UNIVERSITAT DE BARCELONA

Shimura curves and their *p-adic* uniformization

Corbes de Shimura i les seves uniformitzacions p-àdiques

Piermarco Milione

UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques
Departament d'Àlgebra i Geometria

Shimura curves and their *p*-adic uniformizations

Corbes de Shimura i les seves uniformitzacions p-àdiques

Piermarco Milione

UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques
Departament d'Àlgebra i Geometria

Shimura curves and their *p*-adic uniformizations

Corbes de Shimura i les seves uniformitzacions p-àdiques

Memòria presentada per a optar al grau de doctor en Matemàtiques per

Piermarco Milione

Departament d'Àlgebra i Geometria

Doctorand: Piermarco Milione

Tutora i directora de la tesi: Dra. Pilar Bayer i Isant

Pilar Bayer Isant, catedràtica d'àlgebra
de la Facultat de Matemàtiques de la Universitat de Barcelona,
FAIG CONSTAR
que el senyor Piermarco Milione ha realitzat aquesta memòria
per a optar al grau de Doctor en Matemàtiques sota la meva direcció.

Barcelona, novembre del 2015

Signat: Pilar Bayer Isant

“Rien n’est plus fécond, tous les mathématiciens le savent, que ces obscures analogies, ces troubles reflets d’une théorie à une autre, ces furtives caresses, ces brouilleries inexplicables ; rien aussi ne donne plus de plaisir au chercheur.”

De la métaphysique aux mathématiques, André Weil

Introduction

The main purpose of this dissertation is to introduce Shimura curves from the non-Archimedean point of view, paying special attention to those aspects that can make this theory amenable for computations. Despite the fact that the theory of p-adic uniformization of Shimura curves goes back to the 1960s with the results of Cerednik and Drinfeld, only in the last years explicit examples related to these uniformizations have been computed (cf. [FM14]).

First of all, let us recall that the canonical model of a Shimura curve, as defined by Shimura in [Shi67], is actually an Archimedean uniformization of the algebraic curve. Given an indefinite quaternion algebra H over $\mathbb{Q}$ of discriminant D_H and an Eichler order $\mathcal{O}_H$ over $\mathbb{Z}$ of level N, and once a real matricial immersion $\Phi : H \hookrightarrow \mathrm{M}_2(\mathbb{R})$ has been fixed, let $\Gamma(D_H, N)$ be the Fuchsian group defined by

$$\Gamma(D_H, N) := \Phi(\{\alpha \in \mathcal{O}_H^* \mid \mathrm{Nm}_{H/\mathbb{Q}}(\alpha) > 0\})/\{\pm \mathrm{I}_2\} \subseteq \mathrm{PGL}_2(\mathbb{R})_{>0},$$

together with its action on the Poincaré upper half-plane $\mathcal{H}$. The canonical model of the corresponding Shimura curve is formed by an algebraic curve $X(D_H, N)$ defined over $\mathbb{Q}$, and by an analytic function $J = (J_1, \ldots, J_d) : \mathcal{H} \to \mathbb{P}^d(\mathbb{C})$ inducing a bijection

$$J : \Gamma(D_H, N)\backslash\mathcal{H} \simeq X(D_H, N)(\mathbb{C})$$

between the set of complex points of the Riemann surface $\Gamma(D_H, N)\backslash\mathcal{H}$ and the set of complex points of the Shimura curve $X(D_H, N)$.

Moreover, in order to be canonical, this model is required to satisfy an important property related to the classical theory of complex multiplication.

The functions $J_i : \mathcal{H} \to \mathbb{P}(\mathbb{C})$ are called *uniformizing functions* for the Shimura curve $X(D_H, N)$, and the relations of algebraic dependence that these satisfy over $\mathbb{Q}$ provide equations of the canonical model of the curve. We refer to the analytic space $\Gamma(D_H, N)\backslash\mathcal{H}$ as the *space of parameters* of the uniformization.

Making use of the definition of canonical model, many interesting arithmetical properties of the algebraic curve $X(D_H, N)$ can be discovered. Nevertheless, the computation of equations seems to be more complicated in the case $D_H > 1$ and even in many cases in which the equations are known, the uniformizing functions remain unknown. The difficulty in computing the complex uniformizing functions in the case of discriminant $D_H > 1$ is, as is well known, the lack of cusps and, consequentially, the lack of a Fourier series expansion.

The first step in making this complex uniformization explicit is to compute a fundamental domain for the action of the uniformizing group $\Gamma(D_H, N)$. Secondly, one can consider the problem of looking for the functions J_i which are invariant for the action of this group and satisfy the algebraic dependence relations. This process has been carried out for some cases, in a series of research studies: in [AB04] fundamental domains for the action of the groups $\Gamma(D_H, N)$ in the case of discriminant $D_H = 6, 10$ and 15 are computed, and later in [BT07] and [BT08] uniformizing functions for the canonical model of the Shimura curve $X(6, 1)$ are found as solution to a certain differential equation. In [Nua15] a more general approach allows the computation of complex uniformizing functions for all Shimura curves having an Atkin-Lehner quotient of genus zero.

Now then, with the same objective as in the complex case, we have started the study of the p-adic uniformization of the Shimura curves $X(D_H, N)$. First of all we briefly state the theorem of Cerednik-Drinfeld in a form which will allow us to make it explicit.

Let us fix a prime integer $p|D_H$ and let B be the definite quaternion algebra over $\mathbb{Q}$ of discriminant $D_B = p^{-1}D_H$, and $\mathcal{O}_B[1/p]$ be an Eichler order over $\mathbb{Z}[1/p]$ of level N. Once a p-adic matricial immersion $\Phi_p : B \hookrightarrow \mathrm{M}_2(\mathbb{Q}_p)$ has been fixed, we define the following discrete and cocompact subgroup of $\mathrm{PGL}_2(\mathbb{Q}_p)$:

$$\Gamma_{p,+}(D_B, N) := \Phi_p(\{\alpha \in \mathcal{O}_B[1/p]^* \mid v_p(\mathrm{Nm}(\alpha)) \equiv 0 \,(\mathrm{mod}\, 2)\})/\{\pm p^s \mathrm{I}_2 \mid s \in \mathbb{Z}\}.$$

The p-adic points of the Shimura curve $X(D_H, N)$ are obtained thanks to the following bijection:

$$\Gamma_{p,+}(D_B, N)\backslash\mathcal{H}_p(\mathbb{C}_p) \simeq X(D_H, N)(\mathbb{C}_p),$$

where $\mathcal{H}_p(\mathbb{C}_p) := \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{P}^1(\mathbb{Q}_p)$ is the set of $\mathbb{C}_p$-points of the p-adic upper half-plane $\mathcal{H}_p$ over $\mathbb{Q}_p$ and once an immersion of $\overline{\mathbb{Q}}$ inside $\overline{\mathbb{Q}}_p$ has been fixed.

As in the Archimedean case, the first step in order to make explicit the Cerednik-Drinfeld uniformization is, then, to compute a fundamental domain

in $\mathcal{H}_p(\mathbb{C}_p)$ for the action of the group $\Gamma_{p,+}(D_B, N)$, together with its interpretation as an analytic variety. Following this path, first we have to deal with a p-adic analytic geometry, known as *rigid* analytic geometry.

It is well known that the theory of non-Archimedean uniformization of curves starts with Tate's result on the p-adic uniformization of elliptic curves with split multiplicative reduction. In the same way, the birth of non-Archimedean analysis can be recognized in some Tate's notes from the 1960s, published only later in 1971 (cf. [Tat71]). In these notes, Tate defined the theory of non-Archimedean analytic functions which took care to avoid the lack of *analytic continuation* for these functions, caused by the fact that the p-adic analog of the complex plane, $\mathbb{C}_p$, is totally disconnected.

The theory of Tate is adapted, and even extended, by Mumford to the pure algebro-geometric language of some formal schemes, for which rigid analytic varieties turn out to be the *generic fibre*, in a totally new sense of the word since, in general, the generic fibre of a formal scheme is not defined.

Specifically, let A be an integrally closed, local, Noetherian and complete ring, and let K be its field of fractions and k be its residue field. In his celebrated paper [Mum72] Mumford finds a family of algebraic curves C defined over K, with integral model $\mathcal{C}$ over A, admitting a uniformization for certain discrete subgroups of $\mathrm{PGL}_2(K)$. In the language of formal schemes this means that the formal completion $\widehat{\mathcal{C}}$ of the scheme $\mathcal{C}$, along its closed fibre $\mathcal{C}_0/k$, can be expressed as a quotient in the following form:

$$\Gamma\backslash\widehat{\mathcal{H}}_\Gamma \simeq \widehat{\mathcal{C}},$$

where Γ is a certain discrete subgroup of $\mathrm{PGL}_2(K)$ and $\widehat{\mathcal{H}}_\Gamma$ is the "half-plane" associated to Γ, as a formal scheme over $\mathrm{Spf}\, A$.

Mumford's uniformization is the first one to use, in the non-Archimedean context, a space of parameters similar to the hyperbolic spaces of parameters, such as the upper half-plane $\mathcal{H}$, or the upper half-space $\{(z, x) \in \mathbb{C}\times\mathbb{R} \mid x > 0\}$. The p-adic spaces of parameters $\widehat{\mathcal{H}}_\Gamma$ are, in fact, constructed by Mumford starting from the groups Γ in order to obtain a properly discontinuous action: for this reason he has to exclude those points which are accumulation points for the action of the group Γ, i.e. the set of limit points. The groups considered by Mumford are the well-known p-adic Schottky groups. When the ring A has Krull dimension $\dim A = 1$, Mumford's theory can be translated into the language of rigid analytic geometry, as is done in [GvDP80].

The advantage of the theory of p-adic uniformization of curves, compared to the complex one, is the presence of a *reduction map*. Every rigid analytic variety over the field K has naturally associated a reduction map which

coincides with the reduction modulo p of the strictly convergent series locally defining this variety. Hence, as a reduction of a rigid analytic variety over K, we obtain an algebraic variety defined over the residue field k. In those cases in which these rigid analytic varieties are obtained as rigidification of algebraic varieties, that is endowing an algebraic variety over K with a structure of rigid analytic variety, then the reduction of these analytic varieties becomes more interesting since it can be identified with the special fibre of a certain, well-determined, integral model of the algebraic variety. Therefore, computing an explicit uniformization of the curve includes, as a gift, the special fibre of an integral model of this curve.

As we said at the beginning, the canonical model $(X(D_H, N), J)$ is characterized by a certain arithmetical property which has to be satisfied by some "special" parameters of its uniformization. To be more precise, the values of the complex function J at certain imaginary quadratic parameters $\tau \in \mathcal{H}$ must be algebraic points of the Shimura curve $X(D_H, N)$. We refer to these parameters by *complex multiplication parameters* and to the corresponding algebraic points, as is usual, by complex multiplication points. Complex multiplication parameters acquire, as is well known, a geometrical meaning, when the space of parameters $\Gamma(D_H, N)\backslash\mathcal{H}$ is endowed with a modular interpretation in terms of polarized abelian surfaces with quaternionic multiplication of a fixed PEL type. In particular, the complex multiplication parameters define, in each of these modular interpretations, certain abelian surfaces with complex multiplication.

Complex multiplication parameters are fundamental in the explicit computation of the canonical model of a Shimura curve, since they characterize the uniformizing functions J. For this reason it is necessary, making explicit a complex uniformization of the Shimura curve $X(D_H, N)$, to place these parameters inside the fundamental domain associated to the uniformization. In [AB04] some of these parameters are computed, in the cases of discriminant $D_H = 6, 10$ and 15, obtaining them as zeros of binary quadratic forms with algebraic coefficients. In [BR14] a reduction point algorithm associated to the fundamental domain of $\Gamma(D_H, N)\backslash\mathcal{H}$ in the cases $D_H = 6, 10, 15$, makes it possible, given a complex multiplication parameter $\tau \in \mathcal{H}$, to find its $\Gamma(D_H, N)$-equivalent(s) parameter(s), belonging to the fundamental domain considered. Moreover in [BG05] a symplectic basis for the uniformizing lattices of the abelian surfaces corresponding to complex multiplication parameters, is computed in some particular cases.

Finally, as an important application, the computation of complex multiplication parameters in $\Gamma(D_H, N)\backslash\mathcal{H}$ can be used in many cases to compute certain algebraic points on modular elliptic curves (see [Dar03] for an

overview).

If we want to replace the complex uniformization of the curve $X(D_H, N)$ by the p-adic uniformization, then it becomes natural to look for a p-adic analog of complex multiplication parameters. These have to correspond to special points inside the modular interpretation of the quotient space $\Gamma_{p,+}(D_B, N)\backslash\mathcal{H}_p(\mathbb{C}_p)$, given by Drinfeld in [Dri76].

A satisfactory introduction to Shimura curves, following [Shi67], lies on the comprehension and the introduction of Eichler's results on arithmetic in quaternion orders (cf. [Eic37], [Eic38a], [Eic38b], [Eic55]). Hence, concluding this overview on the theory of the p-adic uniformization of Shimura curves, we put in evidence some of its relations with the arithmetic in quaternion algebras.

As we shall see in this dissertation, the main sensation that we obtain, when we investigate results relating to the p-adic uniformization of Shimura curves, is that it is a theory which mirrors and extends the theory of complex uniformization. What is more, studying the original papers of Cerednik, [Cer76a] and [Cer76b], we can see how the *Theorem of interchanging local invariants* is stated as an *isomorphism* between the two uniformizations and we can appreciate how the roles of the primes p and ∞ are, in some sense, interchangeable. Again, this dualism becomes stronger once the p-adic uniformization of the Shimura curve $X(D_H, N)$, and in particular the quotient $\Gamma_{p,+}(D_H, N)\backslash\mathcal{H}_p(\mathbb{C}_p)$, is endowed with a modular interpretation (cf. [Dri76], [BC91]). This last can then be interpreted, with some care, as the natural p-adic translation of the usual modular interpretation of the complex quotient $\Gamma(D_H, N)\backslash\mathcal{H}$, as is presented by Bertolini and Darmon in [BD98].

Our objective is to make clear this parallelism between the two theories thanks to the study of the arithmetic in the quaternion algebras H (the indefinite case) and B (the definite case). We will see that the meeting point between the p-adic and the complex uniformizations of the Shimura curve $X(D_H, N)$ is *Eichler's condition*.

Let us briefly recall this important condition. Let Q be a quaternion algebra over a totally real field F, and S be a set of primes of F containing all the Archimedean primes. An order $\mathcal{O} \subseteq Q$ over the ring $R_F[1/S]$ of integers outside S is said to satisfy Eichler's condition when there is a prime $\mathfrak{p}$ in S such that $Q_\mathfrak{p} \simeq \mathrm{M}_2(F_\mathfrak{p})$. In particular, since the algebra H is indefinite, we see that the $\mathbb{Z}$-order $\mathcal{O}_H \subseteq H$ satisfies Eichler's condition while, since B is definite, the $\mathbb{Z}$-order $\mathcal{O}_B \subseteq B$ does not, but its localized $\mathcal{O}_B \otimes_\mathbb{Z} \mathbb{Z}[1/p]$ does. When this condition is fulfilled, important arithmetical results on the order $\mathcal{O}$ in Q were proved by Eichler, most of which can be obtained as a

consequence of the celebrated *Strong approximation theorem*.

The structure of this dissertation is as follows.

In Chapter 1 we introduce Shimura curves starting from an indefinite quaternion algebra H over a totally real field F. This is done mostly following the fundamental paper of Shimura [Shi67]. We also give the definitions using the adelic approach of [Shi70b] and [Shi70c]. The point of view we adopt is the arithmetical one, since we try to make clear the link connecting Shimura curves to the arithmetic of quaternion algebras. In this sense, we give evidence of why Shimura curves have to be considered a geometric interpretation of most arithmetical phenomena in quaternion orders.

In Section 1.1 we propose an overview of the arithmetic in quaternion orders. First we recall fundamental results holding for Eichler orders satisfying Eichler's condition, such as Eichler's *Normensatz* and *Strong approximation theorem*, and recalling the groupoid structure of the set of ideal classes of the algebra of a given level.

Moreover the arithmetic of quaternion orders is also studied from another point of view, namely in those cases where Eichler's condition is not fulfilled, which is the case for example of $\mathbb{Z}$-orders in definite quaternion algebras. In this context we are able to prove a *Zerlegungssatz*, i.e. a factorization result (cf. Theorem 1.1.27), for orders with ideal class number equal to 1, extending one proved by Hurwitz in [Hur96]. In particular maximal quaternion orders in the definite quaternion algebras of discriminant 2 and 3 are considered, because this will allow us to obtain, later in Chapter 3, results on the reduction graph at p of the Shimura curves $X(2p, 1)$ and $X(3p, 1)$.

With all these elements in Section 1.2 we can introduce the system of canonical models of Shimura curves, as Shimura himself does in [Shi67] which is governed by the Shimura reciprocity law, i.e. the action of the groupoid of ideal classes on complex multiplication points, as explained in Theorem 1.2.18. This can be done thanks to the noncommutative commutative dictionary established in Theorem 1.2.15 where the class numbers of the quaternion algebra H over F are related to the class numbers of the number field F, and which makes it possible to translate the arithmetic of the groupoid into the action of certain Galois groups, thanks to the Artin reciprocity law.

Finally in Section 1.3 we introduce the modular interpretation for the Shimura curve $X(D_H, N)$, in terms of certain polarized abelian surfaces with quaternionic multiplication, also known in the literature under the name of fake elliptic curves.Throughout the section we give evidence of the reason for this nomenclature, insisting on those properties these surfaces share with elliptic curves. In particular, we study a decomposition of these surfaces as

a product of elliptic curves, due to Shioda and Mitani (cf. [SM74]), and we design an algorithm in order to compute it.

Chapter 2 has the aim of introducing those non-Archimedean objects which appear later in the statements of the theorems of Cerednik and Drinfeld.

Specifically, in Section 2.2 we introduce the p-adic upper half-plane $\mathcal{H}_p$ as a rigid analytic variety over $\mathbb{Q}_p$. In Theorems 2.2.19 and 2.2.20 we obtain the inequalities characterizing the points of $\mathcal{H}_p$ and the equations defining $\mathcal{H}_p$ locally as a rigid analytic variety respectively. Successively, we introduce on one side the Bruhat-Tits tree $\mathcal{T}_p$ associated to $\mathrm{PGL}_2(\mathbb{Q}_p)$ and on the other side the reduction map $\mathrm{Red} : \mathcal{H}_p \to \mathcal{T}_p$ which allows us to identify the tree $\mathcal{T}_p$ with the reduction mod p of the rigid analytic variety $\mathcal{H}_p$.

We conclude the chapter with a brief presentation, in Section 2.3, of the theory of Mumford uniformization of curves. To do so, we first study the classification transformations of $\mathrm{PGL}_2(\mathbb{Q}_p)$, which are the analytic transformations of the p-adic upper half-plane. We can then define p-adic Schottky groups and Mumford curves, paying particular attention to cocompact Schottky groups, since these are the ones involved in the uniformization of Shimura curves. As we have noted, Mumford associates to every p-adic Schottky group $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ a certain p-adic "half-plane" $\mathcal{H}_\Gamma$. In Theorem 2.3.21 we prove that the half-plane corresponding to a cocompact Schottky group Γ is independent of the group Γ and it is, in fact, the p-adic upper half-plane introduced in the previous section.

In Chapter 3 we start the study of fundamental domains in $\mathcal{H}_p$ for the action of discrete and cocompact subgroups of $\mathrm{PGL}_2(\mathbb{Q}_p)$ arising in the p-adic uniformization of Shimura curves.

For this reason, in Section 3.1 we start by enunciating different versions of the results regarding the p-adic uniformization of Shimura curves, with particular attention to Cerednik's original result (cf. Theorem 3.1.3) and to the "evolution" of this result into a more precise statement with the theorem of Drinfeld (cf. Theorem 3.1.14). Moreover, as a bridge between these statements we propose the adelic version (cf. Theorem 3.1.12), which highlights the *naturalness* of these results and the *dualism* with the Archimedean uniformization.

Once the Cerednik-Drinfeld theorem has been presented, we can start to make effective, in Sections 3.2 and 3.3, some aspects of this theory.

In [FM14], the authors carry out an algorithm computing fundamental domains in the Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_p)$ for the action of groups of type $\Gamma_{p,+}(D_B, N)$ introduced previously. Consequently, they also

compute the reduction graphs of the corresponding Shimura curves.

In [GvDP80] fundamental domains are computed for the action of certain Schottky groups arising from definite quaternion algebras, with-out mentioning the p-adic uniformization of the Shimura curve. We will employ this method for computing p-adic fundamental domains for Shimura curves. We will base the main idea on a lemma of Selberg (cf. Theorem 2.3.23), extended to the Archimedean context, for which every discrete and finitely generated groups of transformations $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ admits a normal and finite index subgroup which is a Schottky group. Fundamental domains associated to p-adic Schottky groups are easier to compute, thanks to an adaptation to the non-Archimedean case of Ford's method of isometric circles, obtained by Gerritzen in [Ger74].

Together with Laia Amorós we have applied this method to the case of definite quaternion algebras of discriminant $D_B = 2$ and 3, obtaining fundamental domains for certain Mumford curves covering p-adic fundamental domains for the Shimura curves of discriminant $D_H = 2p$ and $D_H = 3p$, with $p \equiv 1 \pmod 4$. These are the results presented in Theorems 3.2.11 and 3.2.13.

Thanks to the study of the arithmetic in a maximal order of the definite quaternion algebra, we are able to find a Schottky group and to compute a free system of generators for it. The method employed allows us to treat the cases $D_H = 2p, 3p$ and level $N = 1$. Nevertheless, we propose an axiomatization of the properties which are sufficient for the Eichler order $\mathcal{O}_B$ to be satisfied, in order to apply this method successfully. Thanks to this vision, we can appreciate that the fundamental step in the realizations of the proposed method is to obtaining a *Zerlegungssatz*, i.e. a factorization result, for the order $\mathcal{O}_B$. Actually, in Theorem 1.1.27 we prove that, when the ideal class number of the Eichler order $\mathcal{O}_B$ is $h(D_B, N) = 1$, then a unique factorization in prime and primitive quaternions is possible, once a certain set of residue classes (to which we refer by *primary classes*, adopting an old nomenclature used Hurwitz) has been determined.

In [Kur79] reduction graphs for Shimura curves $X(D_H, 1)$ are obtained, combining different results about the arithmetic in the quaternion order $\mathcal{O}_B$. In our case, in Theorems 3.3.8 and 3.3.10, we also describe the reduction graphs of the Shimura curves stated, obtaining them directly from the previous results about Mumford curves covering these Shimura curves.

In Chapter 4 we associate to the p-adic uniformization of the Shimura curve $X(D_H, N)$ certain parameters in $\mathcal{H}_p(\mathbb{C}_p)$ analogous to the complex multiplication parameters in $\mathcal{H}$: we refer to them by *p-imaginary multiplica-*

tion paramters, since they are defined over the unramified quadratic extension of $\mathbb{Q}_p$.In the study of these parameters, we follow the p-adic analog of the line adopted in [AB04]. Specifically, we are able to recover these parameters as zeros of certain binary quadratic forms with p-adic coefficients. Finally, in Theorem 4.2.9, we relate the number of $\Gamma_{p,+}(D_B, N)$-classes in $\mathcal{H}_p(\mathbb{C}_p)$ of p-imaginary multiplication parameters with the number of $\Gamma(D_H, N)$-classes in $\mathcal{H}$ of complex multiplication parameters, proving that these two cardinals coincide and giving additional evidence of the Cerednik-Drinfeld theory on the interchanging of the primes p and ∞.

Acknowledgements

At this point I wish to make some acknowledgements strictly related with my thesis. As you can appreciate, I have chosen, in each case, the language in which I'm more comfortable with.

El primer agradecimiento va sin duda a Pilar Bayer, por haberme dado la oportunidad de realizar este doctorado en Teoría de Números: ha sido un pequeño sueño hecho realidad, en el que su apoyo y guía han sido condiciones necesarias.

Sin embargo, no solamente he aprendido sobre teoría de números y curvas de Shimura, sino que he tenido el honor de conocer una persona extraordinaria y he podido enriquecerme de muchas ideas que van más allá de las matemáticas. Quiero agradecerle todo esto. Gràcies!

Por otro lado, tengo la suerte de tener a mi alrededor muchas personas que me hacen la vida feliz, pero darle las gracias en este contexto iría mucho más allá del objetivo de este trabajo de tesis. Sin embargo sí hay unas personas a las que me gustaría reconocer públicamente mis agradeciminientos, porque de alguna manera han estado relacionadas conmigo gracias a esta tesis. En orden alfabético quiero darle las gracias a: Laia Amorós, Iván Blanco, Nuno Freitas, Iago Giné, Elisa Lorenzo, Giulio Meleleo, Marta Narváez, Joan Nualart, Dionís Remón, Klara Stokes, Carlos de Vera, por haber sido, en una manera u otra, compañeros de tesis, y haber compartido conmigo muchas risas y matemáticas.

Un gracias especial va al Seminari de Teoria de Nombres de Barcelona UB-UPC-UAB, esta gran familia de la teoría de números que, a pesar de la crisis que ha vivido estos últimos años la Universidad Española, se va alargando a medida que que pasa el tiempo, gracias a la ilusión de muchos de sus miembros y a las ganas de aprender y de enseñar Matemáticas y Teoría de Números. En particular me gustaría agradecer a Xavier Xarles, porque conversaciones esporádicas mantenidas con él me han ayudado a construir una intuición necesaria y muchas veces esclarecedora. A Montse Alsina, por haberme dado siempre consejos buenos y útiles. Y a todos los demás miembros del grupo que trabajan cada día al servicio de la docencia y de la investigación científica.

Je tiens a remercier particulièrement Pierre Parent pour m'avoir accueillis, pendent trois mois, au sein de l'Equipe de Théorie des Nombre de Bordeaux: grâce a sa disponibilité j'ai eu l'opportunité de connaître un groupe de recherche riche en histoire.

Contents

Chapter 1

Arithmetic of Shimura curves

1.1 Arithmetic of quaternion orders

In this section we will give a brief introduction to quaternion algebras over number fields and their orders. The main aim is to explain why the study of arithmetic in quaternion orders should be considered the natural continuation of the study of arithmetic in number fields and their orders.

A reference for understanding the main trends of arithmetic in quaternion algebras is M. F. Vigneras [Vig80]. Together with that book, the following papers by Eichler should be studied in order to understand how this beautiful theory has come to light: cf. [Eic37], [Eic38a], [Eic38b], and also [Eic55].

1.1.1 Basic definitions and results

Let F be a number field of degree $[F : \mathbb{Q}] = n$ with ring of integers R_F. A **quaternion algebra** Q over F is a simple and central algebra over F of dimension 4. When we say that the algebra Q **admits a presentation** $Q = \left(\frac{a,b}{F}\right)$, with $a, b \in F^*$, we mean that an F-basis for the algebra is a set $\mathcal{B} = \{1, i, j, k\} \subseteq Q$ such that

$$i^2 = a, j^2 = b, k = ij = -ji.$$

As we shall see along as the dissertation progresses, quaternion algebras share many characteristics with number fields, in the sense that they suggest the consideration of the same kind of arithmetic problems. Nevertheless, the main difference between these two scenarios is that, while orders in number fields are commutative rings, orders in quaternion algebras are noncommutative rings.

Every quaternion algebra Q over F is endowed with an involution

$$\begin{array}{ccc} Q = \left(\frac{a,b}{F}\right) & \longrightarrow & Q \\ q = x + yi + zj + tk & \longmapsto & \overline{q} := x - yi - zj - tk \end{array}$$

which is called the **conjugation**. This involution allows us to define the norm and the trace in the context of quaternion algebras, and subsequently the concept of *integral quaternion*.

For every $\alpha \in Q$ we denote by $\mathrm{Nm}_{Q/F}(q)$ the **norm of** q and by $\mathrm{Tr}_{Q/F}(q)$ the **trace of** q, defined by

$$\begin{array}{rccc} \mathrm{Nm}_{Q/F}: & Q & \longrightarrow & F, \\ & q & \longmapsto & q\overline{q}, \end{array} \qquad \begin{array}{rccc} \mathrm{Tr}_{Q/F}: & Q & \longrightarrow & F, \\ & q & \longmapsto & q + \overline{q}. \end{array}$$

A quaternion $q \in Q$ is said to be **pure** if $\mathrm{Tr}_{Q/F}(q) = 0$. In particular if $Q = \left(\frac{a,b}{F}\right)$, then a quaternion $q = x + yi + zj + tk$ is pure if and only if $x = 0$. We usually denote the set of pure quaternions by Q_0.

Moreover we will denote by $\mathrm{N}^{\mathcal{B}}_{Q,4}$ (resp. $\mathrm{N}^{\mathcal{B}}_{Q,3}$) the quaternary (resp. ternary) normic form associated to the basis $\mathcal{B}$ of the quaternion algebra Q. That is, if $Q = \left(\frac{a,b}{F}\right)$ then

(a) $\mathrm{N}^{\mathcal{B}}_{Q,4}(X, Y, Z, T) := X^2 - aY^2 - bZ^2 + abT^2$,

(b) $\mathrm{N}^{\mathcal{B}}_{Q,3}(Y, Z, T) := -aY^2 - bZ^2 + abT^2$.

Note that if we choose another basis $\mathcal{B}'$ for Q then the corresponding normic forms $\mathrm{N}^{\mathcal{B}'}_{Q,4}$ and $\mathrm{N}^{\mathcal{B}'}_{Q,3}$ are linearly equivalent over $\mathbb{Q}$ to the normic forms $\mathrm{N}^{\mathcal{B}}_{Q,4}$ and $\mathrm{N}^{\mathcal{B}}_{Q,3}$; i.e., there exist matrices $A \in \mathrm{GL}_4(\mathbb{Q})$ and $C \in \mathrm{GL}_3(\mathbb{Q})$ such that

$$A^t \mathrm{N}^{\mathcal{B}}_{Q,4} A = \mathrm{N}^{\mathcal{B}'}_{Q,4}, \qquad C^t \mathrm{N}^{\mathcal{B}}_{Q,3} C = \mathrm{N}^{\mathcal{B}'}_{Q,3}.$$

When a presentation $\left(\frac{a,b}{F}\right)$ for the algebra Q is fixed, we simply write $\mathrm{N}_{Q,4}$ and $\mathrm{N}_{Q,3}$ for the corresponding quaternary and ternary normic forms.

When $F = \mathbb{Q}$, a quaternion algebra Q is said to be **indefinite** if its associated normic form $\mathrm{N}_{Q,4}$ is indefinite, and it is said to be **definite** if $\mathrm{N}_{Q,4}$ is definite.

A prime $\mathfrak{p}$ of F is said to be **ramified in** Q if $Q_{\mathfrak{p}} := Q \otimes_F F_{\mathfrak{p}}$ is a (noncommutative) field.

We will sometimes denote by $\mathrm{Ram}(Q)$ the set of (finite and Archimedean) primes ramifying in Q. The product of all finite primes in $\mathrm{Ram}(Q)$ is an ideal of R_F called the **discriminant of the algebra** Q.

A quaternion algebra Q over $\mathbb{Q}$ is indefinite if and only if $Q \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$, i.e. if and only if $\infty \notin \mathrm{Ram}(Q)$, and it is definite if and only if $Q \otimes_{\mathbb{Q}} \mathbb{R}$ is the Hamilton quaternion field, i.e. if and only if $\infty \in \mathrm{Ram}(Q)$.

Before introducing the concept of integral quaternion we need to be more subtile and clarify the concept of *integrality*: for this reason we will introduce different rings of integers inside the number field F.

1.1.1 Definition. Let R_F be the usual ring of integers of F (i.e. its maximal order over $\mathbb{Z}$) and let $S_\infty = \{\mathfrak{p}_{\infty 1}, \dots, \mathfrak{p}_{\infty n}\}$ be the set of Archimedean primes of F. For every finite set S of primes of F such that $S \supseteq S_\infty$, we denote by $R_F[1/S]$ the **ring of integers outside** S, i.e.

$$R_F[1/S] := \left(\bigcap_{\mathfrak{p} \notin S} R_{F,\mathfrak{p}} \right) \cap F.$$

In particular if S contains only the Archimedean primes of F, i.e. $S = S_\infty$, then we have that $R_F[1/S] = R_F$.

If K is a quadratic field extension of F and $\mathcal{O}_K$ is an order in K over R_F, i.e. $\mathcal{O}_K$ is a ring which is a free R_F-module of rank 2 and such that all its elements are integral over R_F, then we will use the notation

$$\mathcal{O}_K[1/S] := \mathcal{O}_K \otimes_{R_F} R_F[1/S]$$

for the corresponding $R_F[1/S]$-order in K. Note that every $R_F[1/S]$-order in K is obtained in this way, starting from an order of K over R_F.

1.1.2 Definition. A quaternion $q \in Q$ is said to be **integral with respect to** $R_F[1/S]$ if the elements $\mathrm{Nm}(q), \mathrm{Tr}(q) \in F$ belong to the ring of integer $R_F[1/S]$.

A **quaternion order over** $R_F[1/S]$ is a ring which is a free $R_F[1/S]$-module $\mathcal{O} \subseteq Q$ of dimension 4 and such that all its elements are integral with respect to $R_F[1/S]$.

A quaternion order $\mathcal{O}$ over $R_F[1/S]$ is called **maximal** if it is maximal among all the $R_F[1/S]$-orders of Q ordered by the inclusion.

A quaternion order $\mathcal{O}$ over $R_F[1/S]$ is called an **Eichler order** if it is the intersection of two maximal orders over $R_F[1/S]$. The level of the Eichler order $\mathcal{O}$ over $R_F[1/S]$ is an integral ideal N of $R_F[1/S]$ which is defined locally (cf. [Vig80, Ch. II, Sec. 2]).

Two orders $\mathcal{O}, \mathcal{O}'$ over $R_F[1/S]$ are said to be **conjugated** if there exists a quaternion $q \in Q^*$ such that $q^{-1}\mathcal{O}q = \mathcal{O}'$. A class of orders with respect to this equivalent relation is called a **type**.

If Q has as a discriminant the integral ideal D of R_F , then the number of types of Eichler orders over $R_F[1/S]$ in Q of level N is denoted by $t(D, N)$.

Let $\mathcal{O}$ be an order in Q over $R_F[1/S]$ and let us fix a $R_F[1/S]$-basis $\mathcal{B}$ of $\mathcal{O}$, as $R_F[1/S]$-free module. We denote by $\mathrm{N}^{\mathcal{B}}_{\mathcal{O},4}$ (resp. $\mathrm{N}^{\mathcal{B}}_{\mathcal{O},3}$) the quaternary (resp. ternary) normic form associated to the order $\mathcal{O}$ with respect to the basis $\mathcal{B}$. Again, when an integral basis for the order $\mathcal{O}$ is fixed, we simply write these quadratic forms as $\mathrm{N}_{\mathcal{O},4}$ and $\mathrm{N}_{\mathcal{O},3}$.For more details and explicit expressions of these quadratic forms, see [AB04, 3.6].

1.1.3 Definition. An **ideal over** $R_F[1/S]$ in the quaternion algebra Q is a $R_F[1/S]$-module $I \subseteq Q$ such that $I \otimes_{R_F[1/S]} F \simeq Q$.

The ideal I is said to have as **associated order on the left** the $R_F[1/S]$-order $\mathcal{O}_\ell$ if

$$\{q \in Q \mid qI \subseteq I\} = \mathcal{O}_\ell$$

and is said to have as **associated order on the right** the $R_F[1/S]$-order $\mathcal{O}_r$ if

$$\{q \in Q \mid Iq \subseteq I\} = \mathcal{O}_r.$$

In this case we also say that I is a **fractional left ideal** (resp. **fractional right ideal**) of the order $\mathcal{O}_\ell$ (resp. $\mathcal{O}_r$) and we denote by $\mathcal{I}_\ell(\mathcal{O})$ (resp. $\mathcal{I}_r(\mathcal{O})$) the set of these ideals.

If in addition $I \subseteq \mathcal{O}_\ell$ (resp. $I \subseteq \mathcal{O}_r$), we say that I is an **integral** left ideal (resp. right ideal) of the order $\mathcal{O}$.

Moreover when I is a fractional (integral) left ideal and right ideal of the same order $\mathcal{O}$ we say that I is a **fractional (integral) bilateral ideal** of $\mathcal{O}$ and we denote by $\mathcal{I}_{bil}(\mathcal{O})$ the set of these ideals, which is a group with respect to the usual product between modules.

In particular, note that any order $\mathcal{O}$ over $R_F[1/S]$ is an integral bilateral ideal over $R_F[1/S]$ of the order $\mathcal{O}$ itself.

Once these definitions are given, it is natural, as in the number field case, to define *ideal class numbers* of quaternion orders. Of course, as is obvious from the previous definitions, we have to distinguish between left and right (and also bilateral) ideals. As we shall see in the next section, where Shimura curves are introduced, these three class numbers associated to a quaternion order are important invariants of the order and encode significant information about some geometric objects naturally associated to them.

1.1.4 Definition. Let I, J be ideals over $R_F[1/S]$ in the quaternion algebra Q.

I, J are **equivalent on the left (resp. on the right)** if there exists a $q \in Q^*$ such that $I = qJ$ (resp. $I = Jq$).

It is immediate to see that if two ideals I, J are equivalent on the left, then they have the same associated order $\mathcal{O}$ on the right and the set of classes of fractional right ideals of $\mathcal{O}$, with respect to this equivalence relation, is called the **set of right ideal classes of the order** $\mathcal{O}$. Analogously, we can define the **set of left ideal classes of the order** $\mathcal{O}$.

In particular the set of classes of bilateral ideals of $\mathcal{O}$ forms a group which is called the **bilateral ideal class group of the order** $\mathcal{O}$.

The set of left ideal classes and that of right ideal classes are in bijection through the map

$$\begin{array}{ccc} \mathcal{I}_\ell(\mathcal{O})/Q^* & \longrightarrow & Q^*\backslash\mathcal{I}_r(\mathcal{O}) \\ I & \longmapsto & I^{-1} \end{array}$$

and the associated cardinality is called the **ideal class number of the order** $\mathcal{O}$ and is denoted by $h(Q, \mathcal{O})$. Moreover this class number does not depend on the type of the order $\mathcal{O}$.

The cardinality of the bilateral ideal class group of the order $\mathcal{O}$ is called the **bilateral ideal class number** and is denoted by $h_{bil}(Q, \mathcal{O})$. This number depends, in general, on the conjugacy class of the order $\mathcal{O}$.

Later in Section 1.2 we will introduce these ideal class numbers making use of adelic language and we will prove statements relating them with their analogous ideal class number in the number fields case: these relations will be referred to as the *noncommutative commutative dictionary*.

1.1.5 Remark. Before doing this, it is important to remark that, depending on the base ring $R_F[1/S]$ with respect to which the integrality is considered, the computation of such class numbers may be completely different and may need the use of different techniques.

For this reason it is of vital importance to introduce a condition which was first considered by Eichler (cf. for example *Voraussetzung* $\mathfrak{R}$ in [Eic38a]) and which, in [Vig80, Ch. III], is named Eichler's condition, between the ring of integers $R_F[1/S]$ and the algebra Q. With the notations introduced so far, we state the condition.

1.1.6 Definition. (Eichler's condition) Let S be a set of primes of F containing the Archimedean primes, i.e. $S \supseteq S_\infty$. Let Q be a quaternion algebra over F and let $\mathcal{O}$ be an $R_F[1/S]$-order in Q.

1. We say that **the set S satisfies Eichler's condition for the algebra** Q if $S \not\subseteq \mathrm{Ram}(Q)$.

2. We say that **the $R_F[1/S]$-order $\mathcal{O}$ satisfies Eichler's condition** if the set of primes S satisfies Eichler's condition for the algebra Q.

Given a quaternion algebra Q over F, associated to it is an algebraic group Q^* defined by $Q^*(A) := (Q \otimes_F A)^*$, for every F-algebra A. In particular $Q^*(F)$ is the group of points Q^* and $Q^*(F_\mathfrak{p})$ is the group of units of the local algebra $Q_\mathfrak{p} := Q \otimes_F F_\mathfrak{p}$.

1.1.7 Definition. Let S be a finite set of primes of F, $S \supseteq S_\infty$, and let $\mathcal{O}[1/S]$ be an $R_F[1/S]$-order in Q. We define the **adelization** of the algebraic group Q^* as the restricted product

$$Q^*_\mathbb{A} := \prod_{\mathfrak{p}\notin S} (Q^*_\mathfrak{p} : \mathcal{O}[1/S]^*_\mathfrak{p}) \times \prod_{\mathfrak{q}\in S} Q^*_\mathfrak{q}.$$

As is well known, this group is canonically isomorphic to the set of adelic points of the algebraic group Q^*, i.e. $Q^*_\mathbb{A} \simeq Q^*(\mathbb{A}_F)$, where $\mathbb{A}_F$ denotes the F-algebra of the *adèles* of F. This definition does not depend on the set of primes S.

The following theorems are fundamental in the arithmetic study of quaternion algebras: these are the *Theorem of Norms* and the *Strong Approximation Theorem*. The first one answers the simply arithmetic question of whether elements of F are norms of some quaternions and was proved by Eichler (cf. [Eic38b, Satz 3]). The second one is a generalization to quaternion algebras of a result first known in number fields (cf. for example [Neu99, Ch. III, Exercise 1]); it was later generalized to the algebraic group of quaternions of norm 1 by M. Kneser (cf. [Kne62] and [Kne65]).

1.1.8 Theorem. (Normensatz) *Let Q be a quaternion algebra over F and let $\sigma_1, \ldots, \sigma_r$ denote the immersions $F \hookrightarrow \mathbb{R}$ associated to the real Archimedean primes $\mathfrak{p}_{\infty 1}, \ldots, \mathfrak{p}_{\infty r}$ of F ramified in Q, i.e.*

$$\{\mathfrak{p}_{\infty 1}, \ldots, \mathfrak{p}_{\infty r}\} = S_{\infty, real} \cap \mathrm{Ram}(Q).$$

Then $x \in F$ is equal to $\mathrm{Nm}_{Q/F}(\alpha)$, for some $\alpha \in Q$, if and only if $\sigma_i(x) > 0$ for $1 \leq i \leq r$.

As a consequence of this theorem we find that if $Q = H$ is an indefinite quaternion $\mathbb{Q}$-algebra, then all elements in $\mathbb{Q}$ are norm, i.e. the map

$$\mathrm{Nm}_{H/F} : H \longrightarrow \mathbb{Q}$$

is surjective, and if $Q = B$ is a definite quaternion $\mathbb{Q}$-algebra, then all positive elements in $\mathbb{Q}$ are norm, i.e. the map

$$\mathrm{Nm}_{B/F} : B \longrightarrow \mathbb{Q}_{\geq 0}$$

is surjective.

1.1.9 Theorem. (Strong Approximation Theorem) *Let Q be a quaternion algebra over F and let Q_1^* denote the algebraic subgroup of Q^* of "quaternions of norm 1", i.e. for every F-algebra A*

$$Q_1^*(A) := \{\alpha \in Q^*(A) \mid \mathrm{Nm}(\alpha) = 1\}.$$

Let S be a finite set of primes of F, $S \supseteq S_\infty$, satisfying Eichler's condition, and let $\mathcal{O}[1/S]$ be an $R_F[1/S]$-order in Q. Then

$$Q_1^*(F) \prod_{\mathfrak{q} \in S} Q_1^*(F_\mathfrak{q})$$

is a dense subgroup of $Q_1^*(\mathbb{A}_F)$.

Observe that Eichler's condition in Definition 1.1.6 is equivalent to requiring in the above statement that there is a prime $\mathfrak{q} \in S$ such that the group $Q_1^*(F_\mathfrak{q}) \simeq \mathrm{SL}_2(F_\mathfrak{q})$ is not compact and such that the product $\prod_{\mathfrak{q} \in S} Q_1^*(F_\mathfrak{q})$ is not compact.

1.1.10 Definition. If $t = t(D, N)$ denotes the number of types of Eichler orders of level N in Q, let $\{\mathcal{O}_1, \ldots, \mathcal{O}_t\}$ be a system of representatives for these types.

For every $1 \leq \lambda \leq t$, let $\{I_{\lambda\mu}\}$ be the set of fractional left ideals of the orders $\mathcal{O}_\lambda$ such that $I_{\lambda\mu}$ has $\mathcal{O}_\mu$ as associated order on the right.

In [Eic55, Satz 4] and [Eic38b, Satz 2] Eichler proved that the set of left ideal classes $\{I_{\lambda\mu} \mid 1 \leq \lambda \leq t\}/Q^*$, with respect to the product of ideals (when this exists) is a finite groupoid such that the *rank* of the groupoid, which is by definition the number of neutral elements of the groupoid, is equal to $t(D, N)$.

This is called the **groupoid of ideal classes and types of Eichler orders of level N in Q** and is denoted by $\mathcal{G}(D, N)$.

In particular, when the orders $\mathcal{O}_i$ satisfy Eichler's condition in Definition 1.1.6, we have the following formula (cf. [Vig80, Lemme 5.6 and Corollaire 5.7, Ch. III] and [Eic38b]).

1.1.11 Theorem. *Let Q be a quaternion algebra over F of discriminant D and let $\mathcal{O}$ be an Eichler order over $R_F[1/S]$ of level N, satisfying Eichler's condition. Then the cardinal $h_{bil}(Q,\mathcal{O})$ does not depend on the type of the order $\mathcal{O}$, so it is denoted by $h_{bil}(D,N)$ and the following formula holds*

$$h(D,N) = h_{bil}(D,N)t(D,N).$$

The cardinal $h_{bil}(D,N)$ is called the *order* of the groupoid and equals the cardinality of each of the groups arising in the groupoid, namely the groups of bilateral ideal classes of the orders $\mathcal{O}_i$ for $1 \leq i \leq t(D,N)$.

1.1.12 Remark. When the orders $\mathcal{O}_i$ do not satisfy Eichler's condition, we find the following general formula (cf. [Eic55]):

$$h(D,N) = \sum_{i=1}^{t} h_{bil}(Q,\mathcal{O}_i),$$

where $h_{bil}(Q,\mathcal{O}_i)$ denotes the cardinal of the bilateral ideal class group of the order $\mathcal{O}_i$, which in this case depends on the order $\mathcal{O}_i$.

1.1.13 Remark. Note that the **order of a groupoid** $\mathcal{G}$ does not coincide with its cardinality as a set. In fact, if $ord(\mathcal{G})$ and $rank(\mathcal{G})$ denote respectively the order and the rank of a groupoid $\mathcal{G}$, then the cardinality of $\mathcal{G}$ is

$$\#\mathcal{G} = ord(\mathcal{G})rank(\mathcal{G})^2.$$

In particular, the cardinality of the groupoid $\mathcal{G}(D,N)$, satisfying Eichler's condition, is

$$\#\mathcal{G}(D,N) = h_{bil}(D,N)t(D,N)^2 = h(D,N)t(D,N).$$

1.1.2 Factorization in quaternion orders

Let Q be a quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O}$ be an Eichler order. In this section we want to study the important problem of factorization of elements of the order $\mathcal{O}$. This problem was considered for the first time in 1989 by Adolf Hurwitz. In one of his celebrated papers, [Hur96], Hurwitz considered the problem of factorization in a maximal order inside the definite quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ of rational Hamilton quaternions.

The problem of factorization in quaternion orders is actually a problem due to the fact that these orders are not commutative. For example if a

quaternion admits as a factorization $\alpha = \pi_1 \cdot \pi_2$, we can construct a different factorization of the same quaternion, namely $\alpha = \pi_1\varepsilon_1 \cdot \varepsilon_1^{-1}\pi_2$, since here we do not have the possibility of switching the units in order to place them together at the beginning of the factorization, as as we do in the case of commutative orders in number fields.

Nevertheless, in some cases this ambiguity can be avoided by introducing the concept of primary quaternion (*primäre Quaternion* in [Hur96]). We will give this definition and then present some examples where we can find some sort of uniqueness of factorizations, following the ideas of Hurwitz.

Let S be a finite set of primes of $\mathbb{Q}$, containing the Archimedean prime $\mathfrak{p}_{\infty 1} = \infty$. Let $\mathcal{O}$ be an Eichler order over $\mathbb{Z}[1/S]$ and $\{\eta_0, \eta_1, \eta_2, \eta_3\}$ be an integral basis for $\mathcal{O}$.

An integral quaternion $\alpha = a_0\eta_0 + a_1\eta_1 + a_2\eta_2 + a_3\eta_3 \in \mathcal{O}$ is said to be **primitive** if the ideal generated in $\mathbb{Z}[1/S]$ by its integral coefficients is $(a_0, a_1, a_2, a_3) = \mathbb{Z}[1/S]$.

1.1.14 Definition. Let $\mathcal{O}$ be an Eichler order over $\mathbb{Z}[1/S]$. Then $\mathcal{O}$ is said to be **euclidean on the right (resp. on the left)** if for every $\alpha, \beta \in \mathcal{O}, \beta \neq 0$, there exist $\gamma, \delta \in \mathcal{O}$ such that

$$\alpha = \beta\gamma + \delta \qquad (\text{resp. } \alpha = \gamma\beta + \delta)$$

with $\delta = 0$ or $\delta \neq 0$ and $\mathrm{Nm}(\delta) < \mathrm{Nm}(\beta)$.

The following result was proved by Eichler in [Eic38a, Satz 3] as an application of the Normensatz.

1.1.15 Proposition. (cf. [Vig80], Ch. III, Théorème 5.10) *Let Q be a quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O}$ be a maximal order over $\mathbb{Z}[1/S]$. If $\mathcal{O}$ satisfies Eichler's condition (cf. Definition 1.1.6) and the ring $\mathbb{Z}[1/S]$ is euclidean, then $\mathcal{O}$ is euclidean on the right and on the left.*

1.1.16 Lemma. *The order $\mathcal{O}$ is euclidean on the right with respect to the norm if and only for every $\alpha, \beta \in \mathcal{O}, \beta \neq 0$ there exists an element $\gamma \in \mathcal{O}$ such that $\mathrm{Nm}(\beta^{-1}\alpha - \gamma) < 1$.*

Proof. Let us prove that $\mathcal{O}$ is euclidean on the right. Let us take $\alpha, \beta \in \mathcal{O}$. By the hypothesis, there exists a $\gamma \in \mathcal{O}$ such that $\mathrm{Nm}(\beta^{-1}\alpha - \gamma) < 1$. Hence if we put $\delta := \beta(\beta^{-1}\alpha - \gamma)$ then $\alpha = \beta\gamma + \delta$ with $\mathrm{Nm}(\delta) < \mathrm{Nm}(\beta)$. The viceversa is now obvious. □

The analogous statement "on the left" holds.

1.1.17 Corollary. *Non-maximal orders are never euclidean.*

PROOF. If $\mathcal{O}'$ is a non-maximal order contained (properly) in a maximal order $\mathcal{O}$, then there exists $x \in \mathcal{O} \smallsetminus \mathcal{O}'$. Moreover $x = \beta^{-1}\alpha \in \mathcal{O}$ for some $\alpha, \beta \in \mathcal{O}'$. Therefore for every $\gamma \in \mathcal{O}$, the element $x - \gamma = \beta^{-1}\alpha - \gamma$ is integral and so $\mathrm{Nm}(\beta^{-1}\alpha - \gamma) \geq 1$. Hence the order $\mathcal{O}'$ is not euclidean, after Lemma 1.1.16. □

1.1.18 Proposition. *If the order $\mathcal{O}$ is euclidean on the left (resp. on the right), then every fractional left ideal (resp. right ideal) I of $\mathcal{O}$ is principal.*

PROOF. The proof of this proposition is the same as in the commutative context, i.e. in number fields. Namely, if I is a fraction left ideal (resp. right ideal) of the order $\mathcal{O}$, then take α to be an element of I such that $|\mathrm{Nm}(\alpha)| \in \mathbb{Z}_{\geq 0}$ is the minimum of the set $\{|\mathrm{Nm}(\beta)| : \beta \in I\}$. Therefore, since $\mathcal{O}$ is euclidean on the left (resp. on the right) it is immediate to see that $I = \mathcal{O}\alpha$ (resp. $I = \alpha\mathcal{O}$). □

1.1.19 Corollary. *If the order $\mathcal{O}$ is euclidean on the right and on the left, then every fractional bilateral ideal I of the order $\mathcal{O}$ is principal, i.e. there exist $\alpha, \beta \in Q^*$ such that $I = \alpha\mathcal{O} = \mathcal{O}\beta$. Moreover, in this case, $\alpha = \beta$.*

PROOF. After the proof of Proposition 1.1.18, we know that for every ideal I which is a left ideal and a right ideal, there exists an element α such that $I = \alpha\mathcal{O} = \mathcal{O}\alpha$. □

1.1.20 Remark. Note that in general when $\mathcal{O}$ is an Eichler order of level N, satisfying Eichler's condition, in which every left ideal is principal, then the ideal class number is $h(D, N) = 1$. After Theorem 1.1.11, we also have $t(D, N) = 1$ and $h_{bil}(D, N) = 1$, which means that every bilateral ideal $\mathcal{I}$ of $\mathcal{O}$ is principal.

1.1.21 Lemma. *Let be $\alpha, \beta \in Q$. Then*

(*a*) *$\alpha\mathcal{O} \subseteq \beta\mathcal{O}$ if and only if $\alpha = \beta\gamma$ for some $\gamma \in \mathcal{O}$.*

*In this case we say that β **divides** α **on the left** and we write $\beta|\alpha$ when there is no ambiguity.*

(*b*) *$\alpha\mathcal{O} = \beta\mathcal{O}$ if and only if $\alpha = \beta\varepsilon$, for some $\varepsilon \in \mathcal{O}^*$.*

PROOF. If $\alpha\mathcal{O} \subseteq \beta\mathcal{O}$ then $\alpha \cdot 1 \in \beta\mathcal{O}$. Viceversa, if $\alpha = \beta\gamma$, for some $\gamma \in \mathcal{O}$, then $\alpha \in \beta\mathcal{O}$ and since $\beta\mathcal{O}$ is a fractional right ideal of $\mathcal{O}$, then $\alpha\mathcal{O} \subseteq \beta\mathcal{O}$.

If $\alpha = \beta\varepsilon_1$ and $\beta = \alpha\varepsilon_2$, for some $\varepsilon_1, \varepsilon_2 \in \mathcal{O}$, then $\alpha = \alpha\varepsilon_1\varepsilon_2$ and $\varepsilon_1\varepsilon_2 = 1$ so $\varepsilon_1^{-1} = \varepsilon_2 \in \mathcal{O}$ and $\varepsilon_1, \varepsilon_2 \in \mathcal{O}^*$. □

1.1.22 Definition. A quaternion $\pi \in \mathcal{O} \setminus \mathcal{O}^*$ is said to be **irreducible** if π cannot be written as a product of quaternions $\alpha, \beta \in \mathcal{O}$ both different from a unit and from α.

The next characterization of irreducible quaternions is proved in [Hur96] for *Hurwitz quaternions*. Here we give the proof for quaternions belonging to an arbitrary euclidean order.

1.1.23 Proposition. *Let $\mathcal{O}$ be a quaternion order in which every right ideal is principal. A primitive quaternion $\alpha \in \mathcal{O}$ is irreducible if and only if its norm $\mathrm{Nm}(\alpha) = p$ is a prime integer.*

PROOF. If $\mathrm{Nm}(\pi)$ is prime then it is obvious that π has to be irreducible.

Let us assume the $\pi \in \mathcal{O}$ is irreducible and that $p|\mathrm{Nm}(\pi)$ is a prime factor of the norm. We are going to show that, when π is primitive, we have strict inclusions

$$p\mathcal{O} \subsetneq p\mathcal{O} + \pi\mathcal{O} \subsetneq \mathcal{O}.$$

If the first inclusion was an equality, then $p|\pi$ and since π is irreducible, $p \in \mathcal{O}^*$ or $\pi = p$. Both options are absurd since p is a prime (of norm $\mathrm{Nm}(p) = p^2$) and π is assumed to be primitive.

If the second inclusion was an equality then it is a simple computation to see that $p|\mathrm{Nm}(x)$, for every $x \in p\mathcal{O} + \pi\mathcal{O} = \mathcal{O}$, an absurd.

By Proposition 1.1.18, $p\mathcal{O} + \pi\mathcal{O} = \alpha\mathcal{O}$, for some $\alpha \in \mathcal{O} \setminus \mathcal{O}^*$ and then $\pi = \alpha\beta$, for some $\beta \in \mathcal{O}$. Moreover $\beta \in \mathcal{O}^*$ since π is irreducible.

Hence $p \in p\mathcal{O} + \pi\mathcal{O} = \alpha\mathcal{O} = \pi\mathcal{O}$, i.e. $\pi|p$, and $\mathrm{Nm}(\pi)|\mathrm{Nm}(p) = p^2$. Since π is irreducible its norm cannot be $\mathrm{Nm}(\pi) = 1$ and since π is primitive it cannot be $\mathrm{Nm}(\pi) = p^2$, neither. Actually $\mathrm{Nm}(\pi) = p^2$ implies $p = \pi\varepsilon$ for a unit $\varepsilon \in \mathcal{O}^*$ and so $\pi = p\varepsilon^{-1}$. Finally the only possible option is $\mathrm{Nm}(\pi) = p$. □

Note that the same holds for quaternion orders in which every left ideal is principal.

1.1.24 Definition. Given integral quaternions $\alpha, \beta, \gamma \in \mathcal{O}$, we say that α **is congruent to** β **modulo** γ and we write

$$\alpha \equiv \beta \pmod{\gamma}$$

if $\alpha - \beta \in \gamma\mathcal{O}$.

Moreover the quotient set $\mathcal{O}/\gamma\mathcal{O}$ is called the **set of quaternion classes modulo** γ.

1.1.25 Proposition. *Let $\mathcal{O}$ be a quaternion order over $\mathbb{Z}^{(S)} := \mathbb{Z}[1/S]$ and let $M \in \mathbb{Z}[1/S]$ be an integer. Then the quotient set $\mathcal{O}/M\mathcal{O}$ is a ring. The set of invertible elements of $\mathcal{O}/M\mathcal{O}$ is formed by all those quaternion classes represented by quaternions $\alpha \in \mathcal{O}$ such that $\mathrm{Nm}(\alpha) \in (\mathbb{Z}^{(S)}/M\mathbb{Z}^{(S)})^*$, i.e.*

$$(\mathcal{O}/M\mathcal{O})^* = \{[\alpha] \in \mathcal{O}/M\mathcal{O} \mid (\mathrm{Nm}(\alpha), M) = \mathbb{Z}[1/S]\}.$$

Proof. Since $M\mathcal{O}$ is a bilateral ideal of $\mathcal{O}$ the quotient set $\mathcal{O}/M\mathcal{O}$ is a ring. Given a quaternion class $[\alpha] \in \mathcal{O}/M\mathcal{O}$ such that $\mathrm{Nm}(\alpha)$ is invertible in the ring $\mathbb{Z}^{(S)}/M\mathbb{Z}^{(S)}$, then $[\beta] := [\overline{\alpha}/\mathrm{Nm}(\alpha)] \in \mathcal{O}/M\mathcal{O}$ such that $[\alpha] \cdot [\beta] = [1]$. The viceversa is clear. □

1.1.26 Definition. Let $\xi \in \mathcal{O}$ be an integral quaternion. We call a subset of quaternion classes $\mathcal{P} \subseteq \mathcal{O}/\xi\mathcal{O}$ a **primary class set mod** ξ if for every quaternion $\alpha \in \mathcal{O}$ there exists a class $[\alpha'] \in \mathcal{P}$ and unique units $\varepsilon_1, \varepsilon_2 \in \mathcal{O}^*$ such that $\varepsilon_1\alpha \in [\alpha']$ and $\alpha\varepsilon_2 \in [\alpha']$.

A quaternion α' belonging to some quaternion class in a primary class set mod ξ is said to be a **ξ-primary quaternion**.

As we have already noted, primary quaternions are very important when we are looking for unique factorization in certain quaternion orders. It is an interesting open problem to find primary representative sets in a given quaternion order.

In [Hur96] a primary representative set is computed when $\mathcal{O}$ is a maximal order in the definite quaternion algebra of discriminant 2. In this case Hurwitz proves a *Zerlegungssatz* for elements in this order. Here we give a statement, in a more general case, based on Hurwitz's statement and we generalize the proof to arbitrary quaternion orders in which all the left and right ideals are principal.

1.1.27 Theorem. (Zerlegungssatz) *Let Q be a quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O}$ be an order over $\mathbb{Z}$ such that $h(Q, \mathcal{O}) = 1$. Let $\xi \in \mathcal{O}$ be an integral quaternion such that $\mathcal{O}/\xi\mathcal{O}$ contains a primary representative set.*

If $\alpha \in \mathcal{O}$ is a primitive and ξ-primary quaternion such that its norm has decomposition in prime power factors

$$\mathrm{Nm}(\alpha) = p_1 \cdot \ldots \cdot p_s,$$

then α admits a decomposition in primitive ξ-primary and irreducible quaternions

$$\alpha = \pi_1 \cdot \ldots \cdot \pi_s$$

such that $\pi_i \in \mathcal{O}$, $\mathrm{Nm}(\pi_i) = p_i$ for every $1 \leq i \leq s$.

PROOF. Let us consider the integral right ideal $p_1\mathcal{O} + \alpha\mathcal{O}$ of $\mathcal{O}$, which is principal by Proposition 1.1.18, i.e.

$$p_1\mathcal{O} + \alpha\mathcal{O} = \pi_1\mathcal{O},$$

for some $\pi_1 \in \mathcal{O}$.

Since $\pi_1 | p_1$, then $\mathrm{Nm}(\pi_1) | \mathrm{Nm}(p_1) = p_1^2$. We exclude the possibilities $\mathrm{Nm}(\pi_1) = 1$ and $\mathrm{Nm}(\pi_1) = p_1^2$.

If $\mathrm{Nm}(\pi_1) = 1$, then $p_1\mathcal{O} + \alpha\mathcal{O} = \mathcal{O}$. Now it is immediate to see by direct computation that every element $x \in p_1\mathcal{O} + \alpha\mathcal{O}$ has a norm such that $p_1 | \mathrm{Nm}(x)$, which is an absurd.

If $\mathrm{Nm}(\pi_1) = p_1^2$, then, since $\pi_1 | p_1$, we find that $\pi_1 = p_1\varepsilon$ for some unit $\varepsilon \in \mathcal{O}^*$. Therefore, $p_1\mathcal{O} + \alpha\mathcal{O} = p_1\mathcal{O}$ and $p_1 | \alpha$, which is an absurd since we are assuming that α is primitive.

Finally we have proved that $\mathrm{Nm}(\pi_1) = p_1$. By Proposition 1.1.23 the primitive integral quaternion π_1 is irreducible and it is clear that $\alpha = \pi_1\alpha_1$, for some $\alpha_1 \in \mathcal{O}$. Moreover, as has been found, π is unique up to multiplication by a unit on the right.

Now we can apply the same reason to the quaternion $\pi^{-1}\alpha = \alpha_1 \in \mathcal{O}$ of norms $\mathrm{Nm}(\alpha_1) = p_2 \ldots p_s$. Iterating the process we find primitive and irreducible quaternions $\pi_1, \ldots, \pi_s \in \mathcal{O}$ of norms $\mathrm{Nm}(\pi_i) = p_i$, such that $\alpha = \pi_1\pi_2 \ldots \pi_s$ and these prime quaternions are uniquely determined up to right multiplication by units of $\mathcal{O}$.

It is clear then that every factorization of α is of the form

$$\alpha = \pi_1\varepsilon_1\varepsilon_1^{-1}\pi_2\varepsilon_2 \ldots \varepsilon_{s-1}^{-1}\pi_s.$$

for units $\varepsilon_1, \ldots, \varepsilon_s \in \mathcal{O}^*$. Therefore these units are uniquely determined by the condition that the $\pi_i\varepsilon_i$ for every $1 \leq i \leq s$ have to be primary. □

The following corollary will be fundamental in the proof of some of the results in Chapter 3.

1.1.28 Corollary. *Let Q be a quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O}$ be an order over $\mathbb{Z}$ such that $h(Q, \mathcal{O}) = 1$. Let $\xi \in \mathcal{O}$ be an integral quaternion such that $\mathcal{O}/\xi\mathcal{O}$ contains a primary representative set.*

Let us fix a prime integer p and let us denote by $\mathcal{O}[1/p] := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ the corresponding order over $\mathbb{Z}[1/p]$.

Then every element $\alpha \in \mathcal{O}[1/p]^*$ can be decomposed uniquely as a product

$$\alpha = p^n \cdot \varepsilon \cdot \prod_{i=1}^{s} \beta_i,$$

where $n \in \mathbb{Z}, \varepsilon \in \mathcal{O}^*$ and $\beta_1, \ldots, \beta_s \in \mathcal{O}$ are primitive and ξ-primary quaternions such that $\mathrm{Nm}(\beta_i) = p$ for every $1 \leq i \leq s$.

Proof. If $\alpha \in \mathcal{O}[1/p]^*$, there exists an integer $n \geq 0$ such that $p^n\alpha \in \mathcal{O}$ and $\mathrm{Nm}(\alpha) = p^s$ for some $s \in \mathbb{Z}$. Let $m \in \mathbb{N}$ be the greatest common divisor of the integer coordinates of $p^n\alpha$ in some basis of $\mathcal{O}$, and put $\beta := \frac{p^n\alpha}{m}$. Then $\beta \in \mathcal{O}$ has norm $\mathrm{Nm}(\beta) = \frac{p^{2n+s}}{m^2} \in \mathbb{Z}$, so m is a power of p, say $m = p^t$.

Now β is a primitive quaternion of norm $\mathrm{Nm}(\beta) = p^{2n+s-2t}$, and it is associated to a unique primitive and ξ-primary quaternion β' having the same norm. Therefore the statement for β follows applying Theorem 1.1.27 to β'. □

1.1.2.1 Definite quaternion algebra of discriminant $D = 2$. Hurwitz quaternions

Let us consider the definite quaternion algebra B over $\mathbb{Q}$ of discriminant $D_B = 2$. This algebra admits a presentation $B = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, k\rangle$, where $i^2 = j^2 = -1, k = ij = -ji$.

The completion at the Archimedean prime ∞ of $\mathbb{Q}$ is the $\mathbb{R}$-algebra of Hamilton quaternions $B_\infty := B \otimes_{\mathbb{Q}} \mathbb{R}$.

The quaternion algebra B has a maximal order $\mathcal{O}$ over $\mathbb{Z}$, unique up to conjugation. An integral basis for this order is $\{1, i, j, \rho\}$, where

$$\rho := \frac{1 + i + j + k}{2}.$$

Moreover each one of the sets $\{1, j, k, \rho\}, \{1, i, k, \rho\}, \{i, j, k, \rho\}$ is an integral basis for $\mathcal{O}$, since the corresponding base change matrices are in $\mathrm{GL}_4(\mathbb{Z})$. In the literature, this is called the **order of Hurwitz quaternions** for obvious reasons.

The quaternary normic form associated to this algebra, with respect to the basis $\{1, i, j, k\}$ and to the presentation given above, is

$$\mathrm{N}_{B,4}(X, Y, Z, T) = X^2 + Y^2 + Z^2 + T^2,$$

which is one of the most famous positive definite quaternary quadratic forms, known as the "sum of four squares".

The normic form associated to the order $\mathcal{O}$ with respect to the basis $\{1, i, j, \rho\}$ is

$$\begin{aligned}\mathrm{N}_{\mathcal{O},4}(X,Y,Z,T) = (X+T/2)^2 + (Y+T/2)^2 + (Z+T/2)^2 + (T/2)^2 = \\ = X^2 + Y^2 + Z^2 + T^2 + XT + YT + ZT.\end{aligned}$$

We now recall some arithmetic properties of the order $\mathcal{O}$, which were presented by Hurwitz in [Hur96].

(a) The order $\mathcal{O}$ is euclidean on the right and on the left.

Note that this cannot be proved by applying Theorem 1.1.15 because the order $\mathcal{O}$ over $\mathbb{Z}$ does not satisfy Eichler's condition (cf. Definition 1.1.6), since the algebra B is definite. Nevertheless, given quaternions $\alpha, \beta \in \mathcal{O}, \beta \neq 0$ we can approximate $\beta^{-1}\alpha$ by a quaternion $\gamma = a_0 + a_1 i + a_2 j + a_3 k$, with $a_i \in \mathbb{Z}$, such that

$$\mathrm{Nm}(\beta^{-1}\alpha - \gamma) \leq (1/2)^2 + (1/2)^2 + (1/2)^2 + (1/2)^2 = 1.$$

If $\mathrm{Nm}(\beta^{-1}\alpha - \gamma) < 1$ then by Lemma 1.1.16 the euclidean division between α and β exists. If $\mathrm{Nm}(\beta^{-1}\alpha - \gamma) = 1$, then $\beta^{-1}\alpha - \gamma$ has to be one of the quaternions $1/2 \pm (1/2)i \pm (1/2)j \pm (1/2)k$ and so in particular $\beta^{-1}\alpha - \gamma \in \mathcal{O}^*$. Finally $\alpha\beta^{-1} \in \mathcal{O}$, so in this case the division is exact and we have proved that the order $\mathcal{O}$ is euclidean on the right. With the same reasoning we can prove that the order is euclidean on the left.

(b) The group of units of $\mathcal{O}$ is

$$\mathcal{O}^* = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\},$$

and there is an isomorphism of non-abelian groups

$$(\mathcal{O}/2\mathcal{O})^* \simeq \mathcal{O}^*/\mathbb{Z}^* \simeq A_4.$$

(c) In [Hur96, Sec. 6], it is proved that the set of quaternion classes

$$\mathcal{P} := \{[1], [1+2\rho]\} \subseteq \mathcal{O}/2(1+i)\mathcal{O}$$

is a primary representative set mod $2(1+i)$ for quaternions with odd norm (cf. Definition 1.1.26) in the maximal order $\mathcal{O}$. Therefore $2(1+i)$-primary quaternions with odd norm are those α satisfying one of the two following congruences:

$$\alpha \equiv 1 \pmod{2(1+i)} \quad \text{or} \quad \alpha \equiv 1 + 2\rho \pmod{2(1+i)}.$$

The proof of this fact may appear quite easy, and perhaps it is, but it reveals the very deep nature of the arithmetic in this order.

Let us take $\alpha \in \mathcal{O}$ with odd norm. After Proposition 1.1.25, we know that $[\alpha] \in (\mathcal{O}/2\mathcal{O})^*$ and by the isomorphism $(\mathcal{O}/2\mathcal{O})^* \simeq \mathcal{O}^*/\mathbb{Z}^*$ there exist unique units $\varepsilon_1, \varepsilon_2 \in \mathcal{O}^*/\mathbb{Z}^*$ such that $\varepsilon_1\alpha \equiv 1 \pmod 2$ and $\alpha\varepsilon_2 \equiv 1 \pmod 2$. So every quaternion $\alpha\mathcal{O}$ is associated on the left (and on the right) to a quaternion $\beta \equiv 1 \pmod 2$ and this quaternion is unique, up to the sign. In order to obtain the unicity, Hurwitz observes that if in addition we take the class of this quaternion mod $(1+i)$ this will be only one of the following classes of $\mathcal{O}/2(1+i)\mathcal{O}$:

$$1, \quad 1+2 \equiv -1, \quad 1+2\rho, \quad 1+2\rho^2 \equiv -1-2\rho \pmod{2(1+i)}.$$

This is because the classes of the quotient ring $\mathcal{O}/(1+i)\mathcal{O}$ are $[0], [1], [\rho]$ and $[\rho^2]$.

The following lemma will be useful in Chapter 3.

1.1.29 Lemma. *Let $p \in \mathbb{Z}$ be an odd prime integer.*

A quaternion $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ belongs to the finite set

$$\{\alpha \in \mathcal{O} \mid \alpha \equiv 1 \pmod 2, \operatorname{Nm}(\alpha) = p\}$$

iff it satisfies the following conditions:

(*i*) $a_i \in \mathbb{Z}$ *for every* $0 \leq i \leq 3$,

(*ii*) $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$,

(*iii*) $a_0 + a_3 \equiv 1 \pmod 2$, *and* $a_i + a_3 \equiv 0 \pmod 2$ *for* $1 \leq i \leq 2$.

Proof. Writing $\alpha = x + yi + zj + t\rho$, we obtain the following relations:

$$a_0 = x + t/2 \quad a_1 = y + t/2 \quad a_2 = z + t/2 \quad a_3 = t/2.$$

Since $\alpha \equiv 1 \pmod 2$ we find $t \equiv 0 \pmod 2$ and so $a_i \in \mathbb{Z}$ for every i.

In addition, $a_0 + a_3 = x + t \equiv 1, \pmod 2$, $a_1 + a_3 = y + t \equiv 0, \pmod 2$, and $a_2 + a_3 = z + t \equiv 0, \pmod 2$.

Viceversa: $a_2 \in \mathbb{Z}$ implies $t \equiv 0 \pmod 2$, $a_i + a_3 \equiv 0 \pmod 2$ for $1 \leq i \leq 2$ implies $y \equiv z \equiv t \equiv 0 \pmod 2$ and $a_0 + a_3 = x + t \equiv 1 \pmod{\ }$ implies $x \equiv 1 \pmod 2$. □

1.1.2.2 Definite quaternion algebra of discriminant $D = 3$

Let $B := \left(\frac{-1,-3}{\mathbb{Q}}\right)$ be the definite quaternion algebra of discriminant $D_B = 3$ of $\mathbb{Q}$-basis $\{1, i, j, k\}$ such that $i^2 = -1, i^2 = -3, k = ij = -ji$.

Let us consider the order $\mathcal{O}$ over $\mathbb{Z}$ of basis $\{1, i, \lambda, \mu\}$, where

$$\lambda := \frac{i+j}{2}, \quad \mu := \frac{1+k}{2}.$$

This is a maximal order of B, as can be seen after computing its discriminant.

The quaternary normic form associated to this algebra, with respect to the basis $\{1, i, j, k\}$ and to the presentation given above, is

$$\mathrm{N}_{B,4}(X, Y, Z, T) = X^2 + Y^2 + 3Z^2 + 3T^2.$$

The normic form associated to the order $\mathcal{O}$ with respect to the basis $\{1, i, \lambda, \mu\}$ is

$$\begin{aligned}\mathrm{N}_{\mathcal{O},4}(X, Y, Z, T) = (X + T/2)^2 + (Y + Z/2)^2 + 3(Z/2)^2 + 3(T/2)^2 = \\ = X^2 + Y^2 + Z^2 + T^2 + XT + YZ.\end{aligned}$$

(a) The order $\mathcal{O}$ is euclidean on the right and on the left.

(b) The group of units of $\mathcal{O}$ is

$$\mathcal{O}^* = \{\pm 1, \pm i, \frac{\pm 1 \pm i}{2}, \frac{\pm i \pm k}{2}\}.$$

and there is an isomorphism of abelian groups

$$(\mathcal{O}/2\mathcal{O})^* \simeq \mathcal{O}^*/\mathbb{Z}^* \simeq C_2 \times C_3.$$

(c) From the previous isomorphism we deduce that for every quaternion $\alpha \in \mathcal{O}$ of odd norm $\mathrm{Nm}(\alpha) \in \mathbb{Z}$ there exist unique units $\varepsilon_1, \varepsilon_2 \in \mathcal{O}^*/\mathbb{Z}^*$ such that $\varepsilon_1 \beta \equiv \beta \varepsilon_2 \equiv 1 \pmod 2$.

1.1.30 Lemma. *Let $p \in \mathbb{Z}$ be an odd prime integer.*

A quaternion $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in B = \left(\frac{-1,-3}{\mathbb{Q}}\right)$ belongs to the finite set

$$\{\alpha \in \mathcal{O} \mid \alpha \equiv 1 \pmod 2, \mathrm{Nm}(\alpha) = p\}$$

iff it satisfies the following conditions:

(*i*) $a_i \in \mathbb{Z}$ *for every* $0 \leq i \leq 3$,

(*ii*) $a_0^2 + a_1^2 + 3a_2^2 + 3a_3^2 = p$,

(*iii*) $a_0 + a_3 \equiv 1 \pmod 2$, $a_1 + a_2 \equiv 0 \pmod 2$.

PROOF. Writing $\alpha = x + yi + z\lambda + t\mu$, we obtain the following relations:

$$a_0 = x + t/2 \quad a_1 = y + z/2 \quad a_2 = z/2 \quad a_3 = t/2$$

Since $\alpha \equiv 1 \pmod 2$ we find $z \equiv t \equiv 0 \pmod 2$ and so $a_i \in \mathbb{Z}$ for every i.

In addition, $a_0 + a_3 = x + t \equiv 1, \pmod 2$ and $a_1 + a_2 = y + z \equiv 0, \pmod 2$.

Viceversa: $a_2, a_3 \in \mathbb{Z}$ implies $t \equiv z \equiv 0 \pmod 2$, $a_0 + a_3 \equiv 1 \pmod 2$ implies $x \equiv 1 \pmod 2$, and $a_1 + a_2 \equiv 0 \pmod 2$ implies $y \equiv 0 \pmod 2$. □

1.2 The system of Shimura curves

In this section we want to introduce the reader to the definition of Shimura curves associated to quaternion algebras from a particular point of view. First of all, we should say that there are two different approaches when one wants to give this definition: the first one follows the fundamental paper by Shimura [Shi67] and the other one is the famous paper by Deligne [Del71] in which, thanks to the powerful theory of algebraic groups and their adelization, a larger class of varieties is considered at the same time, some of them being modular varieties, such as classical Shimura varieties, Hilbert modular varieties and Siegel modular varieties.

We should also mention that Shimura himself first approached the study of *his* varieties following this more general setting in two other papers, namely [Shi70b] and [Shi70c].

The two main aims of this section are the following:

(1) To show how the two definitions are related in the case of Shimura curves associated to quaternion algebras.

(2) To relate these definitions with class field theory of a totally real field F and to show how they can be considered as a geometric interpretation of Artin reciprocity laws for abelian extensions of F.

The first aim is achieved by building up a *global adelic dictionary*, allowing one to pass from the *global* context to the *adelic* one. The ideas are the same

as those employed in class field theory, where theorems can be stated both involving *ideals* and *idèles*.

The second aim is achieved thanks to a *noncommutative commutative dictionary* which is the bridge between the arithmetic in the *quaternion algebras* over a field F and the arithmetic in the *field* F; or, if one prefers, between the algebraic group of invertible quaternions Q^* over F and the multiplicative group $\mathbb{G}_{m,F}$ over F.

1.2.1 Canonical models of Shimura curves

Let us start with some basic notations, most of them given following [Shi67].

Let F be a totally real number field of degree $[F : \mathbb{Q}] = n$ and R_F be its ring of integers. We will denote by $\mathfrak{p}_{\infty 1}, \ldots, \mathfrak{p}_{\infty n}$ the (real) Archimedean primes of F and by $\sigma_i : F \hookrightarrow \mathbb{R}$ the corresponding real immersions.

Let H be a quaternion algebra over F such that H is not ramified in $\mathfrak{p}_{\infty 1}$ and is ramified in the remaining Archimedean primes. If for every $1 \leq i \leq n$ we denote by $H_{\mathfrak{p}_{\infty \mathrm{i}}} := (H \otimes_{\mathbb{Q}} \sigma_i(F))_{\mathfrak{p}_{\infty i}}$ the $\mathbb{R}$-algebra obtained by localizing H at $\mathfrak{p}_{\infty i}$, then the ramification condition at infinity translates into the following isomorphisms:

$$H_{\mathfrak{p}_{\infty 1}} \simeq \mathrm{M}_2(\mathbb{R}), \text{ and } H_{\mathfrak{p}_{\infty i}} \simeq \mathbb{H}_{\mathbb{R}} \text{ for } 2 \leq i \leq n.$$

where $\mathbb{H}_{\mathbb{R}}$ denotes the $\mathbb{R}$-algebra of Hamilton quaternions.

Let $\mathcal{O}_H \subseteq H$ be an Eichler order over R_F.

Recall that if $\mathfrak{u}$ is a product of Archimedean primes of F, then for every $a \in F^*$ the multiplicative congruence

$$a \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u})$$

means that the element a is positive at the Archimedean primes dividing $\mathfrak{u}$, i.e.

$$\text{if } \mathfrak{p}_{\infty i} \mid \mathfrak{u} \text{ then } \sigma_i(a) \in \mathbb{R}_{>0}.$$

Moreover if $\mathfrak{a} \subseteq R_F$ is an integral ideal of F, then the multiplicative congruence

$$a \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{a})$$

is equivalent to the ordinary (additive) congruence $a \equiv 1 \,(\mathrm{mod}\, \mathfrak{a})$.

1.2.1 Remark. If a is a quotient x/y, with $x, y \in R_F$ and the ideal (y) is coprime with $\mathfrak{a}$, then

$$\frac{x}{y} \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{a}) \iff \frac{x}{y} \equiv 1 \,(\mathrm{mod}\, \mathfrak{a}) \iff x - y \equiv 0 \,(\mathrm{mod}\, \mathfrak{a}),$$

so the multiplicative congruence with the definition above actually translates into its additive counterpart.

1.2.2 Notation. We will denote by $\mathfrak{u}_0$ the product of all Archimedean primes of F and by $\mathfrak{u}_1$ the product $\mathfrak{u}_0\mathfrak{p}_{\infty 1}^{-1}$ of Archimedean primes in which the algebra H is ramified, i.e.

$$\mathfrak{u}_0 := \prod_{\mathfrak{p}\in S_\infty} \mathfrak{p},$$

$$\mathfrak{u}_1 := \prod_{\mathfrak{p}\in S_\infty \cap \mathrm{Ram}(H)} \mathfrak{p}.$$

Following [Shi67], we define the following subgroups of $\mathcal{O}_H^*$:

$$\Gamma(\mathcal{O}_H) := \{\alpha \in \mathcal{O}_H^* \mid \mathrm{Nm}_{H/F}(\alpha) \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_1)\},$$

$$\Gamma(\mathcal{O}_H, 1) := \{\alpha \in \mathcal{O}_H^* \mid \mathrm{Nm}_{H/F}(\alpha) \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_0)\}.$$

If $\mathfrak{e}$ is a bilateral and integral ideal of $\mathcal{O}_H$, we define the following subgroup of $\Gamma(\mathcal{O}_H, 1)$:

$$\Gamma(\mathcal{O}_H, \mathfrak{e}) := \{\alpha \in \Gamma(\mathcal{O}_H, 1) \mid \alpha - 1 \in \mathfrak{e}\}.$$

This subgroup is called a **principal congruence subgroup of level $\mathfrak{e}$ associated to the order $\mathcal{O}_H$**.

Once an isomorphism $\Phi_\infty : H_{\mathfrak{p}_{\infty 1}} \simeq \mathrm{M}_2(\mathbb{R})$ is fixed, the group $\Gamma(\mathcal{O}_H, \mathfrak{e})$ is realized as a discrete and properly discontinuous subgroup of $\mathrm{PSL}_2(\mathbb{R})$ acting on the Poincaré upper half-plane $\mathcal{H}$. Moreover the Riemann surface $\Gamma(\mathcal{O}_H, \mathfrak{e})\backslash\mathcal{H}$ is compact if and only if $H \neq \mathrm{M}_2(F)$. In this case $\Gamma(\mathcal{O}_H, \mathfrak{e})$ is said to be a Fuchsian group of the first kind (according to [Shi70a, 1.6]) and is denoted again by $\Gamma(\mathcal{O}_H, \mathfrak{e})$.

In [Shi67], Shimura proved the following historical theorem.

1.2.3 Theorem. *The Riemann surface $\Gamma(\mathcal{O}_H, \mathfrak{e})\backslash\mathcal{H}$ admits an algebraic model given by a pair $(X(\mathcal{O}_H, \mathfrak{e}), J_{\mathfrak{e}})$, where:*

(*a*) *$X(\mathcal{O}_H, \mathfrak{e})$ is a smooth and irreducible projective curve, defined over the ray class field $F^{\mathfrak{m}\mathfrak{u}_0}$ of modulus $\mathfrak{m}\mathfrak{u}_0$, where $\mathfrak{m}$ is the integral ideal $\mathfrak{e} \cap R_F$ of F.*

(*b*) *$J_{\mathfrak{e}} : \Gamma(\mathcal{O}_H, \mathfrak{e})\backslash\mathcal{H} \to X(\mathcal{O}_H, \mathfrak{e})(\mathbb{C}) \subseteq \mathbb{P}^d(\mathbb{C})$ is a bijective holomorphic map between Riemann surfaces, such that the following arithmetic property is satisfied:*

If K is an imaginary quadratic extension of F with ring of integers R_K such that there is an immersion of F-algebras $\varphi : K \hookrightarrow H$ with $\varphi(R_K) \subseteq$

$\mathcal{O}_H$ and $\tau \in \mathcal{H}$ is the fixed point for all the elliptic transformations in $\Phi_\infty(\varphi(K))$, then

$$F^{\mathfrak{mu}_0} K(J_{\mathfrak{e}}(\tau)) = K^{\mathfrak{cu}_0},$$

where $\mathfrak{c}$ is the integral ideal $\varphi^{-1}(\mathfrak{e} \cap \varphi(R_K))$, i.e. the point $J_{\mathfrak{e}}(\tau) \in X(\mathcal{O}_H, \mathfrak{e})(\mathbb{C})$ is algebraic and generates the ray class field of conductor $\mathfrak{cu}_0$ of the imaginary quadratic extensions $K|F$.

An algebraic model of this type is unique, up to $F^{\mathfrak{mu}_0}$-biregular morphisms, and it is called **canonical model of the Shimura curve associated to the order $\mathcal{O}_H$ and of principal level $\mathfrak{e}$**.

1.2.4 Notation. From now on we will focus our attention on Shimura curves arising from groups of the type $\Gamma(\mathcal{O}_H, 1)$, for an Eichler order $\mathcal{O}_H$ in H (i.e. Shimura curve of principal level $\mathfrak{e} = 1$). Therefore it is convenient to change the notation slightly.

1. When $\mathcal{O}_H$ is an Eichler order of level N an integral ideal of R_F, we will denote this group by $\Gamma(H, \mathcal{O}_H)$ and the corresponding algebraic curve by $X(H, \mathcal{O}_H)$. These two objects, namely the group and the curve, depend only, up to isomorphisms in the corresponding category, on the type of the order $\mathcal{O}_H$ inside H.

2. When, in addition, there is only one type of Eichler orders of level N, we will denote the group $\Gamma(H, \mathcal{O}_H)$ by $\Gamma(D_H, N)$ and the corresponding curve by $X(D_H, N)$ and we will sometimes refer to it as the **Shimura curve of discriminant D_H and level N**. This would be the case, as we shall see, when the base field F has strict ideal class number $h_F^+ = 1$.

It is a moral obligation, a this point, to make some "classical remarks" about the above result:

1.2.5 Remark. Let $\tau \in \mathcal{H}$ be a parameter as in the statement of the theorem. Then the corresponding algebraic point $J_{\mathfrak{e}}(\tau) \in X(\mathcal{O}_H, \mathfrak{e})(\mathbb{C})$ is called a **complex multiplication point for the maximal order R_K**. This nomenclature comes from the modular interpretation of the curve $X(\mathcal{O}_H, \mathfrak{e})$ as moduli space of certain families of abelian varieties (namely, polarized abelian varieties with quaternion multiplication by the order $\mathcal{O}_H$). The point $J_{\mathfrak{e}}(\tau)$ corresponds then to an abelian variety, among the ones of the family, having complex multiplication by the quadratic order R_K, compatible with the quaternionic multiplication.

In Section 1.3.1 we will introduce this modular interpretation for all complex points of the curve $X(\mathcal{O}_H, \mathfrak{e})$ and we will refer to a parameter with the

arithmetic property explained above, by a **complex multiplication parameter for the order** R_K (cf. Definition 1.3.15).

1.2.6 Remark. The function $J_{\mathfrak{e}}$, whose existence is predicted by the statement of the theorem, is a wide generalization of the Klein j-function: special values of $J_{\mathfrak{e}}$ provide ray class fields of the imaginary quadratic extension $K|F$, just as special values of j provide ray class fields of imaginary quadratic extensions $K|\mathbb{Q}$.

Actually, as we shall see in the this section and the following ones, the whole canonical model $(X(\mathcal{O}_H, \mathfrak{e}), J_{\mathfrak{e}})$ is a generalization of classical modular curves $X_0(N)$ and $X(N)$, together with their classical uniformizing functions.

1.2.7 Remark. In all the previous definitions, let us take F to be a principal ideal domain. Therefore, for every algebraic integer $N \in R_F$ there exists a unique Eichler order $\mathcal{O}_H$ of level N, up to conjugation, inside the quaternion F-algebra H (i.e. the number of types of this algebra is 1, as can be deduced by combining the Theorem 1.2.15 below with Theorem 1.1.11).

If the discriminant of H is the algebraic integer $D_H \in R_F$, then

$$\Gamma(D_H, N) = \{\alpha \in \mathcal{O}_H^* \mid \mathrm{Nm}_{H/F}(\alpha) \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_0)\}.$$

Finally the Shimura curve $X(D_H, N)$ is defined over $F^{\mathfrak{u}_0}$ (i.e. the Hilbert class field of F of modulus $\mathfrak{u}_0$, in our notations).

1.2.8 Remark. In [Shi67, Main Theorem 1] the statement above is given and proved for the case of maximal orders (i.e. Eichler orders of level 1). Nevertheless all the definitions and results of the paper could apparently be extended to an arbitrary Eichler order.

In any case, later in [Shi70b] and [Shi70c], Shimura extended these results to more general symmetric domains and groups acting on them, both of which arise from reductive algebraic groups, making use of the adelic language. Inside these very general cases, also the case of an arbitrary Eichler order would also be considered.

1.2.2 The noncommutative commutative dictionary

1.2.9 Definition. If $\mathfrak{m}$ is an integral ideal of F and $\mathfrak{u}$ is a product of Archimedean primes of F, then

(a) $I(F, \mathfrak{m})$ denotes the group of fractional ideals of F which are coprime with $\mathfrak{m}$,

(b) $P(F, \mathfrak{m}\mathfrak{u})$ the subgroup of $I(F, \mathfrak{m})$ formed by those principal ideals which are generated by an element $a \in F$ satisfying $a \equiv 1 \,(\mathrm{mod}^* \mathfrak{m}\mathfrak{u})$.

Therefore we have that $I(F) := I(F, 1)$ and $P(F) := P(F, 1)$ will denote the group of all fractional ideals of F and the subgroup of principal ideals of F, respectively.

The following ideal class numbers will be of particular interest:

$$h := [I(F) : P(F)], \quad h_0 := [I(F) : P(F, \mathfrak{u}_0)], \quad h_1 := [I(F) : P(F, \mathfrak{u}_1)].$$

The first cardinal is called **ideal class number of** F and the second cardinal is called **strict ideal class number of** F and is usually also denoted by h^+. The third cardinal does not have a name in the literature, even though, as we shall see immediately below, it is naturally related to Eichler's *Normensatz* (cf. Theorem 1.1.8).

1.2.10 Definition. Let $S \supseteq S_\infty$ be a set of primes of F.

If G is an algebraic group over F and $\mathcal{G}$ is an integral model over $R_F[1/S]$ of G, then the adelization of G is the product

$$G_{\mathbb{A}} := \prod_{\mathfrak{p} \notin S} (G(F_\mathfrak{p}) : \mathcal{G}(R[1/S]_\mathfrak{p})) \times \prod_{\mathfrak{q} \in S} G(F_\mathfrak{q}),$$

where an element α belongs to the *restricted product*

$$\prod_{\mathfrak{p} \notin S} (G(F_\mathfrak{p}) : \mathcal{G}(R[1/S]_\mathfrak{p}))$$

if and only if $\alpha = (\alpha_\mathfrak{p}) \in \prod_{\mathfrak{p} \notin S} G(F_\mathfrak{p})$ and $\alpha_\mathfrak{p} \in \mathcal{G}(R[1/S]_\mathfrak{p})$ for almost every prime $\mathfrak{p} \notin S$.

This definition, as is well known, does not depend either on the integral model $\mathcal{G}$ chosen or on the set of primes S.

It is important to recall that the adelization of an algebraic group is canonically isomorphic to the group of adelic points of the same group, i.e. there is a canonical isomorphism $G_{\mathbb{A}} \simeq G(\mathbb{A}_\mathbb{F})$ where $\mathbb{A}_F$ denotes the F-algebra of the *adèles* of F.

Note also that Definition 1.1.7 is a special case of Definition 1.2.10 when we take $G = Q^*$ and $\mathcal{G} = \mathcal{O}[1/S]$.

1.2.11 Notation. We will denote by $F^*_{\mathbb{A}}$ the adelization of the multiplicative group $\mathbb{G}_{m,F}$ over F, i.e.

$$F^*_{\mathbb{A}} = \prod_{\mathfrak{p}} (F^*_\mathfrak{p} : R^*_{F,\mathfrak{p}}) \times F^*_{\mathfrak{p}_{\infty 1}} \times \cdots \times F^*_{\mathfrak{p}_{\infty n}}.$$

Again we find the canonical isomorphisms $F_{\mathbb{A}}^* \simeq \mathbb{G}_{m,F}(\mathbb{A}_F) = \mathbb{A}_F^*$ which is the group of the *idèles* of F.

Finally we will denote by $H_{\mathbb{A}}^*$ the adelization of the algebraic group H^* over F defined by: $H^*(A) := H^* \otimes_F A$, for every F-algebra A. The Archimedean part of $H_{\mathbb{A}}^*$ is then

$$H_\infty^* = H_{\mathfrak{p}_{\infty 1}}^* \times \cdots \times H_{\mathfrak{p}_{\infty n}}^* \simeq \mathrm{GL}_2(\mathbb{R}) \times (\mathbb{H}_{\mathbb{R}}^*)^{n-1}.$$

1.2.12 Proposition. (Commutative adelic global dictionary) *If $\mathfrak{u}$ is a product of Archimedean primes of F and $\mathfrak{m}$ is a product of finite primes of F then the following isomorphism of commutative groups holds:*

$$\Big(\prod_{\mathfrak{p}\nmid\mathfrak{m}} R_{F,\mathfrak{p}}^* \times \prod_{\mathfrak{p}\mid\mathfrak{m}} (1+\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})}) \times F_\infty^*\Big)\backslash F_{\mathbb{A}}^* / \{x \in F^* \mid x \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u})\} \simeq$$

$$\simeq I(F,\mathfrak{m})/P(F,\mathfrak{m}\mathfrak{u}).$$

Proof. We consider the following morphism:

$$\begin{array}{ccc} F_{\mathbb{A}}^* & \longrightarrow & I(F,\mathfrak{m}) \\ (x_{\mathfrak{p}})_{\mathfrak{p}} & \longmapsto & \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})}, \end{array}$$

which is well defined, i.e. the product on the right-hand side is actually finite, since almost for every prime $\mathfrak{p}$ the element $x_{\mathfrak{p}} \in F_{\mathfrak{p}}^*$ is a unit in $R_{F,\mathfrak{p}}$ so its $\mathfrak{p}$-valuation is $v_{\mathfrak{p}}(x_{\mathfrak{p}}) = 0$. This morphism induces then an epimorphism on the quotients

$$F_{\mathbb{A}}^*/\{x \in F^* \mid x \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u})\} \longrightarrow I(F,\mathfrak{m})/P(F,\mathfrak{m}\mathfrak{u}),$$

and an isomorphism on the double quotients as in the statement. □

1.2.13 Proposition. (Noncommutative adelic global dictionary)

If H_+^* denotes the subgroups of quaternions in H^* with totally positive norm, i.e.

$$H_+^* := \{\alpha \in H \mid \mathrm{Nm}_{H/F}(\alpha) \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_0)\},$$

and $\mathcal{O}_H$ denotes an Eichler order over R_F, then we have the following bijections of sets:

(a) $(\prod_{\mathfrak{p}} \mathcal{O}_{H,\mathfrak{p}}^* \times H_\infty)\backslash H_{\mathbb{A}}^*/H^* \simeq \mathcal{I}_\ell(\mathcal{O}_H)/H^*$,

(b) $H^*\backslash H_{\mathbb{A}}^*/(\prod_{\mathfrak{p}} \mathcal{O}_{H,\mathfrak{p}}^* \times H_\infty) \simeq H^*\backslash \mathcal{I}_\ell(\mathcal{O}_H)$,

(c) $(\prod_{\mathfrak{p}} \mathcal{O}^*_{H,\mathfrak{p}} \times H_\infty)\backslash H^*_{\mathbb{A}}/H^*_+ \simeq \mathcal{I}_\ell(\mathcal{O}_H)/H^*_+$,

(d) $H^*_+\backslash H^*_{\mathbb{A}}/(\prod_{\mathfrak{p}} \mathcal{O}^*_{H,\mathfrak{p}} \times H_\infty) \simeq H^*_+\backslash \mathcal{I}_r(\mathcal{O}_H)$.

PROOF. We have to consider the following maps:

$$\begin{array}{ccc} H^*_{\mathbb{A}} & \longrightarrow & \mathcal{I}_\ell(\mathcal{O}_H), \\ (\alpha_{\mathfrak{p}})_{\mathfrak{p}} & \longmapsto & \bigcap_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}}\alpha_{\mathfrak{p}} \cap H), \end{array} \qquad \begin{array}{ccc} H^*_{\mathbb{A}} & \longrightarrow & \mathcal{I}_r(\mathcal{O}_H), \\ (\alpha_{\mathfrak{p}})_{\mathfrak{p}} & \longmapsto & \bigcap_{\mathfrak{p}}(\alpha_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}} \cap H), \end{array}$$

which induce the bijections of the statement. □

1.2.14 Lemma. *Let $\mathcal{O}_H$ be an Eichler R_F-order in H.*

Then for every finite prime $\mathfrak{p}$, we have

$$\mathrm{Nm}_{H_{\mathfrak{p}}/F_{\mathfrak{p}}}(\mathcal{O}^*_{H,\mathfrak{p}}) = R^*_{F,\mathfrak{p}}.$$

PROOF. When $\mathfrak{p} \notin \mathrm{Ram}(H)$, the statement is trivial.

Let us take an element $x \in R^*_{F,\mathfrak{p}}$. Since the quaternary normic form $\mathrm{Nm}_{4,H_{\mathfrak{p}}}$ is universal over $F_{\mathfrak{p}}$ (cf. [Ser70] for $F = \mathbb{Q}$ and [O'M71] for the general case), then $x = \mathrm{Nm}(\alpha)$ for some $\alpha \in H^*_{\mathfrak{p}}$. Hence we have to prove that actually $\alpha \in \mathcal{O}^*_{H,\mathfrak{p}}$.

Recall (cf. [Vig80, Ch. II]) that when $\mathfrak{p} \in \mathrm{Ram}(H)$, then

$$\mathcal{O}^*_{H,\mathfrak{p}} = \{\beta \in H_{\mathfrak{p}} \mid v_{\mathfrak{p}}(\mathrm{Nm}(\beta)) = 0\}.$$

But $v_{\mathfrak{p}}(\mathrm{Nm}(\alpha)) = v_{\mathfrak{p}}(x) = 0$, so $\alpha \in \mathcal{O}^*_{H,\mathfrak{p}}$. □

The following result is one of the most important in the study of quaternion algebras because it relates the sets of ideal classes arising from quaternion algebras with their corresponding abelian class groups coming from number fields. It was first proved by Eichler ([Eic37, Satz 1, 2]).

1.2.15 Theorem. (Noncommutative commutative dictionary)

Let $\mathcal{O}_H$ be an Eichler R_F-order in H, of level N.

1. *The ideal class number $h(D_H, N)$ of $\mathcal{O}_H$ is equal to the ideal class number h_1 defined above, for the number field F, thanks to the bijection induced by the norm:*

$$(\prod_{\mathfrak{p}} \mathcal{O}^*_{H,\mathfrak{p}} \times H_\infty)\backslash H^*_{\mathbb{A}}/H^* \xrightarrow{\mathrm{Nm}} (\prod_{\mathfrak{p}} R^*_{F,\mathfrak{p}} \times F^*_\infty)\backslash F^*_{\mathbb{A}}/\{x \in F^* \mid x \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_1)\}.$$

2. *The strict ideal class number $h^+(D_H, N)$ of $\mathcal{O}_H$ is equal to the strict ideal class number h^+ of the number field F defined above, thanks to the bijection induced by the norm:*

$$(\prod_{\mathfrak{p}} \mathcal{O}_{H,\mathfrak{p}}^* \times H_\infty)\backslash H_{\mathbb{A}}^*/H_+^* \xrightarrow{\mathrm{Nm}} (\prod_{\mathfrak{p}} R_{F,\mathfrak{p}}^* \times F_\infty^*)\backslash F_{\mathbb{A}}^*/\{x \in F^* \mid x \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_0)\}.$$

Proof. The norm map

$$\mathrm{Nm}_{H_{\mathbb{A}}^*/F_{\mathbb{A}}^*} : (\alpha_{\mathfrak{p}})_{\mathfrak{p}} \in H_{\mathbb{A}}^* \longmapsto (\mathrm{Nm}_{H_{\mathfrak{p}}/F_{\mathfrak{p}}}(\alpha_{\mathfrak{p}}))_{\mathfrak{p}} \in F_{\mathbb{A}}^*$$

induces a well-defined map between the double quotient sets:

$$(\prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^* \times H_\infty^*)\backslash H_{\mathbb{A}}^*/H^* \longrightarrow (\prod_{\mathfrak{p}} R_{F,\mathfrak{p}}^* \times F_\infty^*)\backslash F_{\mathbb{A}}^*/\{x \in F^* \mid x \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_1)\}.$$

It is immediate to see that the map is surjective, thanks to Theorem 1.1.8 (i.e. the *Normensatz*).

Now, let $[\alpha] \in (\prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^* \times H_\infty^*)\backslash H_{\mathbb{A}}^*/H^*$ be a double class belonging to the kernel of this map, i.e. its representative $\alpha \in H_{\mathbb{A}}^*$ is such that

$$\mathrm{Nm}_{H_{\mathbb{A}}^*/F_{\mathbb{A}}^*}(\alpha) \in \prod_{\mathfrak{p}} R_{F,\mathfrak{p}}^* \cdot \{x \in F^* \mid x \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_1)\},$$

Since $\mathrm{Nm}_{H_{\mathfrak{p}}/F_{\mathfrak{p}}}(\mathcal{O}_{H,\mathfrak{p}}^*) = R_{F,\mathfrak{p}}^*$ by Lemma 1.2.14, then we can choose the representative α such that $\mathrm{Nm}_{H_{\mathbb{A}}^*/F_{\mathbb{A}}^*}([\alpha]) = 1$. Now we can apply Theorem 1.1.9, i.e. the Strong Approximation Theorem for the quaternion algebra H and the Eichler order $\mathcal{O}_H$, since the order $\mathcal{O}_H$ over R_F satisfies Eichler's condition. Therefore

$$\alpha \in (\prod_{\mathfrak{p}} \mathcal{O}_{H,\mathfrak{p}}^* \times H_\infty^*)H^*,$$

and so the class of α inside the double quotient space of the domain of the map is 1. □

So finally we find the following compact result which will be the *leitmotiv* of the whole chapter.

1.2.16 Corollary. *There is a bijection of sets*

$$(\prod_{\mathfrak{p}} \mathcal{O}_{H,\mathfrak{p}}^* \times H_\infty^*)\backslash H_{\mathbb{A}}^*/H_+^* \simeq \mathrm{Gal}(F^{\mathfrak{u}_0}/F)$$

where $F^{\mathfrak{u}_0}$ is the Hilbert class field of the number field F (i.e. the ray class field of modulus $\mathfrak{u}_0$).

PROOF. By Theorem 1.2.15 (2) and by Artin reciprocity law for (finite abelian) extensions of the number field F (cf. for example [Neu99, Ch. VI Sec. 6]) we have the following chain of bijections

$$(\prod_{\mathfrak{p}} \mathcal{O}_{H,\mathfrak{p}}^* \times H_\infty^*)\backslash H_{\mathbb{A}}^*/H_+^* \simeq$$

$$\simeq (\prod_{\mathfrak{p}} R_{F,\mathfrak{p}}^* \times F_\infty^*)\backslash F_{\mathbb{A}}^*/\{x \in F^* \mid x \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_0)\} \simeq \mathrm{Gal}(F^{\mathfrak{u}_0}/F).$$

□

These last results, and in particular Theorem 1.2.15, can be extended with out difficulty to a quaternion algebra Q over F and an Eichler order $\mathcal{O}[1/S]$ over $R_F[1/S]$ satisfying Eichler's condition, because in this case Strong approximation theorem 1.1.9 is valid. We do this in Section 3.1 (cf. Theorem 3.1.7).

1.2.3 System of Shimura curves: gobal definition

Following [Shi67] we give the definition of a *system of canonical models*. Actually, once given the algebraic curve $X(H, \mathcal{O}_H)$ defined over the Hilbert class field $F^{\mathfrak{u}_0}$, it is natural to want to consider the action of the Galois group of this abelian extension over the coefficients of the equation(s) defining the curve: this allows us to translate arithmetic information about the algebra H into a geometric context, thanks to class field theory.

These ideas can be formalized using both global and adelic languages, as has been already shown in the previous results. We will see how the first one highlights the connection between the system of canonical models associated to the quaternion order $\mathcal{O}_H$ and the arithmetic in this order, while the second one has the advantage of making it possible to pass from the noncommutative to the commutative case, through the norm map (as in Theorem 1.2.15). Specifically, we will be able to count the number of connected components and the number of non-isomorphic connected components of the system: on one side relating them to certain arithmetic invariants of the quaternion algebra H, and on the other side relating them to the indexes of certain normic subgroups of the *idèles* class group of F.

Let $\mathcal{O}_H$ be an Eichler order over R_F of level N in the algebra H. Since the order $\mathcal{O}_H$ satisfies Eichler's condition (cf. Definition 1.1.6), the number of strict left ideal classes in $H_+^*\backslash\mathcal{I}_r(\mathcal{O}_H)$ is equal to h^+, after Theorem 1.2.15 and, after Definition 1.1.10 and Theorem 1.1.11, the set of right ideal classes form a finite groupoid $\mathcal{G}^+(D_H, N)$ of order h^+ and rank $t := t(D_H, N)$.

Given any system of representatives for right ideal classes in $H_+^*\backslash\mathcal{I}_r(\mathcal{O}_H)$, we can construct a system of representatives for the whole groupoid $\mathcal{G}^+(D_H, N)$.

Namely, let $\{\mathcal{O}_1, \ldots, \mathcal{O}_t\}$ be a system of representatives for types of Eichler orders of level N in H.

Given an Eichler order $\mathcal{O}_i$ and a system of representatives $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_{h^+}\}$ for the set of classes $H_+^*\backslash\mathcal{I}_r(\mathcal{O}_i)$ such that $\mathfrak{a}_i = \mathcal{O}_i$, let

$$\mathcal{R}(D_H, N) := (\mathfrak{a}_{ij})_{1\leq i,j\leq h^+}$$

be the abstract matrix of dimension $h^+ \times h^+$ defined by the following relations:

$$\mathfrak{a}_{ij} := \mathfrak{a}_i\mathfrak{a}_j^{-1}, \quad \mathcal{O}_i := \mathfrak{a}_{ii} = \mathfrak{a}_i\mathfrak{a}_i^{-1}.$$

We call this matrix a **system of strict representatives for Eichler orders of level N and ideals of $\mathcal{G}^+(D_H, N)$.**

The system $\mathcal{R}(D_H, N)$ is actually a system of representatives for the strict groupoid $\mathcal{G}^+(D_H, N)$ associated to the Eichler order $\mathcal{O}_H$ of level N and to the algebra H, as can be seen in the following proposition.

1.2.17 Proposition. *The system of representatives $\mathcal{R}(D_H, N)$ can be chosen such that for every $i, j, k \in \{1, \ldots, h^+\}$:*

(*i*) *$\mathcal{O}_i$ is an Eichler order over R_F of level N.*

(*ii*) $\mathfrak{a}_{ij} = \mathfrak{a}_{ji}^{-1}$.

(*iii*) *$\mathfrak{a}_{ij}$ is a fraction left ideal of the order $\mathcal{O}_i$ and a fraction right ideal of the order $\mathcal{O}_j$.*

(*iv*) $\mathfrak{a}_{ij}\mathfrak{a}_{jk} = \mathfrak{a}_{ik}$.

(*v*) *The i-th line of the matrix $\mathcal{R}(D_H, N)$ is a system of representatives for the strict left ideal classes of $\mathcal{I}_\ell(\mathcal{O}_i)/H_+^*$.*

(*vi*) *The i-th column of the matrix $\mathcal{R}(D_H, N)$ is a system of representatives for the strict right ideal classes of $H_+^*\backslash\mathcal{I}_r(\mathcal{O}_i)$.*

(*vii*) *The diagonal $\{\mathcal{O}_1, \ldots, \mathcal{O}_{h^+}\}$ of the matrix $\mathcal{R}(D_H, N)$ equals $h_{bil}^+(D_H, N)$-times a system of representatives for the types of Eichler orders of level N in H.*

The system of representative $\mathcal{R}(D_H, N)$ then has the following form:

$$\begin{pmatrix} \mathcal{O}_1 & \mathfrak{a}_{12} & \cdots & \cdots & \cdots & \mathfrak{a}_{1h^+} \\ \mathfrak{a}_{21} & \mathcal{O}_2 & \cdots & \cdots & \cdots & \mathfrak{a}_{2h^+} \\ \vdots & \vdots & \ddots & & & \vdots \\ \mathfrak{a}_{t1} & \mathfrak{a}_{t2} & \cdots & \mathcal{O}_t & \cdots & \mathfrak{a}_{th^+} \\ \vdots & \vdots & & & \ddots & \vdots \\ \mathfrak{a}_{h^+1} & \mathfrak{a}_{h^+2} & \cdots & \cdots & \cdots & \mathcal{O}_{h^+} \end{pmatrix}.$$

Starting with such a system of representatives, Shimura constructs a system of canonical models.

Let $\mathcal{R}(D_H, N)$ be a system of strict representatives for Eichler orders of level N and ideals of $\mathcal{G}^+(D_H, N)$. For every $1 \leq i \leq h^+$, the Riemann surface $\Gamma(H, \mathcal{O}_i)\backslash\mathcal{H}$ has a unique canonical model $(X(H, \mathcal{O}_i), J_i)$, which is defined over the Hilbert class field $F^{\mathfrak{u}_0}$ of F (cf. Theorem 1.2.3). In [Shi67, Theorem 3.5], Shimura enunciates the existence of this system of canonical models together with the Galois action of $\mathrm{Gal}(F^{\mathfrak{u}_0}/F)$ on them.

1.2.18 Theorem. *There exists a system*

$$\mathcal{S}(D_H, N) := \{(X(H, \mathcal{O}_i), J_i),\ \{\Sigma^{ji}(\alpha) \mid\ 1 \leq j \leq h^+,\ \alpha \in H_+^*\}\ \}_{1 \leq i \leq h^+}$$

such that:

(*i*) $(X(H, \mathcal{O}_i), J_i)$ *is a canonical model for* $\Gamma(H, \mathcal{O}_i)\backslash\mathcal{H}$.

(*ii*) *For every* $1 \leq j \leq h^+$ *and every* $\alpha \in H_+^*$, *if* $\sigma^{ji}(\alpha)$ *is defined by the Artin symbol*

$$\sigma^{ji}(\alpha) := [\mathrm{Nm}_{H/F}(\alpha\mathfrak{a}_{ij}), F] \in \mathrm{Gal}(F^{\mathfrak{u}_0}/F),$$

then

$$\Sigma^{ji}(\alpha) : X(H, \mathcal{O}_i) \xrightarrow{\simeq} X(H, \mathcal{O}_j)^{\sigma^{ji}(\alpha)}$$

is a biregular morphism defined over $F^{\mathfrak{u}_0}$ *satisfying:*

(*a*) $\Sigma^{ji}(\alpha) = \Sigma^{ji}(\beta)$ *if* $\alpha - \beta$ *is integral,*

(*b*) $\Sigma^{kj}(\beta)^{\sigma^{ji}(\alpha)} \circ \Sigma^{ji}(\alpha) = \Sigma^{ki}(\beta\alpha)$.

The system satisfies the following arithmetical property :

Let K *be an imaginary quadratic extension of* F *with ring of integers* R_K *such that there is an immersion of* F*-algebras* $\varphi : K \hookrightarrow H$ *with* $\varphi(R_K) \subseteq$

$\mathcal{O}_j$ and let $\tau \in \mathcal{H}$ be the fixed point for all the elliptic transformations in $\Phi_\infty(\varphi(K))$, as in Theorem 1.2.3.

If $\mathfrak{b}$ is an ideal of K and $\rho := [\mathfrak{b}, K] \in \mathrm{Gal}(K^{\mathfrak{u}_0}/K)$ the corresponding Artin symbol, then $\varphi(\mathfrak{b})\mathcal{O}_j = \alpha\mathfrak{a}_{ij}$ for a unique i and for some $\alpha \in H_+^*$ and

$$J_j(\tau)^\rho = \Sigma^{ji}(\alpha)\left(J_i(\Phi_\infty(\alpha)^{-1}(\tau))\right).$$

Moreover Shimura proves (cf. [Shi67, Theorem 3.6]) that this last arithmetical property characterizes the system $\mathcal{S}(D_H, N)$. This property, which reveals the action of the different Galois groups $\mathrm{Gal}(K^{\mathfrak{u}_0}/K)$ on complex multiplication points, will be known in the literature as the **Shimura reciprocity law**, since it extends, at least geometrically, Artin reciprocity laws for these imaginary extensions.

1.2.19 Remark. One can deduce from [Shi67, Theorem 3.5] that once given an algebraic model $(X(H, \mathcal{O}_i), J_i)$ of the above system, then all the others can be obtained by conjugating the coefficients of the models defining them, by the Galois action of $\mathrm{Gal}(F^{\mathfrak{u}_0}/F)$.

In this sense, the system of canonical models considered is a "complete system of Galois conjugated", i.e. if we could multiply adequately together all the equations defining the canonical models of the system, then we would obtain an irreducible curve defined over F.

Hence, in some sense, the system of canonical models gives a geometric interpretation of the strict groupoid $\mathcal{G}^+(D_H, N)$ of Eichler orders of level N in the quaternion algebra H. In the following result we will see that actually the *arithmetic invariants* of the groupoid are strictly related to the *geometric invariants* of the system of canonical models.

1.2.20 Corollary. *Given a system of representatives $\mathcal{R}(D_H, N)$ for Eichler orders of level N and ideals of $\mathcal{G}^+(D_H, N)$, let*

$$\mathcal{S}(D_H, N) = \{(X(H, \mathcal{O}_i), J_i)\}_{1 \le i \le h^+}$$

be the associated system of canonical models of Shimura curves.

(*i*) *The number of canonical models in the system is equal to the strict ideal class number $h^+(D_H, N)$ of an Eichler order of level N in H.*

(*ii*) *The number of non-isomorphic canonical models in the system is equal to the number $t(D_H, N)$ of types of Eichler orders of level N in H.* □

1.2.4 System of Shimura curves: adelic definition

Recall that the group of units H^* can be also viewed as the group of $\mathbb{Q}$-rational points of an algebraic subgroup $G^H := G$ of GL_{2n} over $\mathbb{Q}$. Actually, the algebraic group G is the restriction $\mathrm{Res}_{F/\mathbb{Q}}(H^*)$ of scalars *à la Weil* of the algebraic group H^* over F. As a consequence of this construction, the group $G(\mathbb{A}_{\mathbb{Q}})$ of $\mathbb{Q}$-adelic points of G can be identified with the group $H^*(\mathbb{A}_F)$ of F-adelic points of the algebraic group H^*.

As usual, we will denote by $G(\mathbb{A}_{fin})$ and G_∞ respectively the finite and infinite part of the group $G(\mathbb{A})$, so that

$$G_\infty \simeq H^* \otimes \mathbb{R} \simeq \mathrm{GL}_2(\mathbb{R}) \times (\mathbb{H}^*_{\mathbb{R}})^{n-1}.$$

Also, we denote by $G_{\infty+}$ the identity component of the real Lie group G_∞ and by $G(\mathbb{Q})_+ := G_{\infty+} \cap G(\mathbb{Q})$ the identity component of the group of $\mathbb{Q}$-rational points.

1.2.21 Definition. For every integer $N \geq 1$, we define the **principal congruence subgroup of $G(\mathbb{Q})$ of level N**:

$$\Gamma(N) := G(\mathbb{Q}) \cap \{\gamma \in \mathrm{GL}_{2g}(\mathbb{Z}) \mid \ \gamma \equiv \mathrm{I}_{2n} \,(\mathrm{mod}\, N)\}.$$

A **congruence subgroup of level** N is any subgroup Γ of $G(\mathbb{Q})$ containing $\Gamma(N)$.

It is well known that any congruence subgroup of $G(\mathbb{Q})$ is of the type $U \cap G(\mathbb{Q})$ for some open compact subgroup U of $G(\mathbb{A}_{fin})$.

1.2.22 Definition. For any open compact subgroup U of $G(\mathbb{A}_{fin})$ we define the double coset space

$$\mathbb{X}(H, U) := G(\mathbb{Q}) \backslash G(\mathbb{A}) / Z_G(\mathbb{A}) U \mathrm{Stab}(i)$$

where $\mathrm{Stab}(i)$ denotes the stabilizer in $G_{\infty+}$ of the imaginary unit $i \in \mathcal{H}$, and Z_G denotes the center of the group G.

1.2.23 Lemma. *The double coset $G(\mathbb{Q})_+ \backslash G(\mathbb{A}_{fin})/U$ is finite.*

Proof. The double coset of the statement has cardinality

$$h(U) := [F^*_{\mathbb{A}} : F^* \mathrm{Nm}(U)].$$

This is shown by considering the following homomorphism

$$\begin{array}{ccc} H^*_{\mathbb{A}} & \longrightarrow & \mathrm{Gal}(\overline{F}/F) \\ x & \longmapsto & [(\mathrm{Nm}\, x)^{-1}, F] \end{array}$$

which induces an isomorphism

$$H^*_+ \backslash H^*_{\mathbb{A},fin}/U \simeq \mathrm{Gal}(K_U/F).$$

Here $[\ \cdot\ , F]$ denotes the Artin symbol and K_U is the class field extension of F associated to the normic subgroup $\mathrm{Nm}(U)F^*$ of $F^*_{\mathbb{A}}$.(For more details, see [Shi70a, 6.4] and [Neu99, Ch. VI Sec. 6]). □

1.2.24 Lemma. *The map*

$$\begin{array}{ccc} G_{\infty+} = \mathrm{GL}_2(\mathbb{R})_{>0} \times (\mathbb{H}^*_{\mathbb{R},>0})^{n-1} & \longrightarrow & \mathcal{H} \\ \left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \alpha_2, \ldots, \alpha_n\right) & \longmapsto & \gamma \cdot i = (ai+b)(ci+d)^{-1} \end{array}$$

induces the homeomorphism

$$G_{\infty+}/Z_G(\mathbb{R})\mathrm{Stab}(i) \simeq \mathcal{H}.$$

Proof. The proof is an easy generalization of the classic homeomorphism $\mathrm{PGL}_2(\mathbb{R})_{>0}/\mathrm{SO}_2(\mathbb{R}) \simeq \mathcal{H}$ (cf. [Shi70a, 1.2]). □

1.2.25 Theorem. *Let U be an open and compact subgroup of $G(\mathbb{A}_{fin})$ and let $\{x_1, \ldots, x_{h(U)}\}$ be a system of representatives for $G(\mathbb{Q})_+\backslash G(\mathbb{A}_{fin})/U$.*

Then there is a homeomorphism

$$\bigcup_{\lambda=1}^{h(U)} \Gamma_\lambda \backslash \mathcal{H} \simeq \mathbb{X}(H, U),$$

where $\Gamma_\lambda := x_\lambda U x_\lambda^{-1} \cap G(\mathbb{Q})_+$.

Proof. Using Lemma 1.2.24 it can be proved that there is a homeomorphism

$$G(\mathbb{Q})\backslash G(\mathbb{A})/Z_G(\mathbb{A})U\mathrm{Stab}(i) \simeq G(\mathbb{Q})\backslash G(\mathbb{A}_{fin}) \times \mathcal{H}^{\pm}/U.$$

and it is easy to see (cf. [Mil04, 5.11]) that

$$G(\mathbb{Q})_+\backslash G(\mathbb{A}_{fin}) \times \mathcal{H}/U \simeq G(\mathbb{Q})\backslash G(\mathbb{A}_{fin}) \times \mathcal{H}^{\pm}/U.$$

Therefore the following maps are injective:

$$[z] \in \Gamma_\lambda \backslash \mathcal{H} \longmapsto [z, x_\lambda] \in G(\mathbb{Q})_+ \backslash G(\mathbb{A}_{fin}) \times \mathcal{H}/U$$

and the space $G(\mathbb{Q})_+ \backslash G(\mathbb{A}_{fin}) \times \mathcal{H}/U$ is a disjoint union of the images of this map (cf. [Mil04, 5.13]). □

1.2.26 Remark. All the Riemann surfaces $\Gamma_\lambda \backslash \mathcal{H}$ have models which are algebraic connected curves, defined over the class field extension K_U of F, arising in the proof of Lemma 1.2.23, while the complex manifold $\mathbb{X}(H, U)$ has a model always defined over F.

In the following example we will see how from Definition 1.2.22 we can retrieve the system of Shimura curves defined in the previous subsection.

1.2.4.1 Example: Shimura curves assoicated to Eichler orders

Let N be an integral ideal of F and for every prime ideal $\mathfrak{p}$ let us denote by $N_\mathfrak{p}$ the localization of this ideal in $\mathfrak{p}$: this is the ideal $\mathfrak{p}^{e_\mathfrak{p}}$ in the local ring $R_{F,\mathfrak{p}}$, where $e_\mathfrak{p}$ denotes the exponent of $\mathfrak{p}$ in N. Consider the following open compact subgroup of $G(\mathbb{A}_{fin}) \simeq H^*(\mathbb{A}_{F,fin})$:

$$U_0(N) := \prod_\mathfrak{p} U_\mathfrak{p}(N)^*$$

where

$$U_\mathfrak{p}(N) := \begin{cases} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(R_{F,\mathfrak{p}}) \mid c \in N_\mathfrak{p} \right\}, & \text{if } \mathfrak{p} \nmid D_H \\ R_{F,\mathfrak{p}} + N_\mathfrak{p} \mathcal{O}_{H,\mathfrak{p}}, & \text{if } \mathfrak{p} | D_H. \end{cases}$$

Since H is an indefinite quaternion algebra over F of discriminant D_H and $\mathcal{O}_H$ is an Eichler order of level N, then

$$U_0(N) \cap G(\mathbb{Q})_+ = \{\alpha \in \mathcal{O}_H^* \mid \mathrm{Nm}_{H/F}(\alpha) \equiv 1 \,(\mathrm{mod}\, \mathfrak{u}_0)\} = \Gamma(H, \mathcal{O}_H)$$

(cf. Notation 1.2.4).

Applying Theorem 1.2.15, we find that the double coset $H_+^* \backslash H_\mathbb{A}^* / U_0(N)$ of Lemma 1.2.23 has cardinality

$$h(U_0(N)) = h^+(D_H, N) = h^+$$

and the class field attached to it is

$$K_{U_0(N)} = F^{\mathfrak{u}_0}.$$

Finally, Theorem 1.2.25 gives in this case

$$\mathbb{X}(H, U_0(N)) \simeq \bigcup_{i=1}^{h^+} (\alpha_i^{-1} U_0(N) \alpha_i \cap G(\mathbb{Q})_+) \backslash \mathcal{H},$$

where $\{\alpha_1, \ldots, \alpha_{h^+}\}$ is a system of representatives for the double coset of strict right ideal classes of the order $\mathcal{O}_H$.

If $t := t(D_H, N)$ denotes the number of types of Eichler orders in H of level N and $\{\mathcal{O}_1, \ldots, \mathcal{O}_t\}$ is a set of representatives for these types such that $\mathcal{O}_1 = \mathcal{O}_H$, then two such groups

$$\alpha_\lambda^{-1} U_0(N) \alpha_\lambda \cap G(\mathbb{Q})_+, \quad \alpha_\mu^{-1} U_0(N) \alpha_\mu \cap G(\mathbb{Q})_+$$

are equal if the ideals represented by α_λ and α_μ are bilateral ideals of the same order $\mathcal{O} \in \{\mathcal{O}_1, \ldots, \mathcal{O}_t\}$. In this case

$$\alpha_\lambda^{-1} U_0(N) \alpha_\lambda \cap G(\mathbb{Q})_+ = \alpha_\mu^{-1} U_0(N) \alpha_\mu \cap G(\mathbb{Q})_+ = \Gamma(H, \mathcal{O}).$$

Therefore for every $1 \leq j \leq t$ we find h^+/t Riemann surfaces

$$(\Gamma(D_H, \mathcal{O}_j) \backslash \mathcal{H})_1 = \cdots = (\Gamma(D_H, \mathcal{O}_j) \backslash \mathcal{H})_{h^+/t}$$

whose isomorphic canonical models are all defined over $K_{U_0(N)} = F^{\mathfrak{u}_0}$.

Finally we find the following isomorphism, which imitates the formula of Theorem 1.1.11:

$$\mathbb{X}(H, U_0(N)) \simeq \bigcup_{j=1}^{t} \bigcup_{i=1}^{h^+/t} (\Gamma(D_H, \mathcal{O}_j) \backslash \mathcal{H})_i$$

and the integer h^+/t is the strict bilateral ideal class number of an Eichler order of level N in H.

We have shown that the quotient space $\mathbb{X}(H, U_0(N))$ is the system of canonical models $\mathcal{S}(D_H, N)$ of Shimura curves of discriminant D_H and level N.

1.3 Complex multiplication points on Shimura curves

Let H be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant D_H and let $\mathcal{O}_H$ be an Eichler order over $\mathbb{Z}$ of level N. In this section we will recall the *modular interpretation* that can be given to the complex points of the Shimura curve $X(D_H, N)$, as defined in Section 1.2.

In particular we will fix our attention on those special points that, according to Theorem 1.2.3, provide ray class fields of imaginary quadratic extensions K of $\mathbb{Q}$, namely complex multiplication points. As we have already noted (cf. Remarks 1.2.5 and 1.2.6), these points are algebraic over some ray class field and they are obtained as values of the uniformizing function at some special parameter τ of the quotient space $\Gamma(D_H, N)\backslash\mathcal{H}$, which we will call *complex multiplication parameters* (or CM parameters).

Since Shimura curves are a wide generalization of classical modular curves, the modular interpretation in question can be read without difficulty as a (possible, since others exist) generalization of the modular interpretation of the modular curves $X_0(N)$ in terms of isomorphism classes of elliptic curves with some N-level structure: for this reason, abelian surfaces arising from this modular interpretation will be called *fake elliptic curves*. In this section, we will see that these have a great deal in common with elliptic curves (the *original ones*).

1.3.1 Modular interpretation of Shimura curves

For the basic definitions and properties about abelian varieties and polarized abelian varieties over $\mathbb{C}$, see [LB92].

1.3.1 Definition. Let F be a totally real field of degree $[F : \mathbb{Q}] = n$.

We define a **type over** F to be a datum $\Omega = (H, \Phi, *)$ consisting of:

(i) H an indefinite quaternion algebra over F such that

$$H \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R}) \times \mathbb{H}_{\mathbb{R}}^{n-1},$$

(ii) $\Phi : H \hookrightarrow \mathrm{M}_2(\mathbb{R})$ an embedding of F-algebras,

(iii) $* : \alpha \in H \longmapsto \alpha^* \in H$ a positive involution of the algebra H, i.e. $*$ is an involution such that $\mathrm{Tr}_{H/F}(\alpha\alpha^*)$ is a totally positive element of F for every $\alpha \in H$.

We know from [Shi63, Lemma 1] that the involution $*$ is uniquely determined by an element $\mu \in H$ such that $\mu^2 \in F$ and $\mathrm{Nm}_{F/\mathbb{Q}}(\mu^2) < 0$, once it has been defined as follows: $\alpha^* := \mu^{-1}\bar{\alpha}\mu$ for every $\alpha \in H$.

When the base field is $F = \mathbb{Q}$, such an element can be chosen with the property that $\mu^2 = -D_H$, where D_H denotes the discriminant of the quaternion algebra H.

1.3.2 Definition. Let Ω be a type over F. A triple $\mathscr{P} = (A, \mathcal{L}, \iota)$ is called a **complex abelian variety of type** Ω if it satisfies the following conditions:

(i) A is an abelian variety over $\mathbb{C}$ of dimension $2n$.

(ii) $\iota : H \hookrightarrow \mathrm{End}^0(A)$ is an immersion of F-algebras such that for every $\alpha \in H$ the analytic representation of $\iota(\alpha)$ is the real matrix $\Phi(\alpha)$.

(iii) $\mathcal{L}$ is a polarization of A such that the Rosati involution

$$\phi_{\mathcal{L}} : \mathrm{End}^0(A) \to \mathrm{End}^0(A)$$

induced by $\mathcal{L}$ makes the following diagram commutative:

$$\begin{array}{ccc} H & \xhookrightarrow{\iota} & \mathrm{End}^0(A) \\ {\scriptstyle *}\downarrow & & \downarrow{\scriptstyle \phi_{\mathcal{L}}} \\ H & \xhookrightarrow[\iota]{} & \mathrm{End}^0(A). \end{array}$$

The immersion ι is called a **quaternion multiplication** or also a **QM-structure**.

When $F = \mathbb{Q}$, an abelian surface of a fixed type Ω over $\mathbb{Q}$ is also called a **fake elliptic curve**. One of the aims of the present section is to understand the reasons for this terminology.

1.3.3 Definition. A morphism of abelian varieties of the same type Ω, written

$$(A_1, \mathcal{L}_1, \iota_1) \longrightarrow (A_2, \mathcal{L}_2, \iota_2),$$

is a morphism of the underlying abelian varieties $\varphi : A_1 \to A_2$ such that:

(i) φ preserve the polarizations, i.e. $\varphi^*(\mathcal{L}_1) = \mathcal{L}_2$.

(ii) φ preserves the QM-structure, i.e. the following diagram is commutative

$$\begin{array}{ccc} A_1 & \xrightarrow{\varphi} & A_2 \\ {\scriptstyle \iota(\alpha)}\downarrow & & \downarrow{\scriptstyle \iota(\alpha)} \\ A_1 & \xrightarrow[\varphi]{} & A_2 \end{array}$$

for every $\alpha \in \mathcal{O}_H$.

The following result is [Shi63, Theorems 1 and 2]:

1.3.4 Theorem. *Let us fix a type $\Omega = (H, \Phi, *)$ over $\mathbb{Q}$ and let us denote by $\mathcal{F}(\Omega)$ the family of isomorphism classes of abelian varieties of type Ω.*

Then, for an ideal $\mathfrak{M}$ in H and a non-degenerate alternating form $T : H \times H \to \mathbb{R}$ satisfying $T(\mathfrak{M} \times \mathfrak{M}) \subseteq \mathbb{Z}$, the following map is well-defined:

$$\begin{array}{rccc} \Psi(\mathfrak{M}, T): & \mathcal{H} & \longrightarrow & \mathcal{F}(\Omega) \\ & \tau & \longmapsto & \mathscr{P}_\tau := [A_\tau, \mathcal{L}_\tau, \iota_\tau], \end{array}$$

where $\mathscr{P}_\tau$ is the isomorphism class in $\mathcal{F}(\Omega)$ represented by the following triple:

(*a*) *A fake elliptic curve A_τ whose set of complex points is*

$$\mathbb{C}^2/\Lambda_\tau \simeq A_\tau(\mathbb{C}),$$

with $\Lambda_\tau := \Phi(\mathfrak{M}) \begin{pmatrix} \tau \\ 1 \end{pmatrix}$.

(*b*) *A polarization $\mathcal{L}_\tau$ on A_τ, whose first Chern class is represented by the Hermitian form $\mathscr{H}_\tau$ induced by the alternating form:*

$$\begin{array}{rccc} E_\tau: & \Lambda_\tau \times \Lambda_\tau & \longrightarrow & \mathbb{Z} \\ & \left(\Phi(\alpha)\begin{pmatrix} \tau \\ 1 \end{pmatrix}, \Phi(\beta)\begin{pmatrix} \tau \\ 1 \end{pmatrix}\right) & \longmapsto & T(\alpha, \beta). \end{array}$$

(*c*) *A quaternion multiplication $\iota_\tau : H \hookrightarrow \mathrm{End}^0(A_\tau)$ such that for every $\alpha \in H$, the analytic representation of $\iota_\tau(\alpha)$ is the (real) matrix $\Phi(\alpha)$.*

The map $\Psi(\mathfrak{M}, T)$ is surjective and moreover if $\mathcal{O}_H = \mathcal{O}_\ell(\mathfrak{M})$ denotes the associated left order in H of the ideal $\mathfrak{M}$, then

$$\mathscr{P}_{\tau_1} = \mathscr{P}_{\tau_2} \iff \tau_1 = \gamma\tau_2$$

for some $\gamma \in \Gamma(H, \mathcal{O}_H) = \Phi(\{\alpha \in \mathcal{O}_H^* \mid \mathrm{Nm}(\alpha) > 0\}) \subseteq \mathrm{SL}_2(\mathbb{R})$.

The above result shows that in the data of a type we should also take into account a certain lattice $\mathfrak{M}$ and an alternating form T, this giving rise to the following definition (cf. [Shi67, 4.1]).

1.3.5 Definition. A **PEL-type over** $\mathbb{Q}$ is a datum $\Omega = (H, \Phi, *; T, \mathfrak{M}; V)$ consisting of

(*i*) $(H, \Phi, *)$ a type over $\mathbb{Q}$, as in Definition 1.3.1,

(*ii*) $\mathfrak{M}$ an ideal of H obtained from the datum $(H, \Phi, *)$, as in the proof of Theorem 1.3.4,

(*iii*) $T : H \times H \to \mathbb{R}$ a real non-degenerate alternating form of the algebra H such that $T(\mathfrak{M} \times \mathfrak{M}) \subseteq \mathbb{Z}$,

(*iv*) $V = (v_1, \ldots, v_s)$ be a vector of finitely many quaternion classes $v_i \in \mathfrak{M} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathfrak{M} \simeq H/\mathfrak{M}$.

1.3.6 Definition. Let $\Omega = (H, \Phi, *; T, \mathfrak{M}; V)$ be a PEL-type and let $\mathcal{O}_H$ denote the left order of the ideal $\mathfrak{M}$ in H.

A **complex abelian surface of PEL-type** Ω is a triple $(A, \mathcal{L}, \iota, W)$ such that:

(a) $(A, \iota, \mathcal{L})$ is an abelian surface of type $(H, \Phi, *)$ satisfying the following additional properties:

(i) The immersion $\iota : H \hookrightarrow \mathrm{End}^0(A)$ restricts to an immersion of rings

$$\iota_{|\mathcal{O}_H} : \mathcal{O}_H \hookrightarrow \mathrm{End}(A)$$

such that the $\mathbb{Z}$-lattice $H_1(A, \mathbb{Z})$, regarded as a left $\mathfrak{M}$-module, is isomorphic to $\mathfrak{M}$.

(ii) The first Chern class of the polarization $\mathcal{L}$ is represented by a Hermitian form induced by the alternating form T, as in Theorem 1.3.4.

(b) $W = (w_1, \ldots, w_s)$ is a vector of complex points of A such that if $V = (v_1, \ldots, v_s)$ and $\xi : \mathbb{C}^2/\Lambda \simeq A(\mathbb{C})$, then $W = (\xi(v_1), \ldots, \xi(w_s))$.

A type $\Omega = (H, \Phi, *; T, \mathfrak{M}; V)$ as the one in Definition 1.3.6 is called a PEL-type structure since, as is clear, it fixes the following structure on the abelian variety:

1. The polarization (P), by T.

2. The endomorphism ring (E), by $\mathfrak{M}$.

3. The level points (L), by V.

1.3.7 Remark. From the definition of the map $\Psi(\mathfrak{M}, T)$ in Theorem 1.3.4, we can see that if we change the ideal $\mathfrak{M}$ for the ideal $\mathfrak{M}q$ which represents the same class in $\mathcal{O}_\ell(\mathfrak{M})/H^*$, then

$$\Psi(\mathfrak{M}, T)(\tau) = \Psi(\mathfrak{M}', T)(\tau)$$

for every $\tau \in \mathcal{H}$ (cf. [Shi63, Proposition]).

If in addition we choose the ideal $\mathfrak{M}$ to have as associated order on the left $\mathcal{O}_\ell(\mathfrak{M}) = \mathcal{O}_H$, an Eichler order of level N, then we can take the ideal $\mathfrak{M} = \mathcal{O}_\ell(\mathfrak{M})$ (since the strict ideal class number is in this case $h^+(D_H, N) = h^+_{\mathbb{Q}} = 1$).

This is consistent with definitions and notations of [BG05].

1.3.8 Definition. Let A be an abelian variety and let $\mathcal{O}_H$ be an order in an indefinite quaternion algebra H over $\mathbb{Q}$.

We say that A has **quaternionic multiplication by** $\mathcal{O}_H$ (also **QM by** $\mathcal{O}_H$) if there exists an embedding of rings $\iota : \mathcal{O}_H \hookrightarrow \mathrm{End}(A)$. This embedding, as well as its rational extension $H \hookrightarrow \mathrm{End}^0(A)$, is sometimes referred to as the **QM-structure**.

The following result gives a first idea of what abelian surfaces of PEL-type over $\mathbb{Q}$ have in common with elliptic curves, namely the unicity of the polarization.

1.3.9 Proposition. *Let $\Omega = (H, \Phi, *; T, \mathcal{O}_H; V)$ be a PEL-type over $\mathbb{Q}$ and let (A, ι) be a pair formed by a complex abelian surface A and the immersion of $\mathbb{Q}$-algebras*

$$\begin{array}{rccc} \iota: & H & \longrightarrow & \mathrm{End}^0(A) \\ & \alpha & \longmapsto & \Phi(\alpha). \end{array}$$

Then there exists a unique polarization $\mathcal{L}$ such that $\mathscr{P} = (A, \mathcal{L}, \iota)$ is an abelian surface of PEL-type Ω.

Proof. Let Λ be a lattice in $\mathbb{C}^2$ such that

$$\mathbb{C}^2/\Lambda \simeq A(\mathbb{C}).$$

Since A has quaternion multiplication by the order $\mathcal{O}_H$, then V is a H-module.

Let us fix an element $\mu \in \mathcal{O}_H$ such that $\mu^2 = -D_H$ and let us define

$$E : (v, w) \in \mathbb{C}^2 \times \mathbb{C}^2 \longmapsto \mathrm{Tr}_{H/\mathbb{Q}}(v\mu w^*) \in \mathbb{C}$$

On the other side, we have the chain of isomorphisms of $\mathbb{C}$-vector spaces

$$\mathbb{C}^2 \simeq H \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R}),$$

since $\mathrm{M}_2(\mathbb{R})$ has a complex structure given by a matrix $\gamma \in \mathrm{SL}_2(\mathbb{R})$ such that $\gamma^2 = -\mathrm{I}_2$: such a matrix has to be conjugated to the matrix $\left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right)$.

Therefore we can see that

$$E(iv, iw) = E(v\gamma, w\gamma) = \mathrm{Tr}(v\gamma\overline{w\gamma}\mu) = \mathrm{Tr}(v\gamma\gamma^{-1}w\mu) = E(v, w).$$

and we can define the polarization $\mathcal{L}$ such that its first Chern class is represented by the Hermitian form

$$\mathscr{H} : (v, w) \in \mathbb{C}^2 \times \mathbb{C}^2 \longmapsto E(iv, w) + iE(v, w) \in \mathbb{C}.$$

It is an easy computation to prove that the Rosati involution induced by this polarization coincide with the involution $*$ defined by the quaternion μ.

We have to prove that $\mathcal{L}$ is unique. The Hermitian form $\mathscr{H}$ defined above, when restricted to $H \hookrightarrow V$, induced a non-degenerate pairing

$$\mathscr{H} : H \times H \longrightarrow \mathbb{Q}.$$

Therefore the map $\alpha \in H \longmapsto E(1, \alpha) \in \mathbb{Q}$ is a linear map and so it has to be $E(1, \alpha) = \mathrm{Tr}_{H/\mathbb{Q}}(q\alpha\mu\alpha^*)$, for some q. But since E is non-degenerate, then $q \in \mathbb{Q}_{>0}$ and so it induces the same polarization $\mathcal{L}$. □

Proposition 1.3.9 together with Remark 1.3.7, says that in a PEL-type over $\mathbb{Q}$ the information about the alternating form and the ideal is superfluous, since these data are uniquely determined by the others.

1.3.10 Remark. If Ω is a PEL-type over $\mathbb{Q}$, then after Proposition 1.3.9 it is clear that every morphism preserving the QM-structure and the level is actually a morphism of abelian varieties of PEL-type Ω.

1.3.11 Corollary. *Let $\Omega = (H, \Phi, *; T, \mathcal{O}_H; V)$ be a fixed PEL-type over $\mathbb{Q}$, such that the algebra H has discriminant D_H and $\mathcal{O}_H$ is an Eichler order of level N in H, and let $X(D_H, N)$ be the canonical model for the Shimura curve associated to the order $\mathcal{O}_H$.*

Then the set of complex points of the Shimura curve $X(D_H, N)$ is a coarse moduli-space for isomorphism classes of abelian varieties of PEL-type Ω.

PROOF. Since the set of complex points $X(D_H, N)(\mathbb{C})$ is analytically isomorphic to the compact Riemann surface $\Gamma(D_H, N)\backslash\mathcal{H}$ (cf. Theorem 1.2.3), where $\Gamma(D_H, N) = \Phi(\mathcal{O}^*_{H,+})$, the result follows from Theorem 1.3.4 taking the ideal $\mathfrak{M} = \mathcal{O}_H$. □

1.3.2 Abelian varieties with complex multiplication

1.3.12 Definition. Let $\Omega = (H, \Phi, *; T, \mathcal{O}_H; V)$ be a PEL-type. Let $(A, \mathcal{L}, \iota)$ be a fake elliptic curve of PEL-type Ω and let $\mathcal{O}_K$ be an order in an imaginary quadratic field K.

We say that $(A, \mathcal{L}, \iota)$ has **complex multiplication by $\mathcal{O}_K$** (also **CM by $\mathcal{O}_K$**) if there exists an optimal embedding $\varphi : \mathcal{O}_K \hookrightarrow \mathcal{O}_H$ such that

$$\mathrm{End}(A, \mathcal{L}, \iota) = \iota(\varphi(\mathcal{O}_K)).$$

In particular $\mathrm{End}^0(A, \mathcal{L}, \iota) \simeq K$ and we also say that $(A, \mathcal{L}, \iota)$ has CM by K.

The following lemma, which is a direct consequence of *Poincaré's complete reducibility theorem* (cf. [Mum08, IV.19 Theorem 1, Corollaries 1 and 2]) is of fundamental importance in the study of the endomorphism algebras of abelian varieties.

1.3.13 Lemma. *If A is isogenous to a square of an elliptic curve E, i.e. $A \sim E^2$, then $D := \mathrm{End}^0(E)$ is a division $\mathbb{Q}$-algebra and there is an isomorphism of $\mathbb{Q}$-algebras $\mathrm{End}^0(A) \simeq \mathrm{M}_2(D)$.* □

1.3.14 Proposition. *Let $\Omega = (H, \Phi, *; T, \mathcal{O}_H; V)$ be a PEL-type. Let $(A, \mathcal{L}, \iota)$ be a fake elliptic curve of PEL-type Ω and let $\mathcal{O}_K$ be an imaginary quadratic order in an imaginary quadratic field K*

The following conditions are equivalent:

(i) $(A, \mathcal{L}, \iota)$ *is CM by* K.

(ii) $\mathrm{End}^0(A) \simeq \mathrm{M}_2(K)$.

(iii) A *is isogenous to a square of an elliptic curve* E *with CM by* K.

(iv) H *is not isomorphic to* $\mathrm{End}^0(A)$.

PROOF. If $(A, \mathcal{L}, \iota)$ is CM by K then $\mathrm{End}^0(A, \mathcal{L}, \iota) \simeq K$ and since

$$\mathrm{End}^0(A, \mathcal{L}, \iota) = \{\psi \in \mathrm{End}^0(A) \mid \psi\Phi(\alpha) = \Phi(\alpha)\psi \ \forall\, \alpha \in \mathcal{O}_H\}$$

then the center of $\mathrm{End}^0(A)$ is isomorphic to K and so $\mathrm{End}^0(A) \simeq \mathrm{M}_2(K)$.

Viceversa, if $\mathrm{End}^0(A) \simeq \mathrm{M}_2(K)$ then its center is K and so $\mathrm{End}^0(A, \mathcal{L}, \iota) \simeq K$. This proves the equivalence between (i) and (ii).

Let us assume (ii). If the abelian surface A were simple, then $\mathrm{End}^0(A)$ would be a division algebra over $\mathbb{Q}$ (because in this case every isogeny $A \to A$ would be invertible) and so it could not be isomorphic to the matrix algebra $\mathrm{M}_2(K)$. Hence A cannot be simple in the category of abelian surfaces with isogenies as morphisms; i.e. $A \sim E_1 \times E_2$ for some elliptic curves E_1, E_2, and $\mathrm{End}^0(A) \simeq \mathrm{End}^0(E_1) \times \mathrm{End}^0(E_2)$ has to be the matrix algebra $\mathrm{M}_2(K)$ (by Lemma 1.3.13), so E_1 and E_2 have to be isogenous to the same elliptic curve E, with CM by K.

The viceversa is immediate. This proves the equivalence between (ii) and (iii).

It remains to prove that (iii) is equivalent to (iv). One of the two implications is trivial after Lemma 1.3.13. Let us assume that $H \not\simeq \mathrm{End}^0(A)$ and A is simple. Since A is assumed to be simple, again $\mathrm{End}^0(A)$ is a division algebra and then $H_1(A, \mathbb{Q})$ is a $\mathrm{End}^0(A)$-free module, let us say of dimension d. Hence $4 = \dim_{\mathbb{Q}}(H_1(A, \mathbb{Q})) = d[\mathrm{End}^0(A) : \mathbb{Q}] = 4d$ and so $d = 1$. Therefore $\mathrm{End}^0(A) \simeq H$ which is an absurd. This concludes the proof of the equivalences. □

Fake elliptic curves with complex multiplication correspond in the bijection of Theorem 1.3.4 to some special parameter which we will call the complex multiplication parameter. Here is the exact definition which should be compared with the one in Theorem 1.2.3.

1.3.15 Definition. Let H be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant D_H and let $\mathcal{O}_H$ be an Eichler order over $\mathbb{Z}$ of level N. Let K be an imaginary quadratic field such that there is an embedding $K \hookrightarrow H$ and let $\mathcal{O}_K$ be a $\mathbb{Z}$-order in K.

A parameter $\tau \in \Gamma(D_H, N)\backslash\mathcal{H}$ is said to be a **complex multiplication parameter by $\mathcal{O}_K$** (or **CM by $\mathcal{O}_K$**) if there exists an optimal embedding $\varphi : \mathcal{O}_K \hookrightarrow \mathcal{O}_H$ such that τ is fixed point for all the elliptic transformations represented by $\gamma \in \Phi(\varphi(\mathcal{O}_K)) \subseteq \mathrm{M}_2(\mathbb{R})$.

1.3.16 Theorem. *Let $\Omega = (H, \Phi, *; T, \mathcal{O}_H; V)$ be a PEL-type over $\mathbb{Q}$. A fake elliptic curve $\mathscr{P} = (A, \mathcal{L}, \iota)$ of PEL-type Ω is CM by an imaginary quadratic order $\mathcal{O}_K$ iff $\mathscr{P} = \mathscr{P}_\tau$ for some parameter $\tau \in \Gamma(D_H, N)\backslash\mathcal{H}$ which is CM by the order $\mathcal{O}_K$.*

PROOF. Let us assume that $\tau \in \Gamma(D_H, N)\backslash\mathcal{H}$ is the fixed point of the optimal embedding $\varphi : \mathcal{O}_K \hookrightarrow \mathcal{O}_H$ and $(A_\tau, \mathcal{L}_\tau, \iota_\iota)$ is the associated fake elliptic curve as constricted in Theorem 1.3.4.

Then let us consider the following map

$$\begin{array}{ccc} \varphi(\mathcal{O}_K) & \longrightarrow & \{\lambda \in \mathbb{C}^* \mid \lambda\Lambda_\tau \subseteq \Lambda_\tau\} \\ \alpha & \longmapsto & \lambda_\alpha \end{array}$$

such that

$$\Phi(\alpha)\begin{pmatrix}\tau\\1\end{pmatrix} = \lambda_\alpha \begin{pmatrix}\tau\\1\end{pmatrix}.$$

It is easy to prove that this induces an isomorphism of ring $\mathcal{O}_K \simeq \mathrm{End}(A_\tau, \mathcal{L}_\tau, \iota_\tau)$. □

The following result is [SM74, Theorem 4.1]

1.3.17 Theorem. *Let A be a complex abelian surface. Then the following conditions are equivalent:*

(i) A is isogenous to the square of an elliptic curve E with complex multiplication.

(ii) A is isomorphic to a product $E_1 \times E_2$ of isogenous elliptic curves with complex multiplication.

1.3.18 Remark. The elliptic curves E_1, E_2 in the decomposition of A are CM by the same quadratic field K but, in general, not by the same quadratic order, as we will see in some examples.

1.3.19 Corollary. *Let $\mathcal{O}_H$ be an order in an indefinite quaternion algebra H over $\mathbb{Q}$ and let $\mathcal{O}_K$ be an order in an imaginary quadratic field K.*

If A is a complex abelian surface with QM by $\mathcal{O}_H$ and CM by $\mathcal{O}_K$, then A is isomorphic to a product $E_1 \times E_2$ of isogenous elliptic curves, both with CM by the field K.

1.3.20 Corollary. *Let $\Omega = (H, *, \Phi; T, \mathcal{O}_H; V)$ be a PEL-type over $\mathbb{Q}$ such that $\mathcal{O}_H$ is an Eichler order of level N in H, and let $\tau \in \mathcal{H}$ be a CM parameter in $\Gamma(D_H, N)\backslash\mathcal{H}$.*

If $\mathscr{P}_\tau = [A_\tau, \mathcal{L}_\tau, \iota_\tau]$ is the class of abelian surfaces of PEL-type Ω corresponding to the CM parameter τ, then there exist CM parameters $\tau^{(1)}, \tau^{(2)} \in \Gamma_0(N)\backslash\mathcal{H}$ such that

$$\mathscr{P}_\tau = [E_{\tau^{(1)}} \times E_{\tau^{(2)}}, \mathcal{L}_{(\tau^{(1)},\tau^{(2)})}, \iota_{(\tau^{(1)},\tau^{(2)})}].$$

where $E_{\tau^{(i)}} := \mathbb{C}/\langle \tau^{(i)}, 1\rangle$, for $i = 1, 2$.

1.3.3 Shioda-Mitani decompositions

In [BG05] some examples of abelian surfaces associated to complex multiplication points on Shimura curves are computed. Specifically, given a complex multiplication parameter $\tau \in \Gamma(D_H, N)\backslash\mathcal{H}$ a point $Z_\tau \in \mathcal{H}_2$, which represents the abelian surface A_τ on the Igusa three-fold $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$, is computed. Moreover the PEL-type is used in order to compute equations of genus 2 curves which have these abelian surfaces as Jacobians.

We examine these examples further and compute, with the help of Magma (cf. [BCP97]), for each one of these abelian surfaces a decomposition into products of elliptic curves.

We now explain briefly how to apply the method presented in [SM74] to a polarized abelian surface $A = (\mathbb{C}^2/\Lambda, \mathcal{L})$ over $\mathbb{C}$.

Recall that we have the following exact sequence of sheaves:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{j} \mathcal{O}_A \xrightarrow{\exp} \mathcal{O}_A^* \longrightarrow 0$$

which induces the cohomological sequence

$$H^1(A, \mathcal{O}_A^*) \xrightarrow{\delta} H^2(A, \mathbb{Z}) \xrightarrow{j^*} H^2(A, \mathcal{O}_A)$$

and the Néron-Severi group of A can be defined as $S_A := \mathrm{Im}\delta = \mathrm{Ker}j^*$, and its rank $\rho(A) := \mathrm{rank}(S_A)$ is called the Picard number of A.

When the group $H^2(A, \mathcal{O}_A)$ is identified with $\mathbb{C}$, the map j^* is called the period map of A and is denoted by p_A. The image of p_A is called the group of transcendental cocycles of A and is denoted by T_A.

The following proposition is [SM74, Proposition 1.1].

1.3.21 Proposition. *If A is an abelian surface over $\mathbb{C}$ with Picard number $\rho(A) = 4$, then T_A is an euclidean lattice in $\mathbb{C}$ and $\mathbb{C}/T_A$ is a complex torus.*

Once we have written the set of complex points of A as $\mathbb{C}^2/\Lambda \simeq A(\mathbb{C})$, for some lattice $\Lambda \subseteq \mathbb{C}^2$, we have the following well known identifications:

$$\begin{aligned} &H_1(A,\mathbb{Z}) \simeq \Lambda \\ &H^1(A,\mathbb{Z}) \simeq \Lambda^* := \mathrm{Hom}(\Lambda,\mathbb{Z}) \\ &H^2(A,\mathbb{Z}) \simeq \textstyle\bigwedge^2(\Lambda^*). \end{aligned}$$

Let $\{v_1,v_2,v_3,v_4\}$ be a basis of Λ and $\{v_1^*,v_2^*,v_3^*,v_4^*\}$ the dual basis of Λ^* such that $v_i^*(v_j)=\delta_{ij}$. Then $\{v_i^* \wedge v_j^* \mid 1 \le i < j \le 4\}$ is a $\mathbb{Z}$-basis for $H^2(A,\mathbb{Z}) \simeq \mathbb{Z}^6$ and also a $\mathbb{C}$-basis for $H^2(A,\mathbb{C}) := H^2(A,\mathbb{Z}) \otimes \mathbb{C}$.

Now, as the period map p_A is defined as an element of $\mathrm{Hom}(H^2(A,\mathbb{Z}),\mathbb{C})$, then it can be represented by a 1×6 complex-matrix with respect to the given basis of $H^2(A,\mathbb{Z})$ and the canonical basis of $\mathbb{C}$. It is proved in [Shi78, p.53] that this matrix is the vector $(\mathrm{Det}(v_i,v_j))_{i<j} \in \mathrm{M}_{1\times 6}(\mathbb{C})$ and then so it follows that:

$$T_A \simeq \langle \mathrm{Det}(v_i,v_j) \mid \ 1 \le i < j \le 4 \rangle.$$

1.3.22 Theorem. *Let A be an abelian surface with Picard number $\rho(A)=4$ and let*

$$\tau^{(1)} = \frac{-b+\sqrt{b^2-4ac}}{2a} \in \mathcal{H}$$

such that $\langle \tau^{(1)}, 1\rangle$ is the euclidean lattice T_A associated to A. Let us define

$$\tau^{(2)} := \frac{-b+\sqrt{b^2-4ac}}{a}$$

Then there is an isomorphism of complex abelian surfaces $A \simeq E_{\tau^1} \times E_{\tau_2}$, where $E_{\tau^{(i)}}$ is the elliptic curve such that

$$E_{\tau^{(i)}}(\mathbb{C}) \simeq \mathbb{C}/\langle 1, \tau^{(i)}\rangle.$$

Following this description we want to compute "Shioda-Mitani decompositions" for the CM abelian surfaces of [BG05], together with an isomorphism over $\mathbb{C}$, and decide whether or not the polarization induced by the isomorphism is the *product polarization.*

Just to fix some notations, we recall the following elementary proposition (cf. [LB92, Proposition 2.3]).

1.3.23 Proposition. *Let A_1, A_2 be two complex abelian varieties of dimension g with big period matrices respectively $\Pi_1, \Pi_2 \in \mathrm{M}_{g\times 2g}(\mathbb{C})$.*

If $\psi : A_1 \to A_2$ is a morphism, then there exist matrices $M_{\psi,rat} \in \mathrm{M}_{2g}(\mathbb{Z})$, $M_{\psi,an} \in \mathrm{M}_g(\mathbb{C})$ such that

$$M_{\psi,an}\Pi_1 = \Pi_2 M_{\psi,rat}.$$

□.

We say that $M_{\psi,rat}$ (resp. $M_{\psi,an}$) is the **rational representation** (resp. **analytical representation**) of the morphism ψ.

Now, the following easy lemma, whose proof is straightforward by applying Proposition 1.3.23, will be useful to understand the examples below.

1.3.24 Lemma. (*i*) *If* $Z = \Omega_2^{-1}\Omega_1$, *then there is an isomorphism*

$$\psi : \mathbb{C}^2/\langle \Omega_1, \Omega_2 \rangle \simeq \mathbb{C}^2/\langle Z, I_2 \rangle$$

such that $M_{\psi,rat} = I_4$ *and* $M_{\psi,an} = \Omega_2^{-1}$.

(*ii*) *If* Λ, Λ' *are two lattices of* $\mathbb{C}^2$ *such that* $\Lambda = \Lambda'$, *then there is an isomorphism*

$$\psi : \mathbb{C}^2/\Lambda \simeq \mathbb{C}^2/\Lambda'$$

such that $M_{\psi,rat}$ *is the base change matrix from* Λ *to* Λ' *and* $M_{\psi,an} = I_2$.

1.3.3.1 Modular curves as Shimura curves

In the following example we show how, among the PEL-types defined in the previous section, we can find a moduli problem which gives rise to the modular curve $X_0(1)$. The moduli problem is a "double copy" of the usual modular problem defining classical modular curves.

Let us take the following PEL-type $\Omega = (H, \Phi, *; T, \mathcal{O}_H; V)$ over $\mathbb{Q}$ given by:

$$H = \left(\tfrac{1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, k \rangle,\ D_H = 1,$$

$$\begin{array}{rccc} \Phi : & H & \longrightarrow & \mathrm{M}_2(\mathbb{R}) \\ & x + yi + zj + tk & \longmapsto & \begin{pmatrix} x+y & z+t \\ -(z-t) & x-y \end{pmatrix}, \end{array}$$

$$\begin{array}{ccc} H & \longrightarrow & H \\ \alpha & \longmapsto & \alpha^* := \mu^{-1}\bar{\alpha}\mu \end{array} \quad \text{with } \mu = -j,$$

$$\mathcal{O}_H = \langle (-j+k)/2, (1-i)/2, (1+i)/2, (j+k)/2 \rangle_{\mathbb{Z}},$$

$$\begin{array}{rccc} T: & \mathcal{O}_H \times \mathcal{O}_H & \to & \mathbb{Z} \\ & (\alpha, \beta) & \longmapsto & \mathrm{Tr}(j\alpha\bar{\beta}) \end{array}.$$

Observe that Φ induces an isomorphism $H \simeq \mathrm{M}_2(\mathbb{Q})$ and that the basis of $\mathcal{O}_H \simeq \mathrm{M}_2(\mathbb{Z})$ is symplectic with respect to T. In fact

$$\Phi(\mathcal{O}_H) = \langle \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \rangle = \mathrm{M}_2(\mathbb{Z}).$$

For every $\tau \in \Phi(\mathcal{O}_{H,+}^*)\backslash\mathcal{H} = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ we can build the uniformization map $\Psi(\mathcal{O}_H, T)$ of Theorem 1.3.4.

Actually $\mathscr{P}_\tau = [A_\tau, \mathcal{L}_\tau, \iota_\tau]$ where the abelian surface A_τ is uniformized on $\mathbb{C}$ by the lattice

$$\Lambda_\tau = \langle \begin{pmatrix} \tau \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \tau \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rangle$$

the polarization $\mathcal{L}_\tau$ is the one represented by the Hermitian form $\mathscr{H}_\tau : \mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{C}$ of matrix (in the canonical basis)

$$\mathscr{H}_\tau = \begin{pmatrix} \frac{1}{\mathrm{Im}(\tau)} & 0 \\ 0 & \frac{1}{\mathrm{Im}(\tau)} \end{pmatrix},$$

and the QM-structure is given by the immersion of rings ι such that the analytic representation of the endomorphism

$$\iota_\tau(a_0\frac{-j+k}{2} + a_1\frac{1-i}{2} + a_2\frac{1+i}{2} + a_3\frac{j+k}{2}) \in \mathrm{End}(A_\tau)$$

is the matrix

$$\begin{pmatrix} a_0 & a_1 \\ a_2 & a_3 \end{pmatrix}.$$

Clearly, if E_τ is the elliptic curve such that $\mathbb{C}/\langle\tau, 1\rangle \simeq E_\tau(\mathbb{C})$, then there is an isomorphism of abelian surfaces over $\mathbb{C}$

$$\psi : A_\tau \simeq E_\tau \times E_\tau.$$

Moreover if $\mathcal{L}_{E_\tau}$ denotes the unique polarization of E_τ, then the above isomorphism is an isomorphism of polarized abelian varieties, i.e. $\psi^*(\mathcal{L}) = \mathcal{L}_{E_\tau} \otimes \mathcal{L}_{E_\tau}$.

Hence in this case there is an immersion

$$\begin{array}{rcl} \mathcal{H} & \longrightarrow & \mathcal{H}_2 \\ \tau & \longmapsto & \begin{pmatrix} \tau & 0 \\ 0 & \tau \end{pmatrix}, \end{array}$$

which induces the immersion of the Shimura curve inside the Igusa three-fold:

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \hookrightarrow \mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2.$$

1.3.3.2 Shimura curve of discriminant $D_H = 10$

We consider the PEL-type $\Omega = (H, \Phi, *; T, \mathcal{O}_H; V)$ over $\mathbb{Q}$ given as follows:

$$H = \left(\tfrac{2,5}{\mathbb{Q}}\right) = \langle 1, i, j, k\rangle, D_H = 10,$$

$$\begin{array}{rccc} \Phi: & H & \longrightarrow & \mathrm{M}_2(\mathbb{R}) \\ & x + yi + zj + tk & \longmapsto & \begin{pmatrix} x + y\sqrt{2} & 5(z - t\sqrt{2}) \\ x - \sqrt{2}y & \end{pmatrix}, \end{array}$$

$$\begin{array}{ccc} H & \longrightarrow & H \\ \alpha & \longmapsto & \alpha^* := \mu^{-1}\bar{\alpha}\mu \end{array} \text{ with } \mu = -k,$$

$$\mathcal{O}_H = \langle 1, i, (1+j)/2, (i+k)/2\rangle_{\mathbb{Z}}$$

$$\begin{array}{rccc} T: & \mathcal{O}_H \times \mathcal{O}_H & \to & \mathbb{Z} \\ & (\alpha, \beta) & \longmapsto & \mathrm{Tr}(-k\alpha\bar{\beta}) \end{array}.$$

We consider the following parameters, which are CM by the maximal order $\mathcal{O}_K = \mathbb{Z}[\sqrt{-10}]$ of $K = \mathbb{Q}(\sqrt{-10})$:

$$\tau_1 = \frac{(3\sqrt{5} - 2\sqrt{10})i}{5}, \quad \tau_2 = \frac{\sqrt{5}i}{5}.$$

and the corresponding abelian surfaces of PEL-type Ω are the following:

$$A_{\tau_i}(\mathbb{C}) \simeq \frac{\mathbb{C}^2}{\langle Z_i, I_2\rangle},\ i = 1, 2.$$

where

$$Z_1 = \begin{pmatrix} \frac{3\sqrt{10}}{2}i & -\frac{1}{2} + \sqrt{10}i \\ -\frac{1}{2} + \sqrt{10}i & \frac{3\sqrt{10}i}{4} \end{pmatrix}, \quad Z_2 = \begin{pmatrix} \frac{\sqrt{10}}{2}i & -\frac{1}{2} \\ -\frac{1}{2} & \frac{\sqrt{10}}{4}i \end{pmatrix}.$$

The two points $Z_1, Z_2 \in \mathcal{H}_2$ are obtained after computing a symplectic basis of the order $\mathcal{O}_H$ with respect to the Hermitian form induced by T. This

implies that the Hermitian form has matrix $(\operatorname{Im} Z_i)^{-1}$ in the canonical basis of $\mathbb{C}^2$ and that the class $[Z_i] \in \mathrm{Sp}_4(\mathbb{Z})/\mathcal{H}_2$ represents the polarized abelian surface A_{τ_i} on the Igusa three-fold $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}_2$.

Since A_1 and A_2 are isomorphic as principle polarized abelian surfaces (cf. [Rot04] for the theoretical explanation and [BG05], where the Igusa invariants are computed), in order to find a "Shioda-Mitani decomposition" for these abelian surfaces it is sufficient to consider one of them. Let us take the abelian surface A_2.

We compute the group T_{A_2} of transcendental cocycles of A_2:

$$T_{A_{\tau_2}} = \langle 1, -\frac{1}{2}, \frac{\sqrt{10}}{4}i, -\frac{\sqrt{10}}{2}i, -\frac{3}{2}\rangle = \langle -\frac{1}{2}, \frac{\sqrt{10}i}{4}\rangle.$$

We obtain the following elliptic curve $E_{\tau_2^{(1)}}$ such that

$$\frac{\mathbb{C}}{\langle 1, \frac{\sqrt{10}i}{2}\rangle} \simeq E_{\tau_2^{(1)}}(\mathbb{C}),$$

which is CM by the maximal order $\mathbb{Z}[\sqrt{-10}]$.

So $\tau_2^{(1)} = \dfrac{\sqrt{10}i}{2} = \dfrac{-b+\sqrt{D_K}}{2a}$ and this implies $a = 2, b = 0, c = 5$.

Therefore $\tau_2^{(2)} = \sqrt{10}i$ and this gives rise to the elliptic curve $E_{\tau_2^{(2)}}$ such that

$$\frac{\mathbb{C}}{\langle 1, \sqrt{10}i\rangle} \simeq E_{\tau_2^{(2)}}(\mathbb{C}),$$

which is CM by the maximal order of K.

The two elliptic curves are not isomorphic, since their uniformizing lattices $\langle \tau_2^{(1)}, 1\rangle, \langle \tau_2^{(2)}, 1\rangle$ represent different ideal classes inside the ideal class group of K, which is cyclic of order 2.

So there is an isomorphism of polarized abelian varieties

$$\psi : (A_{\tau_2}, \mathcal{L}_{\tau_2}) \xrightarrow{\sim} (E_{\tau_2^1} \times E_{\tau_2^2}, \psi^*\mathcal{L})$$

The abelian surface $E_{\tau_2^{(1)}} \times E_{\tau_2^{(2)}}$, as a complex manifold, is isomorphic to the 2-dimensional torus

$$\frac{\mathbb{C}^2}{\Lambda_{(\tau_2^{(1)}, \tau_2^{(2)})}}$$

where

$$\Lambda_{(\tau_2^{(1)}, \tau_2^{(2)})} := \langle \begin{pmatrix} \tau_2^{(1)} & 0 \\ 0 & \tau_2^{(2)} \end{pmatrix}, I_2 \rangle$$

We find that an isomorphism ψ is the one having analytic and rational representation given by the following matrices:

$$M_{\psi,rat} = \begin{pmatrix} -4 & 2 & -1 & 2 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & -3 & 3 \\ -6 & 3 & -1 & 2 \end{pmatrix}, \quad M_{\psi,an} = \begin{pmatrix} -3 - \dfrac{\sqrt{10}}{2}i & 3 + \sqrt{10}i \\ -1 + \sqrt{10}i & 2 - \sqrt{10}i \end{pmatrix}.$$

It easy to see that the base of the lattice $\Lambda_{(\tau_2^1,\tau_2^2)}$ is not symplectic with respect to the Hermitian form induced by the isomorphism ψ.

This can be seen by direct calculation of the Hermitian form induced by the isomorphism ψ or by taking a fundamental domain in $\mathcal{H}_2$ for the action of $\mathrm{Sp}_4(\mathbb{Z})$ (cf. [Got59] for explicit inequalities defining this) and observing that the point $\begin{pmatrix} \tau_2^{(1)} & 0 \\ 0 & \tau_2^{(2)} \end{pmatrix} \in \mathcal{H}_2$ is on the boundary of this fundamental domain, while Z_2 is in its interior.

We can compute a symplectic base with respect to the induced Hermitian form and we obtain the following chain of isomorphisms of complex torus:

$$\mathbb{C}^2/\langle Z_2, I_2\rangle \xrightarrow{\psi} \mathbb{C}^2/\Lambda_{(\tau_2^{(1)},\tau_2^{(2)})} \xrightarrow{\psi_2} \mathbb{C}^2/\langle \Omega_1, \Omega_2\rangle \xrightarrow{\psi_3} \mathbb{C}^2/\langle \Omega_2^{-1}\Omega_1, I_2\rangle$$

where

$$\Omega_1 = \begin{pmatrix} 1 & -1468 - \dfrac{195\sqrt{10}}{2}i \\ 9\sqrt{10}i & 1 + 438\sqrt{10}i \end{pmatrix}, \quad \Omega_2 = \begin{pmatrix} 7 + \dfrac{\sqrt{10}}{2}i & 30 + 2\sqrt{10}i \\ -7\sqrt{10}i & -9\sqrt{10}i \end{pmatrix}.$$

The isomorphism ψ_2 is the one whose rational representation is the base change from $\Lambda_{(\tau_2^{(1)},\tau_2^{(2)})}$ to $\langle \Omega_1, \Omega_2\rangle$ and the isomorphism ψ_3 is the "multiplication by $\Omega_2^{-1} \in \mathrm{GL}_2(\mathbb{C})$".

Therefore, applying Lemma 1.3.24, we find that the point $\Omega_2^{-1}\Omega_1 \in \mathcal{H}_2$ is $\mathrm{Sp}_4(\mathbb{Z})$-equivalent to Z_2 through the matrix obtained as product

$$\begin{aligned} &M_{\psi_3,rat}\, M_{\psi_2,rat}\, M_{\psi,rat} = \\ &\quad = I_4 \begin{pmatrix} -147 & -2 & 19 & 103 \\ 0 & 0 & 0 & 1 \\ -279 & -4 & 36 & 195 \\ 70 & 1 & -9 & 0 \end{pmatrix} \begin{pmatrix} -4 & 2 & -1 & 2 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & -3 & 3 \\ -6 & 3 & -1 & 2 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Z}). \end{aligned}$$

Finally, the analytic representation of this isomorphism is

$$M_{\psi_3,an}\, M_{\psi_2,an}\, M_{\psi,an} = \Omega_2^{-1} I_2 M_{\psi,an}.$$

The class of binary quadratic forms associated to the parameter τ_2 is represented by the form

$$f_{\tau_2} = (10\sqrt{2}, 0, 2\sqrt{2}) \in \mathcal{H}^*_\infty(\mathbb{Z} + 2\mathcal{O}_H, -40),$$

with notations as in Chapter 4.

The classes of binary quadratic forms associated to the parameters $\tau_2^{(1)}, \tau_2^{(2)}$ are represented by

$$f_{\tau_2^{(1)}} = (2, 0, 5), \quad f_{\tau_2^{(2)}} = (1, 0, 10).$$

Chapter 2

p-adic uniformization of curves

2.1 Rigid analytic geometry

In this section, K will denote a local field, with non-Archimedean absolute value $|\cdot|$, $\overline{K}$ its algebraic closure, $\mathcal{O}_K := \{x \in K \mid |x| \leq 1\}$ its ring of integers and k its residue field.

Since $\overline{K}$ is not complete (with respect to the norm extending the norm $|\cdot|$ on K), we need also to consider its completion $\widehat{\overline{K}}$, which is an algebraically closed field, when K is of characteristic 0.

The aim of this section is to give the definition of rigid analytic variety over K, corresponding to the desire to transfer to a non-Archimedean complete field the classic definition of analytic variety over $\mathbb{C}$. As usual, we will start by studying the *functions* before defining the *varieties* themselves.

2.1.1 Motivation

If L is a field extension of K (not necessary finite), $L \subseteq \widehat{\overline{K}}$, we will denote by $\mathbb{B}^n(L)$ the **unit ball in** L^n:

$$\mathbb{B}^n(L) := \{(z_1, \ldots, z_n) \in L^n : \max_{1 \leq i \leq n} |z_i| \leq 1\}.$$

Recall that an **analytic function over** $\mathbb{C}$ is a function $f : U \subseteq \mathbb{C}^n \longrightarrow \mathbb{C}$, defined on an open subset U of $\mathbb{C}^n$, admitting a power series development, which converges in a neighborhood of every point of its domain of definition.

If we try to give this same definition in the non-Archimedean context, we immediately see that important properties of analytic functions over $\mathbb{C}$, are

no longer satisfied. More specifically, let us consider the following well-known property of analytic functions.

2.1.1 Proposition. (Archimedean principle of identity) *If an analytic function $f : U \subseteq \mathbb{C}^n \longrightarrow \mathbb{C}$, defined over an open connected subset $U \subset \mathbb{C}^n$, has a power series development which is zero in a neighborhood of a point, then $f = 0$ on all U.*

On the other side, let us now consider the function $f : K \longrightarrow K$ defined by

$$\begin{cases} f(z) := 0, & z \in \mathbb{B}^n(K), \\ \\ f(z) := 1, & z \in K \smallsetminus \mathbb{B}^n(K). \end{cases}$$

Let us observe that f has a power series development in a neighborhood of every point of K, namely

$$f(z) := \textstyle\sum_{n\geq 0} 0 \cdot z^n, \qquad z \in \mathbb{B}^n(K),$$

$$f(z) := 1 + \textstyle\sum_{n\geq 1} 0 \cdot z^n, \qquad z \in K \smallsetminus \mathbb{B}^n(K),$$

and the subsets $\mathbb{B}^n(K)$ and $K \smallsetminus \mathbb{B}^n(K) = \{z \in K : \ |z| > 1\}$ are both open subsets of K with respect to the topology induced by the non-Archimedean absolute values of K. Nevertheless, f is not identically equal to 0 or to 1 on its domain of definition. Pathological phenomena of this kind are due to the fact that the topological space K is totally disconnected, and actually $K = \mathbb{B}^n(K) \cup (K \smallsetminus \mathbb{B}^n(K))$ is a non-trivial decomposition in open subsets.

For this first simple reason, one starts by considering only functions with power series development on the unit ball in $\overline{K}$.

2.1.2 Definition. Let us denote by T_n the K-algebra of power series in n variables and with coefficients in K, converging on the unit ball $\mathbb{B}^n(\overline{K})$:

$$T_n := K\langle\zeta_1, \ldots, \zeta_n\rangle = \{f = \sum_{\nu\in\mathbb{N}^n} a_\nu \zeta^\nu \in K[[\zeta_1, \ldots, \zeta_n]] : \lim_{|\nu|\to\infty} |a_\nu| = 0\}.$$

The K-algebra T_n is called the **Tate algebra in n variables over K**.

On T_n there is the Gauß norm, i.e. the natural norm defined by

$$|f| := \max_{\nu\in\mathbb{N}^n} |a_\nu|$$

with respect to which T_n is a Banach K-algebra, i.e. T_n is complete with respect to the Gauß norm.

The following result is very useful and also easy to understand.

2.1.3 Proposition. *If $\mathcal{O}_K\langle\zeta_1,\dots,\zeta_n\rangle$ denotes the $\mathcal{O}_K$-algebra of series $f \in T_n$ with coefficients in the ring of integers of K, then*

$$\mathcal{O}_K\langle\zeta_1,\dots,\zeta_n\rangle = \{f \in T_n : \ |f| \leq 1\}.$$

Moreover the epimorphism of reduction of integers

$$a \in \mathcal{O}_K \longmapsto \tilde{a} \in k$$

induces an epimorphism of reduction of series*:*

$$f = \sum a_\nu \zeta^\nu \in \mathcal{O}_K\langle\zeta_1,\dots,\zeta_n\rangle \longmapsto \tilde{f} := \sum \tilde{a}_\nu \zeta^\nu \in k[\zeta_1,\dots,\zeta_n].$$

Note that the series are reduced into polynomials with coefficients in the residue field k.

One reason to consider the series of T_n is the fact that they provide all the analytic functions on the unit ball in $\overline{K}^n$.

2.1.4 Proposition. *There is a bijection between T_n and the set of functions $g : \mathbb{B}^n(\overline{K}) \longrightarrow \overline{K}$ having a convergent power series expansion and such that $g(\mathbb{B}^n(K)) \subseteq K$.*

This bijection is induced by the map which takes the value of every series of T_n in the points of $\mathbb{B}^n(\overline{K})$, i.e. which associates to the series $f \in T_n$ the well-defined function $a \in \mathbb{B}^n(\overline{K}) \longmapsto f(a) \in \overline{K}$.

Proof. cf. [BGR84, 5.1.4]. □

The fact that the map is injective is actually the *Principle of identity* for non-Archimedean analytic functions.

2.1.5 Corollary. (Non-Archimedean principle of identity) *If the series $f \in T_n$ takes value 0 in every point of $\mathbb{B}^n(\overline{K})$, then $f = 0$.*

We are now going to reveal the good properties this algebra of functions has.

2.1.6 Theorem. (Noether normalization lemma) *For every proper ideal $\mathfrak{a}$ in T_n there exist an integer d and a morphism of K-algebras $T_d \longrightarrow T_n$ such that the composition*

$$T_d \longrightarrow T_n \longrightarrow T_n/\mathfrak{a}$$

is a finite morphism of K-modules (i.e. $T_n/\mathfrak{a}$ is a finitely generated T_d-module).

Moreover the integer d coincides with the Krull dimension of the ring $T_n/\mathfrak{a}$ and so it is uniquely determined.

PROOF. (cf. [BGR84, 6.1.2]). □

As a direct consequence we have the following result.

2.1.7 Corollary. *Let $\mathfrak{m}$ be a maximal ideal of the ring T_n. Then the field $T_n/\mathfrak{m}$ is a finite extension of K.*

2.1.8 Corollary. *Let $\operatorname{Max} T_n$ denote the set of maximal ideals of T_n. Then the map*

$$\begin{array}{rccc} \rho: & \mathbb{B}^n(\overline{K}) & \longrightarrow & \operatorname{Max} T_n \\ & z & \longmapsto & \mathfrak{m}_z := \{f \in T_n \mid \ f(z) = 0\} \end{array}$$

is surjective.

Moreover for every $z_1, z_2 \in \mathbb{B}^n(\overline{K})$ there is an element $\sigma \in \operatorname{Gal}(\overline{K}/K)$ such that

$$\rho(z_1) = \rho(z_2) \iff z_1 = \sigma(z_2).$$

In particular ρ is a bijective map when K is algebraically closed.

PROOF. For every $z = (z_1, \ldots, z_n) \in \mathbb{B}^n(\overline{K})$ the ideal $\mathfrak{m}_z$ is the kernel of the following epimorphism

$$h_z : f \in T_n \longmapsto f(a) \in K(z_1, \ldots, z_n)$$

and so $\mathfrak{m}_z$ is a maximal ideal.

We now prove the surjectivity of ρ. Let $\mathfrak{m}$ be a maximal ideal of T_n. Therefore, by Corollary 2.1.7, $T_n/\mathfrak{m}$ is a finite and, thus, algebraic extension of K and there is a continous immersion $T_n/\mathfrak{m} \hookrightarrow \overline{K}$, equivalently there is a continuous map $\varphi : T_n \longrightarrow \overline{K}$ of kernel equal to $\mathfrak{m}$. Specifically, if $z := (z_1, \ldots, z_n) := (\varphi_1(\zeta_1), \ldots, \varphi_n(\zeta_n))$, then φ is the following map:

$$\varphi : \sum a_\nu \zeta^\nu \in T_n \longmapsto \sum a_\nu z^\nu \in \overline{K}.$$

Hence it is clear that φ is the map which evaluates a series of T_n in the point $(z_1, \ldots, z_n) \in \overline{K}^n$, i.e. $\varphi = h_z$. Finally, since the kernel of h_z is the maximal ideal $\rho(z) = \mathfrak{m}_z$, we have the equalities $\mathfrak{m} = \ker \varphi = \ker h_z = \mathfrak{m}_z$.

After what we have just seen, it is clear that different immersions of $T_n/\mathfrak{m}$ in $\overline{K}$ give different points inside $\rho^{-1}(\mathfrak{m})$ and that every point $\rho^{-1}(\mathfrak{m})$ is obtained by such an immersion. Hence, points of $\rho^{-1}(\mathfrak{m})$ are in bijection with the continuous immersions $\{T_n/\mathfrak{m} \hookrightarrow \overline{K}\}$ and there is only a finite number of these (since $T_n/\mathfrak{m}$ is a finite extension of K). Moreover, given two different points $z_1, z_2 \in \rho^{-1}(\mathfrak{m})$, we have that $\rho(z_1) = \rho(z_2)$ if and only if there is an isomorphism of fields $K(z_1) \simeq K(z_2)$ sending z_1 to z_2: such an isomorphism extends to an automorphism $\sigma \in \operatorname{Gal}(\overline{K}/K)$. □

2.1.9 Remark. Proposition 2.1.4 and Corollary 2.1.8 give an interpretation of the series of T_n as functions on the set of its maximal ideals $\operatorname{Max} T_n$.

Specifically, to the series $f \in T_n$ we can associate the following map, which we again denote by f:

$$f : \mathfrak{p} \in \operatorname{Max} T_n \longmapsto f(\mathfrak{p}) \in \bigsqcup_{\mathfrak{m} \in \operatorname{Max} T_n} T_n/\mathfrak{m},$$

where $f(\mathfrak{p})$ is defined as the reduction of the series f modulo the maximal ideal $\mathfrak{p}$. This map is known to be well-defined, thanks to Corollary 2.1.7.

When the field K is algebraically closed, the maximal ideals of T_n can be thought of as *points* of the unit ball $\mathbb{B}^n(K)$ and the series in T_n as *functions* defined in this ball.

2.1.2 Affinoid varieties

We start by appreciating how the aim of extending the concepts of *analytic variety* and *analytic functions* leads us to consider the unit ball $\mathbb{B}^n(\overline{K})$, instead of the affine space $\mathbb{C}^n = \mathbb{A}^n_{\mathbb{C}}(\mathbb{C})$, together with the convergent series on this ball.

However, we are still far from defining non-Archimedean analytic varieties, since we have first to consider a topology on the set $\operatorname{Max} T_n$. Going in this direction, we will focus on certain special subsets of $\operatorname{Max} T_n$ which are suggested by the algebraic geometrical language. After this, a local theory of varieties is developed in order to give the global definition.

2.1.10 Definition. For every subset $F \subseteq T_n$ the **set of zeros of** F is defined to be:

$$\mathbf{V}(F) := \{\mathfrak{m} \in \operatorname{Max} T_n \mid \ f(\mathfrak{m}) = 0,\ \forall f \in F\},$$

$$\widetilde{\mathbf{V}}(F) := \{z \in \mathbb{B}^n(\overline{K}) \mid \ f(z) = 0,\ \forall f \in F\}.$$

A subset of T_n of the type $\mathbf{V}(F)$ (resp. $\widetilde{\mathbf{V}}(F)$), for some $F \subseteq T_n$, is called an **affinoid subset of** $\operatorname{Max} T_n$ (resp. **affinoid subset of** $\mathbb{B}^n(\overline{K})$).

The set $\widetilde{\mathbf{V}}(F)$ is the pre-image of $\mathbf{V}(F)$ by the map ρ of Corollary 2.1.8, which then induces a bijection

$$\rho : \widetilde{\mathbf{V}}(F)/\operatorname{Gal}(\overline{K}/K) \simeq \mathbf{V}(F).$$

Note that $\mathbb{B}^n(\overline{K})$ itself is an affinoid set, since it is the set of zeros of $\operatorname{Max} T_n$.

After this, we might decide to develop the local theory of analytic varieties working only with affinoid subsets of $\mathbb{B}^n(\overline{K})$; this certainly would make more clear the parallel with the theory of holomorphic functions. On the other hand, we would lose the elegant parallel with the theory of affine algebraic varieties.

2.1.11 Definition. For every subset $Y \subseteq \operatorname{Max} T_n$, the **ideal of** Y is defined as follows:

$$\mathbf{I}(Y) := \{f \in T_n \mid \ f(\mathfrak{m}) = 0, \ \forall\, \mathfrak{m} \in Y\}.$$

If $Y \subseteq \operatorname{Max} T_n$ is an affinoid subset, then

$$\mathbf{V}(\mathbf{I}(Y)) = Y$$

(cf. [BGR84, 7.1.2/2]).

2.1.12 Theorem. (Hilbert Nullstellensatz) *If $\mathfrak{a} \subseteq T_n$ is a non-zero ideal, then*

$$\boldsymbol{I}(\,\boldsymbol{V}(\mathfrak{a})) = \mathfrak{R}(\mathfrak{a}),$$

where $\mathfrak{R}(\mathfrak{a})$ denotes the radical of the ideal $\mathfrak{a}$.

Without any difficulty it can be proved that the affinoid subsets of $\operatorname{Max} T_n$ are the closed subsets of a topology on $\operatorname{Max} T_n$: this is the well-known (in the algebro-geometric context) **Zariski topology**.

2.1.13 Definition. An **affinoid variety over** K (also an **affinoid space over** K) is a couple

$$\operatorname{Sp} A := (\operatorname{Max} A, A),$$

formed by an affinoid K-algebra A and the topological space $\operatorname{Max} A$ with the Zariski topology induced by its affinoid subsets.

A **morphism of affinoid** K**-varieties** (also a K**-affinoid morphism**) is a couple (φ^{af}, φ), where $\varphi : B \to A$ is a morphism of K-algebras and φ^{af} is the following map associated φ:

$$\varphi^{af} : \mathfrak{m} \in \operatorname{Max} A \longmapsto \varphi^{-1}(\mathfrak{m}) \in \operatorname{Max} B.$$

We use the following notation to denote it:

$$\operatorname{Sp}\varphi := (\varphi^{af}, \varphi) : \operatorname{Sp} A \longrightarrow \operatorname{Sp} B.$$

We have formed a category whose objects are affinoid varieties over K and whose morphisms are K-affinoid morphisms: this is the **category of affinoid varieties over** K and it is the opposite category of the one of affinoid K-algebras. The functor **Sp** sending the affinoid K-algebra A to the affinoid K-varitey $\operatorname{Sp} A$ and the morphism $\varphi : B \to A$ to the K-affinoid morphisms $\operatorname{Sp}\varphi := (\varphi^{af}, \varphi) : \operatorname{Sp} A \to \operatorname{Sp} \mathrm{B}$ is an anti-equivalence between these two categories.

It is usual (and sometimes confusing), talking about affinoid varieties, to use the notation $\operatorname{Sp} A$ to refer only to the topological space $\operatorname{Max} A$. With the same spirit, notation $\operatorname{Sp}\varphi$ refers only to the map $\varphi^{af} : \operatorname{Max} A \to \operatorname{Max} B$.

2.1.14 Definition. An affinoid morphism $\operatorname{Sp}\varphi : \operatorname{Sp} A \to \operatorname{Sp} B$ is called **closed immersion** if $\varphi : B \to A$ is an epimorphism.

It is easy to see that a closed immersion is an injective morphism in the category of affinoid varieties and so it allows the identification of $\operatorname{Max} A$ with an affinoid subset of $\operatorname{Max} B$ in a manner such that every function on $\operatorname{Sp} A$ is obtained as restriction of a function on $\operatorname{Sp} B$.

2.1.15 Definition. Let $\operatorname{Sp} A = (\operatorname{Max} A, A)$ be an affinoid variety. A subset of points $U \subseteq \operatorname{Max} A$ is called an **affinoid subdomain** if there exist an affinoid variety $\operatorname{Sp} B$ and a morphism $(\sigma^{af}, \sigma) : \operatorname{Sp} B \to \operatorname{Sp} A$ with the following properties:

(a) The map $\sigma : \operatorname{Max} B \to \operatorname{Max} A$ is injective.

(b) $\sigma^{af}(\operatorname{Max} B) = U$.

(c) For every point $\mathfrak{m} \in \operatorname{Max} B$ and for every integer $n \geq 1$, the morphism of affinoid K-algebras $\sigma : A \to B$ induces a local isomorphism

$$A/\sigma^{af}(\mathfrak{m})^n \simeq B/\mathfrak{m}^n.$$

(d) **Universal Property**: For every affinoid variety $\operatorname{Sp} B'$ and every morphism of affinoid varieties

$$(\varphi^{af}, \varphi) : \operatorname{Sp} B' \to \operatorname{Sp} A \text{ satisfying } \varphi^{af}(\operatorname{Max} B') = U,$$

there is a unique morphism $(\psi^{af}, \psi) : \operatorname{Sp} B' \to \operatorname{Sp} B$ such that the following diagram is commutative:

$$\begin{array}{ccc} \operatorname{Sp} B' & \xrightarrow{\varphi} & \operatorname{Sp} A \\ \downarrow{\scriptstyle \psi} & \nearrow_{\sigma} & \\ \operatorname{Sp} B. & & \end{array}$$

When these properties are satisfied we can write, with abuse of notation,

$$U = \operatorname{Sp} B.$$

2.1.16 Remark. Roughly speaking, Definition 2.1.15 says that the subset of points $U \subseteq \operatorname{Max} A$ can be canonically realized as an affinoid variety. So, again abusing the notation, we will write $U \subseteq \operatorname{Sp} A$.

Nevertheless, even if we have an immersion of the set of points of U inside $\operatorname{Max} A$, the affinoid morphism $(\sigma, \sigma^{af}) : U = \operatorname{Sp} B \to \operatorname{Sp} A$ is not always an immersion of affinoid varieties (i.e. $\sigma^{af} : A \to B$ is not always an epimorphism), so we would be wrong to think of U as a subvariety "inside" the variety $\operatorname{Sp} A$.

This is the essential reason why we are naturally led to consider a weaker concept of topology in which open subsets do not have to be necessarily subsets of the space: this kind of topology is the well-known *Grothendieck topology*.

To understand the definition of affinoid subdomains is of fundamental importance to understand the statement of the famous **Tate aciclicity theorem**.

Let X be an affinoid variety over K. Let us consider the functor $\mathcal{O}_X$ from the category of affinoid subdomain of X (where morphisms are injective affinoid morphisms) to the category of affinoid K-algebras:

- To the affinoid subdomain $\operatorname{Sp} A \to X$ the K-algebra A of functions is associated.
- To the inclusion $\operatorname{Sp} B \hookrightarrow \operatorname{Sp} A$ of affinoid subdomains of X the following morphism of restriction

  $$f \in A \longmapsto f\,|_{\operatorname{Sp} B} \in B$$

  is associated.

The functor $\mathcal{O}_X$ is a pre-sheaf of K-algebras (of functions) over a base for the canonical topology of X, but this is *not* a sheaf.

Recall that for $\mathcal{O}_X$ to be a sheaf it is necessary (and sufficient) that the following properties hold for every affinoid subdomain $U \subseteq X$ and for every cover $\{U_i\}_{i \in I}$ of U constituted of affinoid subdomains the following properties:

(a) If $f \in \mathcal{O}_X(U)$ is zero restricted to every U_i, then $f = 0$ on the whole U.

(b) If $\{f_i\}_{i\in I}$ is a family of functions $f_i \in \mathcal{O}_X(U)$ such that $f_i = f_j$ on $U_i \cap U_j$ for every $i, j \in I$, there exists $f \in \mathcal{O}_X(U)$ such that $f \mid_{U_i} = f_i$ for every $i \in I$.

The first of these properties is basically Corollary 2.1.5); nevertheless, the second one, also known in the theory of holomorphic functions as the *analytic continuation*, fails due to the fact that the space X with the canonical topology is totally disconnected.

At this point Tate's result makes its triumphal entry, since it proves that the property of analytic continuation is valid when we restrict ourselves to considering *finite* covers of the affinoid subdomain U of X.

In order to prove the result one should first define the cohomological theory associated to this pre-sheaf of functions: this can be followed in [BGR84, 8.2.2], and also in the original paper of Tate [Tat71], where a slightly different language is used.

2.1.17 Theorem. (Tate's aciclicity theorem) *Let X be an affinoid variety of K.*

If $\mathcal{U} = \{U_i\}_{i\in I}$ is a finite cover of X in affinoid subdomains $U_i \subseteq X$, then $\mathcal{U}$ is acyclic, i.e. $\mathcal{U}$ satisfies the following properties:

(a) There is a bijection $\mathcal{O}_X(X) \simeq H^0(\mathcal{U}, \mathcal{O}_X)$.

(b) $H^q(\mathcal{U}, \mathcal{O}_X) = 0$, for every integer $q \neq 0$.

2.1.3 Rigid analytic varieties

Tate's result has to be considered as the starting point of a *rigid* theory of non-Archimedean analytic functions.

We finally give the definition of rigid analytic variety.

Given an affinoid variety X, we take on it a Grothendieck topology in which *admissible opens* are open affinoid subdomains of X and *admissible covers* are finite covers of affinoid subdomains. This topology is called **weak G-topology of** X.

The main objective of the section was to define rigid analytic varieties, which are constructed, as we have noted above, from glueing together affinoid varieties. So they should be considered the local pieces of the theory, as affine algebraic varieties are for algebraic varieties.

For this reason, we will need a finer Grothendieck topology, which we now define.

2.1.18 Definition. (Strong G-topology) Let X be an affinoid variety over X. A **strong Grothendieck topology in** X (also a **strong G-topology**) is a Grothendieck topology on X where admissible open subsets and admissible covers are defined as follows:

(a) A subset of points $U \subseteq X$ is an **admissible open subset of** X if there is a cover $\mathcal{U} = \{U_i\}_{i\in I}$ in affinoid subdomains satisfying: for every affinoid morphism $\varphi : Y \to X$ such that $\varphi(Y) \subseteq U$, the cover $\varphi^{-1}(\mathcal{U})$ of Y admits a finer and finite cover in affinoid subdomains.

(b) A cover in admissible open subsets $\mathcal{V} = \{V_i\}_{i\in I}$ of an admissible open subset $V \subseteq X$ is an **admissible cover** if: for every affinoid morphism $\varphi : Y \to X$ such that $\varphi(Y) \subseteq V$, the cover $\varphi^{-1}(\mathcal{V})$ of Y admits a finer and finite cover in affinoid subdomains.

The strong G-topology is a finer topology than the weak G-topology: actually, as is clear from the definition, in addition to affinoid subdomains and finite unions of affinoid subdomains, one also admits certain unions of affinoid subdomains as admissible open subsets, and certain infinite covers as admissible covers.

2.1.19 Definition. Let R be a ring. A **ringed G-space over** R is a pair $(X, \mathcal{O}_X)$ formed by a topological G-space X and by a sheaf $\mathcal{O}_X$ of R-algebras over X. The sheaf will be referred to as the **structural sheaf of** X.

A ringed G-space $(X, \mathcal{O}_X)$ is said to be **local** if for every $x \in X$, the direct limit

$$\mathcal{O}_{X,x} := \varinjlim_{U\ni x} \mathcal{O}_X(U)$$

is a local ring.

A **morphism of ringed G-spaces over** R is a couple

$$(\varphi, \varphi^*) : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$$

formed by a continuous map $\varphi : X \to Y$ of topological G-spaces and by a family of homomorphisms of R-algebras

$$\varphi^* : \{\varphi_V^* : \mathcal{O}_Y(V) \longrightarrow \mathcal{O}_X(\varphi^{-1}(V))\}_{V\in\mathcal{V}}$$

indexed in the system of admissible open subsets $\mathcal{V}$ of Y such that φ_V^* is compatible with all the restriction morphisms.

If in addition the ringed G-spaces $(X, \mathcal{O}_X), (Y, \mathcal{O}_Y)$ are local and for every $x \in X$ the homomorphism of rings

$$\varphi_x^* : \mathcal{O}_{Y,\varphi(x)} \longrightarrow \mathcal{O}_{X,x}$$

is local as well, then the morphism $(\varphi, \varphi^*) : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ is called a **morphism of local ringed G-spaces**.

2.1.20 Definition. A **rigid analytic variety over** K is a local ringed G-space $(X, \mathcal{O}_X)$ such that:

(a) The Grothendieck topology on X is the strong G-topology.

(b) X admits an admissible cover $\{U_i\}_{i\in I}$ such that $(U_i, \mathcal{O}_X\ |_{U_i})$ is an affinoid variety over K, for every $i \in I$.

If $(X, \mathcal{O}_X), (Y, \mathcal{O}_Y)$ are rigid analytic varieties over K, then a morphism of ringed G-spaces

$$(\varphi, \varphi^*) : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$$

is called a **rigid K-analytic morphism**.

2.1.21 Theorem. *Given the following data:*

(*a*) *A family* $\{X_i\}_{i\in I}$ *of rigid analytic varieties over* K.

(*b*) *For every* $i, j \in I$, *rigid analytic varieties* $X_{ij} \subseteq X_i, X_{ji} \subseteq X_j$ *and isomorphisms between them* $\varphi_{ij} : X_{ij} \simeq X_{ji}$.

Moreover let us assume that the previous data are compatible in the following sense:

(*i*) $\varphi_{ij}\varphi_{ji} = \mathrm{id}_{X_{ii}}$, $X_{ii} = X_i$, $\varphi_{ii} = \mathrm{id}_{X_{ii}}$ *for every* $i, j \in I$.

(*ii*) φ_{ij} *induces isomorphisms* $\varphi_{ijk} : X_{ij} \cap X_{ik} \simeq X_{ji} \cap X_{jk}$ *such that* $\varphi_{ijk} = \varphi_{kji}\varphi_{ikj}$, *for every* $i, j, k \in I$.

Then a rigid analytic variety X *over* K *can be constructed by glueing together* X_{ij} *with* X_{ji} *through the morphism* φ_{ij}, *for every* $i, j \in I$.

Moreover the family $\{X_i\}_{i\in I}$ *is an admissible cover for* X.

Proof. (cf. [BGR84, 9.3.4/1]). □

2.2 The p-adic upper half-plane

Let $\mathbb{Q}_p$ denote the field of p-adic numbers and let $\mathbb{C}_p$ denote the completion of a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. As usual, we take the absolute value on $\mathbb{Q}_p$ defined by

$$|z| := \frac{1}{p^{v_p(z)}}$$

for every $z \in \mathbb{Q}_p$, where $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ denotes the p-adic discrete valuation on $\mathbb{Q}_p$.

For every algebraic extension $L|\mathbb{Q}_p$, let us denote by $|\cdot|$ the unique absolute value extending the p-adic absolute value on $\mathbb{Q}_p$ (cf. [Neu99, Ch. II Theorem 4.8]). We will also denote by $|\cdot|$ the unique absolute value on $\mathbb{C}_p$ extending the one on $\mathbb{Q}_p$ and with respect to which this field is complete.

In this section we will introduce the p-adic upper half-plane: this is a p-adic rigid analytic variety $\mathcal{H}_p$ over $\mathbb{Q}_p$ whose set of L-points, for every extension $\mathbb{Q}_p \subseteq L \subseteq \mathbb{C}_p$, is

$$\mathcal{H}_p(L) = \mathbb{P}^{1,rig}(L) \smallsetminus \mathbb{P}^{1,rig}(\mathbb{Q}_p)$$

and such that its reduction can be "identified" with the p-adic Bruhat-Tits tree.

We will describe this rigid analytic space following three steps:

1. First we exhibit an admissible cover, endowing the set $\mathcal{H}_p(L)$ with a structure of rigid analytic variety.

2. Then we define the Bruhat-Tits tree $\mathcal{T}_p$ associated to $\mathrm{PGL}_2(\mathbb{Q}_p)$.

3. Finally we show that the tree $\mathcal{T}_p$ is the *reduction graph* of the rigid analytic variety $\mathcal{H}_p$, with respect to the admissible cover defined.

This will complete the portrait of a rigid analytic space which will later become, the set of parameters in the p-adic uniformization of Shimura curves.

In the literature, the Bruhat-Tits tree is usually defined first, and then p-adic upper half-plane: actually this can be done after adequately defining a *reduction map* associated to the tree.

As we have said, this is the commonest process in the literature, as in [Mum72], where the p-adic upper half-plane is defined as a formal scheme, or as in [BC91, Introduction] and [Dar03, Chapter 5], where this is defined as a rigid analytic variety.

The construction we propose here is more natural and linear after having fixed the basic definitions on rigid analytic varieties, as was done in previous section. To do so, we follow [SS91, Sec. 1] where the Drinfeld symmetric space of dimension d is defined. We take advantage of the fact that we are working in low dimension to make the description explicit, giving the equations that locally define the rigid analytic variety $\mathcal{H}_p$ (cf. Theorem 2.2.20).

2.2.1 The p-adic upper half-plane: generic fibre

Before starting to define the p-adic upper half-plane, we need to recall some basic facts about rigid analytic geometry: namely, we will see how the affine space $\mathbb{A}^n_{\mathbb{Q}_p}$ and the projective space $\mathbb{P}^n_{\mathbb{Q}_p}$, both algebraic varieties over $\mathbb{Q}_p$, can be endowed with a structure of rigid analytic variety over $\mathbb{Q}_p$. This will turn out to be a special case of the rigid *gaga* functor (cf. [Bos08, 1.13]). Even if the p-adic upper half-plane turns out to be non-algebraizable, i.e. it cannot be obtained with such a construction starting with an algebraic variety, we will see that its structure as a rigid analytic variety is strongly influenced by the one of the rigid analytic projective line $\mathbb{P}^{1,rig}_{\mathbb{Q}_p}$, basically due to the fact that its sets of points are subsets of $\mathbb{P}^1_{\mathbb{Q}_p}(\mathbb{C}_p)$.

Let $\zeta = (\zeta_1, \dots, \zeta_n)$ be an ordinate set of variables and let us choose $c \in \mathbb{Q}_p$ of absolute value $|c| > 1$.

For every integer $i \geq 0$ we define the $\mathbb{Q}_p$-algebra of series in the indeterminates ζ and with coefficients in $\mathbb{Q}_p$, converging on the ball of $\mathbb{C}_p^n$ of center 0 and radius $|c|^i$,

$$T_n^{(i)} := \{ \sum_{\nu \in \mathbb{N}^n} a_\nu \zeta^\nu \in \mathbb{Q}_p[[\zeta_1, \dots, \zeta_n]] \ | \ \lim_{|\nu| \to \infty} |a_\nu| |c^i|^\nu = 0 \}.$$

The $\mathbb{Q}_p$-algebras $T_n^{(i)}$ are affinoids: indeed $T_n^{(i)}$ is isomorphic to the Tate algebra T_n over $\mathbb{Q}_p$ in the n indeterminates $(\xi_1, \dots, \xi_n)$, through the map

$$\xi_\nu \in T_n \longmapsto c^{-i} \zeta_\nu \in T_n^{(i)}.$$

If we let the sup-index $i \geq 0$ vary, we obtain a sequence of affinoids varieties

$$\mathbb{B}^n(|c|^i) := \operatorname{Sp} T_n^{(i)} = (\operatorname{Max} T_n^{(i)}, T_n^{(i)}).$$

Moreover, with the same procedure as in Corollary 2.1.8, we can identify the set $\operatorname{Max} T_n^{(i)}$ with the set of points of the ball in $\mathbb{Q}_p^n$ of center 0 and radius $|c|^i$:

$$\mathbb{B}^n(|c|^i)(\mathbb{C}_p) := \{(z_1, \dots, z_n) \in \mathbb{C}_p^n \ | \ \max_{1 \leq s \leq n} |z_s| \leq |c|^i \}.$$

For $i = 0$ we find the well-known affinoid variety over $\mathbb{Q}_p$:

$$\mathbb{B}^n_{\mathbb{Q}_p} := \mathbb{B}^n(1) = \operatorname{Sp} \mathbb{Q}_p \langle \zeta_1, \dots, \zeta_n \rangle.$$

To the chain of algebras

$$T_n^{(0)} \longrightarrow T_n^{(1)} \longrightarrow \dots \longrightarrow T_n^{(\infty)} := \mathbb{Q}_p[\zeta_1, \dots, \zeta_n]$$

corresponds the ascending chain of the respective maximal spectra

$$\operatorname{Max} T_n^{(0)} \subseteq \operatorname{Max} T_n^{(1)} \subseteq \cdots \subseteq \operatorname{Max} \mathbb{Q}_p[\zeta_1, \ldots \zeta_n].$$

For every $i \geq 0$, the affinoid variety $\mathbb{B}^n(|c|^i)$ is an affinoid subdomain of $\mathbb{B}^n(|c|^{i+1})$, through the rigid analytic morphism induced by the monomorphism of $\mathbb{Q}_p$-algebras $\varphi_i : T_n^{(i)} \longrightarrow T_n^{(i+1)}$ (cf. Definition 2.1.15).

Hence, we are now in a position to apply Theorem 2.1.21 to the following data:

$$X_i := \operatorname{Sp} T_n^{(i)}, \quad X_{ij} := X_{\min\{i,j\}}, \quad \varphi_{ij} := \mathrm{id}_{X_{ij}}$$

in order to obtain a rigid analytic variety composed by the G-space

$$\bigcup_{i \in \mathbb{N}} \operatorname{Max} T_n^{(i)} = \operatorname{Max} \mathbb{Q}_p[\zeta_1, \ldots, \zeta_n]$$

and by the $\mathbb{Q}_p$-algebra of functions $\varprojlim T_n^{(i)}$.

The rigid analytic variety constructed is called **rigid analytic affine space of dimension** n **over** $\mathbb{Q}_p$ and it is denoted by $\mathbb{A}^{n,rig}_{\mathbb{Q}_p}$. Hence we have:

$$\mathbb{A}^{n,rig}_{\mathbb{Q}_p} = \left(\bigcup_{i \in \mathbb{N}} \operatorname{Max} T_n^{(i)}, \varprojlim T_n^{(i)} \right)$$

From what we have just shown it is clear that the set of $\mathbb{C}_p$-valued points of $\mathbb{A}^{n,rig}_{\mathbb{Q}_p}$ coincides with the set of $\mathbb{C}_p$-valued points of the algebraic variety $\mathbb{A}^n_{\mathbb{Q}_p}$, i.e. $\mathbb{A}^{n,rig}_{\mathbb{Q}_p}(\mathbb{C}_p) = \mathbb{A}^n_{\mathbb{Q}_p}(\mathbb{C}_p)$.

This is why we can affirm that we have endowed the algebraic variety $\mathbb{A}^n_{\mathbb{Q}_p}$ with a structure of rigid analytic variety over $\mathbb{Q}_p$. Actually, the family of affinoids varieties $\{\operatorname{Sp} T_n^{(i)}\}_{i \in \mathbb{N}}$ is an admissible cover for the rigid analytic variety $\mathbb{A}^{n,rig}_{\mathbb{Q}_p}$. More in general we can associate to every smooth algebraic variety

$$X = \operatorname{Spec} \left(\mathbb{Q}_p[\zeta_1, \ldots, \zeta_n]/(f_1, \ldots, f_r) \right)$$

a rigid analytic variety which is usually denoted by X^{rig} (also, X^{an}) and which is referred to as the **rigidification of** X. This is done considering the admissible cover of affinoid varieties $\operatorname{Sp}\left(T_n^{(i)}/(f_1, \ldots, f_r)\right)$, for every $i \geq 0$.

It can be proved that for every scheme X of finite type over $\mathbb{Q}_p$ there is a unique rigid analytic variety X^{rig} such that the set of $\mathbb{C}_p$-points $X(\mathbb{C}_p)$ coincides with the set of closed points of X^{rig} (cf. [BGR84, 9.3.4]). A rigid analytic space which is obtained as rigidification of such a scheme is called **algebraizable**. Specifically, a rigid analytic variety is algebraizable if and

only if its set of closed points is the set of closed points of some scheme of finite type.

We are going to work with projective varieties, so we want to describe explicitly the rigidification of the projective space $\mathbb{P}^n_{\mathbb{Q}_p} := \operatorname{Proj} \mathbb{Q}_p[\zeta_0, \ldots, \zeta_n]$.

Recall that $\mathbb{P}^n_{\mathbb{Q}_p}$ is obtained by glueing the following $n+1$ affine varieties

$$U_i := \operatorname{Spec} \mathbb{Q}_p[\zeta_1, \ldots, \hat{\zeta}_i, \ldots, \zeta_n] \simeq \mathbb{A}^n_{\mathbb{Q}_p},$$

where $0 \leq i \leq n$.

Therefore it is natural to apply Theorem 2.1.21 in order to glue together the $n+1$ rigid analytic varieties $U_0^{rig}, \ldots, U_n^{rig}$ (all of them which are isomorphic to the rigid analytic affine space $\mathbb{A}^{n,rig}_{\mathbb{Q}_p}$).

This procedure would give an admissible cover but it would not be formed by affinoid subdomains, so it is more convenient to look for another admissible cover formed by affinoid varieties (as in the case of the algebraic construction of $\mathbb{P}^n_{\mathbb{Q}_p}$).

The following remark gives an idea of which affinoid varieties can be glued together in order to cover the rigid projective space.

2.2.1 Remark. Every $\mathbb{C}_p$-valued point z of the algebraic variety $\mathbb{P}^n_{\mathbb{Q}_p}$ always admits coordinates $(z_0, \ldots, z_n) \in \mathbb{C}_p^{n+1}$ such that $\max_{0 \leq i \leq n} |z_i| = 1$. Intuitively this is because we can multiply all the coordinates by a sufficiently large power of p, clearing up denominators. Coordinates of z with such a property are called **unimodular coordinates**.

Hence, as sets, we have that $\mathbb{P}^n(\mathbb{C}_p)$ can be recovered by $n+1$ copies of the unit ball $\mathbb{B}^n_{\mathbb{Q}_p}(\mathbb{C}_p)$. This suggests that we can apply Theorem 2.1.21 to $n+1$ affinoid varieties, all of them analytically isomorphic to $\mathbb{B}^n_{\mathbb{Q}_p}$ (cf. [BGR84, 9.3.4/3]). We obtain a rigid analytic variety which is denoted by $\mathbb{P}^{n,rig}_{\mathbb{Q}_p}$.

Let us consider the particular case of the **rigid projective line over** $\mathbb{Q}_p$.

Let ζ_0, ζ_1 be variables. We define the following affinoid varieties:

$$X_0 := \operatorname{Sp} \mathbb{Q}_p\langle \frac{\zeta_0}{\zeta_0}, \frac{\zeta_1}{\zeta_0} \rangle \simeq \operatorname{Sp} \mathbb{Q}_p\langle \zeta \rangle, \quad X_1 := \operatorname{Sp} \mathbb{Q}_p\langle \frac{\zeta_0}{\zeta_1}, \frac{\zeta_1}{\zeta_1} \rangle \simeq \operatorname{Sp} \mathbb{Q}_p\langle \frac{1}{\zeta} \rangle,$$

$$X_{01} := \operatorname{Sp} \mathbb{Q}_p\langle \frac{\zeta_1}{\zeta_0}, \frac{\zeta_0}{\zeta_1} \rangle \simeq \operatorname{Sp} \mathbb{Q}_p\langle \zeta, \frac{1}{\zeta} \rangle, \quad X_{10} := \operatorname{Sp} \mathbb{Q}_p\langle \frac{\zeta_0}{\zeta_1}, \frac{\zeta_1}{\zeta_0} \rangle \simeq \operatorname{Sp} \mathbb{Q}_p\langle \frac{1}{\zeta}, \zeta \rangle.$$

The affinoid isomorphisms above are induced by the isomorphisms of $\mathbb{Q}_p$-algebras, induced i turn by the change of variables $\zeta \mapsto \zeta_1/\zeta_0$.

Obviously, $X_0 \simeq X_1 \simeq \mathbb{B}^1_{\mathbb{Q}_p}$ and then we have isomorphisms

$$\varphi_{01} : X_{01} \to X_{10}, \qquad \varphi_{10} : X_{10} \to X_{01}.$$

Applying Theorem 2.1.21 to the datum $X_i, X_j, X_{ij}, \varphi_{ij}$ we obtain the rigid analytic variety $\mathbb{P}^{1,rig}_{\mathbb{Q}_p}$, whose set of closed points is

$$\mathbb{P}^{1,rig}(\mathbb{C}_p) := X_0(\mathbb{C}_p) \cup X_1(\mathbb{C}_p) \simeq \mathbb{B}(\mathbb{C}_p) \cup \mathbb{B}(\mathbb{C}_p).$$

After this description it is clear that every closed point $z \in \mathbb{P}^{1,rig}_{\mathbb{Q}_p}(\mathbb{C}_p)$ admits unimodular coordinates, so in particular the two sets of *algebraic points* and *analytic points* of $\mathbb{P}^1_{\mathbb{Q}_p}$ coincide:

$$\mathbb{P}^{1,rig}(\mathbb{C}_p) = \mathbb{P}^1(\mathbb{C}_p).$$

2.2.2 Remark. The role of the *affinoid* variety $\mathbb{B}^n_{\mathbb{Q}_p}$ in the context of rigid *analytic geometry* is the same as the one of the *affine* variety $\mathbb{A}^n_{\mathbb{Q}_p}$ in *algebraic geometry*.

As in the algebraic context we have the following bijection of points:

$$\mathbb{P}^1(\mathbb{C}_p) \simeq \mathbb{A}^1(\mathbb{C}_p) \cup \{\infty\} = \mathbb{C}_p \cup \{\infty\}.$$

Analytically we can write the bijection as well:

$$[z_0 : z_1] \in \mathbb{P}^{1,rig}(\mathbb{C}_p) \longmapsto \begin{cases} [z_0/z_1 : 1], & \text{if } z_1 \neq 0 \\ [1 : 0], & \text{if } z_1 = 0 \end{cases} \in \mathbb{B}(\mathbb{Q}_p) \cup \{\infty\}$$

where ∞ denotes the point of projective unimodular coordinates $[1 : 0]$.

We will draw the rigid projective line over $\mathbb{Q}_p$ as a disk of center 0 (or equivalently any $\mathbb{Q}_p$-rational point) and radius 1, confining it with a "circle of center ∞ and radius 1", that is, the complement of the circle of center 0 and radius 1.

2.2.3 Definition. Let be $a \in \mathbb{B}(\mathbb{Q}_p)$ and $r \in \mathbb{R}_{\geq 0}$. Then the following subsets of points

$$\mathbb{B}^+(a, |p|^r) := \{z \in \mathbb{B}(\mathbb{C}_p),\ |z - a| \leq |p|^r\} = \{z \in \mathbb{B}(\mathbb{C}_p),\ v(z - a) \geq r\},$$

$$\mathbb{B}^-(a, |p|^r) := \{z \in \mathbb{B}(\mathbb{C}_p),\ |z - a| < |p|^r\} = \{z \in \mathbb{B}(\mathbb{C}_p),\ v(z - a) > r\}$$

are called resp. **closed ball** and **open ball** with center a and radius $|p|^r$ of the affinoid variety $\mathbb{B}_{\mathbb{Q}_p}$.

2.2.4 Definition. Let be $a = [a_0 : a_1] \in \mathbb{P}^{1,rig}(\mathbb{Q}_p)$ and $r \in \mathbb{R}_{\geq 0}$. Then the following subsets

$$\begin{aligned}\mathbb{B}^+(a, |p|^r) &:= \{[z_0 : z_1] \in \mathbb{P}^{1,rig}(\mathbb{C}_p) : \ |z_0a_1 - z_1a_0| \leq |p|^r\} = \\ &= \{z \in \mathbb{P}^{1,rig}(\mathbb{C}_p) : \ v(z_0a_1 - z_1a_0) \geq r\}, \\ \mathbb{B}^-(a, |p|^r) &:= \{[z_0 : z_1] \in \mathbb{P}^{1,rig}(\mathbb{C}_p) : \ |z_0a_1 - z_1a_0| < |p|^r\} = \\ &= \{z \in \mathbb{P}^{1,rig}(\mathbb{C}_p) : \ v(z_0a_1 - z_1a_0) > r\}\end{aligned}$$

are called resp. **closed ball** and **open ball** with center a and radius $|p|^r$ of the rigid analytic projective line $\mathbb{P}^{1,rig}$.

It should be obvious that the adjectives "closed" and "open" do not have any topological meaning, since in the topological space $\mathbb{Q}_p$ (as well as in its compactification) all balls are clopen (i.e. $\mathbb{Q}_p$ with its natural p-adic topology is totally disconnected).

2.2.5 Remark. Thanks to the point-set bijection $\mathbb{P}^{1,rig}(\mathbb{C}_p) \simeq \mathbb{B}(\mathbb{C}_p) \cup \{\infty\}$ explained in Remark 2.2.2, we can define alternatively the (open or closed) ball of $\mathbb{P}^{1,rig}$, with center $[a_0 : a_1]$ and radius $|p|^r$ as one of the following subsets:

(a) If $[a_0 : a_1] = [a : 1] \simeq a \in \mathbb{B}(\mathbb{Q}_p)$,

$$\{z \in \mathbb{B}(\mathbb{C}_p) : \ |z - a| \leq |p|^r\} = \{z \in \mathbb{C}_p : \ |z - x| \leq |p|^r\} = \mathbb{B}^+(a, |p|^r).$$

(b) If $[a_0, a_1] = [1 : 0] =: \infty$,

$$\{z \in \mathbb{C}_p : \ |z| \geq |p|^r\} \cup \{\infty\} = \mathbb{B}^+(\infty, |p|^r).$$

2.2.6 Definition. We call a subset of points $Y \subseteq \mathbb{P}^{1,rig}(\mathbb{Q}_p)$ a **ball with holes** of the affinoid variety $\mathbb{B}_{\mathbb{Q}_p} = \operatorname{Sp} \mathbb{Q}_p\langle\zeta\rangle$ if there exist points $a_0, a_1, \ldots, a_s \in \mathbb{P}^{1,rig}(\mathbb{Q}_p)$ and positive real numbers $r_0, r_1, \ldots, r_s \in \mathbb{R}_{\geq 0}$ such that

$$Y = \mathbb{B}^+(a_0, |p|^{r_0}) \smallsetminus \bigcup_{i=1}^{s} \mathbb{B}^-(a_i, |p|^{r_i}).$$

2.2.7 Definition. We call a subset $Y \subseteq \mathbb{P}^{1,rig}(\mathbb{C}_p)$ a **subdomain with holes** of the rigid analytic variety $\mathbb{P}^{1,rig}_{\mathbb{Q}_p}$ if there exist points $a_1, \ldots, a_s \in \mathbb{P}^{1,rig}(\mathbb{Q}_p)$ and positive real numbers $r_1, \ldots, r_s \in \mathbb{R}_{\geq 0}$ such that

$$Y = \mathbb{P}^{1,rig}(\mathbb{C}_p) \smallsetminus \bigcup_{i=1}^{s} \mathbb{B}^-(a_i, |p|^{r_i}).$$

2.2.8 Proposition. *A ball with holes of $\mathbb{B}_{\mathbb{Q}_p}$ holds a structure of affinoid subdomain of $\mathbb{B}_{\mathbb{Q}_p}$.*

Proof. Let $Y := \mathbb{B}^+(a_0, |p|^{r_0}) \setminus \bigcup_{i=1}^{s} \mathbb{B}^-(a_i|p|^{,r_i})$ be a ball with holes in $\mathbb{B}_{\mathbb{Q}_p}$ such that the open balls $\mathbb{B}^-(a_i, |p|^{r_i})$, $1 \leq i \leq s$ are pairwise disjoint. Therefore Y can be written in the following way as a set of points:

$$Y = \{z \in \mathbb{C}_p : \ |z - a_0| \leq |p|^{r_0},\ |z - a_i| \geq |p|^{r_i},\ 1 \leq i \leq s\}.$$

Let us define the following change of coordinates:

$$x_0 := (z - a_0)/p^{r_0}$$

$$x_i := p^{r_i}/(z - a_i) \quad 1 \leq i \leq s$$

and the following set of points

$$Y' := \{(x_0, x_1, \ldots, x_s) \in \mathbb{B}^{s+1}(\mathbb{C}_p) \mid \ x_0 = \frac{z - a_0}{p^{r_0}},\ x_i = \frac{p^{r_i}}{z - a_i},\ 1 \leq i \leq s\}.$$

Hence the sets Y and Y' are in bijection.

Now, Y' is the set of points of $\mathrm{Sp}(T_{s+1}/\mathfrak{a}) = \mathbb{Q}_p\langle\chi_0, \ldots, \chi_s, \zeta\rangle/\mathfrak{a}$, where $\mathfrak{a}$ is the following ideal:

$$\mathfrak{a} := (\chi_0 p^{r_0} - (\zeta - a_0), \chi_1(\zeta - a_1) - p^{r_1}, \ldots, \chi_s(\zeta - a_s) - p^{r_s}),$$

i.e. there is a bijection $\mathrm{Max}(T_{s+1}/\mathfrak{a}) \simeq Y'$.

Finally it is easy to prove that the affinoid $\mathbb{Q}_p$-variety $\mathrm{Sp}(T_{s+1}/\mathfrak{a})$ and the affinoid morphism $\mathrm{Sp}(T_{s+1}/\mathfrak{a}) \to \mathrm{Sp}\,\mathbb{Q}_p\langle\zeta\rangle$ induced by the change of variables

$$\zeta \in \mathbb{Q}_p\langle\zeta\rangle \longmapsto \left(\frac{\zeta - a_0}{p^{r_0}}, \frac{p^{r_1}}{\zeta - a_1}, \ldots, \frac{p^{r_s}}{\zeta - a_s}\right) \in T_{s+1}/\mathfrak{a}$$

satisfy all the conditions of Definition 2.1.15. □

The following theorem is proved in [BGR84, 9.7.2/2].

2.2.9 Theorem. *Every admissible open subset of the rigid analytic variety $\mathbb{B}_{\mathbb{Q}_p}$ is obtained as a union of balls with holes of $\mathbb{B}_{\mathbb{Q}_p}$.* □

2.2.10 Proposition. *Every admissible open subset of the rigid analytic variety $\mathbb{P}^{1,rig}$ over $\mathbb{Q}_p$ is obtained as a union of subdomains with holes of $\mathbb{P}^{1,rig}$.*

PROOF. Straightforward after Theorem 2.2.9, since we have seen that $\mathbb{P}^{1,rig}$ admits an admissible cover in affinoid subvarieties isomorphic to $\mathbb{B}_{\mathbb{Q}_p}$. □

2.2.11 Remark. If we write the rigid projective line again as a union of affnoid varieties $\mathbb{P}^{1,rig} = X_0 \cup X_1$ such that $X_i \simeq \mathbb{B}_{\mathbb{Q}_p}$, $i = 0, 1$, then we can see that every admissible open subset of $\mathbb{P}^{1,rig}$ is of the type $Y \subseteq \mathbb{P}^{1,rig}(\mathbb{C}_p)$ such that $Y \cap X_0$ and $Y \cap X_1$ are affinoid subdomains of the affinoid variety $\mathbb{B}_{\mathbb{Q}_p}$.

2.2.12 Definition. We define a functor from the category of field extensions $L|\mathbb{Q}_p$ such that $\mathbb{Q}_p \subseteq L \subseteq \mathbb{C}_p$, to the category of sets: for every extension $L|\mathbb{Q}_p$ let us define the following subset of $\mathbb{P}^{1,rig}(L)$:

$$\mathcal{H}_p(L) := \mathbb{P}^{1,rig}(L) \smallsetminus \mathbb{P}^{1,rig}(\mathbb{Q}_p)$$

In particular, $\mathcal{H}_p(\mathbb{C}_p) = \mathbb{P}^{1.rig}(\mathbb{C}_p) \smallsetminus \mathbb{P}^{1,rig}(\mathbb{Q}_p)$ and $\mathcal{H}_p(\mathbb{Q}_p) = \emptyset$.

2.2.13 Remark. Note that if we replace $\mathbb{Q}_p$ by $\mathbb{R} = \mathbb{Q}_\infty$ and $\mathbb{C}_p$ by $\mathbb{C} = \widehat{\overline{\mathbb{Q}}}_\infty = \overline{\mathbb{Q}}_\infty$ what we obtain is actually two copies of the Poincaré upper half-plane:

$$\mathcal{H}_\infty := \mathbb{P}^1(\mathbb{C}) \smallsetminus \mathbb{P}^1(\mathbb{R}) = \{z \in \mathbb{C} \mid \operatorname{Im}(z) \neq 0\}.$$

We are going to show that $\mathcal{H}_p(L)$ is not only a subset of $\mathbb{P}^{1,rig}(L)$ but that it is actually a rigid analytic variety over $\mathbb{Q}_p$ which is called the **p-adic upper half-plane over $\mathbb{Q}_p$**.

2.2.14 Definition. For every integer $i \geq 0$ let us define the following subsets of points of $\mathbb{P}^{1,rig}(L)$:

$$\mathcal{H}_p^{(i),+}(L) := \mathbb{P}^{1,rig}(L) \smallsetminus \bigcup_{a \in \mathbb{P}^{1,rig}(\mathbb{Q}_p)} \mathbb{B}^+(a, |p|^i),$$

$$\mathcal{H}_p^{(i)}(L) := \mathbb{P}^{1,rig}(L) \smallsetminus \bigcup_{a \in \mathbb{P}^{1,rig}(\mathbb{Q}_p)} \mathbb{B}^-(a, |p|^i).$$

2.2.15 Notation. Let us denote by $\mathcal{P}_i$ a system of representatives for the points of $\mathbb{P}^1(\mathbb{Q}_p)$ mod p^i.

Specifically, $\mathcal{P}_i$ is the set of points $[a_0 : a_1] \in \mathbb{P}^1(\mathbb{Q}_p)$ such that its unimodular coordinates (a_0, a_1) are a system of representatives for $\mathbb{P}^1(\mathbb{Z}_p/p^i\mathbb{Z}_p)$, i.e.

$$(\tilde{a}_0, \tilde{a}_1) \in \mathbb{Z}_p/p^i\mathbb{Z}_p \times \mathbb{Z}_p/p^i\mathbb{Z}_p \text{ not both of them} \equiv 0 \,(\operatorname{mod} p).$$

Therefore we can also write:

$$\mathcal{P}_i := \mathbb{P}^1\left(\frac{\mathbb{Z}_p}{p^i\mathbb{Z}_p}\right) \simeq \frac{\mathbb{Z}_p}{p^i\mathbb{Z}_p} \cup \frac{p\mathbb{Z}_p}{p^i\mathbb{Z}_p}$$

The cardinality of this set is $p^i + p^{i-1} = p^{i-1}(p+1)$. This is very enlightening, as we shall see later in the section regarding the Bruhat-Tits tree (cf. Remark 2.2.25).

In particular

$$\mathcal{P}_1 = \mathbb{P}^1(\mathbb{F}_p) \simeq \mathbb{F}_p \cup \{\infty\}.$$

The following lemma allows us to simplify the description of the subsets in Definition 2.2.14.

2.2.16 Lemma. *Let $i > 0$ be an integer, $a, a' \in \mathbb{P}^{1,rig}(\mathbb{Q}_p)$. Then*

(a) $\mathbb{B}^+(a, |p|^i) \cap \mathbb{B}^+(a', |p|^i) \neq \emptyset \iff a \equiv a' \,(\mathrm{mod}\, p^i)$.

(b) $\mathbb{B}^-(a, |p|^i) \cap \mathbb{B}^-(a', |p|^i) \neq \emptyset \iff a \equiv a' \,(\mathrm{mod}\, p^{i+1})$.

Proof. Point (a) is proved by the equivalences

$$|a - a'| \leq |p|^i \iff v(a - a') \geq i \iff p^i | (a - a').$$

Point (b) is proved by the equivalences

$$|a - a'| < |p|^i \iff v(a - a') \geq i + 1 \iff p^{i+1} | (a - a').$$

□

2.2.17 Proposition. *For every integer $i > 0$, we have the following equalities of sets:*

$$\mathcal{H}_p^{(i),+}(L) = \mathbb{P}^{1,rig}(L) \smallsetminus \bigcup_{a \in \mathcal{P}_i} \mathbb{B}^+(a, |p|^i),$$

$$\mathcal{H}_p^{(i)}(L) = \mathbb{P}^{1,rig}(L) \smallsetminus \bigcup_{a \in \mathcal{P}_i} \mathbb{B}^-(a, |p|^{i-1}).$$

Proof. This is immediate after Lemma 2.2.16 and recalling the basic properties of non-Archimedean balls to be either disjoint or one contained in the other (but never with non-trivial intersection). □

2.2.18 Corollary. *The sets $\mathcal{H}_p^{(i)}$ are admissible open subsets of the rigid analytic variety $\mathbb{P}^{1,rig}$.*

PROOF. By Proposition 2.2.17, the subsets $\mathcal{H}_p^{(i)}$ are subdomains with holes of $\mathbb{P}^{1,rig}$ and so by Proposition 2.2.10 they have a structure of admissible open subsets of $\mathbb{P}^{1,rig}$. □

Following the same idea as the proof of Proposition 2.2.9, we want to write down explicitly the *equations* realizing the subsets $\mathcal{H}_p^{(i)}$ as an affinoid subdomain of $\mathbb{P}^{1,rig}_{\mathbb{Q}_p}$.

2.2.19 Proposition. *Let $n > 0$ be a fixed integer.*

Let $\alpha_0, \ldots, \alpha_{p^n-1}$ and $\beta_0, \ldots, \beta_{p^{n-1}-1}$ be representatives for the $p^{n-1}(p+1)$ classes of $\mathbb{P}^1(\mathbb{Z}_p/p^n\mathbb{Z}_p)$ such that

(a) $\alpha_i \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ for every $0 \leq i \leq p^n - 1$,

(b) $\beta_0 = 0$ and $\beta_j \in p\mathbb{Z}_p$ for every $1 \leq j \leq p^{n-1} - 1$.

Then a point $z \in \mathbb{P}^{1,rig}(L)$ belongs to the sets $\mathcal{H}_p^{(n)}(L)$ if and only if it satisfies one and only one of the following inequalities:

(i) $|z - \alpha_i| \geq |p|^{n-1}$, for every $0 \leq i \leq p^n - 1$,

(ii) $|z - \frac{1}{\beta_j}| \geq |p|^{n-1-v_p(\beta_j)}$, for every $1 \leq j \leq p^{n-1} - 1$,

(iii) $|z| \geq |p|^{-(n-1)}$.

PROOF. Let (a_0, a_1) be the unimodular coordinates of a point $a \in \mathcal{P}_n$. We the distinguish three cases:

(1) If $a_1 \not\equiv 0 \pmod{p}$, then $[a_0 : a_1] = [a_0/a_1 : 1] \simeq \alpha \in \mathbb{Z}_p/p^n\mathbb{Z}_p$, and we obtain inequality (i).

(2) If $a_1 \equiv 0 \pmod{p}$ and $a_1 \not\equiv 0 \pmod{p}$, then $[a_0 : a_1] = [1 : \frac{a_1}{a_0}] = [1 : \beta]$, where β is a class in $p\mathbb{Z}_p/p^n\mathbb{Z}_p$, and $\beta \not\equiv 0 \pmod{p^n}$. In this case we would first obtain the inequality:

$$|z\beta - 1| \geq |p|^{n-1}$$

and dividing everything by $|\beta| > 0$, we find inequality (ii).

(3) If $a_1 \equiv 0 \pmod{p^n}$ and $[a_0 : a_1] = [1 : a_1/a_0] = [1 : 0] =: \infty \in \mathbb{P}^{1,rig}(\mathbb{Q}_p)$, then

$$|1/z| \leq |p|^{n-1},$$

and so in this case we find inequality (iii).

□

2.2.20 Corollary. *Lat $n > 0$ be a positive integer and let $\alpha_0, \ldots, \alpha_{p^n-1}$ and $\beta_0, \ldots, \beta_{p^{n-1}-1}$ be as in Proposition 2.2.19.*

Let $T_{p^{n-1}(p+1)}$ be the Tate algebra over $\mathbb{Q}_p$ with variables

$$X, Y := (Y_0, \ldots, Y_{p^n-1}), Z := (Z_0, \ldots, Z_{p^{n-1}-1})$$

and let $\mathfrak{a}$ be the ideal of $T_{p^{n-1}(p+1)}$ generated by the following strictly convergent series:

(*i*)
$$f_i(X, Y, Z) := Y_i(X - \alpha_i) - p^{n-1} \qquad 0 \leq i \leq p^n - 1,$$

(*ii*)
$$g_j(X, Y, Z) := Z_j \left(X - \frac{1}{\beta_j} \right) - p^{n-1-v_p(\beta_j)} \qquad 0 \leq j \leq p^{n-1} - 1,$$

(*iii*)
$$g_0(X, Y, Z) := Z_0 - p^{n-1} X.$$

Then the subset $\mathcal{H}_p^{(n)}(L)$ is the set of L-points of the affinoid variety $\mathrm{Sp}(T_{p^{n-1}(p+1)}/\mathfrak{a})$.

Finally we have endowed the subset of points $\mathcal{H}_p(L) \subseteq \mathbb{P}^{1,rig}(L)$, for every L, with a cover in admissible affinoid subdomains of $\mathbb{P}^{1,rig}$. If we prove that the cover $\{\mathcal{H}_p^{(i)}\}_{i>0}$ is admissible, then by Definition 2.1.20, $\mathcal{H}_p$ is a rigid analytic variety over $\mathbb{Q}_p$, as claimed at the beginning of the section. This is proved in [SS91].

Moreover it can be also proved that the subsets $\mathcal{H}_p^{(i),+}$ are admissible open subsets of $\mathbb{P}^{1,rig}$, although in this case these are not affinoid subdomains of $\mathbb{P}^{1,rig}$, and that the cover $\{\mathcal{H}_p^{(i),+}\}$ is an admissible cover for the rigid analytic variety $\mathcal{H}_p$, , according to Definition 2.1.18.

2.2.2 Special fibre: the Bruhat-Tits tree

In this section we define the p-adic Bruhat-Tits tree. Roughly speaking this is the dual of the reduction mod p of the p-adic upper half-plane $\mathcal{H}_p$ described in the previous section.

We will see that this tree can be presented in, at least, four different ways. Indeed, its vertices admit a description as:

(1) Classes of homothetic *lattices* in $\mathbb{Q}_p^2$.

(2) Classes of equivalent *norms* on these lattices.

(3) Classes of *matrices* in $\mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$.

(4) Types of maximal *quaternion orders* in the quaternion algebra $\mathrm{M}_2(\mathbb{Q}_p)$.

2.2.2.1 Tree of lattices

A lattice $M \subseteq \mathbb{Q}_p^2$ is a free $\mathbb{Z}_p$-module of rank 2. Two lattices $M, M' \subseteq \mathbb{Q}_p^2$ are said to be homothetic if there exists $\lambda \in \mathbb{Q}_p^*$ such that $M' = \lambda M$. We will denote by $\{M\}$ the homothety class of M. For every two such homothety classes $\{M\}, \{M'\}$, we can always choose the representatives such that $p^n M \subseteq M' \subseteq M$, for some $n \in \mathbb{N}$ (cf. [Ser77, 1.1]). For example, if $M = \langle u, v\rangle$, then we can take $M' = \langle u, p^n v\rangle$. We say that two homothety classes $\{M\}, \{M'\}$ are **adjacent** if their representatives can be chosen such that $pM \subsetneq M' \subsetneq M$.

2.2.21 Definition. We define the graph $\mathcal{T}_p$ whose set of vertices $\mathrm{Ver}(\mathcal{T}_p)$ is formed by the homothety classes of lattices of $\mathbb{Q}_p^2$ and whose set of oriented edges $\mathrm{Ed}(\mathcal{T}_p)$ is formed by the pairs of adjacent classes.

Moreover the set of of unoriented edges is formed by unordered pairs of adjacent classes and is denoted by $\mathrm{Ed}^*(\mathcal{T}_p)$.

The graph $\mathcal{T}_p$ is actually a $(p+1)$-regular tree (cf. [Ser77, 1.1]) which in the literature is called the **Bruhat-Tits tree associated to** $\mathrm{PGL}_2(\mathbb{Q}_p)$.

The group $\mathrm{PGL}_2(\mathbb{Q}_p)$ acts on the set of vertices $\mathrm{Ver}(\mathcal{T}_p)$ by *base change*. Let us describe this action in detail.

Let us take a $\mathbb{Z}_p$-base $\mathcal{B} = \{e_1, e_2\}$ of the vectorial space $\mathbb{Q}_p^2$ and a lattice $M = \langle u, v\rangle \subseteq \mathbb{Q}_p^2$ such that $u = (u_1, u_2)_{\mathcal{B}}, v = (v_1, v_2)_{\mathcal{B}}$. If $\gamma \in \mathrm{GL}_2(\mathbb{Q}_p)$ then $\gamma \cdot M := \langle \gamma u^t, \gamma v^t\rangle$. The induced action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on the classes of lattices is then clearly well-defined and is a transitive action.

2.2.22 Notation. If $y = (v, v') \in \mathrm{Ed}(\mathcal{T}_p)$ is an oriented edge then we will denote by $\overline{y} := (v', v)$ the **inverse** edge and we will sometimes denote by $\{y, \overline{y}\}$ the corresponding unoriented edge (according to [Kur79, Definition 3-1]), so that

$$\mathrm{Ed}^*(\mathcal{T}_p) = \{\{y, \overline{y}\} \mid y \in \mathrm{Ed}(\mathcal{T}_p)\}.$$

Finally, we will denote by v^0 the vertex of $\mathcal{T}_p$ whose representative is the lattice $M^0 := \langle (1,0), (0,1)\rangle$.

Once we have fixed v^0 as a distinguished vertex, we can describe the Bruhat-Tits tree $\mathcal{T}_p$ in the following form.

(a) We start describing the set of vertices of $\mathcal{T}_p$ adjacent to v^0.

For every $i \in \mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\}$, let v_i^0 denote the vertex represented by the lattice M_i^0 where

$$\begin{cases} M_i^0 := \langle (p,0),(i,1)\rangle, & \text{if } i \neq \infty, \\ \\ M_\infty^0 := \langle (1,0),(0,p)\rangle, & \text{if } i = \infty. \end{cases}$$

It is an easy computation to see that we have actually defined $p+1$ different vertices $v_0^0, \ldots, v_{p-1}^0, v_\infty^0$ which are adjacent to v^0.

We will denote by y_i the oriented edge (v^0, v_i^0).

(b) For every new vertex v_i^0 we define the $p+1$ adjacent vertices as the vertices v_{ij}^0 represented by the lattices

$$\begin{cases} M_{ij}^0 := \langle (p^2,0),(j,1)\rangle, & \text{if } i \neq \infty,\ \ 0 \leq j \leq p^2-1,\ \ j \equiv i \,(\mathrm{mod}\, p), \\ \\ M_{\infty j}^0 := \langle (1,j),(0,p^2)\rangle, & \text{if } i = \infty,\ \ 0 \leq j \leq p^2-1,\ \ j \equiv 0 \,(\mathrm{mod}\, p). \end{cases}$$

We will denote by y_{ij} the oriented edge (v^0, v_{ij}^0).

2.2.2.2 Tree of norms

Let us now consider a geometric realization of the tree $\mathcal{T}_p$: this means that we can think of each oriented edge (v, v') as the real open interval $(0,1)$ such that the extremal vertices v, v' correspond respectively to the real numbers 0 and 1. Specifically, for every edge $(v, v') \in \mathrm{Ed}(\mathcal{T}_p)$ we can define a map:

$$t \in [0,1] \longmapsto P(t) := \begin{cases} (1-t)v + tv' & t \in (0,1) \\ v & t = 0 \\ v' & t = 1 \end{cases} \in (v, v') \cup \{v, v'\}.$$

The point $P(t)$ is called **the point at distance t from the vertex v** .

This will be done in three steps:

(1) If $v = [M] \in \mathrm{Ver}(\mathcal{T}_p)$ such that $M = \langle u_1, u_2\rangle$, then we associate to v the class of equivalent norms on M represented by the following norm

$$|au_1 + bu_2|_M := \sup\{|a|, |b|\}.$$

(2) If $(v, v') \in \mathrm{Ed}(\mathcal{T}_p)$ such that $M = \langle u_1, u_2 \rangle$ and $M' = \langle u_1, pu_2 \rangle$, then to the edge (u, v) there corresponds, by (1), the pair of classes of equivalent norms on M and M' respectively, represented by the norms:

$$|au_1 + bu_2|_M = \sup\{|a|, |b|\}, \qquad |au_1 + bu_2|_{M'} := \sup\{|a|, p|b|\}.$$

(3) Finally the point $P(t) = (1-t)v + tv'$ on the edge (v, v') is natural is obtained as the class of norms represented by the norm

$$|au_1 + bu_2|_t := \sup\{|a|, p^t|b|\},$$

even if this norm does not correspond to any norm on a lattice in $\mathbb{Q}_p^2$.

In this way the tree $\mathcal{T}_p$, which is a combinatorial object, is realized as a topological space which we continue to denote by $\mathcal{T}_p$. For more details see [BC91, Introduction, Sec. 1].

When we restrict the same construction to points $P(t)$ on the tree $\mathcal{T}_p$ arising from rational parameters $t \in [0, 1] \cap \mathbb{Q}$, we refer to the corresponding geometric realization as the **rational geometric realization of the tree** $\mathcal{T}_p$ and we denote it by $\mathcal{T}_{p,\mathbb{Q}}$.

2.2.2.3 Tree of matrices

The following would be the p-adic analog of Proposition 1.2.24.

2.2.23 Proposition. *If we denote by v^0 the vertex of $\mathcal{T}_p$ with representatives $\mathbb{Z}_p^2 = \langle (1, 0), (0, 1) \rangle$, then the map*

$$\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p) \longmapsto \gamma \cdot v^0 \in \mathrm{Ver}(\mathcal{T}_p)$$

induces a homeomorphism

$$\mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p) \simeq \mathcal{T}_p,$$

where the topology on $\mathcal{T}_p$ is the natural one induced on its geometric realization.

Proof. As usual, this is immediate after [Shi70a, 1.2], once we have observed that the map is surjective, since the action is transitive, and the stabilizer of the vertex v^0 inside $\mathrm{PGL}_2(\mathbb{Q}_p)$ is $\mathrm{PGL}_2(\mathbb{Z}_p)$. □

By Proposition 2.2.23, we can represent each vertex by a class of matrices. Namely, if $v = \{M\}$ then v is represented by the class

$$\{\alpha_M\} \in \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p),$$

such that α_M is the matrix whose columns are the base vectors of M.

2.2.24 Remark. Note that matrices lying in the same class do not always have the same determinant. Their determinants, though, have the same parity in the p-adic valuation.

So we can say that a vertex $v = \{\alpha\} \in \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$ is **even** if $v_p(\det \alpha) \equiv 0 \pmod 2$ and that it is **odd** otherwise.

Note also that a transformation $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$ sends a vertex v to another one with the same parity if and only if $v_p(\det \gamma)$ is even.

With this description of the tree, we can define an ascending chain of subtrees of $\mathcal{T}_p$. For every integer $i \geq 0$, we define the tree $\mathcal{T}_p^{(i)}$ as the subtree of $\mathcal{T}_p$ whose set of vertices is

$$\mathrm{Ver}(\mathcal{T}_p^{(i)}) := \{v = \{\alpha\} \mid \ v_p(\det \alpha) \leq i\}.$$

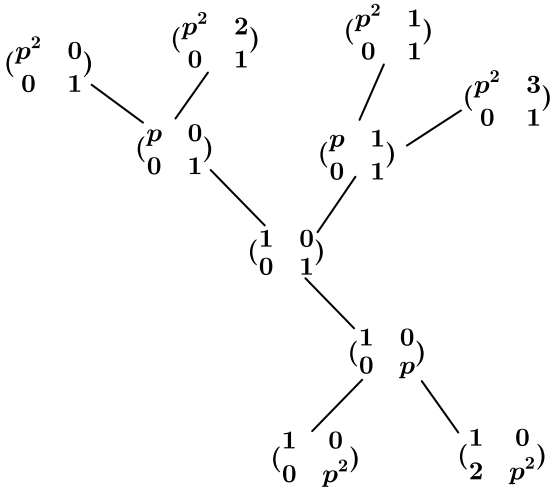
Clearly,

(a) $\mathrm{Ver}(\mathcal{T}_p^{(0)}) = \{v^0\}$,

(b) $\mathrm{Ver}(\mathcal{T}_p^{(i)}) \subseteq \mathrm{Ver}(\mathcal{T}_p^{(i+1)})$ for every $i \geq 0$,

(c) $\mathcal{T}_p = \bigcup_{i \geq 0} \mathcal{T}_p^{(i)}$.

We can now give a picture of the Bruhat-Tits as a "tree of matrices", using the system of representatives just computed. We do it below for the subtree $\mathcal{T}_p^{(2)}$ and for $p = 2$:



2.2.25 Remark. The vertex v^0 corresponds to the projective line $\mathbb{P}^1_{\mathbb{Z}_p} = \mathbb{P}(M^0)$ associated to the lattice $M^0 = \mathbb{Z}_p^2$ in [Mum72, Sec. 2] and the $p+1$ adjacent vertices correspond to projective lines obtained by blowing up the $p+1$ $\mathbb{F}_p$-rational points of $\mathbb{P}^1_{\mathbb{F}_p}$ inside $\mathbb{P}^1_{\mathbb{Z}_p}$.

2.2.26 Remark. (Intuitive) If we look back at the admissible cover defined for the upper half-plane $\mathcal{H}_p$ in Definition 2.2.14 and Proposition 2.2.17, then we will observe that the set of representatives $\mathcal{P}_i$ for the points of the projective line $\mathbb{P}(\mathbb{Z}_p/p^i\mathbb{Z}_p)$ corresponds bijectively with set of "added vertices" of the subtree $\mathcal{T}_p^{(i-1)}$, i.e. there is a bijection of sets

$$\mathrm{Ver}(\mathcal{T}_p^{(i-1)}) \smallsetminus \mathrm{Ver}(\mathcal{T}_p^{(i-2)}) \simeq \mathcal{P}_i,$$

for every $i \geq 1$.

The intuition then would suggest that removing open balls in $\mathbb{P}^{1,rig}(\mathbb{C}_p)$ with center in $\mathcal{P}_i$ corresponds through this bijection to adding to the subtree $\mathcal{T}_p^{(i-2)}$ the vertices of the subtree $\mathcal{T}^{(i-1)}$. This intuition will find its theoretical explanation in Theorem 2.2.31, as will be explained in the related remarks.

2.2.2.4 Tree of quaternion orders

Let B be a definite quaternion algebra over $\mathbb{Q}$ of discriminant D_B such that the prime p does not divide D_B.

Another description of the Bruhat-Tits tree defined above can be given in terms of maximal orders and Eichler orders of the local algebra $B_p :=$

$B \otimes_{\mathbb{Q}} \mathbb{Q}_p$, which is the matrix algebra $\mathrm{M}_2(\mathbb{Q}_p)$. Let us fix once and for all an isomorphism $\Phi_p : B_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$.

Therefore in [Vig80, II, 2.1] the following result is proved.

2.2.27 Lemma. *If M is a lattice in $\mathbb{Q}_p^2$, then the ring of endomorphism $\mathrm{End}(M) \subseteq \mathrm{M}_2(\mathbb{Q}_p)$ is a maximal order inside the $\mathbb{Q}_p$-algebra of endomorphisms $\mathrm{End}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \simeq \mathrm{M}_2(\mathbb{Q}_p)$, which is uniquely determined up to conjugation. Moreover every maximal order of $\mathrm{End}(\mathbb{Q}_p^2)$ is of this form.* □

Given a homothety class of lattices $\{M\}$, we denote by $\mathcal{O}_{\{M\}}$ the corresponding maximal order in B_p which is well defined up to conjugation, namely

$$\mathcal{O}_{\{M\}} := \Phi_p^{-1}(\mathrm{End}(M)).$$

2.2.28 Proposition. *Let $\mathcal{O}_1, \mathcal{O}_2$ be maximal orders of B_p and put $\mathcal{O} := \mathcal{O}_1 \cap \mathcal{O}_2$. Then $\mathcal{O}$ is an Eichler order of level p if and only if there exist two classes of adjacent vertices $\{M_1\}, \{M_2\} \in \mathrm{Ver}(\mathcal{T}_p)$ such that $\mathcal{O}_1 = \mathcal{O}_{\{M_1\}}$ and $\mathcal{O}_2 = \mathcal{O}_{\{M_2\}}$.* □

This suggests the following bijection:

2.2.29 Proposition. (*i*) *There is a bijection between the set of vertices $\mathrm{Ver}(\mathcal{T}_p)$ of the Bruhat-Tits tree $\mathcal{T}_p$ and the set of maximal local orders of B_p, given by*

$$\{M\} \in \mathrm{Ver}(\mathcal{T}_p) \longmapsto \mathcal{O}_{\{M\}} \subseteq B_p.$$

The map depends on the isomorphism Φ_p and also on the choice of a basis for $\mathbb{Q}_p^2$.

(*ii*) *There is a bijection between the set $\mathrm{Ed}^*(\mathcal{T}_p)$ of unoriented edges of the Bruhat-Tits tree $\mathcal{T}_p$ and the set of Eichler orders of level p of B_p, given by*

$$\{\{M_1\}, \{M_2\}\} \in \mathrm{Ed}^*(\mathcal{T}_p) \longmapsto \mathcal{O}_{12} := \mathcal{O}_{\{M_1\}} \cap \mathcal{O}_{\{M_2\}} \subseteq B_p.$$

Proof. After Proposition 2.2.28, we only need to show that the map is well-defined and injective, i.e. that two latices $M, M' \subseteq \mathbb{Q}_p^2$ have the same endomorphism ring if and only if they are homothetic, which is trivial. □

The action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on the tree $\mathcal{T}_p$, with respect to this new description is explained in the following result.

2.2.30 Proposition. *Let $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$. Then*

(i) If $\{M\}$ is a vertex of $\mathcal{T}_p$, then

$$\mathcal{O}_{\gamma\{M\}} = \gamma \mathcal{O}_{\{M\}} \gamma^{-1}.$$

(ii) If $\{\{M_1\}, \{M_2\}\}$ is an edge of $\mathcal{T}_p$ and $\mathcal{O} := \mathcal{O}_{\{M_1\}} \cap \mathcal{O}_{\{M_2\}}$ is its associated Eichler order of level p, then

$$\mathcal{O}_{\gamma\{M_1\}} \cap \mathcal{O}_{\gamma\{M_2\}} = \gamma \mathcal{O} \gamma^{-1}.$$

Proof. The proof is an immediate application of base changes in the lattices M_1, M_2. □

This interpretation of the Bruhat-Tits tree in terms of orders of the local algebra B_p can be easily translated into one considering orders of the global algebra B.

Let us fix a maximal order $\mathcal{O}_B \subseteq B$ and let us consider the set of maximal orders $\mathcal{O}'_B \subseteq B$ such that

$$\begin{cases} \mathcal{O}'_{B,\ell} := \mathcal{O}_{B,\ell} & \text{for } \ell \neq p \\ \mathcal{O}'_{B,p} := x\mathcal{O}_{B,p}x^{-1} & \text{for some } x \in B_p. \end{cases}$$

This set is clearly in bijection with the one of local maximal orders of B_p.

Moreover if we take the maximal order $\mathcal{O}_B \subseteq B$ to be such that $\mathcal{O}_{B,p} = \mathcal{O}_{\{M^0\}}$, where we have defined $M^0 := \langle (1,0), (0,1) \rangle = \mathrm{M}_2(\mathbb{Z}_p)$. In this way we have the following bijections:

$$\mathrm{Ver}(\mathcal{T}_p) \simeq \mathrm{GL}_2(\mathbb{Q}_p)/\mathbb{Q}_p^* \mathrm{GL}_2(\mathbb{Z}_p) \simeq B_p^*/\mathbb{Q}_p^* \mathcal{O}_{B,p}^*.$$

Note that the $\mathbb{Q}_p^* \mathcal{O}_{B,p}^*$ is isomorphic to the normalizer

$$\mathrm{Nor}(\mathcal{O}_{B,p}) := \{\alpha \in B_p^* \mid \alpha^{-1} \mathcal{O}_{B,p} \alpha = \mathcal{O}_{B,p}\}.$$

2.2.3 The reduction map

2.2.31 Theorem. *For every extension L of $\mathbb{Q}_p$ contained in $\mathbb{C}_p$, there exists a map*

$$\mathrm{Red} : \mathcal{H}_p(L) \to \mathcal{T}_p$$

which is equivariant with respect to the action of the group $\mathrm{PGL}_2(\mathbb{Q}_p)$*, i.e. such that*

$$\mathrm{Red}(\gamma \cdot z) = \gamma \cdot \mathrm{Red}(z)$$

for every $z \in \mathcal{H}_p(L)$ *and every* $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$*.*

Moreover the image of this map is the rational geometric realization of the tree $\mathcal{T}_p$*, i.e.*

$$\mathrm{Red}(\mathcal{H}_p) = \mathcal{T}_{p,\mathbb{Q}}.$$

Proof. Let us fix an extension $\mathbb{Q}_p \subseteq L \subseteq \mathbb{C}_p$.

Given a point $z = [z_0 : z_1] \in \mathcal{H}_p(L)$ we can define a non-zero injective $\mathbb{Q}_p$-linear map

$$\begin{array}{rccc} \lambda_z : & \mathbb{Q}_p^2 & \longrightarrow & L \\ & (x,y) & \longmapsto & z_0 x + z_1 y \end{array}$$

and the association

$$\begin{array}{ccc} \mathcal{H}_p(L) & \longrightarrow & \{\mathbb{Q}_p^2 \to L \mid \mathrm{non-zero\,and\,injective}\}/\mathbb{Q}_p^* \\ z & \longmapsto & \lambda_z. \end{array}$$

is actually a bijection between the set of L-points $\mathcal{H}_p(L)$ and the set of $\mathbb{Q}_p^*$-homothety classes of non-zero and injective $\mathbb{Q}_p$-linear map $\mathbb{Q}_p^2 \hookrightarrow L$.

Now, we can define $\mathrm{Red}(z)$ to be the class of equivalent norms $\{|\cdot|_z\}$ on $\mathbb{Q}_p^2$ defined by

$$|(x,y)|_z := |\lambda_z(x,y)|, \quad (x,y) \in \mathbb{Q}_p^2.$$

Hence, since the norm $|\cdot|_z$ associated to a point $z \in \mathbb{P}^1(\mathbb{C}_p)$ has values in $\{p^r \mid r \in \mathbb{Q}\}$, then $\mathrm{Red}(z)$ defines a point $P(t)$ on the rational geometric realization $\mathcal{T}_{p,\mathbb{Q}}$ of the tree $\mathcal{T}_p$.

Finally the fact that the map Red is equivariant is a simple calculation. □

We write this map as $\mathrm{Red} : \mathcal{H}_p \to \mathcal{T}_p$ and call it **reduction map associated to** $\mathcal{H}_p$.

The reduction map just defined owes its name to the fact that it is intimately related with the usual reduction modulo the prime p, as is explained in the following important remark.

2.2.32 Remark. We can restrict the reduction map defined to the local pieces $\mathcal{H}_p^{(i)}$ by defining the rigid analytic spaces $\mathcal{H}_p$ and obtaining a *finite* reduction map.

(1) Using the inequalities of Corollary 2.2.19 defining the affinoid cover $\{\mathcal{H}_p^{(i)}\}_{i\geq 1}$, it can be seen explicitly that for every $i \geq 1$,

$$\mathrm{Red}^{-1}(\mathcal{T}_{p,\mathbb{Q}}^{(i-1)}) = \mathcal{H}_p^{(i)}.$$

This is done in [BC91, 2.3] where actually the affinoid subdomain $\mathcal{H}_p^{(i)}$ is defined by this last equality.

(2) On the other side, equations given in Theorem 2.2.20 can be reduced modulo p through the "reduction mod p of restricted series" described in Proposition 2.1.3, and this gives an algebraic variety over $\mathbb{F}_p$.

It is then an exercise to see that the dual graph of the reduction mod p of $\mathcal{H}_p^{(i)}$ (i.e. the graph whose vertices are the irreducible components of the algebraic variety over $\mathbb{F}_p$ and such two vertices are adjacent iff the corresponding irreducible components meet) is the tree $\mathcal{T}_p^{(i-1)}$.

This should explain the affirmations of Remark 2.2.25.

Note here that the reduction mod p of $\mathcal{H}_p^{(i)}$ is a finite algebraic variety and the corresponding tree $\mathcal{T}_p^{(i-1)}$ is a finite tree, which makes perfect sense!

(3) Passing the construction of (1) and (2) to the direct limit, we obtain that the dual graph of the reduction mod p of the *rigid analytic variety* $\mathcal{H}_p$ is the *infinite tree* $\mathcal{T}_p$.

Finally we can affirm concisely that: **the map** Red **of Theorem 2.2.31 is the *dual* of the reduction mod p associated to the rigid analytic space $\mathcal{H}_p$.**

2.3 Mumford uniformization

For every extension $L|\mathbb{Q}_p$, the group of automorphisms of the set $\mathcal{H}_p(L) = \mathbb{P}^1(L) \smallsetminus \mathbb{P}^1(\mathbb{Q}_p)$ is isomorphic to the group $\mathrm{PGL}_2(\mathbb{Q}_p)$, since every automorphism of this set can be expressed as

$$\begin{array}{ccc} \mathbb{P}^1(L) & \longrightarrow & \mathbb{P}^1(L) \\ z = [z_0 : z_1] & \longmapsto & [az_0 + bz_1 : cz_0 + dz_1] \end{array}$$

for a unique matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Q}_p)$.

The action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ over the set of points $\mathcal{H}_p(L) = L \smallsetminus \mathbb{Q}_p$ can also be defined in the following way:

Given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Q}_p)$ and $\tau \in \mathcal{H}_p(L)$,

$$\gamma \cdot \tau := \frac{a\tau + b}{c\tau + d}.$$

After what we have seen in Section 2.2, we know that:

(*i*) The group $\mathrm{PGL}_2(\mathbb{Q}_p)$ is actually the group of rigid analytic automorphisms of the rigid analytic space $\mathcal{H}_p$ over $\mathbb{Q}_p$, i.e.

$$\mathrm{Aut}(\mathcal{H}_p) \simeq \mathrm{PGL}_2(\mathbb{Q}_p).$$

(*ii*) The group $\mathrm{PGL}_2(\mathbb{Q}_p)$ is also the group of automorphisms of the Bruhat-Tits tree $\mathcal{T}_p$.

(*iii*) The reduction map

$$\mathrm{Red}_p : \mathcal{H}_p \to \mathcal{T}_p$$

defined in Theorem 2.2.31 is equivariant with respect to this action, i.e.

$$\mathrm{Red}_p(\gamma \cdot z) = \gamma \cdot \mathrm{Red}_p(z)$$

for every $z \in \mathcal{H}_p(L)$ and every $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$.

Note the analogy (and difference!) with respect to the Archimedean case: the Poincaré upper half-plane $\mathcal{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ has group of automorphisms isomorphic to $\mathrm{PGL}_2(\mathbb{R})_{>0} \simeq \mathrm{PSL}_2(\mathbb{R})$, because the complex analytic space $\mathbb{P}^1(\mathbb{C}) \smallsetminus \mathbb{P}^1(\mathbb{R})$ is not connected, although $\mathcal{H}_p$ it is, so we usually take one connected component and this reflects on the group of automorphisms.

The aim of this section is to introduce certain discrete subgroups of $\mathrm{PGL}_2(\mathbb{Q}_p)$ which are of particular interest in the theory of non-Archimedean uniformization of curves: these are the *p-adic Schottky groups*.

2.3.1 Transformations in $\mathrm{PGL}_2(\mathbb{Q}_p)$

We start by recalling how transformations in $\mathrm{PGL}_2(\mathbb{Q}_p)$ are classified. The following results have to be compared to the ones holding for transformations in $\mathrm{PSL}_2(\mathbb{R})$ in [Shi70a, Sec.1.2] and [AB04, Sec. 2.2].

2.3.1 Definition. Let $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$ be a transformation represented by a matrix having eigenvalues $\mu_1, \mu_2 \in \overline{\mathbb{Q}}_p$.

(*i*) γ is called **hyperbolic** if $|\mu_1| \neq |\mu_2|$.

(*ii*) γ is called **elliptic** if $\mu_1 \neq \mu_2, |\mu_1| = |\mu_2|$.

(*iii*) γ is called **parabolic** if $\mu_1 = \mu_2$.

2.3.2 Proposition. *Let us consider the following well-defined map*

$$t: \quad \mathrm{PGL}_2(\mathbb{Q}_p) \quad \longrightarrow \quad \mathbb{Q}_p$$

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \longmapsto \quad \frac{(a+d)^2}{ad-bc}.$$

Then we have the following characterizations:

(*i*) γ *is hyperbolic* $\iff |t(\gamma)| > 1$.

(*ii*) γ *is elliptic or parabolic* $\iff |t(\gamma)| \leq 1$.

(*iii*) γ *is hyperbolic if and only if* γ *is conjugated to a transformation in* $\mathrm{PGL}_2(\mathbb{Z}_p)$ *represented by a matrix* $\begin{pmatrix} \mu & 0 \\ 0 & 1 \end{pmatrix}$ *such that* $v_p(\mu) > 0$.

(*iv*) γ *is elliptic if and only if* γ *is conjugated to a transformation in* $\mathrm{PGL}_2(\mathbb{Z}_p)$ *represented by a matrix* $\begin{pmatrix} \mu & 0 \\ 0 & 1 \end{pmatrix}$ *such that* $v_p(\mu) = 0$.

(*v*) γ *is parabolic or elliptic if and only if* γ^2 *is conjugated to a transformation in* $\mathrm{PGL}_2(\mathbb{Z}_p)$.

Proof. If we set $\mu := \mu_1/\mu_2 \in \mathbb{C}_p$, then we have the following equality:

$$t(\gamma) = \frac{\mathrm{Tr}^2(\gamma)}{\mathrm{Det}(\gamma)} = \mu + \mu^{-1} + 2. \tag{2.3.1}$$

Condition $|\mu| = 1 = |\mu^{-1}|$ is equivalent to

$$|\mu + \mu^{-1} + 2| \leq \max\{|\mu|, |\mu^{-1}|, |2|\} = 1.$$

This proves equivalences (*i*) and (*ii*). To prove (*iii*), let us observe that for any $\sigma \in \mathrm{PGL}_2(\mathbb{Q}_p)$

$$t\left(\sigma \begin{pmatrix} \mu & 0 \\ 0 & 1 \end{pmatrix} \sigma^{-1}\right) = \frac{(\mu+1)^2}{\mu}$$

and so all the conjugated of $\begin{pmatrix} \mu & 0 \\ 0 & 1 \end{pmatrix}$, with $v_p(\mu) > 0$, represent hyperbolic transformations, by equivalence (i). Conversely, assume that γ is a hyperbolic element. By (i) we have that $\nu := v_p(t(\gamma)^{-1}) > 0$, i.e. $\mathrm{Det}(\gamma) = \nu \mathrm{Tr}^2(\gamma)$ and $v_p(\mathrm{Tr}(\gamma)) = 0$. So the characteristic polynomial of γ is

$$P_\gamma(X) = X^2 - \mathrm{Tr}(\gamma)X + \nu \mathrm{Tr}^2(\gamma)$$

and reducing it modulo p we find a polynomial with coefficient in $\mathbb{F}_p$ having two different roots $\{0, \overline{\mathrm{Tr}(\gamma)}\}$. By Hensel's lemma these two roots lift to two p-adic roots of the characteristic polynomials P_γ namely

$$x_1 = u\mathrm{Tr}(\gamma), \qquad x_2 = \nu u^{-1}\mathrm{Tr}(\gamma),$$

for some unit $u \in \mathbb{Z}_p^*$. Therefore γ is equivalent in $\mathrm{PGL}_2(\mathbb{Q}_p)$ to the matrix $\nu\mathrm{Tr}(\gamma)^{-1}\gamma$ and so it is a hyperbolic transformation.

For point (v) see [GvDP80, Lemma 1.4]. □

2.3.3 Definition. We can associate to every matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Q}_p)$, the following p-adic binary quadratic form:

$$f_\gamma(X, Y) := cX^2 + (d - a)XY - bY^2 \in \mathbb{Q}_p[X, Y].$$

We call **zeros of the quadratic form** f_γ the zeros of the quadratic polynomial $f_\gamma(X, 1) \in \mathbb{Q}_p[X]$.

2.3.4 Remark. Observe that the form f_γ has the following properties:

(i) The discriminant of the polynomial $f_\gamma(X, 1)$ is

$$\mathrm{disc}(f_\gamma(X, 1)) = (d - a)^2 + 4bc = \mathrm{Tr}^2(\gamma) - 4\mathrm{Det}(\gamma),$$

which turns out to be equal to the discriminant of the characteristic polynomial associated to γ.

(ii) The zeros of the form f_γ are the fixed points in $\mathcal{H}_p$ of the transformation represented by the matrix γ, i.e.

$$f_\gamma(\tau, 1) = 0 \iff \gamma \cdot \tau = \tau.$$

These important remarks make it clear that the binary quadratic form f_γ allows us to classify the transformation γ.

2.3.5 Proposition. *The following characterizations hold:*

(*i*) γ *is hyperbolic* $\iff$ $\operatorname{disc}(f_\gamma(X,1)) \in \mathbb{Q}_p^{*2}$ $\iff$ γ *has two different fixed points in* $\mathbb{P}^1(\mathbb{Q}_p)$.

(*ii*) γ *is elliptic* $\iff$ $\operatorname{disc}(f_\gamma(X,1)) \notin \mathbb{Q}_p^{*2}$ $\iff$ γ *has two different fixed points in* $\mathcal{H}_p(\mathbb{Q}_{p^2})$, *where* $\mathbb{Q}_{p^2}$ *denotes the unique unramified quadratic extension of* $\mathbb{Q}_p$ *contained in* $\mathbb{C}_p$.

(*iii*) γ *is parabolic* $\iff$ $\operatorname{disc}(f_\gamma(X,1)) = 0$ $\iff$ γ *has a unique fixed point in* $\mathbb{P}^1(\mathbb{Q}_p)$.

Note that, in contrast to the Archimedean case, the connectedness of the space $\mathcal{H}_p$ reflects into the fact that elliptic transformations have two fixed points instead of one. This phenomenon will be studied in more detail in Chapter 4, since these fixed points are the p-adic analogous of complex multiplication parameters of Definition 1.3.15.

2.3.2 p-adic Schottky groups

2.3.6 Definition. Let Γ be a subgroup of $\mathrm{PGL}_2(\mathbb{Q}_p)$.

A point $z \in \mathbb{P}^1(\mathbb{C}_p)$ is called a **limit point with respect to** Γ if there exist a point $y \in \mathbb{P}^1(\mathbb{C}_p)$ and a sequence $\{\gamma_n\}_{n\in\mathbb{N}}$ of elements of Γ, with $\gamma_n \neq \gamma_m \; \forall\, n \neq m$, such that $\lim(\gamma_n \cdot y) = z$.

We denote by $\mathcal{L}_\Gamma \subseteq \mathbb{P}^1(\mathbb{C}_p)$ the set of limit points with respect to Γ and the subgroup Γ is said to be **discontinuous** if $\mathcal{L}_\Gamma \neq \mathbb{P}^1(\mathbb{C}_p)$.

2.3.7 Proposition. *If* $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ *is a discontinuous subgroup, then* Γ *is discrete.*

Proof. If Γ was not a discrete subgroup of $\mathrm{PGL}_2(\mathbb{Q}_p)$ then a sequence $\{\gamma_n\}_{n\geq 0}$ of elements $\gamma_n \in \Gamma$ would exist, such that $\lim_n \gamma_n = \gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$. Therefore, every $z \in \mathbb{P}^1(\mathbb{C}_p)$ could be written as a limit $z = \lim_n(\gamma_n\gamma^{-1} \cdot z) = z$, which is an absurd. □

2.3.8 Definition. A subgroup $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ is called a **p-adic Schottky group** if it satisfies the following conditions:

(i) Γ is discontinuous.

(ii) Γ is finitely generated.

(iii) Γ has no elements of finite order different from the identity I_2.

2.3.9 Lemma. *Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a discontinuous subgroup generated by one element $\gamma \neq \mathrm{I}_2$. If γ is not hyperbolic, then it must be an element of finite order. In particular, γ cannot be parabolic.*

Proof. If the generator γ is an elliptic transformation, then it is represented by a matrix conjugated to $\left(\begin{smallmatrix}\mu & 0\\ 0 & 1\end{smallmatrix}\right)$, with $|\mu| = 1$. Since the closure of every orbit $\overline{\Gamma z} = \overline{\{\mu^n z \mid n \in \mathbb{N}\}}$, is compact, and since the group Γ is discrete by Proposition 2.3.7, then $\overline{\Gamma z}$ is finite for every $z \in \mathbb{P}^1(\mathbb{C}_p)$. In particular μ has to be a root of unity in $\mathbb{C}_p$.

Analogously, if γ is a parabolic transformation, then it is represented by a matrix conjugated to $\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right)$ and so in this case we have that $nb = 0$ for some $n \in \mathbb{Z}$; thus $b = 0$ and the transformation γ is the identity I_2. □

After Lemma 2.3.9, we can rewrite Definition 2.3.8, replacing condition (*iii*) as follows.

2.3.10 Definition. A subgroup $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ is called a **p-adic Schottky group** if it satisfies the following conditions:

(i) Γ is discontinuous.

(ii) Γ is finitely generated.

(iii) Every element $\gamma \in \Gamma, \gamma \neq \mathrm{I}_2$, is hyperbolic.

The following statement was first proved by Ihara in [Iha66a, 2-1].

2.3.11 Theorem. (Ihara) *Every Schottky group is free*

Proof. By [Ser77, 3.3, Théorème 4] a group is free if there exists a tree on which this group acts freely, so to prove (*ii*) we only need to prove that any Schottky group Γ acts freely on the Bruhat-Tits tree $\mathcal{T}_p$, as described in Section 2.2. In the same section we have also seen that $\mathrm{PGL}_2(\mathbb{Q}_p)$ acts transitively on the tree $\mathcal{T}_p$. If Γ does not act freely on $\mathcal{T}_p$, then there exists an element $\gamma \in \Gamma, \gamma \neq \mathrm{I}_2$, fixing a vertex or an (oriented) edge of $\mathcal{T}_p$. In the case γ fixes an edge, γ^2 fixes the extreme vertices of this edge, so in both cases γ cannot be hyperbolic, which is a contradiction. □

2.3.12 Remark. The reason why the transformation γ, fixing the edge or a vertex in $\mathcal{T}_p$ in the proof above, cannot be hyperbolic is that γ would then have fixed points in $\mathbb{P}^1(\mathbb{Q}_p)$ which is identified with the "boundary" of the tree $\mathcal{T}_p$ (cf. next Proposition 2.3.18).

We are interested in a particular family of p-adic Schottky groups, namely *cocompact* Schottky groups, because these are the ones that arise in the p-adic uniformization of Shimura curves.

2.3.13 Definition. A discrete subgroup $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ is said to be **cocompact** if the quotient space $\mathrm{PGL}_2(\mathbb{Q}_p)/\Gamma$ is compact.

2.3.14 Proposition. *If $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ is a discrete cocompact subgroup, then the quotient graph $\Gamma\backslash\mathcal{T}_p$ is compact, i.e. its set of vertices $\mathrm{Ver}(\Gamma\backslash\mathcal{T}_p)$ is finite.*

Proof. It is an immediate consequence of the homeomorphism

$$\mathcal{T}_p \simeq \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$$

(cf. Proposition 2.2.23), and the continuity of the map

$$\Gamma\backslash\mathrm{PGL}_2(\mathbb{Q}_p) \longrightarrow \Gamma\backslash\mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p).$$

□

2.3.3 Mumford curves

The importance of p-adic Schottky groups defined above resides in the fact that they allow the p-adic uniformization of stable curves of genus $g \geq 1$, defined over $\mathbb{Z}_p$, having $\mathbb{F}_p$-split degenerate reduction.

This is the well-known theory of non-Archimedean uniformization of curves started by Tate with its celebrated result on elliptic curves with split multiplicative reduction and extended by Mumford to curves of genus $g \geq 2$ (cf. [Mum72] and [Mil15]).

We resume here the main result of this theory in the way we will use it in this memory. First, we recall briefly the definition of stable curve according to [Mum72, Definition 3.2].

2.3.15 Definition. Let C be a smooth projective curve over $\mathbb{Q}_p$. A model $\mathcal{C}$ over $\mathbb{Z}_p$ for the curve C is said to be **semistable** if

(i) The scheme $\mathcal{C}$ is proper and flat over $\mathbb{Z}_p$.

(ii) The special fibre $\mathcal{C}_0$ is geometrically reduced and connected.

(iii) All the singular points of $\mathcal{C}_0 \otimes \overline{\mathbb{F}}_{\mid}$ are ordinary double points.

(iv) All irreducible components of $\mathcal{C}_0 \otimes \overline{\mathbb{F}}_p$, if any, meet the remaining components in at least 2 points.

If moreover all non-singular rational irreducible components of $\mathcal{C}_0 \otimes \overline{\mathbb{F}}_p$, if any, meet the remaining components in at least 3 points, we say that the model $\mathcal{C}$ is **stable**.

In general, a proper and flat scheme $\mathcal{C}$ over $\mathbb{Z}_p$, with 1-dimensional fibres, is said to be stable if it is the stable model of its generic fibre $\mathcal{C}_\eta$, according to the definition above.

Let $\mathcal{C}$ be a stable scheme over $\mathbb{Z}_p$. Its special fibre $\mathcal{C}_0$ is said to be **$\mathbb{F}_p$-split degenerate** if the normalizations of all its irreducible components are isomorphic to $\mathbb{P}^1_{\mathbb{F}_p}$ and all the double points are $\mathbb{F}_p$-rational. In particular the local ring in a singular point P of the special fibre is

$$\mathcal{O}_{\mathcal{C}_0,P} \simeq \mathbb{F}_p[x,y]/(xy).$$

2.3.16 Definition. When a curve C over $\mathbb{Q}_p$ admits a stable model $\mathcal{C}$ with special fibre a $\mathbb{F}_p$-split degenerate curve, then the **stable reduction graph of C (with respect to $\mathcal{C}$)** is the graph $\mathcal{G}(C,\mathcal{C})$ defined by the following properties:

(a) The set of vertices of $\mathcal{G}(C,\mathcal{C})$ is the set of irreducible components of $\mathcal{C}_0$.

(b) Two vertices are connected by an edge if and only if the corresponding irreducible components of $\mathcal{C}_0$ meet each other.

2.3.17 Notation. Given a Schottky group $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$, we will denote by $\mathcal{T}_\Gamma$ the tree associated to Γ, as constructed in [Mum72, Sec. 1].

We will denote by $\mathcal{H}_\Gamma$ the rigid analytic space over $\mathbb{Q}_p$, which generic fibre of the admissible formal scheme $\widehat{\mathcal{H}}_\Gamma$ associated to the tree $\mathcal{T}_\Gamma$, as constructed in [Mum72, Sec. 2].

The following result is [Mum72, Proposition 1.18].

2.3.18 Proposition. *Let $\partial\mathcal{T}_\Gamma$ be the set of ends of the tree $\mathcal{T}_\Gamma$. Then there is an injective map*

$$\iota : \partial\mathcal{T}_\Gamma \hookrightarrow \mathbb{P}^1(\mathbb{Q}_p).$$

Moreover when $\mathcal{T}_\Gamma = \mathcal{T}_p$, this map is surjective, i.e. there is a bijection of sets

$$\iota : \partial\mathcal{T}_p \simeq \mathbb{P}^1(\mathbb{Q}_p).$$

2.3.19 Proposition. *Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a Schottky group.*

(1) *For every extension* $\mathbb{Q}_p \subseteq L \subseteq \mathbb{C}_p$*, the rigid analytic space* $\mathcal{H}_\Gamma$ *is a subdomain of* $\mathcal{H}_p$ *such that*

$$\mathcal{H}_\Gamma(L) = \mathbb{P}^1(L) \smallsetminus \mathcal{L}_\Gamma,$$

where $\mathcal{L}_\Gamma$ *is the set of limit points with respect to* Γ *(cf. Definition 2.3.6).*

In particular, when $\Gamma = \mathrm{PGL}_2(\mathbb{Q}_p)$*, this rigid analytic space is* $\mathcal{H}_\Gamma = \mathcal{H}_p$*.*

(2) *The tree* $\mathcal{T}_\Gamma$ *is a subtree of* $\mathcal{T}_p$ *such that the map*

$$\iota : \partial\mathcal{T}_\Gamma \hookrightarrow \mathbb{P}^1(\mathbb{Q}_p)$$

has image $\iota(\partial\mathcal{T}_\Gamma) = \mathcal{L}_\Gamma$*.*

In particular, when $\Gamma = \mathrm{PGL}_2(\mathbb{Q}_p)$*, then* $\mathcal{T}_\Gamma = \mathcal{T}_p$*.*

(3) *The reduction map of Theorem 2.2.31*

$$\mathrm{Red} : \mathcal{H}_p \longrightarrow \mathcal{T}_p$$

restricts to a reduction map

$$\mathrm{Red}_\Gamma : \mathcal{H}_\Gamma \longrightarrow \mathcal{T}_\Gamma$$

for the rigid analytic space $\mathcal{H}_\Gamma$*.*

Therefore the tree $\mathcal{T}_\Gamma$ *is the reduction graph of the rigid analytic space* $\mathcal{H}_\Gamma$*.*

2.3.20 Theorem. (cf. Theorem 3.3. and Corollary 4.11, [Mum72]) *Let* $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ *be a Schottky group of rank* g *as a free group. Then there exists a proper and flat scheme* $\mathcal{C}_\Gamma$ *over* $\mathbb{Z}_p$ *such that:*

(*i*) $\mathcal{C}_\Gamma$ *is stable and its generic fibre* C_Γ *is a genus* g *curve.*

(*ii*) *The rigid analytic space* $\Gamma\backslash\mathcal{H}_\Gamma$ *over* $\mathbb{Q}_p$ *is isomorphic to the rigidification of the curve* C_Γ*, i.e.*

$$\Gamma\backslash\mathcal{H}_\Gamma \simeq C_\Gamma^{rig}.$$

(*iii*) *The reduction mod* p *of the rigid analytic space* C_Γ^{rig} *is an* $\mathbb{F}_p$*-split degenerate curve.*

(*iv*) *The stable reduction graph of the curve* C_Γ*, with respect to the model* $\mathcal{C}_\Gamma$*, is the finite graph* $\Gamma\backslash\mathcal{T}_\Gamma$*.*

Moreover the curve $\mathcal{C}_\Gamma$ is uniquely determined, up to isomorphism, by the conjugacy class of the Schottky group Γ inside $\mathrm{PGL}_2(\mathbb{Q}_p)$.

The (non-Archimedean) curve C_Γ is called **Mumford curve associated to the Schottky group** Γ.

Note that condition (ii) of the Theorem is equivalent to say that the completion of the scheme $\mathcal{C}_\Gamma$, along its special fibre $\mathcal{C}_{\Gamma,0}$, is an admissible formal scheme isomorphic to $\Gamma\backslash\widehat{\mathcal{H}}_\Gamma$, where $\widehat{\mathcal{H}}_\Gamma$ is the formal scheme of [Mum72, Proposition 2.8].

2.3.21 Theorem. *Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a cocompact Schottky group. Then the set of limit points with respect to Γ is*

$$\mathcal{L}_\Gamma = \mathbb{P}^1(\mathbb{Q}_p).$$

Proof. By Proposition 2.3.18 we know that $\iota(\partial\mathcal{T}_p) = \mathbb{P}^1(\mathbb{Q}_p)$. Therefore for every point $z \in \mathbb{P}^1(\mathbb{Q}_p)$ there is a half-line $\{v_n\}_{n\geq 0}$, formed of vertices $v_n \in \mathrm{Ver}(\mathcal{T}_p)$, such that the associated end $e := [\{v_n\}_{n\geq 0}] \in \partial\mathcal{T}_p$ corresponds to the point z, i.e. $\iota(e) = z$.

Let $\mathcal{F}_p$ be a fundamental domain for the graph $\Gamma\backslash\mathcal{T}_p$ such that $v_0 \in \mathcal{F}_p$. Since the group Γ is cocompact, by Proposition 2.3.14 we know that the graph $\mathcal{F}_p$ has a finite number of vertices and so the integer

$$j_1 := \max\{n \geq 0 \mid v_n \in \mathcal{F}_p\}$$

exists.

Therefore there exists $\gamma_1 \in \Gamma, \gamma \neq \mathrm{I}_2$, such that $\gamma_1 \cdot \mathcal{F}_p \ni v_{j_1+1}$. Let $w_1 \in \gamma_1 \cdot \mathcal{F}_p$ be such that $\Gamma w_1 = \Gamma v_0$, so $w_1 = \gamma_1' v_0$ for some $\gamma_1' \in \Gamma$. Iterating this process we find a sequence

$$w_0 := v_0,\ w_1 := \gamma_1' \cdot v_0, \ldots,\ w_n := \gamma_n' \cdot v_0', \ldots$$

having the same limit, for $n \to \infty$, of the sequence $\{v_n\}_{n\geq 0}$, namely the point $z \in \mathbb{P}^1(\mathbb{Q}_p)$. □

2.3.22 Corollary. *If $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ is a cocompact Schottky group then*

$$\mathcal{T}_\Gamma = \mathcal{T}_p \ \textit{and}\ \mathcal{H}_\Gamma = \mathcal{H}_p.$$

Proof. It is immediate after Theorem 2.3.21 and Proposition 2.3.19. If Γ is cocompact then for every extension $\mathbb{Q}_p \subseteq L \subseteq \mathbb{C}_p$,

$$\mathcal{H}_\Gamma(L) = \mathbb{P}^1(L) \smallsetminus \mathcal{L}_\Gamma = \mathbb{P}^1(L) \smallsetminus \mathbb{P}^1(\mathbb{Q}_p) = \mathcal{H}_p.$$

and applying the reduction map

$$\mathcal{T}_{\Gamma,\mathbb{Q}} = \mathrm{Red}_\Gamma(\mathcal{H}_\Gamma) = \mathrm{Red}(\mathcal{H}_p) = \mathcal{T}_{p,\mathbb{Q}}.$$

□

The following theorem is the p-adic analog of a well-known result about discrete subgroups of $\mathrm{PSL}_2(\mathbb{R})$, and more in general about discrete subgroups of $\mathrm{PGL}_2(\mathbb{C})$, which was first proved by Selberg (cf. [Sel60, Lemma 8]). This is one of the main ingredients in the proof of the Cerednik Theorem as well as in the computation of the examples of explicit p-adic uniformizations of Shimura curves.

2.3.23 Theorem. *Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a discontinuous and finitely generated group. Then there exists a subgroup Γ_0 of finite index, which is torsion-free. In particular Γ_0 is a p-adic Schottky group.*

Proof. Let S be a subset of elements of finite order of Γ such that every element of finite order of Γ is conjugated to an element of S. It is easy to prove that the set S can be taken to be finite (cf. for example [GvDP80, Lemma 3.3.2]).

Since Γ is finitely generated, we can find a ring $R \subseteq \mathbb{Q}_p$ which is finitely generated over $\mathbb{Z}_p$ and such that $\Gamma \subseteq \mathrm{PGL}_2(R) \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$.

Since S is finite, there exists a maximal ideal $\mathfrak{m} \subseteq R$ such that for every $\sigma \in S$, $\sigma \neq \mathrm{I}_2$, we have $\sigma - \mathrm{I}_2 \notin \mathfrak{m}$. Therefore, the group

$$\Gamma_0 := \Gamma(\mathfrak{m}) := \{\gamma \in \Gamma \mid \gamma - \mathrm{I}_2 \in \mathfrak{m}\}$$

is a normal subgroup of Γ of finite index (since $R/\mathfrak{m}$ is a finite field) and it follows directly from the fact that $\Gamma(\mathfrak{m})$ is normal that $\Gamma(\mathfrak{m})$ does not contain any of the elements of finite order of Γ. □

Chapter 3

p-adic fundamental domains of Shimura curves and their reductions

3.1 p-adic uniformization of Shimura curves

Let H be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant $D_H > 1$ and let $\mathcal{O}_H$ be an Eichler order over $\mathbb{Z}$ of level N. In Section 1.2 we introduced the canonical model $X(D_H, N)$ of the Shimura curve associated to (the conjugacy class of) the Eichler order $\mathcal{O}_H$.

After Theorem 1.2.3, we know that this is a smooth and proper algebraic curve defined over $\mathbb{Q}$, whose set of complex points are uniformized (hyperbolically) by the group of quaternions

$$\Gamma(D_H, N) := \{\alpha \in \mathcal{O}_H^* \mid \mathrm{Nm}(\alpha) > 0\} = \{\alpha \in \mathcal{O}_H \mid \mathrm{Nm}(\alpha) = 1\},$$

viewed as subgroup of transformations in $\mathrm{PGL}_2(\mathbb{Q}_\infty)_{>0} = \mathrm{Aut}(\mathcal{H})$, once an immersion $\Phi_\infty : H \hookrightarrow \mathrm{M}_2(\mathbb{Q}_\infty)$ is fixed, i.e.

$$\Gamma(D_H, N)\backslash\mathcal{H} \simeq X(D_H, N)(\mathbb{C}).$$

Depending on which side of this analytic isomorphism we prefer to look at, we can naturally consider two questions arising from replacing the prime ∞ by a finite prime p (eventually dividing the discriminant D_H of the algebra H):

(1) To study discrete subgroups of transformations $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p) = \mathrm{Aut}(\mathcal{H}_p)$ and to look for a family of algebraic curves $\{C_\Gamma\}_\Gamma$ providing algebraic

models for the rigid analytic varieties $\Gamma\backslash\mathcal{H}_p$, i.e. such that

$$\Gamma\backslash\mathcal{H}_p \simeq C_\Gamma^{rig}.$$

(2) To study the set of p-adic points of the curve $X(D_H, N)$ and to find a non-Archimedean uniformization for this set of points, i.e. to find a subgroup of transformations $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ such that

$$\Gamma\backslash\mathcal{H}_p \simeq X(D_H, N)(\mathbb{C}_p).$$

As we shall see in this chapter, each of these questions provides an answer to the other, at least in the case when $p|D_H$.

The first question was first considered by Ihara. In a series of works (cf. [Iha66a], [Iha66b], [Iha67]) he studied some algebraic curves associated to discrete subgroups $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{R}) \times \mathrm{PGL}_2(\mathbb{Q}_p)$ such that the projections on each factor are dense subgroups. He proved a series of conjectures (cf. [Iha68, Conjectures 1, 2 and 3]) regarding these curves and which he brought together under the name of **the congruence monodromy problems**.

Later, Cerednik went further into this line of research and discovered that actually such curves arising from quotients as in (1), and as in the works of Ihara, were the non-Archimedean counterpart of the complex uniformization of Shimura curves: he found out (somewhat magically) the **Theorem on interchanging local invariants** (cf. [Cer76b, Theorem 2.1]), better known today as the *Cerednik-Drinfeld Theorem*.

Maybe the history of this fascinating result should not be explained in such a simplified way: it is clear, though, that Ihara knew the works of Shimura on arithmetic quotients of the Poincaré upper half-plane and their canonical models, and so he surely expected to have a result relating the two uniformizations, which he actually considered simultaneously. On the other hand, Cerednik was able to prove and make the connexion between the curves considered by Ihara and those by Shimura thanks to the recent work of Mumford [Mum72] on the non-Archimedean uniformization of curves. Actually, as we are going to throughout this chapter, the fundamental step from Mumford's paper to Cerednik's one, i.e. from the uniformization of Mumford curves to the uniformization of Shimura curves, lies in considering certain *supergroups* of Schottky groups containing elements of finite order (while Schottky groups are torsion-free).

3.1.1 Cerednik theorem

We will now state the theorem of Cerednik on interchanging local invariants in its original version. Nevertheless, we restrict ourselves to the case when

the base field is $F = \mathbb{Q}$.

Let $p \in \mathbb{Z}$ be a fixed prime and let R be a set of primes of $\mathbb{Q}$ such that $\{\infty, p\} \subseteq R$ and the cardinality of R is odd.

Let H and B be quaternion algebras over $\mathbb{Q}$ such that their sets of ramification satisfy the following relations:

$$\mathrm{Ram}(H) = R \smallsetminus \{\infty\}, \quad \mathrm{Ram}(B) = R \smallsetminus \{p\}.$$

In particular we have that

(1) H is *indefinite*, $p|D_H$, and there is an immersion

$$\Phi_\infty : H \hookrightarrow \mathrm{M}_2(\mathbb{Q}_\infty).$$

(2) B is *definite*, $p \nmid D_B$, and there is an immersion

$$\Phi_p : B \hookrightarrow \mathrm{M}_2(\mathbb{Q}_p).$$

Let $\mathcal{O}_H, \mathcal{O}_B$ be Eichler orders over $\mathbb{Z}$ in H and in B respectively, of the same level N.

(1) Let us denote by $\mathcal{O}_H[1/\infty] := \mathcal{O}_H \otimes_{\mathbb{Z}} \mathbb{Z}[1/\infty]$ the corresponding Eichler order over $\mathbb{Z}[1/\infty] := \mathbb{Z}$ of level N and let us define the following group:

$$\Gamma_{\infty,+}(D_H, N) := \Phi_\infty(\{\alpha \in \mathcal{O}_H[1/\infty]^* \mid \mathrm{Nm}(\alpha) > 0\})/\mathbb{Z}[1/\infty]^*.$$

This is a discrete and cocompact subgroup of $\mathrm{PGL}_2(\mathbb{Q}_\infty)_{>0} = \mathrm{Aut}(\mathcal{H})$ and there exists an algebraic curve $X(D_H, N)$ over $\mathbb{C}$ such that

$$\Gamma_{\infty,+}(D_H, N)\backslash\mathcal{H} \simeq X_\infty(D_H, N)^{an}.$$

(2) Let us denote by $\mathcal{O}_B[1/p] := \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ the corresponding Eichler order over $\mathbb{Z}[1/p]$ and let us define the following group

$$\Gamma_p(D_B, N) := \Phi_p(\mathcal{O}_B[1/p]^*)/\mathbb{Z}[1/p]^*.$$

This is a discrete and cocompact subgroup of $\mathrm{PGL}_2(\mathbb{Q}_p) = \mathrm{Aut}(\mathcal{H}_p)$ and there exists an algebraic curve $X_p(D_B, N)$ over $\mathbb{Q}_p$ such that

$$\Gamma_p(D_B, N)\backslash\mathcal{H}_p \simeq X_p(D_B, N)^{rig}.$$

3.1.1 Remark. Observe that

(1) The set of matrices

$$\Phi_p(\{\alpha \in \mathcal{O}_H[1/\infty]^* \mid \mathrm{Nm}(\alpha) = 1\})$$

is a system of representatives for the transformations in $\Gamma_{\infty,+}(D_H, N)$.

(2) The set of matrices

$$\Phi_p(\{\alpha \in \mathcal{O}_B[1/p]^* \mid \mathrm{Nm}(\alpha) \in \{1, p\}\})$$

is a system of representatives for the transformations in $\Gamma_p(D_B, N)$. Moreover this group has an index 2 subgroup which is the one represented by matrices in

$$\Phi_p(\{\alpha \in \mathcal{O}_B[1/p]^* \mid \mathrm{Nm}(\alpha) = 1\})$$

and it will be denoted in the following by $\Gamma_{p,+}(D_B, N)$ (cf. next Theorem 3.1.14 and Corollary 3.1.16).

Note that the fact that the quotient rigid analytic variety $\Gamma_p(D_B, N)\backslash\mathcal{H}_p$ is algebraizable is a consequence of the theory of Mumford uniformization, as we recall in what follows. This is proved in Cerednik's original paper as an application of Mumford's results (cf. Section 2.3.3).

As a matter of fact, the group $\Gamma_p(D_B, N)$ is a discrete and cocompact subgroup of $\mathrm{PGL}_2(\mathbb{Q}_p)$ but it is not torsion-free since it can contain elliptic transformations. Nevertheless, by Theorem 2.3.23 we know that there exists an integer $M \geq 1$ such that the subgroup

$$\Gamma_p(D_B, N)(M) := \{\gamma \in \Gamma_p(D_B, N) \mid \gamma - \mathrm{I}_2 \in M\Phi_p(\mathcal{O}_B[1/p])\}$$

is a Schottky group. Hence by Theorem 2.3.20 and Theorem 2.3.21 the quotient $\Gamma_p(D_B, N)(M)\backslash\mathcal{H}_p$ is algebraizable, i.e. there exists an algebraic curve $X_p(D_B, N; M)$ over $\mathbb{Q}_p$ such that

$$\Gamma_p(D_B, N)(M)\backslash\mathcal{H}_p \simeq X_p(D_B, N; M)^{rig},$$

and then the curve $X_p(D_B, N)$ is a finite quotient of the Mumford curve $X_p(D_B, N; M)$ by the group $\Gamma_p(D_B, N)/\Gamma_p(D_B, N)(M)$.

The following result, which is [Cer76b, Theorem 1.12], shows that the algebraic curves $X_p(D_B, N)_{/\mathbb{Q}_p}$ and $X_\infty(D_H, N)_{/\mathbb{C}}$ both have models defined over some algebraic extensions of $\mathbb{Q}$.

3.1.2 Theorem. *There exist K_B, K_H finite algebraic extensions of $\mathbb{Q}$ such that the curve $X_p(D_B, N)$ is defined over K_B and the curve $X_\infty(D_H, N)$ is defined over K_H.*

As is also observed in [Cer76b], throughout the proof of this theorem, the statement for the curve $X_\infty(D_H, N)$ is a consequence of the stronger result of Shimura about the existence of canonical models (cf. Theorem 1.2.3). In any case, in [Cer76a] and [Cer76b] this is proved by making use of the "technique of elliptic transformations" developed by Ihara.

We are now in a position to state the main result of the paper [Cer76b, Theorem 2.1], relating these two algebraic models arising from the two uniformizations.

3.1.3 Theorem. (Cerednik theorem) (*i*) *There is an isomorphism of* $\mathbb{Q}$*-extensions*

$$\tau : K_B \simeq K_H,$$

and all finite primes $\ell | pD_B$ *are not ramified in these fields.*

(*ii*) *For every* $\sigma : K_B \hookrightarrow \mathbb{C}$*, compatible with the inclusions* $\mathbb{Q} \subseteq \mathbb{Q}_\infty \subseteq \mathbb{C}$*, there is an isomorphism of complex analytic curves*

$$X_p(D_B, N) \otimes_{K_B} \mathbb{C} \simeq X_\infty(D_H, N) \otimes_{K_H} \mathbb{C},$$

where the second isomorphism is taken with respect to the induced embedding $\sigma \circ \tau^{-1} : K_H \hookrightarrow \mathbb{C}$*.*

(*iii*) *There is an isomorphism of algebraic curves*

$$\sigma' : X(D_B, N) \simeq X(D_H, N)$$

such that σ'*, restricted to* K_B*, is compatible with the inclusions* $\mathbb{Q} \subseteq \mathbb{Q}_\infty \subseteq \mathbb{C}$*.*

3.1.4 Remark. (1) As a consequence of point (*ii*) of Theorem 3.1.3 we obtain the following isomorphism of Riemann surfaces

$$\Gamma_{\infty,+}(D_H, N) \backslash \mathcal{H} \simeq (X_p(D_B, N) \otimes_{K_B} \mathbb{C})^{an}.$$

(2) From point (*iii*) we deduce that, once an embedding $K_H \hookrightarrow \overline{\mathbb{Q}}$ has been fixed, there is an isomorphism of rigid analytic varieties over $K_{H,p} := K_H \otimes_{\mathbb{Q}} \mathbb{Q}_p$,

$$(\Gamma_p(D_B, N) \backslash \mathcal{H}_p) \otimes_{\mathbb{Q}_p} K_{H,p} \simeq (X(D_H, N) \otimes_{K_H} \mathbb{Q}_p)^{rig}.$$

(3) Finally from point (*i*) we know that the p-adic field $K_{H,p} = K_H \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is contained in the maximal unramified extension $\mathbb{Q}_p^{nr} | \mathbb{Q}_p$.

Again, the assertion about the behavior of the primes $\ell | pD_B$ inside the extension K_H is a consequence of Shimura's Theorem 1.2.3.

3.1.2 Drinfeld theorem

In [Dri76] Drinfeld gives a different proof of Cerednik's theorem. While Cerednik made use of the technique of "elliptic elements" introduced by Ihara in order to prove the algebraicity of the p-adic model of the Shimura curve $X(D_H, N)$, Drinfeld extends the modular interpretation of the complex points of the Shimura curve to this local model. In particular he gives a modular interpretation of the p-adic upper half-plane in terms of certain formal modules. This induces a modular interpretation on the p-adic curve $X_p(D_B, N)$ which is a candidate to be the local Shimura curve. Finally he proves the coincidence of the two modular interpretations.

In this section we are going to state Cerednik's theorem in the more precise version provided and proved by Drinfeld.

First of all, we need to translate the scenario of the previous section into the adelic language, paying particular attention to the similarities arising with Section 1.2.4, where Shimura curves are introduced adelically.

Given a finite set S of primes of $\mathbb{Q}$ we will denote by $\mathbb{A}^{(S)}$ the $\mathbb{Q}$-algebra of *adèles* outside S, i.e.

$$\mathbb{A}^{(S)} := \prod_{p \notin S} (\mathbb{Q}_p : \mathbb{Z}_p),$$

and by $\mathbb{A}_S$ the S-part of $\mathbb{A}$, i.e.

$$\mathbb{A}_S := \prod_{p \in S} \mathbb{Q}_p,$$

so that $\mathbb{A} = \mathbb{A}^{(S)}\mathbb{A}_S$.

When $S = \{\infty\}$ we also write $\mathbb{A}_{fin}$, as usual, for the *adèles* outside $\{\infty\}$.

The relation between the ramification sets of the algebras H and B translates into the following isomorphisms:

$$H^*(\mathbb{Q}_\infty) \simeq \mathrm{GL}_2(\mathbb{R}), \quad H^*(\mathbb{A}^{(\infty,p)}) \simeq B^*(\mathbb{A}^{(\infty,p)}), \quad B^*(\mathbb{Q}_p) \simeq \mathrm{GL}_2(\mathbb{Q}_p).$$

Let $U_0(N)$ be the subgroup of $H^*(\mathbb{A}^{(\infty)}) = H^*(\mathbb{A}_{fin})$ such that

$$U_0(N) \cap H^*(\mathbb{Q}) = \Gamma(D_H, N),$$

as defined in Example 1.2.4.1, and let us decompose it as a product

$$U_0(N) = U_0(N)^{(p)} \times U_0(N)_p \subseteq H^*(\mathbb{A}^{(\infty,p)}) \times H^*(\mathbb{Q}_p).$$

3.1.5 Notation. Let us denote by $V_0(N)^{(p)}$ the image of the group $U_0(N)^{(p)}$ inside $B^*(\mathbb{A}^{(\infty,p)})$, through the isomorphism $H^*(\mathbb{A}^{(\infty,p)}) \simeq B^*(\mathbb{A}^{(\infty,p)})$.

Therefore $V_0(N)^{(p)} \times B^*(\mathbb{Q}_p)$ is an open compact subgroup of $B^*(\mathbb{A}_{fin})$.

Mirroring Lemma 1.2.23, we can prove the following result:

3.1.6 Proposition. *The double quotient space*

$$(V_0(N)^{(p)} \times B^*(\mathbb{Q}_p))\backslash B^*(\mathbb{A}_{fin})/B^*(\mathbb{Q})$$

is finite, and its cardinality is the strict ideal class number of $\mathbb{Z}[1/p]$*, which is equal to* 1*.*

This result is a consequence of the theorem we are going to state and which is a generalization of Theorem 1.2.15.

3.1.7 Theorem. (General noncommutative commutative dictionary) *Let* F *be a totally real field,* R_F *its ring of integers and let* S *be a set of primes of* F*,* $S \supseteq S_\infty$*. Let* Q *be a quaternion* F*-algebra,* $\mathcal{O}$ *an Eichler order over* R_F*, and let* $\mathfrak{u}_1$ *be the product of Archimedean primes at which the algebra* Q *is ramified, i.e.*

$$\mathfrak{u}_1 := \prod_{\mathfrak{q} \in \mathrm{Ram}_\infty(Q)} \mathfrak{q},$$

If the order $\mathcal{O}[1/S] := \mathcal{O} \otimes_{R_F} R_F[1/S]$ *over* $R_F[1/S]$ *satisfies Eichler's condition, i.e.* $S \not\subseteq \mathrm{Ram}(Q)$*, then the norm map induces the following bijection of sets:*

$$(\prod_{\mathfrak{p} \notin S} \mathcal{O}_\mathfrak{p}^* \prod_{\mathfrak{q} \in S} Q_\mathfrak{q}^*)\backslash Q_\mathbb{A}^*/Q^* \simeq$$
$$\simeq (\prod_{\mathfrak{p} \notin S} R_{F,\mathfrak{p}}^* \prod_{\mathfrak{q} \in S} F_\mathfrak{q}^*)\backslash F_\mathbb{A}^*/\{x \in F^* \mid x \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_1)\}.$$

In particular, the left ideal class number $h(Q, \mathcal{O}[1/S])$ *of the order* $\mathcal{O}[1/S]$ *equals the strict ideal class number* $h_1(R_F[1/S])$ *of the order* $R_F[1/S]$ *defined as*

$$h_1(R_F[1/S]) := [I(F) : P(F, \mathfrak{u}_1)],$$

where $I(F)$ *is the group of fractional ideals of* F *which are stable for* $R_F[1/S]$ *and* $P(F, \mathfrak{u}_1)$ *the subgroup of principal ideals generated by elements in* $\{x \in F^* \mid x \equiv 1 \,(\mathrm{mod}^*\, \mathfrak{u}_1)\}$*.*

PROOF. Observe first that for every $\mathfrak{p} \notin S$

$$\mathcal{O}[1/S]^*_{\mathfrak{p}} = \mathcal{O}^*_{\mathfrak{p}}, \quad R_F[1/S]^*_{\mathfrak{p}} = R^*_{F,\mathfrak{p}}.$$

Therefore the proof of Theorem 1.2.15 can be adapted to this case, since Eichler's *Normensatz* (Theorem 1.1.8) and Strong approximation theorem (Theorem 1.1.9) can be applied to the algebra Q and the order $\mathcal{O}[1/S]$. □

PROOF.(of Theorem 3.1.6)

Since the set $S = \{\infty, p\}$ satisfies Eichler's condition in Definition 1.1.6, we can apply Theorem 3.1.7 to the algebra B and to the order $\mathcal{O}_B[1/p]$ over $\mathbb{Z}[1/p]$. We find that in this case $\mathfrak{u}_1 = \mathbb{Q}_{>0}$ and

$$V_0(N)^{(p)} \times B^*(\mathbb{Q}_p) \times B^*(\mathbb{Q}_\infty) = \prod_{\ell \notin S} \mathcal{O}^*_{B,\ell} \prod_{q \in S} B^*_q.$$

□

Finally we can prove the following statement, which is the p-adic analog of Theorem 1.2.25.

3.1.8 Theorem. *There is an isomorphism of rigid analytic varieties over* $\mathbb{Q}_p$:

$$(V_0(N)^{(p)} \times B^*(\mathbb{Q}_p))\backslash \mathcal{H}_p \times B^*(\mathbb{A}_{fin})/B^*(\mathbb{Q}) \simeq \Gamma\backslash \mathcal{H}_p,$$

where $\Gamma := V_0(N)^{(p)} \cap B^*(\mathbb{Q})$.

PROOF. The proof is the same as in Theorem 1.2.25. Note that, in the case we are considering, the double coset has class number 1 so only one component arises in the decomposition. □

3.1.9 Remark. The group $\Gamma := V_0(N)^{(p)} \cap B^*(\mathbb{Q})$ can be viewed as subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$ through the isomorphism $B^*(\mathbb{Q}_p) \simeq \mathrm{GL}_2(\mathbb{Q}_p)$.

In fact it is immediate, following the definition, that if $U_0(N) \cap H^*(\mathbb{Q}) = \mathcal{O}^*_H$ then $\Gamma = \mathcal{O}_B[1/p]^*$.

In order to state a more precise version of Theorem 3.1.3 due to Drinfeld, we have to introduce a certain *unramified p-adic upper half-plane*. We will do this now.

When $\mathcal{O}_L$ is the ring of integers of a finite extension $L|\mathbb{Q}_p$ of degree r, the formal scheme

$$\widehat{\mathcal{H}}_p \hat{\otimes}_{\mathbb{Z}_p} \mathrm{Spf}\, \mathcal{O}_L$$

over $\operatorname{Spf}\mathcal{O}_L$ can also be thought of as a formal scheme over $\operatorname{Spf}\mathbb{Z}_p$, by composing with the morphism of formal schemes $\operatorname{Spf}\mathcal{O}_L \to \operatorname{Spf}\mathbb{Z}_p$. We will denote it by $\widehat{\mathcal{H}}_p^{\mathcal{O}_L}$.

In order to understand better what kind of formal scheme $\widehat{\mathcal{H}}_p^{\mathcal{O}_L}$ is, let us extend scalars to $\mathcal{O}_L$. We find the following isomorphism of formal schemes over $\mathbb{Z}_p$

$$\widehat{\mathcal{H}}_p^{\mathcal{O}_L} \otimes_{\mathbb{Z}_p} \operatorname{Spf}\mathcal{O}_L \simeq \left(\coprod_{i=1}^{r} \widehat{\mathcal{H}}_p \otimes_{\mathbb{Z}_p} \operatorname{Spf}\mathcal{O}_L\right) / \sim$$

where $\sim$ is the Galois action of $\operatorname{Gal}(L|\mathbb{Q}_p)$ on the formal scheme $\widehat{\mathcal{H}}_p \otimes_{\mathbb{Z}_p} \operatorname{Spf}\mathcal{O}_L$ over $\operatorname{Spf}\mathcal{O}_L$. Therefore the formal scheme $\widehat{\mathcal{H}}_p^{\mathcal{O}_L}$ is obtained as a Galois descent of the formal scheme

$$\coprod_{i=1}^{r} (\widehat{\mathcal{H}}_p \otimes_{\mathbb{Z}_p} \operatorname{Spf}\mathcal{O}_L) \to \operatorname{Spf}\mathcal{O}_L.$$

In particular, if $\mathcal{H}_p^{\mathcal{O}_L}$ is the rigid analytic variety over $\mathbb{Q}_p$ which is a generic fibre of the formal scheme $\widehat{\mathcal{H}}_p^{\mathcal{O}_L}$, then

$$\mathcal{H}_p^{\mathcal{O}_L}(\mathbb{Q}_p) = \mathcal{H}_p(\mathbb{Q}_p) = \emptyset.$$

3.1.10 Notation. Let us denote by $\mathbb{Q}_p^{nr}$ the maximal unramified extension of $\mathbb{Q}_p$, which is unique inside the algebraic closure $\overline{\mathbb{Q}}_p$ that we chose at the beginning. The digression above taking $L = \mathbb{Q}_p^{nr}$ gives the following tuned upper half-plane over $\mathbb{Q}_p$:

$$\mathcal{H}_p^{nr} := \mathcal{H}_p \otimes_{\mathbb{Q}_p} \mathbb{Q}_p^{nr},$$

as a rigid analytic variety over $\mathbb{Q}_p$.

3.1.11 Definition. The action of $B^*(\mathbb{Q}_p) \simeq \mathrm{GL}_2(\mathbb{Q}_p)$ on $\mathcal{H}_p^{nr}$ is defined by:

$$\begin{array}{ccc} \mathrm{GL}_2(\mathbb{Q}_p) \times \mathcal{H}_p^{nr} & \longrightarrow & \mathcal{H}_p^{nr} \\ (\gamma, [z,x]) & \longmapsto & [\gamma \cdot z,\ \mathrm{Fr}^{-v_p(\mathrm{Det}(\gamma))}(x)]. \end{array}$$

where $\mathrm{Fr} : \mathbb{Q}_p^{nr} \to \mathbb{Q}_p^{nr}$ is a lifting of the Frobenius automorphism of $\overline{\mathbb{F}}_p$.

3.1.12 Theorem. (Cerednik-Drinfeld theorem)

There is an isomorphism of rigid analytic varieties over $\mathbb{Q}_p$:

$$(X(D_H,N)\otimes_{\mathbb{Q}}\mathbb{Q}_p)^{rig}\simeq (V_0(N)^{(p)}\times B^*(\mathbb{Q}_p))\backslash\mathcal{H}_p^{nr}\times B^*(\mathbb{A}_{fin})/B^*(\mathbb{Q}).$$

As a corollary we find the global version of the theorem, which has to be compared with Cerednik's original theorem (cf. Theorem 3.1.3 and 3.1.4).

3.1.13 Corollary. *Let us denote by* $\tilde{\Gamma}_p(D_B,N)$ *the subgroup of* $\mathrm{GL}_2(\mathbb{Q}_p)$ *defined by*

$$\tilde{\Gamma}_p(D_B,N):=\Phi_p(\mathcal{O}_B[1/p]^*).$$

Then there is an isomorphism of rigid analytic varieties over $\mathbb{Q}_p$:

$$(X(D_H,N)\otimes_{\mathbb{Q}}\mathbb{Q}_p)^{rig}\simeq\tilde{\Gamma}_p(D_B,N)\backslash(\mathcal{H}_p\otimes_{\mathbb{Q}_p}\mathbb{Q}_{p^2}).$$

Proof. First, the group $\tilde{\Gamma}_p(D_B,N)$ is the one described in Remark 3.1.9, i.e.

$$\tilde{\Gamma}_p(D_B,N)=\Phi_p(V_0(N)\cap B^*(\mathbb{Q})).$$

Thus, applying Theorem 3.1.6, we find the following isomorphism of rigid analytic varieties over $\mathbb{Q}_p$:

$$(X(D_H,N)\otimes_{\mathbb{Q}}\mathbb{Q}_p)^{rig}\simeq\tilde{\Gamma}_p(D_B,N)\backslash\mathcal{H}_p^{nr}.$$

Let us denote by $Z:=\tilde{\Gamma}_p(D_B,N)\cap\mathbb{Q}_p^*$ the center of $\tilde{\Gamma}_p(D_B,N)$ inside $\mathrm{GL}_2(\mathbb{Q}_p)$. Since Z acts trivially on $\mathcal{H}_p$, we have the following isomorphisms of rigid analytic varieties:

$$\tilde{\Gamma}_p(D_B,N)\backslash\mathcal{H}_p^{nr}\simeq\Gamma_p(D_B,N)\backslash(Z\backslash\mathcal{H}_p^{nr})\simeq\Gamma_p(D_B,N)\backslash(\mathcal{H}_p\otimes_{\mathbb{Q}_p}(Z\backslash\mathbb{Q}_p^{nr})),$$

and since Z contains the matrix $\left(\begin{smallmatrix}p&0\\0&p\end{smallmatrix}\right)$, its action on $\mathbb{Q}_p^{nr}$ gives the following isomorphism of rigid analytic spaces over $\mathbb{Q}_p$:

$$\Gamma_p(D_B,N)\backslash(\mathcal{H}_p\otimes_{\mathbb{Q}_p}(Z\backslash\mathbb{Q}_p^{nr}))\simeq\Gamma_p(D_B,N)\backslash\mathcal{H}_p\otimes_{\mathbb{Q}_p}\mathbb{Q}_{p^2},$$

(cf. Definition 3.1.11). □

3.1.14 Theorem. (Drinfeld theorem) *Let* $\Gamma_{p,+}(D_B,N)$ *be the subgroup of* $\mathrm{PGL}_2(\mathbb{Q}_p)$ *defined by*

$$\Gamma_{p,+}(D_B,N):=\{\gamma\in\tilde{\Gamma}_p(D_B,N)\mid v_p(\mathrm{Det}(\gamma))\equiv 0\,(\mathrm{mod}\,2)\}/\mathbb{Z}[1/p]^*,$$

and let $X_{p,+}(D_B,N)$ *be the algebraic curve over* $\mathbb{Q}_p$ *such that*

$$X_{p,+}(D_B,N)^{rig}\simeq\Gamma_{p,+}(D_B,N)\backslash\mathcal{H}_p.$$

Then there is an isomorphism of curves over $\mathbb{Q}_{p^2}$,

$$(X(D_H,N)\otimes_{\mathbb{Q}}\mathbb{Q}_p)\otimes_{\mathbb{Q}_p}\mathbb{Q}_{p^2}\simeq X_{p,+}(D_B,N)\otimes_{\mathbb{Q}_p}\mathbb{Q}_{p^2}.$$

PROOF. Let us define the quotient group $W := \Gamma_p(D_B, N)/\Gamma_{p,+}(D_B, N)$: this is a cyclic group of order 2. Let us denote by w_p a generator of W: this is a class of transformations $\gamma \in \Gamma_p(D_B, N)$ such that $v_p(\mathrm{Det}(\gamma))$ is odd.

With these notations, and applying Corollary 3.1.13, we find the following chain of isomorphisms of rigid analytic varieties over $\mathbb{Q}_p$:

$$(X(D_H, N) \otimes_{\mathbb{Q}} \mathbb{Q}_p)^{rig} \simeq \Gamma_p(D_B, N)\backslash(\mathcal{H}_p \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2}) \simeq$$
$$\simeq W\backslash\left(\Gamma_{p,+}(D_B, N)\backslash(\mathcal{H}_p \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2})\right) \simeq W\backslash\left((\Gamma_{p,+}(D_B, N)\backslash\mathcal{H}_p) \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2}\right).$$

This induces an isomorphism of the underlying algebraic curves over $\mathbb{Q}_p$:

$$X(D_H, N) \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq W\backslash(X_{p,+}(D_B, N) \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2})$$

where the action of W is induced by the one in Definition 3.1.11, and so is given by

$$\begin{array}{rccc} w_p: & X_{p,+}(D_B, N) \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2} & \longrightarrow & X_{p,+}(D_B, N) \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2} \\ & [z, x] & \longmapsto & [w_p \cdot z,\ \mathrm{Fr}^{-1}(x)]. \end{array}$$

Therefore the curve $X(D_H, N) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is the twist of the curve $X_{p,+}(D_B, N)$ given by the class $\chi \in \mathrm{H}^1(\mathrm{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p), \mathrm{Aut}(X_{p,+}(D_B, N) \otimes \mathbb{Q}_{p^2}))$, i.e.

$$X(D_H, N) \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq X_{p,+}(D_B, N)^{\chi}.$$

(cf. [JL84, Proposition 3.7]). □

3.1.15 Definition. The **Drinfeld integral model** of the Shimura curve $X(D_H, N)$ is the integral model $\mathcal{X}(D_H, N)$ over $\mathbb{Z}_p$ such that the completion along its special fibre is the formal scheme over $\mathrm{Spf}\,\mathbb{Z}_p$

$$\widehat{\mathcal{X}(D_H, N)} \simeq \Gamma(D_B, N)\backslash(\widehat{\mathcal{H}}_p \otimes_{\mathrm{Spf}\,\mathbb{Z}_p} \mathrm{Spf}\,\mathbb{Z}_{p^2}).$$

As a corollary of Theorem 3.1.14 we can obtain a description of the $\mathbb{Q}_{p^2}$-points of the Shimura curve $X(D_H, N)$ and of its reduction in p.

3.1.16 Corollary. *The set of $\mathbb{Q}_{p^2}$-points of the algebraic curve $X(D_H, N)$ can be expressed as a quotient of the p-adic upper half-plane by the action of a discrete cocompact subgroup of* $\mathrm{PGL}(\mathbb{Q}_p)$*, i.e. there is a bijection of sets*

$$\Gamma_{p,+}(D_B, N)\backslash\mathcal{H}_p(\mathbb{Q}_{p^2}) \simeq X(D_H, N)(\mathbb{Q}_{p^2}).$$

Moreover if $\mathcal{X}(D_H, N)$ denotes the Drinfeld integral model of $X(D_H, N)$, then the reduction graph of the special fibre of $\mathcal{X}(D_H, N)$ is the quotient graph

$$\mathcal{G}_p := \Gamma_{p,+}(D_B, N)\backslash\mathcal{T}_p.$$

where $\mathcal{T}_p$ denotes the Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_p)$.

3.1.17 Remark. If we think of the field of the complex number $\mathbb{C}$ as the quadratic unramified extension of $\mathbb{Q}_\infty = \mathbb{R}$, we obtain that the Archimedean analog of Corollary 3.1.16 is the well-known bijections of sets:

$$\Gamma_{\infty,+}(D_H, N)\backslash\mathcal{H} \simeq X(D_H, N)(\mathbb{C})$$

described in Section 1.2.

3.1.2.1 Cerednik-Drinfeld theorem for covers of Shimura curves

We can actually give a more general version of the Cerednik-Drinfeld theorem 3.1.12. We have not done this before since we preferred to give a more comprehensible exposition in the cases we treat, namely those Shimura curves arising from Eichler orders and with principal level 1.

For every open and compact subgroup

$$U = U_p \times U^{(p)} \subseteq H^*(\mathbb{Q}_p) \times H^*(\mathbb{A}^{(\infty,p)})$$

such that U_p is maximal, i.e. $U_p = \mathcal{O}_{H,p}^*$, let us write

$$V := B^*(\mathbb{Q}_p) \times V^{(p)} \subseteq B^*(\mathbb{Q}_p) \times B(\mathbb{A}^{(\infty,p)})$$

for the image of U, through a fixed isomorphism $H^*(\mathbb{A}^{(\infty,p)}) \simeq B^*(\mathbb{A}^{(\infty,p)})$.

Then there is an isomorphism of rigid analytic varieties over $\mathbb{Q}_p$

$$\mathbb{X}(H, U)^{rig} \simeq V\backslash\mathcal{H}_p^{nr} \times B^*(\mathbb{A}^{(\infty)})/B^*(\mathbb{Q}),$$

where $\mathbb{X}(H, U)$ is the double quotient space of Definition 1.2.22 and whose decomposition as disjoint union of Riemann surfaces is described in Theorem 1.2.25.

Moreover this isomorphism is compatible with the projections induced by the different open and compact subgroups $U \subseteq H^*(\mathbb{A}^{(\infty)})$.

3.1.18 Remark. When $U = U_0(N)$ we find Theorem 3.1.12 as a particular case of the isomorphism above.

3.1.19 Remark. It can be proved that the double quotient space

$$V\backslash B^*(\mathbb{A}^{(\infty)})/B^*(\mathbb{Q})$$

is finite of cardinality $h(V)$ and that if $\{x_1, \ldots, x_{h(V)}\}$ is a system of representatives for it, then there is a decomposition in rigid analytic varieties

$$V\backslash\mathcal{H}_p^{nr} \times B^*(\mathbb{A}^{(\infty)})/B^*(\mathbb{Q}) \simeq \bigcup_{\lambda=1}^{h(V)} \Gamma_\lambda\backslash\mathcal{H}_p^{nr},$$

where $\Gamma_\lambda := x_\lambda^{-1}(V \cap B^*(\mathbb{Q}))x_\lambda$ for every $1 \leq \lambda \leq h(V)$.

This is done with the same tools used for proving Proposition 3.1.7 and Theorem 3.1.6, namely Eichler's *Normensatz* and Strong approximation theorem for the algebra B and the Eichler order $\mathcal{O}_H[1/p]$. In this direction the reader may find very useful to compare this presentation with the one offered in [dVP14, Ch. 3], which provides detailed study of this general situation.

3.2 Fundamental domains for p-adic Schottky groups

As explained in Section 3.1, the theory of p-adic uniformization of Shimura curves gives rise to the consideration of certain discrete, cocompact subgroups of $\mathrm{PGL}_2(\mathbb{Q}_p)$. Now these groups are, in general, no longer torsion-free: actually they contain elliptic transformations, as we will see in the examples. So making use of some language,

"A Shimura curve over $\mathbb{Q}_p$ is not (even the twist of) a Mumford curve".

Nevertheless, the theory of Mumford curves is of crucial importance since, as we can extrapolate from Corollary 3.1.16,

"A Shimura curve is the twist over $\mathbb{Q}_{p^2}$ of a finite quotient of a Mumford curve".

Therefore, if we want to draw fundamental domains for the rigid analytic uniformization of a p-adic Shimura curve it is useful to first understand how to obtain these domains in the torsion-free case, i.e. the case of Mumford curves.

3.2.1 Good fundamental domains

3.2.1 Definition. Let $\mathbb{P}^1 = \mathbb{P}^{1,rig}_{\mathbb{Q}_p}$ be the rigid projective line over $\mathbb{Q}_p$ (as defined at the beginning of Section 2.2) and let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a Schottky group of rank g and $S = \{\gamma_1, \ldots, \gamma_g\}$ be a system of generators fro Γ.

A **good fundamental domain for Γ with respect to** S is a subdomain with holes (cf. Definition 2.2.7)

$$\mathcal{F}_\Gamma = \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \bigcup_{i=1}^{2g} \mathbb{B}^-(\alpha_i, \rho_i)$$

satisfying the following conditions:

(i) The centers α_i are in $\mathbb{P}^1(\mathbb{Q}_p)$, for every $1 \leq i \leq 2g$.

(ii) All the closed balls $\mathbb{B}_i^+(\alpha_i, \rho_i)$, for $1 \leq i \leq 2g$, are pair-wise disjoint.

(iii) For every $1 \leq i \leq g$,

$$\gamma_i(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{B}^-(\alpha_i, \rho_i)) = \mathbb{B}^+(\alpha_{i+g}, \rho_{i+g}),$$

$$\gamma_i(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{B}^+(\alpha_i, \rho_i)) = \mathbb{B}^-(\alpha_{i+g}, \rho_{i+g}).$$

The fact that the domain $\mathcal{F}_\Gamma$ defined above is "fundamental" for the action of the group Γ on $\mathcal{H}_p$ is expressed in the following proposition (cf. [GvDP80, 4.1]).

3.2.2 Proposition. *Let Γ be a Schottky group in $\mathrm{PGL}_2(\mathbb{Q}_p)$ with free system of generators $S = \{\gamma_1, \ldots, \gamma_g\}$ and let $\mathcal{F}_\Gamma$ be a good fundamental domain for the group Γ with respect to S. Then*

(a) We have the following equality of sets:

$$\bigcup_{\gamma \in \Gamma} \gamma \cdot \mathcal{F}_\Gamma = \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathcal{L}_\Gamma.$$

(b) $(\gamma \cdot \mathcal{F}_\Gamma) \cap \mathcal{F}_\Gamma \neq \emptyset$ if and only if $\gamma \in \{\mathrm{I}_2, \gamma_1, \ldots, \gamma_g, \gamma_1^{-1}, \ldots, \gamma_g^{-1}\}$.

(c) $(\gamma \cdot \mathring{\mathcal{F}}_\Gamma) \cap \mathcal{F}_\Gamma = \emptyset$ if $\gamma \neq \mathrm{I}_2$.

3.2.3 Remark. As observed by Gerritzen in [Ger74], it is possible to construct a subdomain with holes $\mathcal{F} \subseteq \mathbb{P}^1(\mathbb{C}_p)$ satisfying conditions (a)-(c) of Proposition [GvDP80] and which is not a good fundamental domain with respect to any system of generators of the group Γ considered. In this case we would say that $\mathcal{F}$ is a fundamental domain for Γ but it is not a *good* fundamental domain.

Moreover in [Ger74] and in [GvDP80, Ch. I] the existence of a good fundamental domain for every Schottky group is proved, making use of the non-Archimedean analog of Ford's method of isometric circles (cf. [For51] and [AB04, Section 2.2]).

Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a Schottky group and let $\chi : \Gamma \to \mathbb{C}_p^*$ be a one dimensional character of the group Γ. For every $z \in \mathbb{P}^1(\mathbb{C}_p)$ and $\gamma \in \Gamma$ we define the following p-adic factor of automorphy, depending on the character χ,

$$j(\gamma, z) := \chi(\gamma) \frac{d}{dz}(\gamma \cdot z)) = \chi(\gamma) \frac{\det \gamma}{(cz + d)^2},$$

satisfying the usual chain-rule: $j(\gamma\sigma, z) = j(\gamma, \sigma \cdot z) j(\sigma, z)$.

3.2.4 Definition. For every $\gamma \in \Gamma$, we define the following open ball and closed ball:

$$B_\gamma^- := \{z \in \mathbb{C}_p : \ |j(\gamma, z)| > 1\}, \qquad B_\gamma^+ := \{z \in \mathbb{C}_p : \ |j(\gamma, z)| \geq 1\}.$$

We can call the "boundary" of these two balls, which is the set of points

$$\{z \in \mathbb{C}_p : \ |j(\gamma, z)| = 1\},$$

a **p-adic circle of isometry of the transformation** γ.

It is a simple calculation to check that if γ is represented by a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p)$, then

$$B_\gamma^\pm = \mathbb{B}^\pm \left(-\frac{d}{c}, \frac{\sqrt{|\chi(\gamma)(ad-bc)|}}{|c|} \right)$$

is the ball of center $-d/c$ and radius $\sqrt{|\chi(\gamma)\det(\gamma)|}/|c|$.

It is then immediate to see that the ball $B_\gamma^\pm$ does not depend on the matrix representing the transformation $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$.

3.2.5 Lemma. *Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a Schottky group. Then for every $\gamma \in \Gamma, \gamma \neq \mathrm{I}_2$, and every character $\chi : \Gamma \to \mathbb{C}_p^*$ we have*

$$\gamma(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus B_\gamma^-) = B_{\gamma^{-1}}^+, \quad \gamma(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus B_\gamma^+) = B_{\gamma^{-1}}^-.$$

Proof. Let $z = \gamma w \in \gamma(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus B_\gamma^-)$, so $|d(\gamma \cdot w)/dw| \leq 1$ by the definition of B_γ^-. Therefore

$$\left| \frac{d(\gamma^{-1} \cdot z)}{dz} \right| = \left| \frac{d(\gamma^{-1}\gamma \cdot w)}{d(\gamma \cdot w)} \right| = \left| \frac{dw}{d(\gamma \cdot w)} \right| \geq 1$$

and $z \in B_{\gamma^{-1}}^+$.

Viceversa if $z \in B_{\gamma^{-1}}^+$, then $|d(\gamma^{-1} \cdot z)/dz| \geq 1$. Hence if we put $w := \gamma^{-1} \cdot z$ we find that $z = \gamma \cdot w$ and

$$1 \leq \left| \frac{d(\gamma^{-1} \cdot z)}{dz} \right| = \left| \frac{dw}{d(\gamma \cdot w)} \right|,$$

so $w \in \mathbb{P}^1(\mathbb{C}_p) \smallsetminus B_\gamma^-$. □

3.2.6 Theorem. ([Ger74], Satz 1) *Let Γ be a Schottky group of rank g. Then there exist a system of generators $S = \{\gamma_1, \ldots, \gamma_g\}$ for Γ and a character $\chi : \Gamma \to \mathbb{C}_p^*$ such that the admissible subdomain with holes*

$$\mathcal{F}_\Gamma := \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \bigcup_{i=1}^{g} (B^-_{\gamma_i} \cup B^-_{\gamma_i^{-1}})$$

is a good fundamental domain for Γ with respect to S.

3.2.7 Remark. After Lemma 3.2.5 we see that given a Schottky Γ, for any system of generators S of Γ condition (i) and (iii) of Definition 3.2.1 are satisfied for the fundamental domain $\mathcal{F}_\Gamma$ of Theorem **??**. So, in some sense, the important condition for which we have to choose a *good* system of generators is condition (ii).

3.2.8 Proposition. *Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a cocompact Schottky group of rank g and free system of generators $S = \{\gamma_1, \ldots, \gamma_g\}$. Let us assume that:*

(a) The rank of Γ is $g = (p+1)/2$.

(b) The balls $B_{\gamma_i}, B_{\gamma_i^{-1}}$, for $1 \leq i \leq g$, have all the same radius $\rho < 1$.

Then a good fundamental domain for Γ with respect to S is

$$\mathcal{F}_\Gamma = \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \bigcup_{i=1}^{g} B^-_{\gamma_i} \cup \bigcup_{i=1}^{g} B^-_{\gamma_i^{-1}}.$$

Proof. We have to see that $\mathcal{F}_\Gamma$ satisfies conditions (i)-(iii) of Definition 3.2.1.

Condition (i) is satisfied because the centers of the balls $B^-_{\gamma_i}, B^-_{\gamma_i^{-1}}$ are clearly in $\mathbb{P}^1(\mathbb{Q}_p)$. Condition (iii) is satisfied after Lemma 3.2.5. Finally we have only to look at condition (ii).

Let us suppose that there exist $i, j \in \{1, \ldots, (p+1)/2\}, i \neq j$, such that $B^+_{\gamma_i} \cap B^+_{\gamma_j} \neq \emptyset$, and so $B^+_{\gamma_i} = B^+_{\gamma_j}$, because they have the same radius by hypothesis (a).

Applying the reduction map of Theorem 2.2.31 we find that the reductions

$$y_i := \mathrm{Red}(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus B^-_{\gamma_i}), \quad y_{i+g} := \mathrm{Red}(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus B^-_{\gamma_i^{-1}}), \quad 1 \leq i \leq \frac{p+1}{2}$$

are open edges all corresponding to different vertexes in the first level $\mathcal{T}_p^{(1)}$ of the Bruhat-Tits tree. This is because the radii of the balls are all equal to some $\rho < 1$.

Moreover since

$$\mathrm{Red}(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus B^+_{\gamma_i}) = \mathrm{Red}(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus B^+_{\gamma_j}),$$

then we have at most p of such edges. Hence there exists an edge $y_a := (v^0, v^0_a)$, with $a \in \mathbb{P}^1(\mathbb{F}_p)$ such that

$$\gamma_i^{-1}(v^0_a) = \mathrm{Red}(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus B^+_{\gamma_i}) \quad \gamma_j^{-1}(v^0_a) = \mathrm{Red}(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus B^+_{\gamma_j})$$

so $\gamma_i\gamma_j^{-1}(v^0_a) = v^0_a$, which is an absurd since the group Γ is torsion-free. □

3.2.2 p-adic Schottky groups arising from definite quaternion algebras

Let B be a definite quaternion algebra over $\mathbb{Q}$ of discriminant D_B and let p be a prime integer not dividing D_B. Let $\mathcal{O}_B$ be an Eichler order over $\mathbb{Z}$ of level N coprime with p. As usual, we denote by

$$\mathcal{O}_B[1/p] := \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$$

the corresponding Eichler order over $\mathbb{Z}[1/p]$ and by $\mathcal{O}[1/p]^*$ its group of units, which is the group of quaternions in $\mathcal{O}_B[1/p]$ of norm some power of p. Moreover we denote by $\mathcal{O}_B[1/p]^*_+$ the corresponding group of "positive" units, i.e.

$$\mathcal{O}_B[1/p]^*_+ := \{\alpha \in \mathcal{O}_B[1/p]^* \mid v_p(\mathrm{Nm}_{B/\mathbb{Q}}(\alpha)) \equiv 0 \,(\mathrm{mod}\, 2)\}.$$

This is clearly a group of index 2 in $\mathcal{O}_B[1/p]^*$, and a system of representatives for this group is the group of quaternions $\alpha \in \mathcal{O}_B[1/p]^*$ of norm 1.

The algebra B admits a representation $B = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ such that $\left(\frac{\alpha}{p}\right) = 1$ and then we have the following p-adic matricial immersion:

$$\begin{array}{ccccc} \Phi_p : & B & \longrightarrow & \mathrm{M}_2(\mathbb{Q}_p(\sqrt{\alpha})) = \mathrm{M}_2(\mathbb{Q}_p) \\ x_0 + x_1 i + x_2 j + x_3 k & \longmapsto & \begin{pmatrix} x_0 + x_1\sqrt{\alpha} & x_2 + x_3\sqrt{\alpha} \\ \beta(x_2 - x_3\sqrt{\alpha}) & x_0 - x_1\sqrt{\alpha} \end{pmatrix} \end{array}$$

We want to study the following discrete and cocompact subgroups of $\mathrm{PGL}_2(\mathbb{Q}_p)$:

(i) $\Gamma_p(D_B, N) := \Phi_p(\mathcal{O}_B[1/p]^*)/\mathbb{Z}[1/p]^*$,

(ii) $\Gamma_{p,+}(D_B, N) := \Phi_p(\mathcal{O}_B[1/p]^*_+)/\mathbb{Z}[1/p]^*$,

because these are the important subgroups arising in the p-adic uniformization of a Shimura curve of discriminant pD_B.

We will show that under certain assumptions on the algebra B and on the Eichler order $\mathcal{O}_B$, we can find a Schottky subgroup $\Gamma^{Sch} \subseteq \Gamma_p(D_B, N)$ and a system of generators as a free group. As predicted by Theorem 2.3.23, we can look for this Schottky subgroup among the *principal* congruence subgroups of $\Gamma_p(D_B, N)$. For this reason we introduce the following notations: for every integer $M \geq 2$ coprime with p we have an exact sequence

$$1 \to \{\alpha \in \mathcal{O}_B[1/p]^* \mid \alpha \equiv 1 \,(\mathrm{mod}\, M)\} \to \mathcal{O}_B[1/p]^* \to (\mathcal{O}_B/M\mathcal{O}_B)^* \to 1.$$

The last map, which is reduction mod M of the integral coordinates of quaternions $\alpha \in \mathcal{O}_B$, is well-defined according to Proposition 1.1.25 since $(p, M) = 1$ and so $p^s \in (\mathbb{Z}/N\mathbb{Z})^*$. The fact that this map is surjective is a consequence of the Strong approximation theorem for the algebra B and the Eichler order $\mathcal{O}_B[1/p]$ (cf. Theorem1.1.9). The analogous proof in the case of the algebraic group SL_2 over $\mathbb{Q}$ is given in [Shi70a, Lemma1.38]. Finally we define

$$\widetilde{\Gamma}_p(D_B, N)(M) = \Phi_p(\{\alpha \in \mathcal{O}[1/p]^* \mid \alpha \equiv 1 \,(\mathrm{mod}\, M)\} \subseteq \mathrm{GL}_2(\mathbb{Q}_p),$$

and

$$\Gamma_p(D_B, N)(M) := \tilde{\Gamma}_p(D_B, N)(M)/\mathbb{Z}[1/p]^* \cap \tilde{\Gamma}_p(D_B, N)(M) \subseteq \mathrm{PGL}_2(\mathbb{Q}_p).$$

First, we will make some *ad hoc* assumptions regarding these quaternionic groups. Later we will exhibit two (numerable) families of examples satisfying them and showing interesting and detailed examples of fundamental domains for the Shimura curves and Mumford curves covering them.

For every integer $M \geq 1, (M, p) = 1$, let us consider the following subset of quaternions

$$S := \{\alpha \in \mathcal{O}_B \mid \alpha \equiv 1 \,(\mathrm{mod}\, M)\,, \mathrm{Nm}(\alpha) = p\} \subseteq \mathcal{O}_B.$$

It is clear that the cardinality of S is equal to the cardinality of the following set of integral representations:

$$\{(x, y, z, t) \in \mathbb{Z}^4 \mid \mathrm{N}_{\mathcal{O}_B,4}(x, y, z, t) = p,\ (x, y, z, t) \equiv (1, 0, 0, 0) \,(\mathrm{mod}\, M)\}.$$

We denote this cardinality by $r_M(\mathrm{N}_{\mathcal{O}_B,4}, p; \mathbb{Z})$: it is a finite cardinal, since the quaternary quadratic form $\mathrm{N}_{\mathcal{O}_B,4}$ is positive definite.

We can split the set R into two disjoint sets

$$S^{pure} := S \cap B_0 \qquad S^{npure} := S \smallsetminus S^{pure}$$

depending on whether the quaternion is pure or not. With this simple splitting idea we can write each one of the sets as

$$S^{npure} := \{\pm\alpha_1, \ldots, \pm\alpha_s, \pm\overline{\alpha}_1, \ldots, \pm\overline{\alpha}_s\}, \qquad S^{pure} = \{\pm\beta_1, \ldots, \pm\beta_t\},$$

when $M = 2$ and as

$$S^{npure} := \{\alpha_1, \ldots, \alpha_s, \overline{\alpha}_1, \ldots, \overline{\alpha}_s\}, \qquad S^{pure} = \{\pm\beta_1, \ldots, \pm\beta_t\},$$

when $M > 2$, since in both cases $\overline{\beta}_i = -\beta_i$ for every $1 \leq i \leq t$ and only when $M = 2$, $\alpha_i \in S^{npure}$ is equivalent to $-\alpha_i \in S^{npure}$.

Therefore we have that

$$r_M(\mathrm{N}_{\mathcal{O}_B,4}, p; \mathbb{Z}) = \begin{cases} 4s + 2t, & \text{if } M = 2 \\ 2s + 2t, & \text{otherwise} \end{cases}.$$

Now we prove the following important result:

3.2.9 Proposition. *With the same notations as above, let us assume that the group* $\{\alpha \in \mathcal{O}_B[1/p]^* \mid \alpha \equiv 1 \,(\mathrm{mod}\, M)\}$ *is generated by the set* S*.*

Then the quotient group $\{\alpha \in \mathcal{O}_B[1/p]^* \mid \alpha \equiv 1 \,(\mathrm{mod}\, M)\}/\mathbb{Z}[1/p]^*$ *admits a finite presentation as*

$$\langle [\alpha_1], \ldots, [\alpha_s], [\beta_1], \ldots, [\beta_t] \mid [\beta_i]^2 = 1,\ 1 \leq i \leq t \rangle.$$

In particular, when $t = 0$*, then* $\{[\alpha_1], \ldots, [\alpha_s]\}$ *is a free system of generators for this quotient group.*

Proof. Since we are assuming that $\mathcal{O}_B[1/p]^*$ is generated by the set S then it is clear that $\{\alpha \in \mathcal{O}_B[1/p]^* \mid \alpha \equiv 1 \,(\mathrm{mod}\, M)\}/\mathbb{Z}[1/p]^*$ is generated by the set of classes $\{[\alpha_1], \ldots, [\alpha_s], [\beta_1], \ldots, [\beta_t]\}$ with relations $[\beta_i]^2 = 1$. This is because $\alpha_i\overline{\alpha}_i = p$ and $\beta_i\overline{\beta}_i = -\beta_i^2 = p$ which is a unit in $\mathbb{Z}[1/p]$.

Finally we have only to prove that these are the only relations. First observe that a relation between the $[\alpha_i]$ can only contained an even number of elements. Therefore we are reduced to proving that there is no pair of elements $[\alpha_i], [\alpha_j]$ such that $[\alpha_i][\alpha_j] = [1]$.

If there exist two such classes, then we have that $\alpha_i\alpha_j = p^n$ for some $n \in \mathbb{Z}$ and taking the norm we find that it has to be $n = 1$. Hence $\alpha_i\alpha_j = p$ and so $\alpha_i = \overline{\alpha}_j$, which is an absurd because we have already excluded the conjugates of all the α_i's. □

In some cases (at least the ones we are going to develop later in details) a knowledge of the arithmetic in the quaternion order $\mathcal{O}_B$ makes it possible to find examples where the hypothesis of Proposition 3.2.9 are fulfilled. Before working explicitly on the examples, we explain how in these cases we will be able to apply Proposition 3.2.9. This is the following result.

3.2.10 Proposition. *Let B be a definite quaternion algebra of discriminant D_B and $p \in \mathbb{Z}$ a prime $p \nmid D_B$. Let $\mathcal{O}_B$ be an Eichler order over $\mathbb{Z}$ of level N and let $\mathcal{O}_B[1/p] := \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ be the corresponding Eichler order over $\mathbb{Z}[1/p]$.*

Let us assume that there exists an integer $M \geq 2, (M,p) = 1$ such that the following hypothesis are fulfilled by the quaternion algebra B and the Eichler order $\mathcal{O}_B$.

(*i*) *There is an isomorphism of groups*

$$\mathcal{O}_B^*/\mathbb{Z}^* \simeq (\mathcal{O}_B/M\mathcal{O}_B)^*,$$

(*ii*) *The group $\mathcal{O}[1/p]^*$ admits a decomposition, as a semi-direct product,*

$$\mathcal{O}[1/p]^* \simeq \mathcal{O}_B^* \ltimes \langle \{\alpha \in \mathcal{O}_B \mid \mathrm{Nm}(\alpha) = p,\ \alpha \equiv 1 \,(\mathrm{mod}\, M)\}\rangle.$$

(*iii*) *There is no pure quaternion $\alpha \in \mathcal{O}_B$ of norm p satisfying the congruence condition $\alpha \equiv 1 \,(\mathrm{mod}\, M)$.*

Then the group $\Gamma_p(D_B, N)(M)$ is a Schottky group of rank

$$s = \begin{cases} r_M(\mathrm{N}_{\mathcal{O}_B,4}, p; \mathbb{Z})/4, & \text{if } M = 2 \\ \\ r_M(\mathrm{N}_{\mathcal{O}_B,4}, p; \mathbb{Z})/2, & \text{otherwise} \end{cases}$$

and a free system of generators is given by the classes of matrices of determinant p.

Proof. On the one hand we have the exact sequence described before,

$$1 \longrightarrow \{\alpha \in \mathcal{O}[1/p]^* \mid \alpha \equiv 1 \,(\mathrm{mod}\, M)\} \longrightarrow \mathcal{O}[1/p]^* \longrightarrow (\mathcal{O}_B/M\mathcal{O}_B)^* \longrightarrow 1,$$

which gives an isomorphism

$$\mathcal{O}[1/p]^* \simeq (\mathcal{O}_B/M\mathcal{O}_B)^* \ltimes \{\alpha \in \mathcal{O}_B \mid \alpha \equiv 1 \,(\mathrm{mod}\, M)\}$$

and on the other hand, by hypothesis (ii), we have

$$\mathcal{O}[1/p]^* \simeq \mathcal{O}_B^* \ltimes \langle \{\alpha \in \mathcal{O}_B \mid \mathrm{Nm}(\alpha) = p,\ \alpha \equiv 1 \,(\mathrm{mod}\, M)\}\rangle.$$

Passing on to the quotient by $\mathbb{Z}[1/p]^*$ and using the isomorphism of hypothesis (i), we deduce that

$$\Gamma_p(D_B, M)(N) = \langle \{\gamma \in \Gamma_p(D_B, N)(M) \mid \mathrm{Det}(\gamma) = p\}\rangle,$$

so we have found a finite set of generators for the group $\Gamma_p(D_B, N)(M)$.

Moreover after hypothesis (iii), we can apply Proposition 3.2.9 to the group $\Gamma_p(D_B, N)(M)$ in order to deduce that this is a Schottky group of the desired rank s. □

Conditions (i) and (ii) come from the study of the arithmetic of the order $\mathcal{O}_B$. As we shall see, these conditions become natural after studying the simplest case of a certain maximal order in a definite quaternion algebra over $\mathbb{Q}$, which is the order of **quaternions of Hurwitz**. Basic results about the arithmetic of this order were presented in Chapter 1.1 and will be applied in the following section, in order to obtain results about the reduction graphs of Shimura curves of discriminant $D_H = 2p$, when $p \equiv 1 \,(\mathrm{mod}\, 4)$.

In this section we will see that the quaternion algebras B of discriminant $D_B = 2$ or $D_B = 3$ together with their corresponding maximal orders $\mathcal{O}_B$ satisfy the hypothesis of Proposition 3.2.10 for every prime $p \equiv 1 \,(\mathrm{mod}\, 4)$ and with $M = 2$. After that we will compute explicitly generators for the p-adic matricial group $\Gamma_p(D_B, 1)(2)$.

The following examples have been worked out together with Laia Amorós and they are part of a common project, in which we wish to compute more and more examples in this direction, in order to obtain p-adic fundamental domains for any Shimura curves defined over $\mathbb{Q}$, as well as its reduction graphs.

3.2.3 The case of discriminant $D_H = 2p$

3.2.11 Theorem. *Let B be the definite quaternion algebra over $\mathbb{Q}$ of discriminant $D_B = 2$ and let $\mathcal{O}_B \subseteq B$ be a maximal order over $\mathbb{Z}$. Let $p \in \mathbb{Z}$ be a prime $p \equiv 1 \,(\mathrm{mod}\, 4)$.*

(a) The group $\Gamma_p(D_B, 1)(2)$ is a Schottky group of rank $(p+1)/2$.

(*b*) *A free system of generators for the Schottky group* $\Gamma_p(D_B,1)(2)$ *is given by the transformations represented by the following matrices:*

$$\begin{pmatrix} a_0+a_1\sqrt{-1} & a_2+a_3\sqrt{-1} \\ -(a_2-a_3\sqrt{-1}) & a_0-a_1\sqrt{-1} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p(\sqrt{-1})) = \mathrm{GL}_2(\mathbb{Q}_p)$$

such that

$$a_0,a_1,a_2,a_3 \in \mathbb{Z},$$

$$a_0^2+a_1^2+a_2^2+a_3^2 = p,$$

$$a_0+a_3 \equiv 1 \,(\mathrm{mod}\, 2),\ a_1+a_3 \equiv a_2+a_3 \equiv 0 \,(\mathrm{mod}\, 2).$$

(*c*) *A good fundamental domain for the action of the group* $\Gamma_p(D_B,1)(2)$ *is the following admissible open subset of* $\mathbb{P}^{1,rig}$:

$$\mathcal{F}_p(D_B,1;2) := \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \bigcup_{a\in\mathbb{P}^1(\mathbb{F}_p)} \mathbb{B}^-(a,1/\sqrt{p}).$$

(*d*) *If we denote by* $X_p(D_B,1;2)$ *the Mumford curve associated to the Schottky group* $\Gamma_p(D_B,1)(2)$*, then its rigidification* $X_p^{rig}(D_B,1;2)$ *is isomorphic to the domain* $\mathcal{F}_p(D_B,1;2)$ *with the following identifications:*

if $\gamma = \begin{pmatrix} a_0+a_1\sqrt{-1} & a_2+a_3\sqrt{-1} \\ -(a_2-a_3\sqrt{-1}) & a_0-a_1\sqrt{-1} \end{pmatrix}$ *then*

$$\gamma\left(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{B}^-(a_\gamma,1/\sqrt{p})\right) = \mathbb{B}^+(a_{\gamma^{-1}},1/\sqrt{p}),$$

$$\gamma\left(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{B}^+(a_\gamma,1/\sqrt{p})\right) = \mathbb{B}^-(a_{\gamma^{-1}},1/\sqrt{p}),$$

where a_γ *and* $a_{\gamma^{-1}}$ *are defined as the classes in* $\mathbb{P}^1(\mathbb{F}_p)$ *of the p-adic integers* $\dfrac{a_0-a_1\sqrt{-1}}{a_2-a_3\sqrt{-1}}$ *and* $\dfrac{a_0+a_1\sqrt{-1}}{-a_2+a_3\sqrt{-1}}$*, respectively.*

(*e*) *With the notations as in Section 2.2.2, the stable reduction graph of the Mumford curve* $X_p(D_B,1;2)$ *is the subtree* $\mathcal{T}_p^{(1)} \smallsetminus \{v_a^0 \mid a \in \mathbb{P}^1(\mathbb{F}_p)\}$ *of* $\mathcal{T}_p$ *with the following identifications of the oriented edges:*

$$\gamma\cdot\left(v^0, v^0_{a_\gamma}\right) = \left(v^0_{a_{\gamma^{-1}}}, v^0\right)$$

for every $\gamma \in \{\gamma_1,\ldots,\gamma_{(p+1)/2}\}$.

3.2.12 Remark. Before starting with the proof of the theorem above, we want only to remark that we already know, by the theory of Mumford curves, that $X_p(D_B, 1; 2)$ is a curve over $\mathbb{Z}_p$ of genus $(p+1)/2$. In any case, this can be deduced or confirmed by looking at the genus of the stable reduction graph $\Gamma_p(D_B, 1)(2)\backslash\mathcal{T}_p$ described in the theorem (see also Figures 3.1b, 3.2b).

Passing through the dual, we can also see that the special fibre of the curve $X_p(D_B, 1; 2)$ has one irreducible component isomorphic to the projective line $\mathbb{P}^1_{\mathbb{F}_p}$ over $\mathbb{F}_p$, with $(p+1)/2$ double points obtained by the pairwise identification of its $\mathbb{F}_p$-rational points, namely the reduction mod p of the p-adic integers $a_\gamma \sim a_{\gamma^{-1}}$ for every $\gamma \in \{\gamma_1, \ldots, \gamma_{(p+1)/2}\}$.

Proof. First let us show that the quaternion algebra $B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ together with the maximal order $\mathcal{O}_B = \langle 1, i, j, (1+i+j+k)/2\rangle_{\mathbb{Z}}$ of quaternions of Hurwitz satisfy the hypothesis of Proposition 3.2.10, taking $M = 2$.

Hypothesis (i) in Proposition 3.2.10 is shown to be fulfilled in Example 1.1.2.1 (b). Hypothesis (ii) is a consequence of Corollary 1.1.28, once we have observed that every odd quaternion $\alpha \in \mathcal{O}_B$ is uniquely associated on the right and on the left, modulo the sign of the units, to a quaternion $\alpha' \equiv 1 \pmod 2$ (cf. Example 1.1.2.1 (c)). In fact, we find an isomorphism of groups

$$\mathcal{O}_B[1/p]^* \simeq \mathcal{O}^*/\mathbb{Z}^* \ltimes \langle\{\alpha \in \mathcal{O}_B \mid \mathrm{Nm}(\alpha) = p,\ \alpha \equiv 1 \pmod 2\}\rangle/\mathbb{Z}[1/p]^*.$$

It only remains to show that hypothesis (iii) in Proposition 3.2.10 is also satisfied: this is clear since, by Lemma 1.1.29, we know that every pure quaternion $\alpha \in \mathcal{O}_B \cap B_0$ of norm p, satisfying $\alpha \equiv 1 \pmod 2$, is of the form

$$\alpha = a_1 i + a_2 j + a_3 k, \text{ with } a_1 \equiv a_2 \equiv a_3 \equiv 1 \pmod 2$$

and so reducing mod 4 the equation $\mathrm{Nm}(\alpha) = a_1^2 + a_2^2 + a_3^2 = p$ we obtain that $p \equiv 3 \pmod 4$. Hence the set of such quaternions is empty when $p \equiv 1 \pmod 4$.

For every prime $p \geq 5$, it is easy to see that

$$r_2(\mathrm{N}_{\mathcal{O}_B,4}, p; \mathbb{Z}) = \frac{1}{4}\, r(\mathrm{N}_{B,4}, p; \mathbb{Z}).$$

From a theorem of Jacobi we know that $r(\mathrm{N}_{B,4}, p; \mathbb{Z}) = 8(p+1)$ for every odd prime integer p, so in our cases we have $r_2(\mathrm{N}_{\mathcal{O}_B,4}, p; \mathbb{Z}) = 2(p+1)$.

Hence, by Proposition 3.2.10, the group $\Gamma_p(D_B, N)(2)$ is a Schottky group of rank

$$\frac{r_2(\mathrm{N}_{\mathcal{O}_B,4}, p; \mathbb{Z})}{4} = \frac{p+1}{2},$$

and point (a) of the statement is proved.

Point (b) is a restatement of Lemma 1.1.29 in terms of matrices.

Now we are going to apply Proposition 3.2.8 to the group $\Gamma_p(D_B,1)(2)$ and to the free system of generators $S=\{\gamma_1,\dots,\gamma_{(p+1)/2}\}$ described in point (b), in order to prove point (c).

It is easy to see that the group $\Gamma_p(D_B,1)(2)$ together with the system of generators S satisfy the hypothesis of Proposition 3.2.8. In fact, $\Gamma_p(D_B,1)(2)$ is a Schottky group of rank $(p+1)/2$ and if we take the character $\chi:\Gamma\to\mathbb{C}_p^*$ defined by $\chi(\gamma_i)=1$ for every $1\leq i\leq (p+1)/2$, then the radii of the balls $B^-_{\gamma_i},B^-_{\gamma_i^{-1}}$ are all equal to $1/\sqrt{p}<1$. Actually looking at how the balls $B^-_{\gamma_i},B^-_{\gamma_i^{-1}}$ are defined (cf. Definition 3.2.4) we find that the radius of $B^-_{\gamma_i}$ is

$$\frac{\sqrt{|\chi(\gamma_i)\mathrm{Det}(\gamma_i)|}}{|-(a_2-\sqrt{-1}a_3)|}=\frac{1}{\sqrt{p}},$$

since γ_i has determinant equal p and $|-(a_2-\sqrt{-1}a_3)|=1$. And the same holds for the radius of $B_{\gamma_i^{-1}}$. This concludes the proof of point (c).

By the definition of good fundamental domain (cf. Definition 3.2.1) we know that the boundaries of the balls $B^+_{\gamma},B^+_{\gamma^{-1}}$ are identified by the transformations γ and γ^{-1}. This proves point (d).

Finally point (e) follows by applying the reduction map of Theorem 2.2.31 to the affinoid subdomain $\mathcal{F}_p(D_B,1;2)$. Actually for every $a\in\mathbb{P}^1(\mathbb{F}_p)$ we have

$$\mathbb{P}^1(\mathbb{C}_p)\smallsetminus\mathbb{B}(a,1/\sqrt{p})\subsetneq\mathbb{P}^1(\mathbb{C}_p)\smallsetminus\mathbb{B}(a,1/p)$$

and the reduction of these two admissible open subsets of $\mathcal{H}_p$ are the following open edge and closed edge respectively,

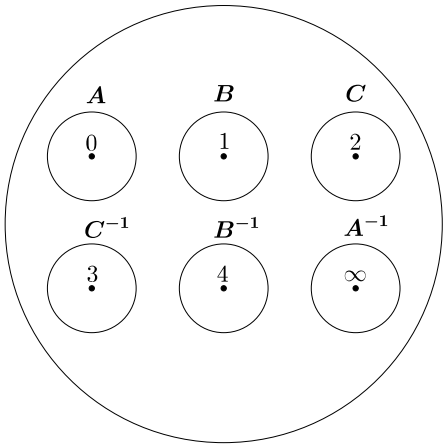
$$\mathrm{Red}(\{z\in\mathbb{C}_p\mid 0\leq v_p(z)\leq 1/2<1\})=\{v^0\}\cup(v^0,v^0_a),$$

$$\mathrm{Red}(\{z\in\mathbb{C}_p\mid 0\leq v_p(z)\leq 1\})=\{v^0,v^0_a\}\cup(v^0,v^0_a),$$

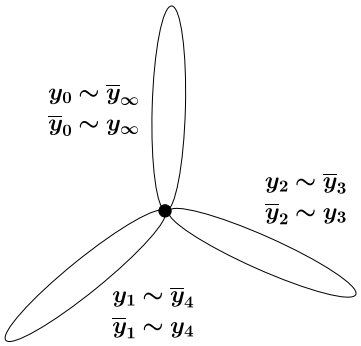
inside the rational geometric realization $\mathcal{T}_{p,\mathbb{Q}}$ of the tree $\mathcal{T}_p$, described in Section 2.2.2. □

3.2.3.1 Examples for $D_B=2$

(1) $D_B=2,p=5$.



(a) $\Gamma_5(2,1)(2)\backslash\mathcal{H}_5$



(b) $\Gamma_5(2,1)(2)\backslash\mathcal{T}_5$

Figure 3.1: Fundamental domain and reduction graph for the Mumford curve $X_5(2,1;2)$

The group $\Gamma_5(2,1)(2)$ is generated by the transformations represented by the following matrices:

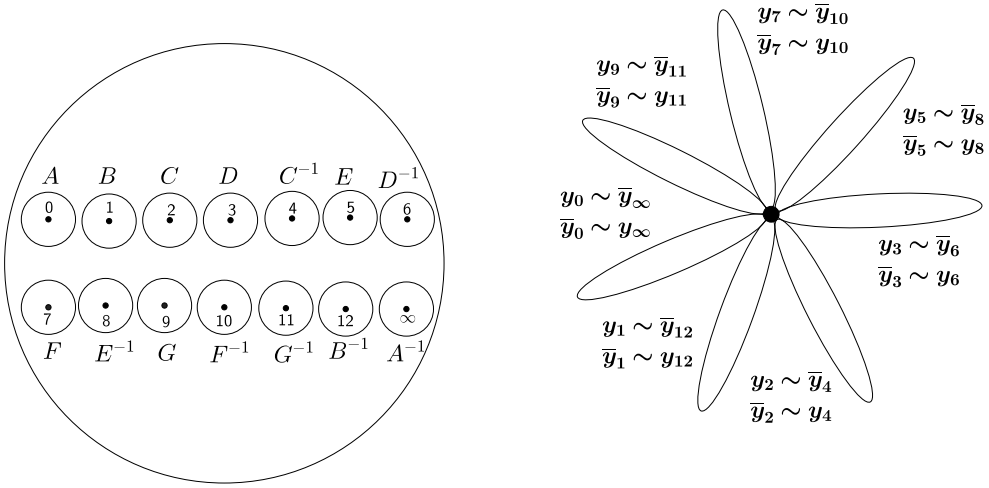
$$\gamma_1 = \begin{pmatrix} -1+2\sqrt{-1} & 0 \\ 0 & -1-2\sqrt{-1} \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 1 & 2\sqrt{-1} \\ 2\sqrt{-1} & 1 \end{pmatrix},$$

$$\gamma_3 = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}.$$

The good fundamental domain $\mathcal{F}_5(2,1;2)$ is represented in Figure 3.1a, and the stable reduction graph of the Mumford curve $X_5(2,1;2)$ is the graph in Figure 3.1b.

(2) $D_B = 2, p = 13$.

The group $\Gamma_{13}(2,1)(2)$ is generated by the transformations represented



(a) $\Gamma_{13}(2,1)(2)\backslash\mathcal{H}_{13}$ (b) $\Gamma_{13}(2,1)(2)\backslash\mathcal{T}_{13}$

Figure 3.2: Fundamental domain and reduction graph of the Mumford curve $X_{13}(2,1;2)$

by the following matrices:

$$\gamma_1 = \begin{pmatrix} -3+2\sqrt{-1} & 0 \\ 0 & -3-2\sqrt{-1} \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 1+2\sqrt{-1} & 2-2\sqrt{-1} \\ -2-2\sqrt{-1} & 1-2\sqrt{-1} \end{pmatrix},$$

$$\gamma_3 = \begin{pmatrix} 1+2\sqrt{-1} & -2-2\sqrt{-1} \\ 2-2\sqrt{-1} & 1-2\sqrt{-1} \end{pmatrix}, \quad \gamma_4 = \begin{pmatrix} -1+2\sqrt{-1} & -2+2\sqrt{-1} \\ 2+2\sqrt{-1} & -1-2\sqrt{-1} \end{pmatrix},$$

$$\gamma_5 = \begin{pmatrix} -1+2\sqrt{-1} & 2+2\sqrt{-1} \\ 2-2\sqrt{-1} & -1-2\sqrt{-1} \end{pmatrix}, \quad \gamma_6 = \begin{pmatrix} 3 & -2\sqrt{-1} \\ -2\sqrt{-1} & 3 \end{pmatrix},$$

$$\gamma_7 = \begin{pmatrix} -3 & -2 \\ 2 & -3 \end{pmatrix}.$$

The good fundamental domain $\mathcal{F}_{13}(2,1;2)$ is represented in Figure 3.2a, and the stable reduction graph of the Mumford curve $X_{13}(2,1;2)$ is the graph in Figure 3.2b.

3.2.4 The case of discriminant $D_H = 3p$

3.2.13 Theorem. *Let B be the definite quaternion algebra over $\mathbb{Q}$ of discriminant $D_B = 3$ and let $\mathcal{O}_B \subseteq B$ be a maximal order over $\mathbb{Z}$. Let $p \in \mathbb{Z}$ be a prime $p \equiv 1 \pmod 4$.*

(*a*) *The group* $\Gamma_p(D_B,1)(2)$ *is a Schottky group of rank* $(p+1)/2$.

(*b*) *A free system of generators for the group* $\Gamma_p(D_B,1)(2)$ *is given by the transformations represented by the following matrices:*

$$\begin{pmatrix} a_0+a_1\sqrt{-1} & a_2+a_3\sqrt{-1} \\ -3(a_2-a_3\sqrt{-1}) & a_0-a_1\sqrt{-1} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p(\sqrt{-1})) = \mathrm{GL}_2(\mathbb{Q}_p)$$

such that

$$a_0,a_1,a_2,a_3 \in \mathbb{Z},$$

$$a_0^2+a_1^2+3a_2^2+3a_3^2 = p, \quad a_0+a_3 \equiv 1 \,(\mathrm{mod}\, 2),\ a_1+a_2 \equiv 0 \,(\mathrm{mod}\, 2).$$

(*c*) *A good fundamental domain for the action of the Schottky group* $\Gamma_p(D_B,1)(2)$ *is the following admissible open subset of* $\mathbb{P}^{1,rig}$:

$$\mathcal{F}_p(D_B,1;2) := \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \bigcup_{a\in\mathbb{P}^1(\mathbb{F}_p)} \mathbb{B}^-(a,1/\sqrt{p}).$$

(*d*) *If we denote by* $X_p(D_B,1;2)$ *the Mumford curve associated to the Schottky group* $\Gamma_p(D_B,1)(2)$*, then its rigidification* $X_p^{rig}(D_B,1;2)$ *is isomorphic to the domain* $\mathcal{F}_p(D_B,1;2)$ *with the following identifications:*

if $\gamma = \begin{pmatrix} a_0+a_1\sqrt{-1} & a_2+a_3\sqrt{-1} \\ -3(a_2-a_3\sqrt{-1}) & a_0-a_1\sqrt{-1} \end{pmatrix}$ *then*

$$\gamma\left(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{B}^-(a_\gamma,1/\sqrt{p})\right) = \mathbb{B}^+(a_{\gamma^{-1}},1/\sqrt{p}),$$

$$\gamma\left(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{B}^+(a_\gamma,1/\sqrt{p})\right) = \mathbb{B}^-(a_{\gamma^{-1}},1/\sqrt{p}),$$

where a_γ *and* $a_{\gamma^{-1}}$ *are defined as the classes in* $\mathbb{P}^1(\mathbb{F}_p)$ *of the p-adic integers* $\dfrac{a_0-a_1\sqrt{-1}}{3(a_2-a_3\sqrt{-1})}$ *and* $\dfrac{a_0+a_1\sqrt{-1}}{-3(a_2-a_3\sqrt{-1})}$ *respectively.*

(*e*) *The stable reduction graph of the Mumford curve* $X_p(D_B,1;2)$ *is is the subtree* $\mathcal{T}_p^{(1)} \smallsetminus \{v_a^0 \mid a \in \mathbb{P}^1(\mathbb{F}_p)\}$ *of* $\mathcal{T}_p$ *with the following identifications of the oriented edges:*

$$\gamma \cdot \left(v^0, v^0_{a_\gamma}\right) = \left(v^0_{a_{\gamma^{-1}}}, v^0\right)$$

for every $\gamma \in \{\gamma_1,\ldots,\gamma_{(p+1)/2}\}$.

PROOF. The proof of point (a) is similar to the one of Theorem 3.2.11, applying Proposition 3.2.10 to the quaternion algebra $B = \left(\frac{-1,-3}{\mathbb{Q}}\right)$ together with the maximal order $\mathcal{O}_B = \langle 1, i, (i+j)/2, (j+k)/2\rangle_{\mathbb{Z}}$ and taking the level $M = 2$. Actually, hypothesis (i) in Proposition 3.2.10 is shown to be satisfied in Example 1.1.2.2 (b) and hypothesis (ii) is fulfilled as a consequence of Corollary 1.1.28 applied to the order $\mathcal{O}_B$. Finally for proving that hypothesis (iii) in Proposition 3.2.10 is also satisfied, let us consider a pure quaternion $\alpha \in \mathcal{O}_B \cap B_0$ of norm p, satisfying $\alpha \equiv 1 \pmod 2$. By Lemma 1.1.30 we know that $\alpha = a_1 i + a_2 j + a_3 k$ with $a_i \in \mathbb{Z}$ such that

$$a_1^2 + 3a_2^2 + 3a_3^2 = p, \quad a_3 \equiv 1 \pmod 2, \quad a_1 + a_2 \equiv 0 \pmod 2.$$

Reducing modulo 4 we find that $p \equiv 3 \pmod 4$ so there is no such quaternion α when $p \equiv 1 \pmod 4$.

Hence we obtain that the group $\Gamma_p(D_B, 1)(2)$ is a Schottky group of rank $r_2(\mathrm{N}_{\mathcal{O}_B,4}, p; \mathbb{Z})/4$.

We know that $r(\mathrm{N}_{B,4}, p; \mathbb{Z}) = 4(p+1)$ for every prime $p \geq 3$ (cf. for example [AALW07, Theorem 1.9] or also [Lio60]), and then a simple calculation shows that

$$r_2(\mathrm{N}_{\mathcal{O}_B,4}, p; \mathbb{Z}) = \frac{1}{2} r(\mathrm{N}_{B,4}, p; \mathbb{Z}) = 2(p+1).$$

Hence $\Gamma_p(D_B, 1)(2)$ is a Schottky group of rank $r_2(\mathrm{N}_{\mathcal{O}_B}, p; \mathbb{Z})/2 = (p+1)/2$.

Note also that point (b) is proved in Lemma 1.1.30 and the proof of (c)-(e) is again an application of Proposition 3.2.8 and a computations of the balls $B^-_{\gamma_i}, B^-_{\gamma_i^{-1}}$, as is done in the proof of Theorem 3.2.11. □

3.2.4.1 Examples for $D_B = 3$

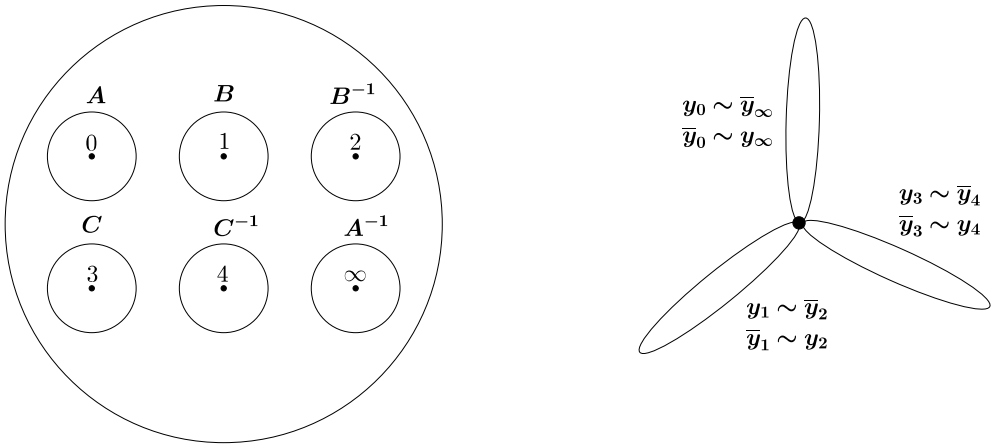
1. $D_B = 3, p = 5$.

   The group $\Gamma_{13}(3,1)(2)$ is generated by

   $$\gamma_1 = \begin{pmatrix} -1+2\sqrt{-1} & 0 \\ 0 & -1-2\sqrt{-1} \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} -1-\sqrt{-1} & 1 \\ -3 & -1+\sqrt{-1} \end{pmatrix},$$

   $$\gamma_3 = \begin{pmatrix} -1+\sqrt{-1} & 1 \\ -3 & -1-\sqrt{-1} \end{pmatrix}.$$

   The good fundamental domain $\mathcal{F}_5(3,1;2)$ and the stable reduction graph of the Mumford curve $X_5(3,1;2)$ are represented in Figures 3.3a and 3.3b, respectively.



(a) $\Gamma_5(3,1)(2)\backslash\mathcal{H}_5$ (b) $\Gamma_5(3,1)(2)\backslash\mathcal{T}_5$

Figure 3.3: Fundamental domain and reduction graph for the Mumford curve $X_5(3,1;2)$

2. $D_B = 3, p = 13$.

   The group $\Gamma_{13}(3,1)(2)$ is generated by the transformation represented by the following matrices:

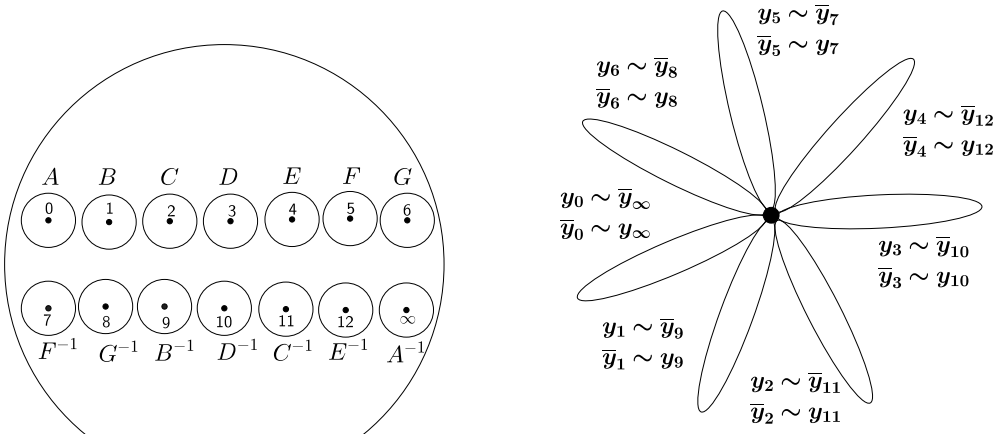
$$\gamma_1 = \begin{pmatrix} 3+2\sqrt{-1} & 0 \\ 0 & 3-2\sqrt{-1} \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 1+3\sqrt{-1} & 1 \\ -3 & 1-3\sqrt{-1} \end{pmatrix},$$

$$\gamma_3 = \begin{pmatrix} 3+\sqrt{-1} & -1 \\ 3 & 3-\sqrt{-1} \end{pmatrix}, \quad \gamma_4 = \begin{pmatrix} -3-\sqrt{-1} & -1 \\ 3 & -3+\sqrt{-1} \end{pmatrix},$$

$$\gamma_5 = \begin{pmatrix} 1 & -2 \\ 6 & 1 \end{pmatrix}, \quad \gamma_6 = \begin{pmatrix} 1-3\sqrt{-1} & 1 \\ -3 & 1+3\sqrt{-1} \end{pmatrix},$$

$$\gamma_7 = \begin{pmatrix} 1 & 2\sqrt{-1} \\ 6\sqrt{-1} & 1 \end{pmatrix}.$$

   The good fundamental domain $\mathcal{F}_{13}(3,1;2)$ is represented in Figure 3.4a, and the stable reduction graph of the Mumford curve $X_{13}(3,1;2)$ is the graph in Figure 3.4b.



(a) $\Gamma_{13}(3,1)(2)\backslash\mathcal{H}_{13}$ (b) $\Gamma_{13}(3,1)(2)\backslash\mathcal{T}_{13}$

Figure 3.4: Fundamental domain and reduction graph of the Mumford curve $X_{13}(3,1;2)$

3.3 Reduction graphs of Shimura curves

In this section we will describe the dual graph of Shimura curves $X(D_H,1)$ where $D_H = 2p$ and $D_H = 3p$, with $p \in \mathbb{Z}$ a prime $p \equiv 1 \pmod 4$. The obtained results intersect with the ones of [Kur79] for the curves in question, and some of the arguments are also the same. Nevertheless we deduce these results from Theorems 3.2.11 and 3.2.13, describing a Mumford curve covering the p-adic Shimura curve.

As we have seen the groups arising in the p-adic uniformization of these curves come from definite quaternion algebras B of discriminant $D_B = 2$ and $D_B = 3$. Moreover these groups are not Schottky groups since they contain elements of finite order. Therefore the reduction graphs of these curves will not be the usual reduction graphs associated to Mumford curves as described in Definition 2.3.16 and Theorem 2.3.20. Actually they will be *graphs with lengths*, where to every edge a weight is associated, taking into account the action of the transformations of finite order.

3.3.1 Graphs with lengths and admissible curves

3.3.1 Definition. Let C be a smooth projective curve over $\mathbb{Q}_p$. A model $\mathcal{C}$ over $\mathbb{Z}_p$ for the curve C is said to be **admissible** if

(i) The scheme $\mathcal{C}$ is proper and flat over $\mathbb{Z}_p$.

(ii) The special fibre $\mathcal{C}_0$ is geometrically reduced and connected.

(iii) All the singular points of $\mathcal{C}_0$ are double points.

(iv) The special fibre $\mathcal{C}_0$ is $\mathbb{F}_p$-split degenerate.

(v) For every double point P, if $\mathcal{O}_{\mathcal{C},P}$ denotes the local ring at P and $\mathcal{O}_{Z^{(m)},z}$ denotes the local ring of the scheme $Z^{(m)}$ defined by

$$Z^{(m)} := \operatorname{Spec}\left(\mathbb{Z}_p^{nr}[x,y]/(xy-p^m)\right),$$

at the double point z of the special fibre $Z_0^{(m)}$, then the formal completions

$$\widehat{\mathcal{O}_{C,P}\otimes_{\mathbb{Z}_p}\mathbb{Z}_p^{nr}}, \text{ and } \widehat{\mathcal{O}_{Z^{(m)},z}}$$

of these local rings are isomorphic over $\mathbb{Z}_p^{nr}$, for some $m \geq 1$.

Compare Definition 3.3.1 with Definition 2.3.15.

Note that if in the definition above $\widehat{\mathcal{O}_{C,P}\otimes_{\mathbb{Z}_p}\mathbb{Z}_p^{nr}} \simeq \widehat{\mathcal{O}_{Z^{(1)},z}}$ for every double point P, then the scheme $\mathcal{C}$ is still not a stable model for the curve C. Actually in this case $\mathcal{C}$ is stable if and only if every irreducible component of $\mathcal{C}_0$, if there are any, meets the remaining components or itself, in at least three points.

3.3.2 Definition. Let $\mathcal{G}$ be a graph with set of vertices $\operatorname{Ver}(\mathcal{G})$ and set of oriented edges $\operatorname{Ed}(\mathcal{G})$ and let Γ be a group acting on the left on $\mathcal{G}$.

(*i*) For every vertex $[v] \in \operatorname{Ver}(\Gamma\backslash\mathcal{G})$ we define **the length of** $[v]$ **(with respect to** Γ**)** as the cardinality of the stabilizer Γ_v of a representative vertex $v \in \operatorname{Ver}(\mathcal{G})$ inside the group Γ. We denote it by $\ell([v])$.

(*ii*) For every edge $[y] \in \operatorname{Ed}(\Gamma\backslash\mathcal{G})$ we define **the length of** $[y]$ **(with respect to** Γ**)** as the cardinality of the stabilizer Γ_y of a representative edge $y \in \operatorname{Ed}(\mathcal{G})$ inside the group Γ. We denote it by $\ell([y])$.

Of course, the definition of length does not depend on the representative chosen for the class of edges or vertices.

The following result is [Kur79, Proposition 3-2].

3.3.3 Proposition. *Let Γ be a discrete cocompact subgroup of $\mathrm{PGL}_2(\mathbb{Q}_p)$, Then the rigid analytic variety $\Gamma\backslash\mathcal{H}_p$ is algebraizable, i.e. there exists an algebraic curve $\mathcal{C}$ over $\mathbb{Q}_p$ such that*

$$\Gamma\backslash\mathcal{H}_p \simeq \mathcal{C}^{rig}.$$

The curve $\mathcal{C}$ is an admissible curve and so its reduction graph $\Gamma\backslash\mathcal{T}_p$ is a graph with lengths.

Now we proceed to state and prove theorems describing the p-adic fundamental domains of the corresponding Shimura curves. We will do so by allowing the elliptic transformations of the quotient group $\Gamma_p(D_B,1)/\Gamma_p(D_B,1)(2)$ to act on the reduction graph $\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p$ described above: the graph obtained is then the reduction graph $\Gamma_p(D_B,1)\backslash\mathcal{T}_p$ which is a cover of degree 2 of the reduction graph $\Gamma_{p,+}(D_B,1)\backslash\mathcal{T}_p$ of the Shimura curve $X(pD_B,1)$.

With these notations we can state and prove the following results first obtained by Kurihara (cf. [Kur79, Sec. 4]).

3.3.4 Proposition. *Let B be a definite quaternion algebra over $\mathbb{Q}$ of discriminant D_B and $p\nmid D_B$ a prime integer. Let $\mathcal{O}_B$ be a maximal order over $\mathbb{Z}$ and let us denote by h_B the ideal class number of this order.*

Then the quotient-graph $\Gamma(D_B,1)\backslash\mathcal{T}_p$ has h_B vertices.

Proof. Since the order $\mathcal{O}_B[1/p]$ over $\mathbb{Z}[1/p]$ satisfies the Eichler's condition (cf. Definition 1.1.6), we can apply Theorem 3.1.7 and we find that the norm map induces a bijection of sets

$$\mathrm{Nm} : B^*\backslash B_{\mathbb{A}}^*/\prod_{\ell\neq p}\mathcal{O}_{B,\ell}^*B_p^*B_\infty^* \simeq \mathbb{Q}_{>0}^*\backslash\mathbb{Q}_{\mathbb{A}}^*/\prod_{\ell\neq p}\mathbb{Z}[1/p]_\ell\mathbb{Q}_p^*\mathbb{Q}_\infty^*.$$

The cardinal of these double quotient spaces is equal on one side to the right ideal class number of the order $\mathcal{O}_B[1/p]$, and on the other side to the strict ideal class number of the order $\mathbb{Z}[1/p]$, and so it is equal to 1, since $\mathbb{Z}[1/p]$ is a principal ideal domain of strict ideal class number 1.

Therefore given a class $[\alpha]\in B^*\backslash B_{\mathbb{A}}^*/\prod_{\ell\neq\infty}\mathcal{O}_{B,\ell}^*B_\infty^*$, we can always suppose that its representative $\alpha\in B_{\mathbb{A}}^*$ is $(1,\dots,1,\alpha_p,1,\dots)$ with $\alpha_p\in B_p^*$ and $\mathrm{Nm}_{B_p/\mathbb{Q}_p}(\alpha_p)\in\mathbb{Z}[1/p]^*$ and the map

$$\begin{array}{ccc} B^*\backslash B_{\mathbb{A}}^*/\prod_{\ell\neq\infty}\mathcal{O}_{B,\ell}^*B_\infty^* & \longrightarrow & \mathcal{O}_B[1/p]^*\backslash B_p^*/\mathbb{Q}_p^*\mathcal{O}_{B,p}^* \\ [(1,\dots,1,\alpha_p,1,\dots)] & \longmapsto & [\alpha_p]. \end{array}$$

is a bijection. Finally we find the following chain of bijections:

$$\mathrm{Ver}(\Gamma_p(D_B,N)\backslash\mathcal{T}_p)\simeq\Gamma(D_B,N)\backslash\mathrm{Ver}(\mathcal{T}_p)\simeq\mathcal{O}_B[1/p]^*\backslash B_p^*/\mathbb{Q}_p^*\mathcal{O}_{B,p}^*\simeq$$
$$\simeq B^*\backslash B_{\mathbb{A}}^*/\prod_{\ell\neq\infty}\mathcal{O}_{B,\ell}^*B_\infty^*$$

and by Theorem 1.2.13, this last set is in bijection with the set of right ideal classes of the maximal order $\mathcal{O}_B$ over $\mathbb{Z}$. □

3.3.5 Lemma. *Let $\mathcal{G}$ be a graph and let Γ be group acting on the left on $\mathcal{G}$. Then $\ell([v])$ is a multiple of $\ell([y])$ for every $[y]\in Star([v])$ and the following formula holds:*

$$\#Star(v)=\sum_{[y]\in Star([v])}\frac{\ell([v])}{\ell([y])}.$$

Proof. There is a natural surjective map

$$\pi_\Gamma : y\in Star(v)\longmapsto[y]:=\Gamma y\in\Gamma\backslash Star(v)=Star([v]).$$

Therefore

$$\#Star(v)=\coprod_{[y]\in Star([v])}\#\pi_\Gamma^{-1}([y])$$

and by the orbit-stabilizer theorem we obtain that $\#\pi_\Gamma^{-1}([y])=\#[y]=[\Gamma:\Gamma_y]$. □

3.3.6 Remark. By Theorem 3.3.4 we know that the number of vertexes of the quotient graph $\Gamma_p(D_B,1)\backslash\mathcal{T}_p$ is equal to 1 in the cases we are considering. So this unique vertex, which we can choose to have as a representative the *principal vertex* v^0, is necessarily fixed by all classes of transformations in the quotient group $\Gamma_p(D_B,N)/\Gamma_p(D_B,N)(2)$. Moreover the same can also be deduced by Theorems 3.2.11 and 3.2.13, since we have seen that the reduction graph of the Mumford curve $X_p(D_B,1;2)$ always has one vertex.

So now we have to understand the action of the elements of finite order on the $p+1$ oriented edges of the covering graph $\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p$. In order to do so, we are going to describe theoretically how this action works.

If we identify the vertex $v_0\in\mathrm{Ver}(\mathcal{T}_p)$ with the projective line $\mathbb{P}^1_{\mathbb{F}_p}$ and we denote by $Star(v_0)$ the set of oriented edges $y\in\mathrm{Ed}(\mathcal{T}_p)$ with origin in $[v_0]$, then we find that this identification restricts to the following bijection:

$$\delta : Star(v_0)\simeq\mathbb{P}^1_{\mathbb{F}_p}(\mathbb{F}_p)=\mathbb{F}_p\cup\{\infty\}.$$

Now, on one side, we know that $\mathrm{PGL}_2(\mathbb{Z}_p)$ acts on $Star(v_0)$ in the usual way (since the group $\mathrm{PGL}_2(\mathbb{Z}_p)$ is the stabilizer of the vertex v_0 for the action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on $\mathrm{Ver}(\mathcal{T}_p)$); thus there is a natural action of $\mathrm{PGL}_2(\mathbb{Z}_p)$ on the set of points $\mathbb{P}^1_{\mathbb{F}_p}(\mathbb{F}_p)$, which is equivariant with respect to the previous bijection.

On the other side, $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}_p}(\mathbb{F}_p)) \simeq \mathrm{PGL}_2(\mathbb{F}_p)$ so the action of $\mathrm{PGL}_2(\mathbb{Z}_p)$ on $\mathbb{P}^1_{\mathbb{F}_p}(\mathbb{F}_p)$ is the one induced by the reduction map

$$\pi : \mathrm{PGL}_2(\mathbb{Z}_p) \longrightarrow \mathrm{PGL}_2(\mathbb{Z}_p/p\mathbb{Z}_p) \simeq \mathrm{PGL}_2(\mathbb{F}_p).$$

More specifically, for every $\gamma \in \mathrm{PGL}_2(\mathbb{Z}_p)$ and every $y \in Star(v_0)$,

$$\gamma \cdot y = \pi(\gamma) \cdot \delta(y).$$

3.3.2 The case $D_H = 2p$

3.3.7 Lemma. *Let $B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ be the definite quaternion algebra over $\mathbb{Q}$ of discriminant $D_B = 2$ and let $\mathcal{O}_B$ be the maximal order over $\mathbb{Z}$ with basis $\{1, i, j, \frac{1 \pm i \pm j \pm k}{2}\}$. Let p be a prime integer $p \equiv 1 \pmod 4$ and let Φ_p be the following p-adic matricial immersion:*

$$\begin{array}{ccccc} \Phi_p : & B & \longrightarrow & \mathrm{M}_2(\mathbb{Q}_p(\sqrt{-1})) = \mathrm{M}_2(\mathbb{Q}_p) \\ & x_0 + x_1 i + x_2 j + x_3 k & \longmapsto & \begin{pmatrix} x_0 + x_1\sqrt{-1} & x_2 + x_3\sqrt{-1} \\ -(x_2 - x_3\sqrt{-1}) & x_0 - x_1\sqrt{-1} \end{pmatrix}. \end{array}$$

Then the quotient group $\Gamma_p(D_B, 1)/\Gamma_p(D_B, 1)(2)$ is isomorphic to the unit group $\mathcal{O}_B^*/\mathbb{Z}^*$ of order 12.

(a) The order 2 transformations are represented by the matrices

$$\Phi_p(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \Phi_p(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \Phi_p(k) = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

(b) The order 3 transformations are represented by the matrices

$$\Phi_p\left(\frac{1 \pm i + j + k}{2}\right) = \begin{pmatrix} \frac{1}{2} \pm \frac{1}{2}\sqrt{-1} & \frac{1}{2} + \frac{1}{2}\sqrt{-1} \\ -\frac{1}{2} + \frac{1}{2}\sqrt{-1} & \frac{1}{2} \mp \frac{1}{2}\sqrt{-1} \end{pmatrix},$$

$$\Phi_p\left(\frac{1 + i \pm j + k}{2}\right) = \begin{pmatrix} \frac{1}{2} + \frac{1}{2}\sqrt{-1} & \pm\frac{1}{2} + \frac{1}{2}\sqrt{-1} \\ \mp\frac{1}{2} + \frac{1}{2}\sqrt{-1} & \frac{1}{2} - \frac{1}{2}\sqrt{-1} \end{pmatrix},$$

$$\Phi_p\left(\frac{1 + i + j \pm k}{2}\right) = \begin{pmatrix} \frac{1}{2} + \frac{1}{2}\sqrt{-1} & \frac{1}{2} \pm \frac{1}{2}\sqrt{-1} \\ -\frac{1}{2} \mp \frac{1}{2}\sqrt{-1} & \frac{1}{2} - \frac{1}{2}\sqrt{-1} \end{pmatrix}.$$

(*c*) *The order* 2 *transformations represented by* $\Phi_p(i), \Phi_p(j), \Phi_p(k)$ *have fixed points* $\{0,\infty\}, \{\sqrt{-1}, -\sqrt{-1}\}, \{1,-1\}$*, respectively.*

(*d*) *Every order* 3 *transformation has* $1+\left(\frac{3}{p}\right)$ *fixed points in* $\mathbb{P}^1(\mathbb{F}_p)$*.*

(*e*) *There is no transformation of order* 3 *fixing a point which is a fixed point of some transformation of order* 2*.*

Proof. From what we have seen in Example 1.1.2.1 and in the proof of Theorem 3.2.13 we know that there are isomorphisms of non-abelian groups

$$\Gamma_p(D_B,1)/\Gamma_p(D_B,1)(2) \simeq (\mathcal{O}_B/2\mathcal{O}_B)^* \simeq \mathcal{O}_B^*/\mathbb{Z}^* = \{1,i,j,k,\frac{1\pm i\pm j\pm k}{2}\}.$$

This group is isomorphic to the abstract group of permutations A_4, having only elements of order 2 and 3, apart from the identity. A simple calculation yields the expressions of points (*a*) and (*b*).

In order to prove points (*c*) and (*d*) we have to compute the fixed points of these 11 transformations. This can be done by computing the zeroes of the associated binary quadratic forms.

The discriminant of the characteristic polynomial of an element γ of order 3 is always

$$\mathrm{disc}(P_\gamma) = \mathrm{tr}^2(\gamma) - 4\det(\gamma) = 1^2 - 4 = -3.$$

Hence, since $\sqrt{-3} \in \mathbb{Q}_p$ if and only if $\left(\frac{3}{p}\right) = 1$ (recall that we are assuming $p \equiv 1 \pmod 4$), the transformation γ has two or no fixed points in $\mathbb{P}^1(\mathbb{F}_p)$ depending on whether 3 is a square or not mod p. Point (*b*) is then proved.

It is a simple calculation to prove that none of the points $0, \infty, \pm 1, \pm\sqrt{-1} \in \mathbb{P}^1(\mathbb{Q}_p)$ is fixed by the transformations of order 3 described above. □

3.3.8 Theorem. *Let* B *be the definite quaternion algebra of discriminant* $D_B = 2$ *and* $\mathcal{O}_B$ *be a maximal order in* B*. Let* p *be a prime integer such that* $p \equiv 1 \pmod 4$*,* $p \nmid D_B$*.*

For every integer $n \geq 1$*, let us denote by*

$$c_n := \#\{y \in \mathrm{Ed}(\Gamma_p(D_B,1)\backslash\mathcal{T}_p) \mid \ell(y) = n\}$$

the number of oriented edges with length n*. Then the quotient graph with lengths* $\Gamma_p(D_B,1)\backslash\mathcal{T}_p$ *is described by the following properties:*

(*a*) $\mathrm{Ver}(\Gamma_p(D_B,1)\backslash\mathcal{T}_p) = \{[v^0]\}$ *such that* $\ell([v^0]) = 12$*.*

(*b*) *There is only one oriented edge* $y \in \mathrm{Ed}(\Gamma_p(D_B,1)\backslash\mathcal{T}_p)$ *of length* $\ell(y)=2$ *and is represented by each of the oriented edges*

$$y_0,\, y_\infty,\, y_1,\, y_{-1},\, y_{\sqrt{-1}}, y_{\sqrt{-1}} \in \mathcal{F}_p(D_B,1;2),$$

where $y_a := (v^0, v^0_a)$ *for every* $a \in \mathbb{P}^1(\mathbb{F}_p)$.

(*c*) *If* $p \equiv 1 \pmod 3$, *then* $c_1 = (p-13)/12, c_2 = 1, c_3 = 2$ *and* $c_n = 0$ *for every* $n \geq 4$.

In this case the edges $y', y'' \in \mathrm{Ed}(\Gamma_p(D_B,1)\backslash\mathcal{T}_p)$ *of length* 3 *are such that* $y'' = \overline{y'}$ *and* y' *is represented by each of the edges* $y_a := (v^0, v^0_a) \in \mathcal{F}_p(D_B,1;2)$ *such that* $a \in \mathbb{P}^1(\mathbb{F}_p)$ *is a fixed point of one of the order* 3 *transformations of* $\Gamma_p(D_B,1)/\Gamma_p(D_B,1)(2)$.

(*d*) *If* $p \equiv 2 \pmod 3$ *then* $c_1 = (p-5)/12, c_2 = 1$ *and* $c_n = 0$ *for every* $n \geq 3$.

Proof. Since the 12 classes of transformations in $\Gamma_p(D_B,1)/\Gamma_p(D_B,1)(2)$ are actually represented by transformations in $\mathrm{PGL}_2(\mathbb{Z}_p)$, we know that they have to fix the vertex $[v^0] \in \mathrm{Ver}(\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p)$, which is the unique vertex of the quotient graph $\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p$, after Theorem 3.2.11. Hence we have proved that

$$\mathrm{Ver}(\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p) = \{[v^0]\}, \text{ and } \ell([v^0]) = \#(\mathcal{O}_B^*/\mathbb{Z}^*) = 12.$$

Let us apply Lemma 3.3.5 to the graph $\mathcal{G} := \Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p$, the group $\Gamma := \Gamma_p(D_B,1)/\Gamma_p(D_B,1)(2)$, acting on it, and the vertex $v := v^0$.

We find that for every $y \in Star([v^0]) = \mathrm{Ed}(\Gamma_p(D_B,1)/\mathcal{T}_p)$, it has to be $\ell(y) = 1,2,3,4,6,12$. From Lemma 3.3.7 (*c*) and (*e*) we deduce respectively that $\ell(y)$ cannot be either 4, or 6 or 12. In particular the formula of Lemma 3.3.5 gives:

$$\frac{p+1}{2} = 6c_1 + 3c_2 + 2c_3.$$

From the expressions of the order 3 transformations of the quotient group $\Gamma_p(D_B,1)/\Gamma_p(D_B,1)(2)$, given in Lemma 3.3.7 (*b*), we can easily see that the three unoriented edges of $\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p$, corresponding to the points $\{1 \sim -1, 0 \sim \infty, \mathrm{Red}(\sqrt{-1}) \sim -\mathrm{Red}(-\sqrt{-1})\}$, are always identified by the action of these transformations on the quotient graph $\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p$. Hence these three unoriented edges of $\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p$ gives rise to one unoriented edge, say $y \in \mathrm{Ed}^*(\Gamma_p(D_B,1)\backslash\mathcal{T}_p)$, which corresponds to the $\mathbb{F}_p$-rational point

$$\{1 \sim -1 \sim 0 \sim \infty \sim \mathrm{Red}(\sqrt{-1}) \sim \mathrm{Red}(-\sqrt{-1})\},$$

of the special fibre of the corresponding Mumford $X_p(D_2, 1; 2)$ curve described in Theorem 3.2.11. This edge has length $\ell(y) = 2$, by Lemma 3.3.7 (c).

We now have two options for c_2, namely $c_2 = 1$ if the edge y is such that $\overline{y} = y$ and $c_2 = 2$ if not. From an explicit computation we deduce that $c_2 = 1$.

Finally by Lemma 3.3.7 (d) we obtain that:

(1) If $p \equiv 1 \pmod 3$, then $c_3 = 2$ and so $c_1 = (p - 13)/12$.

(2) If $p \equiv 2 \pmod 3$, then $c_3 = 0$ and so $c_1 = (p - 5)/12$.

The proof is then concluded. □

3.3.3 The case $D_H = 3p$

By computing explicitly the fixed points for the finite order transformations of the quotient group $\Gamma_p(D_B, 1)/\Gamma_p(D_B, 1)(2)$, we find the following result which is the analogous of Lemma 3.3.9

3.3.9 Lemma. *Let $B = \left(\frac{-1,-3}{\mathbb{Q}}\right)$ be the definite quaternion algebra over $\mathbb{Q}$ of discriminant $D_B = 3$ and let $\mathcal{O}_B \subseteq B$ be the maximal order over $\mathbb{Z}$ with basis $\{1, i, \frac{i+j}{2}, \frac{1+k}{2}\}$. Let p be a prime integer $p \equiv 1 \pmod 4$ and let Φ_p be the following p-adic matricial immersion:*

$$\begin{array}{rccc} \Phi_p : & B & \longrightarrow & \mathrm{M}_2(\mathbb{Q}_p(\sqrt{-1})) = \mathrm{M}_2(\mathbb{Q}_p) \\ & x_0 + x_1 i + x_2 j + x_3 k & \longmapsto & \begin{pmatrix} x_0 + x_1\sqrt{-1} & x_2 + x_3\sqrt{-1} \\ -3(x_2 - x_3\sqrt{-1}) & x_0 - x_1\sqrt{-1} \end{pmatrix}. \end{array}$$

Then the group $\Gamma_p(D_B, 1)/\Gamma_p(D_B, 1)(2)$ is isomorphic to the abelian group $\mathcal{O}_B^*/\mathbb{Z}^*$ of order 6.

(a) *The order 2 transformations are represented by the following matrices:*

$$\Phi_p(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \Phi_p\left(\frac{i \pm j}{2}\right) = \begin{pmatrix} \frac{1}{2}\sqrt{-1} & \pm\frac{1}{2} \\ \mp\frac{3}{2} & -\frac{1}{2}\sqrt{-1} \end{pmatrix}$$

(b) *The order 3 transformations are represented by the following matrices:*

$$\Phi_p\left(\frac{1 \pm k}{2}\right) = \begin{pmatrix} \frac{1}{2} & \pm\frac{1}{2}\sqrt{-1} \\ \pm\frac{3}{2}\sqrt{-1} & \frac{1}{2} \end{pmatrix}$$

(c) *The order* 2 *transformations* $\Phi_p(i), \Phi_p((i+j)/2), \Phi_p((i-j)/2)$ *have fixed points* $\{0,\infty\}, \{-\sqrt{-1}, \sqrt{-1}/3\}, \{\sqrt{-1}, -\sqrt{-1}/3\}$, *respectively.*

(d) *Each order* 3 *transformation has* $1 + \left(\frac{3}{p}\right)$ *fixed points in* $\mathbb{P}^1(\mathbb{F}_p)$.

(e) *There is no order* 3 *transformation fixing a point which is fixed by a transformation of order* 2. □

3.3.10 Theorem. *Let* B *be the definite quaternion algebra of discriminant* $D_B = 3$ *and* $\mathcal{O}_B$ *be a maximal order in* B. *Let* p *be a prime integer such that* $p \equiv 1 \pmod 4$, $p \nmid D_B$.

For every integer $n \geq 1$, *let us denote by*

$$c_n := \#\{y \in \mathrm{Ed}(\Gamma_p(D_B, 1)\backslash\mathcal{T}_p) \mid \ell(y) = n\}$$

the number of oriented edges with length n. *Then the quotient graph with lengths* $\Gamma_p(D_B,1)\backslash\mathcal{T}_p$ *is described by the following properties:*

(a) $\mathrm{Ver}(\Gamma_p(D_B,1)\backslash\mathcal{T}_p) = \{[v^0]\}$ *such that* $\ell([v^0]) = 6$.

(b) *There are exactly two oriented edges of length* 2, *namely*

$$y, \overline{y} \in \mathrm{Ed}(\Gamma_p(D_B,1)\backslash\mathcal{T}_p), \text{ with } y \neq \overline{y},$$

and such that y *is represented by any of the oriented edges*

$$y_0,\ y_{-\sqrt{-1}},\ y_{\sqrt{-1}} \in \mathcal{F}_p(D_B, 1; 2),$$

and $\overline{y}$ *is represented by any of the oriented edges*

$$y_\infty,\ y_{\sqrt{-1}/3},\ y_{-\sqrt{-1}/3} \in \mathcal{F}_p(D_B, 1; 2).$$

(c) *If* $p \equiv 1 \pmod 3$, *then* $c_1 = (p-5)/6, c_2 = 2, c_3 = 1$ *and* $c_n = 0$ *for every* $n \geq 4$.

In this case the edge $y' \in \mathrm{Ed}(\Gamma_p(D_B,1)\backslash\mathcal{T}_p)$ *of length* 3 *is such that* $\overline{y'} = y'$ *and is represented by any of the edges*

$$y_{\sqrt{3}/3}, y_{-\sqrt{3}/3} \in \mathcal{F}_p(D_B, 1; 2).$$

(d) *If* $p \equiv 2 \pmod 3$ *then* $c_1 = (p-7)/6, c_2 = 2$ *and* $c_n = 0$ *for every* $n \geq 3$.

PROOF. Since the six classes of transformations in $\Gamma_p(D_B,1)/\Gamma_p(D_B,1)(2)$ are represented by matrices in $\mathrm{PGL}_2(\mathbb{Z}_p)$ (cf. Lemma 3.3.7), we know that they have to fix the vertex $[v^0] \in \mathrm{Ver}(\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p)$, which is the unique vertex of the quotient graph $\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p$, as has been shown in 3.2.11. Hence we have

$$\mathrm{Ver}(\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p) = \{[v^0]\},$$

$$\ell([v^0]) = (\Gamma_p(D_B,1) : \Gamma_p(D_B,1)(2)) = \#(\mathcal{O}_B/\mathbb{Z}^*) = 6.$$

Applying the formula in Lemma 3.3.5 to the graph $\mathcal{G} = \Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p$, the group $\Gamma = \Gamma_p(D_B,1)/\Gamma_p(D_B,1)(2)$ and the vertex $v = v^0$, we find that for an edge $y \in \mathit{Star}([v^0]) = \mathrm{Ed}(\Gamma_p(D_B,1)/\mathcal{T}_p)$, the possible lengths are $\ell(y) = 1, 2, 3, 4$ or 6. By Lemma 3.3.7 (c) and (e) we deduce that $\ell(y)$ can never be 4 or 6.

Therefore the formula in Lemma 3.3.5 gives:

$$\frac{p+1}{2} = 3c_2 + 2c_3 + 6c_1.$$

From the expressions of the order 3 transformations given in Lemma 3.3.9 (b) we easily see that the three edges corresponding to the points

$$\{0 \sim \infty, \mathrm{Red}(-\sqrt{-1}) \sim \mathrm{Red}(\sqrt{-1}/3), \mathrm{Red}(\sqrt{-1}) \sim \mathrm{Red}(-\sqrt{-1}/3)\}$$

are always identified by the action of these transformation classes on the quotient graph $\Gamma_p(D_B,1)(2)\backslash\mathcal{T}_p$. This gives rise to an edge $y \in \mathrm{Ed}(\Gamma_p(D_B,1)\backslash\mathcal{T}_p)$ represented by any of the three edges as in the statement of (b).

Again, it can be that $\overline{y} = y$, in which case we have $c_2 = 1$, or $\overline{y} \neq y$, in which case $c_2 = 2$. From explicit computations, we deduce that in this case $c_2 = 2$.

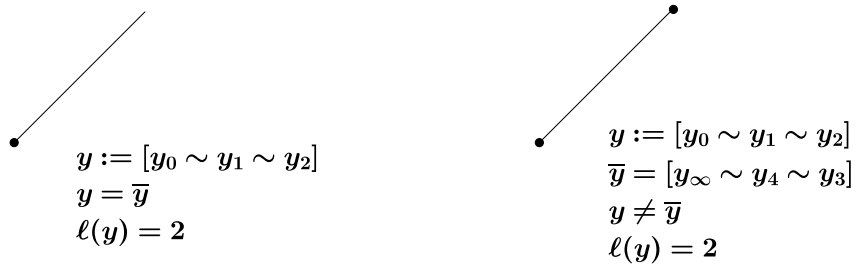
Finally, by Lemma 3.3.9 (d), we obtain that:

(1) If $p \equiv 1 \pmod 3$, then $c_3 = 1$ and so $c_1 = (p-5)/6$.

(2) If $p \equiv 2 \pmod 3$, then $c_3 = 0$ and so $c_1 = (p-7)/6$.

Actually when $\left(\frac{3}{p}\right) = 1$, the order 3 transformations have the same fixed points $\pm\sqrt{3}/3 \in \mathbb{Q}_p$ corresponding to the edge $y_{\sqrt{3}/3} \sim \overline{y}_{-\sqrt{3}/3}$ of the quotient graph $\Gamma_p(D_B,1)(2)/\mathcal{T}_p$. □

In a series of examples, we are going to draw the reduction graphs of the Drinfeld integral model over $\mathbb{Z}_p$ of Shimura curves $X(D_H,1)$.



(a) $\Gamma_5(2,1)\backslash\mathcal{T}_5$ (b) $\Gamma_{5,+}(2,1)\backslash\mathcal{T}_5$

Figure 3.5: Reduction graph of the Shimura curve $\mathcal{X}_5(10,1)$

3.3.3.1 Reduction graphs for Shimura curves $X(2p,1)$

Let H be the indefinite quaternion algebra of discriminant $D_H = 2p$, with $p \equiv 1 \pmod 4$, and let $\mathcal{O}_H \subseteq H$ be a maximal order over $\mathbb{Z}$. Let $X(D_H,1)$ be the Shimura curve associated to the quaternion algebra H and the maximal order $\mathcal{O}_H$ and $\mathcal{X}_p(2p,1)$ be its Drinfeld integral model over $\mathbb{Z}_p$.

Let us take $p = 5$. In Figure 3.5a we find the graph with lengths $\Gamma_5(2,1)\backslash\mathcal{T}_5$, which is obtained as the quotient of the graph in Figure 3.1b by the order 12 group of units $\mathcal{O}_B^*/\mathbb{Z}^*$.

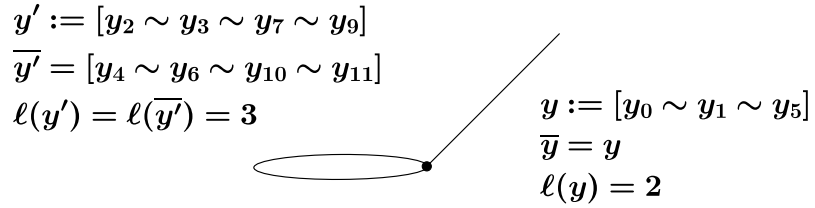
After that we can also show the reduction graph at 5 of the Shimura curve $\mathcal{X}(10,1)$ as the quotient of the graph in Figure 3.5a by the order 2 group $\Gamma_5(2,1)/\Gamma_{5,+}(2,1)$.

We show also the case of the Shimura curve $\mathcal{X}_p(26,1)$ taking the prime $p = 13$, as can be seen in Figure 3.6.

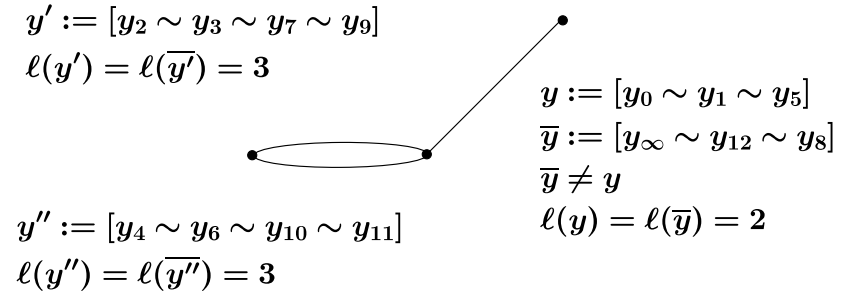
3.3.3.2 Reduction graphs for Shimura curves $X(3p,1)$

Let H be the indefinite quaternion algebra of discriminant $D_H = 3p$ with $p \equiv 1 \pmod 4$ and let $\mathcal{O}_H$ be a maximal order over $\mathbb{Z}$. Let $X(D_H,1)$ be the Shimura curve associated to the quaternion algebra H and the maximal order $\mathcal{O}_H$ and $\mathcal{X}_p(3p,1)$ be its Drinfeld integral model over $\mathbb{Z}_p$.

In Figures 3.7 and 3.8 we exhibit the reduction graphs of the Shimura curves $\mathcal{X}_p(3p,1)$ at the primes $p = 5$ and $p = 13$, respectively. These figures have to be compared with the covering graphs of Figures 3.3 and 3.4.

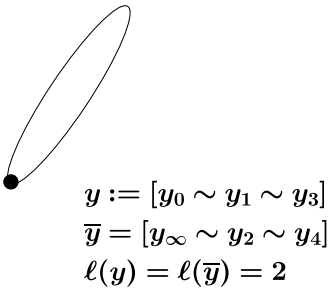


(a) $\Gamma_{13}(2,1)\backslash\mathcal{T}_{13}$

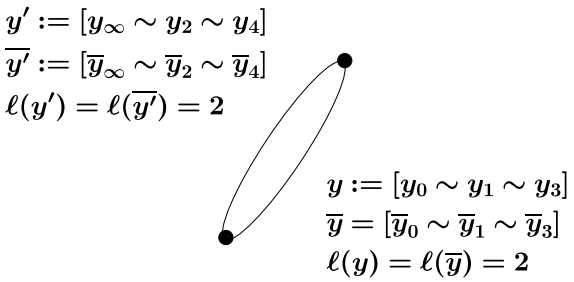


(b) $\Gamma_{13,+}(2,1)\backslash\mathcal{T}_{13}$

Figure 3.6: Reduction graph of the Shimura curve $\mathcal{X}_{13}(26,1)$

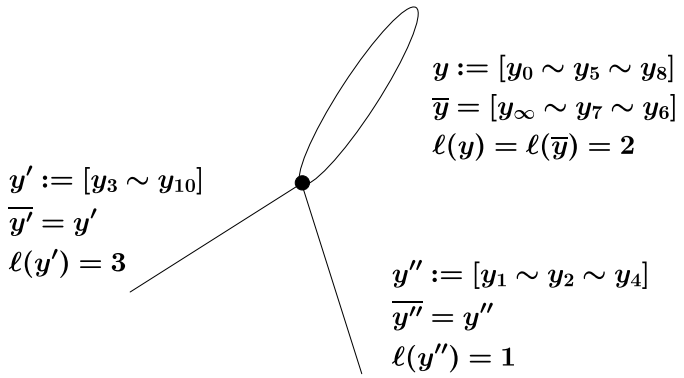


(a) $\Gamma_5(3,1)\backslash\mathcal{T}_5$

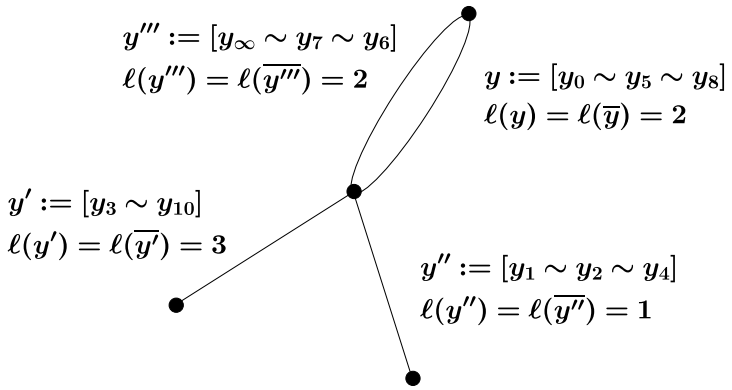


(b) $\Gamma_{5,+}(3,1)\backslash\mathcal{T}_5$

Figure 3.7: Reduction graph of the Shimura curve $\mathcal{X}_5(15,1)$



(a) $\Gamma_{13}(3,1)\backslash\mathcal{T}_{13}$



(b) $\Gamma_{13,+}(3,1)\backslash\mathcal{T}_{13}$

Figure 3.8: Reduction graph of the Shimura curve $\mathcal{X}_{13}(39,1)$

Chapter 4

Singular moduli of p-adic Shimura curves

Before introducing the chapter, we want to fix some basic notations which could be considered "the key of lecture" of the whole chapter. These are the following. When ℓ is a fixed finite prime of $\mathbb{Q}$, we will usually denote by $\mathbb{Q}_{\ell^2}$ the quadratic unramified extension of $\mathbb{Q}_\ell$, which is unique inside a fixed algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$. When $\ell = \infty$ is the Archimedean prime of $\mathbb{Q}$, we use then the following notations: $\mathbb{Q}_\infty = \mathbb{R}$ and $\mathbb{Q}_{\infty^2} := \mathbb{C}$, according to the convention for which $\mathbb{C}$ is the quadratic unramified extension of $\mathbb{R}$ (cf. [Neu99, Ch. III]).

The theory of complex multiplication for $\mathbb{Q}$ provides a concrete way to generate ring class field extensions of imaginary quadratic fields K over $\mathbb{Q}$. These extensions are obtained adjoining to K "special values", known as *singular moduli*, of automorphic functions uniformizing Shimura curves (cf. Theorem 1.2.3 for the correct statement in the general case of Shimura curves and [Sil94, Theorem 5.6] for the statement in the case of classical modular curves). Therefore, it seems of some interest to understand the *nature* of these special algebraic points, with respect to the uniformization of the curve: by this we mean that if (X, J_Γ) is the canonical model over $\mathbb{Q}$ of the Shimura curve X, together with its complex uniformization

$$j_\Gamma : \Gamma\backslash\mathcal{H} \simeq X(\mathbb{C}),$$

and $\tau \in \Gamma\backslash\mathcal{H}$ is a parameter such that $j_\Gamma(\tau)$ is the special value in question, i.e. $K(j_\Gamma(\tau))$ is a certain ring class field of the imaginary quadratic field K, then we wish to understand how to obtain the parameter τ, which is what we call a **complex multiplication parameter by the field** K.

On the one hand, this parameter $\tau \in \mathcal{H}$ has a geometric interpretation,

coming from the fundamental property of the curve X to be a coarse moduli space of abelian varieties with some additional structure (as explained in detail in Chapter 1.3). This modular interpretation is actually the key to understand the theory of complex multiplication and the proofs of its statements.

On the other hand, complex multiplication parameters also arise as zeros of certain integral binary quadratic forms. These quadratic forms have rational integral coefficients when we are looking for complex multiplication parameters arising from Shimura curves of discriminant 1 (i.e. classical modular curves): this is the well-known theory of binary quadratic forms started in Gauß' *Disquisitiones Arithmetiquae*, (cf. [Gau96]). And they have integral quadratic coefficients when classical modular curves are replaced by Shimura curves of discriminant $D > 1$: this is a more general theory of binary quadratic forms developed in [AB04].

All these theories of binary quadratic forms are associated to the complex (and therefore Archimedean) uniformization of Shimura curves, so we want to point out that it seems quite natural to investigate the analogous situation for the non-Archimedean uniformization, in the cases when it is available. Thanks to the Cerednik-Drinfeld theory introduced in Section 3.1 we have a description of the p-adic points of a Shimura curve X over $\mathbb{Q}$. More specifically, we have seen in Corollary 3.1.16 that we have a bijection on the set of $\mathbb{Q}_{p^2}$-points of the Shimura curve X which is the following:

$$\Gamma_{p,+}\backslash\mathcal{H}_p(\mathbb{Q}_{p^2}) \simeq X(\mathbb{Q}_{p^2}).$$

Here $\mathcal{H}_p := \mathbb{P}^{1,rig}_{\mathbb{Q}_p} \smallsetminus \mathbb{P}^1_{\mathbb{Q}_p}(\mathbb{Q}_p)$ denotes, as usual, the p-adic upper half-plane introduced in Section 2.2 and the group $\Gamma_{p,+}$ can be explicitly constructed from the quaternion algebra defining the Shimura curve X, as detailed in Section 3.1.

We want to investigate which is the best theory of p-adic multiplication parameters associated to this uniformization, where the Archimedean field $\mathbb{C}$ is replaced by the quadratic unramified extension $\mathbb{Q}_{p^2}$.

4.1 Embeddings of p-imaginary quadratic fields in definite quaternion algebras

4.1.1 Number of embeddings

4.1.1 Definition. Let ℓ be a (finite or Archimedean) prime of $\mathbb{Q}$. We say that a quadratic field $K/\mathbb{Q}$ is **imaginary at the prime** ℓ (also **ℓ-imaginary**)

if $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \mathbb{Q}_{\ell^2}$.

In particular, a quadratic field K is imaginary at the prime ∞ if and only if it is imaginary in the usual sense. Otherwise, if ℓ is a finite prime then a quadratic field K is imaginary at the prime ℓ if and only if $K = \mathbb{Q}(\sqrt{d})$, for a square-free integer d coprime with ℓ and such that $\left(\frac{d}{\ell}\right) = -1$, i.e. if and only if the prime ℓ is inert in K.

Let B be a definite quaternion $\mathbb{Q}$-algebra of discriminant D_B and let $p \in \mathbb{Z}$ be a prime not dividing D_B. Let us fix an isomorphism $\Phi_p : B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ of $\mathbb{Q}_p$-algebras and let us also denote by Φ_p the corresponding matricial immersion $B \hookrightarrow \mathrm{M}_2(\mathbb{Q}_p)$.

If K is a p-imaginary quadratic field such that there exists an immersion $\varphi : K \hookrightarrow B$ of $\mathbb{Q}$-algebras, then we can consider the corresponding matricial immersion $\Phi_p \circ \varphi : K \hookrightarrow \mathrm{M}_2(\mathbb{Q}_p)$ and the following set of transformations:

$$\{\Phi_p(\varphi(a)) \in \mathrm{GL}_2(\mathbb{Q}_p) \mid a \in K^*\}.$$

We are now going to prove, in Proposition 4.1.3, the p-adic version of [Shi67, Proposition 2.6]. We first need the following easy lemma.

4.1.2 Lemma. *Let $\gamma, \gamma' \in \mathrm{GL}_2(\mathbb{Q}_p)$. Then γ, γ' have the same fixed points if and only if there exist $\lambda, \mu \in \mathbb{Q}_p$, $\lambda \neq 0$, such that $\gamma' = \lambda \mathrm{I}_2 + \mu\gamma$.*

Proof. The proof goes exactly as in [AB04, 6.1], after replacing $\mathbb{R}$ by $\mathbb{Q}_p$. □

4.1.3 Proposition. *Let K be a quadratic field imaginary at the prime p and let $\varphi : K \hookrightarrow B$ be an immersion of $\mathbb{Q}$-algebras. Then for every $a \in K^*$ all the transformations $\Phi_p(\varphi(a)) \in \mathrm{GL}_2(\mathbb{Q}_p)$ are elliptic and they have two fixed points in $\mathcal{H}_p(\mathbb{Q}_{p^2}) = \mathbb{Q}_{p^2} \smallsetminus \mathbb{Q}_p$ not depending on a.*

Proof. Let us write $a = x + y\sqrt{d} \in K^*$. Then $\Phi_p(\varphi(a)) = x\mathrm{I}_2 + y\gamma \in \mathrm{GL}_2(\mathbb{Q}_p)$, where $\gamma := \Phi_p(\varphi(\sqrt{d}))$ is a transformation such that $\gamma^2 = d\mathrm{I}_2$. Hence, by Lemma 4.1.2 it is clear that all the transformations $\Phi_p(\varphi(a))$ have the same fixed points as γ. Now it is easy to see that the discriminant of the characteristic polynomial of $\Phi_p(\varphi(\sqrt{d}))$ is

$$\mathrm{tr}^2(\gamma) - 4\mathrm{det}(\gamma) = 4d \notin \mathbb{Q}_p^{*2}$$

since $\left(\frac{d}{p}\right) = -1$. Finally, by Proposition 2.3.5, the transformation γ is elliptic and its fixed points z_1, z_2 are in $\mathbb{Q}_{p^2} \smallsetminus \mathbb{Q}_p = \mathcal{H}_p(\mathbb{Q}_{p^2})$. Actually, $z_1, z_2 \in \mathbb{Q}_p(\sqrt{d}) \simeq \mathbb{Q}_{p^2}$. □

The reciprocal is also true and it is the following:

4.1.4 Proposition. *If $\alpha \in B, \alpha \notin \mathbb{Q}$, is such that the associated transformation $\Phi_p(\alpha) \in \mathrm{GL}_2(\mathbb{Q}_p)$ has two fixed points $z_1, z_2 \in \mathcal{H}_p(\mathbb{Q}_{p^2})$, then $\mathbb{Q}(\alpha)$ is a quadratic extension of $\mathbb{Q}$, imaginary at the prime p, admitting an embedding in B.*

Proof. For every quaternion $\alpha \in B$ not in $\mathbb{Q}$, the extension $\mathbb{Q}(\alpha)$ is a quadratic subfield of the algebra B, since α satisfies the quadratic equation $X^2 - \mathrm{Tr}_{B/\mathbb{Q}}(\alpha)X + \mathrm{Nm}_{B/\mathbb{Q}}(\alpha) = 0$. Now if we set $\gamma := \Phi_p(\alpha) \in \mathrm{GL}_2(\mathbb{Q}_p)$ then $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$ where d is the discriminant of the characteristic polynomial $P_\gamma(X)$ of γ. Since the transformation γ is elliptic, by Proposition 2.3.5 we have that $d \notin \mathbb{Q}_p^{*2}$ and so $\mathbb{Q}_p(\sqrt{d}) \simeq \mathbb{Q}_{p^2}$. Hence $\mathbb{Q}(\alpha)$ is a p-imaginary quadratic field. □

4.1.5 Remark. If $\gamma := \Phi_p(\varphi(\sqrt{d})) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, then $A + D = 0$ and so its associated binary quadratic form (cf. Definition 2.3.3) is

$$f_\gamma(X, Y) = CX^2 - 2AXY - BY^2.$$

The zeros of f_γ have the following expressions:

$$z_1 = \frac{A + \sqrt{d}}{C}, \qquad z_2 = \frac{A - \sqrt{d}}{C}.$$

Therefore we see that z_1 and z_2 are Galois conjugated in the quadratic extension $\mathbb{Q}_p(\sqrt{d})$, so we can write $z_1 = \overline{z}_2$ and we have that the action of γ on these points is

$$\gamma \begin{pmatrix} z_1 \\ 1 \end{pmatrix} = \sqrt{d} \begin{pmatrix} z_1 \\ 1 \end{pmatrix}, \qquad \gamma \begin{pmatrix} \overline{z}_1 \\ 1 \end{pmatrix} = -\sqrt{d} \begin{pmatrix} z_2 \\ 1 \end{pmatrix}.$$

Following the same spirit as in [AB04] we want to relate the set of embeddings of p-imaginary quadratic fields into the quaternion algebra B with the set of representations of an integer by certain quadratic forms associated to the algebra. For the basic definitions and properties about quaternion algebras and quadratic forms, see Chapter 1.1 and [AB04, Ch. 3].

Recall (cf. Section 1.1) that for every prime ℓ of $\mathbb{Q}$ we denote by $\mathbb{Z}[1/\ell]$ the ring of integers outside ℓ, i.e.

$$\mathbb{Z}[1/\ell] := \left(\bigcap_{q \neq \ell} \mathbb{Z}_q \right) \cap \mathbb{Q}.$$

In particular when $\ell = \infty$, then $\mathbb{Z}[1/\infty] = \mathbb{Z}$.

4.1.6 Definition. An integer m is **represented** by an n-ary quadratic form $f \in \mathbb{Z}[1/\ell][X_1, \ldots, X_n]$ if there exist $a_1, \ldots, a_n \in \mathbb{Z}[1/\ell]$ such that

$$f(a_1, \ldots, a_n) = m.$$

The representation is said to be **primitive** if the ideal generated by $a_1, \ldots, a_n$ is $(a_1, \ldots, a_n) = \mathbb{Z}[1/\ell]$.

We will denote by $\mathrm{Rep}(f, m; \mathbb{Z}[1/\ell])$ the set of representations of the integer m by the form f and by $\mathrm{Rep}^*(f, m; \mathbb{Z}[1/\ell]))$ its subset of primitive representations.

4.1.7 Definition. Let Q be a quaternion $\mathbb{Q}$-algebra, K a quadratic field, and ℓ a prime integer. If $\mathcal{O}_{K,m}[1/\ell] \subseteq K$ is a quadratic order over $\mathbb{Z}[1/\ell]$ of conductor m and $\mathcal{O}[1/\ell]$ is an Eichler order over $\mathbb{Z}[1/\ell]$ in Q, then we will denote by

$$\mathcal{E}(K, Q) \quad \text{and} \quad \mathcal{E}(\mathcal{O}_{K,m}[1/\ell], \mathcal{O}[1/\ell]),$$

respectively, the set of embeddings $K \hookrightarrow Q$ of $\mathbb{Q}$-algebras and the set of embeddings $\varphi : \mathcal{O}_{K,m}[1/\ell] \hookrightarrow \mathcal{O}[1/\ell]$ of $\mathbb{Z}[1/\ell]$-modules.

We can extend the definition of "optimal embedding" (cf. [AB04, Definition 4.7]) to embeddings of $\mathbb{Z}[1/\ell]$-modules:

4.1.8 Definition. Let ℓ be a fixed prime integer. Let Q be a quaternion $\mathbb{Q}$-algebra, $\mathcal{O}[1/\ell]$ be an Eichler order over $\mathbb{Z}[1/\ell]$ and $\mathcal{O}_{K,m}[1/\ell]$ be an order over $\mathbb{Z}[1/\ell]$ inside a quadratic field K.

An embedding $\varphi : \mathcal{O}_{K,m}[1/\ell] \hookrightarrow \mathcal{O}[1/\ell]$ is said to be **optimal** (also **maximal**) if it satisfies the equality $\varphi(\mathcal{O}_{K,m}[1/\ell]) = \mathcal{O}[1/\ell] \cap \varphi(K)$,.

We will denote by

$$\mathcal{E}^*(\mathcal{O}_{K,m}[1/\ell], \mathcal{O}[1/\ell])$$

the subset of $\mathcal{E}(\mathcal{O}_{K,m}[1/\ell], \mathcal{O}[1/\ell])$ of optimal embeddings.

4.1.9 Proposition. *Let B be a definite quaternion algebra over $\mathbb{Q}$.*

If $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field, with d a square-free integer, then there exists a bijection of sets

$$\mathcal{E}(K, B) \simeq \mathrm{Rep}(\mathrm{N}_{B,3}, -d; \mathbb{Q}).$$

In particular, every quadratic field K admitting an embedding $K \hookrightarrow B$ is imaginary at ∞, i.e. $d < 0$.

PROOF. The proof is the same as the one of [AB04, 4.2]. The idea is that if $\varphi : K \hookrightarrow B$ is an embedding, then $\varphi(\sqrt{d})$ is a pure quaternion of norm $\mathrm{Nm}_{B/\mathbb{Q}}(\varphi(\sqrt{d})) = \mathrm{Nm}_{K/\mathbb{Q}}(\sqrt{d}) = -d$ and so its coordinates in a $\mathbb{Q}$-basis of B gives the desired representation. The viceversa is also intuitively clear.

Finally, since the ternary normic form $\mathrm{N}_{B,3}$ is positive definite, condition $-d \leftarrow \mathrm{N}_{B,3}$ implies that d is negative. □

4.1.10 Proposition. *Let B be a definite quaternion algebra over $\mathbb{Q}$ of discriminant D_B and let p be a prime integer not dividing D_B. Let H be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant $D_H = pD_B$ and let K be a quadratic field imaginary at both the primes p and ∞. Then there is a bijection of sets*

$$\mathcal{E}(K, H) \simeq \mathcal{E}(K, B).$$

PROOF. Recall that for the indefinite quaternion algebra H the statement analogous to Proposition 4.1.9 holds (cf. [AB04, 4.2]) so each set of embeddings of the statement can be described by representations.

Let us start by noting that the quaternion algebras H and B are such that $H_\ell \simeq B_\ell$ for every $\ell \notin \{\infty, p\}$, so in order to apply the Principle of Hasse-Minkowski for quadratic forms or, equivalently, for embeddings (cf. [Vig80, 3.2]) we only need to look at the behavior of the immersion/representation at one of the primes p, ∞ (the other one comes for free via the product formula for the Hilbert symbol).

From left to right, we have that the ternary normic form $\mathrm{N}_{3,B}$ always represents all positive integers over $\mathbb{R}$. From right to left, we have that the local quaternion $\mathbb{Q}_p$-algebra H_p is a field containing two copies of $\mathbb{Q}_{p^2} \simeq K_{(p)}$, since p divides the discriminant D_H. □

So we have seen that the set of quadratic fields

$$\{K \mid [K : \mathbb{Q}] = 2,\ K \hookrightarrow B,\ K \otimes \mathbb{Q}_p \simeq \mathbb{Q}_{p^2}\}$$

is included in the set

$$\{K \mid [K : \mathbb{Q}] = 2,\ K \hookrightarrow B,\ K \otimes \mathbb{R} \simeq \mathbb{C}\}$$

and the inclusion is strict since there are negative integers d such that $\left(\frac{d}{p}\right) \neq -1$.

4.1.11 Remark. When $K = \mathbb{Q}(\sqrt{d})$ for a square-free integer d such that $\left(\frac{d}{p}\right) = 0$, then again, as in Proposition 4.1.3, the transformations in $\Phi_p(K^*)$

are elliptic and they all have two fixed points $z, \bar{z}$ belonging to one of the two quadratic ramified extensions of $\mathbb{Q}_p$ and are Galois conjugated inside this quadratic extension. These two points lye in $\mathcal{H}_p(\mathbb{C}_p)$ and since the residue degree of the field of definition is 1, their reduction are $\mathbb{F}_p$-rational points, so they correspond to two different edges of the Bruhat-Tits tree.

The following result is the adaptation of [AB04, Theorem 4.26] and its proof is exactly the same, after replacing $\mathbb{Z}$ by $\mathbb{Z}[1/p]$.

4.1.12 Theorem. *Let B be a definite quaternion algebra over $\mathbb{Q}$ of discriminant D_B and let p be a prime integer such that $p \nmid D_B$. Let $\mathcal{O}$ be an Eichler order of B of level N coprime with p and denote by $\mathcal{O}[1/p] := \mathcal{O} \otimes \mathbb{Z}[1/p]$ the corresponding $\mathbb{Z}[1/p]$-order. Let K be a p-imaginary quadratic field of discriminant D_K and let $\mathcal{O}_{K,m}[1/p]$ be a $\mathbb{Z}[1/p]$-order of conductor m.*

If we denote by $\mathcal{O}'[1/p]$ the order of B equal to $\mathbb{Z}[1/p] + 2\mathcal{O}[1/p]$, then we have the following bijections of sets:

$$\mathcal{E}(\mathcal{O}_{K,m}[1/p], \mathcal{O}[1/p]) \simeq \mathrm{Rep}(\mathrm{N}_{\mathcal{O}',3}, -m^2 D_K; \mathbb{Z}[1/p]),$$

$$\mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}[1/p]) \simeq \mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}',3}, -m^2 D_K; \mathbb{Z}[1/p]).$$

Proof. Even if the proof is the same as the one of [AB04, Theorem 4.26], we sketch the proof of the bijection

$$\mathcal{E}(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p]) \simeq \mathrm{Rep}(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2 D_K; \mathbb{Z}[1/p])$$

because the ideas used here will be applied later to compute explicit examples of families of binary quadratic forms.

Let us assume first that $K = \mathbb{Q}(\sqrt{d})$ is an imaginary quadratic field such that $d \equiv 2, 3 \pmod 4$, so K has discriminant $D_K = 4d$ and $\mathcal{O}_{K,m}[1/p] = \mathbb{Z}[1/p][m\sqrt{d}]$.

If $\varphi : \mathcal{O}_{K,m}[1/p] \hookrightarrow \mathcal{O}_B[1/p]$ is an embedding, then $\omega := \varphi(m\sqrt{d})$ is an element of $\mathcal{O}_B[1/p]$ with $\mathrm{Tr}_{B/K}(\omega) = \mathrm{Tr}_{K/\mathbb{Q}}(m\sqrt{d}) = 0$ and $\mathrm{Nm}_{B/\mathbb{Q}}(\omega) = \mathrm{Nm}_{K/\mathbb{Q}}(m\sqrt{d}) = -m^2 d$.

Now it is very important to observe the following. If $\mathcal{B} = \{1, v_2, v_3, v_4\}$ is a normalized basis for $\mathcal{O}_B[1/p]$, then $\mathcal{O}'_B[1/p]$ admits an integral basis $\mathcal{B}' = \{1, 2v_2, 2v_3, 2v_4 - \mathrm{Tr}(v_4)\}$ such that $2v_2, 2v_3, 2v_4 - \mathrm{Tr}(v_4)$ are pure quaternions (cf. [AB04, Definitions 1.36, 1.37]) and so a quaternion $\alpha = (a_1, a_2, a_3, a_4)_{\mathcal{B}'}$ is pure if and only if $a_1 = 0$.

Therefore $2\omega \in \mathcal{O}'_B[1/p] = \mathbb{Z}[1/p] + 2\mathcal{O}_B[1/p]$, with $\mathrm{Tr}(2\omega) = 0$ and $\mathrm{Nm}(2\omega) = -m^2 4d = -m^2 D_K$. After the observation above it is clear that

the integral coordinates of 2ω in the basis $\mathcal{B}'$ are $(0,x,y,z) \in \mathbb{Z}[1/p]$ and gives a representation $(x,y,z) \in \mathrm{Rep}(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2 D_K; \mathbb{Z}[1/p])$.

Viceversa, given a representation $(x,y,z) \in \mathrm{Rep}(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2 D_K; \mathbb{Z}[1/p])$ we can consider the quaternion $\alpha := (0,x,y,z)_{\mathcal{B}'} \in \mathcal{O}'[1/p]$. Therefore $\alpha/2 = -z\mathrm{Tr}(v_4)/2 + xv_2 + yv_3 + zv_4 \in \mathcal{O}[1/p]$ is such that $\mathrm{Tr}(\alpha/2) = 0$ (after what we have observed about the basis $\mathcal{B}'$) and $\mathrm{Nm}(\alpha/2) = -m^2 d$, so we can define the embedding $\varphi : \mathcal{O}_{K,m}[1/p] \hookrightarrow \mathcal{O}_B[1/p]$ by setting $\varphi(m\sqrt{d}) := \alpha/2$.

In the case $K = \mathbb{Q}(\sqrt{d})$ and $d \equiv 1 \pmod 4$, we have that K has discriminant $D_K = d$ and $\mathcal{O}_{K,m}[1/p] = \mathbb{Z}[1/p][(1+\sqrt{d})/2]$ we can construct the bijection with the same reasoning.

Finally we can summarize the bijection of the statement as follows.

If $(x,y,z) \in \mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2 D_K; \mathbb{Z}[1/p])$ then we define an optimal embedding $\varphi \in \mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p])$ by

$$\varphi(\sqrt{d}) := \begin{cases} \left(-\dfrac{z\mathrm{Tr}(v_{v_4})}{2m}, \dfrac{x}{m}, \frac{y}{m}, \dfrac{z}{m}\right)_{\mathcal{B}}, & \text{if } d \equiv 2,3 \pmod 4 \\ \left(-\dfrac{z\mathrm{Tr}(v_{v_4})}{m}, \dfrac{2x}{m}, \dfrac{2y}{m}, \dfrac{2z}{m}\right)_{\mathcal{B}}, & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

If $\varphi \in \mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p])$ and we put

$$\omega := \begin{cases} \varphi(m\sqrt{d}), & \text{if } d \equiv 2,3 \pmod 4 \\ \varphi\left(m\dfrac{1+\sqrt{d}}{2}\right), & \text{if } d \equiv 1 \pmod 4, \end{cases}$$

then the associated representation is $(x,y,z) \in \mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2 D_K; \mathbb{Z}[1/p])$ such that

$$\omega = \begin{cases} \left(-\dfrac{z\mathrm{Tr}(v_4)}{2}, x, y, z\right)_{\mathcal{B}}, & \text{if } d \equiv 2,3 \pmod 4 \\ \left(\dfrac{m - z\mathrm{Tr}(v_4)}{2}, x, y, z\right)_{\mathcal{B}}, & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

□

4.1.2 Class numbers of embeddings

From now on, B and H will denote, respectively, a definite and an indefinite quaternion algebra over $\mathbb{Q}$ such that $D_H = pD_B$, for a fixed prime integer

prime $p \nmid D_B$. And $\mathcal{O}_H \subseteq H$ and $\mathcal{O}_B \subseteq B$ will denote Eichler orders over $\mathbb{Z}$ of the same level N, $(N,p)=1$.

Let $K=\mathbb{Q}(\sqrt{d})$ be a quadratic field, where d is a square-free integer, and let $\mathcal{O}_{K,m} \subseteq K$ be an order over $\mathbb{Z}$ of conductor m. As usual, we denote by $\mathcal{O}_B[1/p] := \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ and $\mathcal{O}_{K,m}[1/p] := \mathcal{O}_{K,m} \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ the corresponding $\mathbb{Z}[1/p]$-orders resp. in B and in K.

We will consider the following subgroups of quaternions units, arising from the complex and the p-adic uniformizations of the Shimura curve $X(D_H, N)$:

(i) $\mathcal{O}_{H,+}^* := \{\alpha \in \mathcal{O}_H^* \mid \mathrm{Nm}(\alpha) > 0\} = \{\alpha \in \mathcal{O}_H^* \mid \mathrm{Nm}(\alpha) = 1\}$,

(ii) $\mathcal{O}_B[1/p]_+^* := \{\alpha \in \mathcal{O}_B[1/p]^* \mid v_p(\mathrm{Nm}(\alpha)) \equiv 0 \,(\mathrm{mod}\, 2)\}$.

Thus we have the following right actions of these groups over the sets $\mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}[1/p])$ and $\mathcal{E}^*(\mathcal{O}_{K,m}, \mathcal{O}_H)$ respectively:

(i) For any $\alpha \in \mathcal{O}_{H,+}^*$ and any $\varphi \in \mathcal{E}^*(\mathcal{O}_{K,m}, \mathcal{O}_H)$,

$$(\varphi \cdot \alpha)(x) := \alpha^{-1}\varphi(x)\alpha,\ x \in \mathcal{O}_{K,m}.$$

(ii) For any $\alpha \in \mathcal{O}_B[1/p]_+^*$ and any $\varphi \in \mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p])$,

$$(\varphi \cdot \alpha)(x) := \alpha^{-1}\varphi(x)\alpha,\ x \in \mathcal{O}_{K,m}[1/p].$$

Therefore we can define the following cardinalities of sets, following the same notations as in [AB04, 4.2]):

(i) $\nu(D_H, N, d, m; \mathcal{O}_{H,+}^*) := \#\mathcal{E}^*(\mathcal{O}_{K,m}, \mathcal{O}_H)/\mathcal{O}_{H,+}^*$,

(ii) $\nu(D_B, N, d, m; \mathcal{O}_B[1/p]_+^*) := \#\mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}[1/p])/\mathcal{O}_B[1/p]_+^*$.

4.1.13 Remark. The cardinal $\nu(D_B, N, d, m; \mathcal{O}_B[1/p]_+^*)$ does not depend on the type of the order $\mathcal{O}_B[1/p]$ in B and the cardinal $\nu(D_H, N, d, m; \mathcal{O}_{H,+}^*)$ does not depend on the type of the order $\mathcal{O}_H$ in H, since the number of types $t(D_B, N)$ and $t(D_H, N)$ are both equal to 1 after Theorems 1.1.11 and 3.1.7.

In the same way we can define also the cardinals

(i) $\nu(D_H, N, d, m; \mathcal{O}_H^*) := \#\mathcal{E}^*(\mathcal{O}_{K,m}, \mathcal{O}_H)/\mathcal{O}_H^*$,

(ii) $\nu(D_B, N, d, m; \mathcal{O}_B[1/p]^*) := \#\mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}[1/p])/\mathcal{O}_B[1/p]^*$.

In order to compute these cardinals we have to define the following associated local factors:

(i) For every prime integer ℓ,

$$\nu_\ell(D_H, N, d, m; \mathcal{O}_H^*) := \#\mathcal{E}^*(\mathcal{O}_{K,\ell}, \mathcal{O}_{H,\ell})/\mathcal{O}_{H,\ell}^*.$$

(ii) For every prime integer $\ell \neq p$,

$$\nu_\ell(D_B, N, d, m; \mathcal{O}_B[1/p]^*) := \#\mathcal{E}^*(\mathcal{O}_{K,\ell}, \mathcal{O}_{B,\ell})/\mathcal{O}_{B,\ell}^*.$$

4.1.14 Theorem. *Let B and H be respectively a definite and an indefinite quaternion algebra over $\mathbb{Q}$ such that $D_H = pD_B$ and let $\mathcal{O}_H \subseteq H$ and $\mathcal{O}_B \subseteq B$ be Eichler orders over $\mathbb{Z}$ of the same level N. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, with d a square-free integer, and let $\mathcal{O}_{K,m} \subseteq K$ be an order over $\mathbb{Z}$ of conductor m.*

Then the cardinalities

$$\begin{array}{l}\nu(D_H, N, d, m; \mathcal{O}_H^*),\\ \nu(D_B, N, d, m; \mathcal{O}_B[1/p]^*),\\ \nu(D_H, N, d, m; \mathcal{O}_{H,+}^*),\\ \nu(D_B, N, d, m; \mathcal{O}_B[1/p]_+^*)\end{array}$$

are finite. Moreover if the quadratic field K is imaginary at both p and ∞, then the following relations are satisfied:

(i) $\nu(D_B, N, d, m; \mathcal{O}_B[1/p]_+^*) = 2\nu(D_B, N, d, m; \mathcal{O}_B[1/p]^*)$,

(ii) $\nu(D_H, N, d, m; \mathcal{O}_{H,+}^*) = 2\nu(D_H, N, d, m; \mathcal{O}_H^*)$,

(iii) $\nu(D_H, N, d, m; \mathcal{O}_H^*) = 2\nu(D_B, N, d, m; \mathcal{O}_B[1/p]^*)$,

(iv) $\nu(D_H, N, d, m; \mathcal{O}_{H,+}^*) = 2\nu(D_B, N, d, m; \mathcal{O}_B[1/p]_+^*)$.

Proof. We start with the proof of point *(iii)*. Following [Vig80, Theorem 3.1, 3.2] we have that when N is square-free,

$$\nu_\ell(D_H, N, d, m; \mathcal{O}_{H,\ell}^*) = \begin{cases} 1 - \left(\dfrac{d}{\ell}\right), & \text{if } \ell \mid D_H \\ 1 + \left(\dfrac{d}{\ell}\right), & \text{if } \ell \mid N \\ 1, & \text{otherwise,} \end{cases}$$

and for every $\ell \neq p$,

$$\nu_\ell(D_B, N, d, m; \mathcal{O}_B[1/p]^*_\ell) = \begin{cases} 1 - \left(\dfrac{d}{\ell}\right), & \text{if } \ell \mid D_B \\ 1 + \left(\dfrac{d}{\ell}\right), & \text{if } \ell \mid N \\ 1, & \text{otherwise.} \end{cases}$$

In particular note that

$$\nu_\ell(D_H, N, d, m; \mathcal{O}^*_{H,\ell}) = \nu_\ell(D_B, N, d, m; \mathcal{O}_B[1/p]^*_\ell)$$

for every $\ell \neq p$ since $D_H = pD_B$.

Now by [AB04, Theorem 4.19] we already know that $\nu(D_H, d, m; \mathcal{O}^*_H)$ is finite. This is actually [Vig80, Theorem 5.15] since the Eichler order $\mathcal{O}_H$ over $\mathbb{Z}$ satisfies Eichler's condition (cf. Definition 1.1.6). Moreover, we can again apply [Vig80, Theorem 5.15] to the Eichler order $\mathcal{O}[1/p]$ over $\mathbb{Z}[1/p]$, since this satisfies Eichler's condition, and using the computations above for the local factors we find the following equalities:

$$\nu(D_B, N, d, m; \mathcal{O}_B[1/p]^*) = h(\mathcal{O}_{K,m}[1/p]) \prod_{\ell \neq p} \nu_\ell(D_B, N, d, m; \mathcal{O}_B[1/p]^*_\ell) =$$

$$h(\mathcal{O}_{K,m}) \prod_{\ell \neq p} \nu(D_H, N, d, m; \mathcal{O}^*_{H,\ell}) = \nu(D_H, N, d, m; \mathcal{O}^*_H)\nu_p(D_H, d, m; \mathcal{O}^*_{H,p})^{-1} =$$

$$= \frac{1}{2}\nu(D_H, N, d, m; \mathcal{O}^*_H).$$

Note that since K is p-imaginary $\nu_p(D_H, d, m; \mathcal{O}^*_{H,p}) = 2$ and that the class numbers of $\mathcal{O}_{K,m}[1/p]$ and $\mathcal{O}_{K,m}$ coincide. This completes the proof of the equality (iii).

When N is not square-free, the corresponding formulas for the local cardinalities are given in [AB04, Theorem 4.19] (and proven in [Eic55]) and again these formulas depend only on the prime $\ell | N, \ell \neq p$ and on the integer d. Hence the proof of equality (iii) in this case proceeds exactly in the same way.

The first (resp. the second) equality of the statement follows from the simple observation that the group $\mathcal{O}_B[1/p]^*_+$ (resp. $\mathcal{O}^*_{H,+}$) has index 2 inside $\mathcal{O}_B[1/p]^*$ (resp. $\mathcal{O}^*_H$). Finally (iv) is a consequence of (i), (ii) and (iii). □

As a direct consequence of Theorems 4.1.14 and 4.1.12 we have the following result.

4.1.15 Corollary. *Let K be a quadratic field of discriminant D_K, imaginary at both the primes p and ∞, and let $\mathcal{O}_{K,m}$ be an order in K of conductor m. Then, the following are equivalent:*

(*i*) $\mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p]) \neq \emptyset$,

(*ii*) $\mathcal{E}^*(\mathcal{O}_{K,m}, \mathcal{O}_H) \neq \emptyset$,

(*iii*) $\mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2 D_K; \mathbb{Z}[1/p]) \neq \emptyset$,

(*iv*) $\mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_H,3}, -m^2 D_K; \mathbb{Z}) \neq \emptyset$,

(*v*) *All primes $\ell | D_B$ are not split in K and all primes $\ell | N$ are not inert in K.*

4.2 p-imaginary multiplication parameters

4.2.1 Class numbers of p-adic binary quadratic forms

Let B be a definite quaternion algebra of discriminant D_B and let p be a prime integer such that $p \nmid D_B$. Let H be an indefinite quaternion algebra of discriminant $D_H = pD_B$. Let $\mathcal{O}_H \subseteq H$ and $\mathcal{O}_B$ be Eichler orders over $\mathbb{Z}$, both of level $N \in \mathbb{Z}$, $(N, p) = 1$. Put

$$\mathcal{O}'_H = \mathbb{Z} + 2\mathcal{O}_H, \qquad \mathcal{O}'_B = \mathbb{Z} + 2\mathcal{O}_B,$$

$$\mathcal{O}_B[1/p] = \mathcal{O}_B \otimes \mathbb{Z}[1/p], \quad \mathcal{O}'_B[1/p] = \mathcal{O}'_B \otimes \mathbb{Z}[1/p].$$

The algebra B admits a representation $B = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ such that $\left(\frac{\alpha}{p}\right) = 1$ which induces the p-adic matricial immersion

$$\begin{aligned} B \qquad &\longrightarrow \quad \mathrm{M}_2(\mathbb{Q}_p(\sqrt{\alpha})) = \mathrm{M}_2(\mathbb{Q}_p) \\ x + yi + zj + tk \quad &\longmapsto \quad \begin{pmatrix} x + y\sqrt{\alpha} & z + t\sqrt{\alpha} \\ \beta(z - t\sqrt{\alpha}) & x - y\sqrt{\alpha}) \end{pmatrix}, \end{aligned}$$

and the algebra H admits a representation $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ such that $a > 0$ which induces the ∞-adic (or real) matricial immersion

$$\begin{aligned} H \qquad &\longrightarrow \quad \mathrm{M}_2(\mathbb{Q}_\infty(\sqrt{a})) = \mathrm{M}_2(\mathbb{R}) \\ x + yi + zj + tk \quad &\longmapsto \quad \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a}) \end{pmatrix}. \end{aligned}$$

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field imaginary at both the primes ∞ and p and let $\mathcal{O}_{K,m} \subseteq K$ be an order over $\mathbb{Z}$ of conductor m. Put

$$\mathcal{O}_{K,m}[1/p] := \mathcal{O}_{K,m} \otimes \mathbb{Z}[1/p].$$

Recall that if $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{M}_2(\mathbb{Q}_p)$, we denote by f_γ the associated p-adic binary quadratic form (cf. Definition 2.3.3). This is the following quadratic form

$$f_\gamma(X,Y) := CX^2 + (D-A)XY - BY^2 \in \mathbb{Q}_p[X,Y].$$

In the same way, if $\gamma \in \mathrm{M}_2(\mathbb{R})$ we denote by f_γ the binary quadratic form with real coefficients associated to γ (cf. [AB04, Definition 2.11]).

As usual, H_0 and B_0 denote the subset of pure quaternions in H and in B, respectively.

We define the following sets of binary quadratic forms:

$$\mathcal{H}_p(\mathcal{O}'_B[1/p]) := \{f_{\Phi_p(\alpha)} \in \mathbb{Q}_p[X,Y] \mid \ \alpha \in \mathcal{O}'_B[1/p] \cap B_0\},$$

$$\mathcal{H}_\infty(\mathcal{O}'_H) := \{f_{\Phi_\infty(\alpha)} \in \mathbb{R}[X,Y] \mid \ \alpha \in \mathcal{O}'_H \cap H_0\},$$

$$\mathcal{H}_p(\mathcal{O}'_B[1/p], \mathcal{O}_{K,m}[1/p]) := \{f \in \mathcal{H}_p(\mathcal{O}'_B[1/p]) \mid \ \det(f) = -m^2 D_K\},$$

$$\mathcal{H}_\infty(\mathcal{O}'_H, \mathcal{O}_{K,m}) := \{f \in \mathcal{H}_\infty(\mathcal{O}'_H) \mid \ \det(f) = -m^2 D_K\}.$$

The second and the fourth sets are the same as the ones defined in [AB04, Notation 4.42]. The notations $\mathcal{H}_p$ and $\mathcal{H}_\infty$ aim to recall the ones used to denote the p-adic and Poincaré upper half-planes, since these sets are formed by binary quadratic forms whose zeros are "special points" on these two upper "half-planes".

Note also that each of these sets depends on the matricial immersions Φ_∞ and Φ_p and so it depends on the chosen representation for the quaternion algebra.

4.2.1 Proposition. *We have the following bijections of sets:*

(*a*) $\mathcal{E}(\mathcal{O}_{K,m}, \mathcal{O}_H) \simeq \mathrm{Rep}(\mathrm{N}_{\mathcal{O}'_H,3}, -m^2 D_K; \mathbb{Z}) \simeq \mathcal{H}_\infty(\mathcal{O}'_H, \mathcal{O}_{K,m})$.

(*b*) $\mathcal{E}(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p]) \simeq$

$$\simeq \mathrm{Rep}(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2 D_K; \mathbb{Z}[1/p]) \simeq \mathcal{H}_p(\mathcal{O}'_B[1/p], \mathcal{O}_{K,m}[1/p]).$$

PROOF. The bijections of (a) are contained in [AB04, Theorem 4.53] and the proof of (b) is the same, *mutatis mutandis*.

Given an embedding $\varphi \in \mathcal{E}(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p])$, we can associate a binary quadratic form in $\mathcal{H}_p(\mathcal{O}'_B[1/p], \mathcal{O}_{K,m}[1/p])$, considering the elliptic transformation $(\Phi_p \circ \varphi)(\sqrt{d})$ and the binary quadratic form $f_{\Phi_p(\varphi(a))} \in \mathbb{Q}_p[X,Y]$ associated to it. The zeros of this form are the fixed points of the embedding φ. □

4.2.2 Definition. If we denote by

$$\mathfrak{f}_\infty : \mathcal{E}(\mathcal{O}_{K,m}, \mathcal{O}_H) \to \mathcal{H}_\infty(\mathcal{O}'_H, \mathcal{O}_{K,m}),$$

and by

$$\mathfrak{f}_p : \mathcal{E}(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p]) \to \mathcal{H}_p(\mathcal{O}'_B[1/p], \mathcal{O}_{K,m}[1/p])$$

the bijections of Proposition 4.2.1 we can define the following sets of "primitive" binary quadratic forms.

(i) $\mathcal{H}^*_\infty(\mathcal{O}_H, \mathcal{O}_{K,m}) := \mathfrak{f}_\infty(\mathcal{E}^*(\mathcal{O}_{K,m}, \mathcal{O}_H))$.

We refer by $(\mathcal{O}_H, \mathcal{O}_{K,m})$**-primitive quadratic form** to a binary quadratic form belonging to the set $\mathcal{H}^*_\infty(\mathcal{O}_H, \mathcal{O}_{K,m})$.

(ii) $\mathcal{H}^*_p(\mathcal{O}_B[1/p], \mathcal{O}_{K,m}[1/p]) := \mathfrak{f}_p(\mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p]))$.

We refer by $(\mathcal{O}_B[1/p], \mathcal{O}_{K,m}[1/p])$**-primitive quadratic form** to a binary quadratic form belonging to $\mathcal{H}^*_p(\mathcal{O}_B[1/p], \mathcal{O}_{K,m}[1/p])$.

Therefore we have the following result which mirrors [AB04, Corollary 4.5]:

4.2.3 Theorem. *The bijections of sets of Proposition 4.2.1 restrict to the following bijections of sets of optimal embeddings, primitive representations and primitive forms:*

(i) $\mathcal{E}^*(\mathcal{O}_{K,m}, \mathcal{O}_H) \simeq \mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_H,3}, -m^2 D_K; \mathbb{Z}) \simeq \mathcal{H}^*_\infty(\mathcal{O}'_H, \mathcal{O}_{K,m})$,

(ii) $\mathcal{E}^*(\mathcal{O}_{K,m}, \mathcal{O}_B[1/p]) \simeq$

$$\simeq \mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2 D_K; \mathbb{Z}[1/p]) \simeq \mathcal{H}^*_p(\mathcal{O}'_B[1/p], \mathcal{O}_{K,m}[1/p]).$$

4.2.2 Class numbers of p-imaginary multiplication parameters

Now we will rephrase the definition of complex multiplication parameter arising from the complex uniformization of a Shimura curve $X(D_H, N)$ (cf. Definition 1.3.15) by using a notation which is more enlightening in this context. In fact, this new formulation will allow us to establish the analogous definition for the p-adic uniformization of a Shimura curve, thanks to the interchange of the local invariants p and ∞.

Let us fix a prime integer p. Let H be an indefinite quaternion algebra of discriminant D_H such that $p|D_H$ and let $\mathcal{O}_H \subseteq H$ be an Eichler order over $\mathbb{Z}$ of level N. Let B be a definite quaternion algebra of discriminant $D_B = p^{-1}D_H$ and let $\mathcal{O}_B[1/p] \subseteq B$ be an Eichler order over $\mathbb{Z}[1/p]$ of conductor N. Fix two matricial immersions:

$$\Phi_\infty : H \hookrightarrow \mathrm{M}_2(\mathbb{Q}_\infty), \qquad \Phi_p : B \hookrightarrow \mathrm{M}_2(\mathbb{Q}_p).$$

Therefore we can consider the following discrete subgroups:

(a) $\Gamma_\infty(D_H, N) := \Phi_\infty(\mathcal{O}_H^*)\mathbb{Z}^* \subseteq \mathrm{PGL}_2(\mathbb{Q}_\infty)$,

(b) $\Gamma_p(D_B, N) := \Phi_p(\mathcal{O}_B[1/p]^*)\mathbb{Z}[1/p]^* \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$.

(c) $\Gamma_{\infty,+}(D_H, N) := \Phi_\infty(\mathcal{O}_{H,+}^*)\mathbb{Z}^* \subseteq \mathrm{PGL}_2(\mathbb{Q}_\infty)$,

(d) $\Gamma_{p,+}(D_B, N) := \Phi_p(\mathcal{O}_B[1/p]_+^*)\mathbb{Z}[1/p]^* \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$.

4.2.4 Definition. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, imaginary at both the primes ∞ and p, and let $\mathcal{O}_{K,m}$ be an order of K over $\mathbb{Z}$ of conductor m. Put $\mathcal{O}_{K,m}[1/p] := \mathcal{O}_{K,m} \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$.

(a) We say that a point $\tau \in \Gamma_{\infty,+}(D_H, N)\backslash\mathcal{H}$ is an **∞-imaginary multiplication parameter by $\mathcal{O}_{K,m}$** (also a **complex multiplication parameter**) if $\tau \in \mathcal{H}$ is a fixed point for an optimal $\mathbb{Z}$-embedding $\varphi : \mathcal{O}_{K,m} \hookrightarrow \mathcal{O}_H$.

We denote by $\mathrm{CM}_\infty(D_H, N, d, m)$ the subset of $\Gamma_{\infty,+}(D_H, N)\backslash\mathcal{H}$ formed by the complex multiplication points by $\mathcal{O}_{K,m}$ and by $\mathrm{cm}_\infty(D_H, N, d, m)$ its cardinality.

(b) We say that a point $\tau \in \Gamma_{p,+}(D_B, N)\backslash\mathcal{H}_p(\mathbb{Q}_{p^2})$ is a **p-imaginary multiplication parameter by $\mathcal{O}_{K,m}[1/p]$** if $\tau \in \mathcal{H}_p(\mathbb{Q}_{p^2})$ is a fixed point for an optimal $\mathbb{Z}[1/p]$-embedding $\varphi : \mathcal{O}_{K,m}[1/p] \hookrightarrow \mathcal{O}_B[1/p]$.

We denote by $\mathrm{CM}_p(D_B, N, d, m)$ the subset of points in the quotient set $\Gamma_{p,+}(D_B, N)\backslash\mathcal{H}_p(\mathbb{Q}_{p^2})$ having p-imaginary multiplication by $\mathcal{O}_{K,m}[1/p]$ and by $\mathrm{cm}_p(D_B, N, d, m)$ its cardinality.

As observed in Remark 4.1.5, an embedding $\varphi : K \hookrightarrow B$ has two Galois-conjugated fixed points $z, \overline{z} \in \mathbb{Q}_{p^2} \smallsetminus \mathbb{Q}_p$, the Galois conjugation being in this case the one coming from the Galois group of the quadratic extension $\mathbb{Q}_{p^2}|\mathbb{Q}_p$.

4.2.5 Definition. Let K be a quadratic field, $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer. For every embedding $\varphi \in \mathcal{E}(K, B)$ there exists a unique embedding $\psi \in \mathcal{E}(K, B)$ such that:

$$\varphi(\sqrt{d}) = \alpha \iff \psi(-\sqrt{d}) = -\alpha.$$

The embedding ψ is exactly the embedding φ composed with the Galois conjugation of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ and so it has the same fixed points of φ. The embedding ψ is called **the conjugated embedding of** φ and it is denoted by $\overline{\varphi}$.

Moreover, since $\overline{\varphi}(\mathcal{O}_{K,m}) = \varphi(\mathcal{O}_{K,m})$ and $\overline{\varphi}(K) = \varphi(K)$, we have that

$$\varphi \in \mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p]) \iff \overline{\varphi} \in \mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p]).$$

The relation between conjugated embeddings and their fixed points is explained in the following result.

4.2.6 Lemma. *Let $\varphi, \varphi' \in \mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p])$ be optimal embeddings such that*

(*i*) $\{z = z(\varphi), \overline{z} = \overline{z(\varphi)}\}$ *are the fixed points of* φ,

(*ii*) $\{z' = z(\varphi'), \overline{z'} = \overline{z(\varphi')}\}$ *are the fixed point of* φ'.

Then z' is $\Gamma_{p,+}(D_B, N)$-equivalent to z or to $\overline{z}$ if and only if φ' is $\mathcal{O}_B[1/p]^*_+$-equivalent to φ or to $\overline{\varphi}$.

Proof. The proof follows the same idea as in [AB04, Proposition 6.11] with the difference that in our case the transformations have two fixed and Galois conjugated points.

First observe that:

(a) $z(\overline{\varphi}) = \overline{z(\varphi)}$,

(b) $z' = Pz \iff \overline{z'} = P\overline{z}$ for every $P \in \mathrm{PGL}_2(\mathbb{Q}_p)$.

Assume for example that $z = Pz'$, for some $P \in \Gamma_p(D_B, N)$ and let $\sigma \in \mathcal{O}_B[1/p]^*_+/\mathbb{Z}[1/p]$ be such that $\Phi_p(\sigma) = P$.

Let $\alpha \in K^*$, $\mathrm{Tr}(\alpha) = 0$, and put

$$\gamma := \Phi_p(\varphi(\alpha)), \quad \gamma' := \Phi_p(\varphi'(\alpha)), \quad \gamma'' := \Phi_p(\sigma^{-1}\varphi(\alpha)\sigma).$$

Therefore γ'' has fixed points $\{\overline{z}', z'\}$, the same as γ' so by Lemma 4.1.2 $\gamma' = \lambda\gamma'' + \mu \mathrm{I}_2$, for some $\lambda, \mu \in \mathbb{Q}_p$, $\lambda \neq 0$. A computation of the trace and of the determinant of γ' and γ'' gives the equality $\mathrm{Det}(\gamma') = \lambda^2 \mathrm{Det}(\gamma'')$ and so $\lambda = \pm 1$. Hence we have that $\varphi'(\alpha) = \sigma^{-1}(\pm\varphi)(\alpha)\sigma$ for every $\alpha \in K^*$ of null-trace, so φ is $\mathcal{O}_B[1/p]^*_+$-equivalent to φ or to $\overline{\varphi}$. If we assume that $\overline{z} = Pz'$, with the same reasoning we obtain the φ has to be $\mathcal{O}_B[1/p]^*_+$-equivalent to $\overline{\varphi}$ or to φ.

For the viceversa let us assume that φ' is $\mathcal{O}_B[1/p]^*_+$-equivalent to φ, i.e. there exists a $\sigma \in \mathcal{O}_B[1/p]^*_+$ such that $\varphi' = \sigma^1\varphi\sigma$. For every $\alpha \in K$ put

$$P := \Phi_p(\sigma) \quad \gamma := \Phi_p(\varphi(\alpha)) \quad \gamma' := \Phi_p(\varphi'(\alpha)).$$

Therefore $\gamma' = P^{-1}\gamma P$ and a simple calculation yields that γ' fixes $P^{-1}z$ and $P^{-1}\overline{z}$. Since γ has as unique fixed points z' and $\overline{z}'$, then we have that $P^{-1}z = z'$ or $P^1 z = \overline{z'}$. Again, if we assume that φ' is $\mathcal{O}_B[1/p]^*_+$-equivalent to $\overline{\varphi}$, we prove that z has to be $\Gamma_p(D_B, N)$-equivalent to $\overline{z'}$ or z'. □

4.2.7 Lemma. *Let $\varphi \in \mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}_B[1/p])$ be an optimal embedding with fixed points $\{z, \overline{z}\}$. Then z is never $\Gamma_{p,+}(D_B, N)$-equivalent to $\overline{z}$.*

Proof. Let $\mathcal{F}$ be a fundamental domain in $\mathcal{H}_p(\mathbb{Q}_{p^2})$ for the action of $\Gamma_{p,+}(D_B, N)$, so there exists γ such that $z' := \gamma \cdot z \in \mathcal{F}$.

Therefore $\gamma \cdot \overline{z} = \overline{\gamma \cdot z}$, since $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$ and so its coefficient are auto-conjugated. Moreover $\overline{\gamma \cdot z} \in \mathcal{F}$, since $|z' - a| = |\overline{z'} - a|$ for every $a \in \mathbb{Q}_p$, by the definition of the p-adic absolute value on $\mathbb{Q}_{p^2}$. Now we have to consider two cases:

(1) If the points $z', \overline{z}'$ lay in the interior of the fundamental domain $\mathcal{F}$ then it is clear that $z, \overline{z}$ can not be equivalent because $\gamma \cdot z, \gamma \cdot \overline{z} \in \mathcal{F}$ are different.

(2) If $z', \overline{z}'$ are on the boundary of $\mathcal{F}$ then a simple calculation shows that a transformation $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$ such that $\gamma z' = \overline{z}'$ is represented by a matrix $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. But the only option for such a transformation γ belonging to $\Phi_p(\mathcal{O}_B[1/p])$ is $\gamma = \mathrm{I}_2$.

This concludes the proof.
□

4.2.8 Corollary. *Let $\varphi \in \mathcal{E}(K,B)$ be an embedding. Then φ is not $\mathcal{O}_B[1/p]_+^*$-equivalent to $\overline{\varphi}$.*

Proof. Let us suppose that the two embeddings $\varphi, \overline{\varphi}$ are $\mathcal{O}_B[1/p]_+^*$-equivalent and let $z, \overline{z}$ be their fixed points. By Lemma 4.2.6 we know then that z has to be equivalent to z or to $\overline{z}$ and Lemma 4.2.7 gives that z can only be $\Gamma_{p,+}(D_B,N)$-equivalent to z. Nevertheless $z = Pz$ implies that $P = \mathrm{I}_2$ in $\Gamma_{p,+}(D_B,N)$ and so $\varphi = \overline{\varphi}$ which is an absurd. Hence φ and $\overline{\varphi}$ are not $\mathcal{O}_B[1/p]_+^*$-equivalent, as we wanted to prove. □

This last result allows us to prove the following important theorem, where the number of classes of optimal embeddings is related to the number of p-imaginary multiplication parameters (cf. with its Archimedean analog: [AB04, Theorem 6.13]).

4.2.9 Theorem. *The set $\mathrm{CM}_p(D_B,N,d,m)$ is finite and has cardinality*

$$\mathrm{cm}_p(D_B,N,d,m) = \nu(D_B,N,d,m;\mathcal{O}_B[1/p]_+^*).$$

Moreover this cardinality is an even integer.

Proof. By Lemma 4.2.6, Lemma 4.2.7 and Corollary 4.2.8 we know that assigning to an optimal embedding $\varphi \in \mathcal{E}^*(\mathcal{O}_{K,m}[1/p],\mathcal{O}_B[1/p])$ one of its two fixed points $\{z(\varphi), \overline{z(\varphi)}\}$ induces a well-defined bijection between the sets

$$\mathcal{O}_B[1/p]_+^*\backslash\mathcal{E}^*(\mathcal{O}_{K,m}[1/p],\mathcal{O}_B[1/p]) \simeq \mathrm{CM}_p(D_B,N,d,m).$$

The fact that the cardinality is even is clear from the bijection, because for every point/embedding we have a different class given by the Galois conjugated. □

Note that the Archimedean analog of this result, which is [AB04, Theorem 6.13], is "half of Theorem 4.2.9" since the cardinality of the set of ∞-imaginary multiplication points is given by the formula:

$$\mathrm{cm}_\infty(D_H,N,d,m) = \frac{1}{2}\nu(D_H,N,d,m;\mathcal{O}_{H,+}^*).$$

The reason for this difference resides in Lemma 4.2.8, as already pointed out.

4.2.10 Corollary. *The sets of points* $\mathrm{CM}_\infty(D_H, N, d, m)$ *and* $\mathrm{CM}_p(D_B, N, d, m)$ *have the same cardinality, i.e.*

$$\mathrm{cm}_p(D_B, N, d, m) = \mathrm{cm}_\infty(D_H, N, d, m).$$

Proof. This is a consequence of Theorem 4.2.9, Theorem 4.1.14 and [AB04, Theorem 6.13]. □

Now, we can also define the cardinalities of certain sets of binary quadratic forms classes and we can relate them with the number of CM points.

(a) $\mathrm{h}_p(D_B, N, d, m) := \#\mathcal{H}_p^*(\mathcal{O}'_B[1/p], \mathcal{O}_{K,m})/\Phi_p(\mathcal{O}_B[1/p]^*/\mathbb{Z}[1/p]^*)$,

(b) $\mathrm{h}_\infty(D_H, N, d, m) := \#\mathcal{H}_\infty^*(\mathcal{O}'_H, \mathcal{O}_{K,m})/\Phi_\infty(\mathcal{O}_H^*/\mathbb{Z}^*)$.

4.2.11 Corollary. *We have the following equalities between cardinalities:*

(*i*) $\mathrm{h}_p(D_B, N, d, m) = \nu(D_B, N, d, m; \mathcal{O}_B[1/p]^*) = \frac{1}{2}\mathrm{cm}_p(D_B, N, d, m)$,

(*ii*) $\mathrm{h}_\infty(D_H, N, d, m) = \nu(D_H, N, d, m; \mathcal{O}_H^*) = \mathrm{cm}_\infty(D_H, N, d, m)$.

4.2.3 The cases of discriminant $D = 2p$ and $D = 3p$

In the following examples we explicitly compute families of binary quadratic forms arising from the p-adic uniformization of Shimura curves of discriminant $D_H = pD_B$ and level N, in some special cases.

In order to do this we will fix the following data:

(a) The discriminants D_H and D_B, resp. of the indefinite and definite quaternion algebras, and a prime integer $p|D_H$ such that the relation between these three integers is: $D_H = pD_B$.

(b) The level N coprime with p.

(c) The quadratic order $\mathcal{O}_{K,m}$ imaginary at p and ∞ by fixing integers d and m such that d is square-free, $d < 0$, $\left(\frac{d}{p}\right) = -1$ and m is coprime with d.

4.2.12 Example. In this example we compute families of binary quadratic forms associated to the p-adic uniformization of a Shimura curve of discriminant $D_H = 2p$ and level $N = 1$, when p is a prime integer $p \equiv 1 \pmod 4$.

$B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $D_B = 2$, $p \equiv 1 \pmod 4$,

$\mathcal{O} := \mathbb{Z}[1, i, j, \rho]$, where $\rho := (1 + i + j + k)/2$,
$\mathcal{O}' := \mathbb{Z} + 2\mathcal{O} = \langle 1, 2i, 2j, 2\rho - \mathrm{Tr}(\rho)\rangle = \langle 1, 2i, 2j, \rho'\rangle$,
where $\rho' := i + j + k$,
$\mathcal{O}'[1/p] := \mathcal{O}' \otimes \mathbb{Z}[1/p]$,
$\mathrm{N}_{B,4} = X^2 + Y^2 + Z^2 + T^2$,
$\mathrm{N}_{\mathcal{O}',4} = X^2 + (2Y + T)^2 + (2Z + T)^2 + T^2$.
For every $\alpha = x+y(2i)+z(2j)+t\rho' = x+(2y+t)i+(2z+t)j+tk \in \mathcal{O}'[1/p]$,

$$\alpha \in B_0 \iff x = 0.$$

Therefore we can write the ternary normic form associated to the order $\mathcal{O}'_B$:
$\mathrm{N}_{\mathcal{O}',3}(X, Y, Z) = (2X + Z)^2 + (2Y + Z)^2 + Z^2$,
The p-adic immersion we associate to the algebra B is, as usual,

$$\begin{array}{lccc} \Phi_p : & B & \longrightarrow & \mathrm{M}_2(\mathbb{Q}_p) \\ & x_0 + x_1 i + x_2 j + x_3 k & \longmapsto & \begin{pmatrix} x_0 + x_1\sqrt{-1} & x_2 + x_3\sqrt{-1} \\ -(x_2 - x_3\sqrt{-1}) & x_0 - x_1\sqrt{-1} \end{pmatrix}. \end{array}$$

and then for every $\alpha = (2y + t)i + (2z + t)j + tk \in \mathcal{O}'[1/p] \cap B_0$ we have

$$\Phi_p(\alpha) = \begin{pmatrix} (2y + t)\sqrt{-1} & 2z + t + t\sqrt{-1} \\ -(2z + t - t\sqrt{-1}) & -(2y + t)\sqrt{-1} \end{pmatrix},$$

$$f_{\Phi_p(\alpha)} = (-(2z + t) + t\sqrt{-1}, -2(2y + t)\sqrt{-1}, -(2z + t) - t\sqrt{-1}x) \in \mathbb{Z}[1/p][\sqrt{-1}][X, Y].$$

So putting

$$a := -(2z + t), \quad b := t, \quad c := -(2y + t),$$

we see that $a, b, c \in \mathbb{Z}[1/p]$ and they satisfy the following congruent relations:

$$b + c \equiv a + b \equiv 0 \,(\mathrm{mod}\, 2).$$

Let $\mathcal{O}_{K,m}$ be an order of conductor m in a quadratic field $K = \mathbb{Q}(\sqrt{d})$ of discriminant D_K, such that $\left(\frac{D_K}{p}\right) = -1$ and $D_K < 0$.

Since the determinant of the quadratic form $f_{\Phi_p(\alpha)}$ is clearly

$$\det(f_{\Phi_p(\alpha)}) = \mathrm{Nm}(\alpha) = a^2 + b^2 + c^2,$$

we can write the set of binary quadratic forms associated to the order $\mathcal{O}[1/p]$ and having discriminant $-m^2D_K$:

$$\mathcal{H}_p(\mathcal{O}'[1/p], \mathcal{O}_{K,m}[1/p]) = \{(a+b\sqrt{-1}, 2c\sqrt{-1}, a-b\sqrt{-1}) \mid \\ b+c \equiv a+b \equiv 0 \,(\mathrm{mod}\, 2),\ a^2+b^2+c^2 = -m^2D_K\}.$$

We now compute the subset of $(\mathcal{O}[1/p], \mathcal{O}_{K,m}[1/p])$-primitive forms.

As shown in the proof of Theorem 4.1.12, every primitive representation $(x,y,z) \in \mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2D_K; \mathbb{Z}[1/p])$, gives a pure quaternion

$$\alpha = (2x+z)i + (2y+z)j + zk \in B$$

of norm $\mathrm{Nm}(\alpha) = \mathrm{N}_{O'[1/p],3}(x,y,z) = -m^2D_K$, so the associated binary quadratic form

$$f_{\Phi_p(\alpha)} = (-(2y+z) + z\sqrt{-1}, -2(2x+z)\sqrt{-1}, -(2y+z+z\sqrt{-1})),$$

has determinant $\det(f_{\Phi_p(\alpha)}) = -m^2D_K$.

Note that the optimal embedding $\varphi \in \mathcal{E}^*(\mathcal{O}_{K,m}[1/p], \mathcal{O}[1/p])$ corresponding to the representation $(x,y,z) \in \mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_B,3}, -4m^2d; \mathbb{Z}[1/p])$ is then defined by

$$\begin{cases} \varphi(m\sqrt{d}) := \dfrac{\alpha}{2}, & \text{if } d \equiv 2,3 \,(\mathrm{mod}\, 4) \\ \\ \varphi\left(m\dfrac{1+\sqrt{d}}{2}\right) := \dfrac{m}{2} + \dfrac{\alpha}{2}, & \text{if } d \equiv 1 \,(\mathrm{mod}\, 4) \end{cases}$$

(cf. these expressions with the ones given in [AB04, Corollary 4.27, Theorem 4.28, Theorem 4.53]).

Finally, putting

$$a := -(2y+z), \quad b := z, \quad c := -(2x+z),$$

we have that

$$\mathcal{H}_p^*(\mathcal{O}'_B[1/p], \mathcal{O}_{K,m}[1/p]) = \\ = \{(a+b\sqrt{-1}, 2c\sqrt{-1}, a-b\sqrt{-1}) \in \mathcal{H}_p(\mathcal{O}'_B[1/p], \mathcal{O}_{K,m}[1/p]) \mid \\ ((a+b)/2, (c+b)/2, b) = \mathbb{Z}[1/p]\}.$$

Computing the set of zeros of the forms of the family we find that the set of p-imaginary multiplication parameters $\mathrm{CM}_p(2,1,d,m)$ is the the set of $\Gamma_p(2,1)$-equivalence classes of the set of points

$$\left\{ \frac{(2x+z)\sqrt{-1} \pm m\sqrt{D_K}}{-(2y+z)+z\sqrt{-1}} \in \mathcal{H}_p(\mathbb{Q}_{p^2}) \mid (x,y,z) \in \mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2D_K; \mathbb{Z}[1/p]) \right\},$$

or equivalently of the set of points

$$\{\frac{-c\sqrt{-1}\pm m\sqrt{D_K}}{a+b\sqrt{-1}}\in\mathcal{H}_p(\mathbb{Q}_{p^2})\mid (a,b,c)\in\mathbb{Z}[1/p]^3,\ a^2+b^2+c^2=-m^2D_K \\ ((a+b)/2,(c+b)/2,b)=\mathbb{Z}[1/p]\}.$$

4.2.13 Example. In this example we compute families of quadratic forms associated to the p-adic uniformization of a Shimura curve of discriminant $D=3p$ and level $N=1$, when p is a prime $p\equiv 1\,(\mathrm{mod}\,4)$.

$B=\left(\frac{-1,-3}{\mathbb{Q}}\right)$, $D_B=3$, $p\equiv 1\,(\mathrm{mod}\,4)$,

$\mathcal{O}:=\mathbb{Z}[1,i,\lambda,\mu]$, where $\lambda:=(i+j)/2, \mu:=(1+k)/2$,

$\mathcal{O}':=\mathbb{Z}+2\mathcal{O}=\langle 1,2i,2\lambda,2\mu-\mathrm{Tr}\,\mu\rangle=\langle 1,2i,i+j,k\rangle$,

$\mathcal{O}'[1/p]:=\mathcal{O}'\otimes\mathbb{Z}[1/p]$,

$\mathrm{N}_{B,4}=X^2+Y^2+3Z^2+3T^2$,

$\mathrm{N}_{\mathcal{O}',4}=X^2+(2Y+Z)^2+3Z^2+3T^2$

For every $\alpha=x+y(2i)+z(i+j)+tk=x+(2y+z)i+zj+tk\in\mathcal{O}'[1/p]$,

$$\alpha\in\mathcal{O}'[1/p]\cap B_0\iff x=0,$$

and so

$\mathrm{N}_{\mathcal{O}',3}(X,Y,Z)=(2X+Y)^2+3Y^2+3Z^2$

$$\begin{array}{rccc}\Phi_p: & B & \longrightarrow & \mathrm{M}_2(\mathbb{Q}_p)\\ & x_0+x_1i+x_2j+x_3k & \longmapsto & \begin{pmatrix}x_0+x_1\sqrt{-1} & x_2+x_3\sqrt{-1}\\ -3(x_2-x_3\sqrt{-1}) & x_0-x_1\sqrt{-1}\end{pmatrix}.\end{array}$$

For every $\alpha=(2y+z)i+zj+tk\in\mathcal{O}'[1/p]\cap B_0$ we have

$$\Phi_p(\alpha)=\begin{pmatrix}(2y+z)\sqrt{-1} & z+t\sqrt{-1}\\ -3(z-t\sqrt{-1}) & -(2y+z)\sqrt{-1}\end{pmatrix},$$

$$f_{\Phi_p(\alpha)}=(-3(z-t\sqrt{-1}),-2(2y+z)\sqrt{-1},-(z+t\sqrt{-1}))\\ \in\mathbb{Z}[1/p][\sqrt{-1}][X,Y]$$

So putting

$$a:=-z,\quad b:=t,\quad c:=-(2y+z),$$

we see that $a, b, c \in \mathbb{Z}[1/p]$ and they satisfy $a + c \equiv 0 \pmod 2$.

Let $\mathcal{O}_{K,m}$ be an order of conductor m in a quadratic field $K = \mathbb{Q}(\sqrt{d})$ of discriminant D_K, such that $\left(\frac{D_K}{p}\right) = -1$ and $D_K < 0$.

$$\mathcal{H}_p(\mathcal{O}'[1/p], \mathcal{O}_{K,m}[1/p]) = \{(3(a + b\sqrt{-1}), 2c\sqrt{-1}, a - b\sqrt{-1})) \mid a + c \equiv 0 \pmod 2\, a^2 + 3b^2 + 3c^2 = -m^2 D_K\}$$

Given a primitive representation $(x, y, z) \in \mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2 D_K; \mathbb{Z}[1/p])$,

$$\alpha = (2x + y)i + yj + zk \in \mathcal{O}'[1/p] \cap B_0$$

is a pure quaternion of norm $\mathrm{Nm}(\alpha) = \mathrm{N}_{O'[1/p],3}(x, y, z) = -m^2 D_K$ and the associated binary quadratic form

$$f_{\Phi_p(\alpha)} = [-3(y - z\sqrt{-1}), -2(2x + y)\sqrt{-1}, -(y + z\sqrt{-1})],$$

has determinant $\det(f_{\Phi_p(\alpha)}) = -m^2 D_K$.

Putting

$$a := -y, \quad b := z, \quad c := -(2x + y),$$

we have that

$$\mathcal{H}^*_p(\mathcal{O}'_B[1/p], \mathcal{O}_{K,m}[1/p]) = \\ = \{([3(a + b\sqrt{-1}), 2c\sqrt{-1}, a - b\sqrt{-1})] \in \mathcal{H}_p(\mathcal{O}'_B[1/p], \mathcal{O}_{K,m}[1/p]) \mid ((a + c)/2, b, c) = \mathbb{Z}[1/p]\}.$$

Computing the zeros of this family of forms we find the set of p-imaginary multiplication parameters $\mathrm{CM}_p(3, 1, d, m)$.

This is the set of $\Gamma_p(3, 1)$-equivalence classes of the set of points

$$\left\{ \frac{(2x + y)\sqrt{-1} \pm m\sqrt{D_K}}{-3(y - z\sqrt{-1})} \in \mathcal{H}_p(\mathbb{Q}_{p^2}) \mid (x, y, z) \in \mathrm{Rep}^*(\mathrm{N}_{\mathcal{O}'_B,3}, -m^2 D_K; \mathbb{Z}[1/p]) \right\},$$

or equivalently of the set of points

$$\{ \frac{-c\sqrt{-1} \pm m\sqrt{D_K}}{3(a + b\sqrt{-1})} \in \mathcal{H}_p(\mathbb{Q}_{p^2}) \mid (c, a, b) \in \mathbb{Z}[1/p]^3,\, c^2 + 3a^2 + 3b^2 = -m^2 D_K \\ ((a + c)/2, b, c) = \mathbb{Z}[1/p], \}.$$

Appendix A

Resum en Català

Bibliography

[AALW07] A. Alaca, S. Alaca, M. F. Lemire, and K. S. Williams, *Nineteen quaternary quadratic forms*, Acta Arithmetica **130** (2007), no. 3, 277–310. ↑3.2.4

[AB04] M. Alsina and P. Bayer, *Quaternion orders, quadratic forms, and Shimura curves*, CRM Monograph Series, vol. 22, AMS, 2004. ↑(document), 1.1.1, 2.3.1, 3.2.1, 4, 4.1.1, 4.1.1, 4.1.1, 4.1.1, 4.1.1, 4.1.1, 4.1.2, 4.1.2, 4.2.1, 4.2.1, 4.2.1, 4.2.2, 4.2.2, 4.2.2, 4.2.2, 4.2.12

[BC91] J.-F. Boutot and H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld*, Astérisque **196-197** (1991), 45–158. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). ↑(document), 2.2, 2.2.2.2, 1

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265. ↑1.3.3

[BD98] M. Bertolini and H. Darmon, *Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization*, Inventiones Math. **131** (1998), 453–491. ↑(document)

[BG05] P. Bayer and J. Guàrdia, *On equations defining fake elliptic curves*, Journal de Théorie des nombres de Bordeaux **17** (2005), no. 1, 57–67. ↑(document), 1.3.7, 1.3.3, 1.3.3, 1.3.3.2

[BGR84] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean analysis: a systematic approach to rigid analytic geometry*, Grundlehren der mathematischen Wissenschaften, vol. 261, Springer, 1984. ↑2.1.1, 2.1.1, 2.1.11, 2.1.2, 2.1.3, 2.2.1, 2.2.1, 2.2.1

[Bos08] S. Bosch, *Lectures on formal and rigid geometry*, Mathematisches Institut der Universität Münster, 2008. ↑2.2.1

[BR14] P. Bayer and D. Remón, *A reduction point algorithm for cocompact Fuchsian group and applications*, Adv. Math. Commun. **8** (2014), 223–239. ↑(document)

[BT07] P. Bayer and A. Travesa, *Uniformizing functions for certain Shimura curves, in the case $D = 6$*, Acta Arithmetica **126** (2007), 315–339. ↑(document)

[BT08] ———, *On local constants associated to arithmetical automorphic functions*, Pure and Applied Mathematics Quaterly. Special Issue: In honor of Jean-Pierre Serre **1** (2008), 1107–1132. ↑(document)

[Cer76a] I. V. Cerednik, *Towers of algebraic curves uniformized by discrete subgroups of* $\mathrm{PGL}_2(k_w) \times E$, Math. USSR Sbornik **28** (1976), no. 2. ↑(document), 3.1.1

[Cer76b] ———, *Uniformization of algebraic curves by discrete aithmetic subgroups of* $\mathrm{PGL}_2(k_w)$ *with compact quotients*, Math. USSR Sbornik **29** (1976), no. 1, 55–78. ↑(document), 3.1, 3.1.1, 3.1.1

[Dar03] H. Darmon, *Rational points on modular elliptic curves*, AMS, 2003. ↑(document), 2.2

[Del71] P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki Exp. 389. Lecture Notes in Mathematics **244** (1971), 123–165. ↑1.2

[Dri76] V. G. Drinfeld, *Coverings of p-adic symmetric regions*, Functional Analysis and Its Applications **10** (1976), no. 2, 107–115. ↑(document), 3.1.2

[dVP14] C. de Vera Piquero, *Rational points on Shimura curves and Galois representations*, PhD Thesis, 2014. ↑3.1.19

[Eic37] M. Eichler, *Bestimmung de Idealklassenzahl in gewissen normalen einfachen Algebren*, J. Reine Angew. Math. **176** (1937), 192–202. ↑(document), 1.1, 1.2.2

[Eic38a] ———, *Allgemeine Kongruenzklasseneinteilungen der Ideale einfachen Algebren über algebraischen Zahlkörpen und ihre l-Reihen*, J. Reine Angew. Math. **179** (1938), 227–251. ↑(document), 1.1, 1.1.1, 1.1.2

[Eic38b] ———, *Über die Idealklassenzahl hyperkomplexer Systeme*, Math. Z. **43** (1938), 481–494. ↑(document), 1.1, 1.1.1, 1.1.10, 1.1.1

[Eic55] ———, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), 127–151. ↑(document), 1.1, 1.1.10, 1.1.12, 4.1.2

[FM14] C. Franc and M. Masdeu, *Computing fundamental domains for the Bruhat-Tits tree for* $\mathrm{GL}_2(\mathbb{Q}_p)$*, p-adic automorphic forms, and the canonical embedding of Shimura curves*, LSM Journal of Computation in Mathematics **17** (2014), no. 01, 1–23. ↑(document)

[For51] L. R. Ford, *Automorphic functions*, Second Edition, AMS Chelsea Publishing, 1951. ↑3.2.1

[Gau96] C. F. Gauss, *Disquisicions aritmètiques (orig. Disquisitiones Arithmeticae)*, Edició en Català. Traducció de G. Pascual, Societat Catalana de Matemàtiques (IEC), 1996. ↑4

[Ger74] L. Gerritzen, *Zur nichtarquimedischen Uniformisierung von Kurven*, Math. Ann. **210** (1974), 321–337. ↑(document), 3.2.3, 3.2.1, 3.2.6

[Got59] E. Gottschling, *Explizite Bestimmung der Randflächen des Fundamentalbereiches des Modulgruppe zweiten Grades*, Math. Ann. **138** (1959), 103–124. ↑1.3.3.2

[GvDP80] L. Gerritzen and M. van Der Put, *Schottky groups and Mumford curves*, Lecture Notes in Mathematics, vol. 817, Springer, 1980. ↑(document), 2.3.1, 2.3.3, 3.2.1, 3.2.3, 3.2.1

[Hur96] A. Hurwitz, *Über die Zahlentheorie der Quaternionen*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **1896** (1896), 313–340. ↑(document), 1.1.2, 1.1.2, 1.1.2, 1.1.2.1, c

[Iha66a] Y. Ihara, *Algebraic curves mod* $\mathfrak{p}$ *and arithmetic groups*, Proceedings of Symposia in Pure Mathematics **9** (1966), 265–271. ↑2.3.2, 3.1

[Iha66b] ———, *On discrete subgroups of the two by two projective linear group over* $\mathfrak{p}$ *-adic fields*, J. Math. Soc. Japan **18** (1966), no. 3. ↑3.1

[Iha67] ———, *On congruence monodromy problems*, MSJ Memoirs, Mathematical Society of Japan Memoirs, 1967. ↑3.1

[Iha68] ———, *The congruence monodromy problems*, J. Math. Soc. Japan **20** (1968), no. 1-2. ↑3.1

[JL84] B. W. Jordan and R. A. Livné, *Local diophantine properties of Shimura curves*, Math. Ann. **270** (1984), no. 2, 235–248. ↑3.1.2

[Kne62] M. Kneser, *Approximationssätze für algebraische Gruppen*, J. Reine Angew. Math. **209** (1962), 96–97. ↑1.1.1

[Kne65] ———, *Starke Approximation in algebraischen Gruppen*, J. Reine Angew. Math. **218** (1065), 190–203. ↑1.1.1

[Kur79] A. Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Univ. Tokyo, Sect. IA Math **25** (1979), no. 3, 277–300. ↑(document), 2.2.22, 3.3, 3.3.1, 3.3.1

[LB92] H. Lange and Ch. Birkenhake, *Complex abelian varieties*, Grundlehren der mathematischen Wissenschaften, vol. 302, Springer, 1992. ↑1.3.1, 1.3.3

[Lio60] J. Liouville, *Sur la forme* $x^2 + y^2 + 3(z^2 + t^2)$. Journal de mathématiques pures et appliquées **2e série** (1860), no. 5, 147–152. ↑3.2.4

[Mil04] J.S. Milne, *Introduction to shimura varieties*, Notes, 2004. ↑1.2.4

[Mil15] P. Milione (ed.) *Uniformització p-àdica de corbes de g'enere* $g \geq 2$, Notes del Seminari de Teoria de Nombres de Barcelona (UB-UAB-UPC), 2015. ↑2.3.3

[Mum08] D. Mumford, *Abelian varieties*, Vol. 5, Tata Institute of Fundamental Research, Bombay, 2008. ↑1.3.2

[Mum72] ———, *An analytic construction of degenerating curves over complete local rings*, Compositio Math. **24** (1972), 129–174. ↑(document), 2.2, 2.2.25, 2.3.3, 2.3.17, 2.3.3, 2.3.20, 2.3.3, 3.1

[Neu99] J. Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer, 1999. ↑1.1.1, 1.2.2, 1.2.4, 2.2, 4

[Nua15] J. Nualart, *Shimura curves and automorphic forms*, PhD Thesis, 2015. ↑(document)

[O'M71] O. T. O'Meara, *Introduction to quadratic forms*, Second Printing, Corrected, Grundlehren der mathematischen Wissenschaften, vol. 117, Springer, 1971. ↑1.2.2

[Rot04] V. Rotger, *Modular Shimura varieties and forgetful maps*, Trans. Amer. Math. Soc. **356** (2004), no. 4, 1535–1550. ↑1.3.3.2

[Sel60] A. Selberg, *On discontinous groups in higher dimensional symmetric spaces*, Contribution to function theory, Tata Institute of Fundamental Research (1960), 147–164. ↑2.3.3

[Ser70] J.P. Serre, *Cours d'arithmétique*, Collection Sup, Presses Universitaires de France, 1970. ↑1.2.2

[Ser77] J. P. Serre, *Arbres, amalgames,* SL_2. Cours au Collège de France, rédigé avec la collaboration de Hyman Bass, Astérisque, vol. 46, Société Mathèmatique de France, 1977. ↑2.2.2.1, 2.2.21, 2.3.2

[Shi63] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions*, Annals of Mathematics **78** (1963), no. 1, 149–192. ↑1.3.1, 1.3.1, 1.3.7

[Shi67] ———, *Construction of class fields and Zeta functions of algebraic curves*, Annals of Mathematics **85** (1967), no. 1, 58–159. ↑(document), 1.2, 1.2.1, 1.2.1, 1.2.8, 1.2.3, 1.2.3, 1.2.3, 1.2.19, 1.3.1, 4.1.1

[Shi70a] ———, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, 1970. ↑1.2.1, 1.2.4, 1.2.4, 2.2.2.3, 2.3.1, 3.2.2

[Shi70b] ———, *On canonical models of arithmetic quotients of bounded symmetric domains*, Annals of Mathematics **91** (1970), no. 1, 144–222. ↑(document), 1.2, 1.2.8

[Shi70c] ———, *On canonical models of arithmetic quotients of bounded symmetric domains: II*, Annals of Mathematics **92** (1970), no. 3, pp. 528–549. ↑(document), 1.2, 1.2.8

[Shi78] T. Shioda, *The period map of abelian surfaces*, J. Fac. Sci. Univ. Tokyo, Sect. IA Math. **25** (1978), no. 1. ↑1.3.3

[Sil94] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994. ↑4

[SM74] T. Shioda and N. Mitani, *Singular abelian surfaces and binary quadratic forms*, Lecture Notes in Mathematics **412** (1974), 259–287. ↑(document), 1.3.2, 1.3.3

[SS91] P. Schneider and U. Stuhler, *The cohomology of p-adic symmetric domains*, Inv. Math. **105** (1991), no. 1, 47–122. ↑2.2, 2.2.1

[Tat71] J. Tate, *Rigid analytic spaces*, Inv. Math. **12** (1971), 257–289. ↑(document), 2.1.2

[Vig80] M. F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, 1980. ↑1.1, 1.1.2, 1.1.1, 1.1.1, 1.1.15, 1.2.2, 2.2.2.4, 4.1.1, 4.1.2