Equations for arithmetic pointed tori

Thesis committee:
Prof. dr. P. Bayer, Universitat de Barcelona
Prof. dr. G. L. M. Cornelissen, Universiteit Utrecht
Prof. dr. S. J. Edixhoven, Universiteit Leiden
Prof. dr. M. van der Put, Rijksuniversiteit Groningen
Dr. J. Voight, University of Vermont

Cover: The white pattern on the foreground of the cover consists of the edges of part of the quadrilateral tiling of the upper half-plane constructed in Section 1.2 for the arithmetic $(1; e)$-group e2d1D6i (see the Appendix for this notation). The blue background contains the octagonal tiling associated with the group e3d1D6ii, as constructed in Section 1.3.

ISBN: 978-90-393-5373-8.
Printed by Wöhrmann Print Service, Zutphen.

Equations for arithmetic pointed tori

Vergelijkingen voor arithmetische gepunte tori

(met een samenvatting in het Nederlands)

Proefschrift

ter verkrijging van de graad van doctor aan de Universiteit Utrecht
op gezag van de rector magnificus, prof. dr. J. C. Stoof,
ingevolge het besluit van het college voor promoties
in het openbaar te verdedigen op maandag 30 augustus 2010
des middags te 4.15 uur

door

Jan Roelof Sijsling

geboren op 23 december 1983
te Arnhem

Promotor: Prof. dr. F. Beukers

Opgedragen aan mijn grootvader Jan Sijsling

For who would lose,
though full of pain, this intellectual being,
those thoughts that wander through eternity . . .

— John Milton, *Paradise Lost*

Contents

Introduction

Let $\mathrm{GL}_2^+(\mathbf{R})$ be group of matrices in $M_2(\mathbf{R})$ whose determinant is positive, and let $\mathrm{PGL}_2^+(\mathbf{R})$ be the quotient of $\mathrm{GL}_2^+(\mathbf{R})$ by its center $\mathbf{R}^\times$. Denoting the group of holomorphic automorphisms of the complex upper half-plane $\mathcal{H}$ by $\mathrm{Aut}(\mathcal{H})$, one has the well-known isomorphism

$$\begin{aligned} \mathrm{PGL}_2^+(\mathbf{R}) &\xrightarrow{\sim} \mathrm{Aut}(\mathcal{H}) \\ \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] &\longmapsto \left(z \mapsto \frac{az+b}{cz+d}\right). \end{aligned}$$

Let Γ be a Fuchsian group of the first kind, that is, a discrete subgroup of $\mathrm{PGL}_2^+(\mathbf{R})$ of finite covolume. Then the group Γ acts on $\mathcal{H}$, and one can consider the quotient

$$Y(\Gamma) = \Gamma\backslash\mathcal{H}.$$

This thesis is devoted to studying these quotients and their arithmetic nature for a special finite list of $\mathrm{PGL}_2^+(\mathbf{R})$-conjugacy classes of Γ cut out by a rather restrictive set of conditions, as in [Tak83]. The greater part of this introduction is dedicated to describing these conditions and to giving a broader overview by relating them to several congruent areas of mathematics. After this, we describe our study of the resulting list.

Lamé equations

The first conditions that we impose on Γ are of a geometric nature: we demand that

- The quotient $Y(\Gamma)$ is compact and of genus 1; and
- The ramification locus of the canonical projection

  $$\mathcal{H} \xrightarrow{\pi} Y(\Gamma)$$

  consists of a single point P of $Y(\Gamma)$, where π ramifies with index $e \geq 2$.

In the terminology of [Bea95], Γ is a Fuchsian group of signature $(1; e)$. Being a compact Riemann surface, $Y(\Gamma)$ has an algebraic structure: in fact, because of the compactness condition, it is a projective algebraic curve over $\mathbf{C}$. It has a distinguished point, namely P. We are therefore justified in calling $Y(\Gamma)$ a *pointed complex torus*, although in the rest of this thesis, we will usually refer to it as a $(1;e)$-*curve*.

Our motivation for considering such Γ and $Y(\Gamma)$ is the following. Consider the multivalued inverse map

$$Y(\Gamma) \overset{\pi^{-1}}{\dashrightarrow} \mathcal{H}.$$

This inverse map is intimately related to a differential equation on $Y(\Gamma)$. Indeed, choose a Weierstrass equation

$$y^2 = p(x)$$

for $Y(\Gamma)$ such that P is the point at infinity. Then π^{-1} can be described as the quotient of two solutions of the *Lamé differential equation*

$$\left[(y\frac{d}{dx})^2 - (n(n+1)x + A)\right] u = 0 \tag{0.1}$$

on $Y(\Gamma)$. Here we denote

$$n = \frac{1}{2e} - \frac{1}{2} < 0,$$

and $A \in \mathbf{C}$ is an *accessory parameter*. This differential equation has exactly one singular point, given by P, which is regular singular.

Lamé equations can be thought of as being the simplest higher genus analogue of the *hypergeometric differential equations*

$$\left[x(1-x)\frac{d^2}{dx^2} + (c - (a+b+1)x)\frac{d}{dx} - ab\right] u = 0 \tag{0.2}$$

(with $a, b, c \in \mathbf{C}$) on $\mathbf{P}^1$. These hypergeometric equations describe similar multivalued inverse maps

$$Y(\Delta) \dashrightarrow \mathcal{H},$$

namely those arising from *triangle groups* Δ, which are the Fuchsian groups whose signature equals $(0; p, q, r)$ for some $p, q, r \in \mathbf{Z}_{\geq 2}$.

The presence of the extra parameter A in the Lamé equation (0.1) is a new feature that does not occur in the hypergeometric case: like the parameter n in (0.1), the parameters a, b and c in (0.2) are determined by the signature $(0; p, q, r)$ of the associated triangle group Δ.

We now turn to the second demand on Γ that relates these groups to a classical construction due to Shimura.

Arithmeticity

The geometric demands above are satisfied by a continuum of discrete groups $\Gamma \subset \mathrm{PGL}_2^+(\mathbf{R})$, even up to conjugacy. Indeed, let E be an elliptic curve, and let $e \in \mathbf{Z}_{\geq 2}$ be an integer. Consider the maximal cover

$$\widetilde{E}_e \longrightarrow E \tag{0.3}$$

that is unramified outside the origin O of E and such that all ramification indices over O divide e. Then $\widetilde{E}_e$ inherits a complex structure, and as in Section 6.4 of [Ser92], one sees that

- $\widetilde{E}_e$ is isomorphic to $\mathcal{H}$; and
- The map in (0.3) is isomorphic to a projection map $\mathcal{H} \to Y(\Gamma)$.

By construction, then, Γ is of the type considered in the previous paragraph. For a more explicit study of the totality of these groups, we refer to Chapter 1 and [FK65].

We shall consider a smaller class of Γ. Classically, some of the most rewarding subgroups of $\mathrm{PGL}_2^+(\mathbf{R})$ have been the groups

$$\Gamma_0(N) = \left\{ \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right] \in \mathrm{PSL}_2(\mathbf{Z}) : c \equiv 0 \pmod{N} \right\}.$$

The corresponding curves $Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}$ have a moduli interpretation, parametrizing elliptic curves equipped with a cyclic N-isogeny. This moduli interpretation yields a model of $Y_0(N)$ over $\mathbf{Q}$, which can be compactified to yield a proper smooth curve $X_0(N)$ over $\mathbf{Q}$.

The Galois representations and Heegner points obtained from the curves $X_0(N)$ and their Jacobians are a treasure trove of arithmetic information, not least in light of the proof of the Shimura-Taniyama-Weil conjecture by Wiles, Taylor *et al.*

One can describe the groups $\Gamma_0(N)$ in a different way by using orders of the matrix algebra $M_2(\mathbf{Q})$ over $\mathbf{Q}$. This algebra has a maximal order $\mathcal{O}(1)$ given by $M_2(\mathbf{Z})$. Consider the element

$$w_N = \begin{pmatrix} 0 & 1 \\ N & 0 \end{pmatrix}$$

of $\mathcal{O}(1)$. Then we can form the order $\mathcal{O}(N)$ in $M_2(\mathbf{Q})$ given by

$$\mathcal{O}(N) = \mathcal{O}(1) \cap w_N \mathcal{O}(1) w_N^{-1} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) : c \equiv 0 \pmod{N} \right\}.$$

Using the order $\mathcal{O}(N)$, we can recover $\Gamma_0(N)$ in a more involved way as the image in $\mathrm{PGL}_2^+(\mathbf{R})$ of the group $\mathcal{O}(N)^+ \subset \mathrm{GL}_2^+(\mathbf{R})$ consisting of the matrices in $\mathcal{O}(N) \subset M_2(\mathbf{R})$ whose determinant is a totally positive unit of $\mathbf{Z}$ (that is, 1).

In analogy with the above, let F be a totally real number field, and let B be a quaternion algebra over F such that

$$B \otimes_{\mathbf{Q}} \mathbf{R} \cong M_2(\mathbf{R}) \times \mathbf{H} \times \cdots \times \mathbf{H}, \tag{0.4}$$

where $\mathbf{H}$ is the Hamilton quaternion algebra over $\mathbf{R}$. Let $\mathcal{O}$ be an order of B, and let $\mathcal{O}^+$ be the group of units of $\mathcal{O}$ with totally positive norm. Let $\mathrm{P}\mathcal{O}^+$ be the subgroup of $\mathrm{PGL}_2^+(\mathbf{R})$ associated to the image of $\mathcal{O}^+$ in the factor $M_2(\mathbf{R})$ in (0.4). One can then construct the curve

$$Y(\mathcal{O}^+) = \mathrm{P}\mathcal{O}^+\backslash\mathcal{H}.$$

In [Shi70], Shimura proves the existence of *canonical models* of the compactifications $X(\mathcal{O}^+)$ of these curves $Y(\mathcal{O}^+)$, which are analogues of the models of the curves $X_0(N)$ over $\mathbf{Q}$ considered above. When the quaternion algebra B is not isomorphic to a matrix algebra (which is the case, for example, when $F \neq \mathbf{Q}$), then we in fact have $X(\mathcal{O}^+) = Y(\mathcal{O}^+)$.

Shimura's canonical models are models (or forms) of $X(\mathcal{O}^+)$ over an abelian extension of F, which we describe in more detail in Chapter 3. As in the classical case, the study of the Galois representations associated to $X(\mathcal{O}^+)$ has borne a lot of fruit (see [HT01]).

A subgroup Γ of $\mathrm{PGL}_2^+(\mathbf{R})$ is called *arithmetic* if it is commensurable with a group $\mathrm{P}\mathcal{O}^+$ as above, meaning that $\Gamma \cap \mathrm{P}\mathcal{O}^+$ has finite index in both Γ and $\mathrm{P}\mathcal{O}^+$. This arithmeticity condition is the second condition that we impose on Γ.

In terms of the Lamé equation (0.1), arithmeticity of Γ results in overconvergence of the local expansions of the solutions around a regular point. This in turn gives rise to special transcendental numbers. In fact, though we will not get into this, the construction of such transcendental numbers was one of the main motivations for our study of these groups Γ.

A list by Takeuchi

An *arithmetic* $(1;e)$*-group* is a Fuchsian group for which the demands of the previous sections are all satisfied. Up to $\mathrm{PGL}_2^+(\mathbf{R})$-conjugacy, this results in a finite list of 71 possible Γ, which was determined by Takeuchi in [Tak83]. Colloquially, we call the corresponding quotients $Y(\Gamma)$ *arithmetic pointed tori*. However, in the main text, we predominantly use the more accurate term *arithmetic* $(1;e)$*-curves* for these quotients.

Let Γ be an arithmetic $(1;e)$-group, and let A and B be matrices in $\mathrm{SL}_2(\mathbf{R})$ whose images in $\mathrm{PGL}_2^+(\mathbf{R})$ generate Γ and whose commutator is of finite order. We can describe the conjugacy class of the group Γ by giving the *trace triple*

$$(x, y, z) = (\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB)). \tag{0.5}$$

In [Tak83], the full list of arithmetic $(1;e)$-groups Γ is given in terms of trace triples. For these Γ, the compactification $X(\Gamma)$ of $Y(\Gamma)$ is simply equal to $Y(\Gamma)$.

The main objective of this thesis is to determine equations for these arithmetic pointed tori over number fields. Whenever possible, we realize $X(\Gamma)$ as a (possibly trivial) Atkin-Lehner quotient of a Shimura curve and determine the resulting canonical model of the Jacobian $J(\Gamma)$ of $X(\Gamma)$.

Our results can be found in Table A.3 in the appendix, where we give equations for $J(\Gamma)$ for 57 (out of 71) arithmetic $(1;e)$-groups Γ. In all other cases, we still give candidate curves or isogeny classes, whose correctness would follow from standard conjectures on Hilbert modular forms, such as the Fontaine-Mazur conjecture (*cf.* Section 7.2).

Previous results

The first explicit results on arithmetic pointed tori are due to Chudnovsky and Chudnovsky. In [CC89], they gave models for $X(\Gamma)$ over $\mathbf{C}$, along with the accessory parameter A from (0.1), for 13 of the groups in Takeuchi's list. Their results were obtained using numerical approximations: however, [CC89] does not prove the correctness of these models, and some of the accessory parameters are missing or seem incorrect.

For example, we approximated the accessory parameters in the two $(1;4)$-cases determined by Chudnovsky and Chudnovsky using a program kindly shared with us by Yifan Yang. The results agreed with the values $(-17+16\sqrt{2})/2^6$ and $(2-\sqrt{2})/2^4$ up to 50 decimals, which seems contrary to the cubic values claimed (but not calculated) in [CC89]. That said, the j-invariants claimed in [CC89] never contradict our results.

Other results on arithmetic pointed tori can be found among the results in the papers [Kra96], [Elk98] and [GR06]. These papers determine 5 of the 7 arithmetic $(1;e)$-curves whose corresponding quaternion algebras B have ground field F equal to $\mathbf{Q}$.

Outline

This thesis is organized as follows.

In **Chapter 1**, we use the geometry of Fuchsian groups to construct fundamental domains for the groups Γ in Takeuchi's list. As a result, we obtain an algorithm that given an element $\gamma \in \Gamma$ determines its homology class $[\gamma]$ in $H_1(X(\Gamma), \mathbf{Z}) \cong \Gamma^{\mathrm{ab}} \cong \mathbf{Z}^2$. Additionally, we show that the trace triples (0.5) used in Theorem 4.1 of [Tak83] give rise to certain optimally shaped fundamental domains for the corresponding group Γ.

Chapter 2 summarizes the results on quaternion algebras that we use in this thesis.

In **Chapter 3**, we discuss canonical models for Shimura curves and arithmetic pointed tori. We also consider the subgroups $\mathcal{O}^1$ of $\mathcal{O}^+$ consisting of elements of norm 1 and construct canonical models for the associated covers

$$Y(\mathcal{O}^1) = \mathrm{P}\mathcal{O}^1 \backslash \mathcal{H}$$

of the curves $Y(\mathcal{O}^+)$ considered above. It turns out in order to construct a canonical model for $Y(\mathcal{O}^1)$, one has to make a choice of compact open subgroup of the adèlic points of the algebraic group $B^\times$, and that the canonical model of $Y(\mathcal{O}^1)$ may depend on this choice.

Chapter 4 determines the traces of Frobenius of an arithmetic pointed torus $X(\Gamma)$ by calculating the action of a Hecke algebra on $H_1(X(\Gamma), \mathbf{Z})$. We give an algorithm that implements these calculations: it incorporates the algorithm from Chapter 1 described above.

In **Chapter 5**, we explore the consequences of a result of Boutot and Zink ([BZ]) and Varshavsky ([Var98]) generalizing a classical result due to Čerednik and Drinfel'd. We give an algorithm that returns a list of explicit candidate equations for a genus 1 Shimura curve coming from an Eichler order.

A special subclass of arithmetic pointed tori is considered in **Chapter 6**, namely those for which the corresponding group Γ is contained in a triangle group Δ. The corresponding morphism $X(\Gamma) \to X(\Delta)$ is calculated using the theory of Belyĭ maps, resulting in models over $\mathbf{C}$ for the curves $X(\Gamma)$.

Finally, we harvest our results: **Chapter 7** describes how to obtain canonical models for arithmetic pointed tori using the machinery developed in the previous Chapters.

The appendix gives two tables that we computed for use in our calculations, along with a third table summarizing our results in Chapter 7.

The algorithms that we developed and used in this thesis, and that form an important part of it, can be found at [Sij10]. These are to be used with the most recent version of `Magma` ([BCP97]), available at `http://magma.maths.usyd.edu.au/magma/`.

Notation and conventions

- The ring of integers of a number field or a non-archimedean local field F is denoted by $\mathbf{Z}_F$ throughout this thesis. The symbol $\mathcal{O}$ is reserved for quaternion orders.

  If $\mathfrak{p}$ is a prime of F, then we denote the norm of $\mathfrak{p}$ by $\mathrm{Nm}(\mathfrak{p})$. A uniformizer of the localization $\mathbf{Z}_{F,\mathfrak{p}}$ is usually denoted by π. If p is a prime number, then $\mathfrak{p}_p$ denotes a prime of $\mathbf{Z}_F$ over p.

- Let F be a totally real number field. Then we denote the group of totally positive units of F by F^+, and the group of totally positive units of $\mathbf{Z}_F$ by $\mathbf{Z}_F^+$.

- Let F be a field. By a *curve* over F we mean a smooth scheme X over F that is pure of dimension 1. We emphatically remark here that we do not insist on X being proper or connected. If X is a curve over a subfield of $\mathbf{C}$, then we denote the Riemann surface associated to X by $X(\mathbf{C})^{\mathrm{an}}$.

- Let G be a group. Let H be a subgroup of G and let X be a set with an action of G. We denote the center of G by $Z(G)$ and its abelianization by G^{ab}. Moreover, we let
  $$G^{\mathrm{ad}} = G/Z(G),$$
  the adjoint group. The image of H in G^{ad} will occasionally be denoted by $\mathrm{P}H$.

  The normalizer of H in G will be denoted by $N_G(H)$, or $N(H)$ if no confusion can arise, its centralizer by $\mathrm{Cent}_G(H)$ or $\mathrm{Cent}(H)$, and its core $\bigcap_{g\in G} gHg^{-1}$ by $\mathrm{C}_G(H)$ or $\mathrm{C}(H)$. For an element x of X, its stabilizer in G is denoted by $\mathrm{Stab}_G(x)$ or $\mathrm{Stab}(x)$.

- Let X be a set with a left action of the group G_1 and a right action of the group G_2. Let x be an element of X. Then the element of the double quotient $G_1\backslash X/G_2$ represented by x is denoted by $[x]$.
- The cardinality of a set S is denoted by $|S|$.
- For the notation that we shall introduce in the course of this thesis, we refer to the index of notation on page 163.

Chapter 1

Fundamental domains

In this Chapter, we define the notion of a $(1;e)$-group and the algebraic curves associated with them, which we shall call $(1;e)$-curves or pointed tori. Our main objective is the explicit construction of fundamental domains for $(1;e)$-groups.

After introducing the necessary tools from hyperbolic geometry in the first section, the second and third sections are devoted to this construction. Section 1.2 considers quadrilateral fundamental domains for $(1;e)$-groups. We show that Takeuchi's presentation of $(1;e)$-groups in [Tak83] gives rise to quadrilateral fundamental domains that are, in a quantifiable sense, of a more symmetric shape than other such domains.

Section 1.3 constructs Dirichlet domains for $(1;e)$-groups. In the final section, these Dirichlet domains are put to use in an algorithm that, given a $(1;e)$-group $\Gamma \subset \mathrm{PGL}_2^+(\mathbf{R})$ and an element γ of Γ, explicitly determines the homology class $[\gamma] \in H_1(\Gamma\backslash\mathcal{H}, \mathbf{Z})$. We will use this algorithm in Chapter 4 to calculate traces of Frobenius for certain Shimura curves.

1.1 Preliminaries

For the definitions and terminology from hyperbolic geometry used in this Chapter we refer to [Bea95] and the article [Voi09a]. Recall from the introduction that a *Fuchsian group of the first kind* is a discrete subgroup of $\mathrm{PGL}_2^+(\mathbf{R})$ whose covolume is finite.

Definition 1.1.1. *Let $e \in \mathbf{Z}_{\geq 2}$. A* $(1;e)$-group *is a Fuchsian group of the first kind $\Gamma \subset \mathrm{PGL}_2^+(\mathbf{R})$ with presentation*

$$\Gamma = \langle \alpha, \beta, \gamma \mid \gamma = [\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta,\ \gamma^e = 1 \rangle. \tag{1.1}$$

Using the notion of *signature* (as in Section 10.4 of [Bea95]), a $(1;e)$-group is simply a Fuchsian group of the first kind whose signature equals $(1;e)$. We refer to the introduction for a more geometric definition of $(1;e)$-groups.

Remarks. (i) $(1;e)$-groups should be considered as the most elementary class of Fuchsian groups of the first kind after triangle groups: along with these groups, they are the only Fuchsian groups of the first kind generated by two elements.

(ii) Note that by the Riemann mapping theorem, there is no such thing as a Fuchsian group of signature $(1;1)$.

We will often abuse notions by calling a subgroup of $\mathrm{SL}_2(\mathbf{R})$ or $\mathrm{GL}_2^+(\mathbf{R})$ projecting to a $(1;e)$-group in $\mathrm{PSL}_2(\mathbf{R}) \cong \mathrm{PGL}_2^+(\mathbf{R})$ a $(1;e)$-group as well.

Before beginning with the construction of fundamental domains for $(1;e)$-groups, we fix an isomorphism $\mathrm{PGL}_2^+(\mathbf{R}) \to \mathrm{PSU}_{(1,1)}(\mathbf{R})$. Given a matrix M in $\mathrm{PGL}_2^+(\mathbf{R})$, we define

$$\widetilde{M} = \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix} M \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}^{-1} \in \mathrm{PSU}_{(1,1)}(\mathbf{R}).$$

In what follows, we let $\mathrm{PGL}_2^+(\mathbf{R})$ act on the complex unit disc $\mathcal{D}$ through the composed isomorphism

$$\mathrm{PGL}_2^+(\mathbf{R}) \xrightarrow{M \mapsto \widetilde{M}} \mathrm{PSU}_{(1,1)}(\mathbf{R}) \longrightarrow \mathrm{Aut}(\mathcal{D}).$$

Henceforth, given $M \in \mathrm{PGL}_2^+(\mathbf{R})$, we abuse notation by writing Mz for $\widetilde{M}z$. Geometrically, the choice of isomorphism above comes down to fixing the conformal equivalence

$$\begin{aligned} \mathcal{H} &\xrightarrow{\sim} \mathcal{D} \\ z &\longmapsto \frac{z-i}{z+i}. \end{aligned}$$

This is exactly the equivalence obtained by setting $p = i$ in (1.1) of [Voi09a].

Let G be a subgroup of $\mathrm{PSU}_{(1,1)}(\mathbf{R})$, and let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be an element of G. Then the *isometric circle* $I(M)$ of M is given by

$$I(M) = \{z : |cz + d| = 1\}.$$

Denoting the exterior of an isometric circle $I(M)$ by $I(M)^{\mathrm{ext}}$, the *Dirichlet domain* centered at 0 for G is the fundamental domain for G given by

$$\bigcap_{M \in G} I(M)^{\mathrm{ext}} \subset \mathcal{D}.$$

Given a subgroup Γ of $\mathrm{PGL}_2^+(\mathbf{R})$, the choice of isomorphism $\mathrm{PGL}_2^+(\mathbf{R}) \to \mathrm{PSU}_{(1,1)}(\mathbf{R})$ made above allows us to unambiguously define the notion of a *Dirichlet domain based at* 0 for Γ: we define this to be the Dirichlet domain based at 0 for $\widetilde{\Gamma}$. Alternatively, this is the image of the similarly defined Dirichlet domain based at i for Γ under the isomorphism $\mathcal{H} \to \mathcal{D}$ given above.

We shall also use the following result:

Theorem 1.1.2 (Poincaré). *Let $P \subset \mathcal{D}$ be a compact convex polygon with a side pairing grouping the vertices of P into cycles. For a vertex v of P, denote by $\vartheta_P(v)$ the interior angle of P at v.*

Then P is a fundamental polygon for the group G generated by the side-pairing elements of P if and only if for every cycle C of P there exists an $e \in \mathbf{N}$ such that we have the following equality of angle sums:

$$\sum_{v \in C} \vartheta_P(v) = \frac{2\pi}{e}.$$

In addition, if this equality holds, then G is a Fuchsian group of the first kind.

Proof. See [Mas71]. □

1.2 Quadrilaterals

Let $\Gamma \subset \mathrm{PGL}_2^+(\mathbf{R}) \cong \mathrm{PSL}_2(\mathbf{R})$ be a $(1;e)$-group, and choose a presentation (1.1) for Γ. Let A, B be matrices in $\mathrm{SL}_2(\mathbf{R})$ lifting α, β respectively. Then if we denote the commutator $A^{-1}B^{-1}AB$ by $[A,B]$, we have $[A,B]^e = 1$ in $\mathrm{PGL}_2^+(\mathbf{R})$.

Let $(x,y,z) = (\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB))$: we call this the *trace triple* associated with the pair (A,B). A short verification or [Tak83] shows that we have the following equality:

$$x^2 + y^2 + z^2 - xyz - 2 = \mathrm{tr}([A,B]). \tag{1.2}$$

In particular, since $[A,B]$ is elliptic, this quantity is strictly between -2 and 2.

The first step towards the construction of a quadrilateral fundamental domain for Γ is to normalize A and B in a suitable way. In light of the presentation (1.1), A is hyperbolic. Hence after conjugating by a suitable element of $\mathrm{SL}_2(\mathbf{R})$, we have

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

with $|\lambda| > |\lambda^{-1}|$. Suppose that this conjugation transforms B to the matrix

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Proposition 1.2.1. *Let A and B be of the form above. Suppose $[A,B]$ is elliptic. Then we have:*

(i) b and c are non-zero and have the same sign;

(ii) a and d are non-zero and have the same sign.

Proof. Let (x,y,z) be the trace triple of the pair (A,B). One calculates

$$bc = ad - 1 = \frac{xyz - x^2 - y^2 - z^2 + 4}{x^2 - 4}.$$

Now the quantity $xyz - x^2 - y^2 - z^2 + 4$ is strictly larger than 0 because of (1.2). Since clearly $x^2 > 4$, both bc and $ad - 1$ are strictly positive, which concludes the proof. □

Let

$$D = \begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix} \in C_{\mathrm{SL}_2(\mathbf{R})}(A)$$

be an element of the maximal torus centralizing A. Then $DAD^{-1} = A$ and

$$DBD^{-1} = \begin{pmatrix} a & \delta^2 b \\ \delta^{-2}c & d \end{pmatrix}.$$

After choosing $\delta \in \mathbf{R}$ such that $\delta^2 = \sqrt{c/b}$, which is possible by Proposition 1.2.1(i), we see that up to simultaneous $\mathrm{SL}_2(\mathbf{R})$-conjugation, A and B are of the form

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{R}),\ B = \begin{pmatrix} a & b \\ b & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{R}). \tag{1.3}$$

By changing the signs of A and B if necessary, we can by virtue of Proposition 1.2.1 ensure that $\lambda > 1$ and $a, d > 0$. This normalization determines A and B uniquely as matrices in $\mathrm{SL}_2(\mathbf{R})$.

It is not necessarily the case that $b > 0$; however, this can be achieved by replacing B by B^{-1}. The matrices A and B^{-1} then still generate Γ. Their commutator $[A, B^{-1}]$ is Γ-conjugate to $[A, B]^{-1}$.

Definition 1.2.2. *A pair (A, B) as in (1.3) for which $\lambda > 1$ and $a, b, d > 0$ is called an* elliptic standard pair *(of* order *e) if in addition, the commutator $[A, B]$ is elliptic of order $e \geq 2$.*

Remark. Using (1.2), one calculates that the matrices constituting an elliptic standard pair are necessarily hyperbolic: *cf.* the discussion before Proposition 1.2.7.

Given a $(1; e)$-group Γ, the discussion before Definition 1.2.2 shows that, up to a suitable conjugation, Γ is generated by an elliptic standard pair (A, B), whose trace triple then satisfies the fundamental relation (1.2). Conversely, it is not hard to see that an elliptic standard pair (A, B) can be reconstructed from its trace triple (x, y, z), which will satisfy

$$x, y, z > 2 \text{ and } x^2 + y^2 + z^2 - xyz = 2 - 2\cos(n\pi/e),$$

for some n coprime to e. Moreover, any triple (x, y, z) satisfying these conditions gives rise to an elliptic standard pair (A, B). We will later derive a condition on triples (x, y, z) that will ensure that the associated pair (A, B) generates a $(1; e)$-group: see Theorem 1.2.5.

Now consider an elliptic standard pair (A, B), and let p be the fixed point of $[A, B]$ in $\mathcal{D}$. Then one can consider the points Ap, Bp and $ABp = BAp$. These points are elliptic, with stabilizers generated by $[B, A^{-1}]$, $[B^{-1}, A]$ and $[A^{-1}, B^{-1}]$ respectively.

Proposition 1.2.3. *Let (A, B) be an elliptic standard pair, and let p be the fixed point of $[A, B]$ in $\mathcal{D}$.*

(i) We have $ABp = -p$ and $Bp = -Ap$. Consequently, 0 is the center of the hyperbolic quadrilateral with vertex set $\{p, Ap, Bp, ABp\}$.

(ii) p, Ap, Bp and ABp are not on one line.

Proof. For any symmetric matrix M, one has the equality $M(-z) = -M^{-T}z = -M^{-1}z$. Therefore

$$ABA^{-1}B^{-1}(-p) = ABA^{-1}(-Bp) = \ldots = -A^{-1}B^{-1}ABp = -p,$$

so $-p$ is the fixed point of $ABA^{-1}B^{-1} = [A^{-1}, B^{-1}]$, hence equals $BAp = ABp$. A similar argument proves $Bp = -Ap$.

(ii) Since A and B are hyperbolic, the four points are distinct. The matrix A transforms the segment $\{p, Bp\}$ into $\{Ap, ABp\}$, and B transforms the segment $\{p, Ap\}$ into $\{Bp, BAp\} = \{Bp, ABp\}$.

Therefore, if the four points were on a line, then the geodesic that passes through them would be fixed by A as well as B. This would imply that either A and B commute or either A or B is elliptic. The former possibility is ruled out by the hypothesis $e \geq 2$, and the latter by the remark after Definition 1.2.2 regarding hyperbolicity of A and B. □

Remark. Proposition 1.2.3(i) shows the geometric significance of standard pairs: non-standard pairs (A, B) with elliptic commutator will not in general have 0 in the center of the aforementioned hyperbolic quadrilateral.

The convex hyperbolic quadrilateral Q with vertex set $\{p, Ap, Bp, ABp\}$ as in the proposition is called the quadrilateral *associated with* the pair (A, B). We now consider whether Q is a fundamental domain for the group generated by A and B. First we prove the following

Lemma 1.2.4. *Let (A, B) be an elliptic standard pair, and write*

$$\operatorname{tr}([A, B]) = -2\cos(\pi n/e),\ (n, e) = 1,\ 0 < n < e.$$

Then the sum of the interior angles of the quadrilateral Q associated with (A, B) equals $2\pi n/e$.

Proof. Consider the translates Q, AQ, BQ and BAQ of Q. The intersection $AQ \cap Q$ is given by the segment $\{Ap, ABp\}$, $BQ \cap Q$ by the segment $\{Bp, ABp\}$, and $BQ \cap BAQ$ by $\{BAp, BABp\}$. Note that $A \cdot 0$ is to the right of 0 because we have $\lambda > 1$.

Starting with a point close to $ABp = BAp$ on the segment $\{BAp, BABp\}$ bounding BAQ and rotating clockwise, we therefore stay inside of $Q \cup AQ \cup BQ \cup ABQ$ until we meet the segment $\{ABp, A^2Bp\}$ bounding AQ. Figure 1.1 has been added for clarification.

During this clockwise turn, we meet translates of all the angles occuring at the vertices of Q. Consequently, the total angle that is traversed clockwise equals

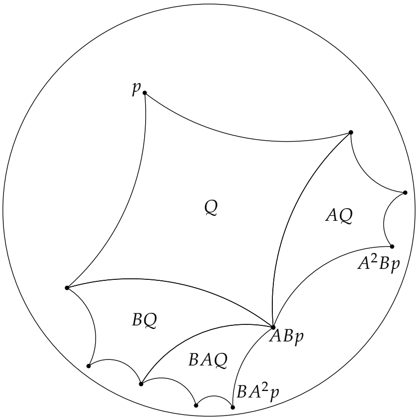


Figure 1.1: An example of $Q \cup AQ \cup BQ \cup BAQ$ with $e = 5, n = 2$.

the angle sum of Q, which we abbreviate by Σ. A matrix inducing this clockwise rotation is given by $[A^{-1}, B^{-1}]$, since this commutator fixes $ABp = BAp$ and sends BA^2p to $ABAp = A^2Bp$.

Therefore $[A^{-1}, B^{-1}]$, hence also the conjugate matrix $[A, B]$, should induce a clockwise rotation about the angle Σ. This implies that $[A, B]$ is $\mathrm{SL}(2, \mathbf{R})$-conjugate to one of the following matrices:

$$\begin{pmatrix} \cos(\Sigma/2) & -\sin(\Sigma/2) \\ \sin(\Sigma/2) & \cos(\Sigma/2) \end{pmatrix} \text{ or } \begin{pmatrix} -\cos(\Sigma/2) & \sin(\Sigma/2) \\ -\sin(\Sigma/2) & -\cos(\Sigma/2) \end{pmatrix}.$$

Since $0 < \Sigma < 2\pi$, we have $\sin(\Sigma/2) > 0$. Now on the hand, this inequality implies that all $\mathrm{SL}_2(\mathbf{R})$-conjugates of the matrix on the left (respectively right) given above all have negative (respectively positive) upper left corner. On the other hand, one can explicitly check that for a standard pair (A, B), the commutator $[A, B]$ has positive upper right corner.

Hence we can conclude that $[A, B]$ is conjugate to the second matrix above. Consequently $\mathrm{tr}([A, B]) = -2\cos(\Sigma/2)$, proving the lemma. □

Theorem 1.2.5. *Let (A, B) be an elliptic standard pair of order e. Let Q be the quadrilateral associated with (A, B). Write*

$$\mathrm{tr}([A, B]) = -2\cos(\pi n/e),\ (n, e) = 1,\ 0 < n < e.$$

The group Γ generated by A and B is a $(1; e)$-group if and only if $n = 1$. Moreover, if Γ is a $(1; e)$-group, then Q is a fundamental domain for Γ, and up to translation, all quadrilateral fundamental domains for Γ are associated with some elliptic standard pair (A', B').

Proof. If n equals 1, then the angle sum of Q equals $2\pi/e$ by Lemma 1.2.4. As $2\pi/e \leq \pi$, the quadrilateral Q is also convex. Since by construction, the vertices of Q from a single cycle, the conditions for Poincaré's Theorem 1.1.2 are all fulfilled. Therefore, Q is a fundamental domain for the Fuchsian group of the first kind generated by its side pairings.

The matrix A clearly pairs the side $\{p, Bp\}$ to $\{Ap, ABp\}$, and B pairs $\{p, Ap\}$ to $\{Bp, ABp\}$. Consequently, the group generated by the side pairings of Q equals $\langle A, B\rangle = \Gamma$, which is therefore a $(1;e)$-group considering that it is Fuchsian of the first kind.

Conversely, suppose that Γ is a $(1;e)$-group. Then by Theorem 10.5.1(iii) in [Bea95], a fundamental polygon for Γ has at least 4 sides, and there exists a fundamental quadrilateral Q' for Γ. Consider such a Q'.

Q' is necessarily convex, since its angle sum equals $2\pi - \text{area}(P') = 2\pi - 2\pi(1-1/e) = 2\pi/e \leq \pi$. Therefore by §9.3 in [Bea95], Q' has a side pairing. Take A' and B' to be the side-pairing elements. Then we have $\Gamma = \langle A', B'\rangle$.

We claim that the side pairing pairs opposite sides of Q'. To prove this, we use the theory of cycles (for which see [Voi09a]): if the claim were false, then either $A'^2 = 1$, $B'^2 = 1$, or $A'^2 = B'^2$. All these possibilities would imply that Γ has an abelianization of rank < 2, which is clearly impossible.

From the claim, it follows that there exists a vertex p' of Q' such that the complete set of vertices of Q' is given by $\{p', A'p', B'p', A'B'p'\}$. Using the theory of cycles once more, we see that all relations between A' and B' are generated by $[A', B']^e = 1$. Hence A' and B' satisfy the relations in the presentation (1.1).

Standardizing A' and B' corresponds to translating Q' (note that this implies the final statement of the theorem). By Lemma 1.2.4, the resulting standard pair (A', B') satisfies $\text{tr}([A', B']) = -2\cos(\pi/e)$ since P' has angle sum $2\pi/e$. By part (2.1) of Theorem 1 in [Ros86], we have $\text{tr}([A, B]) = \text{tr}([A', B'])$ (also see the discussion on elementary transformations below). Hence indeed $n = 1$. The quadrilateral Q is a fundamental domain for Γ by (i). □

The theorem motivates the following

Definition 1.2.6. *An elliptic standard pair (A, B) satisfying*

$$\text{tr}([A, B]) = -2\cos(\pi/e)$$

is called a $(1;e)$-pair. *A trace triple (x, y, z) is called a* $(1;e)$-triple *if the associated elliptic standard pair is a $(1;e)$-pair.*

Remark. Using (1.2), one sees that a trace triple (x, y, z) is a $(1;e)$-triple if and only if

$$x, y, z > 2 \text{ and } x^2 + y^2 + z^2 - xyz = 2 - 2\cos(n\pi/e). \tag{1.4}$$

In light of Theorem 1.2.5, all $(1;e)$-groups are generated by a $(1;e)$-pairs (A, B), with which we have associated a quadrilateral Q. Not all these quadrilaterals are translates of one another. Indeed, consider the Euclidean situation: here, fundamental domains for $\mathbf{Z}^2\backslash\mathbf{R}^2$ can be given by both $[0,1]^2$ and $S([0,1]^2)$, where $S(x, y) = (x, x+y)$. We now consider this phenomenon in more detail in an attempt to construct an "optimally shaped" fundamental domain.

Let (A, B) be a $(1; e)$-pair and consider the following transformations:

$$\begin{aligned} T_1 &: \ (A, B) \longmapsto (B, A) \\ T_2 &: \ (A, B) \longmapsto (AB, A^{-1}) \\ T_3 &: \ (A, B) \longmapsto (A^{-1}, ABA^{-1}). \end{aligned}$$

These are the *elementary transformations* from [Tak83]. The T_i have the property that the pairs $(A', B') = T_i(A, B)$ satisfy $[A', B'] = [A, B]^{\pm 1}$. Note that the $T_i(A, B)$ are $(1; e)$-pairs for the same group Γ as (A, B). The T_i affect the trace triples (x, y, z) as follows:

$$\begin{aligned} T_1 &: \ (x, y, z) \longmapsto (y, x, z) \\ T_2 &: \ (x, y, z) \longmapsto (z, x, y) \\ T_3 &: \ (x, y, z) \longmapsto (x, y, xy - z). \end{aligned}$$

For a $(1; e)$-triple (x, y, z), we have $x, y, z > 2$ by (1.4). We claim that the triples $T_i(x, y, z)$ also satisfy $x', y', z' > 2$. This is trivial for T_1 and T_2. So let $(x', y', z') = T_3(x, y, z) = (x, y, xy - z)$. Clearly $x' = x > 2$ and $y' = y > 2$. By (1.4), we also know that

$$x'^2 + y'^2 + z'^2 - x'y'z' - 4 < 0.$$

This certainly implies $z' > 0$. As a polynomial in t', the discriminant of $x'^2 + t'^2 + z'^2 - x't'z' - 4$ equals $(x'^2 - 4)(z'^2 - 4)$. Since this polynomial has a negative value at $t' = y'$, we see that we must have $(x'^2 - 4)(z'^2 - 4) > 0$, hence also $(z'^2 - 4) > 0$, which proves the claim.

Pairs (A, B) that can be obtained from one another by a finite succession of elementary transformations are called *equivalent*, as are the corresponding trace triples (x, y, z). Quadrilaterals coming from equivalent pairs essentially exhaust all fundamental quadrilaterals for a $(1; e)$-group:

Proposition 1.2.7. *Let (A, B) be a $(1; e)$-pair, and let $\Gamma = \langle A, B \rangle$. Suppose that Q is a fundamental quadrilateral for the group Γ.*

Then there exists a $(1; e)$-pair (A', B') equivalent to (A, B) such that Q is a translate of the quadrilateral associated with the pair (A', B').

Proof. Let (A', B') be a $(1; e)$-pair corresponding to the quadrilateral P' by Theorem 1.2.5. Part (2.1) of Theorem 1 in [Ros86] shows that the pair (A', B') can be obtained from the pair (A, B) by a succession of *Nielsen transformations*

$$\begin{aligned} N_1 &: \ (A, B) \longmapsto (B, A) \\ N_2 &: \ (A, B) \longmapsto (A^{-1}, B) \\ N_3 &: \ (A, B) \longmapsto (AB, A) \end{aligned}$$

Since conjugation of the pair (A, B) merely translates Q, we shall be through if we show that up to conjugation by elements of Γ, the N_i can be generated by elementary transformations.

For N_1, this is obvious, and $N_2(A,B) = A^{-1}T_3(A,B)A$. To conclude, one checks that

$$N_3(A,B) = AT_1(T_3(T_1(T_2(A,B))))A^{-1}. \qquad \square$$

We can reduce a $(1;e)$-triple (x,y,z) with respect to the transformations T_i in the following sense.

Lemma 1.2.8. *Given a $(1;e)$-triple (x,y,z) with $x,y,z > 2$, there exists an equivalent triple (x',y',z') with $2 < x' \leq y' \leq z'$ and $2z' \leq x'y'$.*

Proof. See page 387 of [Tak83] for this brief calculation. □

Definition 1.2.9. *We call a $(1;e)$-triple (x,y,z) satisfying $2 < x \leq y \leq z$ and $2z \leq xy$ a* reduced $(1;e)$-triple. *The associated $(1;e)$-pair (A,B) is also called* reduced.

Given an integer $e \geq 2$, let us for the remainder of this section denote by S_e the set of $(1;e)$-triples. That is, let

$$S_e = \left\{(x,y,z) \in \mathbf{R}^3 : x^2+y^2+z^2-xyz = 2-2\cos(\pi/e),\ x,y,z > 2\right\}.$$

The group T generated by the T_i acts on S_e. We let $\mathcal{F}_e$ be the set of reduced triples in S_e:

$$\mathcal{F}_e = \left\{ \begin{array}{cc} (x,y,z) \in \mathbf{R}^3 : & x^2+y^2+z^2-xyz = 2-2\cos(\pi/e), \\ & 2 < x \leq y \leq z,\ 2z \leq xy \end{array} \right\}.$$

Let (A,B) be a $(1;e)$-pair with trace triple $(x,y,z) \in S_e$. Consider the hyperbolic quadrilateral Q associated with (A,B). Let α_1 be the angle between the sides $\{p, Ap\}$ and $\{p, Bp\}$ of Q, and let α_2 be the angle between the sides $\{p, Ap\}$ and $\{Ap, ABp\}$. These angles are equal to the interior angles between the geodesics containing the given sides.

Definition 1.2.10. *The* angle difference *of the triple (x,y,z) is given by*

$$a(x,y,z) = |\alpha_1 - \alpha_2|.$$

The following theorem shows the geometric significance of reduced $(1;e)$-pairs (A,B): among all pairs generating the associated Fuchsian group $\Gamma = \langle A,B\rangle$, they give rise to the most symmetric quadrilateral fundamental domains.

Theorem 1.2.11. *Let $(x,y,z) \in \mathcal{F}_e$. Then for all $(1;e)$-triples (x',y',z') equivalent to (x,y,z), we have*

$$a(x,y,z) \leq a(x',y',z').$$

The set $\mathcal{F}_e$ is a fundamental domain for S_e under the action of T, and the relations in the group T are generated by

$$T_1^2 = 1, T_2^3 = 1, T_3^2 = 1, T_1T_3 = T_3T_1 \text{ and } T_1T_2 = T_2^{-1}T_1.$$

Proof. The relations in the theorem obviously hold. As a result, every element t of T is of the form

$$t = T_1^a T_2^b T_3 T_2^{c_1} T_3 \cdots T_2^{c_n} T_3^d \tag{1.5}$$

with $a \in \{0,1\}$, $b \in \{-1,0,1\}$, $c_i \in \{\pm 1\}$ and $d \in \{0,1\}$.

We need some explicit calculations. Let λ, a, b, c, and d be as in (1.3). Then one verifies that the geodesic containing $\{p, Ap\}$, respectively$\{p, Bp\}$, is given by $\{z : |z - c_1| = r_1\}$, respectively $\{z : |z - c_2| = r_2\}$, where

$$\begin{aligned}
c_1 =& \frac{2ad}{b(a+d)} i + \frac{-a+d}{a+d} \\
c_2 =& \frac{-2\lambda^2(a-d)}{b(\lambda^4 b - 1)} i + \frac{-\lambda^2 - 1}{\lambda^2 - 1} \\
r_1^2 =& \frac{4ad}{b^2(a+d)^2} \\
r_2^2 =& \frac{4\lambda^2(b^2 + a^2\lambda^2 + 2b^2\lambda^2 - 2ad\lambda^2 + d^2\lambda^2 + b^2\lambda^4)}{b^2(\lambda^2-1)(\lambda^2+1)}
\end{aligned}$$

The law of cosines tells us that

$$\pi - \cos(\alpha_1) = \frac{r_1^2 + r_2^2 - |c_1 - c_2|^2}{2r_1 r_2}.$$

Using Proposition 1.2.3, we also get that

$$\pi - \cos(\alpha_2) = \frac{r_1^2 + r_2^2 - |c_1 + c_2|^2}{2r_1 r_2}.$$

Since by Proposition 1.2.3 the sum $\alpha_1 + \alpha_2$ is equal to π/e on all triples equivalent to (x, y, z), we may as well minimize the expression $|\cos(\alpha_1) - \cos(\alpha_2)|$ instead of $|\alpha_1 - \alpha_2|$. One verifies

$$|\cos(\alpha_1) - \cos(\alpha_2)|^2 = \frac{(xy - 2z)^2(xyz - x^2 - y^2 - z^2)^2}{4(xyz - y^2 - z^2)(xyz - x^2 - z^2)}$$

Note that the factor $(x^2 + y^2 - xyz + z^2)^2$ in this fraction is positive and constant on S_e by (1.4). Therefore it suffices to show that a reduced triple (x, y, z) minimizes the function

$$a'(x,y,z) = \frac{(xy - 2z)^2}{4(xyz - y^2 - z^2)(xyz - x^2 - z^2)}$$

among all equivalent triples. Along the way, we will show that $\mathcal{F}_e$ is a fundamental domain for the action of T.

We first note that the transformations T_1 and T_3 do not affect the value of a'. By (1.5), it remains to examine what happens upon successive applications of T_2 and T_3. We first prove the following claims:

Claim 1: Let $(x,y,z) \in \mathcal{F}_e$. Then

$$\begin{aligned} a'(T_2(x,y,z)) &\geq a'(x,y,z), \\ a'(T_2^{-1}(x,y,z)) &\geq a'(x,y,z), \\ a'(T_2T_3(x,y,z)) &\geq a'(x,y,z), \\ \text{and } a'(T_2^{-1}T_3(x,y,z)) &\geq a'(x,y,z). \end{aligned}$$

Moreover, if $(x,y,z) \in \operatorname{int}(\mathcal{F}_e)$, then these inequalities are strict.

Claim 2: Suppose $a'(T_2(x,y,z)) \geq a'(x,y,z)$. Then

$$\begin{aligned} a'(T_2T_3T_2(x,y,z)) &> a'(T_2(x,y,z)) \\ \text{and } a'(T_2^{-1}T_3T_2(x,y,z)) &> a'(T_2(x,y,z)). \end{aligned}$$

Claim 3: Suppose $a'(T_2^{-1}(x,y,z)) \geq a'(x,y,z)$. Then

$$\begin{aligned} a'(T_2T_3T_2^{-1}(x,y,z)) &> a'(T_2^{-1}(x,y,z)) \\ \text{and } a'(T_2^{-1}T_3T_2^{-1}(x,y,z)) &> a'(T_2^{-1}(x,y,z)). \end{aligned}$$

Naturally enough, we start by proving Claim 1. Explicitly, $a'(T_2(x,y,z)) - a'(x,y,z)$ is given by

$$\frac{y^2(z-y)(z+y)(xyz-x^2-y^2-z^2+4)}{(xyz-x^2-y^2)(xyz-y^2-z^2)(xyz-x^2-z^2)}$$

Because of (1.4), the quantities $xyz-x^2-y^2-z^2+4$, $xyz-x^2-y^2$, $xyz-y^2-z^2$ and $xyz-x^2-z^2$ are positive. And since $(x,y,z) \in \mathcal{F}_e$, we also have $z \geq y$, which proves the first inequality. As $a'(T_2^{-1}(x,y,z)) - a'(x,y,z)$ is equal to $a'(T_2(y,x,z)) - a'(y,x,z)$, the second inequality also follows since we have $z \geq x$ as well.

The inequality $z \geq y$ remains valid under application of T_3 since by reducedness $xy - z \geq xy/2 > y$. We obtain $a'(T_2T_3(x,y,z)) \geq a'(x,y,z)$ and $a'(T_2^{-1}T_3(x,y,z)) \geq a'(x,y,z)$ by T_3-invariance of a', concluding the proof of Claim 1. That these inequalities are strict when $(x,y,z) \in \operatorname{int}(\mathcal{F}_e)$ is clear from the calculations above.

Now for Claim 2. The proof of Claim 1 shows

$$a'(T_2(x',y',z')) \geq a'(x',y',z') \iff z' \geq y'$$

and

$$a'(T_2(x',y',z')) > a'(x',y',z') \iff z' > y'.$$

Therefore, if the hypothesis of Claim 1 holds, then $z \geq y$.

Now $T_3T_2(x,y,z) = (z,x,xz-y)$. Since $x,y > 2$, we have that $xz - y \geq xy - y > x$ from the inequality $(x-1)(y-1) > 1$. So we can conclude that $a'(T_2T_3T_2(x,y,z)) > a'(T_2(x,y,z))$. Similarly,

$$a'(T_2^{-1}(x',y',z')) > a'(x',y',z') \iff z' > x'.$$

But since $z \geq y$, we have $xz - y \geq xz - z > 2z - z = z$, proving the second inequality of Claim 2. As for Claim 3, this is proved the in the same way as Claim 2, interchanging the roles of x and y.

Using these Claims in conjuction with the invariance of a' under T_1 and T_3, it is straightforward to show that $\mathcal{F}_e$ is a fundamental domain. Indeed, by Lemma 1.2.8, every element of $T\backslash S_e$ has a representative in $\mathcal{F}_e$. To show that $\mathcal{F}_e$ is a fundamental domain, we remark that inductively applying the Claims to expression (1.5), we get

$$a'(t(x,y,z)) \geq a'(x,y,z).$$

for all t in T. Moreover, if $(x,y,z) \in \operatorname{int}(\mathcal{F}_e)$, then this inequality is strict if (and only if) the expression (1.5) for t contains a factor T_2. It therefore suffices to check that $t(\operatorname{int}(\mathcal{F}_e)) \cap \operatorname{int}(\mathcal{F}_e) = \emptyset$ for all t in the finite group $\langle T_1, T_3 \rangle$, but this is easily verified.

Finally, if there were any additional relations between T_1, T_2 and T_3, then this would yield a word w in these elements such that $a'(x,y,z) = a'(t(x,y,z))$ regardless of the initial triple w. The Claims show that the expression (1.5) for t would then only contain T_1 and T_3. But clearly there are no more relations between T_1 and T_3 than those in the theorem. □

1.3 Dirichlet domains

This section gives an explicit description of the Dirichlet domains centered at 0 for the Fuchsian groups associated to reduced $(1;e)$-pairs. Throughout, we let (A,B) be a reduced $(1;e)$-pair, (x,y,z) its trace triple, and $\Gamma = \langle A, B \rangle$ the corresponding $(1;e)$-group.

Theorem 1.3.1. *If $2z = xy$, then the Dirichlet domain centered at 0 for Γ is the quadrilateral Q associated with (A,B).*

Proof. If $2z = xy$, then B is of the form

$$B = \begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

One then explicitly calculates (using the expressions (1.6) and (1.7)) that the vertices p, Ap, Bp, ABp are equidistant to 0. Hence the isometric circle $I(A)$ contains the segment $\{p, Bp\}$. Similarly, we obtain the inclusions $\{p, Ap\} \subset I(B)$, $\{Ap, ABp\} \subset I(A^{-1})$, and $\{Bp, ABp\} \subset I(B^{-1})$.

These isometric circles therefore contain the sides of the fundamental domain Q constructed in Theorem 1.2.5. Since all fundamental domains for Γ have the same area $2\pi(1 - 1/e)$ by Corollary 10.4.4 in [Bea95], we see that the Dirichlet domain is in fact given by Q. □

It remains to see what form the Dirichlet domain takes when $2z \neq xy$. We first prove two lemmata.

Lemma 1.3.2. *The fixed point p of $[A, B]$ is in the second quadrant of* $\mathbf{C}$. *Furthermore, the point Bp is in the third quadrant, ABp in the fourth, and Ap in the first.*

Proof. Let $x = \operatorname{tr}(A) = \lambda + \lambda^{-1}$, $y = \operatorname{tr}(B) = a + d$, $z = \operatorname{tr}(AB) = \lambda a + \lambda^{-1} d$. Let

$$w = \sqrt{4 - b^2(\lambda + \lambda^{-1})^2} = \sqrt{x^2 + y^2 + z^2 - xyz}.$$

The point p is given by one of

$$\frac{-(a\lambda^2 + d) \pm \lambda w}{a\lambda^2 - d + b(1 + \lambda^2)i}. \tag{1.6}$$

The quantity λw is real and positive because of (1.4). Obviously, $a\lambda^2 + d > 0$. Furthermore, we have

$$(a\lambda^2 + d)^2 > (\lambda w)^2 = 4\lambda^2 - b^2(\lambda^2 + 1)^2,$$

for using the relation $ad - b^2 = 1$, one can check that this boils down to

$$\lambda^2 xyz - x^2 - y^2 > 0,$$

and this follows from (1.4) and $z > 2$, $\lambda > 1$.

So the numerator of (1.6) is strictly negative. Considering the denominator, $b(1 + \lambda^2)$ is clearly strictly positive. Now

$$a\lambda^2 - d = \frac{xz - 2y}{1 - \lambda^{-2}}.$$

This is strictly positive. Indeed, the denominator is obviously strictly positive, and $xz > 2y$ since $x > 2$ and $z \geq y$. Therefore p is given by a quotient of a strictly negative real number by an imaginary number in the first quadrant, hence is indeed in the second quadrant.

For Bp, the proof is similar. This point is given by one of

$$\frac{a\lambda^2 + d \pm \lambda w}{a - d\lambda^2 + b(1 + \lambda^2)i}. \tag{1.7}$$

Again, the factor inside of the square root is positive, and $a\lambda^2 + d > 0$. We claim that

$$(a + d\lambda^2)^2 > (\lambda w)^2 = 4\lambda^2 - b^2(\lambda^2 + 1)^2.$$

This inequality rewrites as

$$\lambda^2(x^2y^2 - x^2 - y^2 - xyz) > 0,$$

which follows because of the reducedness hypothesis: $x^2y^2 - x^2 - y^2 - xyz \geq (x^2y^2 - 2x^2 - 2y^2)/2$, and $x^2y^2 - 2x^2 - 2y^2 + 4 = (x^2 - 2)(y^2 - 2) > 4$ because $x, y > 2$.

So the numerator of (1.7) is strictly negative. Considering the denominator, $b(1+\lambda^2)$ is clearly strictly positive. Now

$$a - d\lambda^2 = -\frac{x^2y - xz - 2y}{1-\lambda^{-2}}.$$

This is strictly negative. Indeed, the denominator is obviously strictly positive, and again because of reducedness we have $x^2y - xz - 2y \geq y(x^2-4)/2 > 0$. So Bp is given by a quotient of a strictly positive real number by an imaginary number in the second quadrant, hence indeed lives in the third quadrant.

Since $ABp = -p$ and $Bp = -Ap$ by Proposition 1.2.3, we are through. □

Lemma 1.3.3. *We have*

$$d(p,0) = d(ABp,0) = d(BAp,0) \leq d(Ap,0) = d(Bp,0),$$

with equality holding if and only if $2z = xy$.

Proof. Let

$$w = \sqrt{4 - b^2(\lambda+\lambda^{-1})^2} = \sqrt{x^2+y^2+z^2-xyz}.$$

Explicitly determining the points Ap and p, we see that the inequality $|p| \leq |Ap|$ is equivalent to

$$2(xy-2z)(w(x^2+y^2) - xy(x^2+y^2+z^2-xyz)) \geq 0.$$

It therefore suffices to show that

$$w(x^2+y^2) - xy(x^2+y^2+z^2-xyz) > 0.$$

Plugging in w and rearranging, this comes down to

$$(x^2+y^2-xyz)(x^2y^2-xyz-x^2-y^2) \leq 0.$$

The first term is negative because of (1.4). As for the second, since $2z \leq xy$, this term is stricly smaller than $\frac{1}{2}(x^2y^2 - 2x^2 - 2y^2)$. This is a strictly positive quantity: as $x, y > 2$ by (1.4), we have

$$x^2y^2 - 2x^2 - 2y^2 + 4 = (x^2-2)(y^2-2) > 4.$$

We can therefore conclude using Proposition 1.2.3. □

Using these lemmata, we can now prove our main result on Dirichlet domains. Let $M_1, M_2 \in \mathrm{PGL}_2^+(\mathbf{R})$. Then supposing that the set $I(M_1) \cap I(M_2) \cap \mathcal{D}$ is proper and nonempty, we shall abuse notation by identifying it with its single element.

Theorem 1.3.4. *Suppose* $2z \neq xy$. *Then the Dirichlet domain centered at* 0 *for* Γ *is a proper octagon whose sides are, in clockwise order, contained in the geodesics*

$$I(A), I(BA), I(AB), I(B), I(A^{-1}), I((AB)^{-1}), I((BA)^{-1}) \text{ and } I(B^{-1}).$$

Proof. We subdivide the proof into steps.

Step 1: *We have* $-I(A) = I(A^{-1})$, $-I(B) = I(B^{-1})$, $-I(BA) = I((BA)^{-1})$, $-I(AB) = I((AB)^{-1})$.

This follows from the fact that A and B are symmetric and from the more general identity

$$-I(M) = I(M^{-T}),$$

which is proved by remarking that

$$d(M(-x),0) = d(-x,0) \Leftrightarrow d(-M^{-T}x,0) = d(-x,0) \Leftrightarrow d(M^{-T}x,0) = d(x,0)$$

(*cf.* the proof of Proposition 1.2.3). Note that this implies that the octagon we end up with is pointsymmetric around the origin.

Step 2: *The intersections* $I(A) \cap I(BA)$, $I(BA) \cap I(AB)$, $I(AB) \cap I(B)$, $I(B) \cap I(A^{-1})$, $I(A^{-1}) \cap I((AB)^{-1})$, $I((AB)^{-1}) \cap I((BA)^{-1})$, $I((BA^{-1}) \cap I(B^{-1})$, *and* $I(B^{-1}) \cap I(A)$ *are non-empty and contained in* $\mathcal{D}$.

$I(BA)$ and $I(AB)$ intersect in $\mathcal{D}$ because the fixed point p of $[A, B]$ is on both of them by Proposition 1.2.3. As for the other intersections, suppose that $I(B) \cap I(A^{-1})$ is a point q in $\mathcal{D}$. We then have $Bq = I(B^{-1}) \cap I((BA)^{-1})$. Indeed, rearranging the equalities $d(Bq, 0) = d(q, 0) = d(A^{-1}q, 0)$, we obtain that $d(B^{-1}(Bq), 0) = d(Bq, 0) = d((BA)^{-1}(Bq), 0)$.

Similarly, we have $A^{-1}q = I(A) \cap I(BA)$. Therefore, exploiting the same symmetry that was used in Step 1, we see that we are done if $I(B)$ and $I(A^{-1})$ intersect in $\mathcal{D}$. Now the isometric circles $I(B)$ and $I(A^{-1})$ both contain Ap in their interior by Lemma 1.3.3. The only way, then, for these circles not to intersect is for one of them to be contained in the other. However, the center $c_{A^{-1}}$ of $I(A^{-1})$ is in the exterior of $I(B)$. Indeed, one readily calculates

$$|\widetilde{B}_{2,1}c_{A^{-1}} + \widetilde{B}_{2,2}|^2 = \frac{xyz - x^2 - y^2}{x^2 - 4},$$

and this is strictly greater than 1, since

$$xyz - 2x^2 - y^2 + 4 \geq xyz - x^2 - y^2 - z^2 + 4 > 0,$$

the former inequality using that $x \leq z$ and the latter following from (1.4).

Step 3: p *and* $-p$ *are in the exterior of* $I(A)$, $I(A^{-1})$, $I(B)$ *and* $I(B^{-1})$. Ap *is in the interior of* $I(A^{-1})$ *and* $I(B)$ *and in the exterior of* $I(A)$ *and* $I(B^{-1})$. Bp *is in the interior of* $I(A)$ *and* $I(B^{-1})$ *and in the exterior of* $I(A^{-1})$ *and* $I(B)$.

By Step 1, it suffices to prove the statements for p and Ap. The point p is in the exterior of $I(A)$ and $I(B)$ by Lemma 1.3.3. Since $I(A^{-1})$ is contained in the first and fourth quadrants, p is in the exterior of $I(A^{-1})$ by Proposition 1.3.2.

Now note that the proof of Proposition 1.3.2 still goes through if $x > y$. Since applying T_1 does not change the point p and switches the roles of A and B, we can therefore conclude that p is in the exterior of $I(B^{-1})$ as well. The statements for Ap are proved in a similar way.

Step 4: *$q = I(B) \cap I(A^{-1})$ and $-q$ are in the exterior of $I(AB)$, $I((AB)^{-1})$, $I(BA)$ and $I((BA)^{-1})$; p is on $I(AB)$ and $I(BA)$ and in the exterior of $I((AB)^{-1})$ and $I((BA)^{-1})$; and $-p$ is on $I((AB)^{-1})$ and $I((BA)^{-1})$ and in the exterior of $I(AB)$ and $I(BA)$.*

By Step 1, it suffices to prove the statements for q and p. Considering q first, suppose it is not in the exterior of $I(AB)$. Then both q and the point $r = I(B) \cap I(AB)$ are in the closure of the interior of $I(AB)$. Now using the methods of Step 2 and Step 1, one shows that $Bq = I(B^{-1}) \cap I((BA)^{-1}) = -r$ and similarly $Br = -q$. This means that there is a point s on the segment between q and r such that $Bs = -s$. This point would then also be in the closure of the interior of $I(AB)$.

One calculates, however, that s is given by

$$s = -\frac{a+d-2}{a+2ib-d}$$

and we have

$$|\widetilde{AB}_{2,1}s + \widetilde{AB}_{2,2}|^2 - 1 = \frac{xz-2y}{y+2}.$$

This is strictly positive since $x > 2$ and $z \geq y$. So in fact s is in the exterior of $I(AB)$, yielding a contradiction. Replacing $I(B)$ by $I(A^{-1})$ and $I(AB)$ by $I((AB)^{-1})$ leads to a similar calculation showing that q is in the exterior of $I((AB)^{-1})$.

Let c_{AB} and c_{BA} the centers of the isometric circles $I(AB)$ and $I(BA)$, respectively. Then it is straightforward to calculate that $\Im(c_{BA}/c_{AB}) > 0$. Let L be the geodesic connecting p and $-p$. It is given by a straight line. The estimate implies that c_{AB} is to the right of L and that c_{BA} is to its left. Therefore the angle between $I(B) \cap I(AB)$, p and $I(A) \cap I(BA)$ is smaller than π.

This allows us to prove that q is in the exterior of $I(BA)$ and $I((BA)^{-1})$. In fact, since it is situated on $I(A^{-1})$, which is contained in the first and second quadrant of $\mathbf{C}$, the point q is to the right of the geodesic L. We have that $I(AB)$ and $I(BA)$ intersect in p, and $I((AB)^{-1})$ and $I((BA)^{-1})$ in $-p$. By the angle estimate above, then, those parts of the interiors of $I(BA)$ and $I((BA)^{-1})$ that are on the right side of L are already contained in the interiors of $I(AB)$ and $I((AB)^{-1})$, respectively.

As for p, Proposition 1.3.3 shows that it lies on $I(AB)$ and $I(BA)$. It is in the exterior of $I((AB)^{-1})$ and $I((BA)^{-1})$ because $-p$ is on these geodesics, and these do not pass through the origin.

Step 5: *The eight geodesics in the theorem describe a proper compact octagon E.*

This follows from Step 3 and Step 4. A few pictures of the construction process have been added for clarification in Figure 1.2. On the left are the four isometric circles $I(A)$, $I(A^{-1})$, $I(B)$ and $I(B^{-1})$ along with the points p and $-p$. On the right is the complete Dirichlet domain.

Step 6: *E is a fundamental domain for Γ.*

The octagon E is convex. Indeed, the only points of E at which it is tricky to prove that the interior angle of E is smaller than π are p and $-p$. Exploiting

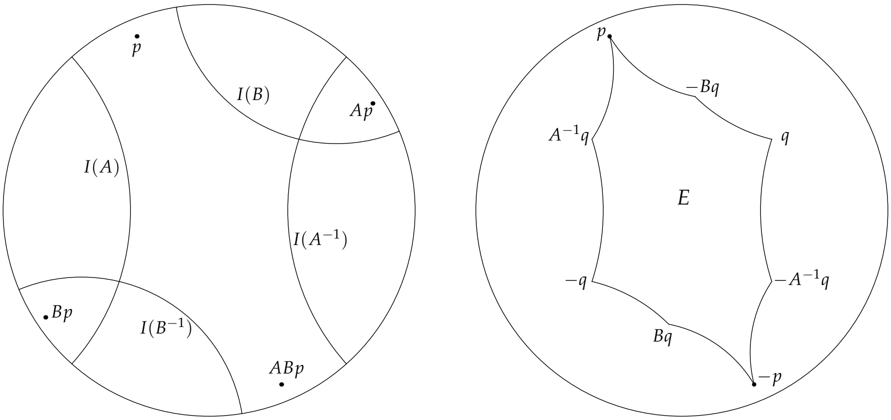


Figure 1.2: Construction of a Dirichlet domain centered at 0.

the usual symmetry from Step 1, however, one can conclude at these points as well by the using the angle estimate in Step 4. E also has a side pairing, as can be seen the argument in the proof of Step 2. For example, B pairs the side contained in $I(B)$ to the side contained in $I(B^{-1})$ because of the following argument:

The side contained in $I(B)$ has vertices given by $I(B) \cap I(A^{-1})$ and $I(B) \cap I(AB)$. We have already seen in Step 2 that the former point is sent to $I(B^{-1}) \cap I((BA)^{-1})$ by B. The latter, call it t, satisfies $d(Bt, 0) = d(t, 0) = d(ABt)$, so $d(B^{-1}(Bt), 0) = d(Bt, 0) = d(A(Bt), 0)$, hence necessarily $At = I(B^{-1}) \cap I(A)$. Now the points $I(B^{-1}) \cap I((BA)^{-1})$ and $I(B^{-1}) \cap I(A)$ are the vertices of the side of E contained in $I(B^{-1})$, therefore B does indeed pair the two sides as described. Verifying that the other sides are paired is no more difficult.

Now consider the elliptic vertex p and the generator $[A, B]$ of its stabilizer. As we have seen in the proof of Lemma 1.2.4, $[A, B]$ induces a rotation around p through a clockwise angle of $2\pi/e$. Consider a point $u \neq p$ on the side contained in $I(AB)$. Then by the usual arguments, ABu is on the side contained in $I((AB)^{-1})$. This is outside of $I((BA)^{-1})$ by Step 4. Hence

$$d([A, B]u, 0) = d(A^{-1}B^{-1}ABu, 0) > d(ABu, 0) = d(BA[A, B]u, 0),$$

therefore $[A, B]u$ is in the interior of $I(BA)$. As a result, the interior angle ϑ between $I(AB)$ and $I(BA)$ is strictly smaller than $2\pi/e$.

Theorem 9.8.6 in [Bea95] tells us that the sum $\sum_{\gamma \in S} \vartheta_\gamma(p)$ is an integer multiple of 2π. Here S is the set of γ in Γ having the property that γ maps p into its E-cycle, and for $\gamma \in S$, the quantity $\vartheta_\gamma(p)$ is given by the interior angle of E at γp.

The E-cycle containing p is given by $\{p, -p\}$. Clearly

$$S = \langle [A, B] \rangle \sqcup AB \langle [A, B] \rangle.$$

Because of the symmetry in Step 1, $\vartheta_\gamma(p)$ is independent of γ. It therefore equals the angle ϑ between $I(AB)$ and $I(BA)$ that we considered above. By the estimate,

$$\sum_{\gamma \in S} \vartheta_\gamma(p) = |S|\vartheta < |S|\frac{2\pi}{e} = 4\pi.$$

So since the outcome should be an integral multiple of 2π, we in fact have $\sum \vartheta_\gamma(p) = 2\pi$, hence for all $\gamma \in S$ we have $\vartheta_\gamma(p) = \vartheta = \pi/e$.

We can now apply Poincaré's theorem. Indeed, Theorem 9.8.6 in [Bea95] tells us that if $\sum \vartheta_\gamma(v)$ equals 2π for one vertex v, then in fact it equals 2π for all vertices. For a vertex v with trivial stabiliser, the sum $\sum \vartheta_\gamma(v)$ simply runs over the cycle of v, so the angle sum for hyperbolic cycles is equal to 2π. Since the argument above shows that the angle sum equals $2\pi/e$ for the elliptic cycle, the conditions of Theorem 1.1.2 are fulfilled. We conclude that E is a fundamental polygon for the group generated by the side pairings of E. But this group is contained in Γ and contains A and B, hence equals Γ.

Step 7: *E is the Dirichlet domain centered at 0 for Γ.*

This is now immediate: the Dirichlet domain is certainly contained in E, but it cannot be smaller because of Step 6. The clockwise order of the sides of E follows from the construction process. □

Remarks. (i) Using the side pairing given in the proof, it is straightforward to verify that p and $-p$ are the only elliptic points in E.

(ii) When $x = y$, the octagon acquires an extra symmetry given by reflection in the line through p and $-p$, as can be verified by considerations analogous to those in the proof of Step 3 above.

(iii) It is possible for the set of geodesics $\{I(A), I(A^{-1}), I(B), I(B^{-1})\}$ to close up into a compact quadrilateral Q when $2z < xy$. However, Q will then not be a fundamental domain. Indeed, even though the geodesics above are paired by A and B, the sides of Q that they give rise to will in general not be mapped onto one another by these matrices.

(iv) We refer to pp. 305-337 [FK65] for more considerations on Dirichlet domains for $(1;e)$-groups. The approach in [FK65] is quite geometric; we took a more explicit algebraic inroad, since our main reason for being interested in Dirichlet domains is developing the reduction algorithm in the next section.

1.4 Explicit homology

Let us denote $\mathcal{H}^{+1} = \mathcal{H}$ and $\mathcal{H}^{-1} = \overline{\mathcal{H}}$. Then given $a \in \{\pm 1\}$ and a Fuchsian group of the first kind $\Gamma \subset \mathrm{PGL}_2^+(\mathbf{R})$, we can consider the quotient

$$Y^a(\Gamma) = \Gamma \backslash \mathcal{H}^a. \tag{1.8}$$

We usually abbreviate $Y^+(\Gamma) = Y^{+1}(\Gamma)$ and $Y^-(\Gamma) = Y^{-1}(\Gamma)$. Moreover, we usually write $Y(\Gamma)$ instead of $Y^+(\Gamma)$. Note that there is an antiholomorphic isomorphism

$$\begin{aligned} Y^{+}(\Gamma) &\longrightarrow Y^{-}(\Gamma) \\ [z] &\longmapsto [\overline{z}]. \end{aligned} \tag{1.9}$$

Let Γ be a subgroup of $\mathrm{SL}_2(\mathbf{R})$ or $\mathrm{GL}_2(\mathbf{R})$, and suppose that $\mathrm{P}\Gamma \subset \mathrm{PGL}_2(\mathbf{R})$ is Fuchsian of the first kind. Then we shall frequently abuse notation and write $Y^a(\Gamma)$ instead of $Y^a(\mathrm{P}\Gamma)$. Finally, we denote the compactifications of the Riemann surfaces $Y^{(a)}(\Gamma)$ by $X^{(a)}(\Gamma)$. Note that $X^a(\Gamma) = Y^a(\Gamma)$ if Γ is a $(1;e)$-group, and that we can recover the curves $Y(\mathcal{O}^+)$ and $Y(\mathcal{O}^1)$ from the introduction, along with their compactifications $X(\mathcal{O}^+)$ and $X(\mathcal{O}^1)$, by taking Γ to equal $(\mathrm{P})\mathcal{O}^+$, respectively $(\mathrm{P})\mathcal{O}^1$.

This thesis considers a special subclass (to be defined in Section 3.3) of the following class of geometric objects:

Definition 1.4.1. *A* $(1;e)$-curve *(or* pointed complex torus*) is a Riemann surface* $X^a(\Gamma)$ *associated with a* $(1;e)$*-group* Γ.

Let (A,B) be a $(1;e)$-pair, and let $\Gamma = \mathrm{P}\langle A,B\rangle$ be the associated $(1;e)$-group. An element γ of Γ gives rise to a homology class $[\gamma] \in H_1(X^a(\Gamma),\mathbf{Z})$: if $x \in \mathcal{H}^a$ is non-elliptic, this $[\gamma]$ can be described as the class of the projection of an arbitrary path in $\mathcal{H}^a$ with initial point $x \in \mathcal{H}^a$ and final point $\gamma x \in \mathcal{H}^a$ (also see Section 4.2).

Using either the explicit description of the fundamental domain for Γ given in Theorem 1.2.5 or the correspondence in Theorem 6.1.5, one observes that this association gives rise to an isomorphism $\Gamma^{\mathrm{ab}} \cong H_1(X^a(\Gamma),\mathbf{Z})$. We get a composed isomorphism

$$H_1(X^a(\Gamma),\mathbf{Z}) \xrightarrow{\sim} \Gamma^{\mathrm{ab}} \xrightarrow{\sim} \mathbf{Z}A \oplus \mathbf{Z}B. \tag{1.10}$$

Note the notational abuse: $\mathbf{Z}A \oplus \mathbf{Z}B$ is the free abelian group on the symbols A and B, and the map $\Gamma^{\mathrm{ab}} \xrightarrow{\sim} \mathbf{Z}A \oplus \mathbf{Z}B$ is given by the factorization of the map determined by $A \mapsto A$ and $B \mapsto B$.

Given an element γ of Γ, we shall in Chapter 4 be interested in explicitly determining the element of $\mathbf{Z}A \oplus \mathbf{Z}B$ corresponding to $[\gamma] \in H_1(X^a(\Gamma),\mathbf{Z})$ under the isomorphism (1.10). This comes down to determining the image of γ under the morphism

$$\Gamma \longrightarrow \Gamma^{\mathrm{ab}} \xrightarrow{\sim} \mathbf{Z}A \oplus \mathbf{Z}B. \tag{1.11}$$

If $\langle A,B\rangle$ is a reduced $(1;e)$-pair, then we can use the Dirichlet domain from the previous section to get the following algorithm (implemented at [Sij10]):

Algorithm 1.4.2. *Let* $\Gamma \subset \mathrm{PGL}_2^+(\mathbf{R})$ *be a* $(1;e)$*-group generated by a reduced* $(1;e)$*-pair* (A,B)*. Let* γ *be an element of* Γ*. This algorithm calculates the image of* γ *under the morphism (1.11).*

```
1. Set $L = \{A, B, A^{-1}, B^{-1}, AB, BA, (AB)^{-1}, (BA)^{-1}\}$.
```

2. *Set $p = \gamma \cdot 0 \in \mathcal{D}$ and $h = 0 \in \mathbf{Z}A \oplus \mathbf{Z}B$.*

3. *If there is an $l \in L$ such that $d(lp, 0) < d(p, 0)$, then set p equal to lp, subtract the class $[l] \in \mathbf{Z}A \oplus \mathbf{Z}B$ from h, and repeat this step. Otherwise, go to step 4.*

4. *Return h.*

Proof of correctness. This is a slight simplification of the standard reduction algorithm using Dirichlet domains: *cf*. Algorithm 4.3 in [Voi09a]. □

Chapter 2

Quaternions

In this Chapter, we give the basic definitions and results on quaternion algebras that we shall need in our considerations of Shimura curves from the next Chapter onwards. For detailed proofs and a more complete exposition, see [Vig80] and [Mila].

2.1 Definitions

Quaternion algebras

Definition 2.1.1. *Let F be a field. A* quaternion algebra *over F is a central simple F-algebra whose dimension as a vector space over F equals* 4.

Examples. (i) The simplest example of a quaternion algebra over F is the matrix algebra $M_2(F)$: this is called the *(everywhere) split* quaternion algebra over F. Up to isomorphism, it is the unique quaternion algebra over F that is not a division algebra ([Vig80], Corollaire I.2.4).

(ii) Given a_1 and a_2 in $F^\times$, one can construct the algebra

$$B = \left(\frac{a_1, a_2}{F} \right)$$

whose underlying vector space is given by $F1 \oplus Fi \oplus Fj \oplus Fk$ and whose multiplication satisfies $i^2 = a_1$, $j^2 = a_2$, and $ij = -ji = k$. As long as F does not have characteristic equal to 2 (which will be the case throughout this thesis), all quaternion algebras over F can be obtained in this way ([Vig80], p. 2). We define the *reduced norm* of an element $b = x_0 + x_1 i + x_2 j + x_3 k \in B$ by

$$\mathrm{nrd}(b) = x_0^2 - a_1 x_1^2 - a_2 x_2^2 + a_1 a_2 x_3^2.$$

and its *reduced trace* by

$$\mathrm{trd}(b) = 2x_0.$$

The reduced norm and trace map coincide with the usual norm and trace maps on the commutative algebra $F(b)$. In particular, we have

$$b^2 - \operatorname{trd}(b)b + \operatorname{nrd}(b) = 0$$

for all $b \in B$. The map $\operatorname{nrd} : B^\times \to F^\times$ is a homomorphism.

(iii): Taking $F = \mathbf{R}$ and $a_1 = a_2 = -1$ in (ii), one obtains the *Hamilton algebra* $\mathbf{H}$ over $\mathbf{R}$.

Classification

For a more complete discussion of the results in this subsection, we refer to Chapter IV of [Mila].

Let F be a field. Then the quaternion algebras over a F are classified by the group $\operatorname{Br}(F)[2]$ of 2-torsion elements in the Brauer group $\operatorname{Br}(F)$. The algebra $M_2(F)$ corresponds to the trivial element of $\operatorname{Br}(F)[2]$. We will now describe $\operatorname{Br}(F)[2]$ more explicitly.

First let F be a local field. Then

(i) if F is non-archimedean, then $\operatorname{Br}(F)$ is isomorphic to $\mathbf{Q}/\mathbf{Z}$. As a result, $\operatorname{Br}(F)[2]$ is isomorphic to $\frac{1}{2}\mathbf{Z}/\mathbf{Z}$: up to isomorphism, there is a unique non-split (or *ramified*) quaternion algebra over F.

(ii) if $F = \mathbf{R}$, then $\operatorname{Br}(F) = \operatorname{Br}(F)[2] \cong \frac{1}{2}\mathbf{Z}/\mathbf{Z}$, with the unique non-trivial element of $\operatorname{Br}(F)$ corresponding to the Hamilton algebra $\mathbf{H}|\mathbf{R}$, which is the unique ramified quaternion algebra over $\mathbf{R}$.

(iii) if $F = \mathbf{C}$, then $\operatorname{Br}(F)$ is trivial: all quaternion algebras over $\mathbf{C}$ are split.

Now let F be a number field. Given a quaternion algebra B over F and a place v of F, B is said to *split at* v if $B_v = B \otimes_F F_v \cong M(2, F_v)$. Otherwise B is said to *ramify at* v. Consider the set

$$\operatorname{Ram}(B) = \left\{ v : B \otimes_F F_v \ncong M(2, F_v) \right\}$$

of places at which B ramifies. The exact sequence of Theorem X.4.2 in [Mila] (or Théorème III.3.1 in [Vig80]) then gives

Theorem 2.1.2 (Classification). *The assignment $B \mapsto \operatorname{Ram}(B)$ establishes a bijection between the set of isomorphism classes of quaternion algebras over F and the finite subsets of even cardinality of the set of non-complex places of F.*

For a given quaternion algebra B, we denote by $\mathfrak{D}(B)$ the product of its ramifying places: it is called the *discriminant* of B. We denote the finite part of $\mathfrak{D}(B)$ by $\mathfrak{D}(B)^f$ and its infinite part by $\mathfrak{D}(B)^\infty$. If F is totally real, then a quaternion algebra B that is split at at least one infinite place is called *indefinite*; the algebras ramifying at all infinite places, which we will usually denote by H, are called *definite*.

Lattices, orders, ideals and adèles

Definition 2.1.3. *Let B be a quaternion algebra over a number field or a non-archimedean local field F. A* lattice *of B is a $\mathbf{Z}_F$-submodule I of B such that the induced map of F-vector spaces*

$$I \otimes_{\mathbf{Z}_F} F \longrightarrow B$$

is an isomorphism. A (quaternion) order *of a quaternion algebra B is a lattice of B that is also a unital subring.*

Given a lattice I of B, one can construct its *left order*

$$\mathcal{O}_l(I) = \{b \in B : bI \subset I\}.$$

Analogously, one defines the *right order* $\mathcal{O}_r(I)$ of I. Conversely, given an order $\mathcal{O}$ and a lattice I, we call I a *left* (respectively *right*) *$\mathcal{O}$-ideal* if $\mathcal{O}_l(I) = \mathcal{O}$ (respectively $\mathcal{O}_r(I) = \mathcal{O}$).

Let F be a number field, and let B be a quaternion algebra over F. We denote the adèle ring over F (see [Neu99], Section VI.1) by $\mathbf{A}_F$, and the closure of $\mathbf{Z}_F$ in this ring by $\widehat{\mathbf{Z}}_F$. There is a decomposition $\mathbf{A}_F = \mathbf{A}_F^f \times \mathbf{A}_F^\infty$, where $\mathbf{A}_F^f$ is the ring of finite adèles. Let

$$\widehat{B} = B \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}}^f \cong B \otimes_F \mathbf{A}_F^f.$$

Given a prime $\mathfrak{p}$ of F, we let $B_\mathfrak{p} \subset \widehat{B}$ be the localization $B \otimes_F F_\mathfrak{p}$, and we let $\widehat{B}^\mathfrak{p} = \widehat{B} \cap \prod_{\mathfrak{q} \neq \mathfrak{p}} B_\mathfrak{q}$.

Let I be a lattice of B. Then we can construct the $\mathbf{Z}_{F,\mathfrak{p}}$-module

$$I_\mathfrak{p} = I \otimes_{\mathbf{Z}_F} \mathbf{Z}_{F,\mathfrak{p}} \subset B_\mathfrak{p}$$

and the $\widehat{\mathbf{Z}}_F$-module

$$\widehat{I} = \prod_{\mathfrak{p}} I_\mathfrak{p} \subset \widehat{B}.$$

Fix a lattice I_0 of B. Then by definition, a *lattice* of $\widehat{B}$ is a $\widehat{\mathbf{Z}}_F$-submodule of $\widehat{B}$ that can be written as a product $\prod_\mathfrak{p} I_\mathfrak{p}$ of lattices $I_\mathfrak{p}$ of $B_\mathfrak{p}$ such that for almost all $\mathfrak{p}$ we have $I_\mathfrak{p} = I_{0,\mathfrak{p}}$. An *order* of $\widehat{B}$ is an lattice that is also a unital subring. One can show (see [Vig80], Proposition III.5.1) that these definitions do not depend on the choice of I_0. The fundamental result relating local lattices to global lattices is

Theorem 2.1.4 (Local-global correspondence). *Let F be a number field, and let B be a quaternion algebra over F. The associations*

$$I \longmapsto \widehat{I}$$
$$B \cap \prod_\mathfrak{p} I_\mathfrak{p} \longleftarrow\!\shortmid \prod_\mathfrak{p} I_\mathfrak{p}$$

give a bijection between the set of lattices of B and the set of lattices of $\widehat{B}$, and restrict to give a bijection between the set of orders of B and the set of orders of $\widehat{B}$.

Let $J \subset I$ be two lattices of B. Then the canonical map $I/J \to \widehat{I}/\widehat{J}$ is an isomorphism.

Proof. [Vig80], Proposition III.5.1. The second part follows from strong approximation for the additive group of B, see [Vig80], Théorème III.1.4.2. Alternatively, this map is an isomorphism by the Chinese remainder theorem. □

Let $\mathcal{O}$ be an order of B. By Proposition I.4.2 in [Vig80], $\mathcal{O}$ is contained in a maximal order $\mathcal{O}(1)$. The quotient $\mathbf{Z}_F$-module $\mathcal{O}(1)/\mathcal{O}$ is a finite $\mathbf{Z}_F$-module, hence there exist $\mathbf{Z}_F$-ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ such that

$$\mathcal{O}(1)/\mathcal{O} \cong \prod_{k=1}^{n} \mathbf{Z}_F/\mathfrak{a}_k, \tag{2.1}$$

We define the *level* of of $\mathcal{O}$ to be the $\mathbf{Z}_F$-ideal $\prod_k \mathfrak{a}_k$. This does not depend on the choice of $\mathcal{O}(1)$. Indeed, we could also have defined it in terms of the discriminant of $\mathcal{O}$, as in Section III.5.A of [Vig80].

Consider the finite idèle group $\widehat{F}^\times$ of F with the idèle topology. Let $\widehat{\mathbf{Z}}_F^\times$ be the unique maximal compact subgroup of $\widehat{F}^\times$. A basis of open subgroups of $\widehat{F}^\times$ is formed by the compact open subgroups

$$\prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(k_{\mathfrak{p}})} \subset \widehat{\mathbf{Z}}_F^\times, \tag{2.2}$$

where the $k_{\mathfrak{p}}$ are non-negative integers that are 0 for almost all $\mathfrak{p}$ and

$$U_{\mathfrak{p}}^{(k_{\mathfrak{p}})} = \mathbf{Z}_{F,\mathfrak{p}}^\times \cap (1 + \mathfrak{p}^{k_{\mathfrak{p}}}). \tag{2.3}$$

Let F^+ be the group of totally positive units of F, and let N be a subgroup of $\widehat{\mathbf{Z}}_F^\times$. Then we denote

$$\mathrm{Cl}(N\infty) = F^+ \backslash \widehat{F}^\times / N$$

and

$$\mathrm{Cl}(N) = F^\times \backslash \widehat{F}^\times / N.$$

If in addition N is open, then we denote by $F_{N\infty}$ the finite abelian extension of F corresponding to $\mathrm{Cl}(N\infty)$ by class field theory. Finally, if N is a basic open subset as in (2.2), then we denote

$$\mathrm{Cl}\left(\prod_{\mathfrak{p}\,:\,k_{\mathfrak{p}}>0} \mathfrak{p}^{k_{\mathfrak{p}}} \infty \right) = \mathrm{Cl}(N\infty).$$

The corresponding class field is denoted in a similar fashion. In particular, taking $k_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$, we obtain the narrow class group $\mathrm{Cl}(\infty)$ of F and the narrow Hilbert class field F_∞.

Now let B be a quaternion algebra over F and consider the multiplicative group $\widehat{B}^\times$ of $\widehat{B}$. As in Chapter 4 of [Milb], the group $\widehat{B}^\times$ has a natural topology. Let $\mathcal{O}$ be an order of B, and let $\widehat{\mathcal{O}}^\times$ be the subgroup $\prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^\times$ of $\widehat{B}^\times$. Let $\mathcal{O}(1)$ be a maximal order containing $\mathcal{O}$. Then by Section 2.9 of [Shi70], a basis of open subgroups of $\widehat{B}^\times$ contained in $\widehat{\mathcal{O}}(1)^\times$ is formed by the compact open subgroups

$$\left\{b \in \widehat{\mathcal{O}}(1)^\times : b - 1 \in \mathfrak{N}\widehat{\mathcal{O}}(1)\right\} = \widehat{\mathcal{O}}(1)^\times \cap \prod_{\mathfrak{p}} \left(1 + \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{N})}\widehat{\mathcal{O}}(1)_{\mathfrak{p}}\right) \qquad (2.4)$$

of $\widehat{B}^\times$. Here $\mathfrak{N}$ is an integral ideal of F. This subgroup is contained in $\widehat{\mathcal{O}}^\times$ when we take $\mathfrak{N}$ equal to the level of $\mathcal{O}$. We conclude that the subgroup $\widehat{\mathcal{O}}^\times$ of $\widehat{B}^\times$ is compact open.

Remark. The group $\widehat{\mathcal{O}}^\times$ need not be the product of the closures of $\mathcal{O}^\times$ in the factors $\widehat{B}_{\mathfrak{p}}^\times$. For instance, if B is definite, then $\mathcal{O}^\times$ is finite, but all the factors $\mathcal{O}_{\mathfrak{p}}^\times$ are infinite.

One can describe the ideals of an order $\mathcal{O}$ of B using the adèlic groups above. We say that a left (respectively right) $\mathcal{O}$-order I is *locally principal* if there exists an element $\widehat{b}$ of $\widehat{B}$ such that $\widehat{I} = \widehat{\mathcal{O}}\widehat{b}$ (respectively $\widehat{I} = \widehat{b}\widehat{\mathcal{O}}$). Moreover, two left (respectively right) $\mathcal{O}$-ideals I and J are called *equivalent* if there exists a b in $B^\times$ such that $I = Jb$ (respectively $I = bJ$). We denote the set of equivalence classes of locally principal left (respectively right) $\mathcal{O}$-ideals by $\mathrm{Pic}_l(\mathcal{O})$ (respectively $\mathrm{Pic}_r(\mathcal{O})$).

Corollary 2.1.5. *Let $\mathcal{O}$ be an order of a quaternion algebra B.*

(i) The assignment

$$\widehat{b} \longmapsto B \cap \widehat{b}\widehat{\mathcal{O}}$$

gives a bijection from the quotient $\widehat{B}^\times/\widehat{\mathcal{O}}^\times$ to the set of locally principal right $\mathcal{O}$-ideals of B.

(ii) The assignment from (i) induces a bijection $B^\times\backslash\widehat{B}^\times/\widehat{\mathcal{O}}^\times \to \mathrm{Pic}_r(\mathcal{O})$.

(iii) Let I be the right $\mathcal{O}$-ideal represented by an element $\widehat{b}$ of $\widehat{B}^\times$. Then given an element b of B, we have

$$b\widehat{b}\widehat{\mathcal{O}}^\times = \widehat{b}\widehat{\mathcal{O}}^\times \iff b\widehat{b}\widehat{\mathcal{O}} = \widehat{b}\widehat{\mathcal{O}} \iff bI = I.$$

2.2 Eichler orders

Throughout this section, let B be a quaternion algebra over a number field or non-archimedean local field F. If F is local and B is ramified, then the algebra B admits a unique maximal order (*cf.* Lemme II.1.5 of [Vig80]). In general, B will have multiple maximal orders. If F is local and B is split, then the set of maximal orders of B is described by a Bruhat-Tits tree (*cf.* Section II.2 of [Vig80], and also see Chapter 5). This section considers the following generalization of maximal orders:

Definition 2.2.1. *Let B be a quaternion algebra. An* Eichler order *of B is the intersection of two maximal orders of B.*

In particular, all maximal orders of B are Eichler. As we saw in the introduction, Eichler orders are natural generalizations of the orders

$$\mathcal{O}(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) : c \equiv 0 \pmod{N} \right\}$$

of $M_2(\mathbf{Q})$ that figure prominently in classical modular arithmetic geometry. We shall further elucidate this connection by giving a local description of Eichler orders.

Proposition 2.2.2. *Let $\mathcal{O}$ be an Eichler order of B.*

(i) At primes $\mathfrak{p}$ where B ramifies, $\mathcal{O}_\mathfrak{p}$ equals the unique maximal order of $B_\mathfrak{p}$.

(ii) At primes $\mathfrak{p}$ where B splits, choose an isomorphism $B_\mathfrak{p} \cong M_2(F_\mathfrak{p})$. Then there is a unique integer $n \in \mathbf{Z}_{\geq 0}$ such that under this isomorphism, $\mathcal{O}_\mathfrak{p}$ is conjugate to the suborder

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}_{F,\mathfrak{p}}) : c \in \mathfrak{p}^n \right\}$$

of $M_2(F_\mathfrak{p})$. This integer equals the exponent of $\mathfrak{p}$ in the level of $\mathcal{O}$.

(iii) Let $\mathfrak{p}$ be a prime where B splits, and suppose that the localization $\mathcal{O}_\mathfrak{p}$ has level $\mathfrak{p}^n$ with $n > 1$. Then there are $n+1$ maximal orders $\mathcal{O}(1)_\mathfrak{p}$ of $B_\mathfrak{p}$ containing $\mathcal{O}_\mathfrak{p}$, and exactly two $\mathcal{O}(1)_\mathfrak{p}$ such that one has an isomorphism of $\mathbf{Z}_F$-modules

$$\mathcal{O}(1)_\mathfrak{p} / \mathcal{O}_\mathfrak{p} \cong \mathbf{Z}_{F,\mathfrak{p}} / \mathfrak{p}^n.$$

(iv) If the level of $\mathcal{O}$ is square-free, then all $\mathcal{O}$-ideals are locally principal.

Proof. See Lemme 1.5, Théorème II.2.3 and Lemme II.2.4 in [Vig80]. Note that although (iii) is stated incorrectly in the conclusion of the proof of Lemme II.2.4, the proof in fact also shows how to obtain (iii). □

The following proposition can be seen as a partial converse of the previous.

Proposition 2.2.3 ([Eic55])**.** *Let $\mathcal{O}$ be an Eichler order maximal at a prime $\mathfrak{p}$, and let $\mathcal{O}(\mathfrak{p})$ be a level $\mathfrak{p}$ suborder of $\mathcal{O}$. Then $\mathcal{O}(\mathfrak{p})$ is an Eichler order.*

We will use the following Proposition in Section 2.5:

Proposition 2.2.4. *Let F be a non-archimedean local field. Let $\mathbf{Z}_F$ be the valuation ring of F, and let $\mathfrak{p}$ be the unique prime ideal of $\mathbf{Z}_F$.*

Let $B = M_2(F)$, and let $\mathcal{O}(\mathfrak{p}^n)$ be a level $\mathfrak{p}^n$ Eichler order of B, where $n \geq 1$. Let $\mathcal{O}(1)$ be a maximal order containing $\mathcal{O}(\mathfrak{p}^n)$, and let $q = |\mathbf{Z}_F/\mathfrak{p}|$. Then

$$[\mathcal{O}(1)^\times : \mathcal{O}(\mathfrak{p}^n)^\times] = (q+1)q^{n-1}$$

and we have

$$\mathrm{nrd}(\mathcal{O}(\mathfrak{p}^n)^\times) = \mathrm{nrd}(\mathcal{O}(1)^\times) = \mathbf{Z}_F^\times.$$

Proof. We use the local description in Lemme II.2.4 of [Vig80]: there exists an F-basis of B such that $\mathcal{O}(1)$ is given by $M_2(\mathbf{Z}_F)$ and the suborder $\mathcal{O}(\mathfrak{p}^n)$ is of the form

$$\mathcal{O}(\mathfrak{p}^n) = \begin{pmatrix} \mathbf{Z}_F & \mathfrak{p}^a \\ \mathfrak{p}^b & \mathbf{Z}_F \end{pmatrix}.$$

One has $n = a + b$.

We can compute the index $[\mathcal{O}(1)^\times : \mathcal{O}(\mathfrak{p}^n)^\times]$ after reducing modulo $\mathfrak{p}^n$. On the one hand, we have

$$|\mathrm{GL}_2(\mathbf{Z}_F/\mathfrak{p}^n)| = (q-1)^2 q^{4n-3}(q+1).$$

On the other hand, the image of $\mathcal{O}(\mathfrak{p}^n)^\times$ in this ring is given by the matrices in $\mathrm{GL}_2(\mathbf{Z}_F)$ whose diagonal elements are invertible and whose off-diagonal elements have valuations are at least a and b, respectively. We get

$$|\mathrm{Im}(\mathcal{O}(\mathfrak{p}^n)^\times)| = ((q-1)q^{n-1})^2 q^{n-a} q^{n-b} = (q-1)^2 q^{3n-2}.$$

Taking the quotient, we get the first statement of the proposition. The statement on norms is also clear from this description. □

2.3 More orders

We now consider somewhat more general orders than Eichler orders. A lot of the orders $\mathcal{O}$ in the upcoming Table A.2 have the property that there exist a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$ and a squarefree ideal $\mathfrak{N}$ such that $\mathfrak{N}\mathcal{O}(1) \subseteq \mathcal{O}$. The propositions constituting this section give a local description of such orders. Throughout, we let F be a non-archimedean local field with valuation ring $\mathbf{Z}_F$. Let $\mathfrak{p}$ be the unique prime ideal of $\mathbf{Z}_F$, uniformized by π. Let κ be the residue field $\mathbf{Z}_F/\mathfrak{p}$, and let $q = |\kappa|$. As in (2.3), we denote

$$U^{(k)} = \mathbf{Z}_F^\times \cap (1 + \mathfrak{p}^k).$$

Let

$$\varphi : \lambda \longrightarrow M_2(\kappa)$$

be an embedding of the unique quadratic field extension λ of κ into the matrix ring $M_2(\kappa)$. For example, a choice of basis for λ over κ results in an embedding

$$\begin{aligned} \lambda &\longrightarrow \mathrm{End}_\kappa(\lambda) \cong M_2(\kappa) \\ x &\longmapsto (x\cdot : y \mapsto xy) \end{aligned}$$

Two such embeddings are conjugate by the Skolem-Noether theorem (I.2.1 in [Vig80]).

Proposition 2.3.1. *Let $B = M_2(F)$. Let $\mathcal{O}(1)$ be the maximal order $M_2(\mathbf{Z}_F)$ of B. Let $\mathcal{O} \subseteq \mathcal{O}(1)$ be an order such that $\mathfrak{p}\mathcal{O}(1) \subset \mathcal{O}$. Then up to conjugation by elements of $\mathcal{O}(1)^\times$, the order $\mathcal{O}$ is of exactly one of the following forms:*

(i) $\mathcal{O} = \mathcal{O}(1)$;

(ii) $\mathcal{O} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{O}(1) : c \equiv 0 \pmod{\mathfrak{p}} \right\}$;

(iii) $\mathcal{O} = \{x \in \mathcal{O}(1) : x \pmod{\mathfrak{p}} \in \varphi(\lambda)\}$;

(iv) $\mathcal{O} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{O}(1) : a \equiv d \pmod{\mathfrak{p}}, c \equiv 0 \pmod{\mathfrak{p}} \right\}$;

(v) $\mathcal{O} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{O}(1) : b \equiv c \equiv 0 \pmod{\mathfrak{p}} \right\}$;

(vi) $\mathcal{O} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{O}(1) : a \equiv d \pmod{\mathfrak{p}}, b \equiv c \equiv 0 \pmod{\mathfrak{p}} \right\}$;

The following table summarizes the properties of the $\mathcal{O}$ above:

Case	*Level*	$[\mathcal{O}(1)^\times : \mathcal{O}^\times]$	$\mathrm{nrd}(\mathcal{O}^\times)$
(i)	(1)	1	$\mathbf{Z}_F^\times$
(ii)	$\mathfrak{p}$	$q+1$	$\mathbf{Z}_F^\times$
(iii)	$\mathfrak{p}^2$	$(q-1)q$	$\mathbf{Z}_F^\times$
(iv)	$\mathfrak{p}^2$	$(q-1)(q+1)$	$U^{(1)}\mathbf{Z}_F^{\times 2}$
(v)	$\mathfrak{p}^2$	$q(q+1)$	$\mathbf{Z}_F^\times$
(vi)	$\mathfrak{p}^3$	$(q-1)q(q+1)$	$U^{(1)}\mathbf{Z}_F^{\times 2}$

$\mathcal{O}$ is an Eichler order if and only if we are in case (i), (ii) or (v). Up to conjugation, the inclusion relations between these orders are as follows:

$$\begin{tikzcd}
& \text{(iii)} \arrow[rrd] & & \\
\text{(vi)} \arrow[ru] \arrow[r] \arrow[rd] & \text{(iv)} \arrow[r] & \text{(ii)} \arrow[r] & \text{(i)} \\
& \text{(v)} \arrow[ru] \arrow[rru] & &
\end{tikzcd}$$

Proof. We have $\mathfrak{p}M_2(\mathbf{Z}_F) \subset \mathcal{O}$ by hypothesis: we are therefore reduced to determining the κ-subalgebras of $M_2(\kappa)$. Note that all these algebras contain the diagonal matrices, hence are at worst of index q^3. Case (i) is clear, and case (ii) is indeed the only index q subalgebra by Proposition 2.2.3. Also, case (vi) clearly corresponds to the only index q^3 subalgebra of $M_2(\kappa)$.

The algebras of index q^2 correspond to the quadratic algebra extensions of κ embedding into $M_2(\kappa)$. It turns out that all these algebras allow an embedding, and the cases (iii), (iv), (v) correspond to the algebras

$$\lambda,\ \kappa[\epsilon],\ \kappa \oplus \kappa$$

respectively. These embedded algebras can indeed be conjugated to the standard form above. We saw this for case (iii) in the discussion before the proposition, and the other two cases are even easier. In case (iv), for example, this follows from the fact that every non-zero nilpotent matrix in $M_2(\kappa)$ is conjugate to the matrix

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

The indices $[\mathcal{O}(1)^\times : \mathcal{O}^\times]$ can be calculated by reducing modulo $\mathfrak{p}$ as in Proposition 2.2.4. We omit the details and focus on the norm groups. If we let

$$\mathcal{O}(1)^{(1)} = \left\{ x \in \mathcal{O}(1) : x \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{p}} \right\},$$

then we obviously have $\mathrm{nrd}(\mathcal{O}(1)^{(1)}) = U^{(1)}$. We have $\mathcal{O}(1)^{(1)} \subset \mathcal{O}^\times$ for all the orders $\mathcal{O}$ under consideration. Hence we need only determine the image of

$$\mathcal{O}^\times \xrightarrow{\mathrm{nrd}} \mathbf{Z}_F^\times \longrightarrow \kappa^\times.$$

Because the diagonal matrices are in $\mathcal{O}$, this image clearly contains $\kappa^{\times 2}$. Hence $\mathrm{nrd}(\mathcal{O}^\times)$ contains $U^{(1)}\mathbf{Z}_F^{\times 2}$.

We clearly have $\mathrm{nrd}(\mathcal{O}^\times) = U^{(1)}\mathbf{Z}_F^{\times 2}$ in case (vi), and we have already seen that $\mathrm{nrd}(\mathcal{O}^\times) = \mathbf{Z}_F^\times$ in case (i) and (ii). As for the remaining cases, they follow because $\kappa[\epsilon]$ is the only algebra extension of κ for which the norm to κ does not surject (except when κ is of characteristic 2, but then $U^{(1)}\mathbf{Z}_F^{\times 2} = \mathbf{Z}_F^\times$ anyhow).

As for the final part of the proposition, cases (i) and (ii) are clearly Eichler. The order $\mathcal{O}$ of case (v) can be obtained as the intersection of maximal orders

$$\mathcal{O} = \begin{pmatrix} 0 & \pi \\ 1 & 0 \end{pmatrix} \mathcal{O}(1) \begin{pmatrix} 0 & \pi \\ 1 & 0 \end{pmatrix}^{-1} \cap \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix} \mathcal{O}(1) \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}^{-1}.$$

Cases (iii), (iv) and (vi) do not correspond to Eichler orders by Lemme 2.4(2) in [Vig80]. Finally, the inclusion relations are clear from what preceded. □

Remark. Part (v) of the proposition also shows that given an Eichler order $\mathcal{O}$, the quotient $\mathbf{Z}_F$-module $\mathcal{O}(1)/\mathcal{O}$ from (2.1) may indeed depend on the choice of a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$.

In what follows, we denote by $A(\lambda, \overline{u})$ the κ-algebra whose underlying κ-vector space is given by

$$\lambda 1 \oplus \lambda \overline{u}$$

and whose multiplication is given by

$$(a_1 + b_1\overline{u})(a_2 + b_2\overline{u}) = a_1a_2 + (a_1b_2 + b_1a_2^q)\overline{u}.$$

The *(reduced) norm* (respectively *(reduced) trace*) of an element $a + b\overline{u}$ of $A(\lambda, \overline{u})$ is defined to be a^{q+1} (respectively $a + a^q$). These maps restrict to the usual norm and trace maps on the quadratic subalgebras of $A(\lambda, \overline{u})$.

Proposition 2.3.2. *Let B be the ramified quaternion algebra over F, and let $\mathcal{O}(1)$ be the maximal order of B. Then there is an isomorphism of algebras*

$$\mathcal{O}(1)/\mathfrak{p}\mathcal{O}(1) \cong A(\lambda, \overline{u}) \tag{2.5}$$

respecting the reduced norm and trace maps.

Let $\mathcal{O} \subseteq \mathcal{O}(1)$ be an order such that $\mathfrak{p}\mathcal{O}(1) \subset \mathcal{O}$, and let $\mathcal{O}/\mathfrak{p}$ be the image of $\mathcal{O}$ under the isomorphism (2.5). Then up to conjugation by the elements of the groups $\mathcal{O}(1)^\times$ or $N(\mathcal{O}(1)^\times)$, the algebra $\mathcal{O}/\mathfrak{p}$ is given by exactly one of the following:

(i) $\mathcal{O}/\mathfrak{p} = A(\lambda, \overline{u})$;

(ii) $\mathcal{O}/\mathfrak{p} = \kappa \oplus \lambda\overline{u}$;

(iii) $\mathcal{O}/\mathfrak{p} = \kappa \oplus \kappa(a + b\overline{u})$, *where a is a fixed element of $\lambda \backslash \kappa$ and b runs through a set of representatives for $\lambda/\lambda^{\times(q-1)}$;*

(iv) $\mathcal{O}/\mathfrak{p} = \kappa \oplus \kappa b\overline{u}$, *where b runs through a set of representatives for $\lambda^\times/\lambda^{\times 2}$;*

(v) $\mathcal{O}/\mathfrak{p} = \kappa \oplus \{0\}$.

The following table summarizes the properties of the $\mathcal{O}$ above:

Case	*Level*	$[\mathcal{O}(1)^\times : \mathcal{O}^\times]$	$\mathrm{nrd}(\mathcal{O}^\times)$
(i)	(1)	1	$\mathbf{Z}_F^\times$
(ii)	$\mathfrak{p}$	$q+1$	$U_\mathfrak{p}^{(1)} U_\mathfrak{p}^2$
(iii)	$\mathfrak{p}^2$	q^2	$\mathbf{Z}_F^\times$
(iv)	$\mathfrak{p}^2$	$q(q+1)$	$U_\mathfrak{p}^{(1)} U_\mathfrak{p}^2$
(v)	$\mathfrak{p}^3$	$q^2(q+1)$	$U_\mathfrak{p}^{(1)} U_\mathfrak{p}^2$

The order of B corresponding to case (ii) is the unique level $\mathfrak{p}$ order of B. Up to conjugation, the inclusion relations between these orders are as follows:

$$\begin{tikzcd}
 & \text{(iii)} \arrow[rrd] & & \\
\text{(v)} \arrow[ru] \arrow[r] & \text{(iv)} \arrow[r] & \text{(ii)} \arrow[r] & \text{(i)}
\end{tikzcd}$$

Proof. The first part of the proposition follows by reducing the isomorphism in Corollaire I.1.7 in [Vig80] modulo $\mathfrak{p}\mathcal{O}(1)$. Note that $\mathfrak{p}\mathcal{O}(1)$ is a two-sided ideal of $\mathcal{O}(1)$ since $\mathbf{Z}_F$ is in the center of $\mathcal{O}(1)$, and that the algebra $\mathcal{O}(1)/\mathfrak{p}\mathcal{O}(1)$ is not central simple over κ.

As in the previous proposition, case (i) and (v) are clear. As for case (ii), the given vector space is clearly a suborder. We claim that it is the unique level $\mathfrak{p}$ suborder of $A(\lambda, \overline{u})$. Indeed, for any other κ-subspace V of $A(\lambda, \overline{u})$, the projection

$$V \xrightarrow{\pi} \lambda \oplus \{0\}$$

is surjective. Let x be an element of the non-trivial intersection $V \cap (\{0\} \oplus \lambda\overline{u})$ Then one checks that $vx = \pi(v)x$ for all $v \in V$. Surjectivity of the projection map therefore implies that V contains the subspace $\{0\} \oplus \lambda\overline{u}$. Now if V were an order, it would also contains the subspace $\kappa \oplus \{0\}$. Hence because V has codimension 1, we would then have $V = \kappa \oplus \lambda\overline{u}$, contrary to what we assumed above.

We now consider the quadratic subalgebras Q of $A(\lambda, \overline{u})$. We have

$$Q = \kappa \oplus \kappa(a + b\overline{u})$$

for some $a + b\overline{u} \notin \kappa \oplus \{0\}$. The isomorphism class of Q as a κ-algebra is determined by the reduced trace and norm of $a + b\overline{u}$.

First we show that Q cannot be isomorphic to the split κ-algebra $\kappa \oplus \kappa$. Indeed, then Q would contain an element $a + b\overline{u}$ with

$$\begin{aligned} \operatorname{trd}(a + b\overline{u}) &= a + a^q = 1 \\ \operatorname{nrd}(a + b\overline{u}) &= a^{q+1} = 0. \end{aligned}$$

This clearly cannot happen.

Next, suppose that Q as above is a field. Then a is an element of $\lambda \backslash \kappa$, and the projection map

$$Q \xrightarrow{\pi} \lambda \oplus \{0\}$$

is an isomorphism. Moreover, one calculates that for $c \neq 0$, one has

$$\begin{aligned} (c + d\overline{u})(a + b\overline{u})(c + d\overline{u})^{-1} &= (c + d\overline{u})(a + b\overline{u})(c^q - d\overline{u})/c^{q+1} \\ &= a + bc^{-q+1}u. \end{aligned}$$

This implies that up to conjugation by elements of $\mathcal{O}(1)^\times$, all Q that are fields are given by exactly one of the algebras in (iii). Note that taking $a = 0$ gives a suborder that is stable under conjugation.

To conclude that the same holds up to $N(\mathcal{O}(1)^\times)$-conjugation, we first remark that if we let $u \in \mathcal{O}(1)$ be a preimage of u, then $N(\mathcal{O}(1)^\times) = B^\times = \langle \mathcal{O}(1)^\times, u \rangle$. If we let $\widetilde{a} + \widetilde{b}u$ be an element of $\mathcal{O}$ lifting $a + b\overline{u}$, then Corollaire I.1.7 in [Vig80] shows that $u(\widetilde{a} + \widetilde{b}u)u^{-1}$ reduces to $a + b^q\overline{u}$ in $A(\lambda, u)$. But $b^q = b \cdot b^{q-1}$, so we could have obtained the corresponding conjugate algebra equally well by conjugating with an element of $\mathcal{O}(1)^\times$.

Finally, we consider the inseparable quadratic subalgebras Q of $A(\lambda, \overline{u})$. These are all of the form

$$Q = \kappa \oplus \kappa b\overline{u}.$$

Q determines b up to a $\kappa^\times$-multiple. The group $\kappa^\times$ consists of the $q+1$-powers in $\lambda^\times$. Conjugating as above again multiplies b by a $q-1$-power. Combining these two statements, we get (iv) up to $\mathcal{O}^\times$-conjugation. The proof up to $N(\mathcal{O}^\times)$-conjugation is the same as in the previous case.

Calculating the indices $[\mathcal{O}(1)^\times : \mathcal{O}^\times]$ is again trivial, so we conclude by calculating the norm groups $\operatorname{nrd}(\mathcal{O}^\times)$. For this, we remark that if we let

$$\mathcal{O}(1)^{(1)} = \operatorname{Ker}(\mathcal{O}(1)^\times \longrightarrow (\mathcal{O}(1)/\mathfrak{p}\mathcal{O}(1))^\times),$$

we have $\mathcal{O}(1)^{(1)} \subseteq \mathcal{O}^\times$ for all $\mathcal{O}$ as above. But if we let L be the unramified quadratic extension of F, then Corollaire II.1.7 in [Vig80] shows that

$$U_L^{(1)} \subseteq \mathcal{O}(1)^{(1)}.$$

Now

$$\operatorname{nrd}(U_L^{(1)}) = U_F^{(1)}$$

by Corollary V.1.2 in [Neu99]. Taking this into consideration, deriving the table and the inclusion relations is straightforward. □

A more general analysis of non-Eichler orders in quaternion algebras can be found in [HPS89].

2.4 Norms

This section is dedicated to the explicit determination of the image of the unit groups of orders of $\widehat{B}^\times$ under the reduced norm map.

Let F be a totally real number field, and let B be a quaternion algebra over F. Then we denote

$$F_B^\times = \left\{ x \in F^\times : \iota(x) > 0 \text{ for all } \iota \text{ dividing } \mathfrak{D}(B)^\infty \right\}.$$

The main result on norms in quaternion algebras, due to Eichler, is as follows.

Theorem 2.4.1 (Eichler norm theorem)**.** *Let B be a quaternion algebra over a field F.*

(i) If F is a non-archimedean local field, then $\operatorname{nrd}(B^\times) = F^\times$.

(ii) If F is a totally real number field, then $\operatorname{nrd}(B^\times) = F_B^\times$.

Proof. Part (i) is clear from the description of quaternion algebras over local fields in Chapitre II of [Vig80]. Part (ii) is Théorème III.4.1 in *loc. cit.* □

Let $\mathbf{Z}_F^+ = \mathbf{Z}_F^\times \cap F^+$ as in the introduction, and let $\mathbf{Z}_{F,B}^\times = \mathbf{Z}_F^\times \cap F_B^\times$. The following proposition is a consequence of strong approximation (Theorem 2.5.1).

Proposition 2.4.2. *Let B be an indefinite quaternion algebra over totally real number field F. Let K be a compact open subgroup of $\widehat{B}^\times$, and let $\mathcal{O}$ be an Eichler order of B.*

(i) The group $\operatorname{nrd}(K)$ *is an open subgroup of $\widehat{\mathbf{Z}}_F^\times$. Moreover,*

$$\operatorname{nrd}(K \cap B^\times) = \operatorname{nrd}(K) \cap \mathbf{Z}_{F,B}^\times.$$

(ii) We have

$$\operatorname{nrd}(\widehat{\mathcal{O}}^\times) = \widehat{\mathbf{Z}}_F^\times$$

and

$$\operatorname{nrd}(\mathcal{O}^\times) = \mathbf{Z}_{F,B}^\times.$$

Proof. The first part can be proved as in [Vig80], Proposition III.5.8. The second part then follows from Proposition 2.2.4. □

For more general orders $\mathcal{O}$, the image $\mathrm{nrd}(\widehat{\mathcal{O}}^\times) \subset \widehat{\mathbf{Z}}_F^\times$ can be determined as follows.

Algorithm 2.4.3. *Let B be a quaternion algebra over a number field or a non-archimedean local field F, and let $\mathcal{O}$ be an order of B. The following algorithm determines the group*

$$N = \mathrm{nrd}(\widehat{\mathcal{O}}^\times) = \prod_{\mathfrak{p}} \mathrm{nrd}(\mathcal{O}_\mathfrak{p}^\times) \subset \widehat{\mathbf{Z}}_F^\times .$$

1. *Determine the level $\mathfrak{N}$ of $\mathcal{O}$.*

2. *For $\mathfrak{p}$ not dividing $\mathfrak{N}$, set $N_\mathfrak{p} = \mathbf{Z}_{F,\mathfrak{p}}^\times$.*

3. *If no primes $\mathfrak{p}$ of F divide $\mathfrak{N}$, then terminate. Otherwise, choose a prime $\mathfrak{p}$ dividing $\mathfrak{N}$ and go to step 4.*

4. *Determine a $\mathbf{Z}_{F,\mathfrak{p}}$-basis for $\mathcal{O}_\mathfrak{p}$, and determine the polynomial map $f : \mathbf{Z}_{F,\mathfrak{p}}^4 \to \mathbf{Z}_{F,\mathfrak{p}}$ corresponding to* nrd.

5. *Determine an n such that all elements of $U_\mathfrak{p}^{(n)}$ lift to an element of $\mathbf{Z}_{F,\mathfrak{p}}^4$ under f.*

6. *Determine the image of* $\mathrm{nrd}(\mathcal{O}_\mathfrak{p})$ *in the finite group $\mathbf{Z}_{F,\mathfrak{p}}^\times / U_\mathfrak{p}^{(n)}$ by calculating the image of the factorization*

$$\overline{f} : (\mathbf{Z}_{F,\mathfrak{p}}/\mathfrak{p}^n)^4 \longrightarrow \mathbf{Z}_{F,\mathfrak{p}}/\mathfrak{p}^n .$$

   Set $N_\mathfrak{p}$ equal to the corresponding subgroup of $\mathbf{Z}_{F,\mathfrak{p}}^\times$.

7. *If $N_\mathfrak{p}$ has been calculated for all $\mathfrak{p}$ dividing $\mathfrak{N}$, then terminate. Otherwise, choose a new $\mathfrak{p}$ dividing $\mathfrak{N}$ and go to step 4.*

Proof of correctness. The only parts that require proof are steps 2, 4 and 5. As for step 2, it follows from the local-global correspondence in Theorem 2.1.4 that $\mathcal{O}$ is maximal at any prime not dividing its level. In step 4, a $\mathbf{Z}_{F,\mathfrak{p}}$-basis for $\mathcal{O}_\mathfrak{p}$ exists since $\mathbf{Z}_{F,\mathfrak{p}}$ is a discrete valuation ring. Finally, the existence of an n as in step 5 follows from the fact (which is just a reformulation of Hensel's lemma) that the reduced norm map, being a polynomial map, is open: note that $1 \in \widehat{\mathbf{Z}}_F^\times$ is in its image. □

Remark. More naively, one can dispense with the use of Hensel's lemma in step 5 by remarking that since $\mathcal{O}_\mathfrak{p}$ contains $\mathbf{Z}_{F,\mathfrak{p}}$, the norm group $\mathrm{nrd}(\mathcal{O}_\mathfrak{p}^\times)$ contains the open subgroup $\mathbf{Z}_{F,\mathfrak{p}}^{\times 2}$ of $\mathbf{Z}_{F,\mathfrak{p}}^\times$. One then takes n such that $\mathbf{Z}_{F,\mathfrak{p}}^{\times 2}$ contains $U_\mathfrak{p}^{(n)}$ and goes to step 6. This is the approach taken in our implementation of this algorithm at [Sij10].

2.5 Indices

Let B be a quaternion algebra over a field F. Let B^1 be the subgroup of elements of $B^\times$ consisting of the elements of reduced norm equal to 1. Additionally, if F is a number field, let $(B \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}})^1$ (respectively $\widehat{B}^1$ and $B^{\mathfrak{p}1}$) be the similarly defined subgroup of $(B \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}})^\times$ (respectively $\widehat{B}^\times$ and $B^{\mathfrak{p}\times}$). We will make use of the following fundamental result.

Theorem 2.5.1 (Strong approximation)**.** *Let F be a number field, let B be a quaternion algebra over F, and S be a set of places of F containing at least one place at which B splits. Consider the group*

$$B_S^1 = \prod_{v \in S} B^1(F_v) \subset (B \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}})^1.$$

Then $B^1 B_S^1$ is dense in $(B \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}})^1$.

Proof. [Vig80], III.4.3. For generalizations, see Theorem 4.6 in [Milb] and the accompanying discussion and references. □

Corollary 2.5.2. *Let F be a totally real number field.*

(i) Let B be an indefinite quaternion algebra over F. Then B^1 is dense in $\widehat{B}^1$.

(ii) Let H be a definite quaternion algebra over F. Then for any finite prime $\mathfrak{p}$ at which H is split, $H^1 H_{\mathfrak{p}}^1$ is dense in $\widehat{H}^1$.

We conclude this section by describing how to compute global indices in terms of local indices for indefinite algebras B, but not before fixing some more notation. We have already defined the group B^1, and now we additionally define B^+ to be the group of units of B whose norm is totally positive. Similarly, given an order $\mathcal{O}$, we can define subgroups $\mathcal{O}^1$ and $\mathcal{O}^+$ of $\mathcal{O}^\times$. Given a compact open subgroup $K \subset \widehat{B}^\times$, we denote $K^1 = K \cap \widehat{B}^1$. We also define the global groups

$$K_B^+ = K \cap B^+ \tag{2.6}$$

and

$$K_B^1 = K \cap B^1. \tag{2.7}$$

Note that $\mathcal{O}^1 = \widehat{\mathcal{O}}_B^1$ and $\mathcal{O}^+ = \widehat{\mathcal{O}}_B^+$. We obtain subgroups $\mathrm{P}K_B^+$ and $\mathrm{P}K_B^1$ of the adjoint group $\mathrm{P}B^\times = B^{\times\mathrm{ad}} = B^\times / F^\times$ of $B^\times$.

Proposition 2.5.3. *Let B be an indefinite algebra and let $K' \subseteq K$ be two compact open subgroups of $\widehat{B}^\times$.*

(i) We have

$$[K_B^1 : K_B'^1] = \frac{[K : K']}{[\mathrm{nrd}(K) : \mathrm{nrd}(K')]}.$$

(ii) *We have*

$$[K_B^+ : K_B'^+] = \frac{h[K : K']}{[\mathrm{nrd}(K) : \mathrm{nrd}(K')]},$$

where

$$h = |\mathrm{Im}(\mathrm{nrd}(K) \cap \mathbf{Z}_F^+ \longrightarrow \mathrm{nrd}(K)/\mathrm{nrd}(K'))|.$$

(iii) *If $K' \cap F^\times = K \cap F^\times$, then the equalities in (i) and (ii) also hold for the indices $[\mathrm{P}K_B^1 : \mathrm{P}K_B'^1]$ and $[\mathrm{P}K_B^+ : \mathrm{P}K_B'^+]$, respectively.*

Proof. We prove (ii): case (i) is similar to case (ii), and (iii) is obvious. Consider the sequence of maps

$$K_B^+/K_B'^+ \xrightarrow{\varphi} K/K' \xrightarrow{\psi} \mathrm{nrd}(K)/\mathrm{nrd}(K').$$

The map φ is clearly injective. We prove (ii) by showing

$$\mathrm{Im}(\varphi) = \psi^{-1}(N), \tag{2.8}$$

where

$$N = \mathrm{Im}(\mathrm{nrd}(K) \cap \mathbf{Z}_F^+ \longrightarrow \mathrm{nrd}(K)/\mathrm{nrd}(K')).$$

The inclusion $\mathrm{Im}(\varphi) \subset \psi^{-1}(N)$ is trivial. Conversely, suppose we are given a coset kK' mapping to an element n of N under ψ. Let $k' \in K'$ be such that $\mathrm{nrd}(kk'^{-1})$ is in $\mathrm{nrd}(K) \cap \mathbf{Z}_F^+$. Using Proposition 2.4.2, we see that there exists an element b of K_B^+ such that $\mathrm{nrd}(b) = \mathrm{nrd}(kk'^{-1})$. Therefore $\mathrm{nrd}(b^{-1}kk'^{-1})$ is equal to 1. By Corollary 2.5.2(i), there exists a $b_1 \in B^1$ and a $k_1 \in K'^1$ for which we have

$$b_1 k_1 = b^{-1}kk'^{-1}.$$

But then $bb_1 = kk'^{-1}k_1^{-1}$ is in K_B^+ and represents the coset kK'. □

We calculate these indices in a few special cases. Note that for all orders $\mathcal{O}$ of B, we have

$$\widehat{\mathcal{O}}^\times \cap F^\times = \mathcal{O}^\times \cap F^\times = \mathbf{Z}_F^\times. \tag{2.9}$$

Corollary 2.5.4. *Let $n > 0$. Let $\mathcal{O}(\mathfrak{p}^n) \subseteq \mathcal{O}(1)$ be an inclusion of a level $\mathfrak{p}^n$ Eichler order into a maximal order, and let $q = \mathrm{Nm}(\mathfrak{p})$. Then*

$$[\mathrm{P}\mathcal{O}(1)^1 : \mathrm{P}\mathcal{O}(\mathfrak{p}^n)^1] = [\mathrm{P}\mathcal{O}(1)^+ : \mathrm{P}\mathcal{O}(\mathfrak{p}^n)^+] = q^{n-1}(q+1).$$

Proof. Using the previous proposition, this is clear considering (2.9) and Proposition 2.2.4. □

Corollary 2.5.5. *Let $\mathcal{O}(1)$ be maximal, and let $\mathcal{O} \subseteq \mathcal{O}(1)$ be a inclusion of orders such that*

$$\mathfrak{p}\mathcal{O}(1) \subseteq \mathcal{O}.$$

Let κ be the residue field $\mathbf{Z}_F/\mathfrak{p}$.

(i) We have

$$[\mathrm{P}\mathcal{O}(1)^1 : \mathrm{P}\mathcal{O}^1] = [\widehat{\mathcal{O}}(1)^\times : \widehat{\mathcal{O}}^\times]/d,$$

where $d \in \{1,2\}$ equals 2 if and only if $\mathfrak{p}$ is odd and the final column of the row corresponding to $\mathcal{O}$ in the table in Proposition 2.3.1 or 2.3.2 is given by $U^{(1)}\mathbf{Z}_F^{\times 2}$.

(ii) We have

$$[\mathrm{P}\mathcal{O}(1)^+ : \mathrm{P}\mathcal{O}^+] = [\widehat{\mathcal{O}}(1)^\times : \widehat{\mathcal{O}}^\times]n/d,$$

where d is as above and $n \in \{1,2\}$ equals 2 if and only if d equals 2 and the canonical map $\mathbf{Z}_F^+ \longrightarrow \kappa^\times/\kappa^{\times 2}$ is surjective.

Proof. This is clear from Propositions 2.3.1 and 2.3.2 as $\mathbf{Z}_{F,\mathfrak{p}}^\times/U_\mathfrak{p}^{(1)} \cong \kappa^\times$ is a cyclic group of order $\mathrm{Nm}(\mathfrak{p}) - 1$, which is odd if and only if $\mathfrak{p}$ is even. □

Remark. The Corollaries above clearly generalize to composite level. In the calculations in Chapter 7, however, the level will contain only one prime.

2.6 Class and type numbers

Let B be a quaternion algebra over a totally real number field F that, for simplicity, we suppose to be split at exactly one infinite place ι of F. Let $K \subset \widehat{B}^\times$ be a compact open subgroup, and consider the double quotients

$$\mathrm{Pic}_r(K) = B^\times \backslash \widehat{B}^\times / K$$

and

$$\mathrm{Pic}_r(K\infty) = B^\times \backslash \{\pm 1\} \times \widehat{B}^\times / K.$$

Here $b \in B^\times$ acts on $\widehat{B}^\times$ through left multiplication and on $\{\pm 1\}$ through multiplication by the sign of $\mathrm{nrd}(b)$ at ι.

We call the cardinality $|\mathrm{Pic}_r(K)|$ (respectively $|\mathrm{Pic}_r(K\infty)|$) the *class number* (respectively *narrow class number*) of K. The motivation for this terminology is the following. Let $K = \widehat{\mathcal{O}}^\times$, where $\mathcal{O}$ is an order of B. Then we have $\mathrm{Pic}_r(K) = \mathrm{Pic}_r(\mathcal{O})$ (*cf.* Section 2.1). Moreover, for elements (a, b) of $\{\pm 1\} \times \widehat{B}^\times$ we can consider the association

$$(a, b) \rightsquigarrow (B \cap b\widehat{\mathcal{O}}, a).$$

This induces a bijection between $\mathrm{Pic}_r(K\infty)$ and the set of equivalence classes of locally principal right $\mathcal{O}$-ideals equipped with an orientation at the infinite place ι.

Similarly, we introduce the double quotient

$$T(K\infty) = B^\times \backslash \{\pm 1\} \times \widehat{B}^\times / N(K)$$

Its cardinality is called the *narrow type number* of K. For $K = \widehat{\mathcal{O}}^\times$, it classifies the orders locally conjugate to $\mathcal{O}$ equipped with an orientation at ι modulo global conjugation. This is accomplished by the association

$$(a, b) \rightsquigarrow (B \cap b\widehat{\mathcal{O}}b^{-1}, a),$$

cf. [Vig80], Section III.5.B.

Remarks. (i) Suppose that K is of the form $\widehat{\mathcal{O}}^\times$. Then since the quotient $B^\times \backslash \{\pm 1\}$ is trivial, we can also describe $\mathrm{Pic}_r(K\infty)$ as the set of locally principal right $\mathcal{O}$-ideals modulo left multiplication by elements of B^+. Similarly, $T(K\infty)$ describes the orders locally conjugate to $\mathcal{O}$ modulo global conjugation by elements of B^+.

(ii) Note that if $K = \widehat{\mathcal{O}}^\times$ for an Eichler order $\mathcal{O}$, then by Théorème II.2.3 and Lemme II.2.4 in [Vig80], we can remove the hypotheses on local principality and local conjugacy in the descriptions of $\mathrm{Pic}_r(K\infty)$ and $T(K\infty)$ in (i).

Proposition 2.6.1. *Let B and K be as at the beginning of this dection.*

(i) The reduced norm map induces a bijection

$$\mathrm{Pic}_r(K\infty) \xrightarrow{\sim} F_B^\times \backslash \{\pm 1\} \times \widehat{F}^\times / \mathrm{nrd}(K) \cong \mathrm{Cl}(\mathrm{nrd}(K)\infty). \qquad (2.10)$$

(ii) Similarly, it induces a bijection

$$T(K\infty) \xrightarrow{\sim} F_B^\times \backslash \{\pm 1\} \times \widehat{F}^\times / \mathrm{nrd}(N(K)) \cong \mathrm{Cl}(\mathrm{nrd}(N(K))\infty). \qquad (2.11)$$

The cardinality $|T(K\infty)|$ is a power of 2.

Proof. The isomorphisms (2.10) and (2.11) are straightforward generalizations of Corollaire III.5.7 in [Vig80]. Since we shall see the proof technique in Proposition 5.1.8, we skip the details of the present proof. The final remark follows from the fact that $\widehat{F}^\times \subset N(K)$, implying $\widehat{F}^{\times 2} \subset \mathrm{nrd}(N(K))$. □

We can make the group $\mathrm{nrd}(N(K))$ more explicit for K coming from Eichler orders:

Proposition 2.6.2. *Let B be as at the beginning of this section, and let $\mathcal{O}(\mathfrak{N})$ be a level $\mathfrak{N}$ Eichler order of B. Let $K = \widehat{\mathcal{O}}(\mathfrak{N})^\times$.*

(i) Let $\mathfrak{p}$ be a prime of F at which B is split. Then

$$\mathrm{nrd}(N(K_\mathfrak{p})) = \langle F_\mathfrak{p}^{\times 2} \mathbf{Z}_{F,\mathfrak{p}}^\times, \pi^{v_\mathfrak{p}(\mathfrak{N})} \rangle.$$

(ii) Let $\mathfrak{p}$ be a prime of F at which B ramifies. Then

$$\mathrm{nrd}(N(K_\mathfrak{p})) = F_\mathfrak{p}^\times.$$

(iii) Let

$$C_2 = \mathrm{Cl}(\infty)/2\mathrm{Cl}(\infty).$$

Then we have

$$T(K\infty) \cong C_2/\langle \{\mathfrak{p} : \mathfrak{p} \text{ divides } \mathfrak{D}(B)^f\} \cup \{\mathfrak{p} : v_{\mathfrak{p}}(\mathfrak{N}) \text{ odd}\}\rangle.$$

Proof. The first two statements follow from the considerations in Section II.2 of [Vig80]. Part (iii) follows by combining the first two parts with Proposition 2.6.1(ii). Also see Corollaire III.5.7 in [Vig80]. □

Remark. For definite quaternion algebras, determining class and type numbers is considerably more complicated. We refer to [KV10] for more on this subject.

Chapter 3

Curves

Our goal in this Chapter is to define the notion of an arithmetic pointed torus. These complex tori are intimately related to Shimura curves, which we introduce in the first section. Shimura curves are generalizations of classical modular curves, and like modular curves, they have canonical models over certain number fields. The results on the arithmetic of quaternion algebras of the previous Chapter will be used to deduce geometric and arithmetic properties of these models.

The third section will at last give the definition of an arithmetic subgroup of $\mathrm{PGL}_2(\mathbf{R})$, along with the corresponding notion of an arithmetic pointed torus. We review the technique used by Takeuchi in [Tak83] to relate such pointed complex tori to Shimura curves. It turns out that in order to develop arithmetic theory for these $(1;e)$-curves, we have to work with adèlic groups K' that are somewhat smaller than those usually considered in the literature: this technical point is discussed in the second section.

The third section also defines canonical models of arithmetic $(1;e)$-curves. The irony here is that although these models fully deserve the name "canonical", as we will explain, they do depend on the choice of a group K' as above.

Throughout this Chapter, let F be a totally real number field, and let B be a quaternion algebra over F that is split at exactly one infinite place ι of F (and possible at some finite places of F as well). Finally, let K be a compact open subgroup of $\widehat{B}^{\times}$.

3.1 Shimura curves

Let $\mathcal{H}^{\pm}$ be the Riemann surface

$$\mathcal{H}^{\pm} = \mathbf{P}^1(\mathbf{C}) - \mathbf{P}^1(\mathbf{R}) = \mathcal{H}^{+} \sqcup \mathcal{H}^{-}.$$

The group $\mathrm{GL}_2(\mathbf{R})$ acts on $\mathcal{H}^{\pm}$ through fractional linear transformations, hence so does $B^{\times}$ after choosing an isomorphism

$$\iota : B \otimes_{F,\iota} \mathbf{R} \xrightarrow{\sim} M_2(\mathbf{R}). \tag{3.1}$$

The group K_B^+ from (2.6) can be considered as a subgroup of $\mathrm{GL}_2^+(\mathbf{R})$ through the embedding ι. Théorème IV.1.1 of [Vig80] shows that $\mathrm{P}K_B^+ \subset \mathrm{PGL}_2^+(\mathbf{R})$ is a Fuchsian group of the first kind. For $a \in \{\pm 1\}$, we denote

$$Y_0^a(K) = Y^a(K_B^+)$$

and we abbreviate $Y_0(K) = Y_0^+(K)$. Moreover, for an order $\mathcal{O}$ of B, we abbreviate $Y_0^a(\mathcal{O}) = Y_0^a(\widehat{\mathcal{O}}^\times)$.

We can define an action of $B^\times$ on $\mathcal{H}^\pm \times \widehat{B}^\times$ by

$$b(x, \widehat{b}) = (bx, b\widehat{b}).$$

There is also a right action of K on $\mathcal{H}^\pm \times \widehat{B}^\times$ given by

$$(x, \widehat{b})k = (x, \widehat{b}k).$$

Consider the double quotient

$$Y(K) = B^\times \backslash \mathcal{H}^\pm \times \widehat{B}^\times / K. \tag{3.2}$$

Again, for an order $\mathcal{O}$ of B, we abbreviate $Y(\mathcal{O}) = Y(\widehat{\mathcal{O}}^\times)$. The following proposition describes the connected components of $Y(K)$, the set of which we denote by $\pi_0(Y(K))$.

Proposition 3.1.1. *Let $Y(K)$ be as in (3.2).*

(i) There is a bijection

$$\pi_0(Y(K)) \xrightarrow{\sim} B^\times \backslash \{\pm 1\} \times \widehat{B}^\times / K = \mathrm{Pic}(K\infty). \tag{3.3}$$

The reduced norm map induces an isomorphism

$$\pi_0(Y(K)) \xrightarrow{\sim} \mathrm{Cl}(\mathrm{nrd}(K)\infty). \tag{3.4}$$

(ii) Let $\{(a_i, b_i)\}$, with $a_i \in \{\pm 1\}$ and $b_i \in \widehat{B}^\times$, be a set of representatives for the quotient (3.3). Then there is an isomorphism

$$Y(K) \cong \coprod_i Y_0^{a_i}(b_i K b_i^{-1}). \tag{3.5}$$

The quotient $Y(K)$ is compact if and only if B is a division algebra.

(iii) There occur at most $|T(K\infty)|$ isomorphism classes of curves on the right hand side of (3.5).

Proof. (i): The first statement follows by identifying $\pi_0(\mathcal{H}^\pm) \cong \{\pm 1\}$. The first isomorphism in (3.4) is then exactly the one from Proposition 2.6.1.

(ii): This results from of Lemma 5.13 and Theorem 3.3 in [Milb].

(iii): An element n of $N(K)$ induces an isomorphism

$$\begin{aligned} Y(K) &\longrightarrow Y(K) \\ [x,b] &\longmapsto [x,bn]. \end{aligned}$$

Under the isomorphism (3.4), the action of n on $\pi_0(Y(K))$ is given by multiplication by $\mathrm{nrd}(n)$. Components that are accordingly permuted are necessarily isomorphic, which proves (iii). □

We call the automorphisms of $Y(K)$ induced by elements of $N(K)$ *Atkin-Lehner automorphisms*. Let $\mathfrak{D} = \mathfrak{D}(B)^f$. Suppose $K = \widehat{\mathcal{O}}(\mathfrak{N})^\times$, where $\mathcal{O}(\mathfrak{N})$ is a level $\mathfrak{N}$ Eichler order of B. Let $\mathfrak{a}$ be a product of primes dividing $\mathfrak{D}\mathfrak{N}$. Then we denote by $w(\mathfrak{a})$ the Atkin-Lehner automorphism of $Y(K)$ induced by an element $n^{\mathfrak{a}}$ of $N(K)$ whose components in the quotient $N(K)/\widehat{F}^\times K$ are non-trivial exactly at the primes dividing $\mathfrak{a}$ (*cf.* Proposition 2.6.2).

Proposition 3.1.1 shows that $Y(K)$ is a Riemann surface in a natural way. Therefore it can be considered as a complex algebraic curve as well. The connected component of $Y(K)$ over $[+1,1] \in \pi_0(Y(K))$ is given by $Y_0^+(K)$: we shall call this the *neutral component* of $Y(K)$. Analogously, the connected component over $[-1,1]$ is given by $Y_0^-(K)$. This notation is not to be confused with the usual notation $Y_0(N)$ for classical modular curves.

The following fundamental result is due to of Shimura ([Shi70]). Modern expositions can be found in [Del71], [Car86] and [Milb].

Theorem 3.1.2. *Let $Y(K)$ be as in (3.2).*

(i) There exists a curve $\mathrm{Sh}(K)$ *over F that is a canonical model of $Y(K)$ over F. In particular,*

$$\mathrm{Sh}(K) \otimes_{F,\iota} \mathbf{C} \cong Y(K).$$

(ii) Let $K' \subset K$. Then the canonical projection map $Y(K') \to Y(K)$ is induced by an F-morphism $\mathrm{Sh}(K') \to \mathrm{Sh}(K)$.

(iii) Let $b \in \widehat{B}^\times$. Then the canonical isomorphism

$$\begin{aligned} Y(K) &\longrightarrow Y(b^{-1}Kb) \\ [x,b'] &\longmapsto [x,b'b] \end{aligned}$$

is induced by an F-morphism $\mathrm{Sh}(K) \to \mathrm{Sh}(b^{-1}Kb)$.

Proof. Part (i) is (1.1.1) in [Car86], and parts (ii) and (iii) are special cases of Theorem 13.6 in [Milb]. □

We will not get into the precise definition of a canonical model, since it is rather technical and we can get by without it, but see Chapter 12 of [Milb]. Note that in contrast with the terminology in Chapter 5, "model" means "model over a number field" rather than "integral model" in this chapter. In particular, Shimura's canonical models are not to be confused with the canonical models in Definition 9.4.21 of [Liu02].

We call both $Y(K)$ and its canonical model $\mathrm{Sh}(K)$ a *Shimura curve*. It follows from Proposition 3.1.1(ii) that $\mathrm{Sh}(K)$ is of finite type and smooth over F. Moreover, $\mathrm{Sh}(K)$ is proper if and only if B is a division algebra. It is not necessarily geometrically connected by part (i) of Proposition 3.1.1.

When B is a matrix algebra, there exist explicit methods using q-expansions for computing an equation for $\mathrm{Sh}(K)$. Unfortunately, such methods are not available in the cases that we consider, where B is a division algebra. Our strategy in this thesis is to determine $\mathrm{Sh}(K)$ by using its arithmetic properties.

Let us first consider the scheme of connected components $\pi_0(\mathrm{Sh}(K))$ of $\mathrm{Sh}(K)$. It is a finite étale scheme over $\mathrm{Spec}(F)$ whose geometric points are given by

$$\pi_0(\mathrm{Sh}(K))(\overline{F}) = \pi_0(\mathrm{Sh}(K))(\mathbf{C}) = \pi_0(Y(K)).$$

This set of points inherits an action of $G_F = \mathrm{Gal}(\overline{F}|F)$. Conversely, this Galois action determines $\pi_0(\mathrm{Sh}(K))$ as a scheme. Now the G_F-set structure of $\pi_0(Y(K))$ can be described as follows.

Theorem 3.1.3 ([Car86], Section 1.2). *Under the isomorphism (3.4), the absolute Galois group G_F acts on $\mathrm{Cl}(\mathrm{nrd}(K)\infty) = F^+\backslash\widehat{F}^\times/\mathrm{nrd}(K)$ through*

$$\sigma([x]) = [s^{-1}x],$$

where $s \in \widehat{F}^\times$ is any idèle whose image under the Artin reciprocity map

$$\widehat{F}^\times \hookrightarrow \mathbf{A}_F^\times \to G_F$$

equals σ.

Using the notation of Section 2.1 of the previous Chapter, we abbreviate $F_K = F_{\mathrm{nrd}(K)\infty}$. Proposition 3.1.3 then gives that G_F acts transitively on $\pi_0(\mathrm{Sh}(K))$, which implies

$$\pi_0(\mathrm{Sh}(K)) \cong \mathrm{Spec}(F_K).$$

Therefore there exists a model $\mathrm{Sh}_0(K) = \mathrm{Sh}_0^+(K)$ for the neutral component $Y_0(K) = Y_0^+(K)$ over the Galois extension F_K of F such that $\mathrm{Sh}(K)$ is isomorphic to the scheme

$$\mathrm{Sh}_0(K) \longrightarrow \mathrm{Spec}(F_K) \longrightarrow \mathrm{Spec}(F)$$

over F. Concretely, this means that there is a finite decomposition

$$(\mathrm{Sh}(K))_{F_K} \cong \coprod_{\sigma\in\mathrm{Gal}(F_K|F)} \mathrm{Sh}_0(K)^\sigma \tag{3.6}$$

over F_K. By notional abuse, we call the model $\mathrm{Sh}_0(K)$ of $Y_0(K)$ over F_K canonical as well. Proceeding analogously, we get a model $\mathrm{Sh}_0^-(K)$ of $Y_0^-(K)$ over F_K. As above, we abbreviate $\mathrm{Sh}(\mathcal{O}) = \mathrm{Sh}(\widehat{\mathcal{O}}^\times)$, and for $a \in \{\pm 1\}$, we let $\mathrm{Sh}_0^a(\mathcal{O}) = \mathrm{Sh}_0^a(\widehat{\mathcal{O}}^\times)$.

Let

$$J(K) = \mathrm{Jac}(\mathrm{Sh}(K)).$$

This is an abelian variety over F. If we let

$$J_0^a(K) = \mathrm{Jac}(\mathrm{Sh}_0^a(K)),$$

where $a \in \{\pm 1\}$, then $J_0(K)$ is an abelian variety over F_K for which

$$J(K) \cong \mathrm{Res}_{F_K|F}(J_0(K)). \tag{3.7}$$

Here Res denotes Weil restriction of scalars, *cf.* the discussion before Theorem B in [Zha01]. We once more abbreviate $J(\mathcal{O})$ and $J_0^a(\mathcal{O})$ as above. We can now formulate a second property of $\mathrm{Sh}(K)$.

Proposition 3.1.4. *Let $n \in N(K)$. Then the Atkin-Lehner automorphism of $Y(K)$ associated to n descends to an F-automorphism of* $\mathrm{Sh}(K)$*.*

In particular, there occur at most $|T(K\infty)|$ isomorphism classes of curves over F_K on the right hand side of (3.6), as over $\mathbf{C}$*.*

Proof. Using the discussion above and part (iii) of Theorem 3.1.2, this is a consequence of Proposition 3.1.1(iii). □

Proposition 3.1.5. *Let $\sigma \in \mathrm{Gal}(\overline{F}|F)$. Then the Jacobians of the curves $\mathrm{Sh}_0(K)^\sigma$ and $\mathrm{Sh}_0(K)$ are isogenous over F_K.*

Proof. We use the decomposition (3.6). By weak approximation for $F^\times$ and surjectivity of the map $\mathrm{nrd} : K_\mathfrak{p} \to \widehat{\mathbf{Z}}_{F,\mathfrak{p}}^\times$ at primes $\mathfrak{p}$ where K is maximal (*cf.* Proposition 2.2.4), we see that we can choose the representatives (a_i, b_i) in Proposition 3.1.1(ii) to satisfy

$$a_i = 1, \text{ and } b_{i,\mathfrak{p}} = 1 \text{ at places where } K \text{ is not maximal or } B \text{ ramifies.}$$

Fix i. Then $K' = K \cap b_i K b_i^{-1}$ is a compact open subgroup of $\widehat{B}^\times$ and therefore of finite index in both K and $b_i K b_i^{-1}$. This gives rise to a correspondence

$$\begin{tikzcd} & \mathrm{Sh}(K') \arrow[dl, "\mathrm{proj}"'] \arrow[dr, "\mathrm{proj}"] & \\ \mathrm{Sh}(K) & & \mathrm{Sh}(b_i K b_i^{-1}) \end{tikzcd} \tag{3.8}$$

We claim that the correspondence (3.8) induces isomorphisms between the schemes $\pi_0(\mathrm{Sh}(K'))$, $\pi_0(\mathrm{Sh}(K))$ and $\pi_0(\mathrm{Sh}(b_i K b_i^{-1}))$.

Indeed, by construction, at primes $\mathfrak{p}$ where b_i is non-trivial, $K'_\mathfrak{p}$ is given by the units of an Eichler order of $B_\mathfrak{p}$, hence $\mathrm{nrd}(K'_\mathfrak{p}) = \widehat{\mathbf{Z}}_{F,\mathfrak{p}}^\times = \mathrm{nrd}(K_\mathfrak{p})$ by Proposition 2.2.2. At $\mathfrak{p}$ where b_i is trivial, obviously $\mathrm{nrd}(K_\mathfrak{p}) = \mathrm{nrd}(K'_\mathfrak{p})$ since $K_\mathfrak{p} = K'_\mathfrak{p}$. Hence $\mathrm{nrd}(K') = \mathrm{nrd}(K)$, which proves the claim in light of Proposition 3.1.1(i).

The correspondence in (3.8), being built out of canonical projection maps, therefore induces trivial maps on the schemes of connected components by Theorem 3.1.2(ii). Consequently, it induces a correspondence over F_K between the neutral components $\mathrm{Sh}_0(K)$ and $\mathrm{Sh}_0(b_iKb_i^{-1})$. But giving such a correspondence is the same as giving an isogeny of the corresponding Jacobians. Since the neutral component of $\mathrm{Sh}(b_iKb_i^{-1})$ can be identified with the connected component of $\mathrm{Sh}(K)$ corresponding to (a_i, b_i), we have proved the proposition. □

Fourthly, we describe the reduction properties of $\mathrm{Sh}(K)$.

Theorem 3.1.6. *Let $\mathfrak{p}$ be a prime of F, and suppose that K is of the form $K = K_{\mathfrak{p}} \times K^{\mathfrak{p}}$, where $K_{\mathfrak{p}} \subset B_{\mathfrak{p}}$ and $K^{\mathfrak{p}} \subset \widehat{B}^{\mathfrak{p}}$. Let $\mathfrak{C}$ be the conductor of $J(K)$ as an abelian variety. Then $v_{\mathfrak{p}}(\mathfrak{C})$ only depends on $K_{\mathfrak{p}}$. Furthermore,*

(i) If $\mathfrak{p} \nmid \mathfrak{D}(B)$ and $K_{\mathfrak{p}}$ is maximal at $\mathfrak{p}$, then $v_{\mathfrak{p}}(\mathfrak{C}) = 0$.

(ii) If $\mathfrak{p} \nmid \mathfrak{D}(B)$ and $K_{\mathfrak{p}}$ is the unit group of a level $\mathfrak{N}$ Eichler order of $B_{\mathfrak{p}}$, where $v_{\mathfrak{p}}(\mathfrak{N}) = 1$, then $v_{\mathfrak{p}}(\mathfrak{C}) = 1$.

(iii) If $\mathfrak{p} \mid \mathfrak{D}(B)$ and $K_{\mathfrak{p}}$ is maximal at $\mathfrak{p}$, then $v_{\mathfrak{p}}(\mathfrak{C}) = 1$.

Proof. The first two statements follow from [Car86]. The third is a consequence of the $\mathfrak{p}$-adic uniformization of $\mathrm{Sh}(K)$ that we will consider in Chapter 5 (*cf.* Proposition 5.1.12(ii)). □

Fifthly and finally, we describe a relation between canonical models coming from different quaternion algebras. Let ι be an infinite place of F. Then we denote

$$\iota^c = \prod_{\substack{\iota' \mid \infty \\ \iota' \neq \iota}} \iota'. \tag{3.9}$$

Theorem 3.1.7. *Let B be a quaternion algebra over F with $\mathfrak{D}(B)^\infty = \iota^c$. Let ι' be another infinite place of F, and let B' be a quaternion algebra for which $\mathfrak{D}(B')^f = \mathfrak{D}(B)^f$ and $\mathfrak{D}(B')^\infty = \iota'^c$. In other words, let B' be ramified at the same finite places as B and let B' be split at a unique infinite place, given by ι'. Let*

$$\widehat{B} = \prod_{v \text{ finite}}{}' B_v \xrightarrow{\varphi} \prod_{v \text{ finite}}{}' B'_v = \widehat{B}' \tag{3.10}$$

be an isomorphism of restricted direct products. Let K be a compact open subgroup of $\widehat{B}^\times$. Then if we let $K' = \varphi(K)$, there exists an isomorphism

$$\mathrm{Sh}(K) \otimes_{F,\iota'} \mathbf{C} \cong \mathrm{Sh}(K') \otimes_{F,\iota'} \mathbf{C} \tag{3.11}$$

of curves over $\mathbf{C}$.

Proof. This is an adèlic translation of the results due to Doi and Naganuma in [DN67]: although the main theorem there is only formulated for principal open subgroups K, the proof in [DN67] in fact shows that the generalization above holds. □

We will use this proposition in conjuction with the following remark. Let σ be an automorphism of F. Then if the F-algebra structure of B is given by

$$F \xrightarrow{i} B,$$

we can consider the F-algebra ${}^{\sigma}B$ obtained by

$$F \xrightarrow{\sigma^{-1}} F \xrightarrow{i} B.$$

Note that

$${}^{\sigma}\left(\frac{a_1, a_2}{F}\right) \cong \left(\frac{\sigma(a_1), \sigma(a_2)}{F}\right).$$

The identity map on B is an isomorphism of $\mathbf{Q}$-algebras $B \longrightarrow {}^{\sigma}B$. We have

$$\mathfrak{D}({}^{\sigma}B) = \sigma(\mathfrak{D}(B)).$$

Here, for a place v of F, we denote by σv the place $v \circ \sigma^{-1}$. Upon tensoring, we obtain an isomorphism of $\mathbf{Q}$-algebras

$$\widehat{B} = B \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}}^{f} \longrightarrow {}^{\sigma}B \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}}^{f} = {}^{\sigma}\widehat{B} \tag{3.12}$$

Let K be a compact open subgroup of $\widehat{B}^{\times}$, and let ${}^{\sigma}K$ be equal to K, but this time considered as a subgroup of ${}^{\sigma}\widehat{B}^{\times}$ through the isomorphism (3.12). Then clearly there is an isomorphism

$$Y(K) = B^{\times}\backslash\mathcal{H}^{\pm} \times \widehat{B}^{\times}/K \cong {}^{\sigma}B^{\times}\backslash\mathcal{H}^{\pm} \times {}^{\sigma}\widehat{B}^{\times}/{}^{\sigma}K = Y({}^{\sigma}K),$$

therefore

$$\mathrm{Sh}(K) \otimes_{F,\iota} \mathbf{C} \cong \mathrm{Sh}({}^{\sigma}K) \otimes_{F,\sigma\iota} \mathbf{C}. \tag{3.13}$$

Combining the isomorphisms (3.11) and (3.13), one can show that $Y(K)$ is defined over a proper subfield of F in a large variety of cases. For example, suppose that F is Galois over $\mathbf{Q}$, and let B be an algebra over F whose finite discriminant $\mathfrak{D}(B)^{f}$ is $\mathrm{Gal}(F|\mathbf{Q})$-invariant. Let $K = \widehat{\mathcal{O}}^{\times}$, where $\mathcal{O}$ is an Eichler order of $\mathrm{Gal}(F|\mathbf{Q})$-invariant level $\mathfrak{N}$. Then $Y(K)$ has field of moduli equal to $\mathbf{Q}$ (*cf.* Section 7 of [GV] and Proposition 1 of [Hal09]). In Chapter 7, we will see that this need not imply that the canonical model $\mathrm{Sh}(K)$ descends to $\mathbf{Q}$, even when $\mathrm{Sh}(K)$ has genus 1.

To prove the claim, it suffices to show

$$\mathrm{Sh}(K) \otimes_{F,\iota} \mathbf{C} \cong \mathrm{Sh}(K) \otimes_{F,\iota'} \mathbf{C}$$

for all pairs of embeddings ι and ι' of F. Given ι and ι', there is an automorphism σ of F such that $\iota' = \sigma\iota$. Then by (3.13), we have

$$\mathrm{Sh}(K) \otimes_{F,\iota} \mathbf{C} \cong \mathrm{Sh}({}^{\sigma}K) \otimes_{F,\sigma\iota} \mathbf{C} = \mathrm{Sh}({}^{\sigma}K) \otimes_{F,\iota'} \mathbf{C}. \tag{3.14}$$

Note that ${}^{\sigma}K$ comes from a level $\sigma(\mathfrak{N}) = \mathfrak{N}$ Eichler order of ${}^{\sigma}B$. By the Galois invariance of $\mathfrak{D}(B)^f$ we can take $B' = {}^{\sigma}B$ in Theorem 3.1.7. We accordingly let $K' = {}^{\sigma}K$.

Since both K' and K come from level $\mathfrak{N}$ Eichler orders, we can choose the isomorphism in (3.10) such that K is mapped to K'. Therefore, by (3.11), we conclude

$$\mathrm{Sh}({}^{\sigma}K) \otimes_{F,\iota'} \mathbf{C} = \mathrm{Sh}(K') \otimes_{F,\iota'} \mathbf{C} \cong \mathrm{Sh}(K) \otimes_{F,\iota'} \mathbf{C}. \tag{3.15}$$

Combining (3.14) and (3.15) proves the claim.

3.2 From K_B^+ to K_B^1

This section considers the subgroup K_B^1 of K_B^+ from (2.7). In the previous section, we obtained the curve $Y(K_B^+)$ as the connected component $Y_0(K)$ of the Riemann surface $Y(K)$, resulting in a canonical model $\mathrm{Sh}_0(K)$ for this curve over F_K.

For reasons that will become clear in the next section, we are also interested in obtaining a canonical model of the curve $Y(K_B^1)$. To obtain this curve as a Shimura curve, we use compact open groups $K' \subset \widehat{B}^\times$ that are slightly smaller than K. This section explains what K' are possible, and how they can be constructed. We start with some global considerations.

Proposition 3.2.1. *The group $\mathrm{P}K_B^1$ is a normal subgroup of $\mathrm{P}K_B^+$ of finite index. Let $N = \mathrm{nrd}(K)$. Then we have an isomorphism*

$$\mathrm{P}K_B^+/\mathrm{P}K_B^1 \cong (N \cap \mathbf{Z}_F^+)/(N \cap \mathbf{Z}_F^{\times 2}).$$

Consequently, the projection $Y(K_B^1) \to Y(K_B^+)$ is Galois with abelian Galois group $(N \cap \mathbf{Z}_F^+)/(N \cap \mathbf{Z}_F^{\times 2})$ of exponent 2. This Galois group is isomorphic to a subgroup of $\mathrm{Ker}(\mathrm{Cl}(\infty) \to \mathrm{Cl}(1))$, with equality holding if $K = \widehat{\mathcal{O}}^\times$ for an Eichler order $\mathcal{O}$.

Proof. Normality is obvious. Let $K_B^{(2)}$ be the subgroup of K_B^+ consisting of those elements whose norm is in $\mathbf{Z}_F^{\times 2}$. Then we have the following commutative diagram with exact rows

$$\begin{tikzcd}
1 \arrow[r] & \mathbf{Z}_F^\times \arrow[r] \arrow[d] & K_B^{(2)}\mathbf{Z}_F^\times \arrow[r] \arrow[d] & \mathrm{P}K_B^1 \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbf{Z}_F^\times \arrow[r] & K_B^+\mathbf{Z}_F^\times \arrow[r] & \mathrm{P}K_B^+ \arrow[r] & 1
\end{tikzcd}$$

Considering this diagram, we see that the canonical map

$$K_B^+\mathbf{Z}_F^\times/K_B^{(2)}\mathbf{Z}_F^\times \longrightarrow \mathrm{P}K_B^+/\mathrm{P}K_B^1$$

is an isomorphism. On the other hand, by Proposition 2.4.2, the reduced norm map induces an isomorphism

$$K_B^+\mathbf{Z}_F^\times/K_B^{(2)}\mathbf{Z}_F^\times \longrightarrow (N \cap \mathbf{Z}_F^+)\mathbf{Z}_F^{\times 2}/(N \cap \mathbf{Z}_F^{\times 2})\mathbf{Z}_F^{\times 2} \cong (N \cap \mathbf{Z}_F^+)/(N \cap \mathbf{Z}_F^{\times 2}).$$

As for the second part, there is a canonical map

$$\mathbf{Z}_F^\times/\mathbf{Z}_F^{\times 2} \longrightarrow \mathbf{A}_F^{\infty\times}/(\mathbf{A}_F^{\infty\times})^2 = \prod_{v|\infty} U_v^{(0)}/U_v^{(1)}. \tag{3.16}$$

Here $U_v^{(0)} = F_v^\times$, and $U_v^{(1)}$ is the connected component of $U_v^{(0)}$ containing 1.

The kernel of the projection $\mathrm{Cl}(\infty) \to \mathrm{Cl}(1)$ is isomorphic to the cokernel of the map (3.16) (*cf.* the proof of Lemma 3.2.3). The kernel of the map (3.16) is given by $\mathbf{Z}_F^+/\mathbf{Z}_F^{\times 2}$. Now because of Dirichlet's unit theorem and the fact that any number field has a root of unity of order 2, both of the groups in (3.16) have the same cardinality, to wit $2^{\deg(F|\mathbf{Q})}$. Therefore the kernel and cokernel of the map above have the same cardinality, and both have exponent 2, they are isomorphic. We can therefore conclude the proof by noting that $\mathrm{nrd}(\widehat{\mathcal{O}}^\times) = \widehat{\mathbf{Z}}_F^\times$ for all Eichler orders $\mathcal{O}$. □

The proposition above indicates that if the narrow class group of F is non-trivial, then usually $Y(K_B^1)$ will be a non-trivial cover of $Y(K_B^+)$. One would like to solve this by working with the algebraic group $\mathrm{Res}_{F|\mathbf{Q}}(B^1)$ directly, instead of with the group $\mathrm{Res}_{F|\mathbf{Q}}(B^\times)$ that gives the canonical models of Theorem 3.1.2 (as in [Car86]).

Unfortunately, there is no way to obtain a Shimura variety from $\mathrm{Res}_{F|\mathbf{Q}}(B^1)$, because it has no Shimura datum. We refer to Chapter 5 of [Milb] for the notion of a Shimura datum and the axioms SV1, SV2 and SV3 that it satisfies.

Proposition 3.2.2. *There exists no Shimura datum (G, h) with $G = \mathrm{Res}_{F|\mathbf{Q}}(B^1)$.*

Proof. Suppose such a datum did exist. Then upon base extension to $\mathbf{R}$, we would end up with a morphism of algebraic groups $h : \mathbf{S} \to G_{\mathbf{R}}$ satisfying SV1 and SV2. Consider the projection $h^0 : \mathbf{S} \longrightarrow \mathrm{SL}_{2,\mathbf{R}}$ obtained by choosing an isomorphism

$$\mathbf{G_R} \cong \mathrm{SL}_{2,\mathbf{R}} \times \mathbf{H}^1 \times \ldots \times \mathbf{H}^1.$$

Let w be the weight homomorphism $w : \mathbf{G}_m \to \mathbf{S}$. The composite map given by

$$\mathbf{G}_{m,\mathbf{R}} \xrightarrow{w} \mathbf{S} \xrightarrow{h^0} \mathrm{SL}_{2,\mathbf{R}} \xrightarrow{\mathrm{proj}} \mathrm{PSL}_{2,\mathbf{R}} = \mathrm{SL}_{2,\mathbf{R}}^{\mathrm{ad}}$$

is trivial because of SV1 and the triviality of the characters $z/\bar{z}$, 1 and $\bar{z}/z$ on the image of w.

Therefore the image of $\mathbf{G}_{m,\mathbf{R}}(\mathbf{C})$ under the map above is contained in the center of $\mathrm{SL}_{2,\mathbf{R}}(\mathbf{C})$, which is isomorphic to $\mu_{2,\mathbf{R}}(\mathbf{C}) \subset \mathbf{G}_{m,\mathbf{R}}(\mathbf{C})$. But the algebraic homomorphisms $\mathbf{G}_{m,\mathbf{R}} \to \mathbf{G}_{m,\mathbf{R}}$ are just the characters $z \mapsto z^n$ for integral n. The only character having finite image on $\mathbf{C}$-points is the trivial character. That is to say, the homomorphism $h^0 w : \mathbf{G}_{m,\mathbf{R}} \to \mathrm{SL}_{2,\mathbf{R}}$ is trivial.

Now $-1 \in \mathbf{S}(\mathbf{R})$ is in the image of w. Therefore $h^0(-1)$ is trivial. We have $h^0(i)^2 = h^0(-1)$, therefore $h^0(i)$ has finite order and is diagonalizable, with eigenvalues in $\{\pm 1\}$. Since $h^0(i)$ is in $\mathrm{SL}_2(\mathbf{R})$, its two eigenvalues are identical, hence it is either given by I or $-I \in \mathrm{SL}_2(\mathbf{R})$. But conjugation with these elements induces the trivial involution of $\mathrm{SL}_2(\mathbf{R})$, which is not Cartan since $\mathrm{SL}_2(\mathbf{R})$, containing $\mathbf{G}_m(\mathbf{R})$, is not compact. Therefore h cannot induce a Cartan involution of $G_{\mathbf{R}}$ either. □

Remark. The terminology used in the literature is somewhat confusing on this point. According to Corollary 5.8 in [Milb], there does exist a *connected Shimura datum* for $\mathrm{Res}_{F|\mathbf{Q}}(B^1)$. Part of the point of Proposition 3.2.2 is that not all these connected Shimura data (in the sense of Definition 4.4 of *loc. cit.*) are Shimura data (in the sense of Definition 5.5 of *loc. cit.*).

Likewise, the Shimura datum on $G = \mathrm{Res}_{F|\mathbf{Q}}(B^\times)$ does not lift to the fiber product P given by the diagram

$$\begin{tikzcd} P \arrow[r] \arrow[d] & \mathbf{G}_m \arrow[d, "x \mapsto x^2"] \\ G \arrow[r, "\mathrm{nrd}"] & \mathbf{G}_m \end{tikzcd}$$

Nevertheless, one can find a way around the problem by considering suitable compact open subgroups of small index in K. The key point is the following lemma:

Lemma 3.2.3. *Let F be a number field, and let N be a compact open subgroup of $\widehat{F}^\times$. Then there exists a compact open subgroup N' of N such that:*

(i) The canonical projection map $\mathrm{Cl}(N'\infty) \to \mathrm{Cl}(N\infty)$ is an isomorphism;

(ii) $\mathbf{Z}_F^+ \cap N' = \mathbf{Z}_F^{\times 2} \cap N$.

Moreover, for any such subgroup N' we have that the canonical map

$$(\mathbf{Z}_F^+ \cap N)/(\mathbf{Z}_F^{\times 2} \cap N) = (\mathbf{Z}_F^+ \cap N)/(\mathbf{Z}_F^+ \cap N') \longrightarrow N/N' \tag{3.17}$$

is an isomorphism.

Proof. We use the fact, easily proved using the Čebotarev density theorem (Theorem VII.13.4 in [Neu99]), that given a nonsquare x in F, the set of places of F at which x is a square has density $1/2$. This allows us to construct N' through a repeated shrinking process.

We may suppose that the inclusion $\mathbf{Z}_F^{\times 2} \cap N \subset \mathbf{Z}_F^+ \cap N$ is strict: otherwise we can take $N' = N$. Let x be a non-square element of $\mathbf{Z}_F^+ \cap N$, and let v be a place such that x is not a square at v and such that N_v does not equal $\mathbf{Z}_{F,v}^{\times 2}$. Such a v always exists: for example, one can take an odd finite place modulo which x is not a square and where N is maximal.

Let N'_v be an index 2 subgroup of N_v such that N'_v contains $\mathbf{Z}_{F,v}^{\times 2}$ and such that x is not in N'_v. Construct $N' = N \cap N'_v$. Now x is not in N'; on the other hand, since N'_v contains $\mathbf{Z}_{F,v}^{\times 2}$, one still has that $\mathbf{Z}_F^{\times 2} \cap N$ is contained in $\mathbf{Z}_F^+ \cap N'$. By construction, we also have

$$[\mathbf{Z}_F^+ \cap N : \mathbf{Z}_F^{\times 2} \cap N] = 2[\mathbf{Z}_F^+ \cap N' : \mathbf{Z}_F^{\times 2} \cap N].$$

We check that the projection map in (i) is an isomorphism for N and N'. Its kernel is given by

$$\frac{F^+N}{F^+N'} = \frac{F^+N'N_v}{F^+N'} \cong \frac{N_v}{N_v \cap F^+N'} \tag{3.18}$$

$$\cong \frac{N_v}{(\mathbf{Z}_F^+ \cap N_v)N_v'}. \tag{3.19}$$

In this string of isomorphisms, we have embedded $F^\times$ diagonally in the idéles $\widehat{F}^\times$ in (3.18), while we embedded it in the factor $F_v^\times$ in (3.19).

The group $(\mathbf{Z}_F^+ \cap N_v)N_v'$ contains N_v', hence is at worst of index 2 in N_v. On the other hand, it also contains $x \in \mathbf{Z}_F^+ \cap N_v$, which is not in N_v', so in fact it equals N_v. Hence the projection map $\mathrm{Cl}(N'\infty) \to \mathrm{Cl}(N\infty)$ is indeed an isomorphism. Inductively repeating this procedure above, one obtains a N' as in the lemma, since $\mathbf{Z}_F^+/\mathbf{Z}_F^{\times 2}$ is finitely generated.

Now for the last statement of the lemma. By (ii), the map (3.17) is injective: it remains to prove that $(\mathbf{Z}_F^+ \cap N)N' = N$. By (i), the quotient

$$F^+N/F^+N' = F^+N'N/F^+N' \cong N/(F^+N' \cap N)$$

is trivial, hence we can conclude by noting that

$$(\mathbf{Z}_F^+ \cap N)N' = \mathbf{Z}_F^+N' \cap N = F^+N' \cap N. \qquad \square$$

Now let a compact open subgroup K of $\widehat{B}^\times$ be given. Then by applying the reduced norm map, one obtains a compact open subgroup $N = \mathrm{nrd}(K)$ of $\widehat{F}^\times$. Choosing an N' satisfying the properties in the lemma, we then construct the subgroup

$$K' = K \cap \mathrm{nrd}^{-1}(N') \tag{3.20}$$

which is again compact open because of the continuity of the reduced norm map. By construction of K', we see that we have achieved our objective at the beginning of this section:

Proposition 3.2.4. *Let K, N' and K' be as above, and let $a \in \{\pm 1\}$.*

(i) We have

$$Y_0^a(K') \cong Y^a(K_B^1).$$

Similarly, the other components of $Y(K')$ do not depend on the choice of N'.

(ii) The canonical projection $\mathrm{Sh}(K') \to \mathrm{Sh}(K)$ induces an F-isomorphism

$$\pi_0(\mathrm{Sh}(K')) \longrightarrow \pi_0(\mathrm{Sh}(K)).$$

between the schemes of connected components of $\mathrm{Sh}(K')$ and $\mathrm{Sh}(K)$. In particular, $F_{K'} = F_K$, and the canonical projection $Y_0^a(K') \to Y_0^a(K)$ descends to an F_K-morphism $\mathrm{Sh}_0^a(K') \to \mathrm{Sh}_0^a(K)$.

As we shall see explicitly in Chapter 7, different choices for K' can give rise to different canonical models of the same Riemann surface. To avoid confusion, we shall often call $\mathrm{Sh}_{(0)}(K')$ a *K'-model* of the Riemann surface $Y_{(0)}(K')$.

3.3 Arithmetic $(1;e)$-curves

Let $\iota : B^\times \to \mathrm{GL}_2(\mathbf{R})$ and $\mathrm{P}K_B^+ \subset \mathrm{PGL}_2^+(\mathbf{R})$ be as in the discussion before Proposition 3.1.1. We can now finally give the following Definition.

Definition 3.3.1. *An* arithmetic subgroup *of* $\mathrm{PGL}_2^+(\mathbf{R})$ *is a subgroup that is commensurable with a group* $\mathrm{P}K_B^+$ *for some choice of* ι *in (3.1).*

Remarks. (i) An inclusion $K' \subset K$ of compact open subgroups of $\widehat{B}^\times$ is of finite index, so using Proposition 2.5.3, we see that $\Gamma \subset \mathrm{PGL}_2^+(\mathbf{R})$ is commensurable with $\mathrm{P}K_B^+$ if and only if it is commensurable with $\mathrm{P}K_B'^+$. Analogously, we see that Γ is commensurable with $\mathrm{P}K_B^+$ if and only if it is commensurable with $\mathrm{P}K_B^1$.

(ii) Since all algebra automorphisms of $M_2(\mathbf{R})$ over $\mathbf{R}$ are inner (*cf.* the proof of Lemma 3.3.4 below), changing the isomorphism (3.1) corresponds to conjugating Γ by elements of $\mathrm{PGL}_2^+(\mathbf{R})$.

In [Tak83], Takeuchi determined the 71 conjugacy classes of arithmetic $(1;e)$-groups. A key ingredient for his classification is the following

Lemma 3.3.2 ([Tak83], Theorem 3.4). *Let* $\Gamma \subset \mathrm{PGL}_2^+(\mathbf{R})$ *be an arithmetic* $(1;e)$-*group. Then*

$$\Gamma^{(2)} = \langle \gamma^2 \mid \gamma \in \Gamma \rangle$$

is a normal subgroup of Γ. *For* $a \in \{\pm 1\}$, *the projection map*

$$X^a(\Gamma^{(2)}) \longrightarrow X^a(\Gamma)$$

induces a map on Jacobians that is isomorphic to multiplication by 2.

The algebra $B(\Gamma) = \mathbf{Q}[\Gamma^{(2)}]$ *is a quaternion algebra over its center, which is a totally real subfield* F *of* $\mathbf{C}$. *The module* $\mathbf{Z}_F[\Gamma^{(2)}]$ *is an order of* $B(\Gamma)$, *and we have* $\Gamma^{(2)} \subset \mathbf{Z}_F[\Gamma^{(2)}]^1$.

Diagrammatically, we get the correspondence

$$\begin{tikzcd} & X^a(\Gamma^{(2)}) \arrow[dl, "{''[2]''}"'] \arrow[dr] & \\ X^a(\Gamma) & & X^a(\mathbf{Z}_F[\Gamma^{(2)}]^1) \end{tikzcd} \tag{3.21}$$

Given Γ, Takeuchi's methods allow one to construct an explicit basis for the order $\mathcal{O} = \mathbf{Z}_F[\Gamma^{(2)}]$ of $B = \mathbf{Q}[\Gamma^{(2)}]$. In the coming Chapters, we usually work with the group $\mathcal{O}^1$ instead of $\Gamma^{(2)}$, due to its more arithmetic nature and due to the fact that testing whether an element of $B^\times$ is in $\mathcal{O}^1$ is considerably easier than testing whether it is in $\Gamma^{(2)}$.

Let Γ be a Fuchsian group of the first kind. To avoid the subtleties involved with proving the presence of a rational point on a model of $X^a(\Gamma)$ in what follows, we consider the Jacobian

$$J^a(\Gamma) = \mathrm{Jac}(X^a(\Gamma)). \tag{3.22}$$

We let $J^a(\mathcal{O}^+)$ and $J^a(\mathcal{O}^1)$ be the Jacobians thus obtained by taking Γ equal to $(\mathrm{P})\mathcal{O}^+$, respectively $(\mathrm{P})\mathcal{O}^1$.

A model C of $X^a(\Gamma)$ over a field L will give rise to an elliptic curve $\mathrm{Jac}(C)$ that is a model of $J^a(\Gamma)$ over L. We now define the notion of a canonical model of $X^a(\Gamma)$ and $J^a(\Gamma)$.

Definition 3.3.3. *Let Γ be a $(1;e)$-group, and let K be a compact open subgroup of $\widehat{B}$. Suppose*

$$\mathrm{P}K_B^+ \subset \mathrm{P}\Gamma \subset \mathrm{P}(N(K)_B^+). \tag{3.23}$$

Then we call the Atkin-Lehner quotient of $\mathrm{Sh}_0^a(K)$ *corresponding to $Y(\Gamma)$ (see Proposition 3.1.4) a* canonical model *of $X^a(\Gamma)$ over F_K. The corresponding quotient of the elliptic curve $J_0^a(K)$ is called a* canonical model *of $J^a(\Gamma)$.*

Our strategy for finding a canonical model for $X^a(\Gamma)$ is therefore the following. Given Γ, we consider the order $\mathcal{O} = \mathbf{Z}_F[\Gamma^{(2)}]$, and let $K_0 = \widehat{\mathcal{O}}^\times$. Then $Y_0^a(K_0) = X^a(\mathbf{Z}_F[\Gamma^{(2)}]^+)$, which is a quotient of $X^a(\mathbf{Z}_F[\Gamma^{(2)}]^1)$. Motivated by the definition above, our goal is to find a group K such that the indices $[K : K \cap K_0]$ and $[K_0 : K \cap K_0]$ are both small and such that K satisfies (3.23); as suggested by Diagram 3.21, K_0 itself may not satisfy these demands. The following lemma is of great use for finding a suitable K.

Lemma 3.3.4. *Let B be as in the first section. Let $\mathcal{O}$ be an order of B such that*

$$\mathcal{O} = \mathbf{Z}_F[\mathcal{O}^1]. \tag{3.24}$$

Let $K = \widehat{\mathcal{O}}^\times$. Then

$$N(\mathrm{P}K_B^1) = N(\mathrm{P}K_B^+) = \mathrm{P}(N(K)_B^+).$$

The normalizer on the left hand side of this equality is taken in $\mathrm{PGL}_2(\mathbf{R})$, *while that on the right hand side is taken in $\widehat{B}^\times$.*

Proof. The inclusion $\mathrm{P}(N(K)_B^+) \subset N(\mathrm{P}K_B^1)$ is trivial. Conversely, the proof of Théorème IV.3.5 of [Vig80] shows that any element x of $N(\mathrm{P}K_B^1)$ also normalizes $B^\times \subset \mathrm{GL}_2(\mathbf{R})$. The Skolem-Noether theorem (Théorème I.2.1 in [Vig80]) then allows us to conclude that up to a scalar, x is equals an element of $B^\times$. Since changing x by a scalar does not affect the resulting automorphism of $Y_0(K)$, we may in fact assume that x is in $B^\times \subset \widehat{B}^\times$.

The hypothesis (3.24) yields that x normalizes the order $\mathcal{O}$. The local-global correspondence (Theorem 2.1.4) then gives that x also normalizes $\widehat{\mathcal{O}}$, which certainly implies that $x \in N(K)$. □

Remark. We will see examples of groups Γ with $\Gamma^{(2)} \subsetneq \mathbf{Z}_F[\Gamma^{(2)}]^1$ and orders $\mathcal{O}$ with $\mathbf{Z}_F[\mathcal{O}^1] \subsetneq \mathcal{O}$ in the calculations in Chapter 7. However, we did not encounter examples where the corresponding normalizers were different.

In Chapter 7, we usually take K to equal $\widehat{\mathcal{O}}^\times \cap \mathrm{nrd}^{-1}(N')$, where $\mathcal{O}$ is a suitable order containing $\mathbf{Z}_F[\Gamma^{(2)}]$ and satisfying (3.24), and where N' is either equal to

$N = \mathrm{nrd}(K)$ or as in Lemma 3.2.3. This almost always gives rise to a genus 1 curve $Y_0(K)$ fitting in a diagram

$$X^a(\Gamma^{(2)}) \longrightarrow Y_0^a(K) \longrightarrow X^a(\Gamma).$$

In such a case, Lemma 3.3.2 shows that $\mathrm{P}\Gamma \subset N(\mathrm{P}K_B^+)$, whence we get $\mathrm{P}K_B^+ \subset \mathrm{P}\Gamma \subset \mathrm{P}(N(K)_B^+)$ by Lemma 3.3.4, giving rise to a canonical model of $Y^a(\Gamma)$ as in Definition 3.3.3.

Chapter 4

Traces

Let $\mathrm{Sh}(K)$ be a Shimura curve, as defined in the previous Chapter. Our present goal is to compute the traces of Frobenius at the primes of good reduction of $\mathrm{Sh}(K)$. The Shimura congruence relation connects these traces with the action of a Hecke algebra on the homology group of $\mathrm{Sh}(K)$: in the third section of this Chapter, we discuss this relation in the generality we need.

In the first section, we define the aforementioned Hecke action. The second section gives an algorithm for its explicit computation, which makes use of the fundamental domains constructed in Chapter 1. Combined with the Shimura congruence relation, this algorithm is one of the main ingredients in the calculation of the canonical models of Chapter 7.

The recent preprints [GV] and [Voi] give more general algorithms for calculating Hecke operators on Shimura curves. Our approach, which was developed independently, has the trifling advantage of being somewhat more elementary on a conceptual level.

4.1 Quaternionic cusp forms

Throughout this section, and as in the first section of the previous Chapter, let F be a totally real field, and let B be a quaternion algebra over F that is split at exactly one infinite place ι of F. Let us furthermore suppose, in order to simplify the exposition, that B is a division algebra; computations in the case $B = M_2(\mathbf{Q})$ can be performed efficiently using the method of modular symbols (see [Ste08]). For a broader view of the material in this section, we refer to [Voi] and [Hid81].

As in Chapter 3, we let $\mathcal{H}^{\pm}$ be the Riemann surface

$$\mathcal{H}^{\pm} = \mathbf{P}^1(\mathbf{C}) - \mathbf{P}^1(\mathbf{R}) = \mathcal{H}^{+} \sqcup \mathcal{H}^{-}.$$

Furthermore, given

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{R})$$

and $x \in \mathcal{H}^{\pm}$, we let

$$j(\gamma, x) = cx + d.$$

Note that $j(\gamma, x)$ is then again an element of $\mathcal{H}^{\pm}$, and that one has the relation

$$j(\gamma_1\gamma_2, x) = j(\gamma_1, \gamma_2 x)\, j(\gamma_2, x) \tag{4.1}$$

and in particular

$$j(\gamma^{-1}, \gamma x)\, j(\gamma, x) = 1. \tag{4.2}$$

The following notion is classical.

Definition 4.1.1. *Let* $\Gamma \subset \mathrm{GL}_2^+(\mathbf{R})$ *be a subgroup whose image in* $\mathrm{PGL}_2^+(\mathbf{R})$ *is discrete and cocompact. A* classical cusp form *for* Γ *(of* weight 2*) is a holomorphic function*

$$f : \mathcal{H} \longrightarrow \mathbf{C}$$

satisfying

$$f(\gamma\tau) = \frac{j(\gamma, \tau)^2}{\det(\gamma)} f(\tau)$$

for all $\gamma \in \Gamma$*.*

Remark. The cocompactness condition on Γ in the definition above implies that $Y(\Gamma) = X(\Gamma)$ does not have any cusps. This allows us to ignore the growth conditions at the cusps needed for general Γ.

Given a group Γ as in the definition, the set of cusp forms of weight 2 for Γ is a finite dimensional complex vector space, which we denote by $S_2(\Gamma)$. The space $S_2(\Gamma)$ can be identified with the space of global sections of the sheaf Ω^1 of holomorphic differential forms on the quotient $X(\Gamma)$:

$$\begin{aligned} S_2(\Gamma) &\xrightarrow{\sim} H^0(X(\Gamma), \Omega^1) \\ f &\longmapsto (\omega_f : \tau \longmapsto f(\tau)\, d\tau). \end{aligned}$$

We call a continuous function $f : \mathcal{H}^{\pm} \times \widehat{B}^{\times} \to \mathbf{C}$ *holomorphic* if it is holomorphic in the first variable. Choosing an isomorphism ι as in (3.1), we get a left action of B on $\mathcal{H}^{\pm}$, for which we correspondingly define $j(b, x) = j(\iota(b), x)$ and $\det(b) = \det(\iota(b))$.

Definition 4.1.2. *Let K be a compact open subgroup of $\widehat{B}^{\times}$. A* (quaternionic) cusp form *for B of* level K *(and* parallel weight 2*) is a holomorphic function*

$$f : \mathcal{H}^{\pm} \times \widehat{B}^{\times} \longrightarrow \mathbf{C}$$

satisfying

$$f(b(x, \widehat{b})k) = \frac{j(b, x)^2}{\det(b)} f(x, \widehat{b}). \tag{4.3}$$

for all $b \in B^{\times}$, $x \in \mathcal{H}^{\pm}$, $\widehat{b} \in \widehat{B}^{\times}$ *and* $k \in K$*.*

Remark. For a definition of quaternionic modular forms of arbitrary weight, we refer to [Hid81] and [Voi]; in this thesis, we shall only use forms of parallel weight 2.

We denote the space of modular forms for B of level K by $S_2(K)$. In accordance with [Hid81], there is the following compatibility with the classical notion:

Proposition 4.1.3. *Let $\{r_i\}_{i=1}^h$ be a set of representatives for the quotient*

$$B^+\backslash\widehat{B}^\times/K. \tag{4.4}$$

Then giving a modular form for B of level K is the same as giving a tuple $(f_i)_{i=1}^h$ of Γ_i-modular forms, where Γ_i is the group

$$(r_iKr_i^{-1})_B^+ = (r_iKr_i^{-1}) \cap B^+ \subset B^+,$$

embedded into $\mathrm{GL}_2^+(\mathbf{R})$ through (3.1).

Proof. Given a modular form of level K, we define the tuple $(f_i)_i$ by

$$f_i(\tau) = f(\tau, r_i).$$

We have to check that f_i is Γ_i-modular. But for $\iota(b_i) \in \Gamma_i$, one has $r_i^{-1}b_ir_i \in K$, so by right K-invariance of f we have

$$\begin{aligned}
f_i(b_i\tau) &= f(b_i\tau, r_i)\\
&= f(b_i(\tau, b_i^{-1}r_i))\\
&= \frac{j(b_i,\tau)^2}{\det(b_i)} f(\tau, b_i^{-1}r_i)\\
&= \frac{j(b_i,\tau)^2}{\det(b_i)} f(\tau, b_i^{-1}r_ir_i^{-1}b_ir_i)\\
&= \frac{j(b_i,\tau)^2}{\det(b_i)} f(\tau, r_i)\\
&= \frac{j(b_i,\tau)^2}{\det(b_i)} f_i(\tau).
\end{aligned}$$

Conversely, suppose that we are given a tuple $(f_i)_i$ of Γ_i-modular forms. Note that because $\{r_i\}$ is a set of representatives for the quotient (4.4), the set $\{+1, r_i\}$ is a set of representatives for the quotient

$$\mathrm{Pic}_r(K\infty) = B^\times\backslash\{\pm 1\} \times \widehat{B}^\times/K$$

from Section 2.6. Hence every $(x, \widehat{b}) \in \mathcal{H}^\pm \times \widehat{B}^\times$ is of the form

$$(x, \widehat{b}) = b(\tau, r_i)k \tag{4.5}$$

$$(b \in B^\times,\ \tau \in \mathcal{H},\ k \in K)$$

for a uniquely determined i. We let

$$f(x,\widehat{b}) = \frac{j(b,\tau)^2}{\det(b)} f_i(\tau).$$

As soon as we show that this is well-defined, modularity of f follows easily, since given $b' \in B^\times$ and $(x,\widehat{b})$ as in (4.5) one has

$$b'(x,\widehat{b}) = (b'b)(\tau,r_i)k,$$

whence, using (4.1), we get

$$\begin{aligned} f(b'(x,\widehat{b})) &= \frac{j(b'b,\tau)^2}{\det(b'b)} f_i(\tau) \\ &= \frac{j(b',b\tau)^2}{\det(b')} \frac{j(b,\tau)^2}{\det(b)} f_i(\tau) \\ &= \frac{j(b',b\tau)^2}{\det(b')} f(x,\widehat{b}). \end{aligned}$$

So suppose that

$$b_1(\tau_1,r_i)k_1 = b_2(\tau_2,r_i)k_2.$$

Then since $b_1\tau_1 = b_2\tau_2$, we have that $b_1^{-1}b_2 \in B^+$. Hence

$$b_1^{-1}b_2 = r_ik_1k_2^{-1}r_i^{-1} \in B^+ \cap r_iKr_i^{-1} = (r_iKr_i^{-1})_B^+.$$

Using (4.1), then (4.2), we therefore get

$$\begin{aligned} \frac{j(b_1,\tau_1)^2}{\det(b_1)} f_i(\tau_1) &= \frac{j(b_1,\tau_1)^2}{\det(b_1)} f_i(b_1^{-1}b_2\tau_2) \\ &= \frac{j(b_1,b_1^{-1}b_2\tau_2)^2}{\det(b_1)} \frac{j(b_1^{-1}b_2,\tau_2)^2}{\det(b_1^{-1}b_2)} f_i(\tau_2) \\ &= \frac{j(b_1,b_1^{-1}b_2\tau_2)^2}{\det(b_1)} \frac{j(b_1^{-1},b_2\tau_2)^2}{\det(b_1^{-1})} \frac{j(b_2,\tau_2)^2}{\det(b_2)} f_i(\tau_2) \\ &= \frac{j(b_2,\tau_2)^2}{\det(b_2)} f_i(\tau_2). \end{aligned}$$

hence $f(x,\widehat{b})$ is indeed well-defined.

By construction, the two associations above are mutually inverse. □

Remarks. (i) Another way to express the demand on the set $\{r_i\}$ in the proposition, which we used in the proof above, is that the set $\{(+1,r_i)\}$ is a set of representatives for the quotient $\mathrm{Pic}_r(K\infty)$. In fact, we could also have worked with an arbitrary set of representatives for $\mathrm{Pic}_r(K\infty)$. This, though, results in the use of functions on $\mathcal{H}^-$. Since classically, only $\mathcal{H}^+$ is used, we have decided only to use sets of representatives $\{(+1, r_i)\}$ in the proposition. However, we will use more general representatives in the next section.

(ii) According to Proposition 3.1.1(ii), the choice of a set $\{r_i\}$ gives rise to an isomorphism

$$Y(K) \cong \coprod_{i=1}^{h} Y(\Gamma_i)$$

Combining the same proposition with Remark (ii) after Definition 4.1.1, we obtain the following isomorphism:

$$\begin{aligned} S_2(K) &\xrightarrow{\sim} H^0(\coprod_{i=1}^{h} Y(\Gamma_i), \Omega_1) \\ f &\longmapsto (f_i(\tau)\, d\tau)_{i=1}^{h} \end{aligned}$$

This isomorphism allows the simpler description

$$\begin{aligned} S_2(K) &\xrightarrow{\sim} H^0(Y(K), \Omega^1) \\ f &\longmapsto (\omega_f : (x, \widehat{b}) \longmapsto f(x, \widehat{b})\, dx). \end{aligned} \tag{4.6}$$

We will later return to this geometric viewpoint.

The reason for the extension of the classical notion in Proposition 4.1.3 is that it allows us to define Hecke operators, which would be missing if we were to concentrate on a single Γ_i.

Definition 4.1.4. *Let f be a modular form for B of level K, and let $u \in \widehat{B}^\times$. Decomposing the double coset*

$$KuK = \coprod_{l=1}^{d} uK$$

with $u_l = k_l u$ ($k_l \in K$), we define

$$f|_{KuK}(x, \widehat{b}) = \sum_{l=1}^{d} f(x, \widehat{b}u_l).$$

This definition is independent of the choice of the set $\{u_l\}$. Indeed, suppose $\{u'_l\}$ is another set of representatives. After renumbering, we may assume that we have $u_l K = u'_l K$ for all l. By right K-invariance of f, one then has $f(x, \widehat{b}u'_l) = f(x, \widehat{b}u_l)$ for all l, hence both choices give rise to the same $f|_{KuK}$. Note that the given decomposition is indeed finite because of the bijection $KuK/K \cong K/(K \cap uKu^{-1})$ from Lemma 5.1.1 in [DS05], considering that both K and uKu^{-1}, hence also $K \cap uKu^{-1}$, are compact open.

We make Definition 4.1.4 explicit in terms of the tuples of Proposition 4.1.3. Let $(f_i)_i$ have associated tuple $(f_i)_i$. Then the i-th component of the tuple $((f|_{KuK})_i)_i$ associated with $f|_{KuK}$ satisfies

$$\begin{aligned} (f|_{KuK})_i(\tau) &= f|_{KuK}(\tau, r_i) \\ &= \sum_{l=1}^{d} f(\tau, r_i u_l). \end{aligned}$$

We can write

$$r_i u_l = b_l r_j k_l$$
$$(b_l \in B^+,\ k_l \in K)$$

for some j that is independent of l because the $r_i u_l$ differ by right multiplication with elements of K, hence represent the same element of (4.4). Using relation (4.2), the expression above takes the form

$$\begin{aligned}(f|_{KuK})_i(\tau) &= \sum_{l=1}^{d} f(b_l(b_l^{-1}\tau, r_j k_l)) \\ &= \sum_{l=1}^{d} \frac{j(b_l, b_l^{-1}\tau)^2}{\det(b_l)} f(b_l^{-1}\tau, r_j k_l) \\ &= \sum_{l=1}^{d} \frac{\det(b_l^{-1})}{j(b_l^{-1},\tau)^2} f_j(b_l^{-1}\tau).\end{aligned}$$

This is exactly the tuple in (1.8.4) of [Hid81], so the definition above ties in with the general one coming from the theory of automorphic forms.

A more geometric and conceptual way of viewing this situation, that also shows that $f|_{KuK}$ is modular (which, though straightforward, we have not proved yet) is the following. Consider the diagram

$$\begin{tikzcd} Y(K \cap uKu^{-1}) \arrow[r, "r_u"] \arrow[d, "p_1"] & Y(K \cap u^{-1}Ku) \arrow[d, "p_2"] \\ Y(K) & Y(K) \end{tikzcd} \tag{4.7}$$

where the p_i are canonical projections and r_u is the isomorphism induced by the map

$$\begin{aligned}\mathcal{H}^{\pm} \times \widehat{B}^{\times} &\xrightarrow{\sim} \mathcal{H}^{\pm} \times \widehat{B}^{\times} \\ (x, \widehat{b}) &\longmapsto (x, \widehat{b}u).\end{aligned}$$

Given a morphism of Riemann surfaces $\varphi : X \to Y$, we denote by φ_* and φ^* the induced pushforward and pullback morphisms on the spaces of global holomorphic differentials $H^0(\mathrm{Sh}(K), \Omega^1)$ (for definitions, see Chapter 5 of [DS05]). We will later also denote the induced pushforward and pullback maps on integral homology by these symbols.

Diagram (4.7) then gives rise to a map

$$p_{1*} r_u^* p_2^* : H^0(\mathrm{Sh}(K), \Omega^1) \longrightarrow H^0(\mathrm{Sh}(K), \Omega^1).$$

Proposition 4.1.5. *Let $f \in S_2(K)$. Then*

$$p_{1*} r_u^* p_2^* \omega_f = \omega_{f|_{KuK}}.$$

In other words, $f \mapsto f|_{KuK}$ is an endomorphism of $S_2(K)$, and corresponds to the endomorphism $p_{1*} r_u^* p_2^*$ of $H^0(\mathrm{Sh}(K), \Omega^1)$ under the isomorphism (4.6).

Proof. Choose a set of representatives $\{k_l\}_l$ for the quotient $K/(K \cap uKu^{-1})$. Then the set $\{k_l u\}_l$ is a set of representatives for KuK/K (*cf.* Lemma 5.1.1 in [DS05]). So

$$f|_{KuK}(x, \widehat{b}) = \sum_{l=1}^{d} f(x, \widehat{b}k_l u).$$

Identifying the cotangent spaces at the points $(x, \widehat{b}) \in \mathcal{H}^{\pm} \times \widehat{B}^{\times}$ for varying $\widehat{b}$, we will now calculate the sequence $p_{1*}r_u^* p_2^*$ of pullbacks and pushforwards. Given a point of $Y(K)$ represented by $(x, \widehat{b})$, the fiber above it in $Y(K \cap uKu^{-1})$ is represented by the set $\{(x, \widehat{b}k_l)\}_l$. Therefore, tracing through the definitions, we obtain

$$\begin{aligned}
[p_{1*}r_u^* p_2^* \omega_f](x, \widehat{b}) &= \sum_{l=1}^{d} [r_u^* p_2^* \omega_f](x, \widehat{b}k_l) \\
&= \sum_{l=1}^{d} [p_2^* \omega_f](x, \widehat{b}k_l u) \\
&= \sum_{l=1}^{d} \omega_f(x, \widehat{b}k_l u) \\
&= \omega_{f|_{KuK}}(x, \widehat{b}).
\end{aligned}$$

Alternatively, one considers ω_f as a $B^{\times}(F) - K$-invariant differential form on $\mathcal{H}^{\pm} \times \widehat{B}^{\times}$ and uses equivariance of the p_i and r_u. □

For a more complete account of what follows, we refer to [Shi70]. Let $\mathfrak{p}$ be a prime of F not dividing the discriminant of B at which K is maximal, that is, given by the unit group $\mathcal{O}(1)_{\mathfrak{p}}^{\times}$ of some maximal order $\mathcal{O}(1)_{\mathfrak{p}}$ of $B_{\mathfrak{p}}$. We can in fact choose an isomorphism $B_{\mathfrak{p}} \cong M_2(F_{\mathfrak{p}})$ such that $\mathcal{O}(1)_{\mathfrak{p}}^{\times}$ corresponds to $M_2(\mathbf{Z}_{F,\mathfrak{p}})$. Let $u_{\mathfrak{p}} \in \mathcal{O}(1)_{\mathfrak{p}}$ be such that $\mathrm{nrd}(u_{\mathfrak{p}})$ is a uniformizer of $\mathbf{Z}_{F,\mathfrak{p}}$.

Let $u^{\mathfrak{p}}$ be the element of $\widehat{B}^{\times}$ having trivial components 1 outside $\mathfrak{p}$ and component $u_{\mathfrak{p}}$ at $\mathfrak{p}$. Then the coset $Ku^{\mathfrak{p}}K$ is independent of the choice of $u^{\mathfrak{p}}$. Indeed, this is clear outside of $\mathfrak{p}$, and at $\mathfrak{p}$ we have

$$K_{\mathfrak{p}} u_{\mathfrak{p}} K_{\mathfrak{p}} = \{x \in \mathcal{O}(1)_{\mathfrak{p}} \ : \ \mathrm{nrd}(x)\mathbf{Z}_{F,\mathfrak{p}} = \mathfrak{p}\mathbf{Z}_{F,\mathfrak{p}}\}.$$

Outside of $\mathfrak{p}$, the groups K and $K \cap u^{\mathfrak{p}}K(u^{\mathfrak{p}})^{-1}$ are identical. At $\mathfrak{p}$, the group $K_{\mathfrak{p}}$ equals the unit group of $\mathcal{O}(1)_{\mathfrak{p}}$, while $(K \cap u^{\mathfrak{p}}K(u^{\mathfrak{p}})^{-1})_{\mathfrak{p}}$ is the unit group of the local Eichler order $\mathcal{O}(1)_{\mathfrak{p}} \cap u_{\mathfrak{p}}\mathcal{O}(1)_{\mathfrak{p}}(u_{\mathfrak{p}})^{-1}$. By Proposition 2.4.2(ii), we therefore have

$$\mathrm{nrd}(K) = \mathrm{nrd}(K \cap u^{\mathfrak{p}}K(u^{\mathfrak{p}})^{-1}). \tag{4.8}$$

Theorem 3.1.2 gives that for any choice of u, Diagram (4.7) descends to the canonical models over F of the corresponding Shimura curves. Hence the morphism $p_{1*}r_u^* p_2^*$ is an element of $\mathrm{End}(J(K))$. By Proposition 4.1.5, this element only depends on the double coset KuK.

Definition 4.1.6. *Let $\mathfrak{p}$ be a prime of F not dividing the discriminant of B at which K is maximal. The* Hecke operator $T(\mathfrak{p})$ *is the endomorphism $p_{1*}r^*_{u^\mathfrak{p}}p_2^*$ of $J(K)$. The* (restricted) Hecke algebra $\mathbf{T}_K$ *of K is the subalgebra of* $\mathrm{End}(J(K))$ *generated by the Hecke operators $T(\mathfrak{p})$. A* Hecke module *is an abelian group equipped with an action of* $\mathbf{T}_K$*.*

Remark. We use the term "restricted" in the definition of the Hecke algebra above because elsewhere (*e.g.* in [Voi]), the Atkin-Lehner and complex conjugation endomorphisms of $J(K)$ are also added. For our purposes, the simplification above will do.

In the next section, we will use the following dualization. Let

$$H_1(Y(K)) = H_1(Y(K), \mathbf{C}) = H_1(Y(K), \mathbf{Z}) \otimes \mathbf{C}.$$

We equip $H_1(Y(K))$ with the following structure of $\mathbf{T}_K \otimes \mathbf{C}$-module:

$$\begin{aligned} \mathbf{T}_K \otimes \mathbf{C} &\longrightarrow \mathrm{End}(H_1(Y(K))) \\ T(\mathfrak{p}) \otimes 1 &\longmapsto p_{2*}r_{u^\mathfrak{p}*}p_1^* \end{aligned}$$

The pairing

$$H_1(Y(K)) \times H^0(Y(K), \Omega^1) \longrightarrow \mathbf{C} \tag{4.9}$$

is then equivariant for the action of the Hecke algebra $\mathbf{T}_K \otimes \mathbf{C}$.

4.2 Computing Hecke operators

We will use the Hecke module $H_1(Y(K))$ to calculate the eigenvalues of the endomorphisms $T(\mathfrak{p})$ of J(K). Before we proceed to do this, we add a few hypotheses to those in the first section. Recall the definitions of $\mathrm{Pic}_r(K)$ and $\mathrm{Pic}_r(K\infty)$ from Section 2.6. We first demand that

$$|\mathrm{Pic}_r(K)| = 1. \tag{4.10}$$

Using the techniques of Proposition 2.6.1(i), we see that this is equivalent to demanding

$$|F_B^\times \backslash \widehat{F}^\times / \mathrm{nrd}(K)| = 1. \tag{4.11}$$

The paper [GV] describes how to compute the Hecke operators if $\mathrm{Pic}_r(K\infty)$ is trivial. Let us therefore additionally suppose that this is not the case: considering that the fibers of the projection $\{\pm 1\} \times \widehat{B}^\times \to \widehat{B}^\times$ have cardinality 2, this is equivalent to demanding that

$$|\mathrm{Pic}_r(K\infty)| = 2. \tag{4.12}$$

or equivalently, by Proposition 2.6.1(i), that

$$|\mathrm{Cl}(K\infty)| = 2. \tag{4.13}$$

Considering the hypotheses in (4.10) and (4.12), Proposition 3.1.1 shows that we have

$$Y(K) \cong K_B^+ \backslash \mathcal{H}^\pm = Y_0^+(K) \sqcup Y_0^-(K).$$

Identifying $Y(K) \cong K_B^+ \backslash \mathcal{H}^\pm$, we correspondingly get a decomposition

$$H_1(Y(K)) = H_1(Y_0^+(K)) \oplus H_1(Y_0^-(K)). \tag{4.14}$$

For $a \in \{\pm 1\}$, we can consider the projection $p^a : \mathcal{H}^a \longrightarrow Y_0^a(K)$. If additionally $k \in K_B^+$ is given, then we denote by $[a, k]$ the homology class

$$[p^a \gamma] \in H_1(Y_0^a(K)) \subset H_1(Y(K)),$$

where for some choice of a non-elliptic point $x \in \mathcal{H}^a$, we let $\gamma : [0,1] \to \mathcal{H}^a$ be a path with $\gamma(0) = x$ and $\gamma(1) = kx$. The homology class $[p^a\gamma]$ is independent of the choice of x. It is also independent of the choice of γ because $\mathcal{H}$ is simply connected.

Let g be the genus of $Y_0^+(K)$, and choose elements $k_1 \ldots k_{2g}$ of K_B^+ that give a basis for $H_1(Y_0^+(K))$ (*cf.* Theorem 6.1.5). The same elements will then give a basis for $H_1(Y_0^-(K))$. We correspondingly rewrite (4.14) as

$$H_1(Y(K)) = \bigoplus_{i=1}^{2g} \mathbf{C}[1, k_i] \oplus \bigoplus_{i=1}^{2g} \mathbf{C}[-1, k_i], \tag{4.15}$$

We also let

$$H = \bigoplus_{i=1}^{2g} \mathbf{C}([1, k_i] + [-1, k_i]) \subset H_1(Y(K)). \tag{4.16}$$

Then the pairing (4.9) restricts to a pairing

$$H \times H^0(Y(K), \Omega^1) \longrightarrow \mathbf{C}. \tag{4.17}$$

This pairing is perfect. Indeed, choose a basis for $H^0(Y_0^+(K), \Omega^1)$ such that the period matrix of $Y_0^+(K)$ with respect to the basis $\{[1, k_1], \ldots, [1, k_{2g}]\}$ of $H_1(Y_0^+(K))$ is given by $(I\ \Omega)$, where I equals the $g \times g$ identity matrix. Then there is a corresponding basis for $H^0(Y_0^-(K), \Omega^1)$ such that the period matrix of $Y_0^-(K)$ with respect to $\{[-1, k_1], \ldots, [-1, k_{2g}]\}$ is given by $(I\ \overline{\Omega})$. But it is well-known that the matrix

$$\begin{pmatrix} I & \Omega \\ I & \overline{\Omega} \end{pmatrix}$$

is non-singular.

We will now make the action of $\mathbf{T}_K$ on the classes $[a, k]$ more explicit: since these classes generate $H_1(Y(K))$, this will allow us to determine the $\mathbf{T}_K \otimes \mathbf{C}$-module structure of $H_1(Y(K))$.

Given a prime ideal $\mathfrak{p}$ at which K is maximal, let $u^{\mathfrak{p}}$ as in the previous section. By (4.10), there exists a $\pi \in B^{\times}$ and a $k \in K$ such that $u^{\mathfrak{p}} = \pi k$. We therefore have

$$K\pi K = Ku^{\mathfrak{p}}K$$

for the global element π. We work our way through the composition

$$H_1(Y(K)) \xrightarrow{p_1^*} H_1(Y(K \cap \pi K \pi^{-1})) \xrightarrow{r_{\pi *}} H_1(Y(K \cap \pi^{-1} K \pi)) \xrightarrow{p_{2*}} H_1(Y(K))$$

in terms of elements $[a,k]$.

$\mathbf{p_1^*}$: We have

$$(K \cap \pi K \pi^{-1})_B^+ \cong K_B^+ \cap \pi^{-1} K_B^+ \pi.$$

Considering the equality (4.8), by Proposition 3.1.1, we can therefore identify

$$Y(K \cap \pi K \pi^{-1}) \cong (K_B^+ \cap \pi^{-1} K_B^+ \pi) \backslash \mathcal{H}^{\pm}.$$

Correspondingly, we identify p_1 with the projection

$$(K_B^+ \cap \pi^{-1} K_B^+ \pi) \backslash \mathcal{H}^{\pm} \longrightarrow K_B^+ \backslash \mathcal{H}^{\pm}.$$

The map p_1^* can be described as follows (*cf.* Chapter 5 of [DS05]). Let γ be a loop in $Y(K)$ with base point P say. Then γ lifts to $\deg(p_1)$ different paths in $Y(K \cap \pi K \pi^{-1})$. Each of these lifted paths starts at a different point of the fiber of $Y(K \cap \pi K \pi^{-1})$ over P. These lifts are not necessarily loops again. However, they do concatenate to give a set of loops in $Y(K \cap \pi K \pi^{-1})$. By definition, $p_1^*[\gamma]$ is the class of the sum of these loops in $H_1(Y(K \cap \pi K \pi^{-1}))$.

Using this description, starting with $(a,k) \in \{\pm 1\} \times K_B^+$, we shall now calculate an element of $\{\pm 1\} \times (K_B^+ \cap \pi^{-1} K_B^+ \pi)$ representing $p_1^*[a,k]$. Choose an x and a γ projecting to $[a,k]$ as above. The fiber of p_1 over a point $K_B^+ x$ of $Y(K)$ is then given by

$$p^{-1}(x) = (K_B^+ \cap \pi^{-1} K_B^+ \pi) \backslash K_B^+ x.$$

Moreover, the canonical map

$$(K_B^+ \cap \pi^{-1} K_B^+ \pi) \backslash K_B^+ \longrightarrow (K_B^+ \cap \pi^{-1} K_B^+ \pi) \backslash K_B^+ x$$

is an isomorphism since $F \cap K_B^+ = F \cap (K_B^+ \cap \pi^{-1} K_B^+ \pi)$.

Choose a coset c_1 in $(K_B^+ \cap \pi^{-1} K_B^+ \pi) \backslash K_B^+$, that is, a point of the fiber $p_1^{-1}(x)$. Since c_1 is in K_B^+, the path $c_1\gamma : t \mapsto c_1(\gamma(t))$ obtained by by applying c_1 to γ projects to the path $[a,k]$ in $Y(K)$. Denote the projection of $c_1\gamma$ to $Y_0^a(K \cap \pi^{-1} K \pi)$ by $[c_1\gamma]$. The path $[c_1\gamma]$ connects the elements of the fiber $p_1^{-1}(x)$ represented by $c_1 x$ and $c_1 k x$, and need not be a loop.

However, one then constructs the path $[c_1 k \gamma]$. This is a lift of $[a,k]$ connecting the elements of $\mathfrak{p}_1^{-1}(x)$ represented by $c_1 k x$ and $c_1 k^2 x$. We can continue this process and construct the paths $[c_1 k^i \gamma]$. We eventually end up with a minimal

n_1 for which $c_1k^{n_1}x$ represents the same element of the fiber as c_1x. The paths $[c_1\gamma], \ldots, [c_1k^{n_1}\gamma]$ then concatenate to give a loop in $Y_0^a(K \cap \pi^{-1}K\pi)$. The integer n_1 is the cardinality of the right $\langle k \rangle$-orbit of the coset represented by c_1 in $(K_B^+ \cap \pi^{-1}K_B^+\pi)\backslash K_B^+$. Since $(c_1k^{n_1}c_1^{-1})c_1x = c_1k^{n_1}x$, the concatenated loop we finally end up with is given by

$$[a, c_1k^{n_1}c_1^{-1}] \in H_1(Y_0^a(K)) \subset H_1(Y(K)).$$

Subsequently, one chooses a new c_2 and inductively repeats the process until the space of cosets $(K_B^+ \cap \pi^{-1}K_B^+\pi)\backslash K_B^+$ is exhausted. In the end, we get an equality

$$p_1^*[a,k] = [a, \prod_j c_jk^{n_j}c_j^{-1}],$$

where the set $\{c_j\}$ is a set of representatives for the quotient

$$(K_B^+ \cap \pi^{-1}K_B^+\pi)\backslash K_B^+ / \langle k \rangle$$

and n_j is the cardinality of the right $\langle k \rangle$-orbit of the coset represented by c_j in $(K_B^+ \cap \pi^{-1}K_B^+\pi)\backslash K_B^+$, which is simply the cardinality of the fiber of the map

$$(K_B^+ \cap \pi^{-1}K_B^+\pi)\backslash K_B^+ \longrightarrow (K_B^+ \cap \pi^{-1}K_B^+\pi)\backslash K_B^+ / \langle k \rangle$$

over the coset on the right hand side represented by c_j.

$\boldsymbol{r_{\pi *}}$: Let $(a,k) \in \{\pm 1\} \times (K_B^+ \cap \pi^{-1}K_B^+\pi)$. Choose x and γ corresponding to $[a,k]$ as before.

The class $r_{\pi *}[a,k]$ is by definition equal to the homology class of the projection of the path $r_\pi\gamma$ to $Y(K \cap \pi K\pi^{-1})$. The path $r_\pi\gamma$ connects the points (x,π) and (kx,π) of $\mathcal{H}^\pm \times \widehat{B}^\times$. It is therefore left $B^\times$-equivalent to a path between the points $(\pi^{-1}x, 1)$ and $(\pi^{-1}kx, 1)$ of $\mathcal{H}^\pm \times \widehat{B}^\times$ whose projection to $Y(K \cap \pi K\pi^{-1})$ is equal to that of $r_\pi\gamma$.

Since $x \in \mathcal{H}^a$, we have that $\pi^{-1}x$ is in $\mathcal{H}^{a'}$, where

$$a' = \mathrm{sgn}(\iota(\mathrm{nrd}(\pi)))a.$$

The sign $\mathrm{sgn}(\iota(\mathrm{nrd}(\pi)))$ is independent of the choice of π because of (4.13). We also have that

$$\pi^{-1}kx = (\pi^{-1}k\pi)\pi^{-1}x.$$

Therefore

$$r_{\pi *}[a,k] = [\mathrm{sgn}(\iota(\mathrm{nrd}(\pi)))a, \pi^{-1}k\pi].$$

$\mathbf{p_{2*}}$: Using the same arguments as for the case $r_{\pi *}$, one sees that this operation corresponds to the inclusion map

$$\{\pm 1\} \times (K_B^+ \cap \pi K_B^+\pi^{-1}) \hookrightarrow \{\pm 1\} \times K_B^+.$$

The description above shows that $H \subset H_1(Y(K))$ is a Hecke submodule. Indeed, we have

$$T(\mathfrak{p})[a_1,k_1] = [a_2,k_2] \Leftrightarrow T(\mathfrak{p})[-a_1,k_1] = [-a_2,k_2].$$

In light of (4.17), we can therefore read off the eigenvalues of the operators $T(\mathfrak{p})$ on $J(K)$ from the Hecke module H. Indeed, the discussion above motivates the following algorithm:

Algorithm 4.2.1. *Let F, B and K satisfy the hypotheses at the beginning of this section. Choose elements $k_1, \dots, k_{2g}$ of K_B^+ generating a homology basis for $Y_0^+(K)$. Let H be the $\mathbf{T}_K \otimes \mathbf{C}$-module from (4.16), and consider the ordered basis*

$$S = \{k_1 + \overline{k}_1, \dots, k_{2g} + \overline{k}_{2g}\}$$

of H.

Let $\mathfrak{p}$ be a prime of F, and let $u_{\mathfrak{p}}$ be as in the discussion before Definition 4.1.6. This algorithm returns the matrix $M(\mathfrak{p})$ of the Hecke operator $T(\mathfrak{p})$ on H with respect to the ordered basis S.

1. *Find a $\pi \in \widehat{B}^\times$ such that $Ku^{\mathfrak{p}}K = K\pi K$.*

2. *Initialize $i = 1$.*

3. *Initialize $c = k = 1 \in K_F^+$, $C = \emptyset$.*

4. *Determine the smallest integer $n \leq 1$ such that $ck_i^n c^{-1} \in K_B^+ \cap \pi^{-1} K_B^+ \pi$. Add the elements $c, ck_i, \dots ck_i^{n-1}$ to C. Set $k := kck_i^n c^{-1}$.*

5. *Determine a set T of generators of K_B^+. Check for each element of the set $CT = \{ct : c \in C, t \in T\}$ if it is left $K_B^+ \cap \pi^{-1} K_B^+ \pi$-equivalent to an element of C. If so, proceed to step 6. If not, set c equal to an element of ST that is not equivalent to any element of C and go to step 4.*

6. *Calculate $k' = \pi^{-1} k \pi$. Decompose*

$$[1, k'] = \sum_{i=1}^{2g} m_{ij} [1, k_i]$$

in $H_1(Y_0^+(K))$. If $i = 2g$, then go to step 7: otherwise increase i by 1 and go to step 2.

7. *Return the matrix $M = (m_{ij})_{i,j=1}^{2g}$.*

Proof of correctness. This follows from the preceding discussion, except perhaps for step 5. But the correctness of this step follows from the proof of correctness of algorithm 6.1.7 in Chapter 6: one checks that C is a set of representatives for the quotient $(K_B^+ \cap \pi^{-1} K_B^+ \pi) \backslash K_B^+$. □

It remains to describe how to implement this pseudo-code using the existing functionality for quaternion algebras in `Magma`, as at [Sij10]. We restricted our considerations to the Shimura curves arising from arithmetic $(1; e)$-curves in

Chapter 7. As mentioned at the end of Section 3.3 for these cases, one can usually find an order $\mathcal{O}$ containing $\mathbf{Z}_F[\Gamma^{(2)}]$ such that the group

$$K = \widehat{\mathcal{O}}^\times \cap \operatorname{nrd}^{-1} N'$$

has the property

$$\mathrm{P}\Gamma^{(2)} \subseteq \mathrm{P}(K_B^+) \subseteq \mathrm{P}\Gamma. \tag{4.18}$$

Here N' is either equal to $N = \operatorname{nrd}(K)$ or as in Lemma 3.2.3. Such a choice of K greatly simplifies the implementation of the steps above:

Preliminaries: First we have to give elements of K_B^+ that form a basis for the homology group $H_1(Y_0^+(K))$. In the final section of Chapter 1, we saw that $\{A, B\}$ is a homology basis for $H_1(X(\Gamma))$. For K_B^+ as in (4.18), one deduces the following table:

K_B^+	Signature	Generators	Basis of H_1
$\Gamma^{(2)}$	$(1; e, e, e, e)$	A^2, B^2, G, AGA^{-1}, $BGB^{-1}, BAGA^{-1}B^{-1}$	$\{A^2, B^2\}$
$\langle\Gamma^{(2)}, A\rangle$	$(1; e, e)$	A, B^2, G	$\{A, B^2\}$
$\langle\Gamma^{(2)}, B\rangle$	$(1; e, e)$	A^2, B, G	$\{A^2, B\}$
$\langle\Gamma^{(2)}, AB\rangle$	$(1; e, e)$	$AB, A^{-1}B, AB^{-1}$	$\{A^2, AB\}$
Γ	$(1; e)$	A, B	$\{A, B\}$

We have also given generators for K_B^+ for use in step 5: these were determined in [Tak83]. In the corresponding column, G denotes the commutator $[A^{-1}, B^{-1}]$.

Step 1: Suppose $\pi \in \mathcal{O}$ has the property that $\operatorname{nrd}(\pi)$ is in $N'^{\mathfrak{p}} = N' \cap B^{\mathfrak{p}}$ and generates the prime ideal $\mathfrak{p} \subset \mathbf{Z}_F$. Then we have $K\pi K = Ku^{\mathfrak{p}}K$. Conversely, by (4.11), there exists an element $\pi \in \mathcal{O}$ such that for some k in K we have $\pi = u^{\mathfrak{p}}k$. This π will satisfy the conditions on $\operatorname{nrd}(\pi)$ described above.

We have searched for such elements π by naively enumerating the elements of $\mathcal{O}$. Whether the $\operatorname{nrd}(\pi)$ generates $\mathfrak{p}$ is easily verified. As for testing whether or not $\operatorname{nrd}(\pi) \in N'^{\mathfrak{p}}$, the group $N = \operatorname{nrd}(K)$ can be calculated explicitly using Algorithm 2.4.3, and in Lemma 3.2.3, we have obtained N' from N by a constructive process. Hence this test reduces to a finite amount of explicit congruence conditions on $\operatorname{nrd}(\pi)$.

Step 4: This reduces to testing whether the element $ck_i^n c^{-1}$ of $K_B^+ \subset \mathcal{O}$ is in $\mathcal{O} \cap \pi\mathcal{O}\pi^{-1}$. Indeed, the norm condition is automatically satisfied by $ck_i^n c^{-1}$ because it is satisfied by k_i. Now testing whether $ck_i^n c^{-1}$ is in $\mathcal{O} \cap \pi\mathcal{O}\pi^{-1}$ is straightforward once a $\mathbf{Z}$-basis of $\mathcal{O}$ is available (either from [Tak83] or by using the `Magma` function `ZBasis`).

Step 5: This step requires no more functionality than step 4.

Step 6: This is a straightforward application of Algorithm 1.4.2.

Remarks. (i) Condition (4.11) is satisfied in all but one case (e3d21D3) in Takeuchi's list. Algorithm 4.2.1 then still allows us to determine $T(\mathfrak{p})$ at prime ideals $\mathfrak{p}$ that are trivial in the class group $F_B^\times \backslash \widehat{B}^\times / \operatorname{nrd}(K)$.

(ii) Let us remark that it is sometimes possible to eschew passage to the homology group and calculate with (Hecke) correspondences directly: this is the approach taken in Section 5.4 of [Elk98], which can also be used to determine the accessory parameter A in (0.1). However, such an inroad only seems amenable to explicit computation if the correspondences involved have small degree. If no small primes outside $\mathfrak{D}(B)^f$ split, then the resulting Hecke correspondences will in general be of too large degree to calculate effectively.

4.3 Shimura congruence

Let F, B and K be as at the beginning of this Chapter, and let $\mathfrak{p}$ be a prime of F at which K is maximal. Consider the Hecke operator $T(\mathfrak{p})$ from Definition 4.1.4. By Theorem 3.1.6, the curve $\mathrm{Sh}(K)$, and hence its Jacobian $J(K)$, has good reduction at $\mathfrak{p}$. As such, we can reduce the operator $T(\mathfrak{p})$ modulo $\mathfrak{p}$ to get an endomorphism

$$\widetilde{T}(\mathfrak{p}) \in \mathrm{End}(\widetilde{J}(K)).$$

of the reduction $\widetilde{J}(K)$ of $J(K)$ modulo $\mathfrak{p}$. A fundamental result, indeed our reason for considering Hecke operators at all, is the following congruence relation.

Theorem 4.3.1 (Shimura congruence relation)**.** *Suppose that K contains $\widehat{\mathbf{Z}}_F^\times$ and is maximal at the prime $\mathfrak{p}$. Additionally, suppose that $\mathfrak{p}$ is trivial in the class group* $\mathrm{Cl}(1)$*.*

Let $\sigma(\mathfrak{p})$ be the relative Frobenius morphism of $\widetilde{J}(K)$, and let $\sigma(\mathfrak{p})_*$ (respectively $\sigma(\mathfrak{p})^*$) be the associated pushforward (respectively pullback) endomorphism of $\widetilde{J}(K)$. Then we have

$$\widetilde{T}(\mathfrak{p}) = \sigma(\mathfrak{p})_* + \sigma(\mathfrak{p})^*. \tag{4.19}$$

Proof. We use the formulation of the general Shimura reciprocity law from Section 3 of [Hid81]. Let $u \in \widehat{B}^\times$. Then we denote the correspondence (4.7) on $\mathrm{Sh}(K)$ induced by the double coset KuK by $C(u)$.

We claim that there is an equality

$$C((u^{\mathfrak{p}})^{-1}) = C(u^{\mathfrak{p}}). \tag{4.20}$$

Take a generator π of $\mathfrak{p}$. We have

$$K(u^{\mathfrak{p}})^{-1}K = K\pi^{-1}u^{\mathfrak{p}}K. \tag{4.21}$$

Indeed, since K contains $\widehat{\mathbf{Z}}_F^\times$, this is true outside $\mathfrak{p}$. At $\mathfrak{p}$, there exists an $F_{\mathfrak{p}}$-isomorphism $\varphi : B_{\mathfrak{p}} \to M_2(F_{\mathfrak{p}})$ for which $\varphi(K_{\mathfrak{p}}) = \mathrm{GL}_2(\mathbf{Z}_{F,\mathfrak{p}})$ and

$$\varphi(u_{\mathfrak{p}}) = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}.$$

Then one clearly has

$$\mathrm{GL}_2(\mathbf{Z}_{F,\mathfrak{p}})\varphi(u_{\mathfrak{p}})^{-1}\mathrm{GL}_2(\mathbf{Z}_{F,\mathfrak{p}}) = \mathrm{GL}_2(\mathbf{Z}_{F,\mathfrak{p}})\pi^{-1}\varphi(u_{\mathfrak{p}})\mathrm{GL}_2(\mathbf{Z}_{F,\mathfrak{p}}),$$

proving (4.21).

Since π is in the center of $B^\times$, the correspondences $C(\pi^{-1}u^{\mathfrak{p}})$ and $C(u^{\mathfrak{p}})$ are identical. This proves (4.20). Combining this equality with relation (3.4.13) in [Hid81], we get

$$^tC(\mathfrak{p}) = C(\mathfrak{p}),$$

where ^{t} denotes transposition. Here we remark that $C(\mathfrak{p})^\sigma = C(\mathfrak{p})$ in relation (3.4.13) of *loc. cit.* since both $\mathrm{Sh}(K)$ and $C(\mathfrak{p})$ are defined over F.

Let $\Phi(\mathfrak{p})$ be the Frobenius correspondence on $\widetilde{J}(K)$. Then Theorem 3.7 in [Hid81] yields

$$\widetilde{C}(\mathfrak{p}) = \Phi(\mathfrak{p}) + {}^t\Phi(\mathfrak{p}) \circ \alpha$$

for some morphism $\alpha : \widetilde{\mathrm{Sh}}(K) \to \widetilde{\mathrm{Sh}}(K)$. This can only be invariant under transposition if α is the identity morphism. Considering the endomorphisms of $\widetilde{J}(K)$ induced by both sides, one obtains the theorem. □

Now let us suppose that the hypotheses of Section 4.1.6 hold, and that K contains $\widehat{\mathbf{Z}}_F^\times$. Then by (4.11), we see that the relation (4.19) holds for all primes $\mathfrak{p} \subset \mathbf{Z}_F$. We explore the consequences of this equality for the component $J_0(K)$ of $J(K)$ under the additional hypothesis that $J_0(K)$ has genus 1.

First suppose that $\mathfrak{p}$ is trivial in the class group $\mathrm{Cl}(K\infty)$, that is, suppose that $\mathfrak{p}$ splits in the degree 2 extension F_K of F. Then $\sigma(\mathfrak{p})$ fixes the neutral component $\mathrm{Sh}_0(K)$ of $\mathrm{Sh}(K)$ by Proposition 3.1.3. On $\mathrm{Sh}_0(K)$, $\sigma(\mathfrak{p})$ induces the relative Frobenius morphism at the primes $\mathfrak{P}$ over $\mathfrak{p}$ in the extension $F_K|F$.

By Proposition 3.1.5, the traces of Frobenius $a(\mathfrak{P})$ of $J_0(K)$ at the aforementioned primes $\mathfrak{P}$ are identical. Therefore, Theorem 4.3.1 implies that the matrix $M(\mathfrak{p})$ from Algorithm 4.2.1 is scalar and that we have

$$M(\mathfrak{p}) = a(\mathfrak{P}).$$

Now suppose that $\mathfrak{p}$ is inert in the extension $F_K|F$. Let $\mathfrak{P}$ be the prime of F_K above $\mathfrak{p}$. This time, the morphism $\sigma(\mathfrak{p})$ exchanges the components of $\mathrm{Sh}(K)$. However, the morphism $\sigma(\mathfrak{p})^2$ fixes both and coincides with the relative Frobenius morphism $\sigma(\mathfrak{P})$ on these components. We have the usual recurrence relation

$$\widetilde{T}(\mathfrak{p})^2 = (\sigma(\mathfrak{p})_* + \sigma(\mathfrak{p})^*)^2 = \sigma(\mathfrak{p})_*^2 + \sigma(\mathfrak{p})^{*2} + 2q,$$

where $q = \mathrm{Nm}(\mathfrak{p})$. Hence if we denote the trace of Frobenius $\sigma(\mathfrak{P})^* + \sigma(\mathfrak{P})^*$ of $J_0(K)$ at $\mathfrak{P}$ by $a(\mathfrak{P})$, then once more Proposition 3.1.5 and Theorem 4.3.1 combine to give that $M(\mathfrak{p})^2$ is a scalar matrix, and that we have an equality

$$M(\mathfrak{p})^2 = a(\mathfrak{P}) + 2q.$$

Summarizing, we obtain the following Proposition.

Proposition 4.3.2. *Suppose that F, B and K satisfy the hypotheses at the beginning of Section 4.2, as well as the condition $\widehat{\mathbf{Z}}_F^\times \subset K$, and suppose that $J_0(K)$ has genus* 1.

Let $\mathfrak{P}$ be a prime of F_K over a prime $\mathfrak{p}$ of F at which K is maximal, and let the inertia degree of $\mathfrak{P}$ over $\mathfrak{p}$ be equal to f. Let $a(\mathfrak{P})$ be the trace of Frobenius $J_0(K)$ at $\mathfrak{P}$. Let $q = \mathrm{Nm}(\mathfrak{p})$ and let $M(\mathfrak{p})^f$ be given by the scalar m. Then we have

$$a(\mathfrak{P}) = \left\{ \begin{array}{cc} m & \text{if } f = 1 \\ m - 2q & \text{if } f = 2. \end{array} \right.$$

In Chapter 7, we will use the equalities from Proposition 4.3.2 to determine the isogeny classes of canonical models of the curves $J(\Gamma)$: the subgroups K used in this Chapter will all satisfy the extra condition $\widehat{\mathbf{Z}}_F^\times \subset K$.

Chapter 5

Uniformizations

Let B and K be as in Chapter 3. Suppose that K is maximal at a prime $\mathfrak{p}$ of F dividing the discriminant $\mathfrak{D}(B)$ of B. In [Čer76], Čerednik constructed a quotient $\mathrm{Sh}(K, \mathfrak{p})$ of the $\mathfrak{p}$-adic upper half-plane that gives a model of $\mathrm{Sh}(K)$ over $\mathbf{Z}_{F,\mathfrak{p}}$. This quotient was studied in more detail by Boutot and Zink in [BZ] (but also see [Var98]), generalizing methods developed by Drinfel'd in [Dri76].

In the first section, we describe the geometric special fiber of the model $\mathrm{Sh}(K, \mathfrak{p})$ in terms of the arithmetic of the "switched" quaternion algebra of discriminant $\mathfrak{D}(B)^f\infty/\mathfrak{p}$ over F. Moreover, we explain how to recover the geometric special fiber of the minimal model of $\mathrm{Sh}(K)$ at $\mathfrak{p}$.

The second section explores the consequences of our description for the purpose of determining the Jacobian $J_0(K)$ explicitly when it has genus 1. It turns out that knowing the special fiber of the minimal model of $\mathrm{Sh}(K)$ at the primes $\mathfrak{p}$ dividing the discriminant of B allows us to find candidate equations for $J_0(K)$ by browsing through a certain thin subset of the F_K-points of a classical modular curve $Y_0(p)$.

5.1 Dual graphs

Throughout this section, the notion of a graph is as in Definition 3-1 of [Kur79]. In particular, we allow graphs to have oriented edges equal to their own inverse. Also, by the term "model" we will mean "integral model" rather than "model over a number field" (*cf.* the discussion after Definition 3.1.2).

Let $\mathfrak{p}$ be a fixed prime of F dividing the discriminant $\mathfrak{D}(B)$ of B. Throughout this chapter, we suppose that the group $K \subseteq \widehat{B}^\times$ is of the form $K = K_\mathfrak{p} \times K^\mathfrak{p}$, where $K_\mathfrak{p}$ is the maximal compact subgroup of $B_\mathfrak{p}^\times$ and $K^\mathfrak{p} \subset \widehat{B}^{\mathfrak{p}\times}$.

Let $F_\mathfrak{p}^{\mathrm{unr}}$ be the maximal unramified extension of $F_\mathfrak{p}$ with ring of integers by $\mathbf{Z}_{F,\mathfrak{p}}^{\mathrm{unr}}$. Let π be a uniformizer of $\mathbf{Z}_{F,\mathfrak{p}}^{\mathrm{unr}}$. Given a scheme X over $\mathbf{Z}_{F,\mathfrak{p}}$, we define $\widehat{X}^{\mathrm{unr}}$ to be the base extension of formal schemes

$$\widehat{X}^{\mathrm{unr}} = \widehat{X} \times_{\mathrm{Spf}(\mathbf{Z}_{F,\mathfrak{p}})} \mathrm{Spf}(\mathbf{Z}_{F,\mathfrak{p}}^{\mathrm{unr}}),$$

where $\widehat{X}$ is the completion of X along its special fiber, and where for a $\mathbf{Z}_{F,\mathfrak{p}}$-algebra R, the formal spectrum of R is denoted by $\operatorname{Spf}(R)$.

Let $\widehat{\Omega}_{\mathfrak{p}}$ be the upper half-plane over $\mathbf{Z}_{F,\mathfrak{p}}$. It is a formal scheme over $\mathbf{Z}_{F,\mathfrak{p}}$ representing the functor defined in Section 1.5 of [BC91]. The group $\mathrm{GL}_2(F_{\mathfrak{p}})$ acts on the scheme $\widehat{\Omega}_{\mathfrak{p}}$ in a natural way, see Section 1.6 of [BC91]. This action factorizes through the adjoint group $\mathrm{PGL}_2(F_{\mathfrak{p}})$. Let

$$\widehat{\Omega}_{\mathfrak{p}}^{\mathrm{unr}} = \widehat{\Omega}_{\mathfrak{p}} \times_{\operatorname{Spf}(\mathbf{Z}_{F,\mathfrak{p}})} \operatorname{Spf}(\mathbf{Z}_{F,\mathfrak{p}}^{\mathrm{unr}}).$$

The special fiber of $\widehat{\Omega}_{\mathfrak{p}}$ consists of a tree of rational curves. As a graph with an action of $\mathrm{GL}_2(F_{\mathfrak{p}})$, the dual graph of this special fiber is isomorphic to the $\mathfrak{p}$-adic Bruhat-Tits tree, which we denote by $T_{\mathfrak{p}}$.

Let H be a quaternion algebra over F of discriminant $\mathfrak{D}(B)^f\infty/\mathfrak{p}$. That is to say, H is ramified everywhere at infinity, and its ramification behavior at the non-archimedean places is exactly the same as that of B, except at $\mathfrak{p}$, where B is ramified and H splits. Such an H exists by Theorem 2.1.2. Choosing an isomorphism of restricted direct products

$$\widehat{H}^{\mathfrak{p}} = \prod_{\substack{v \text{ finite} \\ v\neq\mathfrak{p}}}{}' H_v \cong \prod_{\substack{v \text{ finite} \\ v\neq\mathfrak{p}}}{}' B_v = \widehat{B}^{\mathfrak{p}}, \tag{5.1}$$

we obtain a left action of $\widehat{H}^{\mathfrak{p}\times}$ on $\widehat{B}^{\mathfrak{p}\times}$.

Since $K_{\mathfrak{p}}$ is the maximal compact open subgroup of $B_{\mathfrak{p}}^{\times}$, the norm map induces an isomorphism

$$B_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}} \xrightarrow{\sim} F_{\mathfrak{p}}^{\times}/\mathbf{Z}_{F,\mathfrak{p}}^{\times} \tag{5.2}$$

by Theorem 2.4.1(i) and Lemme II.1.5 in [Vig80]. The group $H_{\mathfrak{p}}^{\times}$ acts on the right side of (5.2) through its own norm map $H_{\mathfrak{p}}^{\times} \to F_{\mathfrak{p}}^{\times}$. We get a corresponding action of $H_{\mathfrak{p}}^{\times}$ on $B_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}$.

Combining the two actions above, we obtain an action of $\widehat{H}^{\times} = H_{\mathfrak{p}}^{\times} \times \widehat{H}^{\mathfrak{p}\times}$ on the quotient $\widehat{B}^{\times}/K$, whence an induced action of $H^{\times} \subset \widehat{H}^{\times}$. We can also make the group $H^{\times}$ act on $\widehat{\Omega}_{\mathfrak{p}}$, and hence on $\widehat{\Omega}_{\mathfrak{p}}^{\mathrm{unr}}$, after choosing an isomorphism of groups $H_{\mathfrak{p}}^{\times} \cong \mathrm{GL}_2(F_{\mathfrak{p}})$. The fundamental result on the $\mathfrak{p}$-adic uniformization of Shimura curves can now be stated as follows.

Theorem 5.1.1 ([BZ], Theorem 0.1)**.** *There exists a model* $\mathrm{Sh}(K,\mathfrak{p})$ *of* $\mathrm{Sh}(K)$ *over* $\mathbf{Z}_{F,\mathfrak{p}}$ *for which there is an isomorphism of formal schemes*

$$\widehat{\mathrm{Sh}}(K,\mathfrak{p})^{\mathrm{unr}} \cong H^{\times}\backslash\widehat{\Omega}_{\mathfrak{p}}^{\mathrm{unr}} \times \widehat{B}^{\times}/K. \tag{5.3}$$

We now consider the special fibers at both sides of the isomorphism (5.3). Motivated by the fact that the dual graph of the special fiber of $\widehat{\Omega}_{\mathfrak{p}}^{\mathrm{unr}}$ is the Bruhat-Tits tree $T_{\mathfrak{p}}$, we make the following

Definition 5.1.2. *The* dual graph with weights *associated to the double quotient*

$$H^\times\backslash\widehat{\Omega}^{\mathrm{unr}}_{\mathfrak{p}} \times \widehat{B}^\times/K$$

is the graph

$$G(K,\mathfrak{p}) = H^\times\backslash T_{\mathfrak{p}} \times \widehat{B}^\times/K.$$

In other words, the vertex set $V(G(K,\mathfrak{p}))$ of $G(K,\mathfrak{p})$ is given by

$$V(G(K,\mathfrak{p})) = H^\times\backslash V(T_{\mathfrak{p}}) \times \widehat{B}^\times/K$$

and its oriented edge set $OE(G(K,\mathfrak{p}))$ by

$$OE(G(K,\mathfrak{p})) = H^\times\backslash OE(T_{\mathfrak{p}}) \times \widehat{B}^\times/K.$$

The vertices and edges of this graph are weighted as follows:

(i) Given a vertex $v \in V(G(K,\mathfrak{p}))$, let $\widetilde{v}$ be a representative of v in $V(T_{\mathfrak{p}}) \times \widehat{B}^\times/K$. Consider the subgroup

$$\mathrm{PStab}(\widetilde{v}) = \mathrm{Im}(\mathrm{Stab}_{H^\times}(\widetilde{v}) \to H^{\times\mathrm{ad}})$$

of $\mathrm{P}H^\times = H^{\times\mathrm{ad}}$*. Then the weight of v is defined to be $w(v) = |\mathrm{PStab}(\widetilde{v})|$.*

(ii) Given an edge $e \in E(G(K,\mathfrak{p}))$, let $\widetilde{e}$ be an oriented edge $\widetilde{e}$ in $OE(T_{\mathfrak{p}}) \times \widehat{B}^\times/K$ representing e. The weight of e is analogously defined as $w(e) = |\mathrm{PStab}(\widetilde{e})|$.

The weights in the definition above are duly independent of the choice of $\widetilde{x}$ and $\widetilde{e}$.

Starting with a semi-stable curve over $\mathbf{Z}^{\mathrm{unr}}_{F,\mathfrak{p}}$, one can also construct a dual graph with weights. For this, we need the following notion (*cf.* Corollary 10.3.22 of [Liu02]).

Definition 5.1.3. *Let C be a semi-stable curve over $\mathbf{Z}^{\mathrm{unr}}_{F,\mathfrak{p}}$, and let P be a singular point of the special fiber of C. Then the completion of the local ring $\mathcal{O}_{C,P}$ is isomorphic to*

$$\mathbf{Z}^{\mathrm{unr}}_{F,\mathfrak{p}}[[x,y]]/(xy - \pi^w).$$

for some uniquely determined integer w. The weight *of P is then defined to be w.*

This motivates

Definition 5.1.4. *Let C be a semi-stable curve over $\mathbf{Z}^{\mathrm{unr}}_{F,\mathfrak{p}}$. The* dual graph with weights *associated to C is the dual graph of the special fiber of C. An edge e of this graph is weighted by the weight of the ordinary double point of C corresponding to e.*

Note that in this definition, the vertices of the dual graph have not been given weights. Nevertheless, we can define a notion of isomorphism:

Definition 5.1.5. *Let G and G' be graphs with weighted edges. An* isomorphism *from G to G' is an isomorphism of graphs $G \to G'$ preserving the weights of the edges.*

After these definitions, we return to the model $\widehat{\mathrm{Sh}}(K,\mathfrak{p})^{\mathrm{unr}}$. Although its special fiber is singular in general, it is still semi-stable. More precisely:

Theorem 5.1.6. *Consider the scheme* $\widehat{\mathrm{Sh}}(K,\mathfrak{p})^{\mathrm{unr}}$ *from Theorem 5.1.1.*

(i) $\widehat{\mathrm{Sh}}(K,\mathfrak{p})^{\mathrm{unr}}$ *is a normal scheme that is flat, proper and semistable over* $\mathbf{Z}_{F,\mathfrak{p}}^{\mathrm{unr}}$.

(ii) The special fiber of $\widehat{\mathrm{Sh}}(K,\mathfrak{p})^{\mathrm{unr}}$ *is reduced. Its components are rational curves, and all its singularities are ordinary double points.*
In particular, let H be a connected component of the dual graph associated to $\widehat{\mathrm{Sh}}(K,\mathfrak{p})^{\mathrm{unr}}$. *Then the (arithmetic) genus of the corresponding component of* $\widehat{\mathrm{Sh}}(K,\mathfrak{p})^{\mathrm{unr}}$ *equals the Betti number* $1+|E(H)|-|V(H)|$.

(iii) The isomorphism in Theorem 5.1.1 induces an isomorphism of the dual graph with weights associated to $\widehat{\mathrm{Sh}}(K,\mathfrak{p})^{\mathrm{unr}}$ *and* $G(K,\mathfrak{p})$.

Proof. This follows directly from Proposition 3-2 in [Kur79] by decomposing

$$H^\times\backslash\widehat{\Omega}_{\mathfrak{p}}^{\mathrm{unr}}\times\widehat{B}^\times/K=\coprod_{i=1}^{h}\Gamma_i\backslash\widehat{\Omega}_{\mathfrak{p}}^{\mathrm{unr}} \tag{5.4}$$

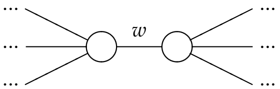
as in Proposition 3.1.1(ii). This decomposition is finite by Proposition 5.1.8(i) below. □

Remark. To simplify the statement of the theorem, we have used that the dual graph of $H^\times\backslash\widehat{\Omega}_{\mathfrak{p}}^{\mathrm{unr}}\times\widehat{B}^\times/K$ has no oriented edges equal to their own inverse: this fact will be proved in Proposition 5.1.8(v) below.

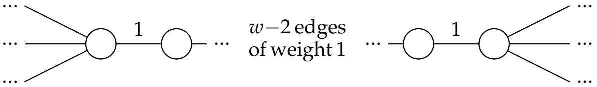
The model $\widehat{\mathrm{Sh}}(K,\mathfrak{p})^{\mathrm{unr}}$ need not be minimal. The dual graph of a minimal regular model can be constructed as follows:

Proposition 5.1.7 ([Kur79]). *Let C be a curve over* $\mathbf{Z}_{F,\mathfrak{p}}^{\mathrm{unr}}$, *and let $\widetilde{C}$ be its minimal desingularization. Suppose that the dual graph with weights of the special fiber of C contains no oriented edges equal to their own inverse.*

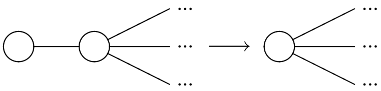
Then the dual graph of $\widetilde{C}$ can be constructed by replacing an edge of weight w by a concatenation of w edges of weight 1. *In a picture: a weighted edge*



is replaced by



From the dual graph of $\widetilde{C}$, the dual graph of the minimal model C_{min} of C can be constructed by removing vertices that belong to a unique edge, along with the edge to *which they belong, until no such vertices are left. Pictorially, one inductively repeats the process*



Proof. For the first part, one uses the explicit description of the desingularization of the scheme $\operatorname{Spec}(\mathbf{Z}_{F,\mathfrak{p}}[x,y]/(xy-\pi^m))$ as found in Example 8.3.53 of [Liu02]: also see page 288 of [Kur79]. The second part follows from Castelnuovo's criterion: see page 289 of [Kur79]. □

By the theorems and propositions above, we can reconstruct the dual graph of the minimal model of $\operatorname{Sh}(K)$ over $\mathbf{Z}_{F,\mathfrak{p}}^{\mathrm{unr}}$ as soon as we can describe the graph with weights $G(K,\mathfrak{p})$. The following proposition relates the weighted dual graph $G(K,\mathfrak{p})$ to arithmetic data of the quaternion algebra H. It is a generalization of Section 4 of [Rib90].

Proposition 5.1.8. *Consider the dual graph with weights $G(K,\mathfrak{p})$ constructed in Definition 5.1.2. This graph has the following properties:*

(i) There is a bijection between $\pi_0(G(K,\mathfrak{p}))$ and the narrow class group $\mathrm{Cl}(K\infty)$. The set $\pi_0(G(K,\mathfrak{p}))$ contains at most $T(K\infty)$ isomorphism classes of graphs.

(ii) Let K_H be a compact open subgroup of $\widehat{H}^\times$ given by $K_H = K_{H\mathfrak{p}} \times K_H^{\mathfrak{p}}$, where $K_{H\mathfrak{p}} \subset H_{\mathfrak{p}}^\times$ is maximal and $K_H^{\mathfrak{p}} \subset \widehat{H}^{\mathfrak{p}\times}$ corresponds to $K^{\mathfrak{p}}$ under the isomorphism (5.1).
Then $V(G(K,\mathfrak{p}))$ is in bijection with the disjoint union of two copies of the set $\mathrm{Pic}_r(K_H)$. An element $[\widehat{h}]$ of one of these two copies is weighted by $w([\widehat{h}]) = |\mathrm{P}(\widehat{h}K_H\widehat{h}^{-1})_H^+|$.

(iii) Let $K_H(\mathfrak{p}) = K_H(\mathfrak{p})_{\mathfrak{p}} \times K_H(\mathfrak{p})^{\mathfrak{p}}$ be a compact open subgroup of $\widehat{H}^\times$ with $K_H(\mathfrak{p})^{\mathfrak{p}} = K_H^{\mathfrak{p}}$ and $K_H(\mathfrak{p})_{\mathfrak{p}} = \mathcal{O}(\mathfrak{p})_{\mathfrak{p}}^\times$, where $\mathcal{O}(\mathfrak{p})_{\mathfrak{p}}$ is an arbitrary level $\mathfrak{p}$ suborder of the matrix order $\mathcal{O}(1)_{\mathfrak{p}}$ for which $K_{H\mathfrak{p}} = \mathcal{O}(1)_{\mathfrak{p}}^\times$.
Then $E(G(K,\mathfrak{p}))$ is in bijection with the set $\mathrm{Pic}_r(K_H(\mathfrak{p}))$. An element $[\widehat{h}]$ of this set is weighted by $w([\widehat{h}]) = |\mathrm{P}(\widehat{h}K_H(\mathfrak{p})\widehat{h}^{-1})_H^+|$.

(iv) Let $w_{\mathfrak{p}}$ be an element of $\mathcal{O}(1)(\mathfrak{p})$ such that

$$\mathcal{O}(\mathfrak{p})_{\mathfrak{p}} = \mathcal{O}(1)_{\mathfrak{p}} \cap w_{\mathfrak{p}}\mathcal{O}(1)_{\mathfrak{p}}w_{\mathfrak{p}}^{-1},$$

and let $w^{\mathfrak{p}}$ be an element of $\widehat{H}^\times$ whose component at $\mathfrak{p}$ is given by $w_{\mathfrak{p}}$ and whose components outside $\mathfrak{p}$ are trivial. Under the bijections in (ii) and (iii), the incidence relation on $G(K,\mathfrak{p})$ has the following description:
Let $e \in E(G(K,\mathfrak{p}))$ be given by the class $[\widehat{h}] \in \mathrm{Pic}_r(K_H(\mathfrak{p}))$. Then the vertices of $G(K,\mathfrak{p})$ connected by e are given by the class $[\widehat{h}]$ in the first copy of $\mathrm{Pic}_r(K_H)$ and the class $[\widehat{h}w^{\mathfrak{p}}]$ in the second copy.

(v) $G(K,\mathfrak{p})$ does not have edges whose endpoints coincide.

(vi) *Let v be a vertex of $G(K,\mathfrak{p})$, and let E_v be the set of edges containing v. Then one has the equality*
$$\sum_{e\in E_v}\frac{w(v)}{w(e)}=\mathrm{Nm}(\mathfrak{p})+1.$$

Proof. (i): This has to hold by Proposition 3.1.1(i), but we give a separate proof as a sanity check, which also gives a direct description of the set of connected components of $G(K,\mathfrak{p})$.

Since $T_{\mathfrak{p}}$ is connected and $\widehat{B}^{\times}/K$ is totally disconnected, the set of connected components of $G(K,\mathfrak{p})$ can also be described as the double quotient $H^{\times}\backslash\widehat{B}^{\times}/K$. Recall that by definition, we have the following isomorphism of groups with a left $H^{\times}$-action:
$$\widehat{B}^{\times}/K\cong F_{\mathfrak{p}}^{\times}/\mathbf{Z}_{F,\mathfrak{p}}^{\times}\times\widehat{H}^{\mathfrak{p}\times}/K_H^{\mathfrak{p}}.$$
The map
$$F_{\mathfrak{p}}^{\times}\times\widehat{H}^{\mathfrak{p}\times}\overset{\mathrm{id}\times\mathrm{nrd}}{\longrightarrow}F_{\mathfrak{p}}^{\times}\times\widehat{F}^{\mathfrak{p}\times}$$
factorizes to give a map
$$H^{\times}\backslash(F_{\mathfrak{p}}^{\times}/\mathbf{Z}_{F,\mathfrak{p}}^{\times}\times\widehat{H}^{\mathfrak{p}\times}/K_H^{\mathfrak{p}})\longrightarrow F^{+}\backslash(F_{\mathfrak{p}}^{\times}/\mathbf{Z}_{F,\mathfrak{p}}^{\times}\times\widehat{F}^{\mathfrak{p}\times}/\mathrm{nrd}(K_H)^{\mathfrak{p}})=\mathrm{Cl}(K\infty).$$
Since $\mathrm{nrd}(H^{\times})=F^{+}$ by Theorem 2.4.1(ii), we can apply strong approximation (Theorem 2.5.1) to conclude that this map is a bijection.

Indeed, let $(x_{\mathfrak{p}},\widehat{x}^{\mathfrak{p}})$ represent a class in $F^{+}\backslash(F_{\mathfrak{p}}^{\times}/\mathbf{Z}_{F,\mathfrak{p}}^{\times}\times\widehat{F}^{\mathfrak{p}\times}/\mathrm{nrd}(K)^{\mathfrak{p}})$. Because of Theorem 2.4.1(i), the fiber above $[(x_{\mathfrak{p}},\widehat{x}^{\mathfrak{p}})]$ is non-empty. Let $(h_{\mathfrak{p}},\widetilde{h}^{\mathfrak{p}})$ be a representative of an element of this fiber. Then the equality $\mathrm{nrd}(H^{\times})=F^{+}$ from Theorem 2.4.1(ii) implies that the complete fiber above $[(h_{\mathfrak{p}},h^{\mathfrak{p}})]$ is given by the image of $\{h_{\mathfrak{p}}\}\times\widehat{H}^{1\mathfrak{p}}x^{\mathfrak{p}}$ in the double quotient $H^{\times}\backslash(F_{\mathfrak{p}}^{\times}/\mathbf{Z}_{F,\mathfrak{p}}^{\times}\times\widehat{H}^{\mathfrak{p}\times}/K_H^{\mathfrak{p}})$.

Since the algebra H splits at the finite place $\mathfrak{p}$, Corollary 2.5.2(ii) implies that $H^1\widehat{H}_{\mathfrak{p}}^1$ is dense in $\widehat{H}^1$. This is the same as saying that H^1 is dense in $\widehat{H}^{\mathfrak{p}1}$. Since $K_H^{\mathfrak{p}}$ is open in $\widehat{H}^{\mathfrak{p}}$, so is $K_H^{\mathfrak{p}1}$ in $\widehat{H}^{\mathfrak{p}1}$. Therefore the quotient $H^1\backslash\widehat{H}^{\mathfrak{p}1}h^{\mathfrak{p}}/K_H^{\mathfrak{p}1}$, and hence the image of $\{h_{\mathfrak{p}}\}\times\widehat{H}^{\mathfrak{p}1}h^{\mathfrak{p}}$ in $H^{\times}\backslash(F_{\mathfrak{p}}^{\times}/\mathbf{Z}_{F,\mathfrak{p}}^{\times}\times\widehat{H}^{\mathfrak{p}\times}/K_H^{\mathfrak{p}})$, is reduced to one element. This completes the proof of the first part of (i); the second part is analogous to Proposition 3.1.1(iii).

(ii): As a set with a left $H_{\mathfrak{p}}^{\times}$-action, we have an isomorphism
$$V(T_{\mathfrak{p}})\cong H_{\mathfrak{p}}^{\times}/F_{\mathfrak{p}}^{\times}K_{H\mathfrak{p}}.\tag{5.5}$$
Therefore
$$V(G(K,\mathfrak{p}))\cong H^{\times}\backslash(H_{\mathfrak{p}}^{\times}/F_{\mathfrak{p}}^{\times}K_{H\mathfrak{p}}\times F_{\mathfrak{p}}^{\times}/\mathbf{Z}_{F,\mathfrak{p}}^{\times}\times\widehat{H}^{\mathfrak{p}\times}/K^{H\mathfrak{p}}).\tag{5.6}$$
The map
$$\begin{aligned}\widehat{H}^{\times}/K_H=H_{\mathfrak{p}}^{\times}/K_{H\mathfrak{p}}\times\widehat{H}^{\mathfrak{p}\times}/K_H^{\mathfrak{p}}&\longrightarrow H_{\mathfrak{p}}^{\times}/F_{\mathfrak{p}}^{\times}K_{H\mathfrak{p}}\times F_{\mathfrak{p}}^{\times}/\mathbf{Z}_{F,\mathfrak{p}}^{\times}\times\widehat{H}^{\mathfrak{p}\times}/K_H^{\mathfrak{p}}\\ [h_{\mathfrak{p}},h^{\mathfrak{p}}]&\longmapsto[h_{\mathfrak{p}},\mathrm{nrd}(h_{\mathfrak{p}}),h^{\mathfrak{p}}]\end{aligned}$$

is $H^\times$-equivariant and injective. Its image is given by the classes $[h_\mathfrak{p}, x_\mathfrak{p}, h^\mathfrak{p}]$ for which $v(\mathrm{nrd}(h_\mathfrak{p})) \equiv v(x_\mathfrak{p}) \pmod 2$.

Let $w_\mathfrak{p}$ be as in part (iv) of the proposition. Then combining the map above with the similar map

$$\begin{aligned} \widehat{H}^\times/K_H = H_\mathfrak{p}^\times/K_{H\mathfrak{p}} \times \widehat{H}^{\mathfrak{p}\times}/K_H^\mathfrak{p} &\longrightarrow H_\mathfrak{p}^\times/F_\mathfrak{p}^\times K_{H\mathfrak{p}} \times F_\mathfrak{p}^\times/\mathbf{Z}_{F,\mathfrak{p}}^\times \times \widehat{H}^{\mathfrak{p}\times}/K_H^\mathfrak{p} \\ [h_\mathfrak{p}, h^\mathfrak{p}] &\longmapsto [h_\mathfrak{p}, \mathrm{nrd}(w_\mathfrak{p})^{-1}\mathrm{nrd}(h_\mathfrak{p}), h^\mathfrak{p}] \end{aligned}$$

whose image is given by the classes $[h_\mathfrak{p}, x_\mathfrak{p}, h^\mathfrak{p}]$ for which $v(\mathrm{nrd}(h_\mathfrak{p})) \equiv v(x_\mathfrak{p}) + 1 \pmod 2$, one obtains, upon modding out $H^\times$, an isomorphism

$$\coprod_{i=1}^{2} (H^\times\backslash\widehat{H}^\times/K_H) \xrightarrow{\sim} H^\times\backslash(H_\mathfrak{p}^\times/F_\mathfrak{p}^\times K_{H\mathfrak{p}} \times F_\mathfrak{p}^\times/\mathbf{Z}_{F,\mathfrak{p}}^\times \times \widehat{H}^{\mathfrak{p}\times}/K_H^\mathfrak{p}). \tag{5.7}$$

Under this string of isomorphisms, the weight of a vertex in $V(G(K,\mathfrak{p}))$ corresponding to an element $[\widehat{h}]$ of a copy of $H^\times\backslash\widehat{H}^\times/K_H = \mathrm{Pic}_r(K_H(\mathfrak{p}))$ is exactly the cardinality of the adjoint group of the left stabilizer of $\widehat{h}K_H \in \widehat{H}^\times/K_H$. Rewriting this, one ends up with (ii). The choice of maximal compact subgroup $K_{H\mathfrak{p}}$ is irrelevant, as it corresponds to a change of base point on $T_\mathfrak{p}$.

(iii): There is an isomorphism of sets with a left $H_\mathfrak{p}^\times$-action

$$E(T_\mathfrak{p}) \cong H_\mathfrak{p}^\times/N_{B_\mathfrak{p}^\times}(K_H(\mathfrak{p})_\mathfrak{p}). \tag{5.8}$$

One now essentially repeats the argument in (ii). We end up with a single copy of $H^\times\backslash\widehat{H}^\times/K_H(\mathfrak{p})_\mathfrak{p} = \mathrm{Pic}_r(K_H)$ because the reduced norm map

$$\mathrm{nrd} : N_{B_\mathfrak{p}^\times}(K_H(\mathfrak{p})_\mathfrak{p}) \longrightarrow \mathbf{Z}_{F,\mathfrak{p}}^\times$$

surjects (*cf.* Proposition 2.6.2(i)). That the resulting weighted edge set does not depend on the choice of $K_H(\mathfrak{p})_\mathfrak{p}$ is also proved as in (ii).

(iv) Under the isomorphisms (5.5) and (5.8) in (ii) and (iii), an edge of $T_\mathfrak{p}$ represented by an element $[h_\mathfrak{p}]$ of $H_\mathfrak{p}^\times/F_\mathfrak{p}^\times N_{B_\mathfrak{p}^\times}(K_H(\mathfrak{p})_\mathfrak{p})$ connects the pair of vertices of $T_\mathfrak{p}$ represented by the classes $[h_\mathfrak{p}]$ and $[h_\mathfrak{p} w_\mathfrak{p}]$ in $H_\mathfrak{p}^\times/F_\mathfrak{p}^\times K_{H\mathfrak{p}}$.

So let $[\widehat{h}] = [h_\mathfrak{p}, h^\mathfrak{p}]$ be an element of $H^\times\backslash\widehat{H}^\times/K_H(\mathfrak{p})$. This gives rise to the edge $[h_\mathfrak{p}, \mathrm{nrd}(h_\mathfrak{p}), h^\mathfrak{p}] \in E(G(K,\mathfrak{p}))$. If we choose our isomorphisms as above, this edge connects the vertices $[h_\mathfrak{p}, \mathrm{nrd}(h_\mathfrak{p}), h^\mathfrak{p}]$ and $[h_\mathfrak{p} w_\mathfrak{p}, \mathrm{nrd}(h_\mathfrak{p}), h^\mathfrak{p}]$ in $V(G(K,\mathfrak{p}))$. Under the bijection in (ii), the former vertex is represented by the class $[\widehat{h}]$ in the first copy of $H^\times\backslash\widehat{H}^\times/K_H$, while the latter corresponds to the class $[\widehat{h}w^\mathfrak{p}]$ in the second.

(v): Given a vertex of $G(K,\mathfrak{p})$, let $[h_\mathfrak{p}, x_\mathfrak{p}, h^\mathfrak{p}]$ be the element corresponding to it under the isomorphism (5.6). Any neighboring vertex is then represented by an element $[h'_\mathfrak{p}, x_\mathfrak{p}, h^\mathfrak{p}]$ for which $v(\mathrm{nrd}(h'_\mathfrak{p})) \neq v(\mathrm{nrd}(h_\mathfrak{p})) \pmod 2$. Therefore the two vertices are on different sides in the decomposition on the left hand side of (5.7). This proves (v).

(vi): Once more, we decompose

$$G(K,\mathfrak{p}) = \coprod_{i=1}^{h} \Gamma_i\backslash T_\mathfrak{p}$$

as in (5.4). This part of the proposition then follows from generalities on group actions on $T_{\mathfrak{p}}$. We give a proof for completeness' sake.

Let Γ be a group acting on $T_{\mathfrak{p}}$. Let v be a vertex of $\Gamma\backslash T_{\mathfrak{p}}$ lifting to a vertex $\widetilde{v}$ of $T_{\mathfrak{p}}$. There are $\mathrm{Nm}(\mathfrak{p})+1$ oriented edges of $T_{\mathfrak{p}}$ starting at $\widetilde{v}$: call the set of these oriented edges S. The stabilizer $\mathrm{Stab}_\Gamma(\widetilde{v})$ acts on S, and the oriented edges of $\Gamma\backslash T_{\mathfrak{p}}$ starting at v correspond to the $\mathrm{Stab}_\Gamma(\widetilde{v})$-orbits of S. Choosing representatives $\widetilde{e}$ for these orbits, one therefore has

$$S = \coprod_{[\widetilde{e}]\in E_v} \mathrm{Stab}_\Gamma(\widetilde{v})/\mathrm{Stab}_\Gamma(\widetilde{e})$$

hence

$$\mathrm{Nm}(\mathfrak{p})+1 = |S| = \sum_{[\widetilde{e}]\in E_v} |\mathrm{Stab}_\Gamma(\widetilde{v})/\mathrm{Stab}_\Gamma(\widetilde{e})|.$$

But one obviously has

$$|\mathrm{Stab}_\Gamma(\widetilde{v})/\mathrm{Stab}_\Gamma(\widetilde{e})| = w(v)/w(e). \qquad \square$$

We now make this description even more explicit for the particularly simple compact open subgroups that we shall be using in Chapter 7. First we consider the case where K comes from an order of B:

Proposition 5.1.9. *Let $\mathcal{O}$ be an order of B, and let $K=\widehat{\mathcal{O}}^\times$. Suppose that $\widehat{\mathcal{O}} = \mathcal{O}_{\mathfrak{p}} \times \widehat{\mathcal{O}}_{\mathfrak{p}}$, where $\widehat{\mathcal{O}}^{\mathfrak{p}} \subset \widehat{B}^{\mathfrak{p}}$ and where $\mathcal{O}_{\mathfrak{p}} \subset B_{\mathfrak{p}}$ is maximal at $\mathfrak{p}$. Let $\mathcal{O}_H$ be an order of H for which $\widehat{\mathcal{O}}_H = \mathcal{O}_{H\mathfrak{p}} \times \widehat{\mathcal{O}}_H^{\mathfrak{p}}$, where $\mathcal{O}_{H\mathfrak{p}}$ is a maximal order of $H_{\mathfrak{p}}$ and where $\widehat{\mathcal{O}}_H^{\mathfrak{p}}$ corresponds to $\widehat{\mathcal{O}}^{\mathfrak{p}}$ under the isomorphism chosen in (5.1).*

(i) The vertex set $V(G(K,\mathfrak{p}))$ is in bijection with two copies of $\mathrm{Pic}_r(\mathcal{O}_H)$. An element $[I]$ of one of these copies is weighted by $w([I]) = |\mathcal{O}_l(I)^\times/\mathbf{Z}_F^\times|$.

(ii) Let $\mathcal{O}_H(\mathfrak{p})$ be a level $\mathfrak{p}$ suborder of $\mathcal{O}_H$. The edge set $E(G(K,\mathfrak{p}))$ is in bijection with $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$. An element $[I(\mathfrak{p})]$ of this set is weighted by $w([I(\mathfrak{p})]) = |\mathcal{O}_l(I(\mathfrak{p}))^\times/\mathbf{Z}_F^\times|$.

(iii) There exists a unique order $\mathcal{O}'_H$ of H such that $\mathcal{O}_H(\mathfrak{p}) = \mathcal{O}_H \cap \mathcal{O}'_H$. There exists a (unique) ideal $I_0 \subset \mathcal{O}_H$ of level $\mathfrak{p}^2$ such that $\mathcal{O}_l(I_0) = \mathcal{O}'_H$ and $\mathcal{O}_r(I_0) = \mathcal{O}_H$. Under the bijections in (i) and (ii), the incidence relation on $G(K,\mathfrak{p})$ has the following description:
Let $e \in E(G(K,\mathfrak{p}))$ be represented by the ideal class $[I(\mathfrak{p})] \in \mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$. Then the edge e connects the vertex of $G(K,\mathfrak{p})$ given by the ideal class $[I(\mathfrak{p})\mathcal{O}_H]$ in the first copy of $\mathrm{Pic}_r(\mathcal{O}_H)$ with the ideal class $[I(\mathfrak{p})I_0]$ in the second.

Proof. Using the notation of Proposition 5.1.9, we have $K_H = \widehat{\mathcal{O}}_H^\times$ and $K_H(\mathfrak{p}) = \widehat{\mathcal{O}}_H(\mathfrak{p})^\times$. The description of the vertex and edge sets in (i) and (ii) is therefore a consequence of this proposition and Corollary 2.1.5(ii). As for the weights, this is a consequence of Corollary 2.1.5(iii).

It remains to prove (iii). The existence and uniqueness of $\mathcal{O}'_H$ follow from Proposition 2.2.2(iii). Adèlically, we have $\widehat{\mathcal{O}}'_H = w^{\mathfrak{p}}\widehat{\mathcal{O}}_H(w^{\mathfrak{p}})^{-1}$, where $w^{\mathfrak{p}}$ is as in part (iv) of Proposition 5.1.9. The ideal I_0 equals $H \cap w^{\mathfrak{p}} \widehat{\mathcal{O}}_H$ by the local-global correspondence (Theorem 2.1.4). Proposition 5.1.8(iv) then allows us to conclude.

Indeed, suppose that the right $\mathcal{O}_H$-ideal class $[I(\mathfrak{p})]$ correspond to the class $[\widehat{h}] \in H^\times \backslash \widehat{H}^\times / K_H(\mathfrak{p})$ under the association in Corollary 2.1.5. Then the class $[\widehat{h}] \in H^\times \backslash \widehat{H}^\times / K_H$ represents the right $\mathcal{O}_H$-ideal class $[H \cap \widehat{h}\widehat{\mathcal{O}}_H] = [I(\mathfrak{p})\mathcal{O}_H]$. Also, we have

$$[\widehat{h} w^{\mathfrak{p}} K_H] = [\widehat{h} w^{\mathfrak{p}} K_H (w^{\mathfrak{p}})^{-1} w^{\mathfrak{p}} K_H].$$

Hence the class $[\widehat{h} w^{\mathfrak{p}}] \in H^\times \backslash \widehat{H}^\times / K_H$ corresponds to the the right $\mathcal{O}_H$-ideal class

$$[(H \cap \widehat{h} w^{\mathfrak{p}} \widehat{\mathcal{O}}_H (w^{\mathfrak{p}})^{-1})(H \cap w^{\mathfrak{p}} \widehat{\mathcal{O}}_H^\times)] = [I(\mathfrak{p})\mathcal{O}'_H I_0] = [I(\mathfrak{p}) I_0].$$

This finishes the proof. □

Remark. Without going into detail, let us mention that in light of the proposition above, the dual graph $G(K, \mathfrak{p})$ can be explicitly constructed if $K = \mathcal{O}(\mathfrak{N})$ is an Eichler order, due to the considerable functionality in `Magma` for ideal class groups of Eichler orders developed by Kirschmer and Voight in [KV10].

Before starting on the second case, we consider the groups K coming from Eichler orders a bit more thoroughly. Recall the definition of the Atkin-Lehner automorphisms $w(\mathfrak{a})$ in the discussion following Proposition 3.1.1. Though we shall never have need of this in Chapter 7, we now give a description of the action of these automorphisms on $G(K, \mathfrak{p})$, which generalizes the more ad hoc description in [Kur79] for the case $F = \mathbf{Q}$.

Let W be a subgroup of the group of Atkin-Lehner automorphisms. The resulting weighted quotient graph $G(K, \mathfrak{p})/W$ may have edges whose endpoints coincide. Therefore we should give a description of the oriented edge set $OE(G(K, \mathfrak{p}))$ as well, so as to be able to detect oriented edges of $G(K, \mathfrak{p})/W$ that equal their own inverse, which is essential for the application of Proposition 3-2 of [Kur79] to the graph $G(K, \mathfrak{p})/W$. Note that this issue did not arise for the graphs $G(K, \mathfrak{p})$ because of Proposition 5.1.8(v).

So let $K = \widehat{\mathcal{O}}^\times$ be given by the adèlic units of an Eichler order $\mathcal{O}$, and let $\mathcal{O}_H$, $\mathcal{O}_H(\mathfrak{p})$ and I_0 be as in Proposition 5.1.9. As in the proof of Proposition 5.1.8(ii), one shows that combining the factorizations of the maps

$$\begin{aligned} \widehat{H}^\times / K_H(\mathfrak{p}) &\longrightarrow H_{\mathfrak{p}}^\times / F_{\mathfrak{p}}^\times K_H(\mathfrak{p})_{\mathfrak{p}} \times F_{\mathfrak{p}}^\times / \mathbf{Z}_{F,\mathfrak{p}}^\times \times \widehat{H}^{\mathfrak{p}\times} / K_H(\mathfrak{p})^{\mathfrak{p}} \\ [h_{\mathfrak{p}}, h^{\mathfrak{p}}] &\longmapsto [h_{\mathfrak{p}}, \mathrm{nrd}(h_{\mathfrak{p}}), h^{\mathfrak{p}}] \end{aligned}$$

and

$$\begin{aligned} \widehat{H}^\times / K_H(\mathfrak{p}) &\longrightarrow H_{\mathfrak{p}}^\times / F_{\mathfrak{p}}^\times K_H(\mathfrak{p})_{\mathfrak{p}} \times F_{\mathfrak{p}}^\times / \mathbf{Z}_{F,\mathfrak{p}}^\times \times \widehat{H}^{\mathfrak{p}\times} / K_H(\mathfrak{p})^{\mathfrak{p}} \\ [h_{\mathfrak{p}}, h^{\mathfrak{p}}] &\longmapsto [h_{\mathfrak{p}} w_{\mathfrak{p}}, \mathrm{nrd}(h_{\mathfrak{p}}), h^{\mathfrak{p}}] \end{aligned}$$

yields a bijection between $OE(G(K, \mathfrak{p}))$ and the disjoint union of two copies of $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$. An element $[I(\mathfrak{p})]$ of the first copy of $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$ corresponds to the oriented edge starting at the class $[I(\mathfrak{p})\mathcal{O}_H]$ in the first copy of $\mathrm{Pic}_r(\mathcal{O}_H)$ and terminating at the class $[I(\mathfrak{p})I_0]$ in the second, while the class $[I(\mathfrak{p})]$ in the second copy of $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$ corresponds to the inverse of this oriented edge.

Having made this incidence relation explicit, it suffices to describe the action of the Atkin-Lehner automorphisms on $OE(G(K,\mathfrak{p}))$, which in turn reduces to describing the action of the automorphisms $w(\mathfrak{q})$ for prime ideals $\mathfrak{q}$. We have the following

Proposition 5.1.10. *Let $K = \widehat{\mathcal{O}}^\times$, where $\mathcal{O}$ is a level $\mathfrak{N}$ Eichler order of B, and let the corresponding Eichler orders $\mathcal{O}_H$ and $\mathcal{O}_H(\mathfrak{p})$ of H be as in Proposition 5.1.9.*

Let $\mathfrak{q}$ be a prime dividing $\mathfrak{p}\mathfrak{N}$. Then the action of the Atkin-Lehner automorphism $w(\mathfrak{q})$ on the oriented edge set $OE(G(K,\mathfrak{p}))$ of $G(K,\mathfrak{p})$ is as follows.

- *(i) Let $\mathfrak{q}|\mathfrak{N}$. Then there exists a (unique) two-sided $\mathcal{O}_H(\mathfrak{p})$-ideal $I_0(\mathfrak{q}) \subset \mathcal{O}_H(\mathfrak{p})$ of level $\mathfrak{q}^2$. The automorphism $w(\mathfrak{q})$ sends an oriented edge $[I(\mathfrak{p})]$ in a copy of $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$ to the oriented edge $[I(\mathfrak{p})I_0(\mathfrak{q})]$ in the same copy.*
- *(ii) Let $\mathfrak{q} = \mathfrak{p}$. Then there exists a (unique) two-sided $\mathcal{O}_H(\mathfrak{p})$-ideal $I_0(\mathfrak{p}) \subset \mathcal{O}_H(\mathfrak{p})$ of level $\mathfrak{p}^2$. The automorphism $w(\mathfrak{p})$ sends an oriented edge $[I(\mathfrak{p})]$ in a copy of $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$ to the oriented edge $[I(\mathfrak{p})I_0(\mathfrak{p})]$ in the other copy.*

Finally, let W be a subgroup of the group of Atkin-Lehner automorphisms, and let $\overline{G}(K,\mathfrak{p}) = G(K,\mathfrak{p})/W$ be the corresponding weighted quotient graph of $G(K,\mathfrak{p})$. Given a vertex or oriented edge $\overline{x}$ of $\overline{G}(K,\mathfrak{p})$ represented by a vertex or oriented edge x of $G(K,\mathfrak{p})$, we have $w(\overline{x}) = |\mathrm{Stab}_W(x)|w(x)$.

Proof. (i): The automorphism $w(\mathfrak{q})$ of $G(K,\mathfrak{p})$ is the factorization of the bijection

$$\begin{aligned} T_\mathfrak{p} \times \widehat{B}^\times/K &\longrightarrow T_\mathfrak{p} \times \widehat{B}^\times/K \\ (t,\widehat{b}) &\longmapsto (t,\widehat{b}n_B^\mathfrak{q}), \end{aligned}$$

where $n_B^\mathfrak{q}$ is as in the discussion after Proposition 3.1.1. Let $n^\mathfrak{q}$ be an element of $\widehat{\mathcal{O}}_H$ whose component at $\mathfrak{p}$ is trivial and whose components outside $\mathfrak{p}$ correspond to the components of $n_B^\mathfrak{q}$ under (5.1). Then under the isomorphism of $H^\times$-sets

$$\widehat{B}^\times/K \cong F_\mathfrak{p}^\times/\mathbf{Z}_{F,\mathfrak{p}}^\times \times \widehat{H}^{\mathfrak{p}\times}/K_H^\mathfrak{p},$$

right multiplication by $n_B^\mathfrak{q}$ on the left hand side corresponds to right multiplication by $n^\mathfrak{q}$ on the right hand side. We let $I_0(\mathfrak{q})$ be the two-sided $\widehat{\mathcal{O}}_H(\mathfrak{p})$-ideal $H \cap n^\mathfrak{q}\widehat{\mathcal{O}}_H(\mathfrak{p})$.

Right multiplication by $n^\mathfrak{q}$ does not interchange the copies of $\mathrm{Pic}_r(\mathcal{O}_H)$ constituting $OE(G(K,\mathfrak{p}))$ since the norm of $n^\mathfrak{q}$ is trivial at $\mathfrak{p}$. Let $[I(\mathfrak{p})]$ be an element of a copy of $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$ that is represented by $\widehat{h} \in \widehat{H}^\times$. Tracing through our bijections, we see that $n(\mathfrak{q})$ sends $[I(\mathfrak{p})]$ to the ideal class in the same copy corresponding to the adèlic element $\widehat{hn^\mathfrak{q}}$. But since $n^\mathfrak{q}$ normalizes $\widehat{\mathcal{O}}_H(\mathfrak{p})^\times$, Proposition 2.1.4 gives

$$H \cap \widehat{h}n^\mathfrak{q}\widehat{\mathcal{O}}_H(\mathfrak{p}) = (H \cap \widehat{h}\widehat{\mathcal{O}}_H(\mathfrak{p}))(H \cap n^\mathfrak{q}\widehat{\mathcal{O}}_H(\mathfrak{p})) = I(\mathfrak{p})I_0(\mathfrak{q}).$$

(ii): This time we can take $n^{\mathfrak{p}}$ to be as in Proposition 5.1.8(iv). The corresponding two-sided ideal $I_0(\mathfrak{p})$ is given by $H \cap n^{\mathfrak{p}} \widehat{\mathcal{O}}_H(\mathfrak{p})$.

Let $\widehat{h}$ be an element of H giving rise to an ideal class $[I(\mathfrak{p})]$ in the first copy of $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$. Under the chosen bijections, it corresponds with the element $[h_{\mathfrak{p}}, \mathrm{nrd}(h_{\mathfrak{p}}), h^{\mathfrak{p}}]$ of $H_{\mathfrak{p}}^{\times}/F_{\mathfrak{p}}^{\times} K_H(\mathfrak{p})_{\mathfrak{p}} \times F_{\mathfrak{p}}^{\times}/\mathbf{Z}_{F,\mathfrak{p}}^{\times} \times \widehat{H}^{\mathfrak{p}\times}/K_H(\mathfrak{p})^{\mathfrak{p}}$. The automorphism $w(\mathfrak{p})$ sends this element to

$$[h_{\mathfrak{p}}, \mathrm{nrd}(h_{\mathfrak{p}})\mathrm{nrd}(n_{\mathfrak{p}}), h^{\mathfrak{p}}] = [(h_{\mathfrak{p}} n_{\mathfrak{p}}) n_{\mathfrak{p}}, \mathrm{nrd}(h_{\mathfrak{p}} n_{\mathfrak{p}}), h^{\mathfrak{p}}].$$

This is the image of the element $\widehat{h}n^{\mathfrak{p}}$ in the second copy of $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$. Arguing as in (i), one shows that it corresponds to the ideal class $[I(\mathfrak{p})I_0(\mathfrak{p})]$ in $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$. The proof for the second copy of $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}))$ is analogous.

The final statement of the proposition is a straightforward consequence of the definitions: *cf.* the proof of Proposition 5.1.8(vi). □

Returning to our main line of argument, we now give some properties of the graph $G(K', \mathfrak{p})$, where K' is as in (3.20):

Proposition 5.1.11. *Let $\mathcal{O}$ be an order of B, and let $K = \widehat{\mathcal{O}}^{\times}$. Let $N = \mathrm{nrd}(\widehat{\mathcal{O}})$, choose N' as in Lemma 3.2.3, and consider $K' = \widehat{\mathcal{O}}^{\times} \cap \mathrm{nrd}^{-1}(N')$.*

Suppose that K' is maximal at $\mathfrak{p}$, that is, suppose that $\mathcal{O}$ and N' are maximal at $\mathfrak{p}$. Then we have:

(i) The fiber of the canonical projection map $V(G(K', \mathfrak{p})) \to V(G(K, \mathfrak{p}))$ above a vertex v of $G(K, \mathfrak{p})$ corresponding to a right $\mathcal{O}_H$-ideal I consists of n/m vertices of weight $w(v)/m$, where

$$n = |N/N'| = |(\mathbf{Z}_F^{+} \cap N)/\mathbf{Z}_F^{\times 2}|$$

and

$$m = |\mathrm{nrd}(\mathcal{O}_l(I)^{\times})/\mathbf{Z}_F^{\times 2}|.$$

(ii) A similar statement holds for the edge set.

The dual graph with weights associated to $\mathrm{Sh}(K', \mathfrak{p})$ is independent of the choice of N'.

Proof. We prove (i): naturally, the proof of (ii) is similar. Let $\widehat{h}K$ be a right coset representing the ideal I. The fiber in question is given by the image of $\widehat{h}K$ in the double quotient $\mathrm{Pic}_r(K') = H^{\times} \backslash \widehat{H}^{\times}/K'$.

The left stabilizer of the subset hK of $\widehat{H}^{\times}/K'$ is still given by $\mathcal{O}_l(I)^{\times}$. We have to determine the action of this stabilizer on the individual elements of the decomposition

$$\widehat{h}K = \coprod_{[k] \in K/K'} \widehat{h}K'k.$$

By Lemma 3.2.3, there are canonical isomorphisms

$$(\mathbf{Z}_F^{+} \cap N)/\mathbf{Z}_F^{\times 2} = (\mathbf{Z}_F^{+} \cap N)/(\mathbf{Z}_F^{+} \cap N') \xrightarrow{\sim} N/N' \xleftarrow{\sim} K/K'. \tag{5.9}$$

which respect the natural left actions of the elements of $\mathcal{O}_l(I)^\times$. Now N/N' is abelian group, and in fact an $\mathcal{O}_l(I)^\times$-module. Considering (5.9), we can therefore conclude the argument by remarking that an element $[h]$ of $\mathcal{O}_l(I)^\times$ fixes the coset $\mathrm{nrd}(\widehat{h})N'$ if and only if $\mathrm{nrd}(h) \in \mathbf{Z}_F^{\times 2}$.

The final statement of the proposition follows from the fact that as in Proposition 3.2.4, the conjugacy classes of the groups Γ_i in the decomposition (5.4) are independent of the choice of N'. □

The incidence relation on the dual graph $G(K', \mathfrak{p})$ seems to be harder to describe globally. Fortunately, in all the cases that we considered in Chapter 7, the graph $G(K', \mathfrak{p})$ could be reconstructed from $G(K, \mathfrak{p})$ using Proposition 5.1.11 and the demands furnished by parts (i), (iv) and (v) of Proposition 5.1.8.

Returning to general compact open subgroups K, let $\overline{G}(K, \mathfrak{p})$ be the dual graph with weights obtained from $G(K, \mathfrak{p})$ by inductively removing the vertices that belong to a unique edge, along with the edge to which they belong, as in Proposition 5.1.7. In the case that $\mathrm{Sh}_0(K)$ has genus 1, the results above take the following explicit form:

Proposition 5.1.12. *Let $\overline{H}_0$ be a connected component of $\overline{G}(K, \mathfrak{p})$. Suppose that $\overline{H}_0$ has genus 1. Then*

(i) All components of $\mathrm{Sh}(K)$ over F_K have genus 1;

(ii) The Jacobian $J_0(K)$ has multiplicative reduction at the primes of F_K above $\mathfrak{p}$;

(iii) Denoting by the primes of F_K over $\mathfrak{p}$ by $\mathfrak{P}$, we have an equality of sets

$$\{v_{\mathfrak{P}}(j(J_0(K))) : \mathfrak{P}|\mathfrak{p}\} = \left\{ -\sum_{e \in E(\overline{H})} w(e) : \overline{H} \in \pi_0(\overline{G}(K, \mathfrak{p})) \right\}.$$

Proof. (i) This follows from Theorem 5.1.6(ii) and the transitivity of the Galois action in Proposition 3.1.3.

(ii): By Theorem 5.1.6(ii), the geometric special fiber of $J_0(K)$ consists of rational curves intersecting in ordinary double points: this implies (ii) by the Néron-Kodaira classification (see Section 10.2 of [Liu02]).

(iii): By maximality of K at $\mathfrak{p}$, the extension $F_K|F$ is unramified at $\mathfrak{p}$. Using the transitivity of the Galois action, we can therefore obtain (iii) from (ii) by applying Tate's algorithm to the Jacobians of the curves in the decomposition (3.6). □

5.2 Searching $Y_0(p)$

In this section, we indicate how one can combine the results above with Algorithm 4.2.1 to find a conjectural equation for $J_0(K)$ by using the classical modular curves $Y_0(N)$. Our approach is much indebted to the method used by Dembélé and Donnelly in [DD08], with the important difference that we use the extra information on the valuations of $j(J_0(K))$ coming from the $\mathfrak{p}$-adic uniformization to narrow down the range of our search considerably.

Suppose that we have at our disposal the following explicit data regarding an elliptic curve E over a number field F:

Data:

(i) The primes M of bad reduction of E;

(ii) A subset S of the primes of multiplicative reduction of E, along with a list W of valuations of $j(E)$ at these primes;

(iii) The traces of Frobenius of E at a finite set P of primes of F.

For $E = J_0(K)$, M can be determined using Theorem 3.1.6, S and W by using the results from the previous section, and the traces at (iii) by Algorithm 4.2.1. Our goal is to find an explicit equation agreeing with the Data above, giving rise to a candidate equation for E (which may or may not be uniquely determined by the Data). For this, we formulate the following

Algorithm 5.2.1. *Let E be an elliptic curve over a number field F for which the Data above are available. The following pseudo-code describes how to obtain a list L of candidate equations for E.*

1. *Find a (large) integer N dividing the point counts* $\mathrm{Nm}(\mathfrak{p}) + 1 - a_{\mathfrak{p}}$ *for all $\mathfrak{p}$ in P.*

2. *Construct a large subset R of F-points on a model of the classical modular curve $Y_0(N)$.*

3. *Set $L = \emptyset$. Choose a point $x \in R$.*

4. *Determine an elliptic curve E_x over F corresponding to x.*

5. *Determine the finite list T of F-twists of E_x whose reduction is good outside M.*

6. *Add to L the equations of those elements of T that are not yet in L and agree with the rest of the Data above.*

7. *Choose a new point $x \in R$ and return to step 4. Repeat until all points in R have been treated.*

8. *If L is non-empty, return it; otherwise, enlarge R and/or decrease N and return to step 3.*

As in [DD08], the rationale for this pseudo-code is the following. Since N divides all the point counts in (i), it is reasonable to suspect that E has an N-isogeny. Hence E should give rise to an F-point x of $Y_0(N)$. Conversely, E can be recovered from x by taking an appropriate F-twist in the geometric isomorphism class corresponding to x. Parts (i) and (ii) of the Data impose restrictions on the point x, while part (iii) thins out the list of F-twists.

We now discuss the implementation of the algorithm above. In the cases in Chapter 7, we restricted to using prime values p for N. We could often take $p = 2$ due to the presence of Atkin-Lehner involutions on $E = J_0(K)$ (*cf.* Proposition 3.3.4). In the cases where these isogenies were not available, we nevertheless always managed to find a prime $p \leq 17$ such that the point counts $\mathrm{Nm}(\mathfrak{p}) + 1 - a_{\mathfrak{p}}$ of $J_0(K)$ were all divisible by p.

The cases $p \in \{11, 17\}$ were quickly dealt with by browsing through the finitely generated group of F-points of the genus 1 curve $Y_0(p)$. Note in passing that for $p > 17$, the set $Y_0(p)$ can either be given the structure of a finitely generated group (as when $p \in \{11, 17\}$) or is a finite set, by Faltings' theorem.

In the remainder of this section, therefore, we describe how to deal effectively with the cases where $N = p$ is prime and $Y_0(p)$ has genus 0.

So let p be a prime, and suppose that $Y_0(p)$ has genus 0, that is, suppose that $p \in \{2, 3, 5, 7, 13\}$. Because the canonical compactification $X_0(p)$ has a rational cusp, the set $Y_0(p)(F)$ is nonempty and therefore infinite. It now turns out that we can use part (i) and (ii) of the Data to tremendously cut down the subset R in step 2 of Algorithm 5.2.1.

Indeed, there exists a model $C \subset \mathbf{A}^2$ of $Y_0(p)$ of the form

$$uj = f(u), \tag{5.10}$$

where f is a monic integral polynomial of degree $p + 1$ whose constant term c_0 is a strictly positive power p^{v_0} of p. For a fixed pair $(u, j) \in C(F)$, the value of j equals the j-invariant of the corresponding geometric isomorphism class of elliptic curves over $\overline{F}$. This gives an easy way to recover a curve $E(u, j)$ over $\overline{F}$ corresponding to (u, j) in step 4 by using the "universal" elliptic curve

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}. \tag{5.11}$$

over $Y_0(1) \cong \mathrm{Spec}(\mathbf{Q}[j])$. Regarding implementation, in `Magma`, a model as in (5.10) can be obtained by using the `Canonical` model of $Y_0(p)$.

We may parametrize

$$\mathbf{G}_m \longrightarrow Y_0(p) \tag{5.12}$$

by

$$u \longmapsto (u, j) = (u, \frac{f(u)}{u}). \tag{5.13}$$

Now $\mathbf{G}_m(F) = F^\times$ is not a finitely generated group. But using part (i) of the Data, we can reduce to searching through a finitely generated subgroup due to two restrictions that we shall describe presently. For the remainder of this discussion, let (u, j) be the element of $Y_0(p)(F)$ corresponding to E.

First restriction (at $\mathfrak{p} \notin M$). Let P_p be the set of primes of F above p. First consider a $\mathfrak{p}$ that is not in $M \cup P_p$, and let $v = v_{\mathfrak{p}}(u)$ be the valuation of u at $\mathfrak{p}$.

Suppose that $v > 0$. Then the terms with a factor u in the numerator of (5.13) all have strictly positive valuation, whereas $v_{\mathfrak{p}}(c_0) = 0$. Hence $v_{\mathfrak{p}}(j) = -v < 0$. We get a contradiction with the hypothesis $\mathfrak{p} \notin M$.

Suppose that $v < 0$. Then the leading term u^{p+1} has strictly smaller valuation than all the other terms in the numerator of (5.13). Hence $v_{\mathfrak{p}}(j) = v_{\mathfrak{p}}(u^{p+1}) - v_{\mathfrak{p}}(u) = pv < 0$. Again we get a contradiction with the good reduction of E at $\mathfrak{p}$.

Hence $v = 0$. Since $\mathfrak{p} \notin M \cup P_p$ was arbitrary, we conclude that in the search for (u, j), we can restrict to browsing through the image under (5.12) of the finitely generated group $\mathbf{Z}_F(M \cup P_p)^\times \subset F^\times$, where $\mathbf{Z}_F(M \cup P_p)$ denotes the ring of $M \cup P_p \cup \infty$-integers of F.

We can slightly extend these considerations. Take a prime $\mathfrak{p}$ in P_p not in M. Then we cannot quite restrict to u with $v = v_{\mathfrak{p}}(u) = 0$. However, we can certainly rule out $v < 0$ as above. On the other hand, suppose $v > v_0 e_{\mathfrak{p}}$, where $e_{\mathfrak{p}}$ equals the ramification index $e(\mathfrak{p}|p)$. Then the non-constant terms in the numerator of (5.13) all have valuation strictly larger than $v_{\mathfrak{p}}(c_0) = v_0 e_{\mathfrak{p}}$. Therefore $v_{\mathfrak{p}}(j) = v_{\mathfrak{p}}(c_0) - v_{\mathfrak{p}}(u) = v_0 e_{\mathfrak{p}} - v < 0$, resulting once more in a contradiction. We conclude that $0 \leq v \leq v_0 e_{\mathfrak{p}}$.

Second restriction (at $\mathfrak{p} \in S$). We can further restrict the search using part (ii) of the Data. Let $\mathfrak{p} \in S$ be given, and denote the given valuation at that prime by $W(\mathfrak{p})$. Again let $v = v_{\mathfrak{p}}(u)$.

First suppose that $\mathfrak{p} \notin P_p$. Then we cannot have $v = 0$, since then by (5.13) we would have $v(j) \geq 0$, which contradicts E having multiplicative reduction. Now if $v > 0$, then all non-constant terms of $f(u)$ have positive valuation, while $v_{\mathfrak{p}}(c_0) = 0$. This results in the equality $W(\mathfrak{p}) = v_{\mathfrak{p}}(j) = 0 - v = -v$. On the other hand, if $v < 0$, then the valuation of the leading term u^{p+1} of $f(u)$ is strictly smaller than that of the other terms. Hence we have $W(\mathfrak{p}) = v_{\mathfrak{p}}(j) = (p+1)v - v = pv$ if $v < 0$ holds.

Now suppose that $\mathfrak{p} \in P_p$. Then we cannot have $0 \leq v \leq v_0 e_{\mathfrak{p}}$. Indeed, if this were to hold, then the constant term c_0 of $f(u)$ would have valuation $v_{\mathfrak{p}}(c_0) = v_0 e_{\mathfrak{p}} \geq v$. Since the non-constant terms clearly also have valuation at least v, we would get $v_{\mathfrak{p}}(j) = v_{\mathfrak{p}}(f(u)) - v_{\mathfrak{p}}(u) \geq v - v = 0$, again contradicting the multiplicative reduction of E. If $v > v_0 e_{\mathfrak{p}}$, then we conclude that $W(\mathfrak{p}) = v(j) = v_0 e_{\mathfrak{p}} - v$ as in the proof of the first restriction, and if $v < 0$, then we can conclude $W(\mathfrak{p}) = pv$ as in the case $\mathfrak{p} \notin P_p$.

We conclude that at the primes $\mathfrak{p} \in S$, we have

$$v = v_{\mathfrak{p}}(u) \in \{v_0 e_{\mathfrak{p}} - W(\mathfrak{p}), W(\mathfrak{p})/p\} \cap \mathbf{Z}$$

if $\mathfrak{p}$ is over p, and

$$v = v_{\mathfrak{p}}(u) \in \{-W(\mathfrak{p}), W(\mathfrak{p})/p\} \cap \mathbf{Z}$$

otherwise.

The discussion above proves the correctness and termination of the following more easily implementable version of Algorithm 5.2.1 for the modular curves $Y_0(p)$ of genus 0. We additionally assume that the class number of F equals 1.

Removing this hypothesis is a technicality which merely complicates the statement of the algorithm, and in Chapter 7 we only consider fields with trivial class group anyhow.

Algorithm 5.2.2. *Let E be an elliptic curve over a number field F with class number* 1 *for which the Data at the beginning of the section are available. Let $p \in \{2,3,5,7,13\}$. Choose a parametrization of $Y_0(p)$ as in (5.13), and let v_0, $e_{\mathfrak{p}}$ and $W(\mathfrak{p})$ be as in the discussion above.*

If E has a p-isogeny, then the following algorithm determines a non-empty list L of candidate equations for E.

1. *Set*

$$V = \prod_{\mathfrak{p} \in S \cap P_p} \{v_0 e_{\mathfrak{p}} - W(\mathfrak{p}), W(\mathfrak{p})/p\} \cap \mathbf{Z} \times \prod_{\mathfrak{p} \in S \setminus P_p} \{-W(\mathfrak{p}), W(\mathfrak{p})/p\} \cap \mathbf{Z}.$$

For $v \in V$, compute an $a_v \in F$ that is integral outside S and has valuations agreeing with v at the places in S. Construct the set $A = \{a_v : v \in V\}$.

2. *Compute a set of generators $\{b_{\mathfrak{p}_1}, \dots, b_{\mathfrak{p}_m}\}$ for the primes $\mathfrak{p}_i$ in $P_p \setminus M$.*

3. *Compute a set of generators $\{c_1, \dots, c_n\}$ for the abelian group $\mathbf{Z}_{F,M\setminus S}^{\times}$.*

4. *Choose a large integer N. Initialize $L = \emptyset$ and set*

$$R = \{a_v b_{\mathfrak{p}_1}^{k_1} \cdots b_{\mathfrak{p}_m}^{k_m} c_1^{l_1} \cdots c_n^{l_n} \mid a_v \in A,\ 0 \le k_i \le v_0 e_{\mathfrak{p}_i},\ -N \le l_j \le N\} \subset F^{\times}.$$

5. *Choose a point $u \in R$. Calculate $j = f(u)/u$ and determine an elliptic curve $E(u,j)$ over F with $j(E(u,j)) = j$ using (5.11).*

6. *Let $M(u,j)$ be the set of primes of bad reduction of $E(u,j)$. Determine a set of representatives for the finite quotient $\mathbf{Z}_{F,M\cup M(u,j)}^{\times} / \mathbf{Z}_{F,M\cup M(u,j)}^{\times e}$. Here*

$$e = \begin{cases} 6 & \text{if } j = 0 \\ 4 & \text{if } j = 1728 \\ 2 & \text{otherwise.} \end{cases}$$

Construct the set of twists T of E by these representatives.

7. *Add to L the equations of those elements of T not yet in L that agree with the rest of the Data. Choose a new point $u \in R$ and return to step 6. Repeat until all points in R have been used.*

8. *If no candidate equations were found, enlarge N and return to step 4. Otherwise, return L.*

We do not go into further detail regarding the implementation of this algorithm: as usual, it can be found at [Sij10].

Chapter 6

Covers

In this Chapter, or more properly in its second section, we use the theory of Belyĭ maps to calculate models over $\mathbf{C}$ of some arithmetic $(1;e)$-curves whose corresponding groups are commensurable with triangle groups. The resulting complex models will be used in the next Chapter to calculate canonical models of these arithmetic pointed tori. The first section gives a short summary of the theory on ramified covers needed to perform these calculations.

6.1 Belyĭ maps

Definition 6.1.1. *Let X be a connected curve over* $\mathbf{C}$. *A* (branched) cover *of X is a pair (Y, f) consisting of a curve Y and a finite surjective morphism $f : Y \to X$. A* morphism of covers $(Y_1, f_1) \to (Y_2, f_2)$ *is a morphism of curves $g : Y_1 \to Y_2$ satisfying $f_1 = f_2 g$.*

A cover (Y, f) is called connected *if Y is connected, and* étale *if f is étale. A connected cover is called* Galois *if the cardinality of its automorphism group equals its degree.*

A Belyĭ map *is an étale cover of the curve $\mathbf{P}^1_* = \mathbf{P}^1_{\mathbf{C}} - \{0, 1, \infty\}$.*

We denote the category of étale covers of a curve X by $\mathfrak{EtCov}_X$, and the category of Belyĭ maps by $\mathfrak{Belyi}$.

Let $f : Y \to X$ be an étale cover with X nonsingular. Then Y is also nonsingular. As in Section I.6 of [Har77], let $\overline{Y}$ (respectively $\overline{X}$) be the unique complete non-singular curve containing containing Y (respectively X) as a dense open subset. Then f extends to a (possibly branched) cover $\overline{f} : \overline{Y} \to \overline{X}$ ([Har77], Proposition I.6.8). In what follows, f and $\overline{f}$ will occasionally be identified.

Let X be connected. Then as a Riemann surface, X has a universal étale cover $\widetilde{X}$, on which the topological fundamental group $\pi_1(X)$ of X acts by path lifting. The following theorem is standard:

Theorem 6.1.2 ([Len], Theorem 1.14)**.** *Let $\pi_1(X)$ be the topological fundamental group of $X(\mathbf{C})^{\mathrm{an}}$. Let $\pi_1(X)$-$\mathfrak{Sets}$ be the category of finite sets equipped with a left* *action of $\pi_1(X)$. Then there exists a natural equivalence of categories*

$$\mathfrak{EtCov}_X \longrightarrow \pi_1(X)\text{-}\mathfrak{Sets}.$$

Connected étale covers of X correspond to transitive $\pi_1(X)$-sets, i.e. *to conjugacy classes of subgroups of finite index of $\pi_1(X)$. With such a subgroup H of $\pi_1(X)$ is associated the algebraization of the cover of Riemann surfaces $\widetilde{X}/H \to X$.*

In particular, there is an equivalence

$$\mathfrak{Belyi} \longrightarrow \pi_1(\mathbf{P}^1_*)\text{-}\mathfrak{Sets},$$

under which connected Belyĭ maps correspond to conjugacy classes of subgroups of $\pi_1(\mathbf{P}^1_*)$ of finite index.

We need to define two more notions. To begin with, let $f : X \to \mathbf{P}^1_*$ be a Belyĭ map, and let $\overline{f} : \overline{X} \to \mathbf{P}^1_{\mathbf{C}}$ be its extension to a branched cover of $\mathbf{P}^1_{\mathbf{C}}$ as defined above. We call the ordered triple of tuples giving the ramification indices of $\overline{f}$ above 0, 1 and ∞ the *ramification type* of the Belyĭ map.

For instance, the Belyĭ map $\mathbf{P}^1_* \to \mathbf{P}^1_*$ given by $z \mapsto z^2$ has ramification type $((2),(1,1),(2))$, or, using more compact notation, $((2),(1^2),(2))$. Note that to a ramification type of a degree n cover one can associate an ordered triple of conjugacy classes of the symmetric group S_n, seeing as how a ramification type is an ordered triple of partitions of n.

Secondly, let $f : Y \to X$ be an étale cover. Then there exists a Galois étale cover $g : Z \to X$ such that g factors through f and such that every other Galois étale cover $g' : Z' \to X$ factors through g. In terms of Theorem 6.1.2, for a connected $\pi_1(X)$-set corresponding to a subgroup H, the cover (Z, g) corresponds to the core $C(H)$ of H in $\pi_1(X)$. The *monodromy group* $\mathrm{Mon}(Y, f)$ of (Y, f) is the automorphism group of the cover (Z, g).

For $P \in \{0, 1, \infty\}$, consider the element γ_P of the fundamental group $\pi_1(\mathbf{P}^1_*)$ given by a counterclockwise loop of winding number 1 around P whose complement in $\mathbf{P}^1(\mathbf{C})$ consists of two connected components, one of which contains P and the other of which contains $\{0, 1, \infty\} - P$. These elements satisfy $\gamma_0\gamma_1\gamma_\infty = 1$, and in fact

$$\pi_1(\mathbf{P}^1_*) = \langle \gamma_0, \gamma_1, \gamma_\infty \mid \gamma_0\gamma_1\gamma_\infty = 1 \rangle.$$

By Theorem 6.1.2, given a Belyĭ map, the γ_P furnish us with three permutations σ_0, σ_1, σ_∞ of the corresponding $\pi_1(\mathbf{P}^1_*)$-set. Conversely, given three permutations $\sigma_0, \sigma_1, \sigma_\infty$ of $\{1, \ldots, n\}$ satisfying $\sigma_0\sigma_1\sigma_\infty = 1$, we can define an action of $\pi_1(\mathbf{P}^1_*)$ on $\{1, \ldots, n\}$ by sending γ_P to σ_P. This gives rise to the following well-known construction.

Proposition 6.1.3. *There is a bijection between the set of isomorphism classes of Belyĭ maps of degree n and the set of simultaneous S_n-conjugacy class of triples $(\sigma_0, \sigma_1, \sigma_\infty)$ satisfying $\sigma_0\sigma_1\sigma_\infty = 1$.*

Morphisms from the Belyĭ map associated with $(\sigma_0, \sigma_1, \sigma_\infty) \in S_n^3$ and that associated with $(\sigma_0', \sigma_1', \sigma_\infty') \in S_m^3$ correspond to maps of sets $h : \{1, \ldots, n\} \to \{1, \ldots, m\}$ satisfying $\sigma_P' h = h\sigma_P$ for all $P \in \{0, 1, \infty\}$.

Given a triple $(\sigma_0, \sigma_1, \sigma_\infty) \in S_n^3$, let M be the subgroup of S_n generated by σ_0, σ_1 and σ_∞. The invariants of the Belyĭ map (X, f) associated with $(\sigma_0, \sigma_1, \sigma_\infty)$ can then be read off as follows:

(i) The degree of f equals n.

(ii) The set of connected components of X is in bijection with the set of orbits of $\{1, \ldots, n\}$ under the action of M.

(iii) The ramification type of (X, f) is the ordered triple of cycle types of σ_0, σ_1 and σ_∞.

(iv) The monodromy group of (X, f) is isomorphic to M.

(v) There is an isomorphism

$$\mathrm{Aut}(X, f) \cong \bigcap_{P \in \{0,1,\infty\}} \mathrm{Cent}_{S_n}(\sigma_P).$$

Proof. This proposition follows from the fact that the equivalence in Theorem 6.1.2 is in fact an equivalence of *Galois categories*. See [Len] for more details. □

Proposition 6.1.3 suggests the following naive algorithm to determine the Belyĭ maps of fixed ramification type.

Algorithm 6.1.4. *Let R be a ramification type, and let (C_0, C_1, C_∞) be the ordered triple of conjugacy classes of S_n corresponding to R.*

This algorithm determines a set S of representatives for the simultaneous S_n-conjugacy classes of triples $(\sigma_0, \sigma_1, \sigma_\infty)$ which satisfy $\sigma_0\sigma_1\sigma_\infty = 1$ and whose ramification type equals R.

1. *Set $S = \emptyset$ and $T = \emptyset$. Choose a $\sigma_0 \in C_0$.*

2. *Run through the pairs $(\sigma_1, \sigma_\infty) \in C_1 \times C_\infty$. If $\sigma_0\sigma_1\sigma_\infty = 1$, then add $(\sigma_0, \sigma_1, \sigma_\infty)$ to T.*

3. *Run through the elements t of T. Set $C = \mathrm{Cent}_{S_n}(\sigma_0)$. If $\{ctc^{-1} : c \in C\}$ has empty intersection with S, then add t to S.*

Proof of correctness. We have to justify step 1 and step 3. As for step 1, we fix $\sigma_0 \in C_0$ to cut down the running time: since we are only interested in the triples $(\sigma_0, \sigma_1, \sigma_\infty)$ up to simultaneous S_n-conjugation, this is unproblematic.

Step 3 sifts out solutions in S that are simultaneously conjugate. Now note that if such a simultaneous conjugation occurs at all, then it is induced by an element of $\mathrm{Cent}_{S_n}(\sigma_0)$. Indeed, by step 1, all elements of S have first component equal to σ_0. □

Remarks. (i) Given a triple $(\sigma_0, \sigma_1, \sigma_\infty)$ of elements of S_n, the invariants in Proposition 6.1.3 can be calculated rapidly. Accordingly, our explicit implementation at [Sij10] returns these invariants as well.

(ii) We typically use Algorithm 6.1.4 to prove non-existence or uniqueness of a Belyĭ map with given ramification type. Additionally, it can be used to distinguish between Belyĭ maps with identical ramification type by calculating their invariants as in the previous remark.

We now give two somewhat less standard results that we shall need in the next section. First recall that a subgroup G of $\mathrm{PGL}_2^+(\mathbf{R})$ with signature $(g; e_1, \ldots, e_n)$ has *(arithmetic) covolume* $\mathrm{Covol}(G)$ equal to

$$\mathrm{Covol}(G) = 2g - 2 + \sum_{i=1}^{n} \left(1 - \frac{1}{e_i}\right).$$

Given G, we can consider the covers *subordinate* to G. These are the covers of $Y(G)$ whose restriction to the complements of the elliptic points of $Y(G)$ is étale and with the additional property that for any elliptic point p of $Y(G)$, the ramification indices at the points above p all divide the index of p. The covers subordinate to G again form a category, which we denote by $\mathfrak{SCov}_{Y(G)}$.

Let S be the set of elliptic points of $Y(G)$. For $p \in S$, let e_p be the index of p and let γ_p be a sufficiently small counterclockwise loop around p (as in the discussion before Proposition 6.1.3). Then as abstract groups we have

$$G = \pi_1(Y(G) - S)/N, \tag{6.1}$$

where N is the normal subgroup generated by the elements $\gamma_p^{e_p}$, $p \in S$. Given Theorem 6.1.2, the following theorem therefore suggests itself.

Theorem 6.1.5. *Let G be a subgroup of $\mathrm{PGL}_2^+(\mathbf{R})$ of finite covolume. Through the isomorphism (6.1), the equivalence from Theorem 6.1.2 induces an equivalence*

$$\mathfrak{SCov}_{Y(G)} \longrightarrow G\text{-}\mathfrak{Sets}.$$

In particular, when G is a triangle group of signature $(0; p, q, r)$, we obtain equivalences between the categories of

(i) Connected subordinate covers of $Y(G)$;

(ii) Conjugacy classes of subgroups of G of finite index; and

(iii) Simultaneous S_n-conjugacy classes of transitive triples $(\sigma_0, \sigma_1, \sigma_\infty)$ satisfying

$$\sigma_0\sigma_1\sigma_\infty = 1,\ \sigma_0^p = \sigma_1^q = \sigma_\infty^r = 1.$$

Given a subgroup $H \subset G$ as above, the corresponding cover is given by the canonical map $Y(H) \to Y(G)$. Its degree equals

$$[G : H] = \mathrm{Covol}(H)/\mathrm{Covol}(G).$$

Proof. The equivalence of categories follows from Section 6.4 in [Ser92]. The statement relating degrees to covolumes is Lemme IV.1.3 in [Vig80]. It also follows from the Riemann-Hurwitz formula. □

Proposition 6.1.6. *Consider a cartesian diagram of covers*

$$\begin{tikzcd} Y_1 \arrow[r] \arrow[d] & Y_0 \arrow[d] \\ X_1 \arrow[r] & X_0 \end{tikzcd} \tag{6.2}$$

Suppose $\deg(X_1|X_0)$ *and* $\deg(Y_1|Y_0)$ *are both equal to m. Then for some divisor d of m we have*

$$|\mathrm{Mon}(Y_0|X_0)| = d|\mathrm{Mon}(Y_1|X_1)|.$$

Proof. To prove the proposition, we use the correspondence between complex curves X and their function fields $\mathbf{C}(X)$ in Section I.6 of [Har77]. The condition that (6.2) be cartesian translates into $\mathbf{C}(Y_1) = \mathbf{C}(X_1)\mathbf{C}(Y_0)$. Furthermore, the condition on the equality of degrees gives that the extensions $\mathbf{C}(Y_0)|\mathbf{C}(X_0)$ and $\mathbf{C}(X_1)|\mathbf{C}(X_0)$ are linearly disjoint.

The Galois closure L_i of the extension $\mathbf{C}(Y_i)|\mathbf{C}(X_i)$ has Galois group equal to the monodromy group of the cover $Y_i \to X_i$. Because of the linear disjointness, we have $L_1 = L_0\mathbf{C}(X_1)$. The degree d of the extension $L_0\mathbf{C}(X_1)|L_0$ divides the degree m of the extension $\mathbf{C}(X_1)|\mathbf{C}(X_0)$, and we have

$$d|\mathrm{Mon}(Y_0|X_0)| = [L_0\mathbf{C}(X_1) : L_0][L_0 : \mathbf{C}(X_0)] = [L_0\mathbf{C}(X_1) : \mathbf{C}(X_0)]$$

$$= [L_1 : \mathbf{C}(X_0)] = [L_1 : \mathbf{C}(X_1)][\mathbf{C}(X_1) : \mathbf{C}(X_0)] = |\mathrm{Mon}(Y_1|X_1)|m.$$

Since m/d is also a divisor of m, the proposition is proved. An alternative proof uses the fact that d equals the index $[S_0 : S_1]$, where the S_i are the images of the fundamental groups $\pi_1(X_i, x_i)$ in the symmetric groups on the fiber of Y_1 over x_0. Here x_0 is a point of X_0 that is not in the branch locus of the cover $Y_1 \to X_0$, and $x_1 \in X_1$ is a point above X_0. □

The following algorithm determines the G-set G/H corresponding to an inclusion $H \subset G$ of groups.

Algorithm 6.1.7. *Let $H \subset G$ be an inclusion of groups of finite index, and let S be a set of generators for the group G.*

Given a procedure to test whether an element $g \in G$ is in H, this algorithm determines a set C of right coset representatives of G/H and calculates the induced G-set structure of C.

1. *Initialize: set $T = \{1\}$, $C = \emptyset$.*

2. *Choose a $t \in T$ and remove it from T. If there exists no $c \in C$ such that $c^{-1}t \in H$, then add t to C, and adjoin the set $St = \{st : s \in S\}$ to T.*

3. *If T is empty, go to step 4. Otherwise, go to step 2.*

4. *For every s in S, construct the following permutation σ_s of C. Given $c \in C$, find a $c' \in C$ such that $c'^{-1}sc \in H$. Then set*

$$\sigma_s(c) = c'.$$

5. *Return the G-set structure on C given by $s \mapsto \sigma_s$.*

Proof of correctness. Let us first prove that C is indeed a set of representatives for G/H. On the one hand, we cannot have $cH = c'H$ for two distinct elements $c, c' \in C$. For suppose that of these two elements, c was the first to be appended to C. Then we would have had $c^{-1}c' \in H$ when we appended c' to C, which does not square with step 2.

On the other hand, because we kept adjoining the sets St in step 2, we know that the elements $SC = \{sc : s \in S, c \in C\}$ are all right H-equivalent to elements of C. Since S is a set of generators of G, in fact all elements of $GC = G$ are right H-equivalent to some element of C.

Likewise, the fact that the algorithm terminates follows from the fact that the index is finite and S is a set of generators of G: a given right coset in G/H is represented by a finite word in S, hence after some finite time, the algorithm will find a representative of it.

The correctness of step 4 and step 5 is also clear: indeed, asking that $c'^{-1}sc$ be an element of H is equivalent to demanding $scH = c'H$. Note that by construction of C, the element c' is unique. □

We implemented this algorithm at [Sij10] in the following case:

- $G \subset \mathrm{PGL}_2^+(\mathbf{R})$ is a subgroup of $\mathrm{PGL}_2^+(\mathbf{R})$ of the form $\mathrm{P}\mathcal{O}(1)^1$ coming from a maximal quaternion order $\mathcal{O}(1)$ in an algebra B; and
- $H \subset G$ is of the form $\mathrm{P}\mathcal{O}^1$ for some quaternion order $\mathcal{O}$ contained in $\mathcal{O}(1)$.

Representatives in $\mathcal{O}(1)^1$ for generators of G can then be found using the `Magma` function `Group`. It is relatively simple to see if a given element of $\mathrm{P}\mathcal{O}(1)^1$ represented by an element b of $\mathcal{O}(1)^1$ is in fact in $\mathrm{P}\mathcal{O}^1$, since this boils down to testing whether b is in $\mathcal{O}$, which is easily checked. A substantial advantage of this approach is that it is exact, since all operations can be performed in the $\mathbf{Q}$-vector space B.

Using Algorithm 6.1.7, we calculated Table A.2 in the appendix, which will feature extensively in the calculations below and in Chapter 7: it studies the orders $\mathbf{Z}_F[G]$ generated by the groups G inbetween $\Gamma^{(2)}$ and Γ, along with their norm 1 groups $\mathbf{Z}_F[G]^1$.

Note that it is very well possible for $\mathbf{Z}_F[G]^1$ to be larger than G: in fact, one of our reasons for implementing Algorithm 6.1.7 was to study the inclusion $G \subseteq \mathbf{Z}_F[G]^1$. As remarked after Lemma 3.3.2, we prefer to work with the groups $\mathbf{Z}_F[G]^1$ whenever possible.

Remark. For covers $Y_0(\mathcal{O}') \to Y_0(\mathcal{O})$ corresponding to inclusions of orders $\mathcal{O}' \subset \mathcal{O}$, the monodromy group can also be calculated by reasoning locally as in Corollary 2.5.3. For example,

- An inclusion $\mathcal{O}(\mathfrak{N}) \subset \mathcal{O}(1)$ of a level $\mathfrak{N}$ Eichler order into a maximal order gives rise to a monodromy group isomorphic to $\mathrm{PSL}(\mathbf{Z}_F/\mathfrak{N})$. The corresponding minimal Galois cover is $Y_0(C) \to Y_0(\mathcal{O}(1))$, where

$$C = (\widehat{\mathbf{Z}}_F + \mathfrak{N}\widehat{\mathcal{O}}(1))^\times$$

  is the core of $\widehat{\mathcal{O}}(\mathfrak{N})^\times$.

- Let $\mathfrak{p}$ be prime dividing the discriminant of B, and let $\mathcal{O}(\mathfrak{p})$ be the unique level $\mathfrak{p}$ suborder of a maximal order $\mathcal{O}(1)$ (*cf.* Proposition 2.3.2). Then the projection

$$Y_0(\mathcal{O}(\mathfrak{p})) \longrightarrow Y_0(\mathcal{O}(1))$$

  is a cyclic Galois cover.

However, since a lot of the orders that we will encounter are non-Eichler, which complicates this approach, we have chosen to perform the calculations below globally, as in Algorithm 6.1.7.

6.2 $(1;e)$-covers

Throughout this section, let Γ be an arithmetic $(1;e)$-group, and let $a \in \{\pm 1\}$. Below, we consider the Γ that are commensurable with triangle groups. These groups can be determined by using the list in [Tak77] of commensurability classes of arithmetic triangle groups. By Proposition 1 of [Tak77], whether or not Γ is commensurable with a triangle group only depends on the associated quaternion algebra $\mathbf{Q}(\Gamma^{(2)})$ from Lemma 3.3.2.

By virtue of Lemma 3.3.2, there exists a cover

$$X^a(\Gamma^{(2)}) \longrightarrow X^a(\mathcal{O}^1)$$

for some maximal quaternion order $\mathcal{O}$. Let us throughout this section denote

$$\begin{aligned} N(\mathcal{O}) &= N_{\mathrm{GL}_2^+(\mathbf{R})}(\mathcal{O}) = \{\gamma \in \mathrm{GL}_2^+(\mathbf{R}) : \gamma\mathcal{O} = \mathcal{O}\gamma\} \\ &= \mathbf{R}^\times \iota(N_{\widehat{B}^\times}(\widehat{\mathcal{O}}^\times) \cap B^+). \end{aligned}$$

Then [Tak77] also shows that if Γ is commensurable with a triangle group, the Atkin-Lehner quotient $X^a(N(\mathcal{O}))$ is a genus 0 curve with three elliptic points. In other words, $\mathrm{P}N(\mathcal{O}) \subset \mathrm{PGL}_2^+(\mathbf{R})$ is a triangle group.

We have a composite map

$$X^a(\Gamma^{(2)}) \longrightarrow X^a(\mathcal{O}^1) \longrightarrow X^a(N(\mathcal{O})). \tag{6.3}$$

Considering on the other hand the composition

$$\mathcal{H} \longrightarrow X^a(\Gamma^{(2)}) \longrightarrow X^a(N(\mathcal{O})),$$

one sees that the cover (6.3) can only ramify above the three elliptic points of the genus 0 curve $X(N(\mathcal{O}))$. Hence by transitivity of $\mathrm{Aut}(\mathbf{P}^1_{\mathbf{C}})$ on triples of points in $\mathbf{P}^1(\mathbf{C})$, we can consider (6.3) as a Belyĭ map. Note that for any triangle group Δ there exists an isomorphism

$$X^+(\Delta) \cong X^-(\Delta). \tag{6.4}$$

Therefore, we are justified in only using the curves $X(N(\mathcal{O})) = X^+(N(\mathcal{O}))$ in what follows. Occasionally, $\mathcal{O}^1$ is a triangle group as well, in which case we can try and calculate the Belyĭ map $X^a(\Gamma^{(2)}) \to X(\mathcal{O}^1)$, which is of smaller degree.

The cover (6.3) need not factor through Γ. However, whenever possible, we have found a triangle group Δ containing Γ, realizing not merely $X^a(\Gamma^{(2)})$ but also $X^a(\Gamma)$ as a Belyĭ cover $X^a(\Gamma) \to X(\Delta)$. In the cases where we did not manage to find such an inclusion $\Gamma \subset \Delta$, we have proved that it cannot exist.

Using the data from Table A.2, we now proceed to calculate some of these Belyĭ maps and the resulting geometric models of $X^a(\Gamma)$. We have not included the details of all calculations, since these were performed in a rather ad hoc manner. However, we will always indicate how to simplify the covers involved as much as possible. Our most frequently applied techniques are the following.

- We will often descend a genus 1 Belyĭ map $Y_1 \to X_1 = \mathbf{P}^1_*$ to a genus 0 Belyĭ map $Y_0 \to X_0$ by constructing a diagram as in Proposition 6.1.6. The cover $Y_0 \to X_0$ is often easier to calculate, and it will always be possible to determine Y_1 given Y_0.

- Arguing in the opposite direction, we can construct $(1;e)$-groups Γ from triangle groups Δ by using Proposition 6.1.5. This is especially useful if there is a unique $(1;e)$-group in the commensurability class of Δ. Knowing e and the signature of Δ, the degree of the corresponding cover can be determined using Proposition 6.1.5, which also puts a restriction on the possible ramification types. The corresponding covers can then be described using Algorithm 6.1.4.

- Finally, the *Atkin/Swinnerton-Dyer differentiation trick* (which is described in [Bir94]) is of great use in computing genus 0 Belyi maps.

Although calculating Belyĭ maps can be rather involved, it is conversely easy enough to check that the Belyĭ maps given below indeed have the properties that we claim them to have.

Throughout the calculations, given an integer d, we denote

$$w_d = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4; \\ \sqrt{d} & \text{otherwise.} \end{cases}$$

as in [Tak83]. Moreover, we use the labels en_e dn_d Dn_D r explained in the appendix.

Remark. In what follows, we often need to determine the signature of some Atkin-Lehner quotient of a Shimura curve. One can derive general formulas for these using the methods of [Voi09b] and Section III.5.C of [Vig80]. However, we have not included the details of these formulas here because it was possible in all cases to circumvent these calculations using geometric arguments (which could in principle be applied to a broader class of covers).

The calculations

$\boxed{\textbf{e2d5D4:}}$ The first three cases are complicated and varied enough to deserve a rather detailed look, so as to illustrate the techniques involved in the calculations. The considerations for the other curves below will for reasons of space be somewhat more terse.

Let B be a quaternion algebra over $F = \mathbf{Q}(w_5)$ for which $\mathfrak{D}(B)^f = \mathfrak{p}_2 = (2)$. Table A.1 shows that there are three $(1;2)$-curves for this algebra B. Before going into detail for the individual cases, let us note the following.

Preamble. Since the narrow class group of F is trivial, by Proposition 3.2.1, we have $\mathrm{P}\mathcal{O}^1 = \mathrm{P}\mathcal{O}^+$ for all orders $\mathcal{O}$, and all groups $\mathcal{O}(1)^1$ coming from maximal orders $\mathcal{O}(1)$ are $\mathrm{GL}_2^+(\mathbf{R})$-conjugate by Proposition 2.6.2(ii). As was shown in [Tak77], for a maximal order $\mathcal{O}(1)$, the signature of $X(N(\mathcal{O}(1)))$ is equal to $(0;2,4,5)$, and $N(\mathcal{O}(1))$ is a maximal arithmetic triangle group Δ. Up to conjugacy, there is only one other maximal arithmetic triangle group Δ' in its commensurability class, which has signature $(0;2,4,10)$.

Theorem 6.1.5 shows that one way to obtain arithmetic $(1;2)$-curves is to construct subordinate covers

$$X(\Gamma) \longrightarrow X(\Delta) = X(N(\mathcal{O}(1))) \tag{6.5}$$

Calculating covolumes as in Theorem 6.1.5, one sees such a subordinate cover has degree equal to 10. Also, the ramification type is forced: it has to equal $((2^5),(4^2,2),(10))$.

Algorithm 6.1.4 now gives that there are two subordinate covers as in (6.5), with monodromy groups of cardinality 120 and 160, respectively. Both have automorphism group $\mathbf{Z}/2\mathbf{Z}$, and they factor through the unique cover of ramification type $((2^2,1),(2^2,1),(5))$ and $((2,1^3),(4,1),(5))$, respectively. Since $X^+(\Delta)$ is isomorphic to $X^-(\Delta)$ by (6.4), we have $X^+(\Gamma) \cong X^-(\Gamma)$ for the resulting $(1;e)$-groups Γ, considering the fact that the corresponding covers are uniquely determined by their ramification indices and monodromy group,

Calculating covolumes, one shows that there are no subordinate covers of $X(\Delta')$ by curves of signature $(1;2)$.

For reasons that will become clear, we now tackle the subcases in reverse order.

$\boxed{\textbf{e2d5D4iii:}}$ As can be seen in Table A.2,

$$\mathrm{P}\langle\Gamma^{(2)},A\rangle = \mathrm{P}\mathcal{O}(\mathfrak{p}_3)^1 = \mathrm{P}\mathcal{O}(\mathfrak{p}_3)^+$$

is a group coming from a level $\mathfrak{p}_3 = (3)$ order $\mathcal{O}(\mathfrak{p}_3) = \mathbf{Z}_F[\Gamma^{(2)}]$. Let $\mathcal{O}(1)$ be a maximal order containing $\mathcal{O}(\mathfrak{p}_3)$. We obtain an inclusion $\mathcal{O}(\mathfrak{p}_3)^1 \subset \mathcal{O}(1)^1$. The order $\mathcal{O}(\mathfrak{p}_3)$ is Eichler by Proposition 2.2.3, whence Corollary 2.5.4 allows us to conclude that

$$[\mathcal{O}(1)^1 : \mathcal{O}(\mathfrak{p}_3)^1] = \mathrm{Nm}(\mathfrak{p}_3) + 1 = 10.$$

Furthermore, by Proposition 2.6.2(i), we have

$$X^+(\mathcal{O}(\mathfrak{p}_3)^1) = Y_0^+(\mathcal{O}(\mathfrak{p}_3)) \cong Y(\mathcal{O}(\mathfrak{p}_3)) \cong Y_0^-(\mathcal{O}(\mathfrak{p}_3)) = X^-(\mathcal{O}(\mathfrak{p}_3)^1)$$

and

$$X^+(\mathcal{O}(1)^1) = Y_0^+(\mathcal{O}(1)) \cong Y(\mathcal{O}(1)) \cong Y_0^-(\mathcal{O}(1)) = X^-(\mathcal{O}(1)^1).$$

Algorithm 6.1.4 yields that the cover

$$X(\mathcal{O}(\mathfrak{p}_3)^1) \longrightarrow X(\mathcal{O}(1)^1)$$

has no non-trivial automorphisms. The cardinality of its monodromy group equals $360 = |\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}_3)|$ (*cf.* the remark after Algorithm 6.1.7). Since the cover

$$X(\mathcal{O}(\mathfrak{p}_3)^1) = X(\langle \Gamma^{(2)}, A\rangle) \longrightarrow X(\Gamma)$$

is a 2-isogeny by Lemma 3.3.2, hence Galois, Lemma 3.3.4 and the equality $\mathcal{O}(\mathfrak{p}_3) = \mathbf{Z}_F[\Gamma^{(2)}]$ imply that $X(\Gamma)$ is an Atkin-Lehner quotient of $X(\mathcal{O}(\mathfrak{p}_3)^1) \cong Y(\mathcal{O}(\mathfrak{p}_3))$.

Suppose that $\mathrm{P}\Gamma$ were contained in the maximal triangle group $\mathrm{P}N(\mathcal{O}(1))$. Then we would get a descent

$$\begin{tikzcd} X(\mathcal{O}(\mathfrak{p}_3)^1) \arrow[r, "2"] \arrow[d, "10"] & X(\Gamma) \arrow[d, "10"] \\ X(\mathcal{O}(1)^1) \arrow[r, "2"] & X(N(\mathcal{O}(1))) \end{tikzcd} \tag{6.6}$$

Diagram (6.6) would then be cartesian because the group $\mathrm{P}\Gamma$ cannot be contained in $\mathrm{P}\mathcal{O}(1)^1$. Indeed, Lemma 3.3.4 shows that there are nontrivial inclusions

$$\mathrm{P}\mathcal{O}(\mathfrak{p}_3)^1 \subsetneq \mathrm{P}\Gamma \subsetneq \mathrm{P}N_{B^+}(\mathcal{O}(\mathfrak{p}_3)).$$

But all subgroups of $N_{B^+}(\mathcal{O}(\mathfrak{p}_3)) \subset B^+$ properly containing $\mathcal{O}(\mathfrak{p}_3)^1$ contain elements whose norm is not a square in F. Hence we can not have $\mathrm{P}\Gamma \subset \mathrm{P}\mathcal{O}(1)^1$.

Therefore Diagram (6.6) would indeed be cartesian. Consequently, Proposition 6.1.6 would imply that the degree 10 cover

$$X(\Gamma) \longrightarrow X(N(\mathcal{O}(1)))$$

has monodromy group would have cardinality 360 or 720 by Proposition 6.1.6. But we have seen in the preamble above that only cardinalities 120 and 160 were possible. Therefore Γ is not contained in a triangle group.

Of course, one can still divide out the Atkin-Lehner involution $w(\mathfrak{p}_2)$ and descend the cover for a diagram

$$\begin{tikzcd} X(\mathcal{O}(\mathfrak{p}_3)^1) \arrow[r, "2"] \arrow[d, "10"] & X(\mathcal{O}(\mathfrak{p}_3)^1)/w(\mathfrak{p}_2) \arrow[d, "10"] \\ X(\mathcal{O}(1)^1) \arrow[r, "2"] & X(N(\mathcal{O}(1))) \end{tikzcd} \tag{6.7}$$

It is possible to calculate the signature of $X(\mathcal{O}(\mathfrak{p}_3)^1)/w(\mathfrak{p}_2)$ directly by using the methods of [Voi09b] and Section III.5.C of [Vig80]. Alternatively, one can exclude that $X(\mathcal{O}(\mathfrak{p}_3)^1)/w(\mathfrak{p}_2)$ has signature $(1;2)$ or $(0;2,2,2,2,2)$ by using Algorithm 6.1.4 and Proposition 6.1.6 in the same way as before, and then the only remaining possibility is $(0;2,2,4,4)$.

Both methods give that the signatures in diagram (6.7) are as follows:

$$\begin{tikzcd} (1;2,2) \arrow[r, "2"] \arrow[d, "10"] & (0;2,2,4,4) \arrow[d, "10"] \\ (0;2,5,5) \arrow[r, "2"] & (0;2,4,5) \end{tikzcd} \tag{6.8}$$

The Belyĭ map on the right is of genus 0, hence simpler than the one on the right. A priori, there are two possible ramification types for this map, namely $((2^3,1^2),(4^2,1^2),(5^2))$ and $((2^5),(4,2^2,1^2),(5^2))$, but Algorithm 6.1.4 shows that the latter gives rise to covers whose monodromy groups have cardinality equal to 160, so we can exclude this ramification type using Proposition 6.1.6.

The former ramification type has 5 Belyĭ maps associated to it, but only one of these has a monodromy group of the correct cardinality. Algorithm 6.1.4 also gives another more tangible feature distinguishing this Belyĭ map from its 4 compeers: it is the only one among these 5 whose automorphism group is trivial.

We place the elliptic points of $X(N(\mathcal{O}(1)))$ of order $2,4,5$ at $1,\infty,0$, respectively. By solving the resulting equations numerically and recognizing the solutions as algebraic numbers, we found the following solution:

$$z \longmapsto \frac{4(w-8)(z^2-45)^5}{3^5 5^5 (z-5)^4 (z^2+(6-2w)z+(15w-75))}. \tag{6.9}$$

where $w = w_{-15}$. This Belyĭ map indeed has trivial automorphism group, which can be checked by verifying that no automorphism of $\mathbf{P}^1_{\mathbf{C}}$ exchanging the zeroes of $z^2+(6-2w)z+(15w-75)$ has the additional property that it fixes the set of zeroes of z^2-45 and the set $\{5,\infty\}$ as well. Note that every automorphism should fix these points by Proposition 6.1.3, since these pairs of points are the only simple points in their respective fibers.

Let us remark that this Belyĭ map is isomorphic to its complex conjugate: one can use the automorphism of $\mathbf{P}^1_{\mathbf{C}}$ induced by the matrix

$$\begin{pmatrix} 5 & -45 \\ 1 & -5 \end{pmatrix}$$

As in [Cou94], one then shows that although this cover is defined over $\mathbf{Q}$, there is no totally real field K such that there exists a rational function $\mathbf{P}^1_K \to \mathbf{P}^1_K$ realizing this cover.

In terms of equation (6.9), the elliptic points of $X(\mathcal{O}(\mathfrak{p}_3)^1)/w(\mathfrak{p}_2)$ are given by the simple points above ∞ and 1. The former are given by the zeroes of $z^2 + (6 - 2w)z + (15w - 75)$: these have index 4. The latter, which have index 2, are the simple zeroes of the numerator minus the denominator, and are given by the zeroes of $z^2 + (5w + 5)z + (-135w - 225)/4$.

As can be seen from diagram (6.8), $X(\Gamma)$ can be recovered by taking the degree 2 elliptic cover of $X(\mathcal{O}(\mathfrak{p}_3)^1)/w(\mathfrak{p}_2)$ branched in these 4 elliptic points to recover $X(\mathcal{O}(\mathfrak{p}_3)^1)$ and then identifying the elliptic points of order 2 on this elliptic curve, which are just the preimages of the zeroes of $z^2 + (6 - 2w)z + (15w - 75)$. This gives that

$$j(J^+(\mathcal{O}(\mathfrak{p}_3)^1)) = \frac{7949^3}{2^5 3^{10}} = j(J^-(\mathcal{O}(\mathfrak{p}_3)^1))$$

and

$$j(J^+(\Gamma)) = \frac{-269^3}{2^{10}3^5} = j(J^-(\Gamma)).$$

The preamble shows that in the remaining two cases, the group Γ is triangular and $X^+(\Gamma) \cong X^-(\Gamma)$. Hence we only consider the curves $X(\Gamma)$.

$\boxed{\textbf{e2d5D4ii:}}$ We have $\Gamma \subsetneq \mathrm{P}\mathbf{Z}[\Gamma]^1$. The order $\mathcal{O}(1) = \mathbf{Z}[\Gamma]$ is maximal, and a consideration of covolumes as in Theorem 6.1.5 shows that $\mathrm{P}\Gamma$ is an index 5 subgroup of $\mathrm{P}\mathcal{O}(1)^1$. The ramification type of the corresponding cover

$$X(\Gamma) \longrightarrow X(\mathcal{O}^1)$$

has to equal $((2^2, 1), (5), (5))$. Algorithm 6.1.4 shows that there exists a unique Belyĭ map with this ramification type, whose monodromy group has cardinality 60.

Since $\mathrm{P}\Gamma$ does not equal $\mathrm{P}\mathcal{O}^1$, we cannot a priori be certain that the Atkin-Lehner involution of $X(\mathcal{O})$ lifts to $X(\Gamma)$. However, one can write down an explicit normalizing element that shows that it does lift.

Let (A, B) be a standard pair (as in (1.3)). Consider the matrix $S \in \mathrm{GL}_2^+(\mathbf{R})$ given by

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

This matrix is not in $\Gamma = \langle A, B \rangle$ since it fixes $0 \in \mathfrak{D}$, which is in the interior of the fundamental domain for Γ constructed in Chapter 1 and hence cannot be fixed by an element of Γ. One can also check that no element of $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma]$ is a multiple of S, hence S is not in $\mathcal{O}(1)^1$ either.

The matrix S also normalizes Γ. Indeed, one calculates that $AS = SA^{-1}$ and $BS = SB^{-1}$ for any standard pair (A, B). Also note that S is in the normalizer of all intermediate groups $\Gamma^{(2)} \subset G \subset \Gamma$.

Clearly S normalizes $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma]$ as well. Hence by Lemma 3.3.4 it in fact corresponds to the unique Atkin-Lehner involution of $\mathcal{O}(1)$. Clearly, S has to fix the elliptic point of $X(\Gamma)$. We can therefore descend for a diagram

$$\begin{tikzcd}
X(\Gamma) \arrow[r, "2"] \arrow[d, "5"] & X(\langle \Gamma, S \rangle) \arrow[d, "5"] \\
X(\mathcal{O}(1)^1) \arrow[r, "2"] & X(N(\mathcal{O}(1)))
\end{tikzcd}$$

with signatures

$$\begin{tikzcd}
(1;2) \arrow[r, "2"] \arrow[d, "5"] & (0;2,2,2,4) \arrow[d, "5"] \\
(0;2,5,5) \arrow[r, "2"] & (0;2,4,5)
\end{tikzcd} \tag{6.10}$$

A priori, the map on the right can have ramification type $((2^2,1),(2^2,1),(5))$ or $((2,1^3),(4,1),(5))$. Algorithm 6.1.4 shows that there are unique Belyĭ maps with these ramification types, having monodromy group of cardinality 10 and 120 respectively. Hence by Proposition 6.1.6, the correct ramification type is in fact the latter.

Placing the elliptic points of order $2,4,5$ at $1,\infty,0$ respectively, the cover is given by

$$z \longmapsto \frac{z^5}{5z-4}$$

Diagram (6.10) then shows that we can recover a geometric model of $X(\Gamma)$ by taking the degree 2 elliptic cover of $\mathbf{P}^1_{\mathbf{C}}$ branched in the simple preimages of 1 and ∞ under this map. We obtain

$$j(J^+(\Gamma)) = \frac{5^1 211^3}{2^{15}} = j(J^-(\Gamma)).$$

We now give an alternative way to derive this result, which does not make use of the explicit matrix S. The group Γ is contained in the maximal triangle group $N(\mathcal{O}(1))$ of signature $(0;2,4,5)$. Let

$$K = \mathbf{C}(X(N(\mathcal{O}(1)))),\ L = \mathbf{C}(X(\mathcal{O}(1)^1)),\ M = \mathbf{C}(X(\Gamma)).$$

Let N_K be the normal closure of the extension $M|K$, and let N_L be the normal closure of the extension $M|L$. Since N_K, being normal over K, is also normal over L, we have a chain of inclusions

$$K \subset L \subset M \subset N_L \subset N_K$$

Hence

$$|\mathrm{Mon}(X(\Gamma) \longrightarrow X(N(\mathcal{O}(1))))| = [N_K : K]$$

is a multiple of

$$|\mathrm{Mon}(X(\Gamma) \longrightarrow X(\mathcal{O}(1)^1))| = [N_L : L]$$

We saw at the beginning of this case that the latter cardinality equals 60.

We conclude that of the two Belyĭ maps $X(\Gamma) \to X(N(\mathcal{O}(1)))$ constructed in the preamble, we are in fact considering the former, of which the cardinality of the monodromy group equals 120. We saw that this Belyĭ map factorizes through an automorphism (induced by S). It can be calculated via the exact same two-step process as above.

$\boxed{\textbf{e2d5D4i:}}$ We have $\Gamma^{(2)} = \mathbf{Z}_F[\Gamma^{(2)}]^1$. Let $\mathcal{O} = \mathbf{Z}_F[\Gamma^{(2)}]$. Then there exists a unique maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$. Algorithm 6.1.7 shows that the map $X(\mathcal{O}^1) \to X(\mathcal{O}(1)^1)$ has degree 20 and 4 automorphisms. Using the corresponding factorization, one can calculate the cover, and with it, $j(J(\Gamma^{(2)})) = j(J(\Gamma))$.

Using the preceding results, however, there is a more direct way to calculate $j(J(\Gamma))$. Note that the cover

$$X(\Gamma) \longrightarrow X(N(\mathcal{O}(1)))$$

has to be the cover in the preamble whose monodromy group has cardinality 160. Indeed, by the previous results, no other entry in Takeuchi's list qualifies. As shown in the preamble, then, $X(\Gamma)$ can be recovered by the following two-step process:

- First take the cover of $X(\mathcal{O}^1)$ with ramification type $((2^2, 1), (2^2, 1), (5))$ above the elliptic points of order $2, 4, 5$ respectively;
- Then take the degree 2 cover ramifying above the 4 elliptic points of the resulting curve.

Keeping track of the ramification indices, we see that these elliptic points are given by

- The elements in the fiber above the elliptic point of index 4, along with
- The unique non-ramifying point in the fiber above the elliptic point of index 2.

The first degree 5 cover was calculated in [Bir94]: placing the elliptic points of index $2, 4, 5$ at $4, 0, \infty$, respectively, it is given by

$$z \longmapsto (z-2)(z^2+z-1)^2.$$

One calculates that the unique non-ramifying point above 4 has z-coordinate equal to -2. The second degree 2 cover therefore has to ramify above the zeroes of $(z+2)(z-2)(z^2+z-1)$. We end up with a genus 1 curve whose Jacobian has j-invariant

$$j(J^+(\Gamma)) = 2^4 17^3 = j(J^-(\Gamma)).$$

e2d8D2: This time $F = \mathbf{Q}(w_2)$ and $\mathfrak{D}(B)^f = \mathfrak{p}_2$. The narrow class group of F is again trivial, so as in the previous case all groups $\mathrm{P}\mathcal{O}(1)^1 = \mathrm{P}\mathcal{O}(1)^1$ arising from maximal orders $\mathcal{O}(1)$ are conjugate.

There is no maximal order $\mathcal{O}(1)$ such that the group $\mathrm{P}\Gamma$ is contained in $\mathrm{P}\mathcal{O}(1)^1$. Indeed, a calculation of covolumes gives that the degree of the map

$$X(\Gamma) \longrightarrow X(\mathcal{O}(1)^1)$$

would then have to equal 6. Since $X(\mathcal{O}(1)^1)$ has signature $(0;3,3,4)$ by [Tak77], the ramification type of the cover above is given by $((3^2),(3^2),(4,2))$. Algorithm 6.1.4 shows that there does not exist a Belyĭ map with this ramification type.

However, [Tak77] also shows that $N(\mathcal{O}(1))$ has signature $(0;2,3,8)$. By Algorithm 6.1.4, this group allows a unique degree 12 subordinate cover with ramification type $((2^6),(3^4),(8,4))$. This cover

$$X(\Gamma) \longrightarrow X(N(\mathcal{O}(1))) \tag{6.11}$$

gives rise to a $(1;2)$-group Γ, which has to be the unique $(1;2)$-group associated to this quaternion algebra.

The cover (6.11) has automorphism group $\mathbf{Z}/4\mathbf{Z}$. It therefore factorizes as a degree 4 Galois cover followed by a degree 3 cover. Now using Proposition 6.1.3, one shows:

- The latter degree 3 cover has ramification type $((2,1),(3),(2,1))$. Its domain is therefore a triangle curve of signature $(0;2,4,8)$.

- The $\mathbf{Z}/4\mathbf{Z}$ Galois cover of this triangle curve has ramification type equal to $((2^2),(4),(4))$.

The latter cover in turn decomposes as

- A cover of degree 2 and genus 0 ramified above the elliptic points of index 4 and 8, preceded by

- A cover of degree 2 and genus 1 ramified above the four elliptic points of the resulting curve of signature $(0;2^3,4)$.

Explicitly, therefore, the map from $X(\Gamma)$ to the curve of signature $(0;2,4,8)$ is given by

$$(x,y) \longmapsto x^2$$

from the curve

$$y^2 = x^3 - x$$

if we set the x-coordinates of the elliptic points of order $2,4,8$ equal to $1,0,\infty$, respectively. Clearly

$$j(J^+(\Gamma)) = 1728 = j(J^-(\Gamma)).$$

$\boxed{\textbf{e2d12D2:}}$ Let $\mathcal{O}(\mathfrak{p}_2) = \mathbf{Z}_F[\Gamma]$ .Then $\Gamma = \mathcal{O}(\mathfrak{p}_2)^1$. Furthermore, $\mathcal{O}(\mathfrak{p}_2)$ is the unique level $\mathfrak{p}_2$ suborder of the unique maximal order $\mathcal{O}(1)$ containing $\mathcal{O}(\mathfrak{p}_2)$ by Proposition 2.3.2. We get a degree 3 Galois cover

$$X(\mathcal{O}(\mathfrak{p}_2)^1) \longrightarrow X(\mathcal{O}(1)^1).$$

As is shown in [Tak77] or [Voi09b], the curve $X(\mathcal{O}(1)^1)$ has signature $(0;3,3,6)$. Hence the cover above is explicitly given by

$$(x,y) \longmapsto (1+y)/2$$

from the curve

$$y^2 = x^3 + 1$$

if we set the coordinates of the elliptic points of order $3,3,6$ equal to $0,1,\infty$, respectively. Obviously, then,

$$j(J^+(\Gamma)) = 0 = j(J^-(\Gamma)).$$

$\boxed{\textbf{e2d12D3:}}$ Although the narrow class group of F is of cardinality 2, Proposition 2.6.2(ii) still shows that the groups $\mathrm{P}\mathcal{O}(1)^1$ and $\mathrm{P}\mathcal{O}(1)^+$ arising from maximal orders $\mathcal{O}(1)$ are all conjugate.

The group Γ is not contained in a triangle group. Indeed, if it were, it would be contained in a triangle group with signature $(0;2,4,12)$, because [Tak77] shows that this is the unique maximal arithmetic triangle group in this commensurability class up to conjugacy. Calculating covolumes gives that the corresponding cover would have degree 3, which manifestly cannot give rise to a group of signature $(1;2)$.

We settle for calculating the curve associated to $\Gamma^{(2)} = \mathcal{O}^1$, where $\mathcal{O}$ equals the order $\mathbf{Z}_F[\Gamma^{(2)}]$. Let $\mathcal{O}(1)$ be a maximal order containing $\mathcal{O}$. Then the cover

$$X(\mathcal{O}^1) \longrightarrow X(\mathcal{O}(1)^1)$$

has degree 6. [Tak77] shows that the signature of $X(\mathcal{O}(1)^1)$ equals $(0;2^3,6)$, and that the signature of $X(N(\mathcal{O}(1)))$ equals $(0;2,4,12)$.

In fact we have

$$\mathrm{P}N(\mathcal{O}(1)) = \mathrm{P}\mathcal{O}(1)^+$$

because both groups contain $\mathrm{P}\mathcal{O}(1)^1$ as a subgroup of index 2. Note that the Atkin-Lehner involution $w(\mathfrak{p}_3)$ is not in $N(\mathcal{O}(1))$, since $\mathfrak{p}_3$ is non-trivial in the narrow class group $\mathrm{Cl}(\infty)$.

Calculating the orders inbetween $\mathcal{O}$ and $\mathcal{O}(1)$, one shows that the level $\mathfrak{p}_2^4$ order $\mathcal{O}$, though non-Eichler itself, is contained in a level $\mathfrak{p}_2$ Eichler order $\mathcal{O}(\mathfrak{p}_2)$. [Voi09b] shows that $X(\mathcal{O}(\mathfrak{p}_2)^1)$ has signature $(0;2^6)$, and $X(\mathcal{O}^1)$ is a degree 2 genus 1 cover of this curve.

We now determine the two covers in the composition

$$X(\mathcal{O}^1) \longrightarrow X(\mathcal{O}(\mathfrak{p}_2)^1) \longrightarrow X(N(\mathcal{O}(1))).$$

As for the cover

$$X(\mathcal{O}(\mathfrak{p}_2)^1) \longrightarrow X(N(\mathcal{O}(1))), \tag{6.12}$$

its possible ramification types are $((2,1^4),(4,2),(6))$ and $((2^2,1^2),(2^3),(6))$. Algorithm 6.1.4 shows that latter of these types gives rise to a unique cover with trivial automorphism group. This cannot be the cover (6.12) because this factors through the quotient

$$X(\mathcal{O}(\mathfrak{p}_2)^1) \longrightarrow X(\mathcal{O}(\mathfrak{p}_2)^+)$$

which has degree 2, and hence is Galois, by Proposition 3.2.1. Therefore the ramification type of (6.12) equals $((2,1^4),(4,2),(6))$, to which there also corresponds a unique Belyĭ map. Putting the elliptic points of index $2,4,12$ at $1,0,\infty$, respectively, it is given by

$$z \longmapsto \frac{27}{4z(z-1)^2}.$$

As we have seen, the second cover

$$X(\mathcal{O}^1) \longrightarrow X(\mathcal{O}(\mathfrak{p}_2)^1)$$

is of degree 2. It has to ramify above 4 of the 6 elliptic points of $X(\mathcal{O}(\mathfrak{p}_2)^1)$. A priori, there are many possibilities for such a cover. However, by Lemma 3.3.2, the resulting curve of signature $(1;2^4)$ should have the property that all elliptic points differ by a 2-torsion point. It then turns out that up to automorphisms of $\mathbf{P}^1_{\mathbf{C}}$, there is only one quadruple of elliptic points that does the trick, given by the set of zeroes of $(z^2-1)(9z^2-4)$.

We obtain the degree 12 cover $X(\mathcal{O}^1) \to X(N(\mathcal{O}(1)))$ by composing the two covers above. It turns out that

$$j(J^+(\Gamma)) = j(J^+(\mathcal{O}^1)) = \frac{2^2 193^3}{3} = j(J^-(\mathcal{O}^1)) = j(J^-(\Gamma)).$$

$\boxed{\textbf{e2d81D1:}}$ We have $\Gamma = \mathcal{O}(\mathfrak{p}_2)^1$, where $\mathcal{O}(\mathfrak{p}_2) = \mathbf{Z}_F[\Gamma]$ is a level $\mathfrak{p}_2 = (2)$ Eichler order. Let $\mathcal{O}(1)$ be a maximal order containing $\mathcal{O}(\mathfrak{p}_2)$. We obtain a curve $X(\mathcal{O}(1)^1)$ of signature $(0;2,3,9)$. Perforce the cover

$$X(\mathcal{O}(\mathfrak{p}_2)^1) \longrightarrow X(\mathcal{O}(1)^1)$$

has ramification type $((2^4,1),(3^3),(9)$. Algorithm 6.1.4 shows that there is a unique cover with this ramification type. An explicit rational map was calculated by Sander Dahmen and is given by

$$(x,y) \longmapsto (Ay+B)/2^{23}$$

from the elliptic curve

$$y^2 = x^3 - 1515x - 46106.$$

Here

$$\begin{aligned} A &= x^3 - 9x^2 - 597x - 3851 \text{ and} \\ B &= -9x^4 + 132x^3 + 11250x^2 + 117108x + 218895. \end{aligned}$$

Another equation was determined in [Elk06]. Regardless, we get

$$j(J^+(\Gamma)) = \frac{-3^2 5^3 101^3}{2^{21}} = j(J^-(\Gamma)).$$

$\boxed{\textbf{e3d5D5:}}$ Because this Γ is the unique $(1;3)$-group for the quaternion algebra associated to it, $X^+(\Gamma) = X^-(\Gamma)$ has to be unique subordinate $(1;3)$-cover

$$X(\Gamma) \longrightarrow X(N(\mathcal{O}(1))).$$

of the signature $(0;2,3,10)$ curve $X(N(\mathcal{O}(1)))$. This cover has ramification type $((2^5),(3^3,1),(10))$. There is a unique Belyĭ map with this ramification type. As in the previous case, this cover was calculated by Sander Dahmen. It is given by

$$(x,y) \longmapsto (Ay + B)/2^8 3^{22} 5^5$$

from the elliptic curve

$$y^2 = x^3 - 3564675x - 4863773250.$$

Here

$$\begin{aligned} A &= 2^1 3^1 5^2 (-x^3 + 405x^2 + 1414125x + 405300375) \text{ and} \\ B &= -x^5 - 5475x^4 + 7206750x^3 + 19533521250x^2 \\ &\quad + 5715377971875x - 1221071756709375. \end{aligned}$$

We get

$$j(J^+(\Gamma)) = -\frac{5281^3}{3^{16}5} = j(J^-(\Gamma)).$$

$\boxed{\textbf{e3d5D9:}}$ Let $\mathcal{O}(\mathfrak{p}_2) = \mathbf{Z}_F[\Gamma^{(2)}]$. Then $\mathcal{O}(\mathfrak{p}_2)^1 = \langle \Gamma^{(2)}, AB \rangle$. As suggested by the notation, $\mathcal{O}(\mathfrak{p}_2)$ is a level $\mathfrak{p}_2 = (2)$ Eichler order. Also, $X(\Gamma) = X^-(\Gamma)$ is once more an Atkin-Lehner quotient of $X(\mathcal{O}(\mathfrak{p}_2)^1)$.

The group Γ is not contained in a triangle group. Indeed, if it were, it would be contained in a triangle group with signature $(0;2,5,6)$, because [Tak77] shows that this is the unique maximal triangle group in this commensurability class up to conjugacy. Calculating covolumes gives that the corresponding cover would have degree 5, which cannot give rise to a group of signature $(1;3)$.

We therefore consider the cover

$$X(\mathcal{O}(\mathfrak{p}_2)^1) \longrightarrow X(\mathcal{O}(1)^1)$$

for a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}(\mathfrak{p}_2)$. There is an Atkin-Lehner involution $w(\mathfrak{p}_3)$ acting on both $X(\mathcal{O}(\mathfrak{p}_2)^1)$ and $X(\mathcal{O}(1)^1)$, yielding a diagram

$$\begin{tikzcd}
X(\mathcal{O}(\mathfrak{p}_2)^1) \arrow[r, "2"] \arrow[d, "5"] & X(\mathcal{O}(\mathfrak{p}_2)^1)/w(\mathfrak{p}_3) \arrow[d, "5"] \\
X(\mathcal{O}(1)^1) \arrow[r, "2"] & X(\mathcal{O}(1)^1)/w(\mathfrak{p}_3)
\end{tikzcd}$$

Calculating signatures (we will discuss how to circumvent this step later), we get the diagram

$$\begin{tikzcd}
(1;3,3) \arrow[r, "2"] \arrow[d, "5"] & (0;2,2,6,6) \arrow[d, "5"] \\
(0;3,5,5) \arrow[r, "2"] & (0;2,5,6)
\end{tikzcd}$$

The map on the right of the diagram above is a Belyĭ map whose ramification type necessarily equals $((2^2,1),(5),(3,1^2))$. Algorithm 6.1.4 gives that there is a unique Belyĭ map with these indices: putting the elliptic points of index $2,5,6$ at $1,\infty,0$, respectively, it is given by

$$z \longmapsto 4z^3(36z^2+15z+10).$$

The elliptic points of the resulting cover are at

- The zeroes of $36z^2+15z+10$, giving the two elliptic points of index 6,
- The point 0, an elliptic point of index 2, and
- The simple zero $1/4$ of $4z^3(36z^2+15z+10)-1$, also of index 2.

One now recovers $X(\Gamma)$ as follows:

- Take the degree 2 cover ramifying above the four elliptic points given above to obtain $X(\mathcal{O}(\mathfrak{p}_2)^1)$:
- Then identify the two resulting elliptic points of index 3 by a 2-isogeny. Note that these elliptic points are simply the preimages of the zeroes of $36z^2+15z+10$.

We get

$$j(J^+(\mathcal{O}(\mathfrak{p}_2)^1)) = \frac{-269^3}{2^{10}3^5} = j(J^-(\mathcal{O}(\mathfrak{p}_2)^1))$$

and

$$j(J^+(\Gamma)) = \frac{7949^3}{2^5 3^{10}} = j(J^-(\Gamma)).$$

Note that we have seen these j-invariants before (at e2d5D4iii).

The signature calculation above is not essential for the argument. In fact, we have already excluded that $X(\mathcal{O}(\mathfrak{p}_2)^1)/w(\mathfrak{p}_3)$ has signature $(1;3)$. Apart from the signature $(0;2,2,6,6)$ above, then, only $(0;2^4,3)$ remains as a possibility.

Now although Proposition 6.1.6 cannot be used to exclude this possibility, a calculation of this cover yields that the two elliptic points on the resulting $(1;3,3)$-curve do not differ by a 2-torsion point. Hence this signature cannot be correct, and we can proceed as above.

e3d12D3: Let $\mathcal{O}(\mathfrak{p}_3) = \mathbf{Z}_F[\Gamma]^1$. Then $\Gamma = \mathcal{O}(\mathfrak{p}_3)^1$. Furthermore, $\mathcal{O}(\mathfrak{p}_3)$ is the unique level $\mathfrak{p}_3$ non-Eichler suborder of the maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$. We get a degree 4 Galois cover

$$X(\mathcal{O}(\mathfrak{p}_3)^1) \longrightarrow X(\mathcal{O}(1)^1) \longrightarrow X(N(\mathcal{O})) = X(\mathcal{O}(1)^+).$$

The curve $X(N(\mathcal{O}))$ has signature $(0;2,4,12)$ by [Tak77]. Hence, as in the case e2d8D2, this cover is explicitly realized by

$$(x,y) \longmapsto x^2$$

from the curve

$$y^2 = x^3 - x$$

if we set the x-coordinates of the elliptic points of order $2,4,12$ equal to $1,0,\infty$, respectively. Clearly

$$j(J^+(\Gamma)) = j(J^+(\mathcal{O}(\mathfrak{p}_3)^1) = 1728 = j(J^-(\mathcal{O}(\mathfrak{p}_3)^1) = j(J^-(\Gamma)).$$

e3d49D1: This case is analogous to the case e2d81D1. This time the cover

$$X(\Gamma) \longrightarrow X(\mathcal{O}(1)^1) = X(N(\mathcal{O}(1)))$$

has ramification type $((2^{14}),(3^9,1),(7^4))$. We postpone the determination of the curve $X^+(\Gamma) = X^-(\Gamma)$ to the next Chapter, due to the difficulty of the dessin involved.

e3d81D1: The $(1;e)$-group Γ can be described as $\Gamma = \mathcal{O}^1$, where $\mathcal{O} = \mathbf{Z}_F[\Gamma]$ is a level $\mathfrak{p}_3^3$ non-Eichler order. After choosing a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$, one calculates the orders inbetween $\mathcal{O}$ and $\mathcal{O}(1)$. This shows that in fact $\mathcal{O}$ is contained in a level $\mathfrak{p}_3$ Eichler order $\mathcal{O}(\mathfrak{p}_3)$. The tables in [Voi09b] show that $X(\mathcal{O}(\mathfrak{p}_3)^1)$ has signature $(0;3,3,9)$.

The map $X(\mathcal{O}^1) \longrightarrow X(\mathcal{O}(\mathfrak{p}_3)^1)$ is a Galois $\mathbf{Z}/3\mathbf{Z}$-cover, and can be calculated as in the case e2d12D2. We obtain

$$j(J^+(\Gamma)) = j(J^+(\mathcal{O})^1) = 0 = j(J^-(\mathcal{O})^1) = j(J^-(\Gamma)).$$

e4d8D2: The narrow class group of $F = \mathbf{Q}(w_2)$ is trivial for these three cases. The quaternion algebra B has $\mathfrak{D}(B)^f = \mathfrak{p}_2 = (w_2)$. As for e2d5D4, we start with some general considerations.

Preamble. The groups $\mathrm{P}\mathcal{O}(1)^1 = \mathrm{P}\mathcal{O}(1)^+$ coming from maximal orders $\mathcal{O}(1)$ of B are all conjugate by Proposition 2.6.2(ii). The signature of $\Delta = \mathrm{P}\mathcal{O}(1)^1$ equals $(0;3,3,4)$, and that of $\Delta' = N(\mathcal{O}(1))$ equals $(0;2,3,8)$ by [Tak77], which also shows that the latter group is a maximal triangle group.

There is one more conjugacy class of maximal triangle groups Δ'' in the commensurability class of Δ', which has signature $(0;2,6,8)$. As in the case e2d5D4, using Theorem 6.1.7, we will try to construct $(1;4)$-curves in this commensurability class by taking subordinate covers of these triangle curves.

First consider the triangle group Δ of signature $(0;3,3,4)$. Calculating covolumes and using Theorem 6.1.7, one sees that a cover

$$X(\Gamma) \longrightarrow X(\Delta)$$

of this curve by a $(1;4)$-curve necessarily has degree equal to 9. Also, the ramification type is forced: it has to equal $((3^3),(3^3),(4^2,1))$. Algorithm 6.1.4 shows that there are two Belyĭ maps with this ramification type, and their automorphism groups have cardinality 2.

Now consider the triangle group $\Delta' \supset \Delta$ of signature $(0;2,3,8)$. A covolume calculation shows that subordinate covers

$$X(\Gamma) \longrightarrow X(\Delta')$$

of the corresponding curve by $(1;4)$-curves will have to be of degree 18. The ramification type of these covers is uniquely determined: explicitly, it is given by $((2^9),(3^6),(8^2,2))$.

The two covers of $X(\Delta)$ constructed above will give rise to covers of $X(\Delta')$ by composing with the degree 2 map $X(\Delta) \to X(\Delta')$. A formula in Section 7.2 of [Ser92] now shows that these are the only two possible covers. Indeed, let S be the set of covers whose ramification type equals $((2^9),(3^6),(8^2,2))$. Then

$$\sum_{(X,f)\in S} \frac{1}{\mathrm{Aut}(X,f)} = \frac{|C_2||C_3||C_8|}{|S_{18}|^2} \sum_{\chi} \frac{\chi(C_2)\chi(C_3)\chi(C_8)}{\chi(1)} = 1,$$

Here C_2, C_3, C_8 are the conjugacy classes in S_{18} corresponding to the tuples $(2^9),(3^6),(8^2,2)$ in the ramification type above, and χ runs over the characters of the irreducible representations of S_{18}.

The two covers constructed using Δ do not become isomorphic after composing with the map $X(\Delta) \to X(\Delta')$, as will follow from the explicit calculation in the case e4d8D2ii. This can also be shown by drawing the associated *dessins d'enfants* (see [Cou94]).

As no Belyĭ map of ramification type $((2^9),(3^6),(8^2,2))$ can have more than two automorphisms by Proposition 6.1.3(v) (also see the reasoning in the case e2d5D4iii), we see that no other covers of this type can arise other than the two already found.

Finally, by considering covolumes, one shows that there are no subordinate covers of the curve $X(\Delta'')$ by $(1;4)$-curves.

Again, for reasons that will become clear, we will now treat these three cases in a different order than that of Table A.2.

$\boxed{\textbf{e4d8D2i/iii:}}$ These two cases give rise to Galois conjugate curves by Theorem 3.1.7. So let us consider the first one. We then have $\langle \Gamma^{(2)}, A \rangle = \mathcal{O}(\mathfrak{p}_{17})^1$, where $\mathcal{O}(\mathfrak{p}_{17}) = \mathbf{Z}_F[\Gamma^{(2)}]$ is a level $\mathfrak{p}_{17}$ Eichler order for one of the two primes $\mathfrak{p}_{17}$ of F above 17. Let $\mathcal{O}(1)$ be a maximal order containing $\mathcal{O}(\mathfrak{p}_{17})$. We get a cover

$$X(\mathcal{O}(\mathfrak{p}_{17})^1) \longrightarrow X(\mathcal{O}(1)^1)$$

of degree 18. As usual, $X(\Gamma)$ is an Atkin-Lehner quotient of $X(\mathcal{O}(\mathfrak{p}_{17})^1)$. In particular, as in the case e2d5D4iii, we see that $\mathrm{P}\Gamma$ is not contained in $\mathrm{P}\mathcal{O}(1)^1$. Hence by the preamble, there is no inclusion of Γ in a triangle group.

The cover obtained above has trivial automorphism group, which makes it rather hard to calculate. In the next Chapter, we will find an equation for the curve $X^+(\mathcal{O}(\mathfrak{p}_{17})^1) \cong X^-(\mathcal{O}(\mathfrak{p}_{17})^1)$ using modular methods.

$\boxed{\textbf{e4d8D2ii:}}$ We have $\Gamma \subsetneq \mathcal{O}(1)^1$, where $\mathcal{O}(1)$ is the maximal order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$. By elimination, this case has to correspond to the two covers of $X(\mathcal{O}(1)^1)$ with ramification type $((3^3), (3^3), (4^2, 1))$.

Let $a \in \{\pm 1\}$. As for the case e2d5D4ii, taking Γ to be generated by a standard pair (A, B) and letting

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

there is a descent

$$\begin{tikzcd} X^a(\Gamma) \arrow[r, "2"] \arrow[d, "9"] & X^a(\langle \Gamma, S \rangle) \arrow[d, "9"] \\ X(\mathcal{O}(1)^1) \arrow[r, "2"] & X(N(\mathcal{O}(1))) \end{tikzcd} \tag{6.13}$$

whose diagram of signatures has to equal

$$\begin{tikzcd} (1;4) \arrow[r, "2"] \arrow[d, "9"] & (0;2,2,2,8) \arrow[d, "9"] \\ (0;3,3,4) \arrow[r, "2"] & (0;2,3,8) \end{tikzcd}$$

A way to derive the descent (6.13) without using the explicit matrix S is as follows. Using Algorithm 6.1.4, one checks that there are exactly two subordinate covers

$$X_1, X_2 \longrightarrow X(N(\mathcal{O}(1))) = X(\Delta')$$

by curves X_i of signature $(0;2,2,2,8)$: both of these covers have ramification type $((2^3, 1^3), (3^3), (8, 1))$. (Note that a priori, $((2^4, 1), (3^3), (4^2, 1))$ is also possible, but Algorithm 6.1.4 also shows that there is no Belyĭ map with this ramification type.) Consequently, we know that the curves $X^a(\langle \Gamma, S \rangle)$ are given by X_1 and X_2.

We saw in the preamble that there were also two subordinate $(1;4)$-covers of $X(\Delta)$, which have to be given by

$$X^a(\Gamma) \longrightarrow X(\Delta'). \tag{6.14}$$

There is no other possibility than that these are the two covers obtained by composing the covers $X_i \to X(\Delta')$ with the degree 2 Galois covers ramifying above the 4 elliptic points of the X_i. Now the preamble shows that the two covers in (6.14) factor through the cover $X(\Delta') \to X(\Delta)$, whence the descent (6.13).

Explicitly, placing the elliptic points of order $2, 3, 8$ at $1, 0, \infty$, the Belyĭ maps with ramification type $((2^3, 1^3), (3^3), (8, 1))$ are given by the two conjugate covers

$$z \longmapsto \frac{(z^3 + 24z^2 + 12(11 \pm w)z + 8(5 \pm w))^3}{177147(7 \pm 4w)z}.$$

where $w = w_{-2}$. One checks that these covers are not isomorphic because Proposition 6.1.3 shows that such an isomorphism would have to fix the branch points 0 and ∞ in the fiber over ∞, hence would be given by scalar multiplication, which is easily ruled out.

We can now recover the curves $X^a(\Gamma)$ by taking the degree 2 elliptic cover ramified above

- The unique elliptic point of order 8 given by 0, and
- The 3 elliptic points of order 2 given by the simple preimages of 1, or more explicitly by the zeroes of $z^3 + 42z^2 + 3(191 \pm 10w)z + 512(5 \pm w)$.

We get the two conjugate j-invariants

$$j(J^{\pm}(\Gamma)) = \frac{119421866 \pm 241123607w}{2^{14}}$$

of norm $3^1 11^3 41^3 691^3 / 2^{27}$. Note that these j-invariants also show that the two covers above can not be isomorphic.

e4d2304D2: We have an equality $\Gamma = \mathcal{O}(\mathfrak{p}_2)^1$, where $\mathcal{O}(\mathfrak{p}_2) = \mathbf{Z}_F[\Gamma]$ is a level $\mathfrak{p}_2$ non-Eichler order. As in the case e2d12D2, we get

$$j(J^+(\Gamma)) = 0 = j(J^-(\Gamma)).$$

e5d5D5: The narrow class group of $F = \mathbf{Q}(w_5)$ is trivial, and B has $\mathfrak{D}(B)^f = \mathfrak{p}_5 = (w_5)$. There are three $(1;5)$-groups in the corresponding commensurability class.

Preamble. The groups $\mathrm{P}\mathcal{O}(1)^1 = \mathrm{P}\mathcal{O}(1)^+$ coming from maximal orders $\mathcal{O}$ in B are all conjugate by Proposition 2.6.2(ii). By [Tak77], the signature of the groups $\mathcal{O}(1)^1$ equals $(0;3,3,5)$, and that of the $N(\mathcal{O})$ equals $(0;2,3,10)$. [Tak77] also shows that the latter groups are maximal triangle groups, and in fact the only maximal triangle groups in this commensurability class up to conjugacy.

As before, we can construct $(1;5)$-curves by taking subordinate covers

$$X(\Gamma) \longrightarrow X(N(\mathcal{O})). \tag{6.15}$$

Calculating covolumes gives that these covers have degree equal to 12. The ramification type is also forced: it has to equal $((2^6),(3^4),(10,2))$. There exists a unique Belyĭ map with this ramification type by Algorithm 6.1.4.

Analogously, one shows that the subordinate covers

$$X(\Gamma) \longrightarrow X(\mathcal{O}^1) \tag{6.16}$$

have ramification type given by $((3^2),(3^2),(5,1))$. Again there exists unique Belyĭ map with this ramification type. Therefore, the cover (6.15) will factor through (6.16).

As usual, we calculate the cases in an order differing from that of Table A.2.

$\boxed{\textbf{e5d5D5iii:}}$ We have $\Gamma \subsetneq \mathcal{O}(1)^1$, where $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma]$ is a maximal order. In particular, we obtain a cover

$$X(\Gamma) \longrightarrow X(\mathcal{O}(1)^1).$$

This cover has to correspond to the cover with ramification $((3^2),(3^2),(5,1))$ described in the preamble. We have the usual diagram as in the case e2d5D4ii:

$$\begin{tikzcd}
X(\Gamma) \arrow[r, "2"] \arrow[d, "6"] & X(\langle\Gamma,S\rangle) \arrow[d, "6"] \\
X(\mathcal{O}^1) \arrow[r, "2"] & X(N(\mathcal{O}))
\end{tikzcd}$$

whose diagram of signatures equals

$$\begin{tikzcd}
(1;5) \arrow[r, "2"] \arrow[d, "6"] & (0;2,2,2,10) \arrow[d, "6"] \\
(0;3,3,5) \arrow[r, "2"] & (0;2,3,10)
\end{tikzcd}$$

This also follows from the uniqueness in the preamble along with the existence of a degree 6 cover of $X(N(\mathcal{O}))$ of signature $(0;2,2,2,10)$, which follows from Algorithm 6.1.4.

The ramification type of the cover

$$X(\langle\Gamma,S\rangle) \longrightarrow X(N(\mathcal{O}))$$

equals $((2^2,1^2),(3^2),(5,1))$. The unique corresponding Belyĭ map is given by

$$z \longmapsto -\frac{(z^2-10z+5)^3}{1728z}$$

if we place the elliptic points of index $2,3,10$ at $1,0,\infty$.

To recover $X(\Gamma)$, one takes a degree 2 cover ramified above

- The simple point $z = 0$ above ∞, which is elliptic of order 10;
- The simple point $z = \infty$ above ∞, which is elliptic of order 2; and
- The simple preimages of 1, which are elliptic of order 2 and given by the simple roots of $(z^2 - 10z + 5)^3 = -1728z$, that is, the zeroes of $z^2 - 22z + 125$.

One ends up with

$$j(J^+(\Gamma)) = \frac{-2^4 109^3}{5^6} = j(J^-(\Gamma)).$$

$\boxed{\textbf{e5d5D5i/ii:}}$ These two cases are Galois conjugate (*cf.* Theorem 3.1.7). One has $\langle \Gamma^{(2)}, B \rangle = \mathcal{O}(\mathfrak{p}_{11})^1$, where $\mathcal{O}(\mathfrak{p}_{11}) = \mathbf{Z}_F[\Gamma]$ is a level $\mathfrak{p}_{11}$ Eichler order. Let $\mathcal{O}(1)$ be a maximal order containing $\mathcal{O}(\mathfrak{p}_{11})$. We obtain a degree 12 cover

$$X(\mathcal{O}(\mathfrak{p}_{11})^1) \longrightarrow X(\mathcal{O}(1)^1)$$

whose monodromy group is of order 660 according to Algorithm 6.1.7. As usual, $X(\Gamma)$ is an Atkin-Lehner quotient of $X(\mathcal{O}(\mathfrak{p}_{11}))$.

Descending by the Atkin-Lehner involution $\iota(\mathfrak{p}_5)$, we get a diagram

$$\begin{tikzcd}
X(\mathcal{O}(\mathfrak{p}_{11})^1) \arrow[r, "2"] \arrow[d, "12"] & X(\mathcal{O}(\mathfrak{p}_{11})^1)/w(\mathfrak{p}_5) \arrow[d, "12"] \\
X(\mathcal{O}(1)^1) \arrow[r, "2"] & X(\mathcal{O}(1)^1)/w(\mathfrak{p}_5)
\end{tikzcd}$$

whose diagram of signatures can be calculated to equal

$$\begin{tikzcd}
(1;5,5) \arrow[r, "2"] \arrow[d, "12"] & (0;2,2,10,10) \arrow[d, "12"] \\
(0;3,3,5) \arrow[r, "2"] & (0;2,3,10)
\end{tikzcd} \tag{6.17}$$

Alternatively, [Tak77] shows that

$$X(\mathcal{O}(1)^1)/w(\mathfrak{p}_5) = X(N(\mathcal{O}(1)))$$

has signature $(0;2,3,10)$. This enables us to exclude the other two a priori possible signatures $(1;5)$ and $(0;2,2,2,2,5)$ of $X(\mathcal{O}(\mathfrak{p}_{11})^1)/w(\mathfrak{p}_5)$. Indeed, Algorithm 6.1.4 shows that there exist Belyĭ maps for both of these ramification types, but none of them has monodromy group of order 660 or 1320, as demanded by Proposition 6.1.6.

The ramification type of the cover on the right of diagram (6.17) is necessarily given by $((2^5,1^2),(3^4),(10,1^2))$. Algorithm 6.1.4 gives that there are 4 Belyĭ maps with this ramification type. Two of these have monodromy group of order 1320; for the other two, this order is 3840. Therefore we are interested in the former pair. These two pairs of Belyĭ maps are also distinguished by the fact that the Belyĭ maps (X, f) in the former pair have $|\mathrm{Aut}(X, f)| = 1$ while those in the latter have $|\mathrm{Aut}(X, f)| = 2$. As we shall see presently, the former pair consists of two conjugate Belyĭ maps realizing the cases e5d5D5i and e5d5D5ii.

Placing the elliptic points of order $2, 3, 10$ at $1, 0, \infty$, respectively, we claim that the former pair of Belyĭ maps is given by

$$z \longmapsto \frac{44281^5 f_4^3}{6912(164w_5 - 587)^5 C(z^2 - 500w_5 + 875)}$$

and its conjugate. Here

$$\begin{aligned} f_4 &= z^4 + 10z^3 + 1160z^2 + 17550z + 326175 - 20w_5(z^3 + 31z^2 + 585z + 9915), \\ C &= 22329243084308461356w_5 - 3603199856376900322. \end{aligned}$$

One checks that this Belyĭ map indeed has trivial automorphism group. Indeed, Proposition 6.1.3(v) gives that an automorphism would have to fix ∞ since it is the only point ramifying of order 10, and it would have to exchange the other two points in the fiber above ∞, given by the zeroes of $z^2 - 500w_5 + 875$. This determines a unique automorphism of $\mathbf{P}^1_{\mathbf{C}}$. One verifies that it does not yield an automorphism of the Belyĭ map above. A similar calculation shows that this cover is not isomorphic to its Galois conjugate.

$X(\mathcal{O}(\mathfrak{p}_{11})^1)$ can be recovered from this by taking the degree 2 cover ramifying above

- The elliptic points of order 10, given by the zeroes of $z^2 - 500w_5 + 875$;
- And the simple preimages of 1, given by the zeroes of $z^2 + (16 - 32w_5)z + (587 - 164w_5)$.

We obtain

$$j(J^+(\mathcal{O}(\mathfrak{p}_{11})^1)) = \frac{1485675267531w_5 + 2666389392178}{5^3 11^6} = j(J^-(\mathcal{O}(\mathfrak{p}_{11})^1))$$

and, identifying the elliptic points of order 5 on this curve,

$$j(J^+(\Gamma)) = \frac{4560282420936767w_5 + 2818578140804845}{5^6 11^3} = j(J^-(\Gamma)),$$

whose respective norms equal $19^3 90019^3 / 5^6 11^6$ and $59^3 167809^3 / 5^{12}$.

$\boxed{\textbf{e5d5D9:}}$ For this case, $\langle \Gamma^{(2)}, AB \rangle = \mathcal{O}(\mathfrak{p}_5)^1$ where $\mathcal{O}(\mathfrak{p}_5) = \mathbf{Z}_F[\Gamma^{(2)}]$ is a level $\mathfrak{p}_5$ Eichler order. Let $\mathcal{O}(1)$ be a maximal order containing $\mathcal{O}(\mathfrak{p}_5)$. This order gives rise to a cover

$$X(\mathcal{O}(\mathfrak{p}_5)^1) \longrightarrow X(\mathcal{O}(1)^1)$$

having degree equal to 6 and monodromy group of order 60. Once again $X(\Gamma)$ is an Atkin-Lehner quotient of $X(\mathcal{O}(\mathfrak{p}_5)^1)$.

Descending by the Atkin-Lehner involution $w(\mathfrak{p}_3)$, we get a diagram

$$\begin{tikzcd}
X(\mathcal{O}(\mathfrak{p}_5)^1) \arrow[r, "2"] \arrow[d, "6"] & X(\mathcal{O}(\mathfrak{p}_5)^1)/w(\mathfrak{p}_3) \arrow[d, "6"] \\
X(\mathcal{O}^1) \arrow[r, "2"] & X(N(\mathcal{O}(1)))
\end{tikzcd}$$

whose diagram of signatures can be calculated to equal

$$\begin{tikzcd}
(1;5,5) \arrow[r, "2"] \arrow[d, "6"] & (1;5) \arrow[d, "6"] \\
(0;3,5,5) \arrow[r, "2"] & (0;2,5,6)
\end{tikzcd}$$

One can dispense with this signature calculation by using a uniqueness argument: indeed, $X(\Gamma)$ is the only $(1;5)$-curve in its commensurability class.

The cover on the right has ramification type $((2^3),(5,1),(6))$, and is determined by these indices by Algorithm 6.1.4. It is given by

$$(x,y) \longmapsto \frac{2^2}{5^5}(9xy - x^3 - 15x^2 - 36x + 32)$$

from the curve

$$y^2 + xy + y = x^3 + x^2 + 35x - 28.$$

One deduces that

$$j(J^+(\Gamma)) = \frac{23^3 73^3}{3^2 5^8} = j(J^-(\Gamma)).$$

$\boxed{\textbf{e5d1125D5:}}$ We have $\Gamma = \mathcal{O}(\mathfrak{p}_5)^1$, where $\mathcal{O}(\mathfrak{p}_5) = \mathbf{Z}_F[\Gamma]$ is a level $\mathfrak{p}_5$ non-Eichler order. As in the case e2d12D2, we obtain

$$j(J^+(\Gamma)) = 0 = j(J^-(\Gamma)).$$

$\boxed{\textbf{e7d49D1:}}$ We have $\langle \Gamma^{(2)}, AB \rangle = \mathcal{O}(\mathfrak{p}_2\mathfrak{p}_7)^1$, where $\mathcal{O}(\mathfrak{p}_2\mathfrak{p}_7) = \mathbf{Z}_F[\Gamma^{(2)}]$ is a level $\mathfrak{p}_2\mathfrak{p}_7$ Eichler order. Let $\mathcal{O}(1)$ be a maximal order containing $\mathcal{O}(\mathfrak{p}_2\mathfrak{p}_7)$. We obtain a cover

$$X(\mathcal{O}(\mathfrak{p}_2\mathfrak{p}_7)^1) \longrightarrow X(\mathcal{O}(1)^1)$$

for which the codomain $X(\mathcal{O}(1)^1)$ has signature $(0;2,3,7)$. Though a Belyĭ map, this cover has degree 72 and a small automorphism group, making it quite intractable.

However, [Tak77] shows that the commensurability class of Γ also contains a triangle group Δ of signature $(0;2,4,7)$. This group allows a degree 8 cover

$$X(\Gamma) \longrightarrow X(\Delta)$$

which is uniquely determined by its ramification type $((2^4),(4^2),(7,1))$. As the notation suggests, this cover has to equal the requested arithmetic $(1;7)$-curve by uniqueness.

This Belyĭ map was computed by Frits Beukers. It is given by

$$(x,y) \longmapsto \frac{C_0 + C_1 y}{D}$$

from the curve

$$y^2 = (x+78)(x^2-78x-39951)$$

if we place the elliptic points of order $2,4,7$ at $1,0,\infty$, respectively. Here

$$\begin{aligned} C_0 &= x^3 - 405x^2 + 6291x + 3297321, \\ C_1 &= -3(7x^4 - 3108x^3 + 9450x^2 + 62545500x + 3089292615), \\ D &= 2^{15}3^7(x-363). \end{aligned}$$

We get

$$j(J^+(\Gamma)) = \frac{5^3 11^3 31^3}{2^3 7^6} = j(J^-(\Gamma)).$$

$\boxed{\textbf{e11d14641D1:}}$ One has the equality $\Gamma = \mathcal{O}(\mathfrak{p}_{11})^1$, where $\mathcal{O}(\mathfrak{p}_{11}) = \mathbf{Z}_F[\Gamma]$ is a level $\mathfrak{p}_{11}$ Eichler order. The inclusion of $\mathcal{O}(\mathfrak{p}_{11})$ into a maximal order $\mathcal{O}(1)$ gives rise to a degree 12 cover

$$X(\mathcal{O}(\mathfrak{p}_{11})^1) \longrightarrow X(\mathcal{O}^1).$$

Since the latter curve has signature $(0;2,3,11)$, the ramification type of this subordinate cover is forced and equals $((2^6),(3^4),(11,1))$. Algorithm 6.1.4 shows that there is a unique cover with this ramification, and it is isomorphic over F to the classical modular cover $X_0(11) \to X_0(1)$. We forgo the calculation of this cover, since this can be done using classical modular methods (for example, by using q-expansions). For use in the next Chapter, it suffices to remark that since $X(\mathcal{O}(\mathfrak{p}_{11})^1)$ is geometrically isomorphic to the strong Weil curve of conductor 11, one has

$$j(J^+(\Gamma)) = j(J^+(\mathcal{O}(\mathfrak{p}_{11})^1)) = \frac{-2^{12}31^3}{11^5} = j(J^-(\mathcal{O}(\mathfrak{p}_{11})^1)) = j(J^-(\Gamma)).$$

The rational cases. There are 4 cases where B has center $\mathbf{Q}$. We refer to [Elk98] and [GR06] for the cases e2d1D6i and e3d1D6i. Using [GR06], we determine the two remaining cases e2d1D6ii and e3d1D6ii:

$\boxed{\textbf{e2d1D6ii:}}$ The order $\mathcal{O} = \mathbf{Z}[\Gamma^{(2)}]$ is of level 2^3 and non-Eichler, with $\Gamma^{(2)} = \mathcal{O}^1$. The group Γ is not a subgroup of the group $\mathcal{O}(1)^1$ associated to the unique maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$. However, the group $\Delta = N(\mathcal{O}(1))$ has signature $(0;2,4,6)$. There is a unique subordinate cover

$$X(\Gamma') \longrightarrow X(\Delta) \tag{6.18}$$

for which $X(\Gamma')$ has signature $(1;2)$. Its ramification type is $((2^3),(4,2),(6))$.

We claim that Γ' equals Γ. Indeed, if it did not, then it would have to come from the case e2d1D6i, and hence would correspond to a subgroup of the normalizer $N(\mathcal{O}(5))$ of the level 5 Eichler order $\mathcal{O}(5)$ obtained in that case. However, [GR06] shows that the unique subgroup of $N(\mathcal{O}(5))$ having signature $(1;2)$ is not a subgroup of Δ. Alternatively, one can of course compare the j-invariant obtained in the next paragraph with the one obtained in [GR06] for the case e2d1D6i.

The subordinate cover (6.18) is in [Bir94]: putting the elliptic points of index $2,4,6$ at $4,0,\infty$, it is given by

$$(x,y) \longmapsto (x-1)^2(x+2)$$

from the elliptic curve

$$y^2 = (x-1)(x-2)(x+2).$$

We get

$$j(J^+(\Gamma)) = \frac{2^4 13^3}{3^2} = j(J^-(\Gamma)).$$

$\boxed{\textbf{e3d1D6ii:}}$ This case is completely analogous to the previous. In this case, Γ gives rise to a subordinate cover

$$X(\Gamma) \longrightarrow X(\Delta) \tag{6.19}$$

with ramification type $((2^4),(4^2),(6,2))$. By Algorithm 6.1.4, there is a unique cover with this ramification type. It has automorphism group $\mathbf{Z}/2\mathbf{Z}$, and decomposes as a degree 2 genus 1 cover of the (see [Bir94]) unique genus 0 cover whose ramification type equals $((2,1,1),(4),(3,1))$.

We omit the details, familiar by now: putting the elliptic points of index $2,4,6$ at $-27,\infty,0$, respectively, we end up with the cover

$$(x,y) \longmapsto x$$

from the genus 1 curve

$$y^2 = (x+3)^3(x-1),$$

and

$$j(J^+(\Gamma)) = \frac{2^1 47^3}{3^8} = j(J^-(\Gamma)).$$

Chapter 7

Equations

In the first section of this Chapter, we use the machinery we have developed in the previous Chapters to find explicit equations defining canonical models of the elliptic curves $J(\Gamma)$. Some of these equations are obtained heuristically: the second section discusses results from the theory of Hilbert modular forms that can be used to prove the correctness of the corresponding models.

7.1 The models

Let Γ be an arithmetic $(1;e)$-group, let $J(\Gamma)$ be as in (3.22), and let $E(\Gamma)$ be a canonical model of $J(\Gamma)$ (as in Definition 3.3.3). This section is dedicated to determining equations for $E(\Gamma)$ by combining the information obtained in the previous Chapters, namely

- The canonical field of definition of $E(\Gamma)$ (using Algorithm 2.4.3);
- The field generated by $j(E(\Gamma))$ (using Theorem 3.1.7);
- The reduction properties of $E(\Gamma)$ (Theorem 3.1.6);
- The traces of Frobenius of $E(\Gamma)$ (Algorithm 4.2.1);
- The valuations of $j(E(\Gamma))$ at the ramifying primes of the quaternion algebra associated to Γ (using Proposition 5.1.12); and, if applicable,
- The value of $j(E(\Gamma))$ obtained in Chapter 6.

When the canonical field of definition is small, we will often give the candidates in explicit minimal Weierstrass form; over larger fields, we either specify them by giving their j-invariant and conductor or as twists of suitable curves over smaller fields. We use the algebraic integers α from Table A.1 and retain the notation w_d from the beginning of Section 6.2 and $\mathrm{e}n_e\,\mathrm{d}n_d\,\mathrm{D}n_D\,\mathrm{r}$ from the appendix. Moreover, whenever we say that two curves over a common ground field are isomorphic or isogenous, the corresponding map is defined over this same ground field.

For the sake of completeness, we have, without proofs, included the cases with ground field $\mathbf{Q}$ that can be found in [Elk98] and [GR06]. The remaining rational cases e2d1D6ii and e3d1D6ii over $\mathbf{Q}$ give rise to canonical models of $(1;e)$-curves that seem to be new.

$\boxed{\textbf{e2d1D6i:}}$ If we let $\mathcal{O}(5)$ be the order $\mathbf{Z}[\Gamma^{(2)}]$, then $\Gamma^{(2)} = \mathcal{O}(5)^1$. The order $\mathcal{O}(5)$ is of index 5 in a maximal order containing it. Therefore it is a level 5 Eichler order by Proposition 2.2.3. As such, the $(1;2)$-curve

$$X(\Gamma^{(2)}) = X(\mathcal{O}(5)^1)$$

has a canonical model given by the Shimura curve $\mathrm{Sh}_0(\mathcal{O}(5))$, which is canonically defined over $\mathbf{Q}_\infty = \mathbf{Q}$ by Proposition 2.4.2.

Since all Atkin-Lehner involutions of $\mathrm{Sh}_0(\mathcal{O}(5))$ are also defined over $\mathbf{Q}$ by Theorem 3.1.2(iii), the Jacobian $J_0(\mathcal{O}(5))$ is a canonical model of $J(\Gamma)$ by Lemma 3.3.2 and Lemma 3.3.4.

The elliptic curve $J_0(\mathcal{O}(5))$ was determined in [Elk98] and [GR06] and is the unique elliptic curve over $\mathbf{Q}$ with j-invariant $7^3 2287^3/2^6 3^2 5^6$ and conductor 30. An explicit equation is given by

$$y^2 + xy + y = x^3 - 334x - 2368.$$

In fact, we can say a bit more about this case. We can equally well construct a canonical model of $X(\Gamma)$ instead of just $J(\Gamma)$ by taking a suitable Atkin-Lehner quotient of the canonical model $\mathrm{Sh}(\mathcal{O}(5))$ of $X(\Gamma^{(2)})$ determined in [GR06].

Since the set of elliptic points of $\mathrm{Sh}(\mathcal{O}(5))$ is invariant under the action of $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$, the unique elliptic point on the resulting model of $X(\Gamma)$ is rational. Therefore the elliptic curve given above is actually a canonical model of $X(\Gamma)$ as well.

We will not consider whether or not the canonical model of $X(\Gamma)$ has a rational point in the subsequent considerations. It is certainly likely that its elliptic point is rational. See [GR06] for a discussion of these matters when K is of the form $\widehat{\mathcal{O}}^\times$ and F has trivial narrow class group.

$\boxed{\textbf{e2d1D6ii:}}$ We know the value of $j(J(\Gamma))$ from Chapter 6, where it was also mentioned that $\Gamma^{(2)}$ generates a level 2^3 non-Eichler order $\mathcal{O} = \mathbf{Z}[\Gamma^{(2)}]$ with $\Gamma^{(2)} = \mathcal{O}^1$.

There is a unique maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$ since the prime 2 divides the discriminant of the quaternion algebra B associated to Γ. (Explicitly, such an order can be determined using the `Magma` function `MaximalOrder`.) As $\mathbf{Z}$-modules, we have

$$\mathcal{O}(1)/\mathcal{O} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}.$$

Algorithm 2.4.3 gives

$$\mathrm{nrd}(\widehat{\mathcal{O}}^\times) = U_2^{(2)} \times \prod_{p \neq 2} U_{\mathfrak{p}}^{(0)},$$

which means that the canonical field of definition of the canonical model $J_0(\mathcal{O})$ of $J(\Gamma)$ equals the non-trivial ray class extension $\mathbf{Q}_{4\infty} = \mathbf{Q}(i)$ of $\mathbf{Q}$. However, if we let

$$\mathcal{O}' = \mathcal{O} + 2\mathcal{O}(1),$$

then $\mathcal{O}'$ is an order with the property $\mathfrak{p}_2\mathcal{O}(1) \subset \mathcal{O}$. We have studied such orders locally in Proposition 2.3.2. In this case

$$\mathcal{O}(1)/\mathcal{O}' \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

Moreover, Algorithm 6.1.7 shows that

$$[\mathcal{O}(1)^1 : \mathcal{O}'^1] = [\mathcal{O}(1)^1 : \mathcal{O}^1],$$

so in fact $\mathcal{O}'^1 = \mathcal{O}^1$. By Corollary 2.5.5, the fact (see Table A.2) that the common index above equals 6 shows that we are in case (iv) of Proposition 2.3.2. The unique order $\mathcal{O}''$ inbetween $\mathcal{O}'$ and $\mathcal{O}(1)$ gives rise to a genus 0 Galois cover.

The elements of Γ normalize the order $\mathcal{O} = \mathbf{Z}[\Gamma^{(2)}]$, hence as we saw in Lemma 3.3.4, the corresponding involutions of $J_0(\mathcal{O})$ can also be obtained by conjugation with elements of $B^\times$. These global elements will normalize the two-sided ideal $2\mathcal{O}(1)_2$ of the unique local maximal order $\mathcal{O}(1)_2$ at 2, hence $\mathcal{O}'$ as well by the local-global correspondence (Theorem 2.1.4). In other words, the elements of Γ also normalize the order $\mathcal{O}'$.

Therefore, by Lemma 3.3.4, a canonical model of $J(\Gamma)$ can also be obtained by taking a $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ Atkin-Lehner quotient of $J_0(\mathcal{O}')$, which will actually be isomorphic to $J_0(\mathcal{O}')$ by Lemma 3.3.2. Since $U_2^{(1)} U_2^2 = \mathbf{Z}_2^\times$, Proposition 2.3.2 gives that $\mathrm{nrd}(\widehat{\mathcal{O}}'^\times) = \widehat{\mathbf{Z}}^\times$. As a result, the canonical model $J_0(\mathcal{O}') = J(\mathcal{O}')$ is defined over $\mathbf{Q}_\infty = \mathbf{Q}$.

By Theorem 3.1.6, we can narrow down the possibilities for $J_0(\mathcal{O}')$ to the 8 elliptic curves over $\mathbf{Q}$ with j-invariant $2^4 13^3/3^2$ having good reduction outside the primes 2 and 3. The traces obtained from Algorithm 4.2.1 then give that the canonical model $J_0(\mathcal{O}')$ is isomorphic to the elliptic curve

$$y^2 = x^3 - x^2 - 4x + 4,$$

the strong Weil curve of conductor 24.

$\boxed{\textbf{e2d1D14:}}$ One has $\langle \Gamma^{(2)}, AB \rangle = \mathbf{Z}[\Gamma^{(2)}]^1$, and the order $\mathbf{Z}[\Gamma^{(2)}]$ is maximal. By [GR06], the resulting canonical model of the Atkin-Lehner quotient $X(\Gamma)$ is given by the unique elliptic curve over $\mathbf{Q}$ with j-invariant $5^3 11^3 31^3/2^3 7^6$ and conductor 14. An explicit equation is given by

$$y^2 + xy + y = x^3 - 36x - 70.$$

$\boxed{\textbf{e2d5D4i:}}$ We know the value of $j(J(\Gamma))$ from Chapter 6. We will now realize $J(\Gamma)$ as an Atkin-Lehner quotient of a Jacobian of a Shimura curve.

Recall that $\Gamma^{(2)}$ generates a level $\mathfrak{p}_2^2$ non-Eichler order $\mathcal{O} = \mathbf{Z}[\Gamma^{(2)}]$ with norm 1 group $\Gamma^{(2)}$. The maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$ has the property that

$\mathfrak{p}\mathcal{O}(1) \subset \mathcal{O}$ and $\mathcal{O}(1)/\mathcal{O} \cong (\mathbf{Z}_F/\mathfrak{p}_2)^2$. Using Table A.2 and Corollary 2.5.5, we see that we are in case (iv) of Proposition 2.3.2. Again, there is a unique level $\mathfrak{p}_2$ order $\mathcal{O}'$ inbetween $\mathcal{O}$ and $\mathcal{O}(1)$, which gives rise to a degree 5 and genus 0 Galois cover of $X(\mathcal{O}(1)^1)$.

Since $\mathfrak{p}_2$ is even, we have $U_{\mathfrak{p}_2}^{(1)} U_{\mathfrak{p}_2}^2 = \mathbf{Z}_{F,\mathfrak{p}_2}^\times$, hence $\mathrm{nrd}(\widehat{\mathcal{O}}^\times) = \widehat{\mathbf{Z}}_F^\times$ by Proposition 2.4.2. Therefore $\mathrm{Sh}(\mathcal{O})$ is defined over $F_\infty = F$. By Lemma 3.3.2 and Lemma 3.3.4, a canonical model of $J(\Gamma)$ can be constructed as a $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ Atkin-Lehner quotient of $J_0(\mathcal{O}) = J(\mathcal{O})$. As in the case e2d1D6ii, we see that this implies that $J_0(\mathcal{O})$ is a canonical model of $J(\Gamma)$.

The curve $J_0(\mathcal{O})$ has good reduction away from $\mathfrak{p}_2$ by Theorem 3.1.6. There are 8 twists over F with the j-invariant from Chapter 6 that have this property. The traces from Algorithm 4.2.1 determine the correct twist: using the algebraic integers α from Table A.1, it is given by

$$y^2 = x^3 + (\alpha - 1)x^2 + (-6\alpha - 5)x + (-11\alpha - 7),$$

which is isomorphic to its $\mathrm{Gal}(F|\mathbf{Q})$-conjugate over F. However, this model does not descend to $\mathbf{Q}$. This is most easily seen by considering its trace of Frobenius at the inert prime $\mathfrak{p}_3$: this trace equals 2, which is not of the form $n^2 - 2 \cdot 3$ with n an integer. The conductor of this curve equals $\mathfrak{p}_2^3$.

$\boxed{\textbf{e2d5D4ii:}}$ This case is rather special in that $\Gamma^{(2)}$ generates an order whose norm 1 group contains the $(1;2)$-group Γ but has signature $(0;2,5^2)$ itself. It is therefore more involved to obtain a canonical model of $X(\Gamma)$ in this case, since no order $\mathcal{O}$ suggests itself for which $J(\Gamma)$ can be realized as an Atkin-Lehner quotient of $J_0(\mathcal{O})$.

We know $j(J(\Gamma))$ from Chapter 6. It turns out that there are two twists over F having conductor $\mathfrak{p}_2\mathfrak{p}_5^2$ with this j-invariant. One of these two twists can be obtained as the base extension of either of the elliptic curves

$$\begin{aligned} y^2 + xy + y &= x^3 + 549x - 2202, \\ y^2 + xy + y &= x^3 + x^2 + 22x - 9 \end{aligned}$$

of conductor 50 over $\mathbf{Q}$; the other is a $\mathfrak{p}_5$-twist of this curve.

Considering Theorem 3.1.6, the preceding paragraph suggests that we can obtain $X(\Gamma)$ using a compact open group $K \subset \widehat{B}^\times$ that is non-maximal at $\mathfrak{p}_5$ only. Let $\mathcal{O}(1)$ be the maximal order generated by $\Gamma^{(2)}$, and consider the group

$$C = (\widehat{\mathbf{Z}}_F + \mathfrak{p}_5\widehat{\mathcal{O}}(1))^\times.$$

It equals the core $C(\widehat{\mathcal{O}}(\mathfrak{p}_5)^\times)$ for any level $\mathfrak{p}_5$ Eichler order $\mathcal{O}(\mathfrak{p}_5)$ contained in $\mathcal{O}(1)$. We clearly have

$$\mathrm{nrd}(C) = U_{\mathfrak{p}_5}^2 \times \prod_{\mathfrak{p} \nmid 5} U_{\mathfrak{p}}^{(0)}. \tag{7.1}$$

The monodromy group M of the cover

$$Y_0(\mathcal{O}(\mathfrak{p}_5)) \longrightarrow Y_0(\mathcal{O}(1))$$

is isomorphic to $\mathrm{PSL}(2, \mathbf{F}_5)$ (*cf.* Remark (i) at the end of Section 6.1). It is isomorphic to the Galois group of the cover

$$Y_0(C) \longrightarrow Y_0(\mathcal{O}(1)). \tag{7.2}$$

Up to conjugation, the group M has a unique subgroup H of index 5. Calculating the action of the elliptic generators of G on G/H by using Algorithm 6.1.7, we see that the cover of $X(\mathcal{O}(1)^1) \cong Y_0(\mathcal{O}(1))$ corresponding to H by Theorem 6.1.2 has ramification type $((2,2,1),(5),(5))$.

But by Algorithm 6.1.4, there is a unique Belyĭ map with this ramification type. Consequently H corresponds to the cover $X(\Gamma) \to X(\mathcal{O}(1)^1)$ that we calculated in Chapter 6. In other words, the cover $X(\Gamma) \to X(\mathcal{O}(1)^1)$ is the unique degree 5 cover of $X(\mathcal{O}(1)^1)$ that is a factorization of the Galois cover (7.2).

A calculation in the group

$$\mathcal{O}(1)^\times_{\mathfrak{p}_5}/C_{\mathfrak{p}_5} \cong \mathrm{PGL}(2, \mathbf{F}_5)$$

shows that there is a unique index 5 subgroup K of $\widehat{\mathcal{O}}(1)^\times$ containing C. Corollary 2.5.3 gives that the degree of the resulting cover

$$Y_0(K) \longrightarrow Y_0(\mathcal{O}(1))$$

also equals 5. Hence $X(\Gamma) \cong Y_0(K)$, realizing this arithmetic $(1;e)$-curve as a Shimura curve. One verifies that this K contains an element whose norm in $\mathbf{Z}_F/\mathfrak{p}_5$ is not a square: considering (7.1), we therefore have $\mathrm{nrd}(K) = \widehat{\mathbf{Z}}_F^\times$.

We conclude that $J(\Gamma)$ has a canonical model $J_0(K) = J(K)$ over $F_K = F_\infty = F$. As in the previous case e2d5D4i, this model can be determined up to isomorphism using Theorem 3.1.6 and Algorithm 4.2.1. However, our implementation of Algorithm 4.2.1 in Section 4.2 is not immediately of use for this case since K does not come from an order $\mathcal{O}$. To remedy this, we wrote an ad hoc program (to be found at [Sij10], as usual) that allows us to compute the traces of Frobenius for this curve as well.

In the end, $J_0(K)$ is given by the $\mathfrak{p}_5$-twist of the base extensions considered above: in a Weierstrass equation, this is the curve

$$y^2 + \alpha xy + (\alpha+1)y = x^3 + (\alpha-1)x^2 + (-111\alpha+220)x + (-287\alpha+528).$$

$\boxed{\textbf{e2d5D4iii:}}$ We have seen in Chapter 6 that $\mathcal{O}(\mathfrak{p}_3) = \mathbf{Z}_F[\Gamma^{(2)}]$ is a level $\mathfrak{p}_3$ Eichler order with norm 1 group $\langle \Gamma^{(2)}, A \rangle$.

The curve $J_0(\mathcal{O}(\mathfrak{p}_3))$ is canonically defined over $F_\infty = F$. Using Theorem 3.1.6, one finds that it has conductor $\mathfrak{p}_2\mathfrak{p}_3$. Along with the j-invariant from Chapter 6, this determines $J_0(\mathcal{O}(\mathfrak{p}_3))$ up to isomorphism. The corresponding canonical model of $J(\Gamma)$ is a $\mathbf{Z}/2\mathbf{Z}$ Atkin-Lehner quotient of this curve. It is explicitly given by

$$y^2 + xy + y = x^3 + (\alpha-1)x^2 + (-45\alpha-28)x + (-847\alpha-524).$$

The same argument as in the case e2d5D4i shows that this model is does not descend to $\mathbf{Q}$.

e2d8D2: We know $j(J(\Gamma)) = 1728$ from Chapter 6. If we let $\mathcal{O}$ be the order $\mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$, then we have $\mathcal{O}^1 = \langle \Gamma^{(2)}, AB \rangle$. Let $\mathcal{O}(1)$ be the maximal order containing $\mathcal{O}$. Then as a $\mathbf{Z}_F$-module, $\mathcal{O}(1)/\mathcal{O} \cong (\mathbf{Z}_F/\mathfrak{p}_2^2)^2$. Using Algorithm 6.1.7, one can check that there are no orders $\mathcal{O}'$ inbetween $\mathcal{O}$ and $\mathcal{O}(1)$ with $\mathcal{O}'^1 = \mathcal{O}^1$. Nor can there be such orders with $\mathcal{O}^1 = \Gamma$, since the matrix A does not correspond to an element of the quaternion algebra associated to Γ. We therefore work with $J_0(\mathcal{O})$.

Algorithm 2.4.3 shows that

$$\mathrm{nrd}(\widehat{\mathcal{O}}^\times) = U_{\mathfrak{p}_2}^{(2)} \times \prod_{\mathfrak{p} \nmid \mathfrak{p}_2} U_{\mathfrak{p}}^{(0)}$$

We see that $F_{\mathfrak{p}_2^2 \infty} = F(i)$ is the canonical field of definition of the elliptic curve $J_0(\mathcal{O})$. By Lemma 3.3.4, there exists an Atkin-Lehner quotient of $J_0(\mathcal{O})$ that is a model of $J(\Gamma)$.

Using Theorem 3.1.6 along with the traces from Algorithm 4.2.1 as usual, one shows that the canonical model of $J(\Gamma)$ is the base extension of either of the elliptic curves

$$y^2 = x^3 + x$$
$$y^2 = x^3 - x$$

over $\mathbf{Q}$. Note that over F, these curves are isogenous, but not isomorphic. Without going into details, we mention that these two curves (and their analogues on future occasions) correspond to the F-factors of the Jacobian $J(\mathcal{O})$ constructed in Theorem 4.4 of [Hid81], which result from a decomposition of the Hecke module H in Algorithm 4.2.1 into 2 sub-Hecke modules of dimension 1.

e2d8D7i/ii: These two cases are conjugate (*cf.* Theorem 3.1.7): we treat the first. If we let $\mathcal{O} = \mathbf{Z}_F[\Gamma^{(2)}]$, then we have $\mathcal{O}^1 = \langle \Gamma^{(2)}, B \rangle$. There is a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$ such that as $\mathbf{Z}_F$-modules $\mathcal{O}(1)/\mathcal{O} \cong (\mathbf{Z}_F/\mathfrak{p}_2)^2$. Since Algorithm 6.1.7 shows that $[\mathcal{O}(1)^1 : \mathcal{O}^1] = 2$, we see that we are in case (iii) of Proposition 2.3.1. In particular, $\mathcal{O}$ is not Eichler, and there is no level $\mathfrak{p}_2$ order inbetween $\mathcal{O}(1)$ and $\mathcal{O}$.

Proposition 2.3.1 shows that $\mathrm{nrd}(\widehat{\mathcal{O}}^\times) = \widehat{\mathbf{Z}}_F^\times$. Therefore the canonical field of definition of $J_0(\mathcal{O}) = J(\mathcal{O})$ is given by $F_\infty = F$. The curve $J_0(\mathcal{O})$ has a 2-isogeny

$$J_0(\mathcal{O}^1) \longrightarrow J(\Gamma)$$

(*cf.* Lemma 3.3.2). This isogeny descends to F by Lemma 3.3.4. A search of $X_0(2)$ using Algorithm 5.2.2 yields the candidate

$$y^2 = x^3 + \alpha x^2 + (-2\alpha - 2)x + (-2\alpha - 3)$$

for the isogeny class of the canonical model $J_0(\mathcal{O})$. It has conductor $\mathfrak{p}_2^2\mathfrak{p}_7$. If this candidate curve is correct, then the canonical model $J(\Gamma)$ is in the same isogeny class.

With the methods at our disposal, we cannot hope to calculate more than an isogeny class in this case. Indeed, we cannot reconstruct the dual graph of $\mathrm{Sh}(K)$ at $\mathfrak{p}_7$ using Proposition 5.1.9 since we only implemented this for Eichler orders as yet. The correctness of the candidate isogeny class given above is discussed in the next section.

e2d12D2: This case and the next have a base field F with non-trivial narrow class group.

We know that $j(J(\Gamma)) = 0$ from Chapter 6. Let $\mathcal{O}(\mathfrak{p}_2)$ be as in that Chapter. Then as in the case e2d5D4i, because $\mathfrak{p}_2$ is even, we get that $\mathrm{nrd}(\widehat{\mathcal{O}}(\mathfrak{p}_2)^\times) = \widehat{\mathbf{Z}}_F^\times$ from Proposition 2.3.2. Since $F_\infty = F(i) \neq F$, we have $\mathrm{nrd}(\mathcal{O}(\mathfrak{p}_2)^\times) = \mathbf{Z}_F^+ \neq \mathbf{Z}_F^{\times 2}$ by Proposition 2.4.2. Using Proposition 3.2.1, we see that

$$[\mathrm{P}\mathcal{O}(\mathfrak{p}_2)^+ : \mathrm{P}\mathcal{O}(\mathfrak{p}_2)^1] = 2.$$

As a result, the group $\mathcal{O}(\mathfrak{p}_2)^+$ has signature $(0; 2^3, 4)$. We therefore have to choose groups N' and K' for $K = \widehat{\mathcal{O}}(\mathfrak{p}_2)^\times$ as in (3.20) in order to obtain a canonical (K'-)model $J_0(K')$ of $J(\Gamma)$ over F_∞.

We first choose

$$N' = U_{\mathfrak{p}_2}^{(2)} \times \prod_{\mathfrak{p} \nmid 2} U_{\mathfrak{p}}^{(0)},$$

which works because the representative $\alpha + 2$ of the unique non-trivial coset in $\mathbf{Z}_F^+ / \mathbf{Z}_F^{\times 2}$ is not congruent to 1 modulo $\mathfrak{p}_2^2$ and $\mathrm{Cl}(\mathfrak{p}_2^2 \infty) \cong \mathrm{Cl}(\infty)$. The equalities (4.11) and (4.13) are satisfied for the resulting group K'. Hence $\mathrm{Sh}(K')$ has two components over

$$F_{K'} = F_{\widehat{\mathcal{O}}(\mathfrak{p}_2)^\times} = F_\infty,$$

given by $\mathrm{Sh}_0^+(K')$ and $\mathrm{Sh}_0^-(K')$, both of them defined over $F_\infty = F(i)$. By construction, the Jacobian $J_0(K')$ of the neutral component is a canonical model of $J(\Gamma)$. Now the narrow type number of K' is equal to 1 by Proposition 2.6.1 and Proposition 3.1.4: indeed, since $\mathcal{O}(\mathfrak{p}_2)$ is the unique level $\mathfrak{p}_2$ suborder of $\mathcal{O}(1)$, we have

$$N(K') \supset N(\widehat{\mathcal{O}}(\mathfrak{p}_2)^\times) = N(\widehat{\mathcal{O}}(\mathfrak{p}_2)) = N(\widehat{\mathcal{O}}(1)),$$

so we can use Proposition 2.6.2 to conclude. The canonical models $J_0^\pm(K')$ of $J(\Gamma)$ are therefore isomorphic over F_K, and the proof above shows that these components will in fact be isomorphic for any choice of K'.

From Theorem 3.1.6, we see that $J(K')$ has good reduction away from $\mathfrak{p}_2$. Hence $J_0(K')$ has good reduction outside $\mathfrak{p}_2 \mathbf{Z}_{F_\infty}$. Using this information in conjuction with the fact that $j(J(\Gamma)) = 0$ and the traces obtained from Algorithm 4.2.1, we can determine the canonical model $J_0(K')$. It is given by the base extension to F_∞ of the curve

$$y^2 = x^3 + \alpha x^2 + x + (3\alpha - 5).$$

This curve has conductor $\mathfrak{p}_2^4\mathbf{Z}_{F_\infty}$. It is F-isogenous and F_∞-isomorphic, but not F-isomorphic, to its Galois conjugate. As in the case e2d8D2, these two conjugate curves correspond to factors of the Hecke module H in Algorithm 4.2.1.

Next we take N' to equal the index 2 subgroup

$$N' = U_{\mathfrak{p}_3}^2 \times \prod_{\mathfrak{p}\nmid 3} U_{\mathfrak{p}}^{(0)}$$

of $\mathbf{Z}_F$ for the odd place $\mathfrak{p}_3$. This time, we get that the corresponding canonical model $J_0(K')$ is the base extension to F_∞ of either of the curves

$$\begin{aligned} y^2 &= x^3 + 1 \\ y^2 &= x^3 - 1 \end{aligned}$$

over $\mathbf{Q}$. These curves have conductor $\mathfrak{p}_2^2\mathfrak{p}_3^2\mathbf{Z}_{F_\infty}$. As above, these curves are isogenous but not isomorphic over F, though they do become isomorphic over F_∞.

In particular, the results above show that the K'-model $J_0(K')$ of $J(\Gamma)$ may indeed depend on the choice of K'. In some sense, though, one can get around this non-uniqueness. The orders $\mathcal{O} = \mathbf{Z}_F[G]$ in Table A.2 other than $\mathbf{Z}_F[\Gamma]$ all satisfy

$$\mathrm{nrd}(\mathcal{O}^\times) = U_{\mathfrak{p}_2}^2 \times \prod_{\mathfrak{p}\nmid 2} U_{\mathfrak{p}}^{(0)}$$

by Algorithm 2.4.3. Therefore $\mathrm{P}\mathcal{O}^1 = \mathrm{P}\mathcal{O}^+$ for these orders, and we get $J_0(\mathcal{O})$ as a canonical model of $J(\Gamma)$. These choices all result in the same model as the first choice of K' above. Since this K'-model also has good reduction outside of $\mathfrak{p}_2$, which is as optimal as can be reasonably wished considering that we started with a quaternion algebra B ramified at $\mathfrak{p}_2$ (*cf.* Theorem 3.1.6), it is this canonical model that we have used in the final Table A.3.

$\boxed{\textbf{e2d12D3:}}$ The latter part of this case resembles the previous, except that the dependency on K' that we encountered there does not seem to occur.

We know $j(J(\Gamma)) = 2^2 193^3/3$ from Chapter 6. We saw there that the group $\Gamma^{(2)}$ generates a level $\mathfrak{p}_2^4$ non-Eichler order $\mathcal{O} = \mathbf{Z}_F[\Gamma^{(2)}]$ with $\mathcal{O}^1 = \Gamma^{(2)}$. There is a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$ such that

$$\mathcal{O}(1)/\mathcal{O} \cong (\mathbf{Z}_F/\mathfrak{p}_2^2)^2$$

as Z_F-modules. Algorithm 2.4.3 gives

$$\mathrm{nrd}(\widehat{\mathcal{O}}^\times) = U_{\mathfrak{p}_2}^{(2)} \times \prod_{\mathfrak{p}\nmid 2} U_{\mathfrak{p}}^{(0)},$$

which implies that $\mathrm{P}\mathcal{O}^+ = \mathrm{P}\mathcal{O}^1$ by Proposition 3.2.1. The curve $J_0(\mathcal{O})$ is defined over $F_{\mathfrak{p}_2^2\infty} = F_\infty = F(i)$.

The traces resulting from Algorithm 4.2.1, along with Theorem 3.1.6, show that $J_0(\mathcal{O})$ can be described as the base extension of either of the curves

$$\begin{aligned} y^2 &= x^3 - x^2 - 64x + 220, \\ y^2 &= x^3 - 579x - 5362. \end{aligned}$$

As in the previous case, the other component $\mathrm{Sh}_0^-(\mathcal{O})$ of $\mathrm{Sh}(\mathcal{O})$ over F_∞ is isomorphic to $\mathrm{Sh}_0^+(\mathcal{O})$.

The two curves above are neither isomorphic nor isogenous over F: as in the case e2d8D2, they correspond to the F-factors of $J(\mathcal{O})$ constructed in Theorem 4.4 of [Hid81]. Their common base extension to F_∞ has conductor $\mathfrak{p}_2^3\mathfrak{p}_3\mathbf{Z}_{F_\infty}$. It is the unique curve over F_∞ with the given j-invariant having this conductor. In Table A.3 in the appendix, we have used this curve as a canonical model of $J(\Gamma)$.

We consider this case a bit further. There is a unique order $\mathcal{O}'$ inbetween $\mathcal{O}$ and $\mathcal{O}(1)$ such that

$$\mathcal{O}(1)/\mathcal{O}' \cong \mathbf{Z}_F/\mathfrak{p}_2 \times \mathbf{Z}_F/\mathfrak{p}_2^2.$$

For this order, Algorithm 2.4.3 shows $\mathrm{nrd}(\widehat{\mathcal{O}}'^\times) = \widehat{\mathbf{Z}}_F^\times$. This time we have

$$[\mathrm{P}\mathcal{O}'^+ : \mathrm{P}\mathcal{O}'^1] = 2.$$

To pass to $\mathrm{P}\mathcal{O}'^1$, we have to choose a K' for $K = \widehat{\mathcal{O}}'^\times$ as in (3.20).

As in the case e2d12D3, one checks that the matrices A and B normalize the order $\mathcal{O}'$, which implies that they correspond to elements of $N(\widehat{\mathcal{O}}'^\times) \subset N(K')$ (*cf.* the case e2d1D6ii). Therefore the curves $J_0(K')$ are also canonical models of $J(\Gamma)$. For all K' that we tried, we found the same traces, hence the same curve, as above. We can recover the $\widehat{\mathcal{O}}^\times$-model $J_0(\mathcal{O})$ above as a K'-model by taking N' in (3.20) to be non-maximal at $\mathfrak{p}_2$.

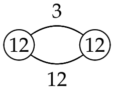
Experimentally, therefore, the canonical models constructed above do not seem to depend on the choice of K', in contrast with the previous case. This is not as simple to prove as in the case e2d21D4 below since $J_0(\mathcal{O}')$ is not an elliptic curve (it has signature $(0; 2^6)$). This independency would in fact follow if the K'-models $J_0(K')$ were all isomorphic to their $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$-conjugates, but we have not been able to prove this fact either.

$\boxed{\textbf{e2d13D4:}}$ The group Γ generates a maximal order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma]$ for which $\Gamma = \mathcal{O}(1)^1$. The canonical model $J_0(\mathcal{O}(1)) = J(\mathcal{O}(1))$ of $J(\Gamma)$ is defined over $F_\infty = F$. Since the finite part $\mathfrak{D}(B)^f$ of the discriminant B is $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$-invariant, the discussion following Theorem 3.1.7 shows that

$$j(J_0(\mathcal{O}(1))) \in \mathbf{Q}.$$

The extension $F|\mathbf{Q}$ is ramified above 13 only. Combining elementary properties of twists with Theorem 3.1.6 therefore shows that $J_0(\mathcal{O})$ is an F-twist of an elliptic curve over $\mathbf{Q}$ with good reduction outside 2 and 13 (or more precisely, of an elliptic curve over $\mathbf{Q}$ whose conductor is of the form $2^1 13^i$).

Upon determining these curves by using either Cremona's tables [Cre06] or [CL07], it turns out that there are only two such twists whose traces of Frobenius are equal to those given by Algorithm 4.2.1. Both of these twists have conductor $\mathfrak{p}_2$, so we cannot use Theorem 3.1.6 to decide which of the two is correct. However, Proposition 5.1.9 gives the following dual graph for $\mathrm{Sh}(\mathcal{O}(1))$ at $\mathfrak{p}_2$:



Therefore the valuation of $j(J_0(\mathcal{O}(1)))$ at $\mathfrak{p}_2$ equals 15 by Proposition 5.1.12. This determines which of the two candidates above is isomorphic to $J_0(\mathcal{O}(1))$. A minimal Weierstrass equation for the correct curve is given by

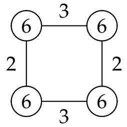
$$y^2 + \alpha xy + (\alpha+1)y = x^3 + (-\alpha-1)x^2 + (-75\alpha-100)x + (-433\alpha-566);$$

it has j-invariant $-29^3 41^3/2^{15}$. Though isomorphic to its Galois conjugate, $J_0(\mathcal{O}(1))$ does not descend to $\mathbf{Q}$, as can be shown using the method first encountered in the case e2d5D4i.

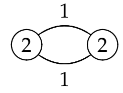
e2d13D36: This case is completely analogous to the previous. The group $\Gamma^{(2)}$ generates a maximal order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$ for which $\Gamma^{(2)} = \mathcal{O}(1)^1$. The canonical model of $J(\Gamma)$ over $F_\infty = F$ is given by $J_0(\mathcal{O}(1)) = J(\mathcal{O}(1))$. Collecting a list of candidates using Cremona's tables and Algorithm 4.2.1, one ends up with 4 candidates this time, all of conductor $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'$.

By Proposition 5.1.9, the dual graphs of $\mathrm{Sh}(\mathcal{O}(1))$ at the primes dividing the discriminant of B are given by

At $\mathfrak{p}_2$:



At $\mathfrak{p}_3$ and $\mathfrak{p}_3'$:



The resulting valuations -10, -2, -2 at $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$ once more determine the correct model. It is given by

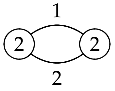
$$y^2 + (\alpha+1)xy + (\alpha+1)y = x^3 + (16383\alpha - 38230)x + (1551027\alpha - 3576436).$$

Though isomorphic to its Galois conjugate, this curve does not descend to $\mathbf{Q}$, since the trace of Frobenius 22 at the inert prime $\mathfrak{p}_{11}$ is not of the form $n^2 - 2\cdot 11$.

e2d17D2i/ii: These two cases are conjugate (*cf.* Theorem 3.1.7). We consider the first. The level $\mathfrak{p}_2'^2$ non-Eichler order $\mathcal{O} = \mathbf{Z}_F[\langle\Gamma^{(2)}, AB\rangle]$ has norm 1 group $\mathcal{O}^1 = \langle\Gamma^{(2)}, AB\rangle$. The index from Table A.2 shows that we are in case (iv) of Proposition 2.3.1. Let $\mathcal{O}(\mathfrak{p}_2')$ be the unique level $\mathfrak{p}_2'$ Eichler order inbetween $\mathcal{O}$ and a maximal order $\mathcal{O}(1)$. This order exists by Proposition 2.3.1, which also shows that we have $\mathcal{O}(\mathfrak{p}_2')^1 = \mathcal{O}^1$.

We take the curve $J_0(\mathcal{O}(\mathfrak{p}_2')) = J(\mathcal{O}(\mathfrak{p}_2'))$, which is canonically defined over $F_\infty = F$, as a canonical model of $J(\mathcal{O}^1)$. Using our implementation of

Proposition 5.1.9, we see that the dual graph of this curve at $\mathfrak{p}_2$ is of the form



Arguing as in the case e2d8D7, one shows that $J_0(\mathcal{O}(\mathfrak{p}_2'))$ has a 2-isogeny. A search on $X_0(2)$ using Algorithm 5.2.2, along with the traces from Algorithm 4.2.1, returns a candidate C for $J_0(\mathcal{O}(\mathfrak{p}_2'))$.

Taking isogenies of prime degree ≤ 50, we found two curves in the isogeny class of C whose j-invariant has the correct valuation at $\mathfrak{p}_2$: the next section will prove that these are the only two such curves. They are given by the $\mathbf{Q}$-curves

$$y^2 + xy + \alpha y = x^3 + (-\alpha + 1)x^2 + (606\alpha - 1553)x + (12977\alpha - 33243)$$

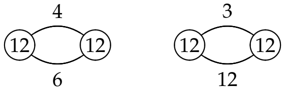
and

$$y^2 + xy + (\alpha + 1)y = x^3 + \alpha x^2 + (981\alpha - 2517)x + (23628\alpha - 60528).$$

The matrices A and B normalize the order $\mathcal{O}(\mathfrak{p}_2')$ as well as $\mathcal{O}$. Therefore, using Lemma 3.3.4, we see that a canonical model of $J(\Gamma)$ can be recovered from the correct model above as the codomain of a 2-isogeny over F coming from an Atkin-Lehner involution. Fortunately, both curves have a unique such 2-isogeny, and we end up with the same curve using either. It is described by the minimal model

$$y^2 + xy + (\alpha + 1)y = x^3 + \alpha x^2 + (61\alpha - 157)x + (348\alpha - 896).$$

$\boxed{\textbf{e2d21D4:}}$ The narrow class group is non-trivial for this case. The maximal order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$ has $\mathcal{O}(1)^1 = \langle \Gamma^{(2)}, B \rangle$. The curve $J_0(\mathcal{O}(1))$ is canonically defined over $F_\infty = F(w)$, where $w = w_{-7}$ is a zero of the polynomial $t^2 - t + 2$. By Proposition 5.1.9, the dual graph of $\mathrm{Sh}(\mathcal{O}(1))$ at $\mathfrak{p}_2$ is the following:



These graphs show that $\mathrm{Sh}_0(\mathcal{O}(1))$ has genus 1 (by Proposition 5.1.6(ii)), hence $\mathcal{O}(1)^+$ has signature $(1;2)$. Consequently $\mathrm{P}\mathcal{O}(1)^+ = \mathrm{P}\Gamma$. The connected components of $\mathrm{Sh}(\mathcal{O}(1))$ are given by $\mathrm{Sh}_0^+(\mathcal{O}(1))$ and $\mathrm{Sh}_0^-(\mathcal{O}(1))$ since the hypotheses (4.11) and (4.13) hold for $K = \widehat{\mathcal{O}}(1)^\times$. We therefore use the curves $J_0^\pm(\mathcal{O}(1))$ as canonical models of $J^\pm(\Gamma)$.

Let K' be as in (3.20). Then the inclusion $K' \subset \widehat{\mathcal{O}}(1)^\times$ gives rise to a 2-isogeny

$$J_0(K') \longrightarrow J_0(\mathcal{O}(1))$$

over F_∞. Therefore we searched $X_0(2)(F_\infty)$ using Algorithm 5.2.2 in combination with Algorithm 4.2.1. There turns out to be a point in

$$X_0(2)(\mathbf{Q}(w)) \subset X_0(2)(F_\infty)$$

that gives rise to the correct traces of Frobenius up to a minus sign and for which the corresponding j-invariant has valuation -15 and -10 at the primes of $\mathbf{Q}(w)$ above 2. A corresponding elliptic curve over $\mathbf{Q}(w)$ is given by

$$y^2 + xy + wy = x^3 - x^2 + (-554w + 1740)x + (-14641w - 9374).$$

This curve has conductor $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3^2$ over $\mathbf{Q}(w)$, but it cannot be twisted over $\mathbf{Q}(w)$ to have good reduction at $\mathfrak{p}_3$. However, it does have a twist of conductor $\mathfrak{p}_2\mathfrak{p}_2'\mathbf{Z}_{F_\infty}$ over F_∞, which we take as a candidate equation for $J_0(\mathcal{O}(1))$.

Using isogenies of prime degree ≤ 50, we encountered 8 curves in the isogeny class of the candidate above. The curves whose j-invariant has valuation in $\{-15, -10\}$ are exactly given by this twist and its $\mathrm{Gal}(F_\infty|F)$-conjugate. Hence if we assume that these 8 curves constitute the full F_∞-isogeny class of $J_0(\mathcal{O}(1))$, then we can conclude that the candidate curve above and its conjugate give canonical models of $J^\pm(\Gamma)$.

We discuss the correctness of this isogeny class in the next section. For now, we note that it satisfies the demands of Theorem 3.1.6, Algorithm 4.2.1 and Proposition 3.1.5.

Finally, we remark that assuming the correctness of this candidate model, the canonical K'-models $J_0(K')$ of $J(\mathcal{O}(1)^1)$ resulting from a choice of K' as in (3.20) are all isomorphic. Indeed, we saw that there are 2-isogenies $J_0(K') \to J_0(\mathcal{O}(1))$ over F_K. But $J_0(\mathcal{O}(1))$ has only one such isogeny. Therefore the model $J_0(K')$ is the same curve in all cases.

$\boxed{\textbf{e2d24D3:}}$ Once more, the narrow class group of F is non-trivial. $\Gamma^{(2)}$ generates a level $\mathfrak{p}_2^2$ order $\mathcal{O} = \mathbf{Z}_F[\Gamma^{(2)}]$ for which $\mathcal{O}^1 = \Gamma^{(2)}$. Let $\mathcal{O}(1)$ be an order containing $\mathcal{O}$. Table A.3 shows that $[\mathcal{O}(1)^1 : \mathcal{O}^1] = 2$. This means that we are in case (iii) of Proposition 2.3.1. Consequently $\mathrm{nrd}(\widehat{\mathcal{O}}^\times)$ equals $\mathbf{Z}_F^\times$. Proposition 3.2.1 shows that $\mathrm{P}\mathcal{O}^+$ contains $\mathrm{P}\mathcal{O}^1$ as a subgroup of index 2. Much of the reasoning that follows runs parallel to the previous case.

The signature of the group $\mathcal{O}^+$ was calculated by John Voight and equals $(1; 2^2)$. The canonical field of definition of the connected components $\mathrm{Sh}_0^\pm(\mathcal{O})$ of $\mathrm{Sh}(\mathcal{O})$ equals $F_\infty = F(w)$, where $w = w_{-2}$. Lemma 3.3.4 shows that canonical models of $J^\pm(\Gamma)$ can be found by taking suitable Atkin-Lehner quotients of the curves $J_0^\pm(\mathcal{O})$.

Because the narrow type number of $\mathcal{O}$ equals 2 in this case as well as the previous, we cannot use Theorem 3.1.7 to conclude that $j(J_0(\mathcal{O}))$ is rational even though the level and discriminant are both Galois invariant. Indeed, though the curve $Y(\mathcal{O})$ is isomorphic to its complex conjugate by Theorem 3.1.7, its components $Y_0^\pm(\mathcal{O})$ need not be isomorphic to theirs.

Since the order $\mathcal{O}$ is not Eichler, we also cannot reconstruct the dual graph of $\mathrm{Sh}(K)$ at $\mathfrak{p}_3$. As in the case e2d8D7, we therefore settle for determining the isogeny class of $J_0(\mathcal{O})$.

The curve $J_0(\mathcal{O})$ has a 2-isogeny over F_∞ coming from the Atkin-Lehner quotient of $J_0(\mathcal{O})$ realizing the model of $J(\Gamma)$. Searching $X_0(2)(F_\infty)$ by combining Algorithm 5.2.2 and Algorithm 4.2.1, we end up with a point in

$$X_0(2)(\mathbf{Q}(w)) \subset X_0(2)(F_\infty)$$

corresponding to the curve

$$y^2 + wxy + wy = x^3 + (w+1)x^2 + (3w+4)x + (2w+4).$$

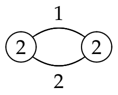
It has non-rational j-invariant and conductor $\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_3'^2$ over $\mathbf{Q}(w)$ and is therefore neither isomorphic nor isogenous to its $\mathrm{Gal}(\mathbf{Q}(w)|\mathbf{Q})$-conjugate. Moreover, this curve has no $\mathbf{Q}(w)$-twist having multiplicative reduction at $\mathfrak{p}_3'$. The base extension of this curve to F_∞ has conductor $\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_3'$ and is F_∞-isogenous its $\mathrm{Gal}(F_\infty|F)$-conjugate, in line with Proposition 3.1.5.

As in the previous case, we conjecture that the isogeny class of the canonical models of the curves $J^\pm(\Gamma)$ is represented by the model above. Again we refer to the next section for a discussion on how to prove this claim.

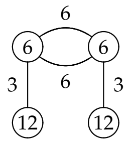
e2d33D12: This case resembles the previous, the major difference being that Proposition 5.1.12 and Theorem 3.1.7 do give us useful information in this case, which allows us to determine the canonical model up to isomorphism.

The group $\Gamma^{(2)}$ generates a maximal order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$ whose norm 1 group is given by $\mathcal{O}(1)^1 = \Gamma^{(2)}$. Consider the Shimura curve $\mathrm{Sh}(\mathcal{O}(1))$. From Proposition 5.1.9, we get the following dual graphs for this curve:

At $\mathfrak{p}_2$ and $\mathfrak{p}_2'$: twice



At $\mathfrak{p}_3$: twice



Proposition 5.1.6(ii) therefore shows that the group $\mathcal{O}(1)^+$ has genus 1, hence signature $(1;2^2)$, and Proposition 5.1.12 yields that the j-invariants of the Jacobians $J_0^\pm(\mathcal{O}(1))$ have valuations 3 and 12 at the primes of F_∞ over 2 and 3, respectively. We can also apply Theorem 3.1.7: since the narrow type number equals 1 by Proposition 2.6.2(ii), we can conclude that

$$j(J_0(\mathcal{O}(1))) \in \mathbf{Q}$$

by Galois invariance of the discriminant of B and the level of $\mathcal{O}(1)$.

The canonical model $J_0(\mathcal{O}(1))$ is defined over $F_\infty = F(w_{-3})$. Using the same technique as in the case e2d13D4, we find that $J_0(\mathcal{O}(1))$ is the base extension of the curve

$$y^2 + xy = x^3 + (\alpha+1)x^2 + (347\alpha - 1164)x + (-6063\alpha + 20448)$$

over F, which has conductor $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3$. As in the case e2d8D2, the fact that the canonical model descends to F follows from Theorem 4.4 in [Hid81] and the Hecke operators from Algorithm 4.2.1.

The curve above is not isogenous to its $\mathrm{Gal}(F|\mathbf{Q})$-conjugate over F, but over F_∞, these conjugates become isomorphic: this again follows from the triviality of the narrow type number, which implies that the Jacobians $J_0^\pm(\mathcal{O}(1))$ are isomorphic over F_∞.

As usual, by Lemma 3.3.4, we can construct a canonical model of $J(\Gamma)$ by taking an Atkin-Lehner quotient of $J_0(\mathcal{O}(1))$. This quotient will be given by a

2-isogeny over F_∞. Fortunately, $J_0(\mathcal{O}(1))$ has only one such isogeny (which in fact descends to F), resulting in a canonical model of $J(\Gamma)$ that can be described as the base extension of either the curve

$$y^2 + xy = x^3 + (\alpha + 1)x^2 + (27\alpha - 84)x + (-63\alpha + 216)$$

or its $\mathrm{Gal}(F|\mathbf{Q})$-conjugate.

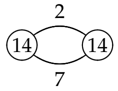
Arguing as in the previous case, one shows that the canonical models of $J(\mathcal{O}(1)^1)$ obtained by choosing a K' as in (3.20) do not depend on the particular choice of K'.

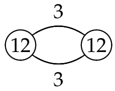
e2d49D56: This is similar to the case e2d13D4. $\Gamma^{(2)}$ generates a maximal order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$ of B whose norm 1 group is given by $\mathcal{O}(1)^1 = \langle \Gamma^{(2)}, A\rangle$. We can obtain a canonical model of $J(\Gamma)$ by taking an Atkin-Lehner quotient of $J_0(\mathcal{O}) = J(\mathcal{O})$, which is defined over $F = F_\infty$.

Theorem 3.1.7 shows that

$$j(J_0(\mathcal{O}(1))) \in \mathbf{Q}.$$

Harvesting a list of candidates as in the case e2d13D4, we end up with 6 curves, all of which descend to $\mathbf{Q}$. The dual graphs of $\mathrm{Sh}(\mathcal{O})$ obtained from Proposition 5.1.9 are as follows:

At $\mathfrak{p}_2$: 

At $\mathfrak{p}_7$: 

This determines the canonical model $J_0(\mathcal{O}(1))$: it is given by

$$y^2 + xy + y = x^3 - 2731x - 55146.$$

Being an Atkin-Lehner quotient, the canonical model of $J(\Gamma)$ is 2-isogenous over F to the curve above. Fortunately, there is a unique non-trivial 2-torsion point on $J_0(\mathcal{O}(1))$. Therefore, as in the previous case, we can conclude that this canonical model is given by

$$y^2 + xy + y = x^3 - 171x - 874.$$

This is the unique curve over F of j-invariant $5^3 1637^3/2^{18}7$ with conductor $\mathfrak{p}_2\mathfrak{p}_7$. The isogeny in question in fact descends to $\mathbf{Q}$.

e2d81D1: We can reason as in the case e2d5D4iii. We get the canonical model

$$y^2 + xy + y = x^3 - x^2 - 95x - 697$$

of conductor $\mathfrak{p}_2$.

e2d148D1i/ii/iii: These three cases are conjugate (*cf.* Theorem 3.1.7). We calculate the first one. As in the case e2d8D7, we cannot hope to determine more than the isogeny class of the canonical model.

Let $\mathcal{O} = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$. This order is of level $\mathfrak{p}_2^4$. Its norm 1 group $\mathcal{O}^1$ is given by $\langle \Gamma^{(2)}, AB \rangle$. There exists a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$, for which

$$\mathcal{O}(1)/\mathcal{O} \cong (\mathbf{Z}_F/\mathfrak{p}_2^2)^2$$

as $\mathbf{Z}_F$-modules. Additionally, there exists a unique order $\mathcal{O}'$ inbetween $\mathcal{O}$ and $\mathcal{O}(1)$ for which

$$\mathcal{O}(1)/\mathcal{O}' \cong \mathbf{Z}_F/\mathfrak{p}_2 \times \mathbf{Z}_F/\mathfrak{p}_2^2.$$

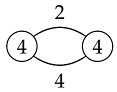
Algorithm 2.4.3 gives that $\mathrm{nrd}(\widehat{\mathcal{O}}'^{\times}) = \widehat{\mathbf{Z}}_F^{\times}$. Moreover, an application of Algorithm 6.1.7 gives $\mathcal{O}'^1 = \mathcal{O}^1$. Note that though the index $[\mathcal{O}(1)^1 : \mathcal{O}^1] = 6$ suggests that $\mathcal{O}^1$ in fact comes from a level $\mathfrak{p}_2^2$ Eichler order, Table 4.3 in [Voi09b] shows that this cannot be the case.

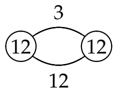
We therefore consider the canonical model $J_0(\mathcal{O}') = J(\mathcal{O}')$, which is defined over $F_\infty = F$. As in the case e2d12D3, we see that a canonical model of $J(\Gamma)$ can be obtained as an Atkin-Lehner quotient of this curve. We search $X_0(2)$ by combining Algorithm 5.2.2 and Algorithm 4.2.1 as usual, ending up with a candidate curve E with

$$j(E) = 2^6(-41\alpha^2 + 24\alpha + 141)$$

and conductor $\mathfrak{p}_2^3$.

$\boxed{\textbf{e2d229D8:}}$ These three cases are conjugate (*cf.* Theorem 3.1.7): we take the first. The order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$ is maximal, and $\mathcal{O}(1)^1 = \langle \Gamma^{(2)}, AB \rangle$. Consider the Shimura curve $\mathrm{Sh}(\mathcal{O}(1))$. From Proposition 5.1.9, we get the following dual graphs for this curve:

At $\mathfrak{p}_2$: twice 

At $\mathfrak{p}_2'$: twice 

Using Proposition 5.1.6, we conclude that the group $\mathcal{O}(1)^+$ has signature $(1;2)$. As in the case e2d33D12, we see that the components of $\mathrm{Sh}(\mathcal{O}(1))$ over the degree 2 extension F_∞ of F are isomorphic: both give the same canonical model $J_0(\mathcal{O}(1))$ of $J(\Gamma)$.

As for the case e2d21D4, we see that $J_0(\mathcal{O}(1))$ has a 2-isogeny over F_∞, and as in the case e2d8D2, the Hecke operators from Algorithm 4.2.1, along with Theorem 4.4 in [Hid81], show that $J_0(\mathcal{O}(1))$ is defined over F. We therefore searched $X_0(2)(F)$ using Algorithm 5.2.2 instead of the larger set $X_0(2)(F_\infty)$. This gives rise to two candidates, one for each isogeny factor of $J(\mathcal{O}(1))$. Both have j-invariant

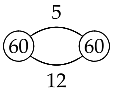
$$(n_2\alpha^2 + n_1\alpha + n_2)/2^{15},$$

where

$$\begin{aligned} n_2 &= 24628729701449988584212043, \\ n_1 &= 52087486182589166202672597, \\ n_0 &= 11645298538324182916131980. \end{aligned}$$

Their conductors both equal $\mathfrak{p}_2\mathfrak{p}_2'$, and they become isomorphic over F_∞.

e2d725D16i/ii: These two cases are conjugate (*cf.* Theorem 3.1.7). We take the first. The group Γ generates a maximal order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma]$ and we have $\Gamma = \mathcal{O}(1)^1$. We consider the canonical model $J_0(\mathcal{O}(1)) = J(\mathcal{O}(1))$ of $J(\Gamma)$. It is defined over $F_\infty = F$. The dual graph of $\mathrm{Sh}(\mathcal{O}(1))$ at $\mathfrak{p}_{17}$ can be calculated using our implementation of Proposition 5.1.9. It is given by



The traces obtained using Algorithm 4.2.1 suggest that though $J_0(\mathcal{O}(1))[2](F)$ is empty, $J_0(\mathcal{O}(1))$ has a 17-isogeny.

Browsing through the F-points of the elliptic curve $X_0(17)$ using Algorithm 5.2.2, we ended up with a candidate for $J_0(\mathcal{O}(1))$, whose conductor duly equals $\mathfrak{p}_2$ (*cf.* Theorem 3.1.6). It is an F-twist of the curve

$$y^2 + xy + w_5 y = x^3 + x^2 + (447w_5 - 4152)x + (-85116w_5 + 59004)$$

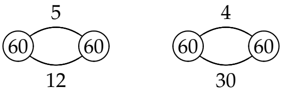
over $\mathbf{Q}(w_5) \subset F$. The base extension of the equation above to F has additive reduction at the prime $\mathfrak{p}_{29}$ over 29 ramifying in the extension $F|\mathbf{Q}(w_5)$, which can be removed upon twisting to yield a candidate model. As in the case e2d5D4i, one shows that $J_0(\mathcal{O}(1))$ does not descend to a subfield of F.

As mentioned before, we will consider methods to prove correctness of this candidate in the next section. For now, we remark that we indeed have

$$j(J_0(\mathcal{O}(1))) \in \mathbf{Q}(w_5) \subsetneq F.$$

Indeed, $\mathfrak{p}_2$ is the only prime above 2 in F, and F has trivial narrow class group. Combining Theorem 3.1.7 with Proposition 3.1.1(i) then shows that $j(J_0(\mathcal{O}(1)))$ is invariant under all automorphisms of F. But the fixed field of $\mathrm{Aut}(F)$ equals $\mathbf{Q}(w_5)$.

e2d1125D16: The narrow class group of F is non-trivial in this case. The group $\Gamma^{(2)}$ generates a maximal order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$ for which $\mathcal{O}(1)^1 = \langle \Gamma^{(2)}, B \rangle$. Consider $\mathrm{Sh}(\mathcal{O}(1))$. At $\mathfrak{p}_2$, this curve has the following dual graph by Proposition 5.1.9:



Therefore, as in the case e2d21D4, the group $\mathcal{O}(1)^+$ has signature $(1;2)$, and the Jacobians $J_0^\pm(\mathcal{O}(1))$ arising from the two connected components $\mathrm{Sh}_0^\pm(\mathcal{O}(1))$ of $\mathrm{Sh}(\mathcal{O}(1))$ over F_∞ give rise to canonical models of the curves $J^\pm(\Gamma)$. Explicitly, we have $F_\infty = F(w)$, where $w = w_{-15}$.

Poring over the traces from Algorithm 4.2.1, one suspects that $J_0(\mathcal{O}(1))$ has a 17-isogeny. Searching through the subset

$$X_0(17)(\mathbf{Q}(w)) \subset X_0(17)(F_\infty),$$

Algorithm 5.2.2 finds a candidate curve whose j-invariant equals

$$(53184785340479w - 30252086554835)/2^{34}$$

and whose conductor equals $\mathfrak{p}_2 \mathbf{Z}_{F_\infty}$. As in the case e2d5D4i, one shows that this curve does not descend to $\mathbf{Q}(w)$. The $\mathrm{Gal}(F_\infty|F)$-conjugate of this curve gives a candidate model of $J_0^-(\mathcal{O}(1))$.

Assuming the correctness of the models above (for which see the next section), we see as in the case e2d21D4 that the canonical models $J_0^\pm(K')$ resulting from a choice of K' in (3.20) for $K = \widehat{\mathcal{O}}(1)^\times$ are in fact independent of this choice. Moreover, there exists an isomorphism $J(K') \cong J(\mathcal{O})$ over F. This is possible because the two models above differ by a 2-isogeny over F_∞.

$\boxed{\textbf{e3d1D6i:}}$ We can reason in analogy with the case e2d1D6i. The group $\Gamma^{(2)}$ generates a level 7 Eichler order $\mathcal{O}(7)$ of B whose norm 1 group $\mathcal{O}(7)^1$ is given by $\Gamma^{(2)}$. The canonical model of $J(\Gamma)$ over $\mathbf{Q} = \mathbf{Q}_\infty$ is therefore isomorphic to the Jacobian $J_0(\mathcal{O}(7)) = J(\mathcal{O}(7))$. From [Elk98] and [GR06], we get the explicit equation

$$y^2 + xy + y = x^3 + x^2 - 104x + 101.$$

$\boxed{\textbf{e3d1D6ii:}}$ We know $j(J(\Gamma))$ from Chapter 6. The order $\mathcal{O} = \mathbf{Z}[\Gamma^{(2)}]$ is of level 4 and has $\mathcal{O}^1 = \langle \Gamma^{(2)}, AB \rangle$. Let $\mathcal{O}(1)$ be the maximal order containing $\mathcal{O}$. Then one calculates that $\mathcal{O}(1)/\mathcal{O} \cong (\mathbf{Z}/2\mathbf{Z})^2$ as $\mathbf{Z}$-modules. Algorithm 6.1.7 shows that we have $[\mathcal{O}(1)^1 : \mathcal{O}^1] = 4$, hence we are in case (iii) of Proposition 2.3.2. In particular, there is no level 2 order inbetween $\mathcal{O}$ and $\mathcal{O}(1)$. Since $\mathrm{nrd}(\widehat{\mathcal{O}}^\times) = \widehat{\mathbf{Z}}^\times$ by Proposition 2.3.2 again, the canonical model $J_0(\mathcal{O}) = J(\mathcal{O})$ of $J(\mathcal{O}^1)$ is defined over $\mathbf{Q}_\infty = \mathbf{Q}$: as usual, we can conclude that there is an Atkin-Lehner quotient of $J_0(\mathcal{O})$ giving a canonical model of $J(\Gamma)$ by invoking Lemma 3.3.4.

Using Theorem 3.1.6 and Algorithm 4.2.1, we conclude that this canonical model of $J(\Gamma)$ is given by

$$y^2 = x^3 - x^2 + 16x - 180,$$

the unique elliptic curve over $\mathbf{Q}$ with j-invariant $2^1 47^3/3^8$ and conductor 24.

$\boxed{\textbf{e3d1D10:}}$ The group $\Gamma^{(2)}$ generates a level 3^2 order $\mathcal{O} = \mathbf{Z}[\Gamma^{(2)}]$ for which $\mathcal{O}^1 = \Gamma^{(2)}$. There exists a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$ such that one has $\mathcal{O}(1)/\mathcal{O} \cong (\mathbf{Z}/3\mathbf{Z})^2$. Since the index $[\mathcal{O}(1)^1 : \mathcal{O}^1]$ equals 4 by Algorithm 6.1.7, we see that we are in case (iv) of Proposition 2.3.1. We also get that $\mathcal{O}^1 = \mathcal{O}(3)^1$ for the unique level 3 Eichler order inbetween $\mathcal{O}$ and $\mathcal{O}(1)$.

As in the case e2d12D3, we see that we can take $J_0(\mathcal{O}(3)) = J(\mathcal{O}(3))$ as a canonical model of $J(\Gamma)$; it is defined over $\mathbf{Q}_\infty = \mathbf{Q}$. This Jacobian was determined in [GR06] and [Elk98]: it is explicitly given by

$$y^2 + xy + y = x^3 - 19x + 26.$$

$\boxed{\textbf{e3d1D15:}}$ We can reason in analogy with the case e2d1D6i. The group $\langle \Gamma^{(2)}, B \rangle$ generates a maximal order $\mathcal{O}(1)$ of B whose norm 1 group $\mathcal{O}(1)^1$ is given by $\langle \Gamma^{(2)}, B\rangle$. Therefore we can obtain a canonical model of $J(\Gamma)$ by taking an Atkin-Lehner quotient of $J_0(\mathcal{O}(1)) = J(\mathcal{O}(1))$. This model can be calculated using [GR06]: it is explicitly given by

$$y^2 + xy + y = x^3 + x^2 - 135x - 660.$$

e3d5D5: There is a completely analogy between the case e2d5D4iii and the current one. $\Gamma^{(2)}$ generates an Eichler order $\mathcal{O}(\mathfrak{p}_3) = \mathbf{Z}_F[\Gamma^{(2)}]$ of level $\mathfrak{p}_3$ and with norm 1 group $\mathcal{O}(\mathfrak{p}_3)^1 = \langle \Gamma^{(2)}, A\rangle$. As usual, Lemma 3.3.4 shows that a canonical model of $J(\Gamma)$ is given by an Atkin-Lehner quotient of $J_0(\mathcal{O}(\mathfrak{p}_3)) = J(\mathcal{O}(\mathfrak{p}_3))$, which is canonically defined over $F_\infty = F$. An explicit equation is given by

$$y^2 + xy + y = x^3 + x^2 - 110x - 880.$$

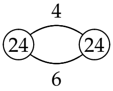
The corresponding curve duly has conductor $\mathfrak{p}_3\mathfrak{p}_5$ (*cf.* Theorem 3.1.6).

e3d5D9: This analogous to the case e2d5D4iii. We get the canonical model

$$y^2 + xy + y = x^3 + (\alpha - 1)x^2 + (-45\alpha - 28)x + (-847\alpha - 524).$$

of conductor $\mathfrak{p}_2\mathfrak{p}_3$. The same argument as in the case e2d5D4i shows that this model does not descend to $\mathbf{Q}$.

e3d8D9: Using the maximal order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma]$, whose norm 1 group equals Γ, this case is completely analogous to the case e2d13D4. Proposition 5.1.9 shows that the dual graph of $\mathrm{Sh}(\mathcal{O}(1))$ at $\mathfrak{p}_3$ is given by



The canonical model $J_0(\mathcal{O}) = J(\mathcal{O})$ has equation

$$y^2 = x^3 + (-2\alpha - 4)x^2 + (-154\alpha - 231)x + (-1064\alpha - 1520).$$

As in the case e2d5D4i, we see that $J_0(\mathcal{O})$ does not descend to $\mathbf{Q}$.

e3d12D3: The narrow class group is non-trivial in this case, which is analogous to the case e2d12D2. We know $j(J(\Gamma)) = 1728$ from Chapter 6. The group Γ generates a level $\mathfrak{p}_3$ non-Eichler order $\mathcal{O}(\mathfrak{p}_3) = \mathbf{Z}_F[\Gamma]$. Proposition 2.3.2 shows that

$$\mathrm{nrd}(\widehat{\mathcal{O}}(\mathfrak{p}_3)^\times) = U_{\mathfrak{p}_3}^2 \times \prod_{\mathfrak{p}\nmid 3} U_{\mathfrak{p}}^{(0)} = U_{\mathfrak{p}_3}^{(1)} \times \prod_{\mathfrak{p}\nmid 3} U_{\mathfrak{p}}^{(0)}.$$

Let $\kappa(\mathfrak{p}_3)$ be the residue field $\mathbf{Z}_F/\mathfrak{p}_3$. Since

$$\mathrm{Ker}(\mathbf{Z}_F^+ \longrightarrow \kappa(\mathfrak{p}_3)^\times/\kappa(\mathfrak{p}_3)^{\times 2}) = \mathbf{Z}_F^{\times 2},$$

we have $\mathrm{P}\mathcal{O}(\mathfrak{p}_3)^+ = \mathrm{P}\mathcal{O}(\mathfrak{p}_3)^1$ by Proposition 3.2.1. This means that we do not have to choose an N' as in Lemma 3.2.3 to construct a canonical model of $J(\Gamma)$:

we can simply take the Jacobian of one of the two components $\mathrm{Sh}_0^{\pm}(\mathcal{O}(\mathfrak{p}_3))$ of $\mathrm{Sh}(\mathcal{O}(\mathfrak{p}_3))$.

The curve $J_0(\mathcal{O}(\mathfrak{p}_3))$ has canonical field of definition $F_{\mathfrak{p}_3\infty} = F_\infty = F(i)$: indeed, since $\mathfrak{p}_3$ is non-trivial in the narrow class group, the proof of Lemma 3.2.3 shows that the projection map $\mathrm{Cl}(\mathfrak{p}_3\infty) \to \mathrm{Cl}(\infty)$ is an isomorphism. As for the case e2d12D2, we see that the elliptic curves $J_0^{\pm}(\mathcal{O}(\mathfrak{p}_3))$ are isomorphic over F_∞.

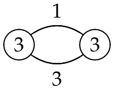
Combining Theorem 3.1.6 and Algorithm 4.2.1, we can determine the curve $J_0(\mathcal{O}(\mathfrak{p}_3))$. It is the base extension to F_∞ of

$$y^2 + (\alpha+1)xy + \alpha y = x^3 + (\alpha-1)x^2.$$

This curve has conductor $\mathfrak{p}_3^2$. It is isogenous but not isomorphic to its $\mathrm{Gal}(F|\mathbf{Q})$-conjugate (*cf.* Theorem 4.4 in [Hid81]): over F_∞, these curves become isomorphic, as can also be deduced from Theorem 3.1.7 using triviality of the narrow type number. Both of these base extensions have conductor $\mathfrak{p}_3^2$ over F_∞.

e3d13D3i/ii: We take the first of these two cases, which are conjugate by Theorem 3.1.7. $\Gamma^{(2)}$ generates a level ${\mathfrak{p}'_3}^2$ non-Eichler order $\mathcal{O} = \mathbf{Z}_F[\Gamma^{(2)}]$ such that $\mathcal{O}^1 = \langle \Gamma^{(2)}, AB \rangle$. The index in Table A.2 shows that we are in case (iv) of Proposition 2.3.1. As for the case e3d1D10, we see that there is a level $\mathfrak{p}'_3$ Eichler order $\mathcal{O}(\mathfrak{p}'_3)$ inbetween $\mathcal{O}(1)$ and $\mathcal{O}$ for which $\mathcal{O}(\mathfrak{p}'_3)^1 = \mathcal{O}^1$.

We use $J_0(\mathcal{O}(\mathfrak{p}'_3)) = J(\mathcal{O}(\mathfrak{p}'_3))$ as a canonical model of $J(\mathcal{O}^1)$. It is defined over $F_\infty = F$, and a canonical model of $J(\Gamma)$ can be obtained by taking a suitable Atkin-Lehner quotient. Proposition 5.1.9 gives the following dual graph at $\mathfrak{p}_3$:



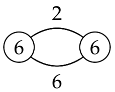
The usual search of $X_0(2)$ gives the candidate curve

$$y^2 + xy + y = x^3 + x^2 + (-190\alpha - 248)x + (1303\alpha + 1697)$$

of conductor $\mathfrak{p}_3\mathfrak{p}'_3$ as a canonical model of $J(\mathcal{O}^1)$. This curve is isogenous to its $\mathrm{Gal}(F|\mathbf{Q})$-conjugate, but it does not descend to $\mathbf{Q}$, since its j-invariant is not rational.

Using prime isogenies of degree ≤ 50, we found 12 elliptic curves in the isogeny class of the candidate curve above. The next section will show how to prove that this is indeed the full isogeny class of $J_0(\mathcal{O}(\mathfrak{p}'_3))$.

It remains to recover the corresponding canonical model of $J(\Gamma)$. Although we could use Proposition 5.1.10 for this, we can also conclude by an ad hoc argument. Indeed, the graph above has 2 non-trivial automorphisms, only one of which gives rise to a genus 1 quotient graph, namely the unique automorphism that fixes the vertices. The corresponding dual graph is



By Proposition 5.1.10, we see that in fact

$$J(\Gamma) \cong J_0(\mathcal{O}(\mathfrak{p}_3'))/w(\mathfrak{p}_3).$$

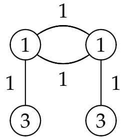
There is a unique curve that is 2-isogenous to $J_0(\mathcal{O}(\mathfrak{p}_3'))$ and whose j-invariant has valuation -8 at $\mathfrak{p}_3$. This curve yields a canonical model of $J(\Gamma)$. It is given by

$$y^2 + xy + y = x^3 + x^2 + (495\alpha + 637)x + (9261\alpha + 12053).$$

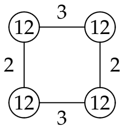
e3d17D36: We are in a similar situation as in the case e2d13D4. $\Gamma^{(2)}$ generates a maximal order $\mathcal{O}$ whose norm 1 group $\mathcal{O}^1$ is given by $\Gamma^{(2)}$. Therefore we can take $J_0(\mathcal{O}) = J(\mathcal{O})$ as a canonical model of $J(\Gamma)$: it has field of definition $F_\infty = F$.

By Theorem 3.1.7, $j(J_0(\mathcal{O}))$ is rational. Using Cremona's tables and Algorithm 4.2.1, we end up with 4 isogenous candidates. Proposition 5.1.9 gives the following dual graphs:

At $\mathfrak{p}_2$ and $\mathfrak{p}_2'$:



At $\mathfrak{p}_3$:



These graphs determine the correct curve: it is given by

$$y^2 + xy + \alpha y = x^3 - \alpha x^2 + (-19694\alpha - 30770)x + (-2145537\alpha - 3350412).$$

and has conductor $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3$. As for the case e2d5D4i, one proves that this curve does not descend to $\mathbf{Q}$.

e3d21D3: The group $\Gamma^{(2)}, AB\rangle$ is the norm 1 group of the level $\mathfrak{p}_3$ non-Eichler order $\mathcal{O}(\mathfrak{p}_3) = \mathbf{Z}_F[\langle\Gamma^{(2)}, AB\rangle]$. We see from Proposition 2.3.2 that

$$\mathrm{nrd}(\widehat{\mathcal{O}}(\mathfrak{p}_3)^\times) = U_{\mathfrak{p}_3}^2 \times \prod_{\mathfrak{p}\nmid 3} U_{\mathfrak{p}}^{(0)} = U_{\mathfrak{p}_3}^{(1)} \times \prod_{\mathfrak{p}\nmid 3} U_{\mathfrak{p}}^{(0)}.$$

A canonical model of $J(\Gamma)$ can be constructed by taking an Atkin-Lehner quotient of $J_0(\mathcal{O}(\mathfrak{p}_3))$. The ray class extension

$$F \subsetneq F_\infty = F(\sqrt{-3}) \subsetneq F_{\mathfrak{p}_3\infty}.$$

of F_∞ over which $J_0(\mathcal{O}(\mathfrak{p}_3))$ is canonically defined is non-trivial.

Proposition 3.2.1 shows that by the same token, we have

$$[\mathrm{P}\mathcal{O}(\mathfrak{p}_3)^+ : \mathrm{P}\mathcal{O}(\mathfrak{p}_3)^1] = 2.$$

The group $\mathcal{O}(\mathfrak{p}_3)^+$ has signature $(0; 2^3, 3)$: as for the case e2d24D3, this was calculated by John Voight. To construct a canonical model of $J(\mathcal{O}(\mathfrak{p}_3)^1)$, we therefore have to choose groups N' and K' as in (3.20) for $K = \widehat{\mathcal{O}}(\mathfrak{p}_3)^\times$. As in the case e2d12D2, we get

$$N(K') \supset N(\widehat{\mathcal{O}}(\mathfrak{p}_3)^\times) = N(\widehat{\mathcal{O}}(1)^\times),$$

and Proposition 2.6.2 then gives that the narrow type number of K' equals 1. Therefore the 4 components of $\mathrm{Sh}(K')$ over $F_{K'} = F_{\mathfrak{p}_3\infty}$ are isomorphic.

We can say more. The discriminant of B and the level $\mathfrak{p}_3$ of $\mathcal{O}(\mathfrak{p}_3)$ are Galois invariant. If we therefore choose the prime at which N' is non-maximal to be Galois invariant as well (taking N' to be non-maximal at the prime $\mathfrak{p}_2$ above 2, for example), then Theorem 3.1.7 shows that

$$j(J_0(K')) \in \mathbf{Q}.$$

Note that this conclusion is true regardless of the choice of N', since the geometric components of $\mathrm{Sh}_0(K')$ are independent of the choice of N' (*cf.* Proposition 3.2.4).

For an explicit calculation of a canonical model $J_0(K')$, we take N' to be non-maximal at $\mathfrak{p}_2$. Proceeding as in the case e2d13D4, we get that the isogeny class of $J_0(K')$ is then given by the unique twist of conductor $\mathfrak{p}_3^2$ over $F_{\mathfrak{p}_3\infty}$ of the elliptic curve

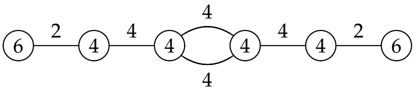
$$y^2 + xy = x^3 - x^2 - 2x - 1.$$

over $\mathbf{Q}$. This twist descends to the subfields of F of discriminant -1323, but the usual argument as in the case e2d5D4i shows that a further descent is not possible.

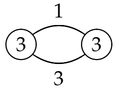
A priori, the model of $J(\mathcal{O}(\mathfrak{p}_3)^1)$ obtained above depends on the choice of N' in Lemma 3.2.3 and the resulting group K' from (3.20). However, the fact that there is no factor $\mathfrak{p}_2$ in the conductor above leads one to suspect that the model is independent of the choice of N'. Experimentally, this is true, but as in the case e2d12D3, we have not been able to prove this fact. We have used the canonical model above in Table A.3.

e3d28D18: $\Gamma^{(2)}$ generates a maximal order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$ with norm 1 group given by $\mathcal{O}(1)^1 = \Gamma^{(2)}$. Proposition 5.1.9 gives the following dual graphs for $\mathrm{Sh}(\mathcal{O}(1))$:

At $\mathfrak{p}_2$: twice



At $\mathfrak{p}_3$ and $\mathfrak{p}_3'$: twice



As in the case e2d21D4, we conclude that $\mathcal{O}(1)^+$ has signature $(1;3,3)$. The canonical model $J_0(\mathcal{O}(1))$ is defined over $F_\infty = F(i)$. We also take

$$N' = U_{\mathfrak{p}_3}^{(1)} \times \prod_{\mathfrak{p} \nmid \mathfrak{p}_3} U_{\mathfrak{p}}^{(0)}$$

in Lemma 3.2.3 and let K' be as in (3.20) for $K = \widehat{\mathcal{O}}(1)^{\times}$. A canonical model of $J(\Gamma)$ is then given by $J_0(K')$. As in the case e2d21D4, this model does not depend on the choice of N'.

Since the narrow type number of $\mathcal{O}(1)$ equals 1 (*cf.* Proposition 2.6.2), we see that the components of $\mathrm{Sh}(\mathcal{O}(1))$ are isomorphic over F_∞. Moreover, since the discriminant of B is Galois invariant, Theorem 3.1.7 gives that

$$j(J_0(\mathcal{O}(1))) \in \mathbf{Q}.$$

We can therefore proceed as in the case e2d13D4. Assisted by the dual graph above we obtain that $J_0(\mathcal{O}(1))$ is the unique twist of conductor $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3\mathfrak{p}_3'$ over F_∞ of either of the elliptic curves

$$\begin{aligned} y^2 + xy &= x^3 + x^2 + 122x - 10940 \\ y^2 + xy + y &= x^3 + 2x + 32 \end{aligned}$$

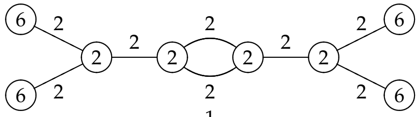
over $\mathbf{Q}$ with conductor $2^1 3^1 7^2$. As suggested by Theorem 4.4 in [Hid81], this twist has two models over F with conductor $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'$. They are given by

$$y^2 + \alpha xy + (\alpha + 1)y = x^3 + (-\alpha - 1)x^2 + (16\alpha + 44)x + (1312\alpha + 3472)$$

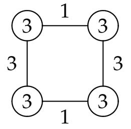
and its conjugate.

The canonical model $J_0(K')$ is 2-isogenous over F_∞ to the model $J_0(\mathcal{O}(1))$ given above. This does not quite determine $J_0(K')$, as $J_0(\mathcal{O}(1))$ has full 2-torsion over F_∞. However, Proposition 5.1.11 enables us to calculate the dual graphs of $\mathrm{Sh}(K')$. These are given by

At $\mathfrak{p}_2$: twice



At $\mathfrak{p}_3$ and $\mathfrak{p}_3'$: twice



Only one 2-isogeny from $J_0(\mathcal{O}(1))$ then results in the correct valuations. This determines the canonical model $J_0(K')$ of $J(\Gamma)$: it can be described as the base extension of

$$y^2 + \alpha xy + (\alpha + 1)y = x^3 + (-\alpha - 1)x^2 + (-944\alpha - 2496)x + (25532\alpha + 67552)$$

or of its $\mathrm{Gal}(F|\mathbf{Q})$-conjugate. The familiar argument from the case e2d5D4i shows that, though isomorphic to its Galois conjugate, $J_0(K')$ does not descend to $\mathbf{Q}$.

e3d49D1: This is analogous to the case e2d81D1. $\Gamma^{(2)}$ generates a level $\mathfrak{p}_3$ Eichler order $\mathcal{O}(\mathfrak{p}_3)$ whose norm 1 group $\mathcal{O}^1$ is given by Γ. We take $J_0(\mathcal{O}) = J(\mathcal{O})$ as a canonical model of $J(\Gamma)$. The usual methods yield that this curve is in the base extension of the $\mathbf{Q}$-isogeny class 147B in Cremona's tables. The calculation of the corresponding Belyĭ map in Chapter 6 would determine $J_0(\mathcal{O})$ up to isomorphism.

e3d81D1: We know that $j(J(\Gamma)) = 0$ from Chapter 6. Let $\mathcal{O} = \mathbf{Z}_F[\Gamma]$. This is a level $\mathfrak{p}_3^3$ non-Eichler order for which $\mathcal{O}^1 = \Gamma$. There exists a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$ such that

$$\mathcal{O}(1)/\mathcal{O} \cong \mathbf{Z}_F/\mathfrak{p}_3 \times \mathbf{Z}_F/\mathfrak{p}_3^2$$

as $\mathbf{Z}_F$-modules. We verified that there is no order inbetween $\mathcal{O}$ and $\mathcal{O}(1)$ whose norm 1 group has genus 1 (which can also be deduced using Proposition 2.3.1). Therefore we take the curves $J_0^{\pm}(\mathcal{O})$ as a canonical models of $J^{\pm}(\Gamma)$.

Algorithm 2.4.3 gives that

$$\operatorname{nrd}(\widehat{\mathcal{O}}^{\times}) = U_{\mathfrak{p}_3}^{(1)} \times \prod_{\mathfrak{p} \nmid 3} U_{\mathfrak{p}}^{(0)},$$

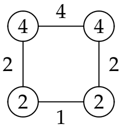
The corresponding ray class field extension $F_{\mathfrak{p}_3\infty} = F(\sqrt{-3})$ is the canonical field of definition for $J_0(\mathcal{O})$. Performing the calculations as for the case e2d5D4i, we obtain that the curve with Weierstrass equation

$$y^2 + y = x^3 - 7$$

is the only twist over $F_{\mathfrak{p}_3\infty}$ (of conductor $\mathfrak{p}_3^3$) whose traces agree with those obtained using Algorithm 4.2.1. Therefore both $J_0^+(\mathcal{O})$ and $J_0^-(\mathcal{O})$ are isomorphic to this elliptic curve.

e4d8D2i/iii: We already encountered these two conjugate cases in Chapter 6, where we failed to calculate them. Consider the first case. Using the order $\mathcal{O}(\mathfrak{p}_{17})$ mentioned in Chapter 6, we get a canonical model $J_0(\mathcal{O}(\mathfrak{p}_{17}))$ of $J(\mathcal{O}(\mathfrak{p}_{17})^1) = J(\langle \Gamma^{(2)}, A \rangle)$. A canonical model of $J(\Gamma)$ can then be obtained as an Atkin-Lehner quotient of this curve.

The curve $J_0(\mathcal{O}(\mathfrak{p}_{17})) = J(\mathcal{O}(\mathfrak{p}_{17}))$ has canonical field of definition $F_\infty = F$. Proposition 5.1.9 gives the following dual graph at $\mathfrak{p}_2$:



Performing the usual search of $X_0(2)$, we obtain the candidate curve

$$y^2 + xy = x^3 + (\alpha - 1)x^2 + (-598\alpha - 851)x + (-9648\alpha - 13635).$$

There is a unique curve over F that is 2-isogenous to this curve. Assuming the correctness of the candidate above, this is then the canonical model of $J(\Gamma)$. It is given by

$$y^2 + xy = x^3 + (\alpha - 1)x^2 + (-38\alpha - 51)x + (-160\alpha - 227).$$

e4d8D2ii: Like the case e2d5D4ii, this case is special: here, too, the order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$ is maximal, and we have a non-trivial inclusion $\Gamma \subsetneq \mathcal{O}(1)^1$. We know $j(J(\Gamma))$ from Chapter 6. Moreover, we have

$$F(j(J(\Gamma))) = F(i) = F_{\mathfrak{p}_2^2\infty}.$$

We see that to obtain a canonical model, we need to pass to the non-trivial ray class field $F_{\mathfrak{p}_2^2\infty}$ at least. Over that field, there is a model with conductor $\mathfrak{p}_2\mathfrak{p}_3^3$.

It follows from the definitions in (2.4) (*cf.* Remark (i) at the end of Section 6.1) that the neutral component of a curve $\mathrm{Sh}(K)$ coming from a compact open subgroup K of $\widehat{B}^\times$ is contained in the Galois closure of a cover

$$X(\mathcal{O}^1) \longrightarrow X(\mathcal{O}(1)^1)$$

arising from a suborder $\mathcal{O}$ of $\mathcal{O}(1)$. Motivated by the conductor above, we have tried orders $\mathcal{O}$ of level $\mathfrak{N} = \mathfrak{p}_2^i\mathfrak{p}_3^j$ with i and j small, and proceeded as for the case e2d5D4ii. Yet we failed to obtain the cover $X(\Gamma) \to X(\mathcal{O}(1)^1)$ as a subcover of the resulting Galois closures, and hence also failed to find a canonical model of $X(\Gamma)$. We conjecture that the group $\Gamma \subset \mathcal{O}(1)^1$ is not congruence.

e4d8D7i/ii: We take the first of these two conjugate cases. The group $\Gamma^{(2)}$ generates a level $\mathfrak{p}_2^4$ non-Eichler order $\mathcal{O} = \mathbf{Z}_F[\Gamma^{(2)}]$ whose norm 1 group is given by $\Gamma^{(2)}$. There exists a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$ such that

$$\mathcal{O}(1)/\mathcal{O} \cong (\mathbf{Z}_F/\mathfrak{p}_2^2)^2.$$

Moreover, there exists a unique level $\mathfrak{p}_2^3$ order $\mathcal{O}'$ inbetween $\mathcal{O}$ and $\mathcal{O}(1)$ such that

$$\mathcal{O}(1)/\mathcal{O} \cong \mathbf{Z}_F/\mathfrak{p}_2 \times \mathbf{Z}_F/\mathfrak{p}_2^2$$

and $\mathcal{O}'^1 = \mathcal{O}^1$. Algorithm 2.4.3 gives $\mathrm{nrd}(\widehat{\mathcal{O}}'^\times) = \widehat{\mathbf{Z}}_F^\times$. We consider $J_0(\mathcal{O}') = J(\mathcal{O}')$: arguing as in the case e2d12D3, we see that this curve gives a canonical model of $J(\Gamma)$ defined over $F_\infty = F$.

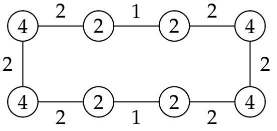
The rest of this case is completely analogous to the case e2d8D7. We get the candidate

$$y^2 + \alpha xy + \alpha y = x^3 + \alpha x^2 + (-10\alpha - 17)x + (-31\alpha - 44).$$

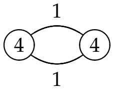
of conductor $\mathfrak{p}_2^3\mathfrak{p}_7$.

e4d8D98: There is a complete analogy between the case e2d13D4 and the current one. We get the dual graphs

At $\mathfrak{p}_2$:



At $\mathfrak{p}_7$ and $\mathfrak{p}_7'$:



and a canonical model

$$y^2 + xy + y = x^3 - 2731x - 55146$$

of $J(\Gamma)$.

e4d2304D2: This is completely analogous to the case e2d12D2. Working with $\mathcal{O}(\mathfrak{p}_2) = \mathbf{Z}_F[\Gamma]$ and choosing

$$N' = U_{\mathfrak{p}_2}^{(2)} \times \prod_{\mathfrak{p} \nmid \mathfrak{p}_2} U_{\mathfrak{p}}^{(0)}$$

in (3.20) for $K = \widehat{\mathcal{O}}(\mathfrak{p}_2)^\times$ yields the model given by the base extension of both

$$y^2 = x^3 + w_3 x^2 + x + (3w_3 + 5)$$

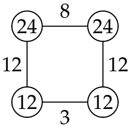
and its conjugate. These curves have conductor $\mathfrak{p}_2^4$ over F_∞, and do not descend to $\mathbf{Q}$.

Choosing a different N' results in a different canonical K'-model. However, the other orders $\mathcal{O}$ in Table A.2 all have

$$\mathrm{nrd}(\widehat{\mathcal{O}}^\times) = U_{\mathfrak{p}_2}^{(2)} \times \prod_{\mathfrak{p} \nmid 2} U_{\mathfrak{p}}^{(0)},$$

and the corresponding canonical models $J_0(\mathcal{O})$ are all isomorphic to the one determined above. Therefore, as in the case e2d12D2, we have chosen this as a canonical model in Table A.3.

e4d2624D4i/ii: We reason in analogy with the case e2d725D16. At $\mathfrak{p}_2$, the dual graph of the canonical model $J_0(\mathcal{O}) = J(\mathcal{O})$ of $J(\Gamma)$ is given by



Spurred on by the traces from from Algorithm 4.2.1 and Theorem 3.1.7, we performed a guided search of $X_0(5)(\mathbf{Q}(w_2))$. The resulting candidate for $J_0(\mathcal{O})$ can be obtained by base extending the curve over $\mathbf{Q}(w_2)$ given by

$$y^2 + xy + y = x^3 + (-w_2 - 1)x^2 + (391w_2 - 448)x + (4342w_2 - 6267)$$

to F and taking the unique twist with conductor $\mathfrak{p}_2$ over F; the base extension itself has additive reduction at the prime $\mathfrak{p}_{41}$ over 41 ramifying in the extension $F|\mathbf{Q}(w_2)$. As in the case e2d5D4i, one shows that $J_0(\mathcal{O})$ does not descend to a subfield of F.

e5d5D5i/ii: These two conjugate cases are completely analogous to the case e2d5D4iii. For the first, we end up with the equation

$$y^2 + (\alpha + 1)xy + \alpha y = x^3 - \alpha x^2 + (-267\alpha - 166)x + (-2416\alpha - 1494)$$

for $J_0(\mathcal{O}(\mathfrak{p}_{11}))$, and

$$y^2 + (\alpha+1)xy + \alpha y = x^3 - \alpha x^2 + (-4217\alpha - 2611)x + (-157816\alpha - 97533).$$

is a canonical model of $J(\Gamma)$.

e5d5D5iii: We determined the $j(J(\Gamma))$ in Chapter 6. The order $\mathcal{O} = \mathbf{Z}_F[\Gamma^{(2)}]$ has norm 1 group $\mathcal{O}^1 = \langle \Gamma^{(2)}, A \rangle$. There exists a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$ such that $\mathcal{O}(1)/\mathcal{O} \cong (\mathbf{Z}_F/\mathfrak{p}_2)^2$ as $\mathbf{Z}_F$-modules. The index from Table A.2 shows that we are in case (iv) of Proposition 2.3.1. That is, $\mathcal{O} = \mathcal{O}(\mathfrak{p}_2^2)$ is a level $\mathfrak{p}_2^2$ Eichler order. By Proposition 2.4.2 we therefore have $\mathrm{nrd}(\widehat{\mathcal{O}}(\mathfrak{p}_2^2)^\times) = \widehat{\mathbf{Z}}_F^\times$, and we can take the curve $J_0(\mathcal{O}(\mathfrak{p}_2^2)) = J(\mathcal{O}(\mathfrak{p}_2^2))$ as a canonical model of $J(G)$. As usual, a canonical model of $J(\Gamma)$ can be obtained as an Atkin-Lehner quotient.

The methods first encountered in the case e2d5D4i the give us the following models. The canonical model of $J(\Gamma)$ is given by

$$y^2 = x^3 + x^2 - 36x - 140.$$

$J_0(\mathcal{O}(\mathfrak{p}_2^2))$ is the unique curve that is 2-isogenous over F to this curve. It has equation

$$y^2 = x^3 + x^2 - 41x - 116.$$

Both curves have conductor $\mathfrak{p}_2^2\mathfrak{p}_5$ and are base extensions of elliptic curves over $\mathbf{Q}$ with conductor $2^2 5$. The isogeny between them also descends to $\mathbf{Q}$.

e5d5D9: In Chapter 6, we have determined $j(J(\Gamma))$ for this case. Though this also narrows down the possibilities for $j(J_0(\mathcal{O}(\mathfrak{p}_5)))$ to 3 values, the cover needed to calculate the correct value was a tad involved.

The theory of canonical models, however, will enable us to determine this j-invariant. Indeed, the canonical model of $J(\Gamma)$ is an Atkin-Lehner quotient of $J_0(\mathcal{O}(\mathfrak{p}_5))$. By Theorem 3.1.6, it is given by the unique twist over $F_\infty = F$ of conductor $\mathfrak{p}_3\mathfrak{p}_5$ whose j-invariant equals the $j(J(\Gamma))$ from Chapter 6. We get the model

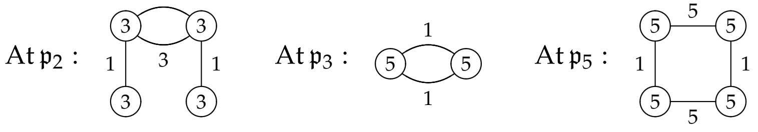
$$y^2 + xy + y = x^3 + x^2 + 35x - 28.$$

It is the base extension of a elliptic curve over $\mathbf{Q}$ of conductor 15. Now this model has a unique 2-isogeny over F, which necessarily has $J_0(\mathcal{O}(\mathfrak{p}_5))$ as its codomain. The latter curve is therefore given by

$$y^2 + xy + y = x^3 + x^2 - 10x - 10$$

and has j-invariant $13^3 37^3/3^4 5^4$.

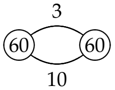
e5d5D180: This is completely analogous to the case e2d13D4. We get the dual graphs



and a canonical model of $J(\Gamma)$ given by

$$y^2 + xy + y = x^3 - 334x - 2368.$$

e5d725D25i/ii: We parallel the reasoning employed in the case e2d725D16. At the prime $\mathfrak{p}_5$, the dual graph of the canonical model $J_0(\mathcal{O}) = J(\mathcal{O})$ of $J(\Gamma)$ is given by



The traces from from Algorithm 4.2.1, along with Theorem 3.1.7, lead us to perform a guided search of $X_0(13)(\mathbf{Q}(w_5))$. The resulting candidate for $J_0(\mathcal{O})$ can be obtained by base extending the curve over $\mathbf{Q}(w_5)$ given by

$$y^2 + (w_5 + 1)y = x^3 + (w_5 - 1)x^2 + (587w_5 - 2331)x + (32400w_5 - 32950)$$

to F and taking the unique twist with conductor $\mathfrak{p}_2$ over F; as in the case e2d726D16, the base extension itself has additive reduction at the prime $\mathfrak{p}_{29}$ over 29 ramifying in the extension $F|\mathbf{Q}(w_5)$. Arguing as in the case e2d5D4i, one shows that $J_0(\mathcal{O})$ does not descend to a subfield of F.

e5d1125D5: The narrow class group is non-trivial for this case. We saw in Chapter 6 that $j(J(\Gamma)) = 0$. The level $\mathfrak{p}_5$ order $\mathcal{O}(\mathfrak{p}_5) = \mathbf{Z}_F[\Gamma^{(2)}]$ satisfies $\mathcal{O}(\mathfrak{p}_5)^1 = \Gamma$. Proposition 2.3.2 gives

$$\mathrm{nrd}(\widehat{\mathcal{O}}(\mathfrak{p}_5)^\times) = U_{\mathfrak{p}_5}^2 \times \prod_{\mathfrak{p}\nmid 5} U_{\mathfrak{p}}^{(0)}.$$

Let $\kappa(\mathfrak{p}_5)$ be the residue field of $\mathbf{Z}_F$ at $\mathfrak{p}_5$. Then one calculates

$$\mathrm{Ker}(\mathbf{Z}_F^+ \longrightarrow \kappa(\mathfrak{p}_5)^\times / \kappa(\mathfrak{p}_5)^{\times 2}) = \mathbf{Z}_F^{\times 2}. \tag{7.3}$$

Hence Proposition 3.2.1 shows that $\mathrm{P}\mathcal{O}(\mathfrak{p}_5)^1 = \mathrm{P}\mathcal{O}(\mathfrak{p}_5)^+$. Moreover, the proof of Lemma 3.2.3 shows that (7.3) also implies that the projection

$$\mathrm{Cl}(\mathrm{nrd}(\widehat{\mathcal{O}}(\mathfrak{p}_5)^\times)\infty) \longrightarrow \mathrm{Cl}(\infty)$$

is an isomorphism. We conclude that the Jacobians $J_0^{\pm}(\mathcal{O}(\mathfrak{p}_5))$, which are defined over

$$F_{\widehat{\mathcal{O}}(\mathfrak{p}_5)^\times} = F_\infty = F(\sqrt{-3}),$$

give canonical models of $J(\Gamma) = J(\mathcal{O}^1)$.

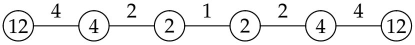
As in the case e2d12D2, we see that the narrow type number of $\mathcal{O}(\mathfrak{p}_5)$ is equal to 1. Therefore the Jacobians $J_0^{\pm}(\mathcal{O}(\mathfrak{p}_5))$ are isomorphic. The standard procedure gives a model of conductor $\mathfrak{p}_5^2$ that be described as the base extension of either

$$\begin{aligned} y^2 + (\alpha + 1)y =& x^3 + (\alpha^3 - \alpha^2 - 1)x^2 \\ &+ (-2\alpha^3 + 7\alpha^2 - 5\alpha - 1)x + (6\alpha^3 - 14\alpha^2 - 2\alpha + 12) \end{aligned}$$

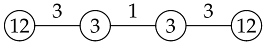
or one of its conjugates. Over F, these 4 conjugate curves give 1 isogeny class and 2 isomorphism classes. As in the case e2d5D4i, this model does not descend to a subfield of F. It has conductor $\mathfrak{p}_5^2$ over F_∞.

e6d12D66i/ii: The base field for this case again has non-trivial narrow class group. These two cases are conjugate (*cf.* Theorem 3.1.7). We consider the first. The order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$ is maximal and satisfies $\mathcal{O}(1)^1 = \Gamma^{(2)}$. The genus of the group $\mathcal{O}(1)^+$ equals 0. Indeed, Proposition 5.1.9 gives the following dual graphs for $\mathrm{Sh}(\mathcal{O}(1))$:

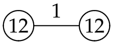
At $\mathfrak{p}_2$: twice



At $\mathfrak{p}_3$: twice



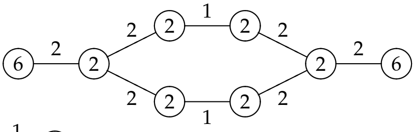
At $\mathfrak{p}_{11}$: twice



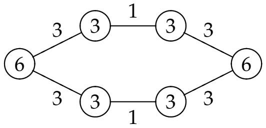
Therefore we have to choose a K' as in (3.20) for $K = \widehat{\mathcal{O}}(1)^\times$ in order to obtain a canonical model $J_0(K')$ of $J(\Gamma)$. The canonical field of definition for $J_0(K')$ is given by $F_\infty = F(i)$. Moreover, the narrow type number equals 1 once again, hence the Jacobian $J_0^-(K')$ of the other connected component of $\mathrm{Sh}(K')$ over F_∞ is isomorphic to $J_0(K')$.

Proposition 5.1.11 gives the following dual graphs for $\mathrm{Sh}(K')$:

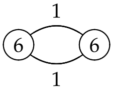
At $\mathfrak{p}_2$: twice



At $\mathfrak{p}_3$: twice



At $\mathfrak{p}_{11}$: twice



These are covers of the graphs obtained for $\mathrm{Sh}(\mathcal{O})$. Also, as in the cases e2d8D7 or e2d21D4, we see that $J_0(K')$ has a 2-isogeny irrespective of the choice of K', and as in the case e2d8D2, $J_0(K')$ is defined over F. Let us first take

$$N' = U^{(1)}_{\mathfrak{p}_3} \times \prod_{\mathfrak{p}\nmid 3} U^{(0)}_{\mathfrak{p}}$$

in (3.20). Searching $X_0(2)(F)$ using Algorithm 5.2.2 then gives the candidate model obtained by base extending the curve

$$y^2 + xy + (\alpha+1)y = x^3 + (\alpha-1)x^2 + (-405\alpha - 836)x + (4739\alpha + 7704).$$

It has conductor $\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_{11}\mathbf{Z}_{F_\infty}$.

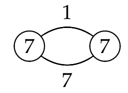
The choice of N' affects the conductor of the resulting canonical K'-model of $J(\Gamma)$: for example, choosing N' to be non-trivial at $\mathfrak{p}_2$, $\mathfrak{p}_{11}$ or $\mathfrak{p}'_{11}$, respectively, we get twists of the K'-model above of conductor $\mathfrak{p}_2^4\mathfrak{p}_3\mathfrak{p}_{11}$, $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{11}^2$ and $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{11}\mathfrak{p}_{11}'^2$.

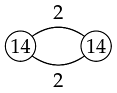
e7d49D1: This case is completely analogous to the case e2d5D4iii. We know $j(J(\Gamma))$ from Chapter 6. The Jacobian $J(\Gamma)$ is given by an Atkin-Lehner quotient of $J_0(\mathcal{O}(\mathfrak{p}_2\mathfrak{p}_7)) = J(\mathcal{O}(\mathfrak{p}_2\mathfrak{p}_7))$, where $\mathcal{O}(\mathfrak{p}_2\mathfrak{p}_7)$ is a level $\mathfrak{p}_2\mathfrak{p}_7$ Eichler order. We obtain the equation

$$y^2 + xy + y = x^3 - 36x - 70$$

for the canonical model of $J(\Gamma)$ over $F_\infty = F$. Finding a canonical model of $J(\mathcal{O}(\mathfrak{p}_2\mathfrak{p}_7))$ from this is not quite straightforward as the model above has full 2-torsion over F.

$\boxed{\textbf{e7d49D91i/ii/iii:}}$ These three conjugate cases are similar to the case e2d8D7. We treat the first. The order $\mathcal{O}(1) = \mathbf{Z}_F[\Gamma^{(2)}]$ is maximal and has norm 1 group $\mathcal{O}(1)^1 = \langle \Gamma^{(2)}, B \rangle$. A canonical model of $J(\Gamma)$ is given by an Atkin-Lehner quotient of $J_0(\mathcal{O}(1))$. It is defined over $F_\infty = F$. Proposition 5.1.9 gives the following dual graphs for $\mathrm{Sh}(\mathcal{O}(1))$:

At $\mathfrak{p}_7$: 

At $\mathfrak{p}_{13}$: 

As in the case e2d8D7, one sees that $J_0(\mathcal{O}(1))$ has a 2-isogeny. Algorithm 5.2.2 yields a candidate model with j-invariant

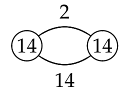
$$(n_2\alpha^2 + n_1\alpha + n_0)/7^3 13^4$$

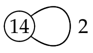
and conductor $\mathfrak{p}_7\mathfrak{p}_{13}$. Here

$$\begin{aligned} n_2 &= 8961331728253148016, \\ n_1 &= -20136149792113936343, \\ n_0 &= 7186826906603787494. \end{aligned}$$

As usual, we refer to the next section for a proof of correctness of the isogeny class above; there we will also show that this class can be generated by using prime isogenies of degree ≤ 50.

To recover a canonical model of $J(\Gamma)$, we have to divide out an Atkin-Lehner involution. As in the case e3d13D3, there is a unique non-trivial involution for which the corresponding quotient of $J_0(\mathcal{O}(1))$ has genus 1. The dual graphs of this quotient are given by

At $\mathfrak{p}_7$: 

At $\mathfrak{p}_{13}$: 

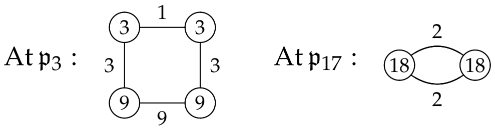
The resulting canonical model of $J(\Gamma)$ has j-invariant

$$(n_2'\alpha^2 + n_1'\alpha + n_0')/7^6 13^2$$

and conductor $\mathfrak{p}_7\mathfrak{p}_{13}$. Here

$$\begin{aligned} n_2' &= -8058460190096647498093, \\ n_1' &= 4472108028759348587577, \\ n_0' &= 1810719565899964740488 5. \end{aligned}$$

e9d81D51i/ii/iii: These cases are completely analogous to the previous. The dual graphs of $\mathrm{Sh}(\mathcal{O}(1))$ obtained from Proposition 5.1.9 are given by



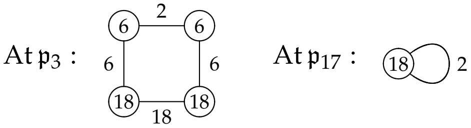
We get a candidate with j-invariant

$$(n_2\alpha^2 + n_1\alpha + n_0)/3^6 17^4$$

and conductor $\mathfrak{p}_3\mathfrak{p}_{17}$. Here

$$\begin{aligned} n_2 &= 257154008212105, \\ n_1 &= 479060149170145, \\ n_0 &= 139274003304361. \end{aligned}$$

To recover $J(\Gamma)$, we use the unique pair of genus 1 quotient graphs



We obtain the unique elliptic curve over F with j-invariant

$$(n_2'\alpha^2 + n_1'\alpha + n_0')/3^{11}17^2$$

and conductor $\mathfrak{p}_3\mathfrak{p}_{17}$. Here

$$\begin{aligned} n_2' &= -78367545688483633, \\ n_1' &= 27216689077016112, \\ n_0' &= 225650240167014325. \end{aligned}$$

e11d14641D1: $j(J(\Gamma))$ is known to us from Chapter 6. We reason as in the case e2d5D4iii. A canonical model of $J(\Gamma)$ is given by $J_0(\mathcal{O}(\mathfrak{p}_{11})) = J(\mathcal{O}(\mathfrak{p}_{11}))$, which is defined over $F_\infty = F$. We get the equation

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

It is the base extension of the strong Weil curve over $\mathbf{Q}$ of conductor 11. This is not surprising considering the way we obtained the j-invariant back in Chapter 6.

7.2 Proving correctness

In the previous section, some candidate equations for $J(\Gamma)$ were obtained in a heuristic way: in particular, we have not yet proved that the corresponding curves $E(\Gamma)$ are indeed models of $J(\Gamma)$. This section justifies these constructions a posteriori by exploiting a connection with Hilbert modular forms. We combine the methods in our main references [DD08], [SW05] and [DD06], to which we also refer for more details: our exposition in this section will be rather summary. Throughout, we denote the absolute Galois group $\mathrm{Gal}(\overline{F}|F)$ of a number field F by G_F.

Correctness of the isogeny class of $E(\Gamma)$. Let K be, as usual, a compact open subgroup of $\widehat{B}^\times$, where B is a quaternion algebra over a totally real field with finite discriminant $\mathfrak{D} = \mathfrak{D}(B)^f$. Choosing a simultaneous eigenvector of the matrices $T(\mathfrak{p})$ from Chapter 4, one obtains a system of eigenvalues

$$e = \{a(\mathfrak{p}) \mid \mathfrak{p} : \ B_\mathfrak{p} \text{ split and } K_\mathfrak{p} \text{ maximal}\}.$$

By Theorem 4.4 in [Hid81], the systems of eigenvalues thus obtained are in bijection with the isogeny factors of $J(K)$ over F. Moreover, given a system e, the corresponding isogeny factor A_e has real multiplication by the number field L generated by the eigenvalues in e, and given a prime λ of L over a rational prime ℓ, we can construct a Galois representation

$$\rho(A_e)_\lambda : G_F \longrightarrow \mathrm{Aut}(V_\lambda(A_e)) \cong \mathrm{GL}_2(L_\lambda)$$

of G_F on the Tate module

$$V_\lambda(A_e) = \varprojlim_n A_e[\lambda^n].$$

Because of Theorem 3.1.6, this representation is unramified at the primes $\mathfrak{p}$ of F that do not divide ℓ and at which $B_\mathfrak{p}$ is split and $K_\mathfrak{p}$ is maximal. Furthermore, if we let $\mathrm{Frob}(\mathfrak{p})$ be a Frobenius lift at such a $\mathfrak{p}$, then

$$\mathrm{tr}(\mathrm{Frob}(\mathfrak{p})) = a(\mathfrak{p}) \tag{7.4}$$

and

$$\det(\mathrm{Frob}(\mathfrak{p})) = \mathrm{Nm}(\mathfrak{p}) = \epsilon_\ell(\mathrm{Frob}(\mathfrak{p})), \tag{7.5}$$

where $\epsilon_\ell : G_F \to \mathbf{Q}_\ell^\times$ is the ℓ-adic cyclotomic character.

Suppose that there exists a Hilbert modular newform f_e of trivial character whose system of eigenvalues also equals e. By [Tay89], a similar representation $\rho(f_e)_\lambda$ satisfying (7.4) and (7.5) can then be attached to the Hilbert modular newform f_e of trivial character whose system of eigenvalues equals e. More precisely, we have

$$\rho(A_e)_\lambda \cong \rho(f_e)_\lambda, \tag{7.6}$$

In the special case that $K = \widehat{\mathcal{O}}(\mathfrak{N})^\times$ comes from a level $\mathfrak{N}$ Eichler order, the Jacquet-Langlands correspondence (for which see Proposition 2.12 of [Hid81]) shows that such an f_e always exists. More precisely, the systems of eigenvalues e are in bijection with the systems of eigenvalues associated with Hilbert modular newforms of level $\mathfrak{D}\mathfrak{N}$ and trivial character.

Instead of associating isogeny factors A_e with systems of eigenvalues e, we now consider the converse approach: finding a system of eigenvalues e corresponding to a candidate isogeny factor of $J(K)$.

In the previous section, we have, for some choices of compact open subgroups K, constructed candidate models $E = E(\Gamma)$ for $J_0(K)$ over F_K. These candidates E were always isogenous to their $\mathrm{Gal}(F_K|F)$-conjugates, which indeed is a necessary condition for E to be a model of $J_0(K)$ by Proposition 3.1.5. More precisely, using these isogenies, one shows that the corresponding Weil restrictions

$$A = \mathrm{Res}_{F_K|F}(E),$$

which are the candidate models for $J(K)$ corresponding to the model E of $J_0(K)$, all have real multiplication by a number field L of degree $[F_K : F]$. We remark here that in all the cases above we have $[F_K : F] \leq 2$. In fact, we usually have $F_K = F$, whence $A = E$, which trivializes the preceding discussion.

Let A_0 be an isogeny factor of A over F. We will usually have $A_0 = A$, in particular if $F_K = F$. For a prime λ of L over a rational prime ℓ, we can consider the representation

$$\rho(A_0)_\lambda : G_F \longrightarrow \mathrm{Aut}(V_\lambda(A_0)) \cong \mathrm{GL}_2(L_\lambda).$$

This representation is unramified at the primes of F that are coprime to ℓ and the conductor of A_0. By § 1(a) of [Mil72], the restriction of $\rho(A_0)_\lambda$ to the subgroup G_{F_∞} of G_F is a direct sum of copies of the representation

$$\rho(E)_\ell : G_{F_\infty} \longrightarrow \mathrm{Aut}(V_\ell(E)) \cong \mathrm{GL}_2(\mathbf{Q}_\ell),$$

and conversely, one can recover $\rho(A_0)_\lambda$ from $\rho(E)_\ell$ as a factor of the induced representation

$$\mathrm{Ind}_{F_\infty|F}(\rho(E)_\ell) = \rho(A)_\ell : G_F \longrightarrow \mathrm{Aut}(V_\ell(A)). \tag{7.7}$$

Hence in light of (7.6) and Faltings' isogeny theorem, proving that E is in the isogeny class of $J_0(K)$ is equivalent to proving that we have an isomorphism

$$\rho(A_0)_\lambda \cong \rho(A_e)_\lambda \tag{7.8}$$

for some isogeny factor A_e of $J_0(K)$. In the case that $K = \mathcal{O}(\mathfrak{N})^\times$ comes from an Eichler order, the Jacquet-Langlands correspondence implies that this, in turn, is equivalent to proving that we have an isomorphism

$$\rho(A_0)_\lambda \cong \rho(f)_\lambda \tag{7.9}$$

for some Hilbert modular newform f of level $\mathfrak{D}\mathfrak{N}$. We now consider two methods to prove the existence of an isomorphism as in (7.8) or (7.9).

$\ell > 2$. Suppose that ℓ is odd and that $K = \mathcal{O}(\mathfrak{N})^\times$ comes from an Eichler order. To prove the existence of an isomorphism as in (7.9), and hence as in (7.8) by (7.6), we use the following special case of a result by Skinner and Wiles (also see Theorem 3 of [DD08]):

Theorem 7.2.1 (Skinner-Wiles). *Let F be a totally real number field. Suppose that $\ell \geq 3$ is prime, and let*

$$\rho : G_F \longrightarrow \mathrm{GL}_2(\overline{\mathbf{Q}}_\ell)$$

be a continuous, absolutely irreducible and totally odd representation unramified away from a finite set of places of F. Suppose that the semi-simplification $\overline{\rho}^{ss}$ of the reduction $\overline{\rho}$ of ρ satisfies

$$\overline{\rho}^{ss} \cong \chi_1 \oplus \chi_2,$$

where χ_1 and χ_2 are characters. Furthermore, suppose that

(i) The splitting field $F(\chi_1/\chi_2)$ is abelian over $\mathbf{Q}$;

(ii) $(\chi_1/\chi_2)|_{D_v} \neq 1$ for all places v of $\overline{F}$ over ℓ;

(iii) $\rho|_{I_v} \cong \begin{pmatrix} \epsilon_\ell & * \\ 0 & 1 \end{pmatrix}$ for all places v of $\overline{F}$ over ℓ; and

(iv) $\det(\rho) = \epsilon_\ell$.

Then ρ comes from a Hilbert modular form.

As is shown in the proof of Proposition 4(a) of [DD08], the conditions (i)-(iv) of the theorem are fulfilled for the representations $\rho(E)_\ell$ if E has an ℓ-isogeny and has ordinary reduction at a prime λ of F_K over ℓ. If $F_K|F$ is unramified, then the factors $\rho(A_0)_\lambda$ of the induced representation

$$\mathrm{Ind}_{F_\infty|F}(\rho(E)_\ell) = \rho(A)_\ell : G_F \longrightarrow \mathrm{Aut}(V_\ell(A))$$

of the absolute Galois group G_F of the totally real field F still satisfy conditions (i)-(iv), and hence are modular. Note that we cannot always apply the theorem to the representation $\rho(E)_l$ since F_K will not be totally real in general.

For the candidate models that we obtained in the cases e2d17D2, e2d21D4, e2d1125D16 and e4d8D2i/iii, one can find primes ℓ and λ as above. Moreover, the extension $F_K|F$ is unramified in all these cases. Hence we can conclude that for these cases we have indeed obtained a representative of the isogeny class of $J_0(K)$.

$\ell = 2$. Though elegant, Theorem 7.2.1 fails to cover a lot of cases, for example those where $J_0(K)$ does not have an isogeny of odd degree or those where F is not Galois. Considering the fact that we can actually calculate the traces $a(\mathfrak{p})$ in e using Algorithm 4.2.1, the following result is therefore of great use to us.

Theorem 7.2.2 (Faltings-Serre, Theorem 10.1 in [SW05]). *Let M be a global field, and let S a finite set of primes of M. Let M_S be the compositum of the quadratic extensions of M unramified outside S. Suppose that*

$$\rho_1, \rho_2 : G_M \longrightarrow \mathrm{GL}_2(\overline{\mathbf{Q}}_2)$$

are continuous representations, unramified outside S, and furthermore satisfying

(i) $\mathrm{tr}(\overline{\rho}_1) = 0 = \mathrm{tr}(\overline{\rho}_2)$ *and* $\det(\overline{\rho}_1) = \det(\overline{\rho}_2)$.

(ii) There exist a set P of primes of M, disjoint from S, for which

- *The image of* $\{\mathrm{Frob}(\mathfrak{p}) : \mathfrak{p} \in P\}$ *in the* $\mathbf{F}_2$*-vector space* $\mathrm{Gal}(M_S|M)$ *is non-cubic (that is, every cubic polynomial vanishing on T vanishes on all of* $\mathrm{Gal}(M_S|M)$*); and*
- *We have equalities*

$$\mathrm{tr}(\rho_1(\mathrm{Frob}(\mathfrak{p}))) = \mathrm{tr}(\rho_2(\mathrm{Frob}(\mathfrak{p})))$$

and

$$\det(\rho_1(\mathrm{Frob}(\mathfrak{p}))) = \det(\rho_2(\mathrm{Frob}(\mathfrak{p})))$$

for all $\mathfrak{p}$ in P.

Then there exists an isomorphism of semi-simplified representations

$$\rho_1^{ss} \cong \rho_2^{ss}.$$

This theorem, which can be considered as a complement of Theorem 7.2.1, was applied in [SW05] to the case where one of ρ_1 and ρ_2 comes from a Hilbert modular form. We will use it to prove the existence of isomorphisms as in (7.8) and (7.9).

In fact, using Theorem 7.2.2, we could always show directly that

$$\rho(E)_2 \cong \rho(J_0(K))_2,$$

whence the correctness of the candidate isogeny class given by E. Indeed, we could take S to equal the set of primes dividing the product of 2 and the conductor of E. Then after explicitly calculating the ray class group R_S corresponding to M_S, one constructs a set P of primes of F_K mapping bijectively to the finite set R_S. For $\mathfrak{p}$ in P, one can calculate $\mathrm{tr}(\rho(J_0(K))_2(\mathrm{Frob}(\mathfrak{p})))$ using Algorithm 4.2.1 and Proposition 4.3.2, while $\mathrm{tr}(\rho(E)_2(\mathrm{Frob}(\mathfrak{p})))$ is easily calculated using the explicit equation for E.

Of course, we have to check that we indeed have

$$\mathrm{tr}(\overline{\rho}(J_0(K))_2(\mathrm{Frob}(\mathfrak{p}))) = 0 \tag{7.10}$$

and

$$\mathrm{tr}(\overline{\rho}(E)_2(\mathrm{Frob}(\mathfrak{p}))) = 0 \tag{7.11}$$

for all $\mathfrak{p}$. This holds for all but three cases because of the existence of a 2-isogeny over F_K on both E and $J_0(K)$, the former of which can be determined explicitly and the latter of which comes from an Atkin-Lehner involution.

In the exceptional cases e2d725D16, e4d2624D4 and e5d725D25, the models E and the curves $J_0(K)$ do not have a 2-isogeny. In principle, one could mimic the calculations in Section 10.1 of [SW05] to prove correctness for these cases as well. However, for lack of time, we have not looked further into this matter.

Another substantial advantage of Theorem 7.2.2 over Theorem 7.2.1 is the fact that it allows one to prove the existence of an isomorphism (7.6) without the hypotheses on K needed to use the Jacquet-Langlands correspondence. In particular, combining Algorithm 4.2.1 with the algorithms from [DD08], Theorem 7.2.2 shows that all $J(K)$ determined in the first section are modular (with the possible exception of the three cases mentioned above).

More precisely, let $J_0(K)$ be a curve from the first section. If we let $\mathfrak{C}_0$ be the conductor of $J_0(K)$ over F_K, then there exists a unique ideal $\mathfrak{C}$ of $\mathbf{Z}_F$ such that we have $\mathfrak{C}_0 = \mathfrak{C}\mathbf{Z}_{F_K}$, and $J(K)$ can be matched up with a Hilbert modular form with trivial character and conductor equal to $\mathfrak{C}$.

Remark. Explicit calculations using the techniques from this section can be found at [Sij10].

Correctness of the isomorphism class of $E(\Gamma)$. Now that we have an explicit representative $E = E(\Gamma)$ of the isogeny class of $J_0(K)$, it remains to determine the isomorphism classes of elliptic curves in this isogeny class: as we have seen in the previous section, this often enables us to prove that E is isomorphic to $J_0(K)$ by using Proposition 5.1.12.

Consider a candidate Jacobian $J(K)$ from the first section. In the first part of this section, we have seen that if we neglect the cases e2d725D16, e4d2624D4 and e5d725D25, we can attach a Galois representation $\rho(f)_\lambda$ coming from a Hilbert modular newform f to $J(K)$. In [DD06], Dieulefait and Dimitrov prove several large image results for the residual representations

$$\overline{\rho}(f)_\lambda : G_F \longrightarrow \mathrm{GL}_2(\kappa_\lambda).$$

(Here κ_λ denotes the residue field of L_λ.) In particular, the proof of Theorem 5.1 in [DD06] carries over word for word to all cases to show that the residual representations $\overline{\rho}(f)_\lambda$ are irreducible for all primes λ of norm > 50.

As a consequence, the elliptic curves $J_0(K)$ have no isogenies of prime degree $\ell > 50$. Indeed, a decomposition

$$\overline{\rho}(E)_\ell \cong \chi_1 \oplus \chi_2$$

would give rise to a corresponding decomposition of the factors $\overline{\rho}(A_0)_\lambda = \overline{\rho}(f)_\lambda$ of the induced representation $\overline{\rho}(A)_\ell$ from (7.7). We conclude that the conjectural isogeny classes of $J_0(K)$ that we constructed in the previous section, using prime isogenies of degree ≤ 50, are indeed complete.

Appendix A

Tables

This appendix contains three tables, along with an explanation of their contents. First, though, we introduce some notation.

We have assigned labels to the arithmetic $(1;e)$-groups Γ in Theorem 4.1 of [Tak83]. Such labels are of the form

$$\mathrm{e}n_e\,\mathrm{d}n_d\,\mathrm{D}n_D\,\mathrm{r},$$

where

- n_e is the index of the unique elliptic point of Γ;
- n_d is the discriminant of the center F of the quaternion algebra $B = \mathbf{Q}[\Gamma^{(2)}]$ from Lemma 3.3.2;
- n_D is the norm of the discriminant $\mathfrak{D}(B)$ of B over F; and
- r is a roman numeral indicating the position at which Γ occurs in Theorem 4.1 of [Tak83] among the Γ with the same n_e, n_d and n_D.

Given an arithmetic $(1;e)$-group Γ, Table A.1 describes:

- The minimal polynomial f^α of a generator α of F;
- The Galois group G of F over $\mathbf{Q}$;
- The narrow class number h^+ of F (the class number always equals 1);
- And the discriminant $\mathfrak{D}(B)$ of B.

In final column describing the discriminants, ι stands for an infinite place of F, and ι^c is as in (3.9). For fixed F, the ι with a different number of primes $'$ are in different orbits under the action of $\mathrm{Aut}(F)$ on the infinite places of F.

We have not copied over Takeuchi's trace triples (x, y, z) from [Tak83] (or the corresponding pairs (A, B)), since these are only used in the explicit construction of a fundamental domain in Algorithm 1.4.2. The interested reader is referred to Theorem 4.1 in [Tak83] or the record `TakeuchiList` in the file `TakData` at [Sij10] for these trace triples.

Table A.1: Fields and quaternion algebras obtained from arithmetic $(1;e)$-groups

Label	f^α	G	h^+	$\mathfrak{D}(B)$
e2d1D6i	$t-1$	C_1	1	$\mathfrak{p}_2\mathfrak{p}_3$
e2d1D6ii	$t-1$	C_1	1	$\mathfrak{p}_2\mathfrak{p}_3$
e2d1D14	$t-1$	C_1	1	$\mathfrak{p}_2\mathfrak{p}_7$
e2d5D4i	t^2-t-1	C_2	1	$\mathfrak{p}_2\iota^c$
e2d5D4ii	t^2-t-1	C_2	1	$\mathfrak{p}_2\iota^c$
e2d5D4iii	t^2-t-1	C_2	1	$\mathfrak{p}_2\iota^c$
e2d8D2	t^2-2	C_2	1	$\mathfrak{p}_2\iota^c$
e2d8D7i	t^2-2	C_2	1	$\mathfrak{p}_7\iota^c$
e2d8D7ii	t^2-2	C_2	1	$\mathfrak{p}_7\iota'^c$
e2d12D2	t^2-3	C_2	2	$\mathfrak{p}_2\iota^c$
e2d12D3	t^2-3	C_2	2	$\mathfrak{p}_3\iota^c$
e2d13D4	t^2-t-3	C_2	1	$\mathfrak{p}_2\iota^c$
e2d13D36	t^2-t-3	C_2	1	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'\iota^c$
e2d17D2i	t^2-t-4	C_2	1	$\mathfrak{p}_2\iota^c$
e2d17D2ii	t^2-t-4	C_2	1	$\mathfrak{p}_2\iota'^c$
e2d21D4	t^2-t-5	C_2	2	$\mathfrak{p}_2\iota^c$
e2d24D3	t^2-6	C_2	2	$\mathfrak{p}_3\iota^c$
e2d33D12	t^2-t-8	C_2	2	$\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3\iota^c$
e2d49D56	t^3-t^2-2t+1	C_3	1	$\mathfrak{p}_2\mathfrak{p}_7\iota^c$
e2d81D1	t^3-3t-1	C_3	1	ι^c
e2d148D1i	t^3-t^2-3t+1	S_3	1	ι^c
e2d148D1ii	t^3-t^2-3t+1	S_3	1	ι'^c
e2d148D1iii	t^3-t^2-3t+1	S_3	1	ι''^c
e2d229D8i	t^3-4t-1	S_3	2	$\mathfrak{p}_2\mathfrak{p}_2'\iota^c$
e2d229D8ii	t^3-4t-1	S_3	2	$\mathfrak{p}_2\mathfrak{p}_2'\iota'^c$
e2d229D8iii	t^3-4t-1	S_3	2	$\mathfrak{p}_2\mathfrak{p}_2'\iota''^c$
e2d725D16i	$t^4-t^3-3t^2+t+1$	D_4	1	$\mathfrak{p}_2\iota^c$
e2d725D16ii	$t^4-t^3-3t^2+t+1$	D_4	1	$\mathfrak{p}_2\iota'^c$
e2d1125D16	$t^4-t^3-4t^2+4t+1$	C_4	2	$\mathfrak{p}_2\iota^c$
e3d1D6i	$t-1$	C_1	1	$\mathfrak{p}_2\mathfrak{p}_3$
e3d1D6ii	$t-1$	C_1	1	$\mathfrak{p}_2\mathfrak{p}_3$
e3d1D10	$t-1$	C_1	1	$\mathfrak{p}_2\mathfrak{p}_5$
e3d1D15	$t-1$	C_1	1	$\mathfrak{p}_3\mathfrak{p}_5$
e3d5D5	t^2-t-1	C_2	1	$\mathfrak{p}_5\iota^c$
e3d5D9	t^2-t-1	C_2	1	$\mathfrak{p}_3\iota^c$
e3d8D9	t^2-2	C_2	1	$\mathfrak{p}_3\iota^c$
e3d12D3	t^2-3	C_2	2	$\mathfrak{p}_3\iota^c$
e3d13D3i	t^2-t-3	C_2	1	$\mathfrak{p}_3\iota^c$
e3d13D3ii	t^2-t-3	C_2	1	$\mathfrak{p}_3\iota'^c$
e3d17D36	t^2-t-4	C_2	1	$\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3\iota^c$

Continued on the next page

Table A.1 – Continued from the previous page

Label	f^α	G	h^+	$\mathfrak{D}(B)$
e3d21D3	$t^2 - t - 5$	C_2	2	$\mathfrak{p}_3\iota^c$
e3d28D18	$t^2 - 7$	C_2	2	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'\iota^c$
e3d49D1	$t^3 - t^2 - 2t + 1$	C_3	1	ι^c
e3d81D1	$t^3 - 3t - 1$	C_3	1	ι^c
e4d8D2i	$t^2 - 2$	C_2	1	$\mathfrak{p}_2\iota^c$
e4d8D2ii	$t^2 - 2$	C_2	1	$\mathfrak{p}_2\iota^c$
e4d8D2iii	$t^2 - 2$	C_2	1	$\mathfrak{p}_2\iota'^c$
e4d8D7i	$t^2 - 2$	C_2	1	$\mathfrak{p}_7\iota^c$
e4d8D7ii	$t^2 - 2$	C_2	1	$\mathfrak{p}_7\iota'^c$
e4d8D98	$t^2 - 2$	C_2	1	$\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_7'\iota^c$
e4d2304D2	$t^4 - 4t^2 + 1$	C_4	2	$\mathfrak{p}_2\iota^c$
e4d2624D4i	$t^4 - 2t^3 - 3t^2 + 2t + 1$	D_4	1	$\mathfrak{p}_2\iota^c$
e4d2624D4ii	$t^4 - 2t^3 - 3t^2 + 2t + 1$	D_4	1	$\mathfrak{p}_2\iota'^c$
e5d5D4	$t^2 - t - 1$	C_2	1	$\mathfrak{p}_2\iota^c$
e5d5D5i	$t^2 - t - 1$	C_2	1	$\mathfrak{p}_5\iota^c$
e5d5D5ii	$t^2 - t - 1$	C_2	1	$\mathfrak{p}_5\iota^c$
e5d5D5iii	$t^2 - t - 1$	C_2	1	$\mathfrak{p}_5\iota'^c$
e5d5D180	$t^2 - t - 1$	C_2	1	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5\iota^c$
e5d725D25i	$t^4 - t^3 - 3t^2 + t + 1$	D_4	1	$\mathfrak{p}_5\iota^c$
e5d725D25ii	$t^4 - t^3 - 3t^2 + t + 1$	D_4	1	$\mathfrak{p}_5\iota'^c$
e5d1125D5	$t^4 - t^3 - 4t^2 + 4t + 1$	C_4	2	$\mathfrak{p}_5\iota^c$
e6d12D66i	$t^2 - 3$	C_2	2	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{11}\iota^c$
e6d12D66ii	$t^2 - 3$	C_2	2	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{11}\iota'^c$
e7d49D1	$t^3 - t^2 - 2t + 1$	C_3	1	ι^c
e7d49D91i	$t^3 - t^2 - 2t + 1$	C_3	1	$\mathfrak{p}_7\mathfrak{p}_{13}\iota^c$
e7d49D91ii	$t^3 - t^2 - 2t + 1$	C_3	1	$\mathfrak{p}_7\mathfrak{p}_{13}\iota'^c$
e7d49D91iii	$t^3 - t^2 - 2t + 1$	C_3	1	$\mathfrak{p}_7\mathfrak{p}_{13}\iota''^c$
e9d81D51i	$t^3 - 3t - 1$	C_3	1	$\mathfrak{p}_3\mathfrak{p}_{17}\iota^c$
e9d81D51ii	$t^3 - 3t - 1$	C_3	1	$\mathfrak{p}_3\mathfrak{p}_{17}\iota'^c$
e9d81D51iii	$t^3 - 3t - 1$	C_3	1	$\mathfrak{p}_3\mathfrak{p}_{17}\iota''^c$
e11d14641D1	$t^5 - t^4 - 4t^3 + 3t^2 + 3t - 1$	C_5	1	ι^c

Let Γ be a $(1;e)$-group, and let $B = \mathbf{Q}[\Gamma^{(2)}]$ be the corresponding quaternion algebra. Table A.2 describes

- The orders $\mathcal{O}$ of B generated by the groups G inbetween $\Gamma^{(2)}$ and Γ;
- The norm 1 groups $\mathcal{O}^1$ associated to these orders; if this is not given by a G as above, then the minimum of the indices $[\mathcal{O}^1 : G]$ is given;
- The level of $\mathcal{O}$;
- Whether or not $\mathcal{O}$ is Eichler;

- Whether or not Γ is commensurable with a triangle group;
- And the degree of the map $X(\mathcal{O}^1) \to X(\mathcal{O}(1)^1)$ for a maximal order $\mathcal{O}(1)$ containing $\mathcal{O}$.

We could always decide whether or not $\mathcal{O}$ was Eichler by using Corollaries 2.5.4 and 2.5.5. For more information on the orders $\mathcal{O}$ and the orders containing them, we refer to Chapter 7.

Table A.2: The orders $\mathbf{Z}_F[G]$ for $\Gamma^{(2)} \subseteq G \subseteq \Gamma$

Label	$\mathcal{O}$	$\mathcal{O}^1$	Level	Eichler?	Δ ?	Deg
e2d1D6i	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_5$	Y	Y	6
e2d1D6ii	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^3$	N	Y	6
e2d1D14	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	(1)	Y	N	1
e2d5D4i	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^2$	N	Y	20
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	2	$\mathfrak{p}_2$	N	Y	5
e2d5D4ii	all $\mathbf{Z}_F[G]$	5	(1)	Y	Y	1
e2d5D4iii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	$\mathfrak{p}_3$	Y	Y	10
e2d8D2	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^5$	N	Y	24
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_2^4$	N	Y	12
e2d8D7i	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	$\mathfrak{p}_2^2$	N	N	2
e2d8D7ii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	$\mathfrak{p}_2^2$	N	N	2
e2d12D2	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^4$	N	Y	12
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	$\mathfrak{p}_2^3$	N	Y	6
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	$\mathfrak{p}_2^3$	N	Y	6
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_2^3$	N	Y	6
	$\mathbf{Z}_F[\Gamma]$	Γ	$\mathfrak{p}_2$	N	Y	3
e2d12D3	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^4$	N	Y	6
e2d13D4	all $\mathbf{Z}_F[G]$	Γ	(1)	Y	N	1
e2d13D36	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	(1)	Y	N	1
e2d17D2i	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2'^4$	N	N	6
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_2'^2$	N	N	3
e2d17D2ii	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2'^4$	N	N	6
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_2'^2$	N	N	3
e2d21D4	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	(1)	Y	N	1
e2d24D3	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^2$	N	N	2
e2d33D12	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	(1)	Y	N	1
e2d49D56	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	(1)	Y	N	1
e2d81D1	all $\mathbf{Z}_F[G]$	Γ	$\mathfrak{p}_2$	Y	Y	9
e2d148D1i	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^5$	N	N	12
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_2^4$	N	N	6
e2d148D1ii	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^5$	N	N	12
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	$\mathfrak{p}_2^4$	N	N	6
e2d148D1iii	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^5$	N	N	12
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	$\mathfrak{p}_2^4$	N	N	6
e2d229D8i	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	(1)	Y	N	1
e2d229D8ii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	(1)	Y	N	1
e2d229D8iii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	(1)	Y	N	1
e2d725D16i	all $\mathbf{Z}_F[G]$	Γ	(1)	Y	N	1
e2d725D16ii	all $\mathbf{Z}_F[G]$	Γ	(1)	Y	N	1
e2d1125D16	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	(1)	Y	N	1

Continued on the next page

Table A.2 – Continued from the previous page

Label	$\mathcal{O}$	$\mathcal{O}^1$	Level	Eichler?	Δ ?	Deg
e3d1D6i	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_7$	Y	Y	8
e3d1D6ii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_2^2$	N	Y	4
e3d1D10	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_3^2$	N	N	4
e3d1D15	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^2$	N	N	2
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	(1)	Y	N	1
e3d5D5	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	$\mathfrak{p}_3$	Y	Y	10
e3d5D9	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_2$	Y	Y	5
e3d8D9	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	$\mathfrak{p}_2^2$	N	N	2
	other G	Γ	(1)	Y	N	1
e3d12D3	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_2^2\mathfrak{p}_3$	N	Y	4
	other G	Γ	$\mathfrak{p}_3$	N	Y	2
e3d13D3i	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_3'^2$	N	N	4
e3d13D3ii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	$\mathfrak{p}_3'^2$	N	N	4
e3d17D36	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	(1)	Y	N	1
e3d21D3	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_3$	N	N	2
e3d28D18	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	(1)	Y	N	1
e3d49D1	all $\mathbf{Z}_F[G]$	Γ	$\mathfrak{p}_3$	Y	Y	28
e3d81D1	all $\mathbf{Z}_F[G]$	Γ	$\mathfrak{p}_3^3$	N	Y	12
e4d8D2i	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	$\mathfrak{p}_{17}$	Y	Y	18
e4d8D2ii	all $\mathbf{Z}_F[G]$	9	(1)	Y	Y	1
e4d8D2iii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_{17}'$	Y	Y	18
e4d8D7i	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^4$	N	N	6
e4d8D7ii	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^4$	N	N	6
e4d8D98	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	(1)	Y	N	1
e4d2304D2	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	$\mathfrak{p}_2^4$	N	Y	12
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	$\mathfrak{p}_2^3$	N	Y	6
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	$\mathfrak{p}_2^3$	N	Y	6
	$\mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_2^3$	N	Y	6
	$\mathbf{Z}_F[\Gamma]$	Γ	$\mathfrak{p}_2$	N	Y	3
e4d2624D4i	all $\mathbf{Z}_F[G]$	Γ	(1)	Y	N	1
e4d2624D4ii	all $\mathbf{Z}_F[G]$	Γ	(1)	Y	N	1
e5d5D5i	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	$\mathfrak{p}_{11}$	Y	Y	12
e5d5D5ii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	$\mathfrak{p}_{11}'$	Y	Y	12
e5d5D5iii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	$\mathfrak{p}_2^2$	N	Y	12
	other G	6	(1)	Y	Y	1
e5d5D9	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	$\mathfrak{p}_5$	Y	Y	6
e5d5D180	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	(1)	Y	N	1
e5d725D25i	all $\mathbf{Z}_F[G]$	Γ	(1)	Y	N	1
e5d725D25ii	all $\mathbf{Z}_F[G]$	Γ	(1)	Y	N	1
e5d1125D5	all $\mathbf{Z}_F[G]$	Γ	$\mathfrak{p}_5$	N	Y	3
e6d12D66i	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	(1)	Y	N	1
e6d12D66ii	$\mathbf{Z}_F[\Gamma^{(2)}]$	$\Gamma^{(2)}$	(1)	Y	N	1
e7d49D1	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	$\mathfrak{p}_2\mathfrak{p}_7$	Y	Y	72
e7d49D91i	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	(1)	Y	N	1
e7d49D91ii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	(1)	Y	N	1
e7d49D91iiii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, AB \rangle]$	$\langle \Gamma^{(2)}, AB \rangle$	(1)	Y	N	1
e9d81D51i	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, B \rangle]$	$\langle \Gamma^{(2)}, B \rangle$	(1)	Y	Y	1
e9d81D51ii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	(1)	Y	Y	1
e9d81D51iii	$\mathbf{Z}_F[\Gamma^{(2)}] = \mathbf{Z}_F[\langle \Gamma^{(2)}, A \rangle]$	$\langle \Gamma^{(2)}, A \rangle$	(1)	Y	Y	1
e11d14641D1	all $\mathbf{Z}_F[G]$	Γ	$\mathfrak{p}_{11}$	Y	Y	12

The final Table A.3 summarizes the conjectural canonical models for the curves $J(\Gamma)$ determined in Chapter 7. For such a canonical model $E(\Gamma)$, it specifies:

- The canonical field of definition F_Γ of $E(\Gamma)$;
- A minimal field of definition M_Γ of $E(\Gamma)$ (as an abstract field, M_Γ turned out to be unique in all cases);
- The j-invariant $j(E(\Gamma))$ of $E(\Gamma)$;
- The conductor $\mathfrak{C}(E(\Gamma))$ of $E(\Gamma)$ over F_Γ;
- Whether or not $E(\Gamma)$ can be obtained as a (possibly trivial) Atkin-Lehner quotient of a component $J_0(\mathcal{O})$ associated with a quaternion order $\mathcal{O}$; and
- Whether or not we succeeded in proving the correctness of $E(\Gamma)$ or its isogeny class.

These data determine $E(\Gamma)$ in all cases. In the cases where multiple conjugate values for j were obtained, we give these j-invariants as distinct embeddings $\iota(j)$ into $\mathbf{C}$ for a fixed element j of F_Γ (*cf.* Theorem 3.1.7).

Frequently, it was only possible to determine an isogeny class of curves over F. In these cases, we have used the j-invariant of smallest height in this isogeny class, even though the experimental evidence indicates that Shimura curves tend to have a j-invariant of rather large height.

We point out a few anomalies in the list:

(i) The cases e4d8D2ii lacks some entries: this is because we have been unable to prove that the associated group is congruence. See the corresponding paragraph in Chapter 7.

(ii) For the case e6d12D66, the canonical model depends on the choice of a certain compact open subgroup K' as in Lemma 3.2.3. See Chapter 7 for information on the models obtained once such a choice is made, and for more on this phenomenon.

(iii) Finally, at e3d21D3, K_{-1321} denotes the subfield of $F_{\mathfrak{p}_3\infty}$ whose discriminant equals -1321, which is uniquely determined up to isomorphism (though not as a subfield of $F_{\mathfrak{p}_3\infty}$).

As in Remark (ii) at the beginning of Section 6.2, given an integer d, we denote

$$w_d = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4; \\ \sqrt{d} & \text{otherwise.} \end{cases}$$

Table A.3: The canonical models for $J(\Gamma)$

Label	F_Γ	M_Γ	$j(E(\Gamma))$	$\mathfrak{C}(E(\Gamma))$	Atkin-Lehner?	Proved?
e2d1D6i	F	F	$7^3 2287^3/2^6 3^2 5^6$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$	Y	Y
e2d1D6ii	F	F	$2^4 13^3/3^2$	$\mathfrak{p}_2^3\mathfrak{p}_3$	Y	Y
e2d1D14	F	F	$5^3 11^3 31^3/2^3 7^6$	$\mathfrak{p}_2\mathfrak{p}_7$	Y	Y
e2d5D4i	F	F	$2^4 17^3$	$\mathfrak{p}_2^3$	Y	Y
e2d5D4ii	F	$\mathbf{Q}$	$5^1 211^3/2^{15}$	$\mathfrak{p}_2\mathfrak{p}_5^2$	N	Y
e2d5D4iii	F	F	$-269^3/2^{10}3^5$	$\mathfrak{p}_2\mathfrak{p}_3$	Y	Y
e2d8D2	$F_{\mathfrak{p}_2^2\infty}$	$\mathbf{Q}$	$2^6 3^3$	$\mathfrak{p}_2^6$	Y	Y
e2d8D7i/ii	F	F	$\iota(j), \iota'(j)$	$\mathfrak{p}_2^2\mathfrak{p}_7$	Y	Y
(isogeny class)	where $j = 2^{12}(\alpha+4)/7$					
e2d12D2	F_∞	F	0	$\mathfrak{p}_2^4$	Y	Y
e2d12D3	F_∞	$\mathbf{Q}$	$2^2 193^3/3^1$	$\mathfrak{p}_2^3\mathfrak{p}_3$	Y	Y
e2d13D4	F	F	$-29^3 41^3/2^{15}$	$\mathfrak{p}_2$	Y	Y
e2d13D36	F	F	$11^3 23831^3/2^{10}3^2$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'$	Y	Y
e2d17D2i/ii	F	F	$\iota(j), \iota'(j)$	$\mathfrak{p}_2\mathfrak{p}_2'$	Y	Y
	where $j = (-203862548967\alpha + 522266467988)/2^{12}$					
e2d21D4	F_∞	F_∞	$\iota(j), \iota'(j)$	$\mathfrak{p}_2\mathfrak{p}_2'$	Y	Y
	where $j = 3^3(3566479289w_{-7} - 3860683875)/2^{15}$					
e2d24D3	F_∞	$\mathbf{Q}(w_{-2})$	$\iota(j), \iota'(j)$	$\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_3'$	Y	Y
(isogeny class)	where $j = 2^{12}(91w_{-2} - 86)/3^3$.					
e2d33D12	F_∞	F	$5^3 31^3/2^6 3^3$	$\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3\mathfrak{p}_3'$	Y	Y
e2d49D56	F	$\mathbf{Q}$	$-5^3 1637^3/2^{18}7^1$	$\mathfrak{p}_2\mathfrak{p}_7$	Y	Y
e2d81D1	F	$\mathbf{Q}$	$-3^2 5^3 101^3/2^{21}$	$\mathfrak{p}_2$	Y	Y
e2d148D1i/ii/iii	F	F	$\iota(j), \iota'(j), \iota''(j)$	$\mathfrak{p}_2^3$	Y	Y
(isogeny class)	where $j = 2^6(-41\alpha^2 + 24\alpha + 141)$					
e2d229D8i/ii/iii	F_∞	F	$\iota(j), \iota'(j), \iota''(j)$	$\mathfrak{p}_2\mathfrak{p}_2'$	Y	Y
	where $j = (246287297014499885842120 43\alpha^2$ $+ 520874861825891662026725 97\alpha$ $+ 1164529853832418291613198 0)/2^{15}$					
e2d725D16i/ii	F	F	$\iota(j), \iota'(j)$	$\mathfrak{p}_2$	Y	N
	where $j = (1823165439649343w_5 - 2950374307928381)/2^{17}$					
e2d1125D16	F_∞	F_∞	$\iota(j), \iota'(j)$	$\mathfrak{p}_2\mathfrak{p}_2'$	Y	Y
	where $j = (53184785340479w_{-15} - 30252086554835)/2^{34}$					
e3d1D6i	F	F	$4993^3/2^2 3^8 7^4$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7$	Y	Y
e3d1D6ii	F	F	$2^1 47^3/3^8$	$\mathfrak{p}_2^3\mathfrak{p}_3$	Y	Y
e3d1D10	F	F	$7^3 127^3/2^2 3^6 5^2$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$	Y	Y
e3d1D15	F	F	$6841^3/3^8 5^2$	$\mathfrak{p}_3\mathfrak{p}_5$	Y	Y
e3d5D5	F	$\mathbf{Q}$	$-5281^3/3^{16}5$	$\mathfrak{p}_3\mathfrak{p}_5$	Y	Y
e3d5D9	F	F	$7949^3/2^5 3^{10}$	$\mathfrak{p}_2\mathfrak{p}_3$	Y	Y
e3d8D9	F	F	$-2^6 239^3/3^{10}$	$\mathfrak{p}_3$	Y	Y
e3d12D3	F_∞	F	$2^6 3^3$	$\mathfrak{p}_3^2$	Y	Y
e3d13D3i/ii	F	F	$\iota(j), \iota'(j)$	$\mathfrak{p}_3\mathfrak{p}_3'$	Y	Y
	where $j = 5^3(135688993163077\alpha + 176772314640989)/3^8$					
e3d17D36	F	F	$11^3 41^3 131^3/2^2 3^{10}$	$\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3$	Y	Y
e3d21D3	$F_{\mathfrak{p}_3\infty}$	K_{-1321}	$3^3 5^3 17^3$	$\mathfrak{p}_3^2$	N	Y
(isogeny class)						
e3d28D18	F_∞	F	$23^3 41^3/2^2 3^8$	$\mathfrak{p}_2'\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'$	Y	Y
e3d49D1	F	$\mathbf{Q}$	$-2^{12}7^1/3^1$	$\mathfrak{p}_3$	Y	Y
(isogeny class)						

Continued on the next page

Table A.3 – Continued from the previous page

Label	F_Γ	M_Γ	$j(E(\Gamma))$	$\mathfrak{C}(E(\Gamma))$	Atkin-Lehner?	Proved?
e3d81D1	$F_{\mathfrak{p}_3\infty}$	$\mathbf{Q}$	0	$\mathfrak{p}_3^4$	Y	Y
e4d8D2i/iii	F	F	$\iota(j), \iota'(j)$	$\mathfrak{p}_2\mathfrak{p}_{17}$	Y	Y
	where $j = (-19513986518\alpha - 25455932221)/2^9 17^3$					
e4d8D2ii	?	?	$\iota(j), \iota'(j)$	?	?	Y
	where $j = (-241123607w_{-2} + 119421866)/2^{14}$					
e4d8D7i/ii	F	F	$\iota(j), \iota'(j)$	$\mathfrak{p}_2^3\mathfrak{p}_7$	Y	Y
(isogeny class)	where $j = 2^4(142140\alpha + 209189)/7^2$					
e4d8D98	F	$\mathbf{Q}$	$5^3 11^3 2383^3/2^9 7^2$	$\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_7'$	Y	Y
e4d2304D2	F_∞	F	0	$\mathfrak{p}_2^4$	Y	Y
e4d2624D4i/ii	F	F	$\iota(j), \iota'(j)$	$\mathfrak{p}_2$	Y	N
	where $j = (316244205973w_2 - 446790817554)/2^{18}$					
e5d5D5i/ii	F	F	$\iota(j), \iota'(j)$	$\mathfrak{p}_5\mathfrak{p}_{11}$	Y	Y
	where $j = (4560282420936767\alpha + 2818578140804845)/5^6 11^3$					
e5d5D5iii	F	$\mathbf{Q}$	$-2^4 109^3/5^6$	$\mathfrak{p}_2^2\mathfrak{p}_5$	Y	Y
e5d5D9	F	$\mathbf{Q}$	$23^3 73^3/3^2 5^8$	$\mathfrak{p}_3\mathfrak{p}_5$	Y	Y
e5d5D180	F	$\mathbf{Q}$	$7^3 2287^3/2^6 3^2 5^6$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$	Y	Y
e5d725D25i/ii	F	F	$\iota(j), \iota'(j)$	$\mathfrak{p}_5$	Y	N
	where $j = 2^{12}(2295328657133w_5 - 3713921284309)/5^7$					
e5d1125D5	F_∞	F	0	$\mathfrak{p}_5^2$	Y	Y
e6d12D66i/ii	F_∞	F	$\iota(j), \iota'(j)$	depends	N	Y
	where $j = (185900600222705\alpha + 322018643570594)/2^5 3^7 11^2$					
e7d49D1	F	$\mathbf{Q}$	$5^3 11^3 31^3/2^3 7^6$	$\mathfrak{p}_2\mathfrak{p}_7$	Y	Y
e7d49D91i/ii/iii	F	F	$\iota(j), \iota'(j), \iota''(j)$	$\mathfrak{p}_7\mathfrak{p}_{13}$	Y	Y
	where $j = (-8058460190096647498093\alpha^2$ $+ 4472108028759348587577\alpha$ $+ 1810719565899647404885)/7^6 13^2$					
e9d81D51i/ii/iii	F	F	$\iota(j), \iota'(j), \iota''(j)$	$\mathfrak{p}_3\mathfrak{p}_{17}$	Y	Y
	where $j = (-7836754568848363 3\alpha^2$ $+ 27216689077016112\alpha$ $+ 225650240167014325)/3^{11} 17^2$					
e11d14641D1	F	$\mathbf{Q}$	$-2^{12} 31^3/11^5$	$\mathfrak{p}_{11}$	Y	Y

Bibliography

[BC91] J.-F. Boutot and H. Carayol. Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfel′d. *Astérisque*, (196-197):7, 45–158 (1992), 1991.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[Bea95] Alan F. Beardon. *The geometry of discrete groups*, volume 91 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[Bir94] Bryan Birch. Noncongruence subgroups, covers and drawings. In *The Grothendieck theory of dessins d'enfants (Luminy, 1993)*, volume 200 of *London Math. Soc. Lecture Note Ser.*, pages 25–46. Cambridge Univ. Press, Cambridge, 1994.

[BZ] J.-F. Boutot and T. Zink. The p-adic Uniformization of Shimura Curves. Preprint available at `http://www.mathematik.uni-bielefeld.de/~zink/p-adicuni.ps`.

[Car86] Henri Carayol. Sur la mauvaise réduction des courbes de Shimura. *Compositio Math.*, 59(2):151–230, 1986.

[CC89] D. V. Chudnovsky and G. V. Chudnovsky. Transcendental methods and theta-functions. In *Theta functions—Bowdoin 1987, Part 2 (Brunswick, ME, 1987)*, volume 49 of *Proc. Sympos. Pure Math.*, pages 167–232. Amer. Math. Soc., Providence, RI, 1989.

[Čer76] I. V. Čerednik. Uniformization of algebraic curves by discrete arithmetic subgroups of $\mathrm{PGL}_2(k_w)$ with compact quotient spaces. *Mat. Sb. (N.S.)*, 100(142)(1):59–88, 165, 1976.

[CL07] J. E. Cremona and M. P. Lingham. Finding all elliptic curves with good reduction outside a given set of primes. *Experiment. Math.*, 16(3):303–312, 2007.

[Cou94] Jean-Marc Couveignes. Calcul et rationalité de fonctions de Belyĭ en genre 0. *Ann. Inst. Fourier (Grenoble)*, 44(1):1–38, 1994.

[Cre06] John Cremona. The elliptic curve database for conductors to 130000. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 11–29. Springer, Berlin, 2006.

[DD06] Luis Dieulefait and Mladen Dimitrov. Explicit determination of images of Galois representations attached to Hilbert modular forms. *J. Number Theory*, 117(2):397–405, 2006.

[DD08] Lassina Dembélé and Steve Donnelly. Computing Hilbert modular forms over fields with nontrivial class group. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 371–386. Springer, Berlin, 2008.

[Del71] Pierre Deligne. Travaux de Shimura. In *Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389*, pages 123–165. Lecture Notes in Math., Vol. 244. Springer, Berlin, 1971.

[DN67] Koji Doi and Hidehisa Naganuma. On the algebraic curves uniformized by arithmetical automorphic functions. *Ann. of Math. (2)*, 86:449–460, 1967.

[Dri76] V. G. Drinfel′d. Coverings of p-adic symmetric domains. *Funkcional. Anal. i Priložen.*, 10(2):29–40, 1976.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Eic55] Martin Eichler. Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine Angew. Math.*, 195:127–151 (1956), 1955.

[Elk98] Noam D. Elkies. Shimura curve computations. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 1–47. Springer, Berlin, 1998.

[Elk06] Noam D. Elkies. Shimura curves for level-3 subgroups of the $(2,3,7)$ triangle group, and some other examples. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 302–316. Springer, Berlin, 2006.

[FK65] Robert Fricke and Felix Klein. *Vorlesungen über die Theorie der automorphen Funktionen.*, volume 4 of *Bibliotheca Mathematica Teubneriana, Bände 3*. Johnson Reprint Corp., New York, 1965.

[GR06] Josep González and Victor Rotger. Non-elliptic Shimura curves of genus one. *J. Math. Soc. Japan*, 58(4):927–948, 2006.

[GV] Matthew Greenberg and John Voight. Computing systems of Hecke eigenvalues associated to Hilbert modular forms. Preprint available at `http://www.cems.uvm.edu/~voight/articles/heckefun-021910.pdf`.

[Hal09] Emmanuel Hallouin. Computation of a cover of Shimura curves using a Hurwitz space. *J. Algebra*, 321(2):558–566, 2009.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Hid81] Haruzo Hida. On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves. *Amer. J. Math.*, 103(4):727–776, 1981.

[HPS89] H. Hijikata, A. Pizer, and T. Shemanske. Orders in quaternion algebras. *J. Reine Angew. Math.*, 394:59–106, 1989.

[HT01] Michael Harris and Richard Taylor. *The geometry and cohomology of some simple Shimura varieties*, volume 151 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2001.

[Kra96] Daan Krammer. An example of an arithmetic Fuchsian group. *J. Reine Angew. Math.*, 473:69–85, 1996.

[Kur79] Akira Kurihara. On some examples of equations defining Shimura curves and the Mumford uniformization. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 25(3):277–300, 1979.

[KV10] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM Journal on Computing*, 39(5):1714–1747, 2010.

[Len] H. W. Lenstra. Galois theory for schemes. Notes available at `http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf`.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002.

[Mas71] Bernard Maskit. On Poincaré's theorem for fundamental polygons. *Advances in Math.*, 7:219–230, 1971.

[Mila] J. S. Milne. Class Field Theory. Notes available at `http://www.jmilne.org/math/CourseNotes/cft.html`.

[Milb] J. S. Milne. Introduction to Shimura Varieties. Notes available at `http://www.jmilne.org/math/articles/2005aX.pdf`.

[Mil72] J. S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17:177–190, 1972.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[Rib90] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[Ros86] Gerhard Rosenberger. All generating pairs of all two-generator Fuchsian groups. *Arch. Math. (Basel)*, 46(3):198–204, 1986.

[Ser92] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992.

[Shi70] Goro Shimura. On canonical models of arithmetic quotients of bounded symmetric domains. *Ann. of Math. (2)*, 91:144–222, 1970.

[Sij10] Jeroen Sijsling. Magma programs for arithmetic pointed tori, 2010. Webpage at `http://sites.google.com/site/sijsling/programs`.

[Ste08] William A. Stein. An introduction to computing modular forms using modular symbols. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 641–652. Cambridge Univ. Press, Cambridge, 2008.

[SW05] Jude Socrates and David Whitehouse. Unramified Hilbert modular forms, with examples relating to elliptic curves. *Pacific J. Math.*, 219(2):333–364, 2005.

[Tak77] Kisao Takeuchi. Commensurability classes of arithmetic triangle groups. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 24(1):201–212, 1977.

[Tak83] Kisao Takeuchi. Arithmetic Fuchsian groups with signature $(1;e)$. *J. Math. Soc. Japan*, 35(3):381–407, 1983.

[Tay89] Richard Taylor. On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98(2):265–280, 1989.

[Var98] Yakov Varshavsky. p-adic uniformization of unitary Shimura varieties. *Inst. Hautes Études Sci. Publ. Math.*, (87):57–119, 1998.

[Vig80] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[Voi] John Voight. Computing automorphic forms on Shimura curves over fields with arbitrary class number. Preprint available at `http://www.cems.uvm.edu/~voight/articles/classno-ants-011310.pdf`; to be published in the proceedings of ANTS-IX.

[Voi09a] John Voight. Computing fundamental domains for Fuchsian groups. *J. Théor. Nombres Bordeaux*, 21(2):469–491, 2009.

[Voi09b] John Voight. Shimura curves of genus at most two. *Math. Comp.*, 78(266):1155–1172, 2009.

[Zha01] Shouwu Zhang. Heights of Heegner points on Shimura curves. *Ann. of Math. (2)*, 153(1):27–147, 2001.

Index of notation

Samenvatting

In wat nu volgt zal ik door het jargon en de notatie van de voorgaande pagina's proberen heen te prikken om ook de lezers van dit proefschrift die niet dagelijks met wiskunde bezig zijn een indruk te geven van de inhoud, en misschien om een enkele twijfelaar aan te zetten tot het daadwerkelijke lezen ervan. Hierdoor zal ik niet overal even precies of volledig kunnen zijn, maar de hoofdmoot van het proefschrift bevat wat dit betreft genoeg aanvullende informatie.

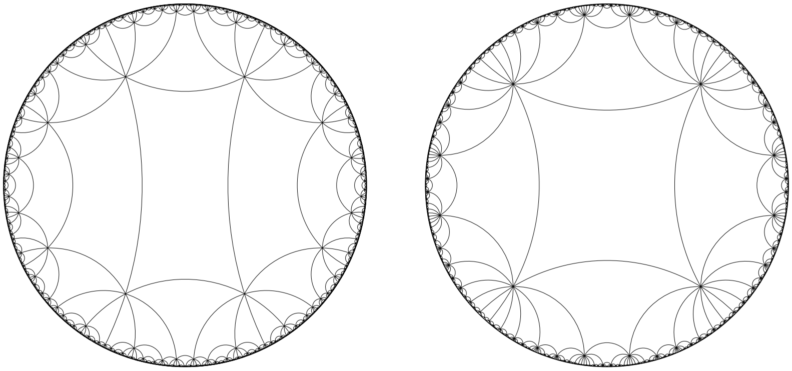
Meetkunde

Zoals vermeld op het titelblad gaat mijn promotieonderzoek over *arithmetische gepunte tori*. Het bevindt zich op het gebied van de *arithmetische meetkunde*, een soort kruispunt tussen meetkunde en getaltheorie. Deze sectie bevat informatie over het meetkundige aspect; later zullen we zien hoe dit verwoven is met het getaltheoretische.

De lezer zal ongetwijfeld een blik op de omslag hebben geworpen: samen met het dankwoord en de samenvatting is dit doorgaans het populairste onderdeel van een proefschrift, en niet alleen bij niet-wiskundigen. Vergeet nu even de achthoek in het watermerk en beschouw het witte patroon van lijnen. Dit is een deel van een betegeling van het *bovenhalfvlak*, dat zich vanaf de omslag oneindig ver naar beide zijden en naar boven uitstrekt (dit is dan ook niet verder bijgevoegd).

Door een meetkundige vervorming kan vanuit deze betegeling ook een betegeling op de zogenaamde *Poincaréschijf* $\mathfrak{D}$ geconstrueerd worden. Deze heeft de omslag helaas niet gehaald, maar is alsnog als het linkerdeel van Figuur 1 opgenomen; het rechterdeel van deze figuur is een andere betegeling van $\mathfrak{D}$. Wellicht komen dergelijke illustraties u bekend voor uit het werk van de Nederlandse graficus M.C. Escher. Zijn prentenreeks *Cirkellimieten* bestaat uit meer van dit soort schijfbetelingen, versierd met vissen, hagedissen, engelen en demonen.

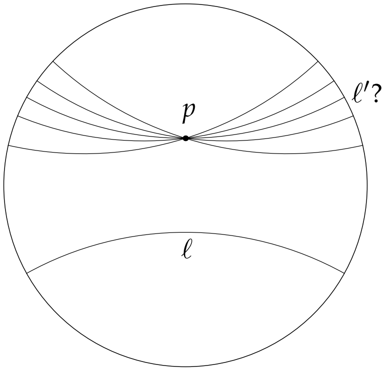
De benaming *Poincaréschijf* voor $\mathfrak{D}$ vereist nog enige toelichting. De schijf $\mathfrak{D}$ is namelijk niet zomaar een schijf, maar is ook nog eens uitgerust met een meetkunde. Dat wil zeggen dat men kan aangeven wat op $\mathfrak{D}$ het juiste analogon is van een rechte lijn. Dit is namelijk een cirkelboog loodrecht staat op de rand van deze schijf. Deze meetkunde is hetzelfde als de meetkunde die we gewend zijn in het platte vlak, met één erg belangrijke uitzondering. In het alledaagse



Figuur 1: Een paar Escherachtige betegelingen.

vlak is het namelijk zo dat gegeven een lijn ℓ samen met een punt p dat niet op ℓ ligt, er een unieke lijn ℓ' bestaat die door p gaat en ℓ niet snijdt. Zo'n lijn heet dan *evenwijdig* aan ℓ te zijn.

Op de Poincaréschijf is dat niet langer waar. Eigenlijk gaat deze constructie op $\mathfrak{D}$ juist te goed, want zoals u in Figuur 2 kunt zien zijn er gegeven p en ℓ verschillende keuzes voor de evenwijdige cirkelboog ℓ', in plaats van een enkele unieke keuze. In jargon wordt dit uitgedrukt door te zeggen dat de meetkunde van $\mathfrak{D}$ *negatief gekromd* is. Positief gekromde ruimtes bestaan ook, zoals het boloppervlak. Hierop wordt het analogon van een rechte lijn gegeven door een cirkel waarvan het middelpunt samenvalt met dat van de bol. Twee zulke cirkels snijden elkaar juist altijd en derhalve kan een ℓ' als boven dus nooit geconstrueerd worden. Overigens wordt een soortgelijk begrip van kromming gebruikt door natuurkundigen als ze zeggen dat de ruimte-tijd gekromd is.

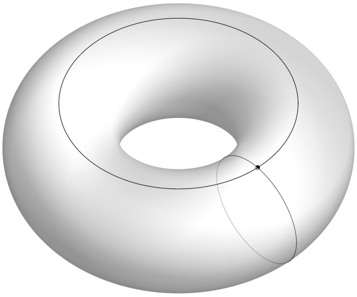


Figuur 2: Verscheidene evenwijdige paren lijnen op de Poincaréschijf.

Deze negatieve kromming zorgt ervoor dat de betegelingen van $\mathfrak{D}$ aanzienlijk spannendere eigenschappen hebben dan betegelingen van het gewone vlak.

Een vierhoeksbetegeling van het vlak heeft bijvoorbeeld de eigenschap dat in alle hoekpunten precies 4 vierhoeken samenkomen (denk aan ruitjespapier). Voor vierhoeksbetegelingen van $\mathfrak{D}$ is dit onmogelijk; in tegenstelling hiermee komen in Figuur 1 bijvoorbeeld links in elk hoekpunt 8 vierhoeken samen, terwijl er rechts zelfs 12 vierhoeken bij elkaar komen. Sterker nog, elk viervoud $8, 12, 16, 20, \ldots$ is mogelijk voor betegelingen van de Poincaréschijf. De lezer kan hier zelf mee experimenteren op de site [Sij10].

Uitgaande van een vierhoeksbetegeling als in Figuur 1 kunnen we met wat knutselen een interessant meetkundig object maken. Als we namelijk de centrale vierhoek in Figuur 1 nemen en dit stuk van $\mathfrak{D}$ zo rekken en rondvouwen dat de twee verticale zijden aan elkaar vast komen te zitten, dan krijgen we een cylinder. We kunnen dan vervolgens ook de boven- en onderkant van deze cylinder aan elkaar vastmaken. Het resultaat is een donut- of fietsbandvormig object dat gewoonlijk een torus wordt genoemd en waarvan u een illustratie kunt zien in Figuur 3. Deze torus heeft een speciaal punt, namelijk het punt waar de twee gelijmde zijden bij elkaar komen. We noemen hem daarom ook wel een *gepunte torus*.



Figuur 3: Een gepunte torus.

Mijn onderzoek betreft een aantal speciale gepunte tori. Misschien denkt u na de bovenstaande beschrijving dat hier niet veel interessants mee gemoeid kan zijn; per slot van rekening weten we uit Figuur 3 precies hoe deze tori er uit zien. Om de zaken simpel te houden is in deze beschrijving echter wat informatie weggelaten. Net zoals namelijk de Poincaréschijf $\mathfrak{D}$ niet zomaar een schijf is, maar een schijf uitgerust met een meetkundige structuur, zo is ook een gepunte torus die afkomstig is van een betegeling van $\mathfrak{D}$ uitgerust met een speciale meetkundige structuur. Deze structuur hangt echter af van de betegeling waar de torus vandaan komt, waardoor een gepunte torus meer behelst dan de illustratie in Figuur 3.

In feite komt het in acht nemen van de meetkundige structuur van een gepunte torus neer op het bijhouden van de hoeveelheid rek die nodig is om de gekromde zijden van de centrale vierhoeken in Figuur 1 aan elkaar te lijmen. Zoals u daar kunt zien, hangt dit proces af van de betegeling.

Gepunte tori kunnen op een wonderlijk eenvoudige manier worden beschreven door *complexe getallen* te gebruiken (dit is geen oxymoron). Complexe getallen zijn getallen van de vorm

$$z = s + ti,$$

waar s en t gewone, *reële* getallen zijn, zoals 1, $-4{,}09$ of π. Wat i betreft, dat is een getal met kwadraat -1. Dit getal woont niet op de gewone getallenlijn: i staat dan ook voor "imaginair". Complexe getallen worden meestal gevisualiseerd door ze in een vlak te tekenen, met de reële getallen, van de vorm $z = s + 0i$ dus, op de horizontale as en de getallen $z = 0 + ti$ op de verticale as. Het complexe getal $4 + 3i$ bijvoorbeeld kan dan vanuit de oorsprong worden bereikt door een afstand 4 naar rechts te gaan en een afstand 3 naar boven.

Het grote mirakel is nu dat voor elke gepunte torus er complexe getallen a en b bestaan zodanig dat deze torus in essentie ("op isomorfie na") wordt gegeven door de complexe getallenparen (x, y) die voldoen aan

$$y^2 = x^3 + ax + b. \tag{1}$$

Wellicht herinnert u zich van de middelbare school dat een vergelijking als deze een *kromme* (een meetkundig object van dimensie 1) definieert, en lijkt het daarom raar dat dit aanleiding kan geven tot een torus, die toch duidelijk een *oppervlak* (een meetkundig object van dimensie 2) is. Toch is het wel degelijk logisch dat de oplossingen van deze vergelijking een torus vormen. Immers, we hebben boven *complexe* paren (x, y) bekeken in plaats van reële paren. Omdat de complexe getallen een vlak vormen (van dimensie 2), heeft een kromme gevormd door complexe paren in totaal dimensie $2 \times 1 = 2$, en is dus welbeschouwd een oppervlak.

Een vergelijking als in (1) heet een *Weierstraßvergelijking*, vernoemd naar de negentiende-eeuwse Duitse wiskundige Karl Weierstraß. De complexe krommen die door dit soort vergelijkingen gedefinieerd worden, heten ook wel *elliptische krommen*. In dit proefschrift proberen we waarden van a en b te vinden voor de elliptische krommen die bij een speciale lijst van gepunte tori horen. Wat deze lijst zo speciaal maakt, wordt beschreven in het volgende deel van deze samenvatting.

Getaltheorie

In dit iets technischere deel van de samenvatting zal het getaltheoretische (oftewel arithmetische) aspect van mijn onderzoeksonderwerp toegelicht worden. Wegens het gebrek aan aanschouwelijke illustraties is de aantrekkingskracht hiervan misschien wat moeilijker om direct in te zien die dat van het meetkundige aspect. Toch vinden de problemen in dit vakgebied hun oorsprong in tamelijk eenvoudige wiskunde, en zijn ze vaak ook gerelateerd met de meetkundige objecten uit de vorige sectie. Kijkt u bijvoorbeeld eens naar de kwadraten

$$0, 1, 4, 9, 16, 25, 36, \ldots$$

en de derdemachten

$$\ldots, -216, -125, -64, -27, -8, -1, 0, 1, 8, 27, 64, 125, 216, \ldots$$

In de zeventiende eeuw vroeg de Franse wiskundige Pierre de Fermat zich af welke gehele getallen er ingeklemd zitten tussen een kwadraat en een derdemacht, in die zin dat het voorgaande gehele getal een kwadraat is en het volgende een derdemacht of omgekeerd. Een flauw antwoord is snel gevonden, namelijk 0. Na wat turen ziet u waarschijnlijk ook de spannender oplossing, te weten 26. Daarna is het een stuk lastiger om een nieuwe oplossing te vinden. Fermat nu bewees dat de twee oplossingen boven ook daadwerkelijk de enige zijn.

Iets formeler opgeschreven komt de vraag hierboven neer op het vinden van alle gehele getallen x en y die voldoen aan

$$y^2 = x^3 + 2$$

of

$$y^2 = x^3 - 2.$$

We zien de Weierstraßvergelijkingen (1) uit de vorige sectie opduiken, met a gelijk aan 0 en $b = \pm 2$. Dit is slechts één voorbeeld van de verbanden tussen getaltheorie en meetkunde die in de arithmetische meetkunde worden gebruikt.

Een essentieel getaltheoretisch hulpmiddel om dergelijke problemen op te lossen, is een veralgemening van gehele getallen en breuken die *algebraïsche getallen* worden genoemd. Dit zijn de getallen die kunnen worden verkregen als oplossing van een vergelijking van de vorm

$$c_n t^n + c_{n-1} t^{n-1} + \cdots + c_1 t + c_0 = 0,$$

waar n en de getallen $c_n, \ldots c_0$ allemaal geheel zijn. Voorbeelden zijn de gulden snede $(1 + \sqrt{5})/2$ (een oplossing van $t^2 - t - 1 = 0$) en $\sqrt[3]{2}$ (een oplossing van $t^3 - 2 = 0$). Voorbeelden van getallen die niet algebraïsch zijn worden gegeven door e en π, en in feite zijn "de meeste" getallen niet algebraïsch.

Zo ook hebben "de meeste" gepunte tori niets met algebraïsche getallen van doen. Er is echter een kleine deelklasse die wel een hoop informatie over deze getallen bevat. Dit zijn de *arithmetische* gepunte tori, maar voordat we deze objecten kunnen beschouwen, is eerst een kleine uitweiding vereist.

Betegelingen afkomstig van gepunte tori, zoals die in Figuur 1, hebben een enorme hoop symmetrie. Deze symmetrie kan worden gecodeerd in een zogeheten *Fuchsgroep*, vernoemd naar een andere negentiende-eeuwse Duitse wiskundige, en wel Lazarus Fuchs. Eén van de simpelste soorten Fuchsgroepen bestaat uit de matrices van de vorm

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

waarbij a, b, c en d geheel zijn, $ad - bc$ gelijk is aan 1, en c deelbaar is door N. Hier is N een vast gekozen geheel getal. Bij deze groepen hoort een kromme (niet noodzakelijk een torus), die gewoonlijk $X_0(N)$ wordt genoemd en een voorbeeld vormt van een *klassieke modulaire kromme*.

Het zij hier vermeld (zonder op details in te gaan) dat de krommen $X_0(N)$ gebruikt kunnen worden om getaltheoretische stellingen te bewijzen die op het eerste gezicht een nogal magische indruk kunnen wekken. Als eerste kan bijvoorbeeld door de punten op $X_0(1)$ te bestuderen een verklaring worden gegeven voor het feit dat het getal

$$e^{\sqrt{163}\pi} \approx 262537412640768744{,}999999999998$$

tot op 11 cijfers na de komma gelijk is aan een geheel getal, iets dat a priori puur toevallig lijkt. Verder is de *Laatste Stelling van Fermat*, die beweert dat de vergelijking

$$x^n + y^n = z^n$$

voor $n \geq 3$ geen niet-triviale oplossingen in gehele getallen heeft, bewezen door het aantonen van een diepgaand verband tussen de krommen $X_0(N)$ en elliptische krommen afkomstig van Weierstraßvergelijkingen waarvoor de a en b in (1) breuken zijn.

De moraal hiervan is dat kennis van de krommen $X_0(N)$ vanuit getaltheoretisch opzicht geweldig nuttig is. In de jaren zestig van de vorige eeuw heeft de Japanse wiskundige Gorō Shimura een manier bedacht om dergelijke krommen niet alleen te construeren met behulp van matrices, maar ook met zogenaamde *quaternionen*. Een arithmetische gepunte torus is nu per definitie een gepunte torus waarvoor de symmetriegroep nagenoeg gelijk is aan de groepen die bij de krommen horen die Shimura beschouwt.

Voor arithmetische gepunte tori is de vergelijking (1) veel specialer. Het is dan bijvoorbeeld zo dat a en b allebei algebraïsche getallen zijn, iets dat voor de meeste gepunte tori absoluut niet het geval is. Verder is het mogelijk om de oplossingen van (1) modulo een priem te bekijken. Het is dan mogelijk dat de kromme gedefinieerd door deze vergelijking er wat minder prettig uit gaat zien, bijvoorbeeld omdat één van de gelijmde zijden in Figuur 3 oneindig lang wordt (het geval van "multiplicatieve reductie"). Voor arithmetische gepunte tori gebeurt dat echter slechts voor een zeer klein aantal priemen. Met andere woorden, deze krommen hebben net als de klassieke modulaire krommen interessante arithmetische eigenschappen te over.

Een motivatie om arithmetische gepunte tori te bestuderen, in plaats van algemene gepunte tori, is dat ze een simpel praktijkvoorbeeld vormen waarin aspecten van Shimura's erg algemene en abstracte theorie kunnen worden bestudeerd. De Japanse wiskundige Kisao Takeuchi heeft in 1983, het jaar van mijn geboorte, een artikel gepubliceerd waarin alle 71 symmetriegroepen worden bepaald die kunnen optreden. In dit proefschrift heb ik naar aanleiding van zijn resultaten (en die van vele anderen voor mij) enkele methoden ontwikkeld om vergelijkingen van de vorm (1) te bepalen voor de corresponderende tori.

Overzicht

Rest me nog om een inhoudsoverzicht van dit proefschrift te geven. Hierbij zal ik iets meer jargon gebruiken: van sommige hoofdstukken is de essentiële simpliciteit helaas iets moeilijker over te brengen dan in de uitleg boven.

Hoofdstuk 1 geeft een wiskundige beschrijving van de betegelingen van de Poincaréschijf die uitgaande van een $(1; e)$-groep geconstrueerd kunnen worden. We bepalen in dit hoofdstuk de meest symmetrische vierhoeksbetegelingen voor zo'n groep, samen met een achthoeksbetegeling die handig is voor een in hoofdstuk 4 opgenomen algoritme en waarvan een voorbeeld gegeven wordt door het watermerk op de omslag van dit proefschrift.

Hoofdstuk 2 en **3** behandelen de begrippen uit de theorie rond quaternionalgebra's en Shimurakrommen die nodig zijn voor de rest van het proefschrift. We definiëren canonieke modellen voor arithmetische gepunte tori en onderzoeken over welke getallenlichamen deze modellen zijn gedefinieerd. In **hoofdstuk 4** worden vervolgens de sporen van Frobenius van deze canonieke modellen uitgerekend met behulp van de Eichler-Shimurabetrekking.

In **hoofdstuk 5** bestuderen we arithmetische gepunte tori bij een priem $\mathfrak{p}$ waar de quaternionalgebra B vertakt. Dit betekent dat de lokalisatie van B bij die priem niet isomorf is met een matrixalgebra. Door de theorie van $\mathfrak{p}$-adische uniformisatie te gebruiken (een $\mathfrak{p}$-adisch analogon van de betegelingen in Figuur 1) kunnen we essentiële informatie verzamelen over de torus, zoals de valuatie van zijn j-invariant bij $\mathfrak{p}$. We geven vervolgens aan hoe door het gebruik van klassieke modulaire krommen deze resultaten toegepast kunnen worden om een Weierstraßvergelijking als in (1) te vinden.

Hoofdstuk 6 beschrijft de tori die horen bij $(1; e)$-groepen die commensurabel zijn met één van de klassieke driehoeksgroepen. Deze driehoeksgroepen zijn de Fuchsgroepen die aanleiding geven tot betegelingen van de Poincaréschijf bestaande uit driehoeken. In dit geval kan een Weierstraßvergelijking worden bepaald door de theorie van Belyi-afbeeldingen (en kindertekeningen) te gebruiken.

In **hoofdstuk 7** geven we eindelijk onze vergelijkingen voor arithmetische gepunte tori, of beter gezegd voor hun canonieke modellen. Hier is nog tamelijk wat werk mee gemoeid, want hoewel we in Hoofdstuk 3 een definitie hebben gegeven voor zulke modellen, is het een stuk lastiger om hier daadwerkelijk mee te rekenen (een vaak voorkomend fenomeen in de wiskunde). Een aantal vergelijkingen in het eerste deel van Hoofdstuk 7 wordt eerst heuristisch afgeleid: we rechtvaardigen onze aannames vervolgens in het tweede deel met behulp van de theorie van Hilbertmodulaire vormen om te concluderen dat deze vergelijkingen inderdaad correct zijn.

Curriculum Vitae

Jeroen Sijsling werd op 23 december 1983 geboren in Arnhem. Zijn jeugd heeft hij doorgebracht in het Gelderse Doetinchem, waar hij in 2001 aan het St. Ludgercollege zijn gymnasiumdiploma verkreeg.

De aansluitende wiskundestudie aan de Rijksuniversiteit Groningen werd in 2006 cum laude afgerond. Zijn doctoraalscriptie, geschreven onder begeleiding van Jaap Top en getiteld *Dessins d'enfants*, betrof een onderzoeksgebied waaraan hij reeds op de kleuterschool enig voorbereidend werk had verricht.

In hetzelfde jaar 2006 begon Jeroen met zijn promotieonderzoek aan de Universiteit Utrecht onder supervisie van Frits Beukers, waarvan u het resultaat in handen heeft. Tijdens zijn onderzoeksperiode assisteerde hij aan deze universiteit bij enige bachelorvakken en maakte hij deel uit van de commissie Onderwijsvormen. Hiernaast heeft hij in 2009 de Nederlandse afvaardiging naar het IMC in Boedapest begeleid en was hij coördinator bij de Benelux Olympiade van 2010.

Buiten Nederland heeft Jeroen verscheidene conferenties en seminaria bijgewoond in onder andere Aken, Barcelona, Bonn, Luminy, Mainz en Montréal. Zijn voordracht in het Intercity-seminarium waarin hij na een vraag uit het publiek het begrip ”canoniek op keuze na” poogde te introduceren mag als laatste niet onvermeld blijven.

Dankwoord

De zandloper van vier jaar is op, het tumult verstild, en de rusteloze urgentie voor even ten einde. Graag zou ik nu de mensen bedanken die zich in de afgelopen periode moeite voor me getroost hebben en me vreugde hebben bezorgd.

Allereerst is dat Frits Beukers, mijn begeleider. Frits, dank je voor de vrijheid die je me gegeven hebt en voor de vele discussies, die me erg hielpen om mijn gedachten op orde te krijgen. Vooral ook bedankt voor de geweldige suggestie voor een promotieonderwerp en, toen dat lastiger bleek dan we hadden gedacht en steeds zwaarder gereedschap uit de kast moest worden getrokken, voor het vertrouwen in de goede afloop. Het was me werkelijk een genoegen.

For spending time and trouble on substantially improving the final version of this thesis, I thank the reading committee, to wit Pilar Bayer, Gunther Cornelissen, Bas Edixhoven, Marius van der Put, and finally John Voight, to whom I owe an additional debt of gratitude, both for developing the `Magma` functionality without which this thesis could not have been written in the first place and for his unstinting support in my attempts to master it, not to mention for helping me with quotidian questions quaternionic.

Gratitude is also due to all the people that helped push my research in the right direction through stimulating conversations and e-mail exchanges. In particular, I hereby thank Frans Oort, Tomoyoshi Ibukiyama, Fumiharu Kato, Santi Molina and Victor Rotger.

Voor de fijne dagelijkse sfeer wil ik mijn kamergenoten van de afgelopen jaren, Oliver, Joost, Ittay, Màrti, Bas en Esther, hartelijk bedanken. Samen met Jakub en dessinmeester Sander dank ik Oliver verder voor de vele interessante en verbredende gesprekken tijdens mijn eerste jaren als AiO, alsook voor het verschaffen van de nodige droge humor.

Naast mijn eigen kamer is ook de aangrenzende op 607 zeer belangrijk geweest tijdens de cruciale tweede helft van mijn promotieperiode. Ik dank Arthur "Buurmannetje" van Dam, Tammo, Jan-Willem en mede-anglofiel Sebastiaan voor de ontspanning, gezelligheid, en vreselijke kantoorhumor gepaard gaande met ons espressoritueel. Arthur, jou dank ik verder voor je uitgebreide LaTeX-hulp, je organisatie van vele plezierige fiets- en schaatstochten, maar boven alles voor je kalme aanmoediging, die een hoop verschil voor me heeft gemaakt. Het spijt me dat er geen Engeland-Italië inzat op het afgelopen WK. Tammo, bedankt voor je onvermoeide grafische inspanningen, die in een omslag hebben geresulteerd die er mooier uitziet dan ik me voor had kunnen stellen, en voor het samen met Brenda verweideren van vele spelfouten en ambiguïteiten in de Nederlandse tekst. Het bewaken van het fort en het verspreiden van gezelligheid nu de oude garde weg is, is aan Sebastiaan en Jan Willem toevertrouwd.

Acute frustraties kon ik altijd botvieren op de *steel wall of niceness* van het instituut, dat wil zeggen kamer 401. Charlene, dank voor je raadsels over Pisotgetallen, waarover ik, hoewel niet in staat ze alle op te lossen, met plezier heb nagedacht. Daarnaast heb ik, samen met een hoop anderen, veel genoegen beleefd aan de spelletjesavonden bij jou en Bas thuis. Vincent, door jouw brede interesse en enthousiasme kon ik bij jou vaak mijn verhaal kwijt. Ook jou dank ik voor het aanleveren van een grote en geschakeerde variëteit aan interessante en uitdagende conundra.

Bas, net als Vincent word jij gekenmerkt door een brede interesse en een bijzonder idiosyncratisch gevoel voor humor. Verder heb ik veel geleerd van je manier van uitleggen, die net als jijzelf in extreme omstandigheden ten diepste kalm en kristalhelder blijft. Jou en medeliefhebster van $\mathfrak{p}$-adica Janne dank ik voor de morele steun (al dan niet in de vorm van gratis eten).

Buiten Utrecht heb ik me ook aan faculteiten elders thuisgevoeld, in het bijzonder aan mijn *alma mater* de Rijksuniversiteit Groningen en de Universiteit Leiden. Uit Groningen zou ik naast de reeds genoemde Marius van der Put ook graag Jaap Top willen bedanken voor het nog steeds aandachtige contact. Uit Leiden dank ik Peter Bruin, René Pannekoek en Marco Streng voor het organiseren van vele erg leerzame seminaria. Weiter möchte ich aus Aachen noch gerne Mohamed Barakat danken für seine unglaubliche Gastfreundschaft.

Further thanks befall Job, Bart, Jantien, Jaap, Aleksandra, Albert Jan, Jan Jitse, Wouter, Arjen, Sebastian, Rogier, Alex, Alex, Erik, Shinji, Lee, Slavik, Andor, Arthemy, Maarten, Angela, Valerio, Steve, Lenny, Bas and Alef for being such fine colleagues.

Mijn vrienden en familie dank ik voor hun onvoorwaardelijke steun tijdens de afgelopen jaren. Naast mijn broer, die samen met Arthur bereid is gebleken als paranimf mijn promotieplechtigheid in goede banen te leiden, wil ik tot slot in het bijzonder mijn ouders bedanken. Pap en mam, de woorden daarvoor ben ik niet in staat te vinden, maar God weet hoe blij ik ben dat ik jullie heb.

And what would even heavenly bliss be
without wishing, without the wish to possess it,
for only sober understanding thinks it
foolish to wish for what one possesses.

— Søren Kierkegaard