and denote its vertices by $(v_1, v_2, v_3, v_4, v_5, v_6)$. The above relations give a pairing of the edges. Its hyperbolic volume is $\frac{8}{3}\pi$. Thus, effectively the hyperbolic polygon $\mathcal{D}(15,1)$ is a fundamental domain for the Shimura curve $X(15,1)$. Its graphical representation is in figure 8.4, setting the pairing of the edges.

By taking into account the Euler-Poincaré characteristic, we see that the genus is 1. Moreover, we obtain the following presentation of the group $\Gamma(15,1)/\pm\mathrm{Id}$:

$$\langle h, \beta, \gamma : (\gamma h)^3 = 1, (h\beta^{-1}\gamma\beta)^3 = 1\rangle.$$

We note that most of the edges are segments of isometric circles, as described in statement (viii). The edges v_2v_3 and v_1v_6 are in the two circles $C(0,r_1)$ and $C(0,r_3)$, where $r_1 = |v_2|$ and $r_3 = |v_1|$. Those circles determine the hyperbolic strip $S(r_1, r_3)$ which is a fundamental domain for $\Gamma(15,1)_\infty$, since the transformation h relates these two edges. We denote by ε_3 the fundamental unit of $\mathbb{Q}(\sqrt{3})$. Put $r_2 := \varepsilon_3 r_1 = \sqrt{5}/5$; then $\varepsilon_3 r_2 = r_3$, hence $S(r_1, r_3)$ is symmetric with respect to $C(0, r_2)$, using 4.38. The hyperbolic lines defined by $C(0, r_i)$ are principal lines, since they come from the transformations η_i given by:

$$\eta_1 = \frac{1}{\sqrt{15}}\begin{pmatrix} 0 & 3-2\sqrt{3} \\ 5(3+2\sqrt{3}) & 0 \end{pmatrix}, \quad \eta_2 = \frac{1}{\sqrt{5}}\begin{pmatrix} 0 & -1 \\ 5 & 0 \end{pmatrix},$$

$$\eta_3 = \frac{1}{\sqrt{15}}\begin{pmatrix} 0 & -3-2\sqrt{3} \\ 5(-3+2\sqrt{3}) & 0 \end{pmatrix}.$$

It is clear that the fundamental domain $\mathcal{D}(15,1)$ is the intersection of the hyperbolic strip and the exterior of the isometric circles that contains the other edges.

Finally, it is easy to check that $\mathcal{D}(15,1)$ is invariant under the hyperbolic symmetry with respect to the principal hyperbolic line $C(0, r_2)$. □

Figure 5.1 represents the fundamental domain for the Shimura curve $X(6,1)$ given in theorem 4.49. We collect the corresponding data in table 1.

The fundamental domain constructed for the Shimura curve $X(10,1)$, cf. 4.50, can be seen in the figure 5.2. We also represent the intersection of the isometric circle C_w with the fundamental domain. It is easy to check graphically that the domain is invariant under the transformation w and that C_w is an axis of symmetry of the domain. Table 2 contains the explicit points and cycles.

We reproduce in figure 5.3 the fundamental domain given in 4.52 for the Shimura curve $X(15,1)$. This graphical representation can also be found in [Vig80]. We also represent the principal hyperbolic line giving the principal symmetry in the domain. In table 3, we present data about points and cycles.

Table 1: *Elliptic cycles of the Shimura curve* $X(6,1)$ *and presentation of the group* $\Gamma(6,1)/\pm\mathrm{Id}$.

k	$n_k(6,1)$	$e_k(6,1)$	cycles of order k of $\Gamma(6,1)$
2	4	2	$\{v_6\}$ and $\{v_1, v_3, v_5\}$
3	2	2	$\{v_2\}$ and $\{v_4\}$

generators	relations
$\gamma_{v_2}, \gamma_{v_4}, \gamma_{v_6}$	$\gamma_{v_2}^3 = 1, \gamma_{v_4}^3 = 1, \gamma_{v_6}^2 = 1, (\gamma_{v_2}^{-1}\gamma_{v_6}\gamma_{v_4})^2 = 1$

Figure 5.2: Fundamental domain for $X(10,1)$.

Table 2: *Elliptic cycles of the Shimura curve* $X(10,1)$ *and presentation of the group* $\Gamma(10,1)/\pm\mathrm{Id}$.

k	$n_k(10,1)$	$e_k(10,1)$	cycles of order k of $\Gamma(10,1)$
2	0	0	
3	6	4	$\{v_2\}$, $\{v_5\}$, $\{v_1, v_3\}$, $\{v_4, v_6\}$

generators	relations
$\gamma_{v_2}, \gamma_{v_5}, h$	$\gamma_{v_2}^3 = 1, \gamma_{v_5}^3 = 1, (h^{-1}\gamma_{v_2})^3 = 1, (h^{-1}\gamma_{v_5})^3 = 1$

Figure 5.3: Fundamental domain for $X(15,1)$.

Table 3: *Elliptic cycles of the Shimura curve* $X(15,1)$ *and presentation of the group* $\Gamma(15,1)/\pm\mathrm{Id}$.

k	$n_k(15,1)$	$e_k(15,1)$	cycles of order k of $\Gamma(15,1)$
2	0	0	
3	6	2	$\{v_1, v_2, v_4, v_5\}, \quad \{v_3, v_6\}$

generators	relations
$h,\ k,\ \gamma$	$(\gamma h)^3 = 1, (hk^{-1}\gamma k)^3 = 1$

Bibliography

[AB00a] A. Arenas and P. Bayer, *Complex multiplication points on modular curves*, *Rev. R. Acad. Cienc. Exact. Fis. Nat.* **94** (2000), no. 3, 333–338.

[AB00b] A. Arenas and P. Bayer, *Heegner points on modular curves*, *Rev. R. Acad. Cienc. Exact. Fis. Nat.* **94** (2000), no. 323-332.

[AlBa04] M. Alsina and P. Bayer, *Quaternion Orders, Quadratic Forms and Shimura Curves*, CRM Monograph Series vol. 22, AMS (2004).

[Alb34] A. A. Albert, *Integral domains of rational generalized quaternion algebras*, Bull. American Mathematical Society **40** (1934), 164–176.

[Alb35] A. A. Albert, *Involutorial simple algebras and real Riemann matrices*, Annals of Math. **36** (1935), 886–964.

[Als97] M. Alsina, *Fundamental domains of the upper half plane by the action of matrix groups*, Meeting on matrix analysis and applications, Dept. Mat. Apl. I, Fac. Informática y Estadística, Univ. de Sevilla (1997), 10–17.

[Als99] M. Alsina, *Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de Shimura*, Tesi doctoral, Universitat de Barcelona (2000), Publicacions de la UB, ISBN: 84-475-2491-4 (2001).

[Als00] M. Alsina, *Dominios fundamentales modulares*, *Rev. R. Acad. Cienc. Exact. Fis. Nat.* **94** (2000), no. 3, 309–322.

[Are87] A. Arenas, *On integral representations by quadratic forms*, Linear and Multilinear Algebra **22** (1987), 149–160.

[BC91] J-F. Boutot and H. Carayol, *Courbes modulaires et courbes de Shimura*, Astérisque, vol. 196-197, ch. Uniformisation p-adique des courbes de Shimura: les théorèmes de Cerednik et Drinfeld, Soc. Math. de France (1991), 45–158.

[Bes95] A. Besser, *CM cycles over Shimura curves*, J. Algebraic Geometry **4** (1995), 659–691.

[BLR91] N. Boston, H. Lenstra, and A. Ribet, *Quotients of group rings from two-dimensional representations*, C. R. Acad. Sci. Paris **312** (1991), 323–328.

[Bra24] H. Brandt, *Der Kompositionsbegriff bei den quaternären quadratischen Formen*, Math. Annalen **91** (1924), 300–315.

[Bra28] H. Brandt, *Idealtheorie in Quaternionenalgebren*, Math. Annalen **99** (1928), 1–29.

[Bra43] H. Brandt, *Zur Zahlentheorie der Quaternionen*, Jahresbericht Deutsche Math. Verein **53** (1943), 23–57.

[Brz80] J. Brzezinski, *Arithmetical quadratic surfaces of genus 0, I*, Math. Scand. **46** (1980), 183–208.

[Brz82] J. Brzezinski, *A characterization of Gorenstein orders in quaternion algebras*, Math. Scand. **50** (1982), 19–24.

[Brz83] J. Brzezinski, *On orders in quaternion algebras*, Comm. in Algebra **11** (1983), 501–522.

[Brz90] J. Brzezinski, *On automorphisms of quaternion orders*, J. reine angew. Math. **403** (1990), 166–186.

[Brz95] J. Brzezinski, *Definite quaternion orders of class number one*, J. de Théorie des Nombres de Bordeaux **7** (1995), 93–96.

[BS66] Z.I. Borevich and I.R. Shafarevich, *Number theory*, Academic Press (1966).

[BT00a] P. Bayer and A. Travesa, *Formas cuadráticas ternarias e inmersiones matriciales de órdenes cuadráticos*, *Rev. R. Acad. Cienc. Exact. Fis. Nat.* **94** (2000), no. 3, 347–355.

[BT00b] P. Bayer and A. Travesa, *Inmersiones de órdenes cuadráticos en el orden generado por* $\Gamma_0(N)$, *Rev. R. Acad. Cienc. Exact. Fis. Nat.* **94** (2000), no. 3, 357–376.

[BT00c] P. Bayer and A. Travesa, *Órdenes matriciales generados por grupos de congruencia*, *Rev. R. Acad. Cienc. Exact. Fis. Nat.* **94** (2000), no. 3, 339–346.

[Buz97] K. Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. **87** (1997), 591–612.

[Car83] H. Carayol, *Sur la mauvaise réduction des courbes de Shimura*, C. R. Acad. Sc. Paris **296** (1983), 557–560.

[Car86] H. Carayol, *Sur la mauvaise réduction des courbes de Shimura*, Compositio Math. **59** (1986), 151–230.

[Cer76] I.V. Cerednik, *Uniformization of algebraic curves by discrete arithmetic subgroups of* $\mathrm{PGL}_2(K_w)$ *with compact quotients*, Math. USSR Sb. **29** (1976), 55–78.

[Coh95] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer (1995).

[CSS97] G. Cornell, J. H. Silverman, and G. Stevens (eds.), *Modular forms and Fermat's last theorem*, Springer, (1997), Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston MA (1995).

[DDT97] H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem*, Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), Internat. Press (1997), 2–140.

[Del71] P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki 23 année 1970-71, Lecture Notes in Math., no. 244, Springer (1971), 123–165.

[Del79] P. Deligne, *Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques*, Proceedings of Symposia in Pure Mathematics (1979), 247–290.

[Deu68] M. Deuring, *Algebren*, Springer (1968).

[Dia97a] F. Diamond, *The refined conjecture of Serre*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Internat. Press (1997), 22–37.

[Dia97b] F. Diamond, *The Taylor-Wiles construction and multiplicity one*, Invent. Math. **128** (1997), 379–391.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp), Lecture Notes, vol. 349, Springer (1973), 143–316.

[Dri76] V.G. Drinfeld, *Coverings of p-adic symmetric regions*, Funct. Anal. Appl. **10** (1976), 107–115.

[DT94] F. Diamond and R. Taylor, *Nonoptimal levels of mod l modular representations*, Invent. Math. **115** (1994), 435–462.

[Eic37] M. Eichler, *Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren*, J. reine angew. Math. **176** (1937), 192–202.

[Eic38] M. Eichler, *Über die Idealklassenzahl hyperkomplexer Systeme*, Math. Z. **43** (1938), 481–494.

[Eic55a] M. Eichler, *Über die Darstellbarkeit von Modulformen durch Thetareihen*, J. reine angew. Math. **195** (1955), 156–171.

[Eic55b] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. reine angew. Math. **195** (1955), 127–151.

[Eic58] M. Eichler, *Quadratische Formen und Modulfunktionen*, Acta Arith. **4** (1958), 217–239.

[Elk98] N.D. Elkies, *Shimura curve computations*, Lect. Notes in Computer Science **1423** (1998), 1–49.

[FJ95] G. Faltings and B. W. Jordan, *Crystalline cohomology and* $\mathrm{GL}(2, \mathbb{Q})$, Israel J. Math. **90** (1995), 1–66.

[For51] L. R. Ford, *Automorphic functions*, 2na ed., Chelsea (1951).

[FK1897] R. Fricke and F. Klein, *Vorlesungen über die Theorie der automorphen Funktionen*, Leipizig (1897).

[Gau1801] C.F. Gauss, *Disquisitiones arithmeticae*, Gerh. Fleischer, 1801. Translation to catalan by G. Pascual, IEC, Soc. Cat. Mat. (1996).

[Ger79] P. Gerardin, *Variétés de Shimura et fonctions L*, Publ. Math. Univ. Paris VII, no. 6, ch. Algebres de quaternions, 145–155, L. Breen and J.P. Labesse, (1979).

[God78] R. Godement, *Algebra*, Ed. Tecnos (1978).

[Has33] H. Hasse, *Die Struktur der R. Brauerschen algebrenklassengruppe über einem algebraischen Zahlkörper*, Math. Annalen **107** (1933), 731–760.

[Hij74] H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\gamma_0(n)$, J. Math. Soc. Japan. **26** (1974), 56–82.

[HM95] K. Hashimoto and N. Murabayashi, *Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of Genus two*, Thoku Math. J. **47** (1995), 271–296.

[Iha68] Y. Ihara, *The congruence monodromy problem*, J. Math. Soc. Japan **20** (1968), 107–121.

[Iha69] Y. Ihara, *On congruence monodromy problems*, Lecture Notes Univ. Tokyo, vol. 1-2, (1969).

[Ish75] N. Ishii, *An application of the Fricke formula for quaternion groups*, Mathematica Japonicae **20** (1975), 171–177.

[Ji98] S. Ji, *Analogs of* $\Delta(z)$ *for triangular Shimura curves*, Acta Arith. **85** (1998), 97–108.

[JL85] B.W. Jordan and R. Livné, *Local diophantine properties of Shimura curves*, Math. Annalen **270** (1985), 235–248.

[JL86] B.W. Jordan and R. Livné, *On the Néron model of jacobians of Shimura curves*, Compositio Math. **60** (1986), 227–236.

[JL87] B.W. Jordan and R. Livné, *Divisor classes on Shimura curves rational over local fields*, J. reine angew. Math. **378** (1987), 46–52.

[JL89] B.W. Jordan and R. Livné, *Conjecture epsilon for weight* $k > 2$, Bull. Amer. Math. Soc. **21** (1989), 51–56.

[JL99] B.W. Jordan and R. Livné, *On Atkin-Lehner quotients of Shimura curves*, Bull. London Math. Soc. **31** (1999), 681–685.

[Jon67] B.W. Jones, *The arithmetic theory of quadratic forms*, The mathematical association of America (1967).

[Jor81] B.W. Jordan, *On the diophantine arithmetic of Shimura curves*, Ph.D. thesis, Harvard University (1981).

[Jor84] B.W. Jordan, *p-adic points on Shimura curves*, Séminaire de théorie des nombres de Paris 1982-83 (M.J. Bertin and C. Goldstein, eds.), Progress in Math., vol. 51, Birkhäuser (1984), 135–142.

[Jor86] B.W. Jordan, *Points on Shimura curves rational over number fields*, J. reine angew. Math. **371** (1986), 92–114.

[Kam90] S. Kamienny, *Points on Shimura curves over fields of even degree*, Math. Annalen **286** (1990), 731–734.

[Kit93] Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge Tracts in Mathematics, no. 106, Cambrigde University Press (1993).

[KM85] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton (1985).

[Kur79] A. Kurihara, *On some exemples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Tokyo **25** (1979), 277–300.

[Kur94] A. Kurihara, *On p-adic Poincaré series and Shimura curves*, Internat. J. Math. **5** (1994), 747–763.

[Lat36] C.G. Latimer, *The quadratic subfields of a generalized quaternion algebra*, Duke Math. J. **2** (1936), 681–684.

[Lat37] C.G. Latimer, *The classis of integral sets in a quaternion algebra*, Duke Math. J. **3** (1937), 237–247.

[Leh64] J. Lehner, *Discontinuous groups and automorphic functions*, Mathematical Surveys n.8, American Mathematical Society (1964).

[Leh92] J.L. Lehman, *Levels of positive definite ternary quadratic forms*, Math. of Computation **58** (1992), 399–417.

[Lin93] S. Ling, *Shimura subgroups of jacobians of Shimura curves*, Proceedings of the Amer. Math. Soc. **118** (1993), 385–390.

[Llo00] P. Llorente, *Correspondencia entre formas ternarias enteras y órdenes cuaterniónicos*, *Rev. R. Acad. Cienc. Exact. Fis. Nat.* **94** (2000), no. 3, 397–416.

[Mic81a] J.F. Michon, *Courbes de Shimura de genre 1*, Séminaire Delange-Pisot-Poitou (1981).

[Mic81b] J.F. Michon, *Courbes de Shimura hyperelliptiques*, Bull. Soc. Math. France **109** (1981), 217–225.

[Mor81] Y. Morita, *Reduction mod* $\mathfrak{p}$ *of Shimura curves*, Hokkaido Math. J. **10** (1981), 209–238.

[MR91] B. Mazur and K. A. Ribet, *Courbes modulaires et courbes de Shimura*, Astérisque, vol. 196-197, ch. Two-dimensional representations in the arithmetic of modular curves, 215–255, Soc. Math. de France (1991).

[Ogg69] A. Ogg, *Modular forms and Dirichlet series*, Mathematics Lecture Note Series, W.A. Benjamin, Inc. (1969).

[Ogg74] A.P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. math. France **102** (1974), 449–462.

[Ogg83] A.P. Ogg, *Real points on Shimura curves*, Progress in mathematics, no. 35, Birkhäuser (1983), 277–303.

[Ogg85] A.P. Ogg, *Mauvaise réduction des courbes de Shimura*, Progress in mathematics, no. 59, Birkhäuser (1985), 199–217.

[Piz73] A. Pizer, *Type numbers of Eichler orders*, J. reine angew. Math. **264** (1973), 76–102.

[Piz76a] A. Pizer, *On the arithmetic of quaternion algebras I*, Acta Arith. **31** (1976), 61–89.

[Piz76b] A. Pizer, *On the arithmetic of quaternion algebras II*, J. Math. Soc. Japan **28** (1976), 676–688.

[Piz80] A. Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)^*$, Journal of Algebra **64** (1980), 340–390.

[Poi1887] H. Poincaré, *Les fonctions fuchsiennes et l'arithémtique*, Journal Math. **4** (1887), en *Ouvres Completes* vol. II, 463-511, Gauthier-Villars (1952).

[Ray70] M. Raynaud, *Specialisation du foncteur de Picard*, Inst. Hautes Etudes Sci. Publ. Math. **38** (1970), 27–76.

[Rei75] I. Reiner, *Maximal Orders*, Academic Press (1975).

[Rib80] K.A. Ribet, *Sur les variétés abéliennes à multiplications réelles*, C.R. Acad. Sci. Paris **291** (1980), 121–123.

[Rib89] K.A. Ribet, *Bimodules and abelian surfaces*, Advanced Studies in Pure Mathematics **17** (1989), 359–407.

[Rib90] K.A. Ribet, *On modular representations of* Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.

[Rib91] K.A. Ribet, *Lowering the levels of modular representations without multiplicity one*, Duke Math. J. **62** (1991), 15–19.

[Rib94] K. A. Ribet, *Report on mod l representations of* Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$, Motives (Seattle, WA, 1991), Amer. Math. Soc. (1994), 639–676.

[RT97] K. A. Ribet and S. Takahashi, *Parametrizations of elliptic curves by Shimura curves and by classical modular curves*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), 11110–11114, Elliptic curves and modular forms (Washington, DC, 1996).

[Ser73] J.P. Serre, *A course in arithmetic*, Graduate texts in Mathematics, no. 7, Springer-Verlag (1973).

[Ser87] J.P. Serre, *Sur les représentations modulaires de degré* 2 *de* Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

[Shi59] G. Shimura, *On the theory of automorphic functions*, Annals of Math. **70** (1959), 101–144.

[Shi63] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions*, Annals of Math. **78** (1963), 149–192.

[Shi65] G. Shimizu, *On zeta functions of quaternion algebras*, Annals of Math. **81** (1965), 166–193.

[Shi66] G. Shimura, *Moduli and fibre systems of abelian varieties*, Annals of Math. **83** (1966), 294–338.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Annals of Math. **85** (1967), 58–159.

[Shi70a] G. Shimura, *On canonical models of arithmetic quotients of bounded symetric domains I*, Annals of Math. **91** (1970), 144–222.

[Shi70b] G. Shimura, *On canonical models of arithmetic quotients of bounded symetric domains II*, Annals of Math. **92** (1970), 528–549.

[Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press (1971).

[Shi75] G. Shimura, *On the real points of arithmetic quotient of a bounded symetric domain*, Math. Annalen **215** (1975), 135–164.

[Sie35] C.L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Annals of Math. **36** (1935), 527–606, en *Gesammelte Abhandlungen*, vol. I, Springer (1966).

[Sie44] C.L. Siegel, *On the theory of indefinite quadratic forms*, Annals of Math. **45** (1944), 577–622, en *Gesammelte Abhandlungen*, vol. II, Springer (1966).

[Sie71] C.L. Siegel, *Topics in complex function theory vol. II*, Wiley-Interscience (1971).

[Tak75] K. Takeuchi, *A characterization of arithmetic fuchsian groups*, J. Math. Soc. Japan **27** (1975), 600–612.

[Tak77a] K. Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), 91–106.

[Tak77b] K. Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo, I.A. **24** (1977), 201–212.

[TW95] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.

[vdP89] M. van-der Put, *Les courbes de Shimura*, Séminaire de Theorie des Nombres de Bordeaux **1** (1989), 89–102.

[Var98] Y. Varshavsky, *p-adic uniformization of unitary Shimura varieties*, Publ. Math. IHES **87** (1998), 57–119.

[Vig80] M.F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., no. 800, Springer (1980).

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

[Zag81] D. Zagier, *Zetafunktionen und quadratische Körper*, Hochschultex, Springer (1981).