Arithmetic aspects of Triangle Groups

Luiz Kazuo Takei

Department of Mathematics and Statistics

McGill University

March 2014

A thesis submitted to McGill University

in partial fulfillment of the requirements for a Ph.D. degree

Abstract

We study some arithmetic properties of Triangle Groups, a family of Fuchsian groups that generalize the modular group. We first recall the basic theory of Fuchsian groups and define precisely a Triangle Group. Secondly, we define congruence subgroups and compute the genus of the curves they uniformize. Thirdly, we characterize the normalizers of certain Triangle Groups and corresponding congruence subgroups. Finally, we study a family of curves that is closely related to Triangle Groups. In particular, we study modular embeddings defined by those curves and their ordinary locus.

Résumé

Cette thèse est consacrée à l'étude de certains aspects arithmétique d'une famille de groupes fuchsiens engendrés par des reflections par rapport aux arrêtes d'un triangle hyperbolique. On commence par rappeler la théorie de groupes fuchsiens et la définition de cette famille de groupes. On définit ensuite les sous-groupes de congruence et on calcule le genre des courbes qu'ils définissent. Ensuite, on décrit les normalisateurs de ces groupes. Les dernières sections sont consacrées à l'étude d'une famille de courbes algébriques étroitement liée à ces groupes. On étudie notamment son image dans certains espaces de modules et son lieu non-ordinaire.

Acknowledgements

I would like to thank my supervisors, Henri Darmon and Eyal Goren, for their support, patience and guidance throughout my studies at McGill University. They have also, together with the Department of Mathematics and Statistics at McGill, provided financial support during that time.

I would also like to mention John Voight and Paulo Ribenboim: the former greatly helped me with his knowledge of triangle groups and related areas, while the latter was a source of kind support and encouragement, especially in difficult times.

I would also like to thank my fellow students, including, but not limited to, Marc Masdeu, Mike Musty, Philip Rempel, Victoria de Quehen, Andrew Fiori, Francesc Castella, Juan Ignacio Restrepo, and Bahare Mirza, who have all helped me at different times.

Finally, I thank my parents, Mitsuca Miyashita and Suguio Takei, my wife, Phạm Nguyễn Hồng Phúc, my siblings, Andrea Mary Takei and Linus Jun Takei, and my in-laws, Phạm Hữu Cương, Nguyễn Thị Đao, Phạm Nguyễn Hữu Ân, Phạm Nguyễn Hồng Quang and Phạm Nguyễn Hữu Thuận: without their moral support I would not have been able to finish this thesis.

Contents

Introduction

The theory of modular forms has been studied for more than one hundred years, dating back, at least, to Felix Klein and his contemporaries. In the previous century, modular forms for the classical modular group $\mathrm{SL}_2(\mathbb{Z})$ and its congruence subgroups were extensively studied. It is now possible to say that we have a polished theory of modular forms. Good textbooks like [Miy06] and [DS05] are evidences of this fact.

The recent interest in modular forms is related to its connection with number theory questions. In particular, motivated by the Taniyama-Shimura conjecture and Fermat's Last Theorem, the second half of the twentieth century witnessed a gigantic effort to understand the relation between modular forms and elliptic curves, culminating in the celebrated proof of Fermat's Last Theorem, more than 350 years after its first appearance in Pierre de Fermat's notes. Since the modular forms of interest for this particular problem are those for $\mathrm{SL}_2(\mathbb{Z})$ and its congruence subgroups, much of the focus was directed toward those groups.

Although much less understood, non-congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ have also been studied in recent years. The pioneering article in this field is probably [ASD71], where Atkin and Swinnerton-Dyer proved some results and conjectured some other results about congruences involving the Fourier coefficients of modular forms for non-congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Scholl ([Sch85], [Sch86]) and Winnie-Li ([LLY05b]) have also contributed to this area. A slightly disappointing but (maybe exactly because of that) interesting fact proved by Serre-Thompson in [Tho89] and by Berger in [Ber94] states that Hecke operators, which play a prominent role in the theory of modular forms for congruence subgroups, yield no new information for non-congruence subgroups. A survey article about this area can be found in [LLY05a].

Even less understood than the non-congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ are the so called triangle groups. These form a special class of Fuchsian groups which includes $\mathrm{SL}_2(\mathbb{Z})$ as a particular example. From a number-theoretic point of view, it is an interesting family of Fuchsian groups because, via Belyĭ's Theorem ([Bel79]), every algebraic curve defined over a number field is uniformized, when viewed as a Riemann surface, by a triangle group. More recently, Darmon speculated in [Dar04] that triangle groups can be used to study the so called generalized Fermat's equation. An example of this strategy can be seen in [DG95] and [Dar97]. Among others, Y. Yang [Yan] and Doran-Gannon-Movasati-Shokri [DGMM] have studied automorphic forms for triangle groups. A valuable resource to learn about triangle groups and facts of interest to number theory is [CV], by Clark and Voight.

We present in the following chapters a study of triangle groups, the algebraic curves they uniformize and, in particular, their relations to number theory. Chapter 0 recalls the basic theory of Fuchsian groups that will be necessary for the later chapters and defines a triangle group.

In Chapter 1, we define subgroups of triangle groups in analogy to the congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. The first natural question then arises: what are the genera of the curves uniformized by those subgroups? We answer this question as well as another interesting question, related to the nature of the quotient of a triangle group by one of these subgroups.

In Chapter 2, we recall a relation found by Hecke in 1928 ([Hec28]) between the class number of some quadratic number fields and the representation of certain quotient groups on the space of holomorphic differentials of classical modular curves. We then prove a generalization of that result, which also appears in [Tak12], to the case where the group $\mathrm{SL}_2(\mathbb{Z})$ is replaced by an arbitrary triangle group.

Chapter 3 studies normalizers of triangle groups. In particular, we give explicit computations of the normalizers of triangle groups and proceed to the computation of the normalizers of their "congruence" subgroups.

Chapter 4 closely investigates a family of hyperelliptic curves with real multiplication. Originally studied by Tautz-Top-Verberkmoes in [TTV91], the TTV family of curves also appeared in [Dar00], where Darmon finds a relation between them and certain triangle groups. We first analyze the case of genus 2 and compute its Igusa-Clebsch invariants. We then study how this family of curves embed in a certain Hilbert modular space.

Finally, Chapter 5 recalls the theory of Hasse-Witt and Cartier-Manin matrices and uses it to study the non-ordinary locus of the reduction mod p of the TTV family of curves. We then end the chapter with a comparison between that and the genus of certain "congruence" subgroups of triangle groups.

Chapter 0

Fuchsian Groups and Triangle Groups

In this chapter we review the basic theory of Fuchsian Groups and, in particular, of Hyperbolic Triangle Groups. Unless otherwise stated, the results stated in this chapter, as well as their proofs, can be found in [Shi94].

0.1 Topological Groups

Definition 0.1.1. A **topological group** is a group G with a topology such that the following maps are continuous:

$$G \times G \to G \qquad\qquad G \to G$$

$$(g,h) \mapsto gh \qquad\qquad g \mapsto g^{-1}$$

Remark 0.1.2. All topological groups will be assumed to be Hausdorff.

Definition 0.1.3. Let G be a topological group and S a topological space. We say that G **acts continuously on** S if a continuous map

$$G \times S \to S \qquad (g,s) \mapsto gs$$

is given and satisfies the following:

(i) $(ab)s = a(bs)$ for every $a, b \in G$ and $s \in S$

(ii) $es = s$ for every $s \in S$ (e denotes the identity element of G)

Proposition 0.1.4. *Let G be a locally compact group, K a compact subgroup, $h : G \to \frac{G}{K}$ the natural projection. If Γ is a discrete subgroup of G, then for every $z \in \frac{G}{K}S$ there exists a neighborhood U of z such that*

$$\{g \in \Gamma | g(z) = z\} = \{g \in \Gamma | g(U) \cap U \neq \emptyset\}.$$

Definition 0.1.5. Two subgroups Γ and Γ' of a group G are said to be **commensurable** if $\Gamma \cap \Gamma'$ is of finite index in Γ and in Γ'.

Proposition 0.1.6. *(1) If Γ_1 is commensurable with Γ_2 and Γ_2 is commensurable with Γ_3, then Γ_1 is commensurable with Γ_3*

(2) Let Γ and Γ' be commensurable subgroups of a topological group G. If Γ is discrete, then so is Γ'.

(3) Let Γ and Γ' be commensurable subgroups of a locally compact group G. If $\Gamma\backslash G$ is compact, then so is $\Gamma'\backslash G$.

Remark 0.1.7. If Γ is a subgroup of a topological group G, then we can consider $\Gamma\backslash G$ (the set of all left cosets of G) as a topological space (with the quotient topology).

0.2 Fuchsian Groups

We will start with a brief study of the group $\mathrm{GL}_2(\mathbb{C})$, which is a (Hausdorff) topological group (when considered as a topological subspace of $\mathbb{C}^5$ defined by $(xw - yz)u = 1$).

For $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$ and $z \in \mathbb{C} \cup \{\infty\}$, we define $\sigma(z) = \dfrac{az+b}{cz+d}$.

If σ is not a multiple of the identity matrix, the Jordan canonical form of σ is one of the following:

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \lambda \neq \mu$$

Definition 0.2.1. In the first case, we say σ is **parabolic**. In the second case, letting $c := \frac{\lambda}{\mu}$, we call σ **elliptic** if $|c| = 1$, **hyperbolic** if c is real and positive and **loxodromic** otherwise.

Proposition 0.2.2. *Let $\sigma \in \mathrm{SL}_2(\mathbb{C})$, $\sigma \neq \pm I$. Then*

$$\begin{aligned} \sigma \textit{ is parabolic} &\Leftrightarrow \operatorname{tr}(\sigma) = \pm 2 \\ \sigma \textit{ is elliptic} &\Leftrightarrow \operatorname{tr}(\sigma) \textit{ is real and } |\operatorname{tr}(\sigma)| < 2 \\ \sigma \textit{ is hyperbolic} &\Leftrightarrow \operatorname{tr}(\sigma) \textit{ is real and } |\operatorname{tr}(\sigma)| > 2 \\ \sigma \textit{ is loxodromic} &\Leftrightarrow \operatorname{tr}(\sigma) \textit{ is not real.} \end{aligned}$$

We will now restrict our attention to $\mathrm{GL}_2(\mathbb{R})$.

It is not hard to show that if $\alpha \in \mathrm{GL}_2(\mathbb{R})$ and $z \in \mathbb{C}$, then

$$\det(\alpha) \cdot \operatorname{Im}(z) = \operatorname{Im}(\alpha(z)) \cdot |j(\alpha, z)|^2$$

where $j(\alpha, z) := rz + s$ and $\alpha = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$

So, if we take $\alpha \in \mathrm{GL}_2^+(\mathbb{R}) = \{\alpha \in \mathrm{GL}_2(\mathbb{R}) | \det(\alpha) > 0\}$, then α maps $\mathcal{H} := \{z \in \mathbb{C} | \operatorname{Im}(z) > 0\}$ onto itself. Since α induces the identity map if and only if it is a multiple of the identity matrix, we may restrict our attention to $\dfrac{\mathrm{GL}_2^+(\mathbb{R})}{\mathbb{R}^* \cdot I} = \dfrac{\mathrm{SL}_2(\mathbb{R})}{\{\pm I\}}$.

Proposition 0.2.3. *Let $\sigma \in \mathrm{SL}_2(\mathbb{R})$, $\sigma \neq \pm I$. Then,*

$$\begin{array}{lll} \sigma \textit{ is parabolic} & \Leftrightarrow & \sigma \textit{ has only one fixed point on } \mathbb{R} \cup \{\infty\} \\ \quad\quad \textit{elliptic} & \Leftrightarrow & \sigma \textit{ has one fixed point in } z \in \mathcal{H} \textit{ and the other is } \overline{z} \\ \quad\quad \textit{hyperbolic} & \Leftrightarrow & \sigma \textit{ has two fixed points on } \mathbb{R} \cup \{\infty\} \end{array}$$

Proposition 0.2.4. *Let $\sigma \in \mathrm{SL}_2(\mathbb{R})$, $\sigma \neq \pm I$ and let $m \in \mathbb{Z}$ such that $\sigma^m \neq \pm I$. Then, σ is parabolic (resp. elliptic, hyperbolic) if and only if σ^m is parabolic (resp. elliptic, hyperbolic).*

Proposition 0.2.5. *$\mathcal{H}$ is homeomorphic to $\dfrac{\mathrm{SL}_2(\mathbb{R})}{\mathrm{SO}(2))}$. Moreover the homeomorphism preserves the left action of $\mathrm{SL}_2(\mathbb{R})$.*

Definition 0.2.6. A subgroup Γ of $\mathrm{SL}_2(\mathbb{R})$ is a **Fuchsian group** if it is discrete.

From now on, let Γ be a Fuchsian group.

Definition 0.2.7. A point $z \in \mathcal{H}$ is an **elliptic point of** Γ if there exists an elliptic element $\sigma \in \Gamma$ such that $\sigma(z) = z$. A point $s \in \mathbb{R} \cup \{\infty\}$ is a **cusp of** Γ if there exists a parabolic $\sigma \in \Gamma$ such that $\sigma(s) = s$.

Proposition 0.2.8. *If z is an elliptic point if Γ, then $\{\sigma \in \Gamma | \sigma(z) = z\}$ is a finite cyclic group.*

Let s be a cusp of Γ. Then, we define

$$F(s) := \{\alpha \in \mathrm{SL}_2(\mathbb{R}) | \alpha(s) = s\}$$

$$P(s) := \{\alpha \in F(s) | \alpha \text{ is parabolic or } \pm I\}$$

Proposition 0.2.9. *Let s be a cusp of Γ and $\Gamma_s = \{\sigma \in \Gamma | \sigma(s) = s\}$. Then $\dfrac{\Gamma_s}{\Gamma \cap \{\pm I\}}$ is isomorphic to $\mathbb{Z}$. Moreover, an element of Γ_s is either $\pm I$ or parabolic, i.e., $\Gamma_s = \Gamma \cap P(s)$.*

Proposition 0.2.10. *The elements of finite order of Γ are exactly the elliptic elements and $\pm I$.*

Proposition 0.2.11. *The set of all elliptic points of Γ has no limit point in $\mathcal{H}$.*

Proposition 0.2.12. *Let σ is an elliptic element of Γ. If σ as a matrix is of order $2h$ (even), then Γ contains $-I$ and the transformation $z \mapsto \sigma(z)$ is of order h.*

Corollary 0.2.13. *If Γ does not contain $-I$, then every elliptic element of Γ is of an odd order.*

Sometimes it is useful to look at the image $\overline{\Gamma}$ of Γ via the natural map

$$\mathrm{SL}_2(\mathbb{R}) \longrightarrow \frac{\mathrm{SL}_2(\mathbb{R})}{\{\pm I\}} = \mathrm{PSL}_2(\mathbb{R})$$

Definition 0.2.14. If z is an elliptic point of Γ, the **order of z (relative to** Γ**)** is the order of the group $\{\sigma \in \overline{\Gamma} | \sigma(z) = z\} \subseteq \overline{\Gamma}$.

Proposition 0.2.15. *Let α of* $\mathrm{SL}_2(\mathbb{R})$ *be an elliptic or parabolic element. Then α is not conjugate to α^{-1} in* $\mathrm{SL}_2(\mathbb{R})$.

0.2.1 The topological space $\Gamma\backslash\mathcal{H}^*$

As before, Γ denotes a Fuchsian group. We define $\mathcal{H}^* := \mathcal{H} \cup \{\text{cusps of } \Gamma\}$.

It is not hard to see that the elements of Γ act on $\mathcal{H}^*$ and, thus, the quotient is meaningful. Let us define a topology on $\mathcal{H}^*$. For every $z \in \mathcal{H}$, as a fundamental system of open neighborhoods of z, we take the usual one. For a fundamental system of open neighborhoods of a cusp $s \neq \infty$ we take all sets of the form:

$$\{s\} \cup \{\text{the interior of a circle in } \mathcal{H} \text{ tangent to the real axis at } s\}.$$

For $s = \infty$ we take the sets

$$\{\infty\} \cup \{z \in \mathcal{H} | \operatorname{Im}(z) > c\}$$

for all positive numbers c.

Now we can consider the quotient space $\Gamma\backslash\mathcal{H}^*$ as a topological space (with the quotient topology). It is not hard to show it is a Hausdorff space and that the elements of Γ act on it as homeomorphisms.

Lemma 0.2.16. *For every cusp s of Γ, there exists a neighborhood U of s in $\mathcal{H}^*$ such that $\Gamma_s = \{\sigma \in \Gamma | \sigma(U) \cap U \neq \emptyset\}$.*

Theorem 0.2.17. *The quotient space $\Gamma\backslash\mathcal{H}^*$ is Hausdorff.*

Proposition 0.2.18. *The quotient space $\Gamma\backslash\mathcal{H}^*$ is locally compact.*

Definition 0.2.19. A Fuchsian group Γ is **of the first kind** if $\Gamma\backslash\mathcal{H}^*$ is compact.

Proposition 0.2.20. *Let Γ and Γ' be mutually commensurable Fuchsian groups. Then Γ and Γ' have the same set of cusps.*

Proposition 0.2.21. *Let Γ and Γ' be as in the previous proposition. Then Γ is of the first kind if and only if Γ' is of the first kind.*

Proposition 0.2.22. *If Γ is of the first kind, then the number of Γ-inequivalent cusps (resp. elliptic points) is finite.*

Proposition 0.2.23. *If $\Gamma\backslash\mathcal{H}$ is compact, then Γ has no parabolic element.*

0.2.2 $\Gamma\backslash\mathcal{H}^*$ as a Riemann surface

We will now define a Riemann surface structure on $\Gamma\backslash\mathcal{H}^*$. Let $\varphi : \mathcal{H}^* \to \Gamma\backslash\mathcal{H}^*$ be the natural projection. For each $v \in \mathcal{H}^*$, define

$$\Gamma_v := \{\gamma \in \Gamma | \gamma(v) = v\}.$$

By Proposition 0.1.4 and Lemma 0.2.16, there exists an open neighborhood U of v such that

$$\Gamma_v = \{\gamma \in \Gamma | \gamma(U) \cap U \neq \emptyset\}.$$

This induces a natural injection $\Gamma_v\backslash U \to \Gamma\backslash\mathcal{H}^*$ and $\Gamma_v\backslash U \to$ is an open neighborhood of $\varphi(v)$ in $\Gamma\backslash\mathcal{H}^*$.

If v is neither an elliptic point nor a cusp, Γ_v contains only I and possibly $-I$. So, $U = \Gamma_v\backslash U$ and we take $(\Gamma_v\backslash U, \varphi^{-1})$ as a member of the atlas of $\Gamma\backslash\mathcal{H}^*$.

What if v is an elliptic point? Let $\overline{\Gamma_v} = \dfrac{\{\pm I\} \cdot \Gamma_v}{\{\pm I\}}$ and λ be a holomorphic isomorphism of $\mathcal{H}$ onto the unit disc D such that $\lambda(v) = 0$. We know $\overline{\Gamma_v}$ is a cyclic group of finite order (Proposition 0.2.8). If its order is n, then $\lambda\overline{\Gamma_v}\lambda^{-1}$ consists of the transformations

$$w \mapsto \zeta^k w, \quad k = 0, 1, ..., n-1, \quad \zeta = e^{\frac{2\pi i}{n}}.$$

This allows us to define a map $p : \Gamma_v \backslash U \to \mathbb{C}$ by $p(\varphi(z)) = \lambda(z)^n$, which is a homeomorphism onto an open subset of $\mathbb{C}$. Thus, we include $(\Gamma_v \backslash U, p)$ in our atlas.

It remains to study the case of a cusp s. Let $\rho \in \mathrm{SL}_2(\mathbb{R})$ such that $\rho(s) = \infty$. Then, by Proposition 0.2.9, we have

$$\{\pm I\} \cdot \rho \Gamma_s \rho^{-1} = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m \middle| m \in \mathbb{Z} \right\}$$

for some positive number h. Hence, we can define a homeomorphism p of $\Gamma_s \backslash U$ onto an open subset of $\mathbb{C}$ by $p(\varphi(z)) = e^{\frac{2\pi i \rho(z)}{h}}$ and include $(\Gamma_s \backslash U, p)$ in our atlas.

These charts endow $\Gamma \backslash \mathcal{H}^*$ with a Riemann surface structure. By abuse of language, we will still call points of $\Gamma \backslash \mathcal{H}^*$ elliptic points and cusps if they come from elliptic points and cusps in $\mathcal{H}^*$.

Let Γ be a Fuchsian group of the first kind and Γ' a subgroup of Γ of finite index.

Exercise 0.2.24. The natural map $f : \Gamma' \backslash \mathcal{H}^* \to \Gamma \backslash \mathcal{H}^*$ is holomorphic. Furthermore, the degree of f is $\left[\overline{\Gamma} : \overline{\Gamma'}\right]$.

We therefore have the commutative diagram

$$\begin{tikzcd}
\mathcal{H}^* \arrow[r, "identity"] \arrow[d, "\varphi'"'] & \mathcal{H}^* \arrow[d, "\varphi"] \\
\Gamma'\backslash\mathcal{H}^* \arrow[r, "f"'] & \Gamma\backslash\mathcal{H}^*
\end{tikzcd}$$

As before, let $\overline{\Gamma}$ and $\overline{\Gamma'}$ denote the images of Γ and Γ' by the natural map

$$\mathrm{SL}_2(\mathbb{R}) \to \frac{\mathrm{SL}_2(\mathbb{R})}{\{\pm I\}}.$$

For every $z \in \mathcal{H}^*$ we define

$$\overline{\Gamma}_z := \{\gamma \in \overline{\Gamma} | \gamma(z) = z\}, \quad \overline{\Gamma}'_z := \overline{\Gamma}_z \cap \overline{\Gamma'}.$$

Let $z \in \mathcal{H}^*$, $p = \varphi(z)$ and $f^{-1}(p) = \{q_1, ..., q_h\}$. Choose points $w_k \in \mathcal{H}^*$ such that $q_k = \varphi'(w_k)$.

Proposition 0.2.25. *The ramification index e_k of f at q_k is $\left[\overline{\Gamma}_{w_k} : \overline{\Gamma}'_{w_k}\right]$. Moreover, if $w_k = \sigma_k(z)$ with $\sigma_k \in \overline{\Gamma}$, then*

$$e_k = \left[\overline{\Gamma}_z : (\sigma_k^{-1}\overline{\Gamma'}\sigma_k) \cap \overline{\Gamma}_z\right] \quad \textit{and} \quad \overline{\Gamma} = \bigcup_{k=1}^{h} \overline{\Gamma'}\sigma_k\overline{\Gamma}_z \ \textit{(disjoint union).}$$

Especially, if $\overline{\Gamma'}$ is a normal subgroup of $\overline{\Gamma}$, then

$$e_1 = ... = e_h \quad \textit{and} \quad \left[\ \overline{\Gamma} : \overline{\Gamma'}\ \right] = e_1 h.$$

0.2.3 Signature of a Fuchsian Group

In this subsection we assume Γ satisfies $\mu(\Gamma\backslash\mathcal{H}) < \infty$ (an explanation of this condition is found in [Kat92], especially Theorem 3.1.1). For the purposes of this thesis, it suffices to say that every Fuchsian group in what follows satisfies this condition.

With this hypothesis, Γ is of the first kind (cf. Theorem 4.5.2 in [Kat92]). Moreover, it has a fundamental region with finitely many sides (Theorem 4.1.1 in [Kat92]) and, hence, $\overline{\Gamma}$ has finitely many conjugacy classes of maximal elliptic cyclic subgroups (Theorem 3.5.2 in [Kat92]) with periods $m_1, \cdots, m_r$. Also, $\overline{\Gamma}$ has s conjugacy classes of maximal parabolic cyclic subgroups. Let g denote the genus of $\Gamma\backslash\mathcal{H}^*$. With that notation, we define the signature of Γ as follows.

Definition 0.2.26. The tuple $(g; m_1, \ldots, m_r; s)$ is the **signature** of Γ.

Remark 0.2.27. Since parabolic elements are of infinite order (cf. Proposition 0.2.9), the signature is sometimes written

$$(g; m_1, \ldots, m_r, m_{r+1}, \ldots, m_{r+s})$$

where $m_{r+1} = \cdots = m_{r+s} = \infty$.

Proposition 0.2.28. *If Γ has signature $(g; m_1, \ldots, m_r; s)$ then, as a group,*

$\overline{\Gamma}$ *is given by the following presentation:*

generators: $A_1, \dots, A_g, B_1, \dots, B_g, X_1, \dots, X_r, P_1, ..., P_s$

relations: $X_1^{m_1} = \cdots = X_r^{m_r} = 1,$ *and*

$$P_1 \cdots P_s X_1 \cdots X_r A_1 B_1 A_1^{-1} B_1^{-1} \cdots A_g B_g A_g^{-1} B_g^{-1} = 1$$

Proof. (see end of section 4.3 in [Kat92]) □

0.3 Triangle groups

Consider $2 \leq a \leq b \leq c$ (integers or ∞) such that

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1.$$

Definition 0.3.1. A **triangle group** of type (a, b, c) (or (a, b, c)-**triangle group**) is a subgroup of $\mathrm{SL}_2(\mathbb{R})$ whose image in $PSL_2(\mathbb{R})$ is generated by r_1r_2, r_2r_3 and r_3r_1, where r_1, r_2, r_3 are the reflections across the sides of a hyperbolic triangle with angles $\frac{\pi}{a}, \frac{\pi}{b}, \frac{\pi}{c}$.

This definition does not tell us explicitly that a triangle group is a Fuchsian group. The next theorem tells us exactly that and also gives a characterization of triangle groups in terms of the signature.

Theorem 0.3.2. (Theorem 10.6.4 in [Bea83]) *A group G is an (a, b, c)-triangle group if and only if it is a Fuchsian group of the first kind with signature* $(0; a, b, c)$.

Remark 0.3.3. From the proof of Theorem 10.6.4 in [Bea83], we obtain a precise statement about the triangle group and its stabilizers. Let P_1, P_2, P_3 be the vertices of a hyperbolic triangle with angles $\pi/a_1, \pi/a_2, \pi/a_3$ respectively. Consider the triangle group G associated to this hyperbolic triangle. Take generators $\gamma_1, \gamma_2, \gamma_3$ of P whose fixed points are P_1, P_2, P_3. Then the stabilizers of P_1, P_2 and P_3 (in $\overline{G} \leq \mathrm{PSL}_2(\mathbb{R})$) are

$$\overline{G}_{P_i} = \langle \overline{\gamma_i} \rangle$$

and, moreover,

$$|\langle \overline{\gamma_i} \rangle| \quad = \quad a_i.$$

Remark 0.3.4. In view of the Proposition 0.2.28, we obtain that an (a, b, c)-triangle group is generated by elements $\gamma_1, \gamma_2, \gamma_3$ whose images in $\mathrm{PSL}_2(\mathbb{R})$ satisfy the following defining relations:

$$\begin{cases} \overline{\gamma}_1\overline{\gamma}_2\overline{\gamma}_3 = 1 \\ \overline{\gamma}_1^a = \overline{\gamma}_2^b = \overline{\gamma}_3^c = 1 \end{cases}$$

(if $a = \infty$, the relation $\overline{\gamma}_1^a = 1$ is omitted; and similarly for b and c).

The next theorem (proved in [Tak77]) tells us that an (a, b, c)-triangle group is essentially unique. Because of its importance, we present an outline of its proof. In what follows, the identity matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ will be denoted I.

Theorem 0.3.5. *Let $2 \leq a \leq b \leq c$ (integers or ∞) such that*

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1.$$

Let r be the number of those which are not ∞. Then

(i) If $r \geq 1$ and at least one of a, b, c is even, then there exists an (a, b, c)-triangle group Γ_0 such that any (a, b, c)-triangle group is $SL_2(\mathbb{R})$-conjugate to Γ_0. The group Γ_0 contains $-I$.

(ii) If $2 \leq r \leq 3$ and a, b, c are all odd (or ∞), then there exist two (non-conjugate) (a, b, c)-triangle groups Γ_0 and Γ_1 such that any (a, b, c)-triangle group is $\mathrm{SL}_2(\mathbb{R})$-conjugate to one of them. The group Γ_0 contains $-I$, while Γ_1 does not contain $-I$. Moreover, Γ_1 is a subgroup of index 2 in Γ_0

(iii) If either ($r = 1$ and a is odd) or ($r = 0$), then there exist three (non-conjugate) (a, b, c)-triangle groups Γ_0, Γ_1 and Γ_2 such that any (a, b, c)-triangle group is $\mathrm{SL}_2(\mathbb{R})$-conjugate to one of them. The group Γ_0 con-

tains $-I$, while Γ_1 and Γ_2 do not contain $-I$. Moreover, both Γ_1 and Γ_2 are subgroups of index 2 in Γ_0.

Furthermore, all (a, b, c)-triangle groups are conjugate to each other in $\mathrm{PSL}_2(\mathbb{R})$ *(for a fixed triple (a, b, c)).*

In order to prove this we need the following lemmas

Lemma 0.3.6. *Let Γ and Γ' be two triangle groups of the same type. Then $\overline{\Gamma}$ and $\overline{\Gamma'}$ are $PSL_2(\mathbb{R})$-conjugate.*

Proof. Let Δ and Δ' be the hyperbolic triangles (with angles α, β, γ) associated with Γ and Γ' respectively. Since these triangle groups are of the same type, the angles of the triangles are the same. It is enough to show that there is an element $g \in PSL_2(\mathbb{R})$ that sends each edge of Δ to an edge of Δ'. Since Δ and Δ' may have different orientations, such a g does not necessarily exist.

But we can assume they have the same orientation. In fact, notice that, by the definition of a triangle group, $\overline{\Gamma} = r_i\overline{\Gamma}r_i^{-1}$ for any i (where r_i are the reflections across the edges of Δ). So, by applying some r_i if necessary, we may assume that the orientation of Δ and Δ' are the same.

Now we will show that we can construct such a g. First we will define

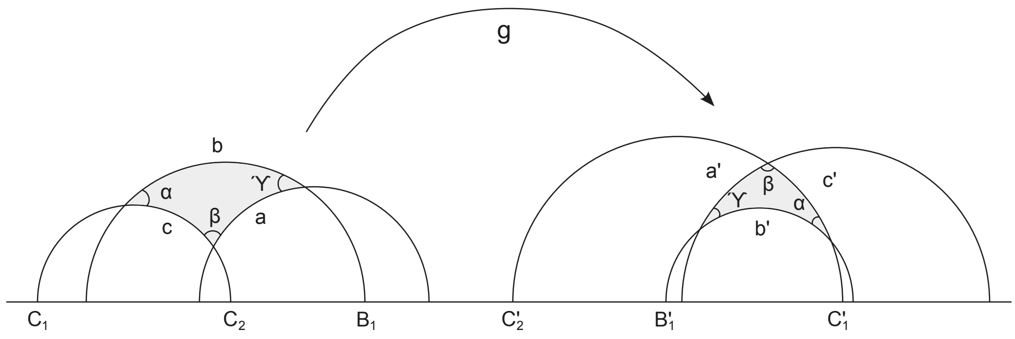

Figure 1: map g

a map h that sends $C_1 \mapsto \infty$, $B_1 \mapsto 0$ $C_2 \mapsto 1$ and a map h' that sends $C_1' \mapsto \infty$, $B_1' \mapsto 0$ $C_2' \mapsto 1$. Then we define $g := h'^{-1} \circ h$ (cf. figure 1).

The transformation h can be defined by $h(z) := \frac{z-B_1}{z-C_1} \cdot \frac{C_2-C_1}{C_2-B_1}$ and h' can be defined similarly. One can check that g is in fact in $\mathrm{PSL}_2(\mathbb{R})$.

Now we have to show that g sends a to a', b to b' and c to c'.

It obviously sends c to c'.

Now b is sent to a line starting at B_1 and intersecting c with an angle of α. Notice there are two such lines (one of them being b'). But since g preserves orientation, b must be sent to b'.

Similarly, a is sent to a'. □

The following result was shown in [Pet37].

Lemma 0.3.7. *Let $2 \leq a \leq b \leq c$ (integers or ∞) such that*

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1.$$

Then there exists an $(a, b, c)-$triangle group Γ_0 generated by

$$\gamma_{01}, \gamma_{02}, \gamma_{03}, \ \textit{and} \ -I$$

such that

$$\operatorname{tr}(\gamma_{01}) = 2\cos\left(\frac{\pi}{a}\right), \operatorname{tr}(\gamma_{02}) = 2\cos\left(\frac{\pi}{b}\right), \ \textit{and} \ \operatorname{tr}(\gamma_{03}) = 2\cos\left(\frac{\pi}{c}\right).$$

Moreover, the elements γ_{0j} satisfy the following defining relations:

$$\begin{cases} \gamma_{01}\gamma_{02}\gamma_{03}(-I) = 1 \\ \gamma_{01}^{a}(-I) = \gamma_{02}^{b}(-I) = \gamma_{03}^{c}(-I) = 1 \\ \gamma_{0j}(-I)\gamma_{0j}^{-1}(-I) = 1 \quad \textit{for all } j \\ (-I)^2 = 1 \end{cases}$$

(if $a = \infty$, the relation $\gamma_{01}^{a}(-I) = 1$ is omitted; and similarly for b and c).

We are now ready to prove Theorem 0.3.5.

Proof. (of Theorem 0.3.5)

Consider the group Γ_0 given by the previous lemma and the natural projection $\pi : SL_2(\mathbb{R}) \to PSL_2(\mathbb{R})$.

(i) Suppose a is even (the cases b even or c even are completely analogous). Let Γ be an (a,b,c)-triangle group. First we will show that $-I \in \Gamma$. Then Γ has an element γ whose image in $\mathrm{PSL}_2(\mathbb{R})$ has order a. So, $\gamma^a = \pm I$. If it is $-I$, then we are done. If we had $\gamma^a = I$, then $\gamma^{a/2} = \pm I$ and then $\operatorname{ord}\overline{\gamma} \leq a/2$, a contradiction. Hence, $\Gamma = \pi^{-1}(\pi(\Gamma))$.

By Lemma 0.3.6, $\pi(\Gamma) = \overline{g}\pi(\Gamma_0)\overline{g}^{-1}$ for some $g \in \mathrm{SL}_2(\mathbb{R})$. So,

$$\begin{aligned} \Gamma &= \pi^{-1}(\pi(\Gamma)) = \pi^{-1}(\overline{g}\pi(\Gamma_0)\overline{g}^{-1}) = \pi^{-1}(\pi(g)\pi(\Gamma_0)\pi(g^{-1})) \\ &= \pi^{-1}(\pi(g\Gamma_0 g^{-1})) = g\Gamma_0 g^{-1} \end{aligned}$$

where the last equality follows from the fact that $-I \in g\Gamma_0 g^{-1}$.

(ii) Let $\gamma_{1j} := -\gamma_{0j}$ and define $\Gamma_1 := \langle \gamma_{11}, \gamma_{12}, \gamma_{13} \rangle$. From the defining relations of the γ_{0j}'s, we obtain defining relations for the γ_{1j}'s:

$$\begin{cases} \gamma_{11}\gamma_{12}\gamma_{13} = 1 \\ \gamma_{11}^a = \gamma_{12}^b = \gamma_{13}^c = 1 \end{cases}$$

(if $a = \infty$, the relation $\gamma_{01}^a = 1$ is omitted; and similarly for b and c)

It is clear that Γ_1 is also of type (a,b,c) since $\pi(\Gamma_1) = \pi(\Gamma_1)$. Looking at the defining relations of Γ_1 and of $\pi(\Gamma_1)$ $(= \pi(\Gamma_0))$, we see that $\pi|_{\Gamma_1}$ is an isomorphism of Γ_1 onto $\pi(\Gamma_1)$. This shows that $-I \notin \Gamma_1$ and that $[\Gamma_0 : \Gamma_1] = 2$. Since $-I \notin \Gamma_1$ and $-I \in \Gamma_0$, Γ_1 and Γ_0 are not $\mathrm{SL}_2(\mathbb{R})$-conjugate.

Let Γ be any (a,b,c)-triangle group. If $-I \in \Gamma$, then Γ is $\mathrm{SL}_2(\mathbb{R})$-conjugate to Γ_0 (proof is similar to the proof in case (i)). Suppose now that $-I \notin \Gamma$. By Lemma 0.3.6 we may assume $\pi(\Gamma) = \pi(\Gamma_0)$ (in fact, the lemma says $\pi(g\Gamma g^{-1}) = \pi(\Gamma_0)$ and if Γ_0 is conjugate to $g\Gamma g^{-1}$, then it is also conjugate to Γ). Since $-I \notin \Gamma$, Γ is isomorphic to $\pi(\Gamma) = \pi(\Gamma_1)$. Hence, we can find a set $\{\gamma_1, \gamma_2, \gamma_3\}$ of generators of Γ such that $\overline{\gamma}_j = \overline{\gamma}_{1j}$. Thus, $\gamma_j = \epsilon_j \gamma_{1j}$, where $\epsilon = \pm I$. So, $\gamma_1^a = \epsilon_1^a \gamma_{11}^a = \epsilon \gamma_{11}^a = \epsilon_1$ and, since $-I \notin \Gamma$, $epsilon_1 = I$. Similarly, $\epsilon_2 = I$. Also, $\gamma_1\gamma_2\gamma_3 = \epsilon_1\epsilon_2\epsilon_3\gamma_{11}\gamma_{12}\gamma_{13} = \epsilon_1\epsilon_2\epsilon_3$ and, hence, $\epsilon_1\epsilon_2\epsilon_3 = 1$. Thus, $\epsilon_3 = I$. So, $\Gamma = \Gamma_1$.

(iii)[case $(a,b,c) = (a,\infty,\infty)$ with a odd] Let Γ_0 and Γ_1 be as in (ii). Define $\gamma_{21} := -\gamma_{01}, \gamma_{22} := \gamma_{02}, \gamma_{23} := \gamma_{03}$ and $\Gamma_2 := \langle \gamma_{21}, \gamma_{22}, \gamma_{23} \rangle$. Like in the proof of (ii), we can show that Γ_2 is isomorphic to $\pi(\Gamma_2)$ and that $-I \notin \Gamma_2$ (and, thus, Γ_2 is not $\mathrm{SL}_2(\mathbb{R})$-conjugate to Γ_0). Let us show now that Γ_2 is not $\mathrm{SL}_2(\mathbb{R})$-conjugate to Γ_1. Suppose it is. Since γ_{23} is a primitive parabolic element of Γ_2 with $\mathrm{tr}(\gamma_{23}) = 2$, Γ_1 also contains a primitive parabolic element γ with $\mathrm{tr}(\gamma) = 2$. So, $\exists \delta \in \Gamma$ such that $\overline{\gamma} = \overline{\delta}\overline{\gamma}_{12}^{\nu}\overline{\delta}^{-1}$ or $\overline{\gamma} = \overline{\delta}\overline{\gamma}_{13}^{\nu}\overline{\delta}^{-1}$, where $\nu = \pm 1$. Since $-I \notin \Gamma_1$, we obtain $\gamma = \delta\gamma_{12}^{\nu}\delta^{-1}$ or $\gamma = \delta\gamma_{13}^{\nu}\delta^{-1}$. But $\mathrm{tr}(\gamma_{12}) = \mathrm{tr}(\gamma_{13}) = -2$, a contradiction.

Now let Γ be any (a,∞,∞)-triangle group. We will show that Γ is $\mathrm{SL}_2(\mathbb{R})$-

conjugate to one of the Γ_i's. By Lemma 0.3.6 we may assume $\pi(\Gamma) = \pi(\Gamma_0)$. If $-I \in \Gamma$, then $\Gamma = \Gamma_0$. Assume now $-I \notin \Gamma$. Then Γ is isomorphic to $\pi(\Gamma)$. So $\Gamma = \langle \gamma_1, \gamma_2, \gamma_3 \rangle$, where $\overline{\gamma}_1 = \overline{\gamma}_{01}$, $\overline{\gamma}_2 = \overline{\gamma}_{02}$ and $\overline{\gamma}_3 = \overline{\gamma}_{03}$. Proceeding as in the proof of (ii) and using the fact that a is odd, we can then prove that $\Gamma = \Gamma_1$ or Γ_2.

(iv)[case $(a, b, c) = (\infty, \infty, \infty)$] We define Γ_0 as an (∞, ∞, ∞)-triangle group with respect to the hyperbolic triangle having sides 0, 1, and ∞ by giving its generators:

$$\gamma_{01} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \gamma_{02} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \qquad \gamma_{03} = \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}.$$

Now define $\Gamma_1 :=$ and $\langle -\gamma_{01}, -\gamma_{02}, -\gamma_{03} \rangle$ and $\gamma_2 := \langle -\gamma_{01}, \gamma_{02}, \gamma_{03} \rangle$. As before, we can see that Γ_1 and Γ_2 do not contain $-I$. Since γ_{02} is a primitive parabolic element of Γ_2, Γ_2 is not $\mathrm{SL}_2(\mathbb{R})$-conjugate to Γ_1.

Let Γ be any (∞, ∞, ∞)-triangle group. By Lemma 0.3.6, we may assume that $\pi(\Gamma) = \pi(\Gamma_0)$. If $-I \in \Gamma$, then $\Gamma = \Gamma_0$. Assume now that $-I \notin \Gamma$. Since $\pi(\Gamma) = \pi(\Gamma_0)$, $\Gamma = \langle \gamma_1, \gamma_2, \gamma_3 \rangle$ such that $\overline{\gamma}_j = \overline{\gamma}_{0j}$ for each $j = 1, 2, 3$. Hence, $\gamma_j = \epsilon_j \gamma_{0j}$ where $\epsilon_j = \pm I$. Using the defining relations of Γ_0 and the fact that $-I \notin \Gamma$, we obtain that

$$(\epsilon_1, \epsilon_2, \epsilon_3) = (-1, -1, -1) \text{ or } (-1, 1, 1) \text{ or } (1, -1, 1) \text{ or } (1, 1, -1).$$

From the relations

$$\begin{array}{l|l}
\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\gamma_{02}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}^{-1} = \gamma_{01}, & \begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}\gamma_{03}\begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}^{-1} = \gamma_{01}, \\
\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\gamma_{01}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}^{-1} = \gamma_{02}, & \begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}\gamma_{01}\begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}^{-1} = \gamma_{02}, \text{ and} \\
 & \begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}\gamma_{02}\begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}^{-1} = \gamma_{03}
\end{array}$$

we see that Γ is $\mathrm{SL}_2(\mathbb{R})$-conjugate to Γ_2 if $(\epsilon_1, \epsilon_2, \epsilon_3) = (1, -1, 1)$ or $(1, 1, -1)$.

□

Chapter 1

Congruence subgroups and modular curves

In the theory of classical modular forms for $\mathrm{SL}_2(\mathbb{Z})$, an important role is played by the congruence subgroups

$$\Gamma(p) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod p\},$$

$$\Gamma_1(p) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod p\}, \text{ and}$$

$$\Gamma_0(p) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod p\}$$

and their respective modular curves

$$\begin{aligned} X(p) &= \Gamma(p)\backslash\mathcal{H}^*, \\ X_1(p) &= \Gamma_1(p)\backslash\mathcal{H}^*, \text{ and} \\ X_0(p) &= \Gamma_0(p)\backslash\mathcal{H}^*. \end{aligned}$$

In this chapter, we define and study the basic properties of congruence subgroups of some triangle groups and their corresponding modular curves.

In Section 1, we will see how to define congruence subgroups of certain triangle groups and, therefore, also define their corresponding modular curves. Those groups will be denoted $\Gamma_{q,r,\infty}(\mathfrak{p})$, $\Gamma^{(1)}_{q,r,\infty}(\mathfrak{p})$ and $\Gamma^{(0)}_{q,r,\infty}(\mathfrak{p})$ in analogy to the classical case.

Section 2 will be devoted to the study of the groups $\Gamma_{q,r,\infty}(\mathfrak{p})$. First we find the genus of the modular curve associated to it. In this process we answer an interesting question: what is the quotient group $\Gamma_{q,r,\infty}/\Gamma_{q,r,\infty}(\mathfrak{p})$? In the classical case, this group is simply $\mathrm{SL}_2(\mathbb{F}_p)$. We will see this is not always the case for triangle groups.

Finally, we end this chapter with the computation of the genus of the modular curve associated to the group $\Gamma^{(0)}_{q,r,\infty}(\mathfrak{p})$ in Section 3.

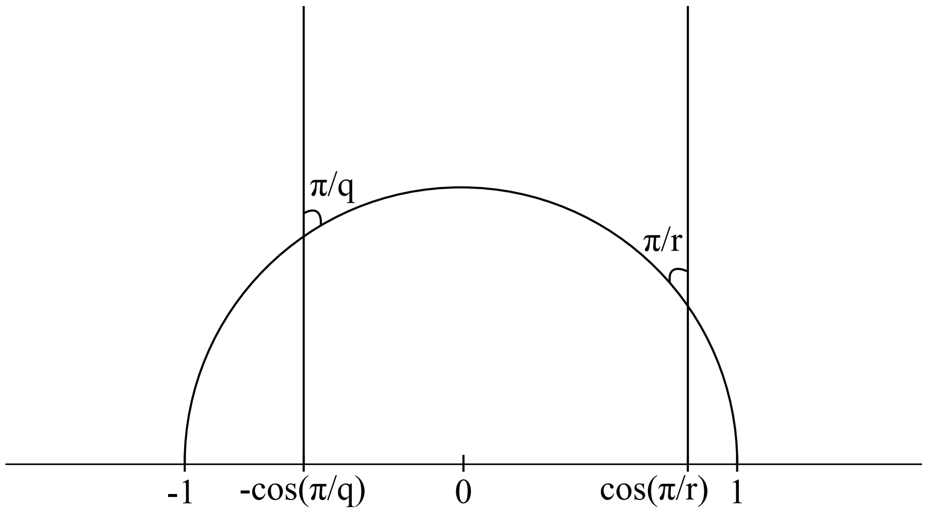

Figure 1.1: Hyperbolic triangle with angles $\pi/q, \pi/r, 0 = \pi/\infty$

1.1 Basic definitions and notations

From now on, unless otherwise stated, for a triple (q, r, ∞), which is assumed to satisfy $q \leq r \leq \infty$, the symbol $\Gamma_{q,r,\infty}$ will denote a 'standard' realization of a (q, r, ∞)-triangle group: namely, it is the triangle group constructed from the hyperbolic triangle having as sides an arc of the unit circle and vertical half-lines as shown on figure 1.1. Such a triangle group is generated as a subgroup of $\mathrm{SL}_2(\mathbb{R})$ by γ_1, γ_2, and γ_3, where

$$\gamma_1 = \begin{pmatrix} -2\cos(\pi/q) & -1 \\ 1 & 0 \end{pmatrix} \ , \ \gamma_2 = \begin{pmatrix} 0 & 1 \\ -1 & 2\cos(\pi/r) \end{pmatrix},$$

$$\gamma_3 = \begin{pmatrix} 1 & 2\cos(\pi/q) + 2\cos(\pi/r) \\ 0 & 1 \end{pmatrix}.$$

Moreover, as was explained in the previous chapter, they satisfy

$$\overline{\gamma}_1\overline{\gamma}_2\overline{\gamma}_3 = 1 \quad \text{and} \quad \overline{\gamma_1}^q = \overline{\gamma_2}^r = 1.$$

So, letting $\zeta_n = \exp(2\pi i/n)$,

$$\Gamma_{q,r,\infty} \subseteq \begin{cases} \mathrm{SL}_2(\mathbb{Z}[\zeta_{2q} + \zeta_{2q}^{-1}]), & \text{if } [q \neq \infty, r = \infty] \text{ or } [q = r \neq \infty] \\ \mathrm{SL}_2(\mathbb{Z}[\zeta_{2q} + \zeta_{2q}^{-1}, \zeta_{2r} + \zeta_{2r}^{-1}]), & \text{if } q, r \neq \infty, q \neq r \\ \mathrm{SL}_2(\mathbb{Z}), & \text{if } q, r = \infty. \end{cases}$$

Each of these rings is the ring of integers of a number field, denoted $\mathcal{O}$. In particular, $\mathbb{Z}[\zeta_{2q} + \zeta_{2q}^{-1}]$ is the ring of integers of $\mathbb{Q}(\zeta_{2q} + \zeta_{2q}^{-1})$, the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{2q})$ (cf. Prop. 2.16 in [Was82]).

This remark makes it possible to give the following definitions in analogy with the case of the modular group $\mathrm{SL}_2(\mathbb{Z})$.

Definition 1.1.1. Given a prime ideal $\mathfrak{p}$ of $\mathcal{O}$, we can define *mock congruence subgroups* of $\Gamma_{q,r,\infty}$ with level $\mathfrak{p}$ as

$$\Gamma_{q,r,\infty}(\mathfrak{p}) := \left\{ M \in \Gamma_{q,r,\infty} \;\middle|\; M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{p}} \right\},$$

$$\Gamma^{(1)}_{q,r,\infty}(\mathfrak{p}) := \left\{ M \in \Gamma_{q,r,\infty} \;\middle|\; M \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{p}} \right\}, \textit{and}$$

$$\Gamma^{(0)}_{q,r,\infty}(\mathfrak{p}) := \left\{ M \in \Gamma_{q,r,\infty} \;\middle|\; M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{\mathfrak{p}} \right\}.$$

Notice that, as in the case of $\mathrm{SL}_2(\mathbb{Z})$, the group $\Gamma_{q,r,\infty}(\mathfrak{p})$ is normal and of finite index in $\Gamma_{q,r,\infty}$.

In analogy with the classical case, we also define the *mock modular curves* associated to those groups:

$$\begin{aligned} X_{q,r,\infty} &:= \Gamma_{q,r,\infty}\backslash\mathcal{H}^*, \\ X_{q,r,\infty}(\mathfrak{p}) &:= \Gamma_{q,r,\infty}(\mathfrak{p})\backslash\mathcal{H}^*, \\ X^{(1)}_{q,r,\infty}(\mathfrak{p}) &:= \Gamma^{(1)}_{q,r,\infty}(\mathfrak{p})\backslash\mathcal{H}^*, \quad \text{and} \\ X^{(0)}_{q,r,\infty}(\mathfrak{p}) &:= \Gamma^{(0)}_{q,r,\infty}(\mathfrak{p})\backslash\mathcal{H}^*. \end{aligned} \tag{1.1}$$

We know that the genus of $X_{q,r,\infty}$ is zero. In the first section, we will find the genus of $X_{q,r,\infty}(\mathfrak{p})$ in terms of the index $[\Gamma_{q,r,\infty} : \Gamma_{q,r,\infty}(\mathfrak{p})]$ and then proceed to compute when the quotient $\Gamma_{q,r,\infty}/\Gamma_{q,r,\infty}(\mathfrak{p})$ is equal to $\mathrm{PSL}_2(\mathbb{F}_{\mathfrak{p}})$. In the second section, we compute the genus of $X^{(i)}_{q,r,\infty}(\mathfrak{p})$ for some ideals $\mathfrak{p}$.

We will focus on the case $r = \infty$ and call

$$\lambda_q = \zeta_{2q} + \zeta_{2q}^{-1} \text{ and } \mu_q = 2 + \lambda_q$$

so that

$$\gamma_1 = \begin{pmatrix} -\lambda_q & -1 \\ 1 & 0 \end{pmatrix}, \ \gamma_2 = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}, \text{ and } \gamma_3 = \begin{pmatrix} 1 & \mu_q \\ 0 & 1 \end{pmatrix}.$$

Let us start by defining the following map:

$$\rho : \Gamma_{q,\infty,\infty} \longrightarrow \mathrm{SL}_2\left(\frac{\mathbb{Z}[\lambda_q]}{\mathfrak{p}}\right) \tag{1.2}$$

which sends each matrix to the matrix with reduced entries. It is easy to see that the kernel of this map is exactly $\Gamma_{q,\infty,\infty}(\mathfrak{p})$. In particular, the group $\Gamma_{q,\infty,\infty}(\mathfrak{p})$ is normal in $\Gamma_{q,\infty,\infty}$.

1.2 Computing the genus of $X_{q,\infty,\infty}(\mathfrak{p})$

The genus of the curves associated to the Hecke triangle groups (that is, $\Gamma_{2,r,\infty}(\mathfrak{p})$) were computed in [LLT00]. In this section we deal in a similar way with the triangle groups $\Gamma_{q,\infty,\infty}$.

The next proposition shows that if we know $\overline{\mu} = \left[\overline{\Gamma_{q,\infty,\infty}} : \overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})}\right]$, then we can compute the genus of $X_{q,\infty,\infty}(\mathfrak{p})$ (for some ideals $\mathfrak{p}$), where $\overline{\Gamma_{q,\infty,\infty}}$ and $\overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})}$ are the images of $\Gamma_{q,\infty,\infty}$ and $\Gamma_{q,\infty,\infty}(\mathfrak{p})$ respectively in $\mathrm{PSL}_2(\mathbb{Z}[\lambda_q])$.

Proposition 1.2.1. *Suppose q is an odd prime number and $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[\lambda_q]$ lying above $p\mathbb{Z}$. Suppose also that $p \neq q$. Then the genus of $X_{q,\infty,\infty}(\mathfrak{p})$ is*

$$1 + \frac{\overline{\mu}}{2}\left(1 - \frac{2}{p} - \frac{1}{q}\right)$$

Proof. To simplify notation, let us call $\Gamma = \Gamma_{q,\infty,\infty}$.

Let $\varphi : \Gamma(\mathfrak{p})\backslash\mathcal{H}^* \longrightarrow \Gamma\backslash\mathcal{H}^*$ be the natural map. We know this map is holomorphic and has degree $\overline{\mu}$ (exercise 0.2.24). So we can use Riemann-Hurwitz formula to compute the genus g of $\Gamma(\mathfrak{p})\backslash\mathcal{H}^*$:

$$\begin{aligned} 2g - 2 &= \overline{\mu}(2 \cdot 0 - 2) + \sum_{P \in \Gamma(J)\backslash\mathcal{H}^*} (e_P - 1) \\ &= -2\overline{\mu} + \sum_{P \in \Gamma(J)\backslash\mathcal{H}^*} (e_P - 1) \end{aligned}$$

where e_P is the ramification index of φ at P.

By Proposition 0.2.25, we see that the only points P which may have $e_P > 1$ are the points which are mapped to cusps or elliptic points.

By looking at a fundamental region of Γ (figure 1.2) we see that this group has:

(i) 2 Γ-inequivalent cusps: 1 and ∞

(ii) 1 Γ-inequivalent elliptic point: $z_0 = e^{i(\pi - \frac{\pi}{q})}$.

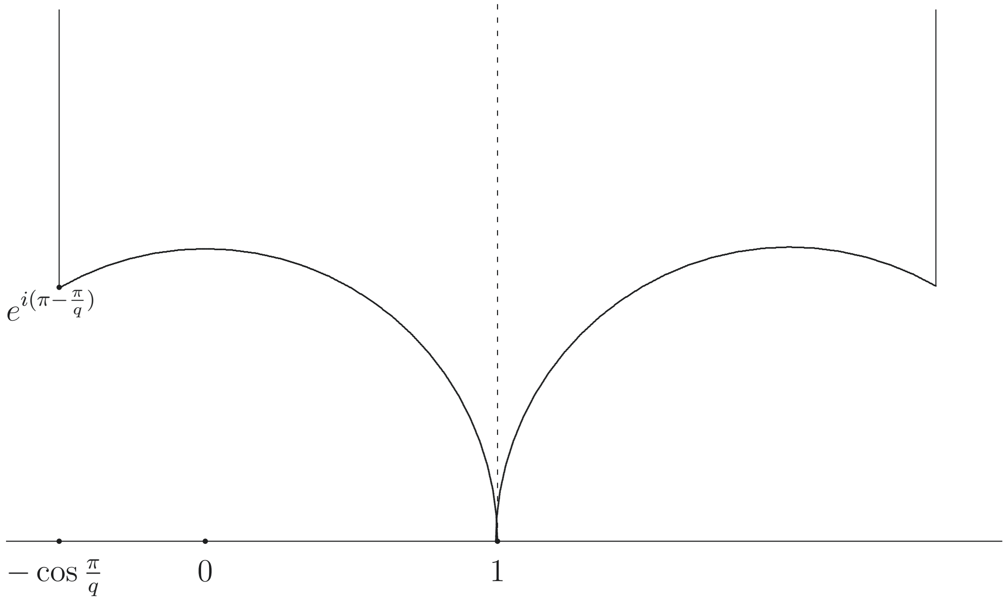

Figure 1.2: A fundamental region for $\Gamma_{q,\infty,\infty}$

Moreover, Remark 0.3.3 implies that $\overline{\Gamma}_1 = \langle\overline{\gamma_2}\rangle$, $\overline{\Gamma}_\infty = \langle\overline{\gamma_3}\rangle$ and $\overline{\Gamma}_{z_0} = \langle\overline{\gamma_1}\rangle$. In particular, $|\overline{\Gamma_{z_0}}| = q$.

Consider $\{w_1, \ldots, w_{k^{(1)}}\} = \varphi^{-1}(1)$ and let $e_1^{(1)}, \ldots, e_{k^{(1)}}^{(1)}$ be their respective ramifications indices. Since $\Gamma(\mathfrak{p}) \trianglelefteq \Gamma$, Proposition 0.2.25 says that $e_1^{(1)} = \cdots = e_k^{(1)} = \left[\overline{\Gamma_1} : \overline{\Gamma(\mathfrak{p})_1}\right]$ and $k^{(1)} e_1^{(1)} = \overline{\mu}$.

$\overline{\Gamma}_1 = \langle\overline{\gamma_2}\rangle$ and $\overline{\Gamma(\mathfrak{p})}_1 = \overline{\Gamma}_1 \cap \overline{\Gamma(\mathfrak{p})}$. Since $\gamma_2^n = \begin{pmatrix} -n+1 & n \\ -n & n+1 \end{pmatrix}$ and

$\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then $\overline{\Gamma(\mathfrak{p})}_1 = \langle \gamma_2^p \rangle$. So,

$$e_1^{(1)} = \cdots = e_k^{(1)} = p \quad \text{and} \quad k^{(1)} = \frac{\overline{\mu}}{p} \tag{1.3}$$

Let us now compute the ramification indices of $\varphi^{-1}(\infty)$. For this we need a claim (recall that $\mu_q = -2 - \zeta_{2q} - \zeta_{2q}^{-1}$):

Claim. $\mathrm{N}_{\mathbb{Q}(\zeta_{2q})/\mathbb{Q}}(\mu_q) = q^2$.

In fact, notice that $\mu_q = -(1 + \zeta_{2q})(1 + \zeta_{2q}^{-1})$. Since q is odd, $-\zeta_{2q}$ is a primitive q-th root of unity. So, the minimal polynomial of ζ_{2q} is $\phi_q(-x)$, where ϕ_q is the q-th cyclotomic polynomial. So, the minimal polynomial of $1+\zeta_{2q}$ is $h(x) = \phi_q(-(x-1)) = \phi_q(-x+1) = (-x+1)^{q-1} + \cdots + (-x+1) + 1$. Thus, the constant term of h is q. Hence, $\mathrm{N}_{\mathbb{Q}(\zeta_{2q})/\mathbb{Q}}(1 + \zeta_{2q}) = q$. Similarly, $\mathrm{N}_{\mathbb{Q}(\zeta_{2q})/\mathbb{Q}}(1 + \zeta_{2q}^{-1}) = q$. So, $\mathrm{N}_{\mathbb{Q}(\zeta_{2q})/\mathbb{Q}}(\mu_q) = (-1)^{q-1} \cdot \mathrm{N}_{\mathbb{Q}(\zeta_{2q})/\mathbb{Q}}(1 + \zeta_{2q}) \cdot \mathrm{N}_{\mathbb{Q}(\zeta_{2q})/\mathbb{Q}}(1 + \zeta_{2q}^{-1}) = q^2$.

Hence, there exists $f(x) \in \mathbb{Z}[x]$ such that $\mu_q f(\mu_q) = q^2$ ($f(\mu_q)$ is the product of all the Galois conjugates of μ_q except for μ_q itself). Since $p \neq q$, this implies $\mu_q \notin \mathfrak{p}$ (in fact, if $\mu_q \in \mathfrak{p}$, then $q^2 = \mu_q f(\mu_q) \in \mathfrak{p}$, which is impossible because $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$).

Now, since $\gamma_3^n = \begin{pmatrix} 1 & n\mu_q \\ 0 & 1 \end{pmatrix}$ and $\overline{\Gamma}_\infty = \langle \overline{\gamma_3} \rangle$, we see that $\overline{\Gamma(\mathfrak{p})}_\infty = \langle \overline{\gamma_3}^p \rangle$. And, hence, $\left[\overline{\Gamma}_\infty : \overline{\Gamma(\mathfrak{p})}_\infty \right] = p$.

Therefore, if $\{v_1, \ldots, v_{k^{(\infty)}}\} = \varphi^{-1}(\infty)$ and $e_1^{(\infty)}, \ldots, e_{k^{(\infty)}}^{(\infty)}$ are their respective ramification indices, by Proposition 0.2.25, we get

$$e_1^{(\infty)} = \cdots = e_{k^{(\infty)}}^{(\infty)} = p \quad \text{and} \quad k^{(\infty)} = \frac{\overline{\mu}}{p} \tag{1.4}$$

Now we shall compute the ramification indices of $\varphi^{-1}(z_0)$. We need to compute $\overline{\Gamma(\mathfrak{p})}_{z_0}$. Since $\overline{\Gamma(\mathfrak{p})}_{z_0} = \overline{\Gamma}_{z_0} \cap \overline{\Gamma(\mathfrak{p})}$ and $\overline{\Gamma}_{z_0}$ has only elliptic elements (in addition to the identity), the next claim tells us that $|\overline{\Gamma(\mathfrak{p})}_{z_0}| = 1$. Therefore, $\left[\overline{\Gamma}_{z_0} : \overline{\Gamma(\mathfrak{p})}_{z_0} \right] = q$.

Claim. $\Gamma(\mathfrak{p})$ has no elliptic element.

Since z_0 is the only inequivalent elliptic point and $\Gamma_{z_0} = \langle \overline{\gamma_1} \rangle$, we see that any elliptic element of Γ is conjugate to some (non-trivial) power of γ_1. Since $\Gamma(\mathfrak{p}) \trianglelefteq \Gamma$, if $\Gamma(\mathfrak{p})$ contains an elliptic element, it would also contain some (non-trivial) power of γ_1. But since $\operatorname{ord}(\overline{\gamma}) = q$ is a prime, $\Gamma(\mathfrak{p})$ would contain γ_1. But $\gamma_1 = \begin{pmatrix} * & * \\ * & 0 \end{pmatrix}$ and, hence, $\gamma_1 \notin \Gamma(\mathfrak{p})$ $(1 \not\equiv 0 \pmod{\mathfrak{p}})$.

Hence, if $\varphi^{-1}(z_0) = \{y_1, \ldots, y_{k^{(z_0)}}\}$ and $e_1^{(z_0)}, \ldots, e_{k^{(z_0)}}^{(z_0)}$ are their respective indices, Proposition 0.2.25 tells us that

$$e_0^{(z_0)} = \cdots = e_{k^{(z_0)}}^{(z_0)} = q \quad \text{and} \quad k^{(z_0)} = \frac{\overline{\mu}}{q} \tag{1.5}$$

Using the Riemann-Hurwitz formula with the information given by (1.3), (1.4) and (1.5) we get:

$$\begin{aligned} 2g - 2 &= -2\overline{\mu} + \tfrac{\overline{\mu}}{p}(p-1) + \tfrac{\overline{\mu}}{p}(p-1) + \tfrac{\overline{\mu}}{q}(q-1) \\ &= \overline{\mu}\left(-2 + 2 - \tfrac{2}{p} + 1 - \tfrac{1}{q}\right) \\ &= \overline{\mu}\left(1 - \tfrac{2}{p} - \tfrac{1}{q}\right). \end{aligned}$$

Hence,

$$g = 1 + \frac{\overline{\mu}}{2}\left(1 - \frac{2}{p} - \frac{1}{q}\right).$$

□

1.2.1 Special linear groups over finite fields

In this section we will use the facts below. Their proofs can either be found in the given reference or be easily deduced by the reader.

Fact 1. *For any prime p, we have $|\operatorname{SL}_2(\mathbb{F}_{p^m})| = (p^m+1)p^m(p^m-1)$.*

Fact 2. *A presentation for $\operatorname{SL}_2(\mathbb{F}_5)$ is given by*

$$\operatorname{SL}_2(\mathbb{F}_5) = \langle x, y \mid x^5 = y^3 = (xy)^4 = 1 \rangle.$$

(cf. Example 4, Section 6, Chapter 2 in [Suz82])

Fact 3. *Let $\langle X \mid R \rangle$ be a presentation of a group G. If R' is another set of relations, then the group $H = \langle X \mid R \cup R' \rangle$ is a homomorphic image of G. (cf. Result 6.7, Chapter 2 in [Suz82])*

We state a theorem due to Dickson (Theorem 6.17, Chapter 3 in [Suz82]).

Theorem 1.2.2. *Let F be an algebraically closed field of characteristic $p \geq 2$ and G be a finite subgroup of $\operatorname{SL}_2(F)$ such that $|G|$ is divisible by p and G admits at least two Sylow p-subgroups of order p^r. Then G is isomorphic to one of the following groups:*

(i) $p = 2$ *and G is dihedral of order $2n$ where n is odd*

(ii) $p = 3$ *and* $G \cong \operatorname{SL}_2(\mathbb{F}_5)$

(iii) $\operatorname{SL}_2(K)$

(iv) $\left\langle \operatorname{SL}_2(K), d_\pi = \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} \right\rangle$

where K is a field of p^r elements and π is an element such that $K(\pi)$ is a field of p^{2r} elements and π^2 is a generator of $K^\times$.

This allows us to prove the following:

Corollary 1.2.3. *Let $p \geq 3$ be a prime number and $E = \mathbb{F}_p(z)$ be the field with p^m elements, where $z \neq 0$. Let G be the subgroup of $\mathrm{SL}_2(E)$ generated by*

$$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$$

Then,

(i) $G \cong \mathrm{SL}_2(\mathbb{F}_5)$ if $p = 3$ and $z^2 = 2$

(ii) $G \cong \mathrm{SL}_2(E)$ otherwise.

Proof. Denote by v and u_z the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$$

respectively. Note that $\mathrm{ord}(v) = \mathrm{ord}(u_z) = p$. We shall prove that v and u_z belong to two distinct Sylow p-subgroups.

Claim. Let $U = \{u_a : a \in \mathbb{F}_q\} \subseteq \mathrm{SL}_2(E)$ where $q = p^m$ and $u_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Then $U \cap G$ is a p-Sylow of G. More generally, $U \cap G$ is the only p-Sylow of G that contains u_z.

Let P be a p-Sylow of $\mathrm{SL}_2(E)$ containing u_z. We will prove $P = U$. The claim would then follow by one of the Sylow theorems (namely the one which says that any p-subgroup is contained in a p-Sylow). In fact, by one of the Sylow theorems, $P = \alpha U \alpha^{-1}$ for some $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$ (because U is a p-Sylow of $\mathrm{SL}_2(\mathbb{F}_q)$). So, there exists $z' \in \mathbb{F}_q \backslash \{0\}$ such that $u_z = \alpha u_{z'} \alpha^{-1} = \begin{pmatrix} 1 - acz' & a^2 z \\ -c^2 z & 1 + acz \end{pmatrix}$. Hence, $c = 0$. Thus, $P = U$.

Hence, v and u_z belong to two distinct p-Sylows of G. Therefore, we can use 1.2.2.

Since we are assuming $p > 2$, there are only 3 possibilities for G: $\mathrm{SL}_2(\mathbb{F}_5)$ (this can only happen when $p = 3$), $\mathrm{SL}_2(\mathbb{F}_{p^r})$ or $\langle \mathrm{SL}_2(\mathbb{F}_{p^r}), d_\pi \rangle$, where p^r is the order a p-Sylow of G.

Claim. $G \ncong \langle \mathrm{SL}_2(\mathbb{F}_{p^r}), d_\pi \rangle$.

Let $H = \langle \mathrm{SL}_2(\mathbb{F}_{p^r}), d_\pi \rangle$. If $G \cong H$, then their respective abelianizations are also isomorphic: $G^{\mathrm{ab}} \cong H^{\mathrm{ab}}$. Since $G = \langle v, u_z \rangle$ and $\mathrm{ord}(v) = \mathrm{ord}(u_z) = p$, every element of G^{ab} has order p. We claim that $\overline{d_\pi}$ (the image of d_π in H^{ab}) can't have order p.

In fact, $\mathrm{ord}(d_\pi) = \mathrm{ord}(\pi)$. We know that $\mathrm{ord}(\pi^2) = p^r - 1$. On the other hand,

$$\mathrm{ord}(\pi) = \begin{cases} \mathrm{ord}(\pi^2) & , \quad \text{if } \mathrm{ord}(\pi) \text{ is odd} \\ 2\,\mathrm{ord}(\pi^2) & , \quad \text{if } \mathrm{ord}(\pi) \text{ is even} \end{cases}$$

So, $\mathrm{ord}(\pi) = (p^r - 1)$ or $2(p^r - 1)$.

Since $\mathrm{ord}(\overline{d_\pi}) \mid \mathrm{ord}(d_\pi)$ and $p \nmid 2(p^r - 1)$, $\mathrm{ord}(\overline{d_\pi}) \neq p$.

It remains to show that if $p = 3$, then $G \cong \mathrm{SL}_2(\mathbb{F}_5)$ if and only if $z^2 = 2$.

Claim. If $p = 3$ and $G \cong \mathrm{SL}_2(\mathbb{F}_5)$, then $z^2 = 2$.

By the corollaries of Theorem 9.8, Chapter 1 in [Suz82], we have $Z(G) = \{\pm I\}$ and, thus, $|Z(G)| = 2$. So, by the corollary of Theorem 9.9, Chapter 1 in [Suz82], $\frac{G}{Z(G)}$ is a simple group of order 60. Therefore, by Exercise 9, Section 3, Chapter 3 in [Suz82], $\frac{G}{Z(G)} \cong A_5$.

Let $\overline{v}$ and $\overline{u_z^{-1}}$ be the images of v and u_z^{-1} respectively in A_5. Since v

and u_z^{-1} are clearly not in $Z(G)$ and their order is 3, we get that $\operatorname{ord}(\overline{v}) = \operatorname{ord}(\overline{u_z^{-1}}) = 3$. So, $\overline{v} = (abc)$ and $\overline{u_z^{-1}} = (def)$. Obviously we need to have $\{a, b, c, d, e, f\} = \{1, 2, 3, 4, 5\}$. Without loss of generality, $\overline{v} = (123)$ and $\overline{u_z^{-1}} = (145)$. So, $\overline{v}\overline{u_z^{-1}} = (12345)$. So, $(vu_z^{-1})^5 = \pm I$. Thus, $\operatorname{ord}(vu_z^{-1}) = 5$ or 10. Hence, looking at the Jordan canonical form of vu_z^{-1}, we get

$$z + 2 = \operatorname{tr}(vu_z^{-1}) = \pm(x + x^{-1})$$

for some x primitive fifth root of unity over $\mathbb{F}_3$.

Since $x^4 + x^3 + x^2 + x + 1 = 0$,

$$(z + 2)^2 = \mp(z + 2) + 1 \quad \text{, i.e.,} \quad z^2 = z + 1 \text{ or } z^2 = 2$$

If $z^2 = z + 1$, then $G = \langle v, u_z \rangle$ has 720 elements[1]. Hence, $z^2 = 2$.

Claim. If $z^2 = 2$, then $G \cong \mathrm{SL}_2(\mathbb{F}_5)$.

We also have[1] that $|G| = 120$. So, $|G| = |\mathrm{SL}_2(\mathbb{F}_5)|$ (by fact 1). Let $h = (vu_z)^2 = \begin{pmatrix} 2 & 2+2z \\ z+1 & 2+2z \end{pmatrix}$. Notice $h^5 = u^3 = (hu)^4 = 1$. Moreover, $\alpha = h^{-1}uh$. Hence, $G = \langle h, u \rangle$. Then, since $G = |\mathrm{SL}_2(\mathbb{F}_5)|$, by facts 2 and 3 we obtain $G \cong \mathrm{SL}_2(\mathbb{F}_5)$. □

[1] Verified using the computer algebra system Sage [S$^+$12].

1.2.2 A bit of algebraic number theory

Our goal in this section is to state some basic facts from algebraic number theory and give an explicit formula for $f(\mathfrak{B}^+|p)$ that will be used later. Unless otherwise mentioned, the facts and definitions in this section can be found in most algebraic number theory textbooks like [Mar77] and [FT93].

Let us start fixing our notation:

- $e(- \mid -)$:= ramification index of one prime above another one,
- $f(- \mid -)$:= inertia degree of one prime above another one,
- $r(- \mid -)$:= number of distinct primes above a given one at the base field.

Moreover, in this section, we assume that

- q is an odd number and p is a prime number,
- $L_q := \mathbb{Q}(\zeta_q)$ is the q-th cyclotomic field and $L_q^+ := \mathbb{Q}(\zeta_q + \zeta_q^{-1})$,
- $\mathfrak{B}^+$ is a prime in $\mathcal{O}_{L_q^+}$ above p and $\mathfrak{B}$ is a prime in $\mathcal{O}_{L_q}$ above $\mathfrak{B}^+$,
- r is the number of primes in $\mathcal{O}_{L_q}$ above p and r^+ is the number of primes in $\mathcal{O}_{L_q^+}$ above p,
- $D(\mathfrak{B}) = D(\mathfrak{B}|\mathbb{Q}) = \{\sigma \in \mathrm{Gal}(L_q|\mathbb{Q}) : \sigma\mathfrak{B} = \mathfrak{B}\}$ is the decomposition

group of $\mathfrak{B}$ over $\mathbb{Q}$ and K^D is the respective decomposition field (i.e., the subfield of L_q that is fixed by $D(\mathfrak{B})$).

Remark 1.2.4. Notice $L_q|\mathbb{Q}$ is a Galois extension and L_q^+ is the field fixed by $H := \{1, -1\}$ (where -1 is the complex conjugation). In particular, $[L_q : L_q^+] = 2$.

Fact 4. *$r(L_q|\mathfrak{B}^+)$ = number of elements in the H-orbit of $\mathfrak{B}$.*

Fact 5. *If $p \nmid q$, then*

(i) $e(\mathfrak{B}|p) = 1$ *(hence,* $e(\mathfrak{B}^+|p) = e(\mathfrak{B}|\mathfrak{B}^+) = 1$*)*

(ii) $f(\mathfrak{B}|p) = f$*, where* f *is the order of* $\overline{p}$ *in* $\left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)^*$

(iii) $r = \frac{\varphi(q)}{f}$

Fact 6. *Let R be a Dedekind domain, K its field of fractions, L a finite Galois extension of K, $\mathcal{O}_L$ the ring of integers of L and $G = \mathrm{Gal}(L|K)$. Let $\mathfrak{p}$ be a prime ideal in R and $\mathfrak{B}_1, \dots, \mathfrak{B}_s$ the distinct prime ideals in $\mathcal{O}_L$ above $\mathfrak{p}$. Then*

(i) $e(\mathfrak{B}_1|\mathfrak{p}) = \cdots = e(\mathfrak{B}_s|\mathfrak{p})$ *and* $f(\mathfrak{B}_1|\mathfrak{p}) = \cdots = f(\mathfrak{B}_s|\mathfrak{p})$

(ii) $e(\mathfrak{B}_j|\mathfrak{p}) \cdot f(\mathfrak{B}_j|\mathfrak{p}) \cdot s = [L : K]$ *(for every* $j = 1, \ldots, s$*)*

Fact 7. $[\mathrm{Gal}(L_q|\mathbb{Q}) : D(\mathfrak{B})] = r$

Fact 8. *The map* $\mathrm{Gal}(L_q|\mathbb{Q}) \to \mathrm{Gal}\left(\frac{\mathcal{O}_{L_q}}{\mathfrak{B}} \big| \frac{\mathbb{Z}}{p}\right)$ *defined by* $\sigma \mapsto \overline{\sigma}$ *is surjective.*

Fact 9. *If* l *is a prime and* α *is a positive integer, then* $\left(\frac{\mathbb{Z}}{l^\alpha \mathbb{Z}}\right)^*$ *is a cyclic group of order* $\varphi(l^\alpha) = l^{\alpha-1}(l-1)$*.*

Fact 10. *(*Theorem 2.13 in [Was82]*) If* $(p, q) = 1$*, then* $f(\mathfrak{B}|p)$ *is the smallest positive integer* f *such that* $p^f \equiv 1 \pmod{q}$*.*

Proposition 1.2.5. *Suppose* $(p, q) = 1$*. Then,*

$$f(\mathfrak{B}^+|p) = \begin{cases} f(\mathfrak{B}|p) & , \quad \text{if } -1 \notin D(\mathfrak{B}) \\ \frac{f(\mathfrak{B}|p)}{2} & , \quad \text{if } -1 \in D(\mathfrak{B}) \end{cases}$$

Proof. Since the inertia degree is multiplicative, we get that $f(\mathfrak{B}^+|p) = f(\mathfrak{B}|p)$ if and only if f$(\mathfrak{B}|\mathfrak{B}^+) = 1$. By fact 6 and 5, we have $f(\mathfrak{B}|\mathfrak{B}^+) \cdot r(L_q|\mathfrak{B}^+) = 2$. So, it is enough to show that $r(L_q|\mathfrak{B}^+) = 1$ if and only if $-1 \in D(\mathfrak{B})$. But this follows easily from fact 4. □

Proposition 1.2.6. $D(\mathfrak{B}) \cong \frac{\mathbb{Z}}{f\mathbb{Z}}$

Proof. We want to use fact 8 to show this.

Let us start by noting that $|D(\mathfrak{B})| = f$. In fact, by facts 7 and 5, we have that $\frac{|Gal(L_q|\mathbb{Q})|}{|D(\mathfrak{B})|} = r = \frac{\varphi(q)}{f}$. Since $|\operatorname{Gal}(L_q|\mathbb{Q})| = \varphi(q)$, we obtain what we claimed.

Notice now that, by definition of inertia degree, $\frac{\mathcal{O}_{L_q}}{\mathfrak{B}} = \mathbb{F}_{p^f}$.

Hence, since $\operatorname{Gal}(\mathbb{F}_{p^f} \mid \mathbb{F}_p) = \frac{\mathbb{Z}}{f\mathbb{Z}}$, we obtain what we wanted. □

Let us now prove a particular case of our main goal.

Lemma 1.2.7. *If $q = l^\alpha$ is a prime power, then $-1 \in D(\mathfrak{B})$ if and only if f is even.*

Proof. Suppose f is odd. Since -1 is an element of order 2, Proposition 1.2.6 tells us that $-1 \notin D(\mathfrak{B})$.

Now suppose f is even. So, Sylow's Theorem and Proposition 1.2.6 says that $D(\mathfrak{B})$ has at least one element of order 2. But since $\operatorname{Gal}(L_q|\mathbb{Q}) = \left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)^\times$ is cyclic (fact 9), it has only one element or oder 2, namely -1. □

Proposition 1.2.8. *If $(p, q) = 1$ then $f(\mathfrak{B}^+|p)$ is the smallest positive integer f^+ such that $p^{f^+} \equiv \pm 1 \pmod{q}$.*

Proof. By Proposition 1.2.5 and the previous lemma, we have that

$$f(\mathfrak{B}^+|p) = \begin{cases} f(\mathfrak{B}|p) & , \quad \text{if } f(\mathfrak{B}|p) \text{ is odd} \\ \frac{f(\mathfrak{B}|p)}{2} & , \quad \text{if } f(\mathfrak{B}|p) \text{ is even.} \end{cases}$$

The result now follows from fact 10. □

We are finally ready to tackle the general case:

Proposition 1.2.9. *If p is any prime number, than $f(\mathfrak{B}^+|p)$ is the smallest positive integer f^+ such that $p^{f^+} \equiv \pm 1 \pmod{q'}$, where $2q = p^a q'$ and $(p, q') = 1$.*

Proof. This follows from the previous proposition and the fact that p is totally ramified in L_p (Lemma 1.4 in [Was82]). □

1.2.3 Computing $\left[\overline{\Gamma_{q,\infty,\infty}} : \overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})}\right]$

Let ρ be the map defined in (1.2). We define

$$\begin{array}{rcccl} \overline{\rho} & : & \overline{\Gamma_{q,\infty,\infty}} & \longrightarrow & \mathrm{PSL}_2(E) \\ & & \overline{g} & \longmapsto & \overline{\rho(g)} \end{array}$$

where $E = \frac{\mathbb{Z}[\lambda_q]}{\mathfrak{p}}$ and $^-$denotes the image in PSL_2. This map is well-defined because $\rho(-g) = -\rho(g)$.

Therefore, we have a commutative diagram

$$\begin{tikzcd}
\Gamma_{q,\infty,\infty} \arrow[r, "\rho"] \arrow[d, two heads] & \mathrm{SL}_2(E) \arrow[d, two heads] \\
\overline{\Gamma_{q,\infty,\infty}} \arrow[r, "\overline{\rho}"'] & \mathrm{PSL}_2(E)
\end{tikzcd}$$

Lemma 1.2.10. $\ker(\overline{\rho}) = \overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})}$.

Proof. Since $\ker(\rho) = \Gamma_{q,\infty,\infty}(\mathfrak{p})$, it is clear that $\overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})} \subseteq \ker(\overline{\rho})$.

Now, take $\overline{g} \in \ker(\overline{\rho})$, i.e., $\rho(g) = \pm I$ (I is the identity matrix). Since $\rho(-g) = -\rho(g)$, we get $\pm g \in \ker(\rho) = \Gamma_{q,\infty,\infty}(\mathfrak{p})$. So, $g \in \pm\Gamma_{q,\infty,\infty}(\mathfrak{p})$. Hence, $\overline{g} \in \overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})}$. □

This shows that $\overline{\Gamma_{q,\infty,\infty}} \,/\, \overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})} \;\cong\; \mathrm{img}(\overline{\rho})$.

Fact 11. *The center $Z(\mathrm{SL}_2(F))$ of $\mathrm{SL}_2(F)$ (where F is any field) is equal to $\{\pm I\}$. (cf. Corollary 2 of Result 9.8, Chapter 1 in [Suz82])*

Fact 12. *If $\mathfrak{a} \subseteq \mathbb{Z}[\lambda_q]$ is a non-zero ideal, then $\frac{\mathbb{Z}[\lambda_q]}{\mathfrak{a}}$ is finite.*

Fact 13. *If n is odd, then $Z(D_{2n}) = \{e\}$. (easy exercise)*

Lemma 1.2.11. *If $\mathfrak{p}$ is a prime ideal lying above $2\mathbb{Z}$ and q is odd, then $\mathrm{img}(\overline{\rho}) \cong D_{2s}$ (for some odd s dividing q). Moreover, if q is a prime, then $s = q$.*

Proof. Notice $\mathrm{img}(\overline{\rho}) = \overline{\mathrm{img}(\rho)}$.

If $p = 2$, one can easily check that $\mathrm{ord}(\rho(\gamma_2)) = \mathrm{ord}(\rho(\gamma_3)) = 2$. Hence, by the first claim in the proof of corollary 1.2.3, $\rho(\Gamma_{q,\infty,\infty})$ has 2 distinct 2-Sylow subgroups. Hence, $\rho(\Gamma_{q,\infty,\infty})$ is one of the groups listed in Theorem 1.2.2.

One can check that $\rho(\gamma_1)\rho(\gamma_3) = \rho(\gamma_3)\rho(\gamma_1)^{-1}$ and $\rho(\gamma_3)^2 = \rho(\gamma_1)^q = I$. Hence, since $\rho(\Gamma_{q,\infty,\infty}) = \langle \rho(\gamma_1), \rho(\gamma_3) \rangle$, fact 3 tells us that $\rho(\Gamma_{q,\infty,\infty})$ is a homomorphic image of D_{2q}. In particular, $|\rho(\Gamma_{q,\infty,\infty})| \mid 2q$. Since q is odd, by Theorem 1.2.2, $\rho(\Gamma_{q,\infty,\infty})$ can only be D_{2n} (for some odd n) or $\mathrm{SL}_2(2)$. But, one can check that $\mathrm{SL}_2(2) = D_{2\cdot 3}$. So, in any case, $\rho(\Gamma_{q,\infty,\infty}) \cong D_{2s}$ (for some odd s).

Now, since $\mathrm{char}(E) = 2$, $I = -I$ in $\mathrm{SL}_2(E)$. Hence, $\mathrm{PSL}_2(E) = \mathrm{SL}_2(E)$. Thus, $\overline{\mathrm{img}(\rho)} \cong \mathrm{img}(\rho) \cong D_{2s}$. So, $2s \mid 2q$. Therefore, since q is odd, $s \mid q$.

Finally, since $\gamma_1 = \begin{pmatrix} -\lambda_q & -1 \\ 1 & 0 \end{pmatrix}$, $\rho(\gamma_1) \neq I$ (because $0 \not\equiv 1 \pmod{\mathfrak{p}}$). So, if q is prime, $\mathrm{ord}(\rho(\gamma_1)) = q$ (because $\mathrm{ord}(\rho(\gamma_1)) \mid \mathrm{ord}(\gamma_1) = q$). □

Lemma 1.2.12. *Suppose $\mathfrak{p}$ is a prime ideal lying above $p\mathbb{Z}$ with $p \geq 3$. Then, $\mathrm{img}(\overline{\rho})$ is isomorphic to*

(i) $\mathrm{PSL}_2(\mathbb{F}_5)$, *if $p = 3$ and $\mu_q^2 - 2 \in \mathfrak{p}$*

(ii) $\mathrm{PSL}_2(E)$, *otherwise (where $E = \frac{\mathbb{Z}[\lambda_q]}{\mathfrak{p}}$)*

Proof. Notice $\operatorname{img}(\overline{\rho}) = \overline{\operatorname{img}(\rho)}$.

If $p = 3$ and $mu_q^2 - 2 \in \mathfrak{p}$, fact 12 and corollary 1.2.3 says that $\operatorname{img}(\rho) \cong \mathrm{SL}_2(\mathbb{F}_5)$. We have to prove that $\overline{\operatorname{img}(\rho)} \cong \mathrm{PSL}_2(\mathbb{F}_5)$. Notice that $\overline{\operatorname{img}(\rho)} = \frac{\operatorname{img}(\rho)}{\{\pm I\} \cap \operatorname{img}(\rho)}$.

We can verify that $-I \in \operatorname{img} \rho$. In fact, there are only two cases to consider and they were computed explicitly using Sage [S$^+$12].

So, $\overline{\operatorname{img}(\rho)} = \frac{\mathrm{SL}_2(\mathbb{F}_5)}{Z(\mathrm{SL}_2(\mathbb{F}_5))} = \mathrm{PSL}_2(\mathbb{F}_5)$.

Otherwise, fact 12 and corollary 1.2.3 says that $\operatorname{img}(\rho) = \mathrm{SL}_2(E)$, i.e., ρ is surjective. Hence, $\overline{\operatorname{img}(\rho)} = \mathrm{PSL}_2(E)$. □

Theorem 1.2.13. *Let $q \geq 3$ be an odd integer and $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\lambda_q]$ lying above $p\mathbb{Z}$ where $p \geq 2$.*

(i) If $p = 2$, then $\overline{\Gamma_{q,\infty,\infty}} \ / \ \overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})} \cong D_{2s}$ (for some odd s that divides q) and, hence, $\left[\overline{\Gamma_{q,\infty,\infty}} : \overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})}\right] = 2s$. Moreover, if q is prime, then $s = q$.

(ii) If $p = 3$ and $\mu_q^2 - 2 \in \mathfrak{p}$, then $\overline{\Gamma_{q,\infty,\infty}} \ / \ \overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})} \cong \mathrm{PSL}_2(\mathbb{F}_5)$ and, hence, $\left[\overline{\Gamma_{q,\infty,\infty}} : \overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})}\right] = 60$;

(iii) Otherwise, $\overline{\Gamma_q} \,/\, \overline{\Gamma_q(\mathfrak{p})} \cong \mathrm{PSL}_2(\mathbb{Z}[\lambda_q]/\mathfrak{p})$ *and, hence,* $\left[\overline{\Gamma_{q,\infty,\infty}} : \overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})}\right] = (p^m+1)p^m(p^m-1)/2.$

Moreover $\mathbb{Z}[\lambda_q]/\mathfrak{p} \cong \mathbb{F}_{p^m}$*, where* m *is the smallest positive integer such that* $p^m \equiv \pm 1 \pmod{q'}$ *(*$2q = p^a q'$ *with* $\gcd(p, q') = 1$*).*

Proof. The theorem follows from Lemmas 1.2.11 and 1.2.12.

The fact that $\mathbb{Z}[\lambda_q]/\mathfrak{p}$ is a field with p^m elements with m as in the statement of the theorem follows from Proposition 1.2.9. □

1.3 Computing the genus of $X^{(0)}_{q,\infty,\infty}(\mathfrak{p})$

In this section, the genus of $X^{(0)}_{q,\infty,\infty}(\mathfrak{p})$, where $\mathfrak{p}$ is a prime above p, is computed. It is assumed that $\overline{\Gamma_{q,\infty,\infty}}\big/\overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})} \cong \mathrm{PSL}_2(\mathbb{F}_{\mathfrak{p}})$ (which is always true when $q \geq 5$ according to Theorem 1.2.13) and $p \neq q$ are prime numbers strictly greater than 2.

Using the Riemann-Hurwitz formula and the natural map $\varphi : X^{(0)}_{q,\infty,\infty}(\mathfrak{p}) \to X_{q,\infty,\infty}(1) = X_{q,\infty,\infty}$, it suffices to compute the ramification indices of φ.

Recall that

$$\left(\overline{\Gamma_{q,\infty,\infty}}\right)_\infty = \left\langle \gamma_3 = \begin{pmatrix} 1 & \mu_q \\ 0 & 1 \end{pmatrix} \right\rangle,$$

$$\left(\overline{\Gamma_{q,\infty,\infty}}\right)_1 = \left\langle \gamma_2 = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \right\rangle,$$

$$\left(\overline{\Gamma_{q,\infty,\infty}}\right)_{z_0} = \left\langle \gamma_1 = \begin{pmatrix} -\lambda_q & -1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

It can be shown, with the help of Proposition 0.2.25, that the monodromy of this map over ∞ is given by the action of γ_3 on the set of cosets $\overline{\Gamma_{q,\infty,\infty}} \Big/ \overline{\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})}$. Similarly, the monodromy of this map over 1 (resp. z_0) is given by the action of γ_2 (resp. γ_1) on $\overline{\Gamma_{q,\infty,\infty}} \Big/ \overline{\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})}$.

Lemma 1.3.1. *Let $\gamma \in \Gamma_{q,\infty,\infty}$. The action of γ on $\overline{\Gamma_{q,\infty,\infty}} \Big/ \overline{\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})}$ is equivalent to the action of $(\gamma \mod \mathfrak{p}) \in \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ on $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ via fractional linear transformations, i.e., the cycle decomposition of γ (viewed as an element of the group of permutations of $\overline{\Gamma_{q,\infty,\infty}} \Big/ \overline{\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})}$ is the same as the cycle structure of $(\gamma \mod \mathfrak{p})$ (viewed as an element of the group of permutations of $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$).*

Proof. The action of $\overline{\Gamma_{q,\infty,\infty}}$ on $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ via linear fractional transformations is transitive (since $\overline{\Gamma_{q,\infty,\infty}}/\overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})} \cong \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$). Moreover, the stabilizer of $\infty \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ is $\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})$. Hence, by group theory, the action of $\overline{\Gamma_{q,\infty,\infty}}$ on $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ is equivalent to the action of $\overline{\Gamma_{q,\infty,\infty}}$ on $\overline{\Gamma_{q,\infty,\infty}} \Big/ \overline{\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})}$. □

Lemma 1.3.2. *The monodromy over* ∞ *is given by*

$$(0)(1\cdots p)(p+1,\cdots,2p)\cdots(p^{f-1}+1,\cdots,p^f),$$

where $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{p^f}$*. So,* $\varphi^{-1}(\infty) = \{w_0, w_1, \ldots, w_{p^{f-1}}\}$ *and*

$$e_{w_0} = 1 \quad \textit{and} \quad e_{w_i} = p, \textit{ for } 1 \leq i \leq p^{f-1}.$$

Proof. Notice that $(\gamma_3 \mod \mathfrak{p}) = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$, where $\beta = (\mu_q \mod \mathfrak{p}) \in \mathbb{F}_{\mathfrak{p}} \backslash \{0\}$ (the fact that $\beta \neq 0$ is part of the proof of Proposition 1.2.1).

Hence, $\infty \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ is fixed by $(\gamma_3 \mod \mathfrak{p})$. Furthermore, since

$$(\gamma_3 \mod \mathfrak{p})^n = \begin{pmatrix} 1 & n\beta \\ 0 & 1 \end{pmatrix}$$

and $\text{char}(\mathbb{F}_{\mathfrak{p}}) = p$, all other points of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ generate an orbit of size p. □

Lemma 1.3.3. *The monodromy over* 1 *has the same cycle decomposition. So,* $\varphi^{-1} = \{w_0, w_1, \ldots, w_{p^{f-1}}\}$ *and*

$$e_{w_0} = 1 \quad \textit{and} \quad e_{w_i} = p, \textit{ for } 1 \leq i \leq p^{f-1},$$

where $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{p^f}$*.*

Proof. Notice that $(\gamma_2 \mod \mathfrak{p}) = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$.

It is easily seen that the only point of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ that is fixed by $(\gamma_2 \mod \mathfrak{p})$ is the point 1.

Now, consider the natural map

$$\psi : X_{q,\infty,\infty}(\mathfrak{p}) \to X_{q,\infty,\infty}(1).$$

Since $e_{v,g} = p$ for all $w = \psi^{-1}(1)$ (this is part of the proof of Proposition 1.2.1) and ψ factors as

$$\begin{tikzcd} X_{q,\infty,\infty}(\mathfrak{p}) \arrow[r] & X^{(0)}_{q,\infty,\infty}(\mathfrak{p}) \arrow[r, "\varphi"] & X_{q,\infty,\infty}(1) \end{tikzcd} ,$$

we have that $e_{w,f} = 1$ or p for all $w \in \varphi^{-1}(1)$.

The previous calculation says that there is only one point above 1 having ramification degree 1. Hence, the result follows. □

Lemma 1.3.4. *Let $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{p^f}$ as before. The ramification behavior above z_0 is given as follows:*

$$\varphi^{-1}(z_0) = \{w_1, \dots, w_n, w'_1, \dots, w'_m\},$$

where

$$e_{w_i} = q \quad , \quad e_{w'_i} = 1 \quad , \quad p^f + 1 = qn + m \quad ,$$

$$m = \begin{cases} 0, & \textit{if } p^f \equiv -1 \pmod q \\ 2, & \textit{if } p^f \equiv 1 \pmod q, \end{cases}$$

Proof. Notice that $(\gamma_1 \mod \mathfrak{p}) = \begin{pmatrix} \beta & -1 \\ 1 & 0 \end{pmatrix}$ for some $\beta \in \mathbb{F}_{\mathfrak{p}}$.

As in the proof of the previous lemma, $e_w = 1$ or q for any $w \in \varphi^{-1}(z_0)$.

Let n denote the number of points whose ramification degree is q and let m denote those whose ramification degree is 1.

Then m is also the number of points in $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ fixed by $(\gamma_1 \mod \mathfrak{p})$. Hence $m \leq 2$.

Since $\deg(\varphi) = p^f + 1$,

$$p^f + 1 = nq + m.$$

Since q and p are distinct primes, it follows that $m \neq 1$. Taking the previous equality $\mod q$, the precise value of m (in terms of $(p^f \mod q)$) follows. □

Proposition 1.3.5. *The genus of the curve $X^{(0)}_{q,\infty,\infty}(\mathfrak{p})$ is given by*

$$g = \frac{(q-1)}{2} n - p^{f-1},$$

where n and f are as in the previous lemma.

Proof. Follows from the Riemann-Hurwitz formula applied to φ, the previous three lemmas and the fact that $g(X_{q,\infty,\infty}(1)) = 0$. □

Chapter 2

Action of $\mathrm{PSL}_2(\mathbb{F}_{\mathfrak{p}})$ on mock modular curves

In 1930 Hecke [Hec30] (cf. [Hec11] for a translation) studied the natural representation of

$$\mathrm{PSL}_2(\mathbb{F}_p) = \overline{\mathrm{SL}_2(\mathbb{Z})}\Big/\overline{\Gamma(p)}$$

on the space of holomorphic differentials of the modular curve $X(p)$ of prime level p. The interesting case arises when $p \equiv 3 \pmod 4$, i.e., when -1 is not a square modulo p.

The character table of $\mathrm{PSL}_2(\mathbb{F}_p)$ for $p \equiv 3 \pmod 4$ contains only two irreducible representations (here denoted π' and π'') that are not isomorphic to their complex conjugate. In fact, the complex conjugate of one is isomorphic to the other. Denoting m' and m'' the multiplicity of π' and π'' in $\Omega^1(X(p))$, Hecke showed that $m' - m'' = h(-p)$, where $h(-p)$ denotes the class number of the quadratic field $\mathbb{Q}(\sqrt{-p})$. In this chapter, whose main content was published in [Tak12], we study what happens when the modular group $\mathrm{SL}_2(\mathbb{Z})$ is replaced by the triangle groups $\Gamma_{q,r,\infty}$ and modular curves are replaced by mock modular curves (as defined in (1.1)).

Notation 2.0.6. α_i = image of $\overline{\gamma_i}$ in $\overline{\Gamma_{q,r,\infty}} / \overline{\Gamma_{q,r,\infty}(\mathfrak{p})}$.

Remark 2.0.7. There is a natural (Galois) covering map given by

$$\begin{tikzcd}
X_{q,r,\infty}(\mathfrak{p}) \arrow[d] \\
X_{q,r,\infty}.
\end{tikzcd}$$

The Galois group of this covering map is exactly $\overline{\Gamma_{q,r,\infty}} / \overline{\Gamma_{q,r,\infty}(\mathfrak{p})}$ and the α_i are the local monodromies around the branch points of $X_{q,r,\infty}$. The goal is, therefore, to study the representation of the Galois group on the space of holomorphic differentials.

2.1 Character table of $\mathrm{PSL}_2(\mathbb{F}_{p^{2n+1}})$ for $p \equiv 3 \pmod 4$

In order to state the main result, it is necessary to recall the character table of $\mathrm{PSL}_2(\mathbb{F}_{p^{2n+1}})$. This section will follow the ideas of paragraph 5.2 of [FH91], where the character table of $\mathrm{SL}_2(\mathbb{F}_{p^{2n+1}})$ is presented. It is then possible to obtain the character table for $\mathrm{PSL}_2(\mathbb{F}_{p^{2n+1}})$ simply by taking a subset of the representations of $\mathrm{SL}_2(\mathbb{F}_{p^{2n+1}})$. It is important to mention that the representations considered in this section are left representations.

From now on, denote $f := 2n + 1$ and $\mathbb{F} := \mathbb{F}_{p^f}$. Moreover, $E := \mathbb{F}_{(p^f)^2}$ and $E_1 := \{\varepsilon \in E \mid N_{E/\mathbb{F}}(\varepsilon) = \varepsilon\overline{\varepsilon} = 1\}$. Note that -1 is not a square in $\mathbb{F}$, since it is not a square in $\mathbb{F}_p$ and f is odd.

Looking at the eigenvalues, the following classification of the conjugacy classes of $\mathrm{PSL}_2(\mathbb{F})$ is obtained:

- Id, having $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ as a representative.

- The *split semi-simple conjugacy classes*

$$c_s(x) \quad \text{for all } x \in \mathbb{F} - \{\pm 1\} \ ,$$

  having $\left(\begin{smallmatrix} x & 0 \\ 0 & 1/x \end{smallmatrix}\right)$ as a representative. These correspond to the matrices having two distinct eigenvalues in $\mathbb{F}$: x and $1/x$. Note that $c_s(x) = c_s(-x) = c_s(1/x) = c_s(-1/x)$.

- The *non-split semi-simple conjugacy classes*

  $$c_{ns}(\varepsilon) \quad \text{for all } \varepsilon \in E_1 - \{\pm 1\} \ \cdot$$

  These correspond to the matrices having two distinct (and conjugate) eigenvalues in $E - \mathbb{F}$: ε and $\overline{\varepsilon}$. Note that $c_{ns}(\varepsilon) = c_{ns}(-\varepsilon) = c_{ns}(\overline{\varepsilon}) = c_{ns}(-\overline{\varepsilon})$.

- The *unipotent conjugacy classes*

  $$c_u(\Delta) \quad \text{for } \Delta \in \mathbb{F}^\times/(\mathbb{F}^\times)^2 \ ,$$

  having $\left(\begin{smallmatrix} 1 & \Delta \\ 0 & 1 \end{smallmatrix}\right)$ as representative. These correspond to the matrices whose characteristic polynomial has only one root: 1 or -1. (Since -1 is not a square in $\mathbb{F}$, the condition "$\Delta \in \mathbb{F}^\times/(\mathbb{F}^\times)^2$" may be replaced by "$\Delta \in \{\pm 1\}$".)

The number of classes in each family and the number of elements in each class are given in the table below:

conj. class	# of classes in the family	# of elements in the class
Id	1	1
$c_s(x)$	$(p^f-3)/4$	$p^f(p^f+1)$
$c_{ns}(\varepsilon_0)$	1	$p^f(p^f-1)/2$
$c_{ns}(\varepsilon)$	$(p^f-3)/4$	$p^f(p^f-1)$
$c_u(\Delta)$	2	$(p^{2f}-1)/2$

where ε_0 is a root of X^2+1.

Since $E_1/\{\pm 1\}$ has a unique element of order 2, it also has a unique character of order 2, here denoted φ_0.

The irreducible representations of $\mathrm{PSL}_2(\mathbb{F})$ are the following:

- the trivial representation of dimension 1;
- the Steinberg representation;
- representations ρ_α parametrized by the characters $\alpha \neq 1$ of the group $\mathbb{F}^\times/\{\pm 1\}$;
- representations π_φ parametrized by the characters $\varphi \neq 1, \varphi_0$ of the group $E_1/\{\pm 1\}$; and
- representations π' and π'', corresponding to the character φ_0.

The character table is given by:

	Id	$c_s(x)$	$c_{ns}(\varepsilon)$	$c_u(1)$	$c_u(-1)$
id	1	1	1	1	1
St	p^f	1	-1	0	0
ρ_α	p^f+1	$\alpha(x)+\alpha(1/x)$	0	1	1
π_φ	p^f-1	0	$-\varphi(\epsilon)-\varphi(1/\epsilon)$	-1	-1
π'	$(p^f-1)/2$	0	$-\varphi_0(\epsilon)$	$\overline{\mathfrak{G}}$	$\mathfrak{G}$
π''	$(p^f-1)/2$	0	$-\varphi_0(\epsilon)$	$\mathfrak{G}$	$\overline{\mathfrak{G}}$

Table 2.1: Irreducible representations of $\mathrm{PSL}_2(\mathbb{F}_{p^{2n+1}})$

where

$$\mathfrak{G} = \frac{p^n-1}{2} + p^n \sum_{\left(\frac{y}{p}\right)=1} \exp(2\pi i y/p) = \frac{p^n-1}{2} + p^n \sum_{\left(\frac{y}{p}\right)=1} \zeta_p^y$$

and $\overline{\mathfrak{G}}$ is its complex conjugate.

Note that each irreducible representation with the exception of π' and π'' can be distinguished from all the other ones: it may be the trivial representation, the Steinberg representation or a representation that comes from a character of either $\mathbb{F}^\times/\{\pm1\}$ or $E_1/\{\pm1\}$.

On the other hand, it is not so clear how to distinguish the representations π' and π''. It is possible to tell these two representations apart from all the other ones: they are the representations associated with φ_0 of $E_1/\{\pm 1\}$, they are the only irreducible representations that have non-real traces and one is the complex conjugate of the other. But the problem arises when trying to tell apart π' from π''. The main theorem, stated in the next section, gives a way to distinguish these two representations: namely π' is chosen to be the one that appears more often in the representation of $\Gamma_{q,\infty,\infty}/\,\Gamma_{q,\infty,\infty}(\mathfrak{p})$ on $\Omega^1(X_{q,\infty,\infty}(\mathfrak{p}))$ in the case where $\Gamma_{q,\infty,\infty}/\,\Gamma_{q,\infty,\infty}(\mathfrak{p}) \cong \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$.

2.2 Statement of the main result

The main result of this chapter can now be stated using the character table 2.1.

Let $\mathfrak{p}$ denote a prime of $\mathcal{O}$ above p and let

$$f := f(\mathfrak{p}/p) = 2n + 1$$

denote the inertia degree, which is assumed to be odd. Moreover, p is still assumed to satisfy $p \equiv 3 \pmod 4$.

The quotient group $\overline{\Gamma_{q,r,\infty}} / \overline{\Gamma_{q,r,\infty}(\mathfrak{p})}$ will be denoted by G and is assumed to satisfy

$$G \cong \mathrm{PSL}_2(\mathbb{F}_{\mathfrak{p}}).$$

This does not always hold but Theorem 1.2.13 from the previous chapter guarantees this holds for many cases. A more general discussion can be found in [CV].

In order to obtain a left representation, the natural representation of G on $\Omega^1(X_{q,r,\infty}(\mathfrak{p}))$ is adapted in the following way. Let $g \in G$ and $\omega \in \Omega^1(X_{q,r,\infty}(\mathfrak{p}))$. Then the action of g on ω is given by the pull-back of ω under g^{-1}:

$$g \cdot \omega := (g^{-1})^* \omega. \tag{2.1}$$

Let m' and m'' denote the multiplicity of π' and π'' in $\Omega^1(X_{q,r,\infty}(\mathfrak{p}))$.

As mentioned before, in the case $\Gamma_{2,3,\infty} = \mathrm{SL}_2(\mathbb{Z})$ studied by Hecke, $m' - m'' = h(-p)$. Note that $\Gamma_{2,3,\infty}$ has only one cusp (up to equivalence). Also, in that case, $\mathcal{O} = \mathbb{Z}$ and, thus, the inertia degree of $\mathfrak{p}$ is always $f(\mathfrak{p}/p) = 1$. So this is a special case of the following theorem, which states roughly that $m' - m'' =$ (number of cusps) × $h(-p^f)$.

Theorem 2.2.1. *Let m' and m'' denote the multiplicity of π' and π'' in the representation of G on the space of holomorphic differentials of $X_{q,r,\infty}(\mathfrak{p})$. Moreover, let $h(-p^f)$ denote the class number of the order of discriminant $-p^f$. Then*

$$m' - m'' = [\delta(\alpha_1) + \delta(\alpha_2) + \delta(\alpha_3)]h(-p^f),$$

where $\delta : \mathrm{PSL}_2(\mathbb{F}_{\mathfrak{p}}) \to \{-1, 0, 1\}$ is the function defined by

$$\delta(\gamma) = \begin{cases} 1, & \gamma \in c_u(1) \\ -1, & \gamma \in c_u(-1) \\ 0, & \textit{otherwise.} \end{cases}$$

Corollary 2.2.2. *Let m', m'' and $h(-p^f)$ be as in the previous theorem.*

(i) If $q = r = \infty$, then

$$m' - m'' = 3h(-p).$$

(ii) If $r = \infty$, q is a prime number and $q \neq p$, then

$$m' - m'' = \begin{cases} 2h(-p^f), & \mathrm{ord}(p \mod q) \textit{ is even} \\ 0, & \textit{otherwise.} \end{cases}$$

(iii) If $q, r \notin \{p, \infty\}$ are prime numbers and $(q, r) \neq (2, 2)$, then

$$m' - m'' = \pm h(-p^f).$$

Moreover, it is + if and only if $\zeta_{2q} + \zeta_{2q}^{-1} + \zeta_{2r} + \zeta_{2r}^{-1}$ *is a square modulo* $\mathfrak{p}$.

Remark 2.2.3. Under the same assumptions of (ii) or (iii) in the theorem, the inertia degree $f = f(\mathfrak{p}/p)$ can be easily computed. Since $p \notin \{q, r\}$, the prime p is unramified in $\mathcal{O}$. This implies that f is the order of the Frobenius element, which is defined by

$$\zeta_x + \zeta_x^{-1} \longmapsto \zeta_x^{p} + \zeta_x^{-p} \ , \text{ for all } x \in \{q, r\} - \{\infty\}.$$

As a consequence of this, it is not hard to see that f is the smallest positive integer such that

$$p^f \equiv \pm 1 \pmod{x} \ , \text{ for all } x \in \{q, r\} - \{\infty\}.$$

The proofs of Theorem 2.2.1 and corollary 2.2.2 are postponed until Section 2.4. The current section will proceed with the computation of some examples.

Example 1. Hecke's result can be recovered using (iii). In fact, if $q = 2$ and $r = 3$, then $\zeta_{2q} + \zeta_{2q}^{-1} = 0$ and $\zeta_{2r} + \zeta_{2r}^{-1} = 1$. Thus $\zeta_{2q} + \zeta_{2q}^{-1} + \zeta_{2r} + \zeta_{2r}^{-1} = 1$, which is always a square. Moreover, $\mathcal{O} = \mathbb{Z}$, which implies that the inertia degree f is always 1. Thus, $m' - m'' = h(-p)$.

Notice that when $q < r = \infty$ (case (ii)), the difference $m' - m''$ depends only on the prime number p chosen and not on the prime ideal $\mathfrak{p}$ above it. When $q, r \neq \infty$, this is not the case: given a prime p, the difference $m' - m''$ may depend on the specific prime ideal $\mathfrak{p}$ above it. The examples below, computed using the Magma algebra system ([BCP97]), illustrate this phenomenon.

Example 2. Let $q = 3$ and $r = 7$. Then $\mathcal{O} = \mathbb{Z}[1, \zeta_{2\cdot 7} + \zeta_{2\cdot 7}^{-1}] = \mathbb{Z}[\zeta_{2\cdot 7} + \zeta_{2\cdot 7}^{-1}]$ (the ring of integers of $\mathbb{Q}(\zeta_{2\cdot 7} + \zeta_{2\cdot 7}^{-1})$, which has degree 3 over $\mathbb{Q}$).

Consider the prime $p = 43$. Above 43, there are three prime ideals in $\mathcal{O}$:

$$\mathfrak{p}_1 = \left(43, 8 + \zeta_{2\cdot 7}^5 - \zeta_{2\cdot 7}^2\right), \mathfrak{p}_2 = \left(43, 15 + \zeta_{2\cdot 7}^5 - \zeta_{2\cdot 7}^2\right),$$

$$\mathfrak{p}_3 = \left(43, 19 + \zeta_{2\cdot 7}^5 - \zeta_{2\cdot 7}^2\right).$$

Finally, Magma verifies that $\zeta_{2q} + \zeta_{2q}^{-1} + \zeta_{2r} + \zeta_{2r}^{-1} = 1 + \zeta_{2\cdot 7} + \zeta_{2\cdot 7}^{-1}$ is a square modulo $\mathfrak{p}_2$ and $\mathfrak{p}_3$ but not modulo $\mathfrak{p}_1$.

Example 3. Now let $q = 7$ and $r = 11$. In this case,

$$\mathcal{O} = \mathbb{Z}[\zeta_{2\cdot 7} + \zeta_{2\cdot 7}^{-1} \ , \ \zeta_{2\cdot 11} + \zeta_{2\cdot 11}^{-1}]$$

is the ring of integers of $\mathbb{Q}(\zeta_{2\cdot 7} + \zeta_{2\cdot 7}^{-1} \ , \ \zeta_{2\cdot 11} + \zeta_{2\cdot 11}^{-1})$, which has degree 15 over $\mathbb{Q}$. Also,

$$\mathbb{Q}(\zeta_{2\cdot 7} + \zeta_{2\cdot 7}^{-1} \ , \ \zeta_{2\cdot 11} + \zeta_{2\cdot 11}^{-1}) = \mathbb{Q}(\mu),$$

where $\mu = \zeta_{2\cdot 7\cdot 11}^{58} - \zeta_{2\cdot 7\cdot 11}^{47} + \zeta_{2\cdot 7\cdot 11}^{30} - \zeta_{2\cdot 7\cdot 11}^{19}$.

$\mathcal{O}$ has five prime ideals above $p = 23$:

$$\mathfrak{p}_1 = \left(23, \mu^3 + 4\mu^2 + 14\mu + 5\right), \mathfrak{p}_2 = \left(23, \mu^3 + 6\mu^2 + 20\mu + 14\right),$$

$$\mathfrak{p}_3 = \left(23, \mu^3 + 10\mu^2 + 7\mu + 12\right), \mathfrak{p}_4 = \left(23, \mu^3 + 11\mu^2 + 11\mu + 3\right),$$

$$\mathfrak{p}_5 = \left(23, \mu^3 + 14\mu^2 + 22\mu + 16\right).$$

In this case, Magma shows that $\zeta_{2\cdot 7} + \zeta_{2\cdot 7}^{-1} + \zeta_{2\cdot 11} + \zeta_{2\cdot 11}^{-1}$ is a square modulo $\mathfrak{p}_2$ and $\mathfrak{p}_3$ but not modulo the other prime ideals.

(The inertia degree of these prime ideals is 3 and the Magma function *IsSquare* is not implemented for the rings $\mathcal{O}/\mathfrak{p}_i$. So the order of $\zeta_{2\cdot 7} + \zeta_{2\cdot 7}^{-1} + \zeta_{2\cdot 11} + \zeta_{2\cdot 11}^{-1}$ modulo $\mathfrak{p}_i$ is computed and, using this information, it is deduced whether that number is a square or not.)

2.3 A formula of Chevalley-Weil

In order to prove the main result, a formula of Chevalley and Weil ([CW34]) will be used. The theorem below is a more modern version of its statement that can be found in [GGH91] (cf. [EL80] for another modern version).

Theorem 2.3.1. *Let $\tilde{X}$ be a complete algebraic curve over the complex numbers $\mathbb{C}$. Consider a finite group G acting faithfully on $\tilde{X}$. Let g be the genus* *of $G\backslash\tilde{X}$. Choose representatives $\{\langle t_i\rangle\}_i$ for the G-classes of stabilizers such that the t_i have index +1 about the fixed point. Then, denoting by $\rho_{\Omega^1(\tilde{X})}$ the representation of G on the holomorphic differentials and by ρ any irreducible representation of G,*

$$(\chi_{\rho_{\Omega^1(\tilde{X})}}, \chi_\rho) = (g-1)\chi_\rho(1) + \left(\sum_i \sum_{k=1}^{\mathrm{ord}(t_i)} N_{\rho,i,k} \frac{\mathrm{ord}(t_i)-k}{\mathrm{ord}(t_i)}\right) + \delta_{\rho,id}$$

where $N_{\rho,j,k} = \dim \mathrm{Eig}\left(\rho(t_j), \exp(\frac{2\pi k}{\mathrm{ord}(t_j)})\right)$ is the dimension of the eigenspace of $\rho(t_j)$ associated to $\exp(\frac{2\pi k}{\mathrm{ord}(t_j)})$ and $\delta_{\rho,id}$ is 1 if ρ is the identity representation and 0 otherwise.

In the case of interest for this chapter,

$$\widetilde{X} = X_{q,r,\infty}(\mathfrak{p}) \quad \text{and} \quad G = \overline{\Gamma_{q,r,\infty}} / \overline{\Gamma_{q,r,\infty}(\mathfrak{p})}.$$

Moreover, the action on $\Omega^1(\widetilde{X})$ was adapted in order to obtain a left representation. Finally, recall that α_i = image of $\overline{\gamma_i}$ in $\overline{\Gamma_{q,r,\infty}} / \overline{\Gamma_{q,r,\infty}(\mathfrak{p})}$. So the following corollary is obtained:

Corollary 2.3.2. *If ρ is an irreducible representation of $G = \overline{\Gamma_{q,r,\infty}} / \overline{\Gamma_{q,r,\infty}(\mathfrak{p})}$ and ρ_{Ω^1} is the representation on the space of holomorphic differentials of $X_{q,r,\infty}(\mathfrak{p})$ defined by (2.1), then*

$$(\chi_{\rho_{\Omega^1}}, \chi_\rho) = -\chi_\rho(1) + \left(\sum_{i=1}^{3} \sum_{k=1}^{\mathrm{ord}(\alpha_i)} M_{\rho,i,k} \frac{\mathrm{ord}(\alpha_i)-k}{\mathrm{ord}(\alpha_i)}\right) + \delta_{\rho,id},$$

where $M_{\rho,j,k} = \dim \mathrm{Eig}\left(\rho(\alpha_j^{-1}), \exp(\frac{2\pi k}{\mathrm{ord}(t_j)})\right)$.

Proof. It follows from the previous theorem and the fact that $G\backslash\widetilde{X} = X_{q,r,\infty}$ has genus 0.

The change from $N_{\rho,j,k}$ to $M_{\rho,j,k}$ reflects the change from the natural right representation to the left representation defined in (2.1). □

2.4 Proof of the main result

The difference $m' - m''$ will be computed using corollary 2.3.2.

First it is shown that if $\mathrm{ord}(\alpha_i)$ is prime, then $M_{\rho,i,k}$ depends only on $\chi_\rho(1)$ and $\chi_\rho(\alpha_i)$.

Lemma 2.4.1. *Let* $u = \mathrm{ord}(\alpha_i)$. *Then* $M_{\rho,i,k}$ *satisfy the following equations:*

$$M_{\rho,i,0} + M_{\rho,i,1} + \ldots + M_{\rho,i,u-1} = \chi_\rho(1) \quad \textit{and}$$

$$M_{\rho,i,0} + M_{\rho,i,1}\zeta_u + \ldots + M_{\rho,i,u-1}\zeta_u^{u-1} = \chi_\rho(\alpha_i^{-1}).$$

In particular, if u *is a prime number, all* $M_{\rho,i,k}$ $(k = 0, \ldots, u-1)$ *are determined by these equations.*

Proof. Let $\rho : \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p}) \to \mathrm{GL}(V_\rho)$. The equations are then a consequence of the following facts:

· $\rho(\alpha_i)$ is diagonalizable;

· $\chi_\rho(1) = \dim V_\rho$; and

· $\chi_\rho(\alpha_i)$ is the sum of the eigenvalues of $\rho(\alpha_i)$ (counted with multiplicity).

□

The next lemma tells us that the order of the α_i are always prime numbers.

Lemma 2.4.2. *Assume $p > 2$ and that*

- $q, r \in \mathbb{P} \cup \{\infty\}$, *where $\mathbb{P}$ = set of all prime numbers;*
- $q \leq r$;
- $(q, r) \neq (2, 2)$;
- $q \neq p$.

Then

$$\operatorname{ord}(\alpha_1) = \begin{cases} q, & \textit{if } q \neq \infty \\ p, & \textit{otherwise} \end{cases} \quad , \quad \operatorname{ord}(\alpha_2) = \begin{cases} r, & \textit{if } r \neq \infty \\ p, & \textit{otherwise} \end{cases}$$

$$\textit{and } \operatorname{ord}(\alpha_3) = p.$$

Proof. First, assume q is a prime. Since $\mathrm{ord}(\overline{\gamma_1}) = q$ is a prime, $\mathrm{ord}(\alpha_1) = 1$ or q but $\mathrm{ord}(\alpha_1) \neq 1$ because α_1 is clearly not the identity matrix in $\mathrm{PSL}_2(\mathbb{F}_{\mathfrak{p}})$. If $q = \infty$, then

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \alpha_1 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which has order p.

Now, assuming r is a prime, it is also true that $\mathrm{ord}(\alpha_2) = r$. On the other hand, if $r = \infty$, then

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \alpha_2 \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which has order p .

For the last claim, assume first that $2 < q < r \neq \infty$. It is enough to see that $\zeta_{2q} + \zeta_{2q}^{-1} + \zeta_{2r} + \zeta_{2r}^{-1} \not\equiv 0 \pmod{\mathfrak{p}}$. Actually, it can be shown that $\zeta_{2q} + \zeta_{2q}^{-1} + \zeta_{2r} + \zeta_{2r}^{-1} \in \mathcal{O}^{\times}$. In fact, let $\zeta = \zeta_{2qr}$ and notice that

$$\begin{aligned} \zeta_{2q} + \zeta_{2q}^{-1} + \zeta_{2r} + \zeta_{2r}^{-1} &= \zeta^r + \zeta^{-r} + \zeta^q + \zeta^{-q} \\ &= \zeta^r(1 + \zeta^{q-r})(1 + \zeta^{-q-r}). \end{aligned}$$

In case $q < r = \infty$, it suffices to show that $\zeta_{2q} + \zeta_{2q}^{-1} + 2 \not\equiv 0 \pmod{\mathfrak{p}}$. But $\zeta_{2q}+\zeta_{2q}^{-1}+2 = (1+\zeta_{2q})(1+\zeta_{2q}^{-1})$ and their norm are $N(1+\zeta_{2q}) = N(1+\zeta_{2q}^{-1}) = q$. This finishes the proof in this case because $q \notin \mathfrak{p}$ (since $q \neq p$).

The other cases are easy. □

Using the notation

$$S_{\rho,i} := \sum_{k=1}^{\mathrm{ord}(\alpha_i)} M_{\rho,i,k} \frac{\mathrm{ord}(\alpha_i) - k}{\mathrm{ord}(\alpha_i)} \ ,$$

the difference can be written as

$$m' - m'' = (S_{\pi',1} - S_{\pi'',1}) + (S_{\pi',2} - S_{\pi'',2}) + (S_{\pi',3} - S_{\pi'',3}).$$

Now notice that $\chi_{\pi'}(g) = \chi_{\pi''}(g)$ for all $g \in \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ except when $g \sim P$ or P^{-1} (cf. table 2.1), where $P = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ (note P has order p). In order to obtain $m' - m''$, it thus suffices to compute $M_{\pi',i,k}$ and $M_{\pi'',i,k}$ for those i such that α_i is in the class of P or of P^{-1}. Looking at the traces and the order of the α_i, it can be seen that they turn out to be the i such that $\mathrm{ord}(\gamma_i) = \infty$ (i.e., those elements which are parabolic).

In order to compute those differences, the following theorem will be used:

Theorem 2.4.3. *(i)* (Chapter 5, Section 4 in [Bor66]) $h(-p) = -\frac{1}{p}\sum_{k=1}^{p-1} k \left(\frac{k}{p}\right)$.

(ii) (Cor. 7.28 in [Cox89]) $h(-p^{2n+1}) = p^n h(-p)$.

The lemma below can now be proved:

Lemma 2.4.4. *Let* $\Delta \in \{\pm 1\}$ *such that* $\alpha_i \sim \left(\begin{smallmatrix} 1 & \Delta \\ 0 & 1 \end{smallmatrix}\right)$. *Then*

$$S_{\pi',i} - S_{\pi'',i} = \Delta \cdot h(-p^f).$$

Proof. Note that, under this assumption, $\mathrm{ord}(\alpha_i) = p$.

First assume $\Delta = 1$. Then use Lemma 2.4.1 to obtain

$$M_{\pi',i,k} = \begin{cases} \frac{1}{2}p^n \left[p^n + \left(\frac{k}{p}\right)\right] & , \quad \left(\frac{k}{p}\right) \neq 0 \\ \frac{1}{2}\left[p^{2n} - 1\right] & , \quad k = 0 \end{cases}$$

and

$$M_{\pi'',i,k} = \begin{cases} \frac{1}{2}p^n \left[p^n - \left(\frac{k}{p}\right)\right] & , \quad \left(\frac{k}{p}\right) \neq 0 \\ \frac{1}{2}\left[p^{2n} - 1\right] & , \quad k = 0. \end{cases}$$

The final formula for $S_{\pi',i} - S_{\pi'',i}$ is then obtained using Theorem 2.4.3.

The same argument proves the case $\Delta = -1$. $\square$

This finishes the proof of Theorem 2.2.1. The proof of corollary 2.2.2 is broken down into the following 3 cases.

Case (i): $q = r = \infty$

In this case, all γ_i are parabolic and the α_i satisfy:

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \alpha_1 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \alpha_2 \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\alpha_3 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Since $\alpha_1, \alpha_2, \alpha_3$ are all in the same conjugacy class,

$$S_{\pi',1} = S_{\pi',2} = S_{\pi',3} \quad \text{and} \quad S_{\pi'',1} = S_{\pi'',2} = S_{\pi'',3}.$$

The result now follows from Lemma 2.4.4 and the fact that $\mathcal{O} = \mathbb{Z}$.

Case (ii): $r = \infty$ and $q \neq \infty$ is a prime number with $q \neq p$

In this case, γ_1 is not parabolic but γ_2 and γ_3 are. Moreover, α_2 and α_3 satisfy:

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \alpha_2 \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\alpha_3 = \begin{pmatrix} 1 & 2 + 2\cos(\pi/q) \\ 0 & 1 \end{pmatrix}$$

After using Lemma 2.4.4, it remains only to characterize when

$$2 + 2\cos(\pi/q) = 2 + \zeta_{2q} + \zeta_{2q}^{-1}$$

is a square modulo $\mathfrak{p}$. To simplify notation, let $\lambda_{2q} = \zeta_{2q} + \zeta_{2q}^{-1}$.

Lemma 2.4.5. *$2 + \lambda_{2q}$ is a square mod $\mathfrak{p}$ if and only if $f(\widehat{\mathfrak{p}}/p) = 2f(\mathfrak{p}/p)$, where $\widehat{\mathfrak{p}}$ is a prime in $\mathbb{Z}[\zeta_{2q}]$ above $\mathfrak{p}$.*

Proof. Recall that $\mathbb{Z}[\zeta_{2q}]$ is the ring of integers of $\mathbb{Q}(\zeta_{2q})$ (cf. Chapter 2 of [Was82]). Now note that, since $[\mathbb{Q}(\zeta_{2q}) : \mathbb{Q}(\lambda_{2q})] = 2$, the inertia degree $f(\widehat{\mathfrak{p}}/p)$ is either $f := f(\mathfrak{p}/p)$ or $2f$.

There is an inclusion

$$\mathbb{F}_{p^f} \cong \mathbb{Z}[\lambda_{2q}]/\mathfrak{p} \hookrightarrow \mathbb{Z}[\zeta_{2q}]/\widehat{\mathfrak{p}}.$$

Note that $2 + \lambda_{2q} = 2 + \zeta_{2q} + \zeta_{2q}^{-1} = 2 - \alpha_q - \alpha_q^{-1}$, where $\alpha_q := -\zeta_{2q} = \exp(\frac{q+1}{q}\pi)$. So, letting $\beta_q := \exp(\frac{q+1}{2q}\pi) \in \mathbb{Z}[\zeta_{2q}]$, then $2+\lambda_{2q} = -(\beta_q - \beta_q^{-1})^2$.

Suppose $f(\widehat{\mathfrak{p}}/p) = f$. In this case the inclusion is actually an isomorphism. Thus $2 + \lambda_{2q} = -(\beta_q - \beta_q^{-1})^2$ is a square modulo $\mathfrak{p}$ if and only if (-1) is a square modulo $\mathfrak{p}$ but since $p \equiv 3 \pmod 4$ and f is odd, (-1) is not a square modulo $\mathfrak{p}$. Hence, $2 + \lambda_{2q}$ is not a square modulo $\mathfrak{p}$.

Conversely, suppose $f(\widehat{\mathfrak{p}}/p) = 2f$. Since (-1) is not a square mod $\mathfrak{p}$, it suffices to show that $(\beta_q - \beta_q^{-1})^2$ is not a square in $\mathbb{F}_{p^f} \cong \mathbb{Z}[\lambda_{2q}]/\mathfrak{p}$. If $(\beta_q - \beta_q^{-1})^2$ is a square mod $\mathfrak{p}$, then $\overline{\beta_q - \beta_q^{-1}}^2 = \overline{r}^2$ where $r \in \mathbb{Z}[\lambda_{2q}]$. So, $\overline{\beta_q - \beta_q^{-1}} = \pm\overline{r}$ viewed in $\mathbb{F}_{p^{2f}} \cong \mathbb{Z}[\lambda_{2q}]/\widehat{\mathfrak{p}}$. This implies that $\overline{\beta_q - \beta_q^{-1}} \in \mathbb{F}_p \cong \mathbb{Z}[\lambda_{2q}]/\mathfrak{p}$. It is also true that $\beta_q + \beta_q^{-1} \in \mathbb{Z}[\lambda_{2q}]$ (in fact, $\mathbb{Z}[\lambda_{2q}] = \mathbb{Z}[\beta_q + \beta_q^{-1}]$ because β_q is also a primitive $2q$-root of unity; cf. Chapter 2 of [Was82]). So $\overline{\beta_q} \in \mathbb{Z}[\lambda_{2q}]/\mathfrak{p}$ (recall that $p > 2$). But $\mathbb{Z}[\zeta_{2q}] = \mathbb{Z}[\beta_q]$ and, hence, $\mathbb{F}_{p^f} \cong \mathbb{Z}[\lambda_{2q}]/\mathfrak{p} = \mathbb{Z}[\beta_q]/\widehat{\mathfrak{p}} \cong \mathbb{F}_{p^{2f}}$, a contradiction. □

Lemma 2.4.6. *Using the same notation as in the previous lemma,*

$$f(\widehat{\mathfrak{p}}/p) = 2f(\mathfrak{p}/p) \qquad \Longleftrightarrow \qquad \operatorname{ord}(p \mod q) \textit{ is even.}$$

Proof. It is known that $f(\widehat{\mathfrak{p}}/p) = \operatorname{ord}(p \mod q)$ (thm 2.13 in [Was82]). Suppose $\operatorname{ord}(p \mod q)$ is even. Since p is not ramified in $\mathbb{Z}[\zeta_{2q}]$ (Prop. 2.3 in [Was82]), $|D(\widehat{\mathfrak{p}}/p)| = f(\widehat{\mathfrak{p}}/p)$, where $D(\widehat{\mathfrak{p}}/p)$ is the decomposition group. So, $D(\widehat{\mathfrak{p}}/p)$ has an element of order 2. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_{2q})/\mathbb{Q})$ is cyclic, it has only one element of order 2, namely, the complex conjugation (denoted here by -1).

Now, it is known that $f(\widehat{\mathfrak{p}}/\mathfrak{p}) \cdot r(\mathbb{Z}[\zeta_{2q}]/\mathfrak{p}) = 2$, where $r := r(\mathbb{Z}[\zeta_{2q}]/\mathfrak{p})$ is the number of primes in $\mathbb{Z}[\zeta_{2q}]$ above $\mathfrak{p}$. It is also known that r is the number of elements in the H-orbit of $\widehat{\mathfrak{p}}$, where $H = \{1, -1\} = \mathrm{Gal}(\mathbb{Q}(\zeta_{2q})/\mathbb{Q}(\zeta_{2q}+\zeta_{2q}^{-1}))$. But by what was seen before, $-1 \in D(\widehat{\mathfrak{p}}/p)$, which implies $r = 1$ and $f(\widehat{\mathfrak{p}}/\mathfrak{p}) = 2$. Hence, $f(\widehat{\mathfrak{p}}/p) = 2f(\mathfrak{p}/p)$. □

Case (iii): $q, r \notin \{p, \infty\}$ are prime numbers and $(q, r) \neq (2, 2)$

In this case, γ_1, γ_2 are not parabolic but γ_3 is:

$$\gamma_3 = \begin{pmatrix} 1 & \zeta_{2q} + \zeta_{2q}^{-1} + \zeta_{2r} + \zeta_{2r}^{-1} \\ 0 & 1 \end{pmatrix}.$$

Hence it is easy to see that

$$\alpha_3 \sim \begin{cases} \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), & \text{if } \zeta_{2q}^{-1} + \zeta_{2r} + \zeta_{2r}^{-1} \text{ is a square modulo } \mathfrak{p} \\ \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right), & \text{if } \zeta_{2q}^{-1} + \zeta_{2r} + \zeta_{2r}^{-1} \text{ is not a square modulo } \mathfrak{p}. \end{cases}$$

This finishes the proof.

Remark 2.4.7. Recall that the numbers m' and m'' refer to the representation of $\Gamma/\Gamma(\mathfrak{p}) \cong \mathrm{PSL}_2(\mathbb{F}_{\mathfrak{p}})$ on the space of holomorphic differentials of $X(\Gamma(\mathfrak{p}))$ and, hence, a priori depend on $\mathfrak{p}$. Nevertheless, a consequence of the last theorem is that the difference $m' - m''$ does not depend on the prime ideal $\mathfrak{p}$ (nor on $\mathfrak{q}$) above a fixed prime p.

Chapter 3

Normalizers of triangle groups

The normalizer of a Fuchsian group gives us automorphisms of the corresponding curve. These automorphisms can provide valuable information as illustrated in the case of classical modular curves by the important role played by the Fricke-Atkin-Lehner involution (which arises as a normalizer element of $\Gamma_0(N)$).

More generally, we can study the commensurator of a Fuchsian group (which, in the classical setting, gives rise to the Hecke operators, crucial objects in the modern theory of modular forms). By a deep result of Margulis (cf. [Mar91]), if a group is not arithmetic, than it has finite index in its commensurator. In our case, Takeuchi showed in [Tak77] that there are only finitely many triangle groups that are arithmetic. In particular, all the triangle groups $\Gamma_{q,\infty,\infty}$ where $q > 3$ are not arithmetic. So, contrary to the classical case $\mathrm{SL}_2(\mathbb{Z})$, we do not have infinitely many "Hecke operators" but it would still be interesting to understand what they can possibly say about general triangle groups.

In this chapter, we will study the normalizers (in $\mathrm{PSL}_2(\mathbb{R})$) of triangle groups and some of their congruence subgroups. Unless otherwise stated, throughout this chapter all normalizers are with respect to $\mathrm{PSL}_2(\mathbb{R})$, i.e.,

$$N(-) = N_{\mathrm{PSL}_2(\mathbb{R})}(-).$$

In Section 1, we fix the notation that will be used in this chapter and prove a result that will guide our study in the following sections.

As a first application of that result, in Section 2, we prove that the normalizer of any Hecke triangle group is trivial, that is, it is equal to the triangle group itself.

In Section 3, we find an explicit characterization for the normalizer of triangle groups of the form $\Gamma_{q,\infty,\infty}$. In particular, we will see that the quotient $N(\Gamma_{q,\infty,\infty})/\Gamma_{q,\infty,\infty}$ has only one non-trivial element. Moreover, we prove that the quotient $N(\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p}))/\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})$ also has only one non-trivial element when $\mathfrak{p}$ sits above a split prime.

3.1 Basic facts about normalizers of Fuchsian groups

Let $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{R})$ be a Fuchsian group and $C(\Gamma)$ its set of cusps, i.e.,

$$C(\Gamma) := \{r \in \mathbb{R} \cup \{\infty\} \mid \gamma r = r \text{ for some } \gamma \in \Gamma \text{ parabolic}\}.$$

Denote by $\mathcal{C}(\Gamma)$ the set of equivalence classes of cusps, i.e.,

$$\mathcal{C}(\Gamma) := \Gamma \backslash C(\Gamma),$$

and by $N(\Gamma)$ the normalizer of Γ in $\mathrm{PSL}_2(\mathbb{R})$, i.e.,

$$N(\Gamma) := N_{\mathrm{PSL}_2(\mathbb{R})}(\Gamma) = \{g \in \mathrm{PSL}_2(\mathbb{R}) \mid g\Gamma g^{-1} = \Gamma\}.$$

Proposition 3.1.1. *If Γ' is a subgroup of finite index in Γ, then*

$$C(\Gamma') = C(\Gamma).$$

(For a proof, cf. Proposition 1.30 in [Shi94].)

Definition 3.1.2. If $r \in C(\Gamma)$, the orbit of r under the action of Γ is denoted

$$[r] = [r]_\Gamma = \mathrm{Orb}(r) = \mathrm{Orb}_\Gamma(r) = \{\gamma \cdot r \mid \gamma \in \Gamma\},$$

where the subscript $_\Gamma$ is omitted when it is clear to which group it refers to.

Proposition 3.1.3. *Let $g \in \mathrm{PSL}_2(\mathbb{R})$.*

1. *The map*

$$\begin{array}{ccc} C(\Gamma) & \longrightarrow & C(g\Gamma g^{-1}) \\ r & \longmapsto & g \cdot r \end{array}$$

   is a bijection.

2. *The previous map induces the bijection*

$$\mathcal{C}(\Gamma) \longrightarrow \mathcal{C}(g\Gamma g^{-1}),$$

   i.e., if $[r]_\Gamma = [s]_\Gamma$, then $[g \cdot r]_{g\Gamma g^{-1}} = [g \cdot s]_{g\Gamma g^{-1}}$.

Corollary 3.1.4. *If $g \in N(\Gamma)$, then g induces a permutation of the set $\mathcal{C}(\Gamma)$ via*

$$[r] \longmapsto [g \cdot r].$$

This induces a group homomorphism

$$\begin{array}{cccc} \varphi: & N(\Gamma) & \longrightarrow & \mathrm{Perm}(\mathcal{C}(\Gamma)) \\ & g & \longmapsto & ([r] \mapsto g \cdot [r] := [g \cdot r]) \end{array}$$

Let

$$H := \ker(\varphi) = \{g \in N(\Gamma) \mid g \cdot [r] = [r], \text{ for all } [r] \in \mathcal{C}(\Gamma)\}.$$

Remark 3.1.5. Let $\varepsilon = |\mathcal{C}(\Gamma)|$ be the number of cusps (up to Γ-equivalence). Then

$$[N(\Gamma) : H] \leq \varepsilon!.$$

It is easy to see that $\Gamma \subseteq H$. As a consequence of this discussion, the following holds

Theorem 3.1.6. $\Gamma = N(\Gamma)$ *if and only if*

(i) $H = \Gamma$

(ii) $[N(\Gamma) : H] = 1.$

This means that $\Gamma = N(\Gamma)$ *if and only if*

(i) $\big(g \in N(\Gamma) \text{ such that } g \cdot [r] = [r] \text{ for all } [r] \in \mathcal{C}(\Gamma)\big) \Rightarrow \big(g \in \Gamma\big)$

(ii) $\big(g \in N(\Gamma)\big) \Rightarrow \big(g \cdot [r] = [r], \text{ for all } [r] \in \mathcal{C}(\Gamma)\big).$

Remark 3.1.7. Notice that the question whether $N(\Gamma)$ is equal to Γ or not is independent of the conjugacy class of Γ in $\mathrm{PSL}_2(\mathbb{R})$, i.e.,

$$N(\Gamma) = \Gamma \Longleftrightarrow N(g\Gamma g^{-1}) = g\Gamma g^{-1}$$

for any $g \in \mathrm{PSL}_2(\mathbb{R})$. (This is because $N_G(gHg^{-1}) = gN_G(H)g^{-1}$, for any group G, $g \in G$ and $H \leq G$.)

3.2 (q, r, ∞)-triangle groups

In this section, the group Γ is assumed to be the triangle group with paramenters (q, r, ∞), with $q, r \neq \infty$, i.e.,

$$\Gamma = \Gamma_{q,r,\infty}.$$

For these triangle groups, $\epsilon = 1$ (there is only one cusp up to Γ-equivalence). This means that $[N(\Gamma) : H] = 1$. So Theorem 3.1.6 in this case reads:

Proposition 3.2.1. *Let $\Gamma = \Gamma_{q,r,\infty}$ and $r_0 \in C(\Gamma)$ be a representative of the cusp of Γ. The normalizer $N(\Gamma)$ is equal to Γ if and only if*

$$\big(g \in N(\Gamma) \textit{ such that } g \cdot r_0 = r_0\big) \Rightarrow \big(g \in \Gamma\big).$$

Proof. Suppose that

$$\big(g \in N(\Gamma) \text{ such that } g \cdot r_0 = r_0\big) \Rightarrow \big(g \in \Gamma\big)$$

holds.

Since $\varepsilon = 1$, condition (ii) in Theorem 3.1.6 is automatically satisfied. It remains to show (i).

So let $g \in N(\Gamma)$ such that $g \cdot [r] = [r]$ for all $[r] \in \mathcal{C}(\Gamma)$. In particular, this implies that

$$g \cdot r_0 \in \mathrm{Orb}(r_0),$$

i.e.,

$$g \cdot r_0 = \gamma \cdot r_0$$

for some $\gamma \in \Gamma$.

Therefore $\gamma^{-1} g \cdot r_0 = r_0$. Hence, by assumption, $\gamma^{-1} g \in \Gamma$ and, thus, $g \in \Gamma$.

Thus, by Theorem 3.1.6, $\Gamma = N(\Gamma)$. □

Theorem 3.2.2. *The normalizer of any Hecke triangle group is the group itself, i.e.,*

$$N(\Gamma_{2,q,\infty}) = \Gamma_{2,q,\infty} =: \Gamma$$

for $q \geq 4$. In particular, $N(\mathrm{SL}_2(\mathbb{Z})) = \mathrm{SL}_2(\mathbb{Z})$ (because $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_{2,3,\infty}$).

Proof. Because of Remark 3.1.7 and the fact that any two triangle groups with the same parameters are conjugate (by Theorem 0.3.5), any realization of $\Gamma_{2,q,\infty}$ in $\mathrm{PSL}_2(\mathbb{R})$ will suffice to show the desired property. In particular, we can assume that

$$\Gamma_{2,q,\infty} = \langle \gamma_1, \gamma_3 \rangle,$$

where

$$\gamma_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \gamma_3 = \begin{pmatrix} 1 & \lambda_q \\ 0 & 1 \end{pmatrix},$$

and $\lambda_q = 2\cos(\pi/q) = \zeta_{2q} + \zeta_{2q}^{-1} \in \mathbb{Z}[\lambda_q]$. Notice that $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z}[\lambda_q])$.

In this realization of Γ, one possible representative of the cusps is $\infty \in C(\Gamma)$.

Let $g \in N(\Gamma)$ such that $g \cdot \infty = \infty$. It suffices to show that $g \in \Gamma$.

Since $g \cdot \infty = \infty$, the matrix g is of the form $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. Therefore

$$\begin{pmatrix} 1 & a^2\lambda_q \\ 0 & 1 \end{pmatrix} = g\gamma_3 g^{-1} \in \Gamma.$$

Hence $g\gamma_3 g^{-1} \in \mathrm{Stab}_\Gamma(\infty) = \langle \pm\gamma_3 \rangle$. Therefore $a^2 \in \mathbb{Z}$. Similarly, considering $g^{-1}\gamma_3 g$, it follows that $d^2 \in \mathbb{Z}$.

Since $ad = \det(g) = 1$, it yields that $a = d = \pm 1$. Without loss of generality (in $\mathrm{PSL}_2(\mathbb{R})$), $a = d = 1$. Hence

$$g = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

Now,

$$\begin{pmatrix} b & * \\ * & * \end{pmatrix} = g\gamma_1 g^{-1} \in \Gamma.$$

In particular, $b \in \mathbb{Z}[\lambda_q]$. If $b = m\lambda_q = \gamma_3^m$, for some $m \in \mathbb{Z}$, the $g \in \Gamma$ and the proof is complete.

Suppose, therefore, that $b \neq m\lambda_q$. Then b and λ_q are linearly independent over $\mathbb{Q}$. Therefore the group generated by them accumulates at 0. In particular, for all $\delta > 0$ there are $m, n \in \mathbb{Z}$ such that $0 < \Delta := mb + n\lambda_q < \delta$.

Hence,

$$\begin{pmatrix} 1 & \Delta \\ 0 & 1 \end{pmatrix} = g^m \gamma_3^n \in N(\Gamma).$$

But then

$$\begin{pmatrix} 1 & \Delta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda_q & 1 \end{pmatrix} \begin{pmatrix} 1 & \Delta \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 + \Delta\lambda_q & \Delta\lambda_q \\ \lambda_q & 1 - \Delta\lambda_q \end{pmatrix} \in \Gamma,$$

which implies that Γ is not discrete, a contradiction.

In the last equation, it was used that

$$\begin{pmatrix} 1 & 0 \\ \lambda_q & 1 \end{pmatrix} = \gamma_3^{-1}\gamma_1^{-1} \in \Gamma.$$

□

3.3 (q, ∞, ∞)-triangle groups

In this section, the group Γ is assumed to be the triangle group with parameters (q, ∞, ∞) with $q \neq \infty$, i.e.,

$$\Gamma = \Gamma_{q,\infty,\infty}.$$

For these triangle groups, $\varepsilon = 2$ (there are two cusps up to Γ-equivalence).

Let $r_1, r_2 \in C(\Gamma)$ be representatives of the cusps, i.e.,

$$C(\Gamma) = \mathrm{Orb}(r_1) \sqcup \mathrm{Orb}(r_2)$$

The translation of Theorem 3.1.6 to this context reads

Proposition 3.3.1. *Let $\Gamma = \Gamma_{q,\infty,\infty}$. Then $\Gamma = N(\Gamma)$ if and only if*

(i) $\big(g \in N(\Gamma)$ *such that* $g \cdot r_1 = r_1\big) \Rightarrow \big(g \in \Gamma\big)$

(ii) $\big(g \in N(\Gamma)\big) \Rightarrow \big(g \cdot r_1 \in \mathrm{Orb}(r_1)\big)$.

To further study the normalizer of $\Gamma_{q,\infty,\infty}$ (and that of some of its congruence subgroups), we will fix a realization of $\Gamma_{q,\infty,\infty}$ different from the 'standard' realization from Chapter 1, namely:

$$\Gamma := \Gamma_{q,\infty,\infty} = \langle \gamma_2, \gamma_3 \rangle,$$

where

$$\gamma_2 = \begin{pmatrix} 1 & 0 \\ -\mu & 1 \end{pmatrix} \quad \text{and} \quad \gamma_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\mu = \lambda + 2 \; \in \; \mathbb{Z}[\mu] = \mathbb{Z}[\lambda] = \mathcal{O}_{\mathbb{Q}(\lambda)}$$

and

$$\lambda = \lambda_q = 2\cos(\pi/q) = \zeta_{2q} + \zeta_{2q}^{-1}.$$

This realization is simply a $\begin{pmatrix} 1/\sqrt{\mu} & -1/\sqrt{\mu} \\ 0 & \sqrt{\mu} \end{pmatrix}$-conjugation of the standard one. This conjugation also preserves the congruence subgroups with respect to primes $\mathfrak{p}$ that are not prime divisors of q.

In particular, this implies that representatives for the two (inequivalent) cusps of $\Gamma_{q,\infty,\infty}$ can be taken to be

$$r_1 = \infty \quad \text{and} \quad r_2 = 0. \cdot$$

Denote by γ_1 the following element

$$\gamma_1 = (\gamma_2\gamma_3)^{-1} = \begin{pmatrix} 1-\mu & -1 \\ \mu & 1 \end{pmatrix} \in \Gamma_{q,\infty,\infty}.$$

Notice that, under this realization,

$$\Gamma = \Gamma_{q,\infty,\infty} \subseteq \mathrm{PSL}_2(\mathbb{Z}[\mu]).$$

In what follows, it is assumed that

$$q \geq 5 \text{ is a prime number}$$

and, moreover, that

$$\mathbb{Z}[\mu] \text{ is a PID.}$$

This assumption holds at least for $q = 5, 7, 11, 13, 17, 19, 23, 29, 31$, as can be verified using a computer algebra system but it is not always true. For a discussion about this hypothesis, cf. [Was82] (in particular Theorem 4.10 and page 230) and [Sch03].

Lemma 3.3.2. *The element $\mu \in \mathbb{Z}[\mu]$ satisfies*

$$\mathrm{Norm}_{\mathbb{Q}(\mu)/\mathbb{Q}}(\mu) = q.$$

In particular, it is a prime element of $\mathbb{Z}[\mu]$ above $q \in \mathbb{Z}$.

Proof. First note that

$$\mu = -(1+\zeta_{2q})(1+\zeta_{2q}^{-1}).$$

Since q is odd, $-\zeta_{2q}$ is a primitive q-th root of unity. So, the minimal polynomial of ζ_{2q} is $\phi_q(-x)$, where

$$\phi_q(x) = x^{p-1} + \cdots + x + 1$$

is the q-th cyclotomic polynomial. Therefore, the minimal polynomial of $1+\zeta_{2q}$ is $\phi_q(-(x-1)) = \phi_q(-x+1))$, which has constant term equal to q. Hence,

$$N_{\mathbb{Q}(\zeta_{2q})/\mathbb{Q}}(1+\zeta_{2q}) = q.$$

Similarly,

$$N_{\mathbb{Q}(\zeta_{2q})/\mathbb{Q}}(1+\zeta_{2q}^{-1}) = q.$$

Thus,

$$N_{\mathbb{Q}(\zeta_{2q})/\mathbb{Q}}(\mu) = q^2,$$

which, combined with the fact that

$$[\mathbb{Q}(\zeta_{2q}) : \mathbb{Q}(\zeta_{2q} + \zeta_{2q}^{-1})] = 2,$$

finishes the proof.

□

Lemma 3.3.3. *If $g = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in N(\Gamma_{q,\infty,\infty})$ for some $b \in \mathbb{Z}[\mu]$, then $g \in \Gamma_{q,\infty,\infty}$.*

Proof. It suffices to show that $b \in \mathbb{Z}$.

By hypothesis, $b = a_0 + v$, where $v = a_1\mu + \cdots + a_n\mu^n$, $a_i \in \mathbb{Z}$ and $n = (q-1)/2$. If $v = 0$, there is nothing to do. Suppose therefore that $v \neq 0$. Then b and 1 are linearly independent over $\mathbb{Q}$ and, thus, the group

$$\mathbb{Z}b + \mathbb{Z}1$$

accumulates at 0.

Therefore, for each $\delta > 0$, there are $\alpha, \beta \in \mathbb{Z}$ such that $0 < \Delta := \alpha b + \beta < \delta$.

Now take

$$g' := \begin{pmatrix} 1 & \Delta \\ 0 & 1 \end{pmatrix} = g^\alpha \gamma_3^\beta \in N(\Gamma_{q,\infty,\infty}).$$

Then, since $\gamma_2 \in \Gamma_{q,\infty,\infty}$, it follows that

$$\begin{pmatrix} 1-\mu\Delta & \Delta^2\mu \\ -\mu & 1+\mu\Delta \end{pmatrix} = g'\gamma_2 g'^{-1} \in \Gamma_{q,\infty,\infty},$$

which shows that $\Gamma_{q,\infty,\infty}$ is not discrete, a contradiction.

□

Lemma 3.3.4. *If $g \in N(\Gamma_{q,\infty,\infty})$ is such that*

$$g \cdot \infty = \infty$$

then $g \in \Gamma_{q,\infty,\infty}$.

Proof. Any such g is of the form $g = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. Since $\det(g) = 1$, it follows that $d = 1/a$.

Therefore, because $\gamma_3 \in \Gamma_{q,\infty,\infty}$,

$$\begin{pmatrix} 1 & a^2 \\ 0 & 1 \end{pmatrix} = g\gamma_3 g^{-1} \in \Gamma^{(0)}.$$

So $g\gamma_3 g^{-1} \in \mathrm{Stab}_{\Gamma_{q,\infty,\infty}}(\infty) = \langle \pm\gamma_3 \rangle$. Hence

$$a^2 \in \mathbb{Z}.$$

Similarly, using that

$$\begin{pmatrix} 1 & d^2 \\ 0 & 1 \end{pmatrix} = g^{-1}\gamma_3 g \in \Gamma_{q,\infty,\infty},$$

it follows that

$$\frac{1}{a^2} = d^2 \in \mathbb{Z}.$$

Thus the only possibility is that $a = \pm 1$. Since all these matrices are being viewed in $\mathrm{PSL}_2(\mathbb{R})$, one can take $a = 1$. So

$$g = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

The goal now is to show that $b \in \mathbb{Z}[\mu]$. The previous lemma then implies that $g \in \Gamma_{q,\infty,\infty}$, finishing the proof.

Using that $\gamma_2 \in \Gamma_{q,\infty,\infty}$, it follows that

$$\begin{pmatrix} 1 - \mu b & \mu b^2 \\ * & * \end{pmatrix} = g\gamma_2 g^{-1} \in \Gamma_{q,\infty,\infty}.$$

In particular,

$$\mu b \ , \ \mu b^2 \ \in \ \mathbb{Z}[\mu].$$

From the first containment, it results that

$$b = \frac{k}{\mu}$$

for some $k \in \mathbb{Z}[\mu]$.

From the second one,

$$\frac{k^2}{\mu} \in \mathbb{Z}[\mu].$$

Since μ is a prime in $\mathbb{Z}[\mu]$, it follows that

$$\mu \mid k$$

in $\mathbb{Z}[\mu]$ (recall that $\mathbb{Z}[\mu]$ is a unique factorization domain) and, thus,

$$b \in \mathbb{Z}[\mu].$$

□

Lemma 3.3.5. *The element*

$$g = \begin{pmatrix} 0 & 1/\sqrt{\mu} \\ -\sqrt{\mu} & 0 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{R})$$

is in $N(\Gamma_{q,\infty,\infty})$.

Proof. This follows from the following easy computations:

$$g\gamma_2 g^{-1} = \gamma_3 \quad \text{and} \quad g\gamma_3 g^{-1} = \gamma_2.$$

□

Theorem 3.3.6. *The normalizer of $\Gamma_{q,\infty,\infty}$ is given by*

$$N(\Gamma_{q,\infty,\infty}) = \Gamma_{q,\infty,\infty} \;\sqcup\; \Gamma_{q,\infty,\infty} \cdot g,$$

where

$$g = \begin{pmatrix} 0 & 1/\sqrt{\mu} \\ -\sqrt{\mu} & 0 \end{pmatrix}.$$

In particular,

$$\frac{N(\Gamma_{q,\infty,\infty})}{\Gamma_{q,\infty,\infty}} \cong \mathbb{Z}/2\mathbb{Z}.$$

Proof. Lemma 3.3.4 says that $\ker(\varphi) = \Gamma_{q,\infty,\infty}$ (in the notation of corollary 3.1.4). Therefore Remark 3.1.5 implies that $[N(\Gamma_{q,\infty,\infty}) : \Gamma_{q,\infty,\infty}] \leq 2$. The previous lemma then finishes the proof. □

3.3.1 Congruence subgroups

In this subsection, the group $\Gamma := \Gamma_{q,\infty,\infty}$ still refers to the realization fixed at the beginning of Section 3.3 where $q \geq 5$ is, again, a prime number such that $\mathbb{Z}[\mu]$ is a PID.

The idea is to study the normalizer of the following congruence subgroups

$$\Gamma^{(0)}(\mathfrak{p}) := \Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p}) = \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \mid c \equiv 0 \pmod{\mathfrak{p}}\},$$

for $\mathfrak{p}$ a prime ideal of $\mathbb{Z}[\mu]$ above a totally split prime $p \in \mathbb{Z}$. In particular $p \neq q$.

In the classical case (i.e., $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_{2,3,\infty}$), its analogous congruence subgroup has a non-trivial normalizer. In fact, the existence of the Fricke involution is an important tool in the study of classical modular curves. In [LT99], it was proved that these congruence groups (when the parent group is the Hecke triangle group $\Gamma_{2,5,\infty}$) have a trivial normalizer. So it is natural to ask whether a similar result holds for $\Gamma_{q,\infty,\infty}$.

Let $\mathfrak{p} = (\tau)$ a prime ideal above a totally split prime $p \in \mathbb{Z}$ (i.e., $p = \tau_1 \cdots \tau_D$, where τ_i are distinct prime ideals in $\mathbb{Z}[\mu]$ above p and $D = (q-1)/2$). The group $\Gamma^{(0)}(\mathfrak{p})$ will also be denoted $\Gamma^{(0)}(\tau)$.

Lemma 3.3.7. *Write $p = \tau_1\tau_2 \cdots \tau_D$, for $\tau_i \in \mathbb{Z}[\mu]$ prime elements. Then there are $n_1, n_2, \ldots, n_D \in \mathbb{Z}$ such that*

(i) $\tau_i \mid (n_i\mu + 1)$ for all i

(ii) $\tau_j \nmid (n_i\mu + 1)$ for all $i \neq j$.

In the proof of this lemma, the notation below will be used.

Notation 3.3.8. If $\varphi(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$, then

$$\widetilde{\varphi}(x) := a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + 1.$$

Remark 3.3.9. If $\varphi(x)$ factors completely into linear terms, so does $\widetilde{\varphi}(x)$. Moreover, if the roots of φ are all distinct, the same holds for $\widetilde{\varphi}$.

Proof. (*of Lemma 3.3.7*) Let $\mu^{(i)}$, $i \in \{1, \ldots, D\}$ be all the Galois conjugates of μ. Then

$$\mathrm{Norm}(m\mu + 1) = (\mu^{(1)} \cdots \mu^{(D)})m^D + \cdots + (\mu^{(1)} + \cdots + \mu^{(D)})m + 1.$$

Let

$$\psi(x) = s_D x^D + \cdots + s_1 x + s_0 \in \mathbb{Z}[x],$$

where

$$s_r = \sum_{i_1 < \cdots < i_r} \mu^{(i_1)} \cdots \mu^{(i_r)}.$$

So

$$\mathrm{Norm}(m\mu + 1) = \psi(m).$$

Note that $\psi(x) = \varphi(-x)\tilde{}$, where φ is the minimal polynomial of μ.

By the assumption that p is totally split in $\mathbb{Z}[\mu]$, it follows that $\overline{\varphi}(x) \in \mathbb{F}_p[x]$ factors completely into linear terms and all its roots lie in $\mathbb{F}_p$. So, by the previous remark, the same is true for $\overline{\psi}(x) \in \mathbb{F}_p[x]$.

Take $\overline{m_1}, \ldots, \overline{m_D} \in \mathbb{Z}/p\mathbb{Z}$ the (distinct) roots of $\overline{\psi}$.

Now consider

$$g(x) = s_D^{(m)} x^D + \cdots + s_1^{(m)} x + s_0^{(m)} \in \mathbb{Z}[x],$$

where

$$s_r^{(m)} = \sum_{i_1 < \cdots < i_r} m_{(i_1)} \cdots m_{(i_r)}.$$

Note that

$$g(\mu) = (m_1\mu + 1) \cdots (\mu_D \mu + 1).$$

Using that $\overline{m_1}, \dots, \overline{m_D}$ are roots of $\varphi(-x)\tilde{}\;$ mod p, it follows that

$$g(\mu) \equiv 0 \pmod{p}.$$

Therefore

$$\tau_1 \cdots \tau_D = p \mid (m_1\mu + 1) \cdots (m_D\mu + 1).$$

If there are $k_1, \dots, k_D \in \mathbb{Z}$ such that

$$n_i = m_i + k_i p$$

satisfies

$$\text{Norm}(n_i\mu + 1) \not\equiv 0 \pmod{p^2},$$

then the lemma is proved.

The existence of the k_i is guaranteed by the fact that $\text{Norm}(\alpha\mu + 1) = \psi(\alpha)$ and the next lemma. $\square$

Lemma 3.3.10. *Let $f(x) \in \mathbb{Z}[x]$ such that $\overline{m} \in \mathbb{Z}/p\mathbb{Z}$ is a simple root of $\overline{f}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$. If $f(m) \equiv 0 \pmod{p^2}$, then $f(m+p) \not\equiv 0 \pmod{p^2}$.*

Proof. Suppose

$$f(x) = a_d x^d + \cdots + a_1 x + a_0.$$

Then, $\mod p^2$,

$$\begin{aligned} f(m+p) &= a_d(m+p)^d + \cdots + a_1(m+p) + a_0 \\ &\equiv da_d m^{d-1}p + \cdots + a_1 p \\ &= pf'(m) \not\equiv 0 \pmod{p^2}. \end{aligned}$$

The last conclusion follows from the fact that $\overline{m}$ is a simple root of $\overline{f}$ in $\mathbb{Z}/p\mathbb{Z}$. □

Proposition 3.3.11. *The group $\Gamma^{(0)}(\mathfrak{p})$ has 4 inequivalent cusps:*

$$\infty, \quad \tfrac{-\mu+1}{\mu}, \quad 0, \quad \gamma_2\gamma_3^{-n_0}\cdot 0,$$

where $n_0 \in \mathbb{Z}$ is taken from the Lemma 3.3.7 satisfying

$$\tau \mid (n_0\mu + 1).$$

Proof. (To simplify notation, $\Gamma^{(0)}$ will denote $\Gamma^{(0)}(\mathfrak{p})$ throughout this proof.)

As explained before, the cusps of $\Gamma := \Gamma_{q,\infty,\infty}$ (up to Γ-equivalence) are $[\infty]_\Gamma$ and $[0]_\Gamma$, the question, basically, is: how many cusps (up to $\Gamma^{(0)}(\mu+1)$-equivalence) are there above $[\infty]_\Gamma$ and $[0]_\Gamma$?

Since p is totally split, it follows from Lemmas 1.3.2 and 1.3.3 that there are two cusps above each cusp of $\Gamma_{q,\infty,\infty}$ (i.e., above $[\infty]_\Gamma$ and $[0]_\Gamma$). The proof will be finished after the following is showed:

1. $[\frac{-\mu+1}{\mu}]_\Gamma = [\infty]_\Gamma$ and $[\gamma_2 {\gamma_3}^{-n} \cdot 0]_\Gamma = [0]_\Gamma$; but

2. $[\frac{-\mu+1}{\mu}]_{\Gamma^{(0)}} \neq [\infty]_{\Gamma^{(0)}}$ and $[\gamma_2 {\gamma_3}^{-n} \cdot 0]_{\Gamma^{(0)}} \neq [0]_{\Gamma^{(0)}}$

The second part of first item is trivial. As for the first part, it follows from:

$$\gamma_1 \cdot \infty = \tfrac{-\mu+1}{\mu}.$$

For the first part of the second item, assume, by contradiction, that $[\frac{-\mu+1}{\mu}]_{\Gamma^{(0)}} = [\infty]_{\Gamma^{(0)}}$. Then there exists $\gamma \in \Gamma^{(0)}$ such that

$$\gamma \cdot \infty = \frac{-\mu+1}{\mu} = \gamma_1 \cdot \infty.$$

This would imply that

$$\gamma_1^{-1}\gamma \in \mathrm{Stab}_\Gamma(\infty) = \langle \pm\gamma_3 \rangle$$

and, hence,

$$\gamma = \pm\gamma_1\gamma_3^n = \pm\left(\begin{smallmatrix} * & * \\ \mu & * \end{smallmatrix}\right),$$

which is impossible because $\mu \notin (\tau)$ (in fact, by Lemma 3.3.2, $\mathrm{Norm}(\mu) = q$).

Finally, assume, by contradiction, that $[\gamma_2 {\gamma_3}^{-n_0} \cdot 0]_{\Gamma^{(0)}} = [0]_{\Gamma^{(0)}}$. Then there exists $\gamma \in \Gamma^{(0)}$ such that

$$\gamma \cdot 0 = -\frac{1}{\mu+1} = \gamma_2 {\gamma_3}^{-n_0} \cdot 0.$$

This would imply that

$$(\gamma_2\gamma_3^{-n_0})^{-1}\gamma \in \mathrm{Stab}_\Gamma(0) = \langle \pm\gamma_2 \rangle$$

and, hence,

$$\gamma = \pm\gamma_2\gamma_3^{-n_0}\gamma_2^m = \pm \begin{pmatrix} * & * \\ -\mu - m\mu(n\mu+1) & * \end{pmatrix},$$

which is impossible because

$$\tau \mid (n_0\mu + 1) \ \text{ and } \ \tau \nmid \mu.$$

□

Theorem 3.3.12. *Let $\mathfrak{p} \subseteq \mathbb{Z}[\mu]$ be a prime ideal above a split prime $p \in \mathbb{Z}$ and $\Gamma^{(0)} = \Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})$. Then*

$$N(\Gamma^{(0)}) = \Gamma^{(0)} \sqcup h\Gamma^{(0)},$$

where

$$h = \gamma_2\gamma_3^{-n_0}\begin{pmatrix} 0 & 1/\sqrt{\mu} \\ -\sqrt{\mu} & 0 \end{pmatrix} = \sqrt{\mu}\begin{pmatrix} n_0 & 1/\mu \\ -(n_0\mu+1) & -1 \end{pmatrix}$$

and n_0 is as in Proposition 3.3.11.

Proof. The following claims are proved in various lemmas below:

1. if $g \in N(\Gamma^{(0)})$ and $g \cdot \infty = \infty$, then $g \in \Gamma^{(0)}$;
2. if $g \in N(\Gamma^{(0)})$ and $g \cdot 0 = 0$, then $g \in \Gamma^{(0)}$;
3. there is no $g \in N(\Gamma^{(0)})$ such that $g \cdot \infty = 0$;
4. there is no $g \in N(\Gamma^{(0)})$ such that $g \cdot \infty = (-\mu + 1)/\mu$; and
5. there is a $h \in N(\Gamma^{(0)})$ such that $h \cdot \infty = \gamma_2 \gamma_3^{-n_0} \cdot 0$.

Note that the first claim implies that $\Gamma^{(0)} = \ker(\varphi)$ (using the notation of corollary 3.1.4) and, hence,

$$\frac{N(\Gamma^{(0)})}{\Gamma^{(0)}} \leq \mathrm{Perm}(\mathcal{C}(\Gamma^{(0)})).$$

In particular, this implies that the element h from claim 5 satisfies

$$h \cdot [\gamma_2 \gamma_3^{-n_0} \cdot 0] = [\infty].$$

In fact, if this was not true, then $h \cdot [r] = [\infty]$ for $[r] \in \{[0], [\gamma_2 \gamma_3^{-n_0} \cdot 0]\}$. But then $h^{-1} \cdot [\infty] = [r]$ for some $[r][r] \in \{[0], [\gamma_2 \gamma_3^{-n_0} \cdot 0]\}$, contradicting either claim 3 or claim 4.

For a similar reason, claim 2 implies that

$$h \cdot [0] = [\frac{-\mu + 1}{\mu}] \;\text{ and }\; h \cdot [\frac{-\mu + 1}{\mu}] = [0].$$

All this shows that, modulo $\Gamma^{(0)}$, there can be only one non-trivial element in $N(\Gamma^{(0)})$, finishing the proof of the theorem. □

Lemma 3.3.13. *If $g \in N(\Gamma^{(0)})$ is of the form*

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$$

for $b \in \mathbb{Z}[\mu]$, then $g \in \Gamma^{(0)}$.

Proof. The proof in the case $g = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ is similar to the proof of Lemma 3.3.3 (just replacing γ_2 by γ_2^p).

Assume now that

$$g = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}.$$

By hypothesis, $b = a_0 + v$, where $v = a_1\mu + \cdots + a_n\mu^n$, $a_i \in \mathbb{Z}$ and $n = (q-1)/2$. If $v = 0$, there is nothing to do. Suppose therefore that $v \neq 0$. Then b and p are linearly independent over $\mathbb{Q}$ and, thus, the group

$$\mathbb{Z}b + \mathbb{Z}p$$

accumulates at 0.

Therefore, for each $\delta > 0$, there are $\alpha, \beta \in \mathbb{Z}$ such that $0 < \Delta := \alpha b - p\beta < \delta$.

Now take

$$g' := \begin{pmatrix} 1 & 0 \\ \Delta & 1 \end{pmatrix} = g^{\alpha}\gamma_2^{p\beta} \in N(\Gamma^{(0)}).$$

Then, since $\gamma_3 \in \Gamma^{(0)}$, it follows that

$$\begin{pmatrix} 1-\Delta & 1 \\ -\Delta^2 & 1+\Delta \end{pmatrix} = g'\gamma_3 g'^{-1} \in \Gamma^{(0)},$$

which shows that $\Gamma^{(0)}$ is not discrete, a contradiction. □

The following lemma proves the first and second claims stated in the proof of Theorem 3.3.12.

Lemma 3.3.14. *If $g \in N(\Gamma^{(0)})$ is such that*

$$g \cdot \infty = \infty \quad or \quad g \cdot 0 = 0$$

then $g \in \Gamma^{(0)}$.

Proof. Assume first that $g \cdot \infty = \infty$. Then it is of the form $g = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. Since $\det(g) = 1$, it follows that $d = 1/a$.

Therefore, because $\gamma_3 \in \Gamma^{(0)}$,

$$\begin{pmatrix} 1 & a^2 \\ 0 & 1 \end{pmatrix} = g\gamma_3 g^{-1} \in \Gamma^{(0)}.$$

So $g\gamma_3 g^{-1} \in \mathrm{Stab}_{\Gamma^(0)}(\infty) = \langle \pm\gamma_3 \rangle$. Hence

$$a^2 \in \mathbb{Z}.$$

Similarly, using that

$$\begin{pmatrix} 1 & d^2 \\ 0 & 1 \end{pmatrix} = g^{-1}\gamma_3 g \in \Gamma^{(0)},$$

it follows that

$$\frac{1}{a^2} = d^2 \in \mathbb{Z}.$$

Thus the only possibility is that $a = \pm 1$. Since all these matrices are being viewed in $\mathrm{PSL}_2(\mathbb{R})$, one can take $a = 1$. So

$$g = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

The goal now is to show that $b \in \mathbb{Z}[\mu]$. The previous lemma then implies that $g \in \Gamma^{(0)}$, finishing the proof.

Using that $\gamma_2^p \in N(\Gamma^{(0)})$, it follows that

$$\begin{pmatrix} 1 - p\mu b & p\mu b^2 \\ * & * \end{pmatrix} = g\gamma_2^p g^{-1} \in \Gamma^{(0)}.$$

In particular,

$$p\mu b \ , \ p\mu b^2 \ \in \ \mathbb{Z}[\mu].$$

From the first containment, it results that

$$b = \frac{k}{p\mu}$$

for some $k \in \mathbb{Z}[\mu]$.

From the second one,

$$\frac{k^2}{p\mu} \in \mathbb{Z}[\mu].$$

Since $\gcd(\mu, p) = 1$, μ is a prime and p is a product of distinct primes in $\mathbb{Z}[\mu]$ (since p is assumed to be totally split), it follows that

$$p\mu \mid k$$

in $\mathbb{Z}[\mu]$ (recall that $\mathbb{Z}[\mu]$ is a unique factorization domain) and, thus,

$$b \in \mathbb{Z}[\mu].$$

A similar argument (with the roles of γ_3 and γ_2 switched) shows that if $g \cdot 0 = 0$, then $g = \left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$ for some $b \in \mathbb{Z}[\mu]$. The previous lemma then implies that $g \in \Gamma^{(0)}$. □

Lemma 3.3.15. *If $g \in N(\Gamma^{(0)})$ and $g \cdot \infty = 0$, then*

$$g = \begin{pmatrix} 0 & -1/\sqrt{p\mu} \\ \sqrt{p\mu} & r\sqrt{p\mu} \end{pmatrix}$$

for some $r \in \mathbb{Z}[\mu]$.

Proof. Any $g \in \mathrm{PSL}_2(\mathbb{R})$ such that $g \cdot \infty = 0$ is necessarily of the form

$$g = \begin{pmatrix} 0 & b \\ c & d \end{pmatrix}.$$

From $\det(g) = 1$, it follows that

$$c = -\frac{1}{b}.$$

Since $\gamma_3, \gamma_2^p \in \Gamma^{(0)}(\mathfrak{p})$,

$$g\gamma_3 g^{-1} = \begin{pmatrix} 1 & 0 \\ -c^2 & 1 \end{pmatrix} \ , \ g^{-1}\gamma_2^p g = \begin{pmatrix} 1 & pb^2\mu \\ 0 & 1 \end{pmatrix} \in \Gamma^{(0)}(\mathfrak{p})$$

Since $g\gamma_3 g^{-1} \cdot 0 = 0$,

$$g\gamma_3 g^{-1} \in \mathrm{Stab}_{\Gamma^{(0)}(\mathfrak{p})}(0) = \langle \pm\gamma_2^p \rangle,$$

and, thus,

$$c^2 \in p\mu\mathbb{Z},$$

i.e.,

$$c^2 = p\mu n$$

for some $n \in \mathbb{Z}$.

A similar analysis for $g^{-1}\gamma_2^p g$ yields

$$\frac{1}{n} = pb^2\mu \in \mathbb{Z}.$$

Since $p\mu n = c^2 > 0$, it implies that $n = 1$ and, hence, (up to multiplication by $\pm I$)

$$c = \sqrt{p\mu} \;\text{ and }\; b = -\frac{1}{\sqrt{p\mu}}.$$

Now,

$$\begin{pmatrix} 1 + d\sqrt{p\mu} & d^2 \\ \\ * & * \end{pmatrix} = g^{-1}\gamma_3 g \in \Gamma^{(0)}.$$

In particular,

$$d\sqrt{p\mu}\ ,\ d^2 \in \mathbb{Z}[\mu].$$

The first condition says that

$$d = \frac{r'}{\sqrt{p\mu}},$$

for some $r' \in \mathbb{Z}[\mu]$.

The second condition then implies that

$$\frac{(r')^2}{p\mu} \in \mathbb{Z}[\mu].$$

Since $\mathbb{Z}[\mu]$ is a UFD and $p\mu$ is square-free, it follows that $(p\mu) \mid r'$ and, thus,

$$d = r\sqrt{p\mu}$$

for some $r \in \mathbb{Z}[\mu]$. □

The next lemma proves the third claim stated in the the proof of Theorem 3.3.12.

Lemma 3.3.16. *There is no $g \in N(\Gamma^{(0)})$ such that $g \cdot \infty = 0$.*

Proof. By the previous lemma, such a g would be of the form

$$g = \begin{pmatrix} 0 & -1/\sqrt{p\mu} \\ \sqrt{p\mu} & r\sqrt{p\mu} \end{pmatrix}$$

for some $r \in \mathbb{Z}[\mu]$.

Take n_0 as in Proposition 3.3.11. Note that

$$\gamma = (\gamma_2\gamma_3^{-n_0})\gamma_2^{-1}(\gamma_2\gamma_3^{-n_0})^{-1} = \begin{pmatrix} * & * \\ \mu(n_0\mu+1)^2 & * \end{pmatrix} \in \Gamma^{(0)}(\tau).$$

In fact, by the choice of n_0 and lemma 3.3.7,

$$\tau \mid (n_0\mu + 1).$$

Then $g\gamma g^{-1} \in \Gamma^{(0)}(\mu+1)$. But

$$g\gamma g^{-1} = \begin{pmatrix} * & -\frac{(n_0\mu+1)^2}{p} \\ * & * \end{pmatrix}.$$

By the choice of n_0 and Lemma 3.3.7, $p \nmid (n_0\mu+1)^2$ and, thus,

$$-\frac{(n_0\mu+1)^2}{p} \notin \mathbb{Z}[\mu],$$

a contradiction. □

Lemma 3.3.17. *If $g \in N(\Gamma^{(0)})$ and $g \cdot \infty = \frac{-\mu+1}{\mu}$, then*

$$g = \begin{pmatrix} \sqrt{p(\mu-1)}(-\mu+1) & \frac{1}{(\mu-1)^{3/2}}\left(\frac{1}{\sqrt{p}} - r\mu\sqrt{p}\right) \\ \sqrt{p(\mu-1)}\mu & \frac{r\sqrt{p}}{\sqrt{\mu-1}} \end{pmatrix}$$

for some $r \in \mathbb{Z}[\mu]$.

Proof. Any such g would be of the form

$$g = \begin{pmatrix} a(-\mu+1) & b \\ a\mu & d \end{pmatrix}.$$

Note that, since $\gamma_1 \cdot \infty = (-\mu+1)/\mu$,

$$\mathrm{Stab}_\Gamma((-\mu+1)/\mu) = \gamma_1 \,\mathrm{Stab}_\Gamma(-\infty)\gamma_1^{-1} = \langle \pm\gamma_1\gamma_3\gamma_1^{-1}\rangle = \langle \pm\gamma_4 \rangle\,,$$

where

$$\gamma_4 = \gamma_1\gamma_3\gamma_1^{-1} = \begin{pmatrix} 1-\mu(-\mu+1) & (-\mu+1)^2 \\ -\mu^2 & 1+\mu(-\mu+1) \end{pmatrix}.$$

It is easy to check that

$$\gamma_4^n = \begin{pmatrix} 1-n\mu(-\mu+1) & n(-\mu+1)^2 \\ -n\mu^2 & 1+n\mu(-\mu+1) \end{pmatrix}.$$

Since $\tau \nmid \mu$, it follows that

$$\mathrm{Stab}_{\Gamma^{(0)}}((-\mu+1)/\mu) = \langle \pm\gamma_4^p \rangle.$$

Note that $g\gamma_3 g^{-1} \cdot \frac{-\mu+1}{\mu} = \frac{-\mu+1}{\mu}$ and, thus,

$$\begin{pmatrix} * & a^2(-\mu+1) \\ & \\ * & * \end{pmatrix} = g\gamma_3 g^{-1} = \pm\gamma_4^{pn}$$

for some $n \in \mathbb{Z}$.

Therefore

$$a^2 = \pm np(-\mu+1).$$

Since $g^{-1}\gamma_4^p g \cdot \infty = \infty$,

$$g^{-1}\gamma_4^p g = \pm\gamma_3^m$$

for some $m \in \mathbb{Z}$.

Hence,

$$\gamma_3 = \pm\gamma_3^{mn}.$$

This implies that $n = m = \pm 1$ and either

$$g\gamma_3 g^{-1} = \gamma_4^{pn} \text{ and } g^{-1}\gamma_4^p g = \gamma_3^m$$

or

$$g\gamma_3 g^{-1} = -\gamma_4^{pn} \text{ and } g^{-1}\gamma_4^p g = -\gamma_3^m.$$

In any case, $a = \pm\sqrt{p(\mu-1)}$. Since all matrices are being viewed in $\mathrm{PSL}_2(\mathbb{R})$, there is no loss of generality in assuming that

$$a = \sqrt{p(\mu-1)},$$

that is,

$$g = \begin{pmatrix} \sqrt{p(\mu-1)}(-\mu+1) & b \\ \sqrt{p(\mu-1)}\mu & d \end{pmatrix}$$

Now,

$$\begin{pmatrix} 1 + d\sqrt{p(\mu-1)}\mu & d^2 \\ * & * \end{pmatrix} = g^{-1}\gamma_3 g \in \Gamma^{(0)}$$

implies that

$$d\sqrt{p(\mu-1)}, d^2 \in \mathbb{Z}[\mu].$$

The first containment says that

$$d = \frac{r'}{\sqrt{p(\mu-1)\mu}}$$

for some $r' \in \mathbb{Z}[\mu]$. The second would then imply that

$$d^2 = \frac{r'^2}{p(\mu-1)\mu^2} \in \mathbb{Z}[\mu].$$

Since $\mathbb{Z}[\mu]$ is assumed to be a UFD, it follows that

$$p \mid r' \text{ and } \mu \mid r'$$

and, so,

$$r = \frac{r\sqrt{p}}{\sqrt{\mu-1}}.$$

The lemma is finished then by taking into account that

$$\det(g) = 1.$$

□

The next lemma proves the fourth claim stated in the the proof of Theorem 3.3.12.

Lemma 3.3.18. *There is no $g \in N(\Gamma^{(0)})$ such that $g \cdot \infty = \frac{-\mu+1}{\mu}$.*

Proof. By the previous lemma, any such g would be of the form

$$g = \begin{pmatrix} \sqrt{p(\mu-1)}(-\mu+1) & \frac{1}{(\mu-1)^{3/2}}\left(\frac{1}{\sqrt{p}} - r\mu\sqrt{p}\right) \\ \sqrt{p(\mu-1)}\mu & \frac{r\sqrt{p}}{\sqrt{\mu-1}} \end{pmatrix}.$$

Note that

$$\gamma := \begin{pmatrix} 1 - n_0\mu(n_0\mu+1) & -n_0^2\mu \\ \mu(n_0\mu+1)^2 & 1+n_0\mu(n_0+1) \end{pmatrix} = (\gamma_2\gamma_3^{-n_0})\gamma_2^{-1}(\gamma_2\gamma_3^{-n_0})^{-1} \in \Gamma^{(0)}.$$

Therefore

$$\left(\begin{smallmatrix} * & B \\ * & * \end{smallmatrix}\right) = g\gamma g^{-1} \in \Gamma^{(0)}$$

and, in particular,

$$B \in \mathbb{Z}[\mu].$$

Computing B yields

$$B = B_0 + \frac{\mu(n_0\mu+1)^2}{(\mu-1)p},$$

where $B_0 \in \mathbb{Z}[\mu]$.

Since

$$p \nmid \mu \text{ and } p \nmid (n_0\mu + 1),$$

that contradicts the fact that $B \in \mathbb{Z}[\mu]$. □

The next lemma proves the fifth claim stated in the the proof of Theorem 3.3.12.

Lemma 3.3.19. *Let n_0 be as in Proposition 3.3.11. Then*

$$\gamma_2{\gamma_3}^{-n_0} \begin{pmatrix} 0 & 1/\sqrt{\mu} \\ -\sqrt{\mu} & 0 \end{pmatrix} \in \Gamma^{(0)}(\mathfrak{p}).$$

Moreover its action on $\mathcal{C}(\Gamma^{(0)}(\mathfrak{p}))$ is given by

$$\begin{array}{lcl} [\infty] & \longmapsto & [\gamma_2{\gamma_3}^{-n_0} \cdot 0] \\ [\frac{-\mu+1}{\mu}] & \longmapsto & [0] \\ [0] & \longmapsto & [\frac{-\mu+1}{\mu}] \\ [\gamma_2{\gamma_3}^{-n_0} \cdot 0] & \longmapsto & [\infty]. \end{array}$$

Proof. By Theorem 3.3.6,

$$g := \begin{pmatrix} 0 & 1/\sqrt{\mu} \\ -\sqrt{\mu} & 0 \end{pmatrix} \in N(\Gamma_{q,\infty,\infty}).$$

It is therefore clear that $h := \gamma_2{\gamma_3}^{-n_0} g \in N(\Gamma_{q,\infty,\infty})$. Hence, in order to show it is in the normalizer of $\Gamma^{(0)}(\tau)$, it suffices to show that if $\gamma =$

$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma^{(0)}(\tau)$, then the $(2,1)$-entry of $h\gamma h^{-1}$ is a multiple of τ. A simple computation shows that

$$h\gamma h^{-1} = \begin{pmatrix} * & * \\ \mu(n_0\mu+1)(a-(n_0\mu+1)b-d)+\mu c & * \end{pmatrix},$$

Since $\tau \mid (n_0\mu+1)$ (by Lemma 3.3.7) and $\tau \mid c$ (by the assumption that $\gamma \in \Gamma^{(0)}(\tau)$), it follows that the $(2,1)$-entry is a multiple of τ.

For the action of h on $\mathcal{C}(\Gamma^{(0)}(\mathfrak{p}))$, the key information is that the action of g (and, thus, of h) on $\mathcal{C}(\Gamma_{q,\infty,\infty})$ is given by:

$$\begin{array}{ccc} [\infty] & \longmapsto & [0] \\ [0] & \longmapsto & [\infty]. \end{array}$$

Because of this, the action of h on $\mathcal{C}(\Gamma^{(0)}(\mathfrak{p}))$ has to send a cusp above ∞ to a cusp above 0 and vice-versa. The definition of h shows that it will send $[\infty]$ to $[\gamma_2\gamma_3^{-n_0}\cdot 0]$. Therefore, it will send $[\frac{-\mu+1}{\mu}]$ to $[0]$. Finally, Claim 3 in the proof of Theorem 3.3.12 shows that h will send $[0]$ to $[\frac{-\mu+1}{\mu}]$ and, thus, it will send $[\gamma_2\gamma_3^{-n_0}\cdot 0]$ to $[\infty]$. □

3.3.2 Final remarks

Theorem 3.3.12 completely characterizes the normalizer of $\Gamma_{q,\infty,\infty}(\mathfrak{p})$ when $\mathfrak{p}$ sits above a split prime p: namely those groups have only one non-trivial normalizer and it comes from the non-trivial normalizer of $\Gamma_{q,\infty,\infty}$. What happens when p is an inert prime is not clear. In fact, the next example shows a possible member of the normalizer of $\Gamma_{5,\infty,\infty}(7)$ which does not come from the normalizer of $\Gamma_{5,\infty,\infty}$.

Example 4. We now try to understand a specific example when p is inert. Here we take $q = 5$ and $p = 7$ and study the normalizer of $\Gamma_{5,\infty,\infty}(7)$.

The first remark is that, just like in the split case, the group $\Gamma_{5,\infty,\infty}(7)$ has a non-trivial normalizer coming from a normalizer of $\Gamma_{5,\infty,\infty}$. In fact, using a computer algebra system one can check that

$$\gamma_2^4\gamma_3^6\gamma_2\gamma_3 \begin{pmatrix} 0 & 1/\sqrt{\mu} \\ -\sqrt{\mu} & 0 \end{pmatrix} = \sqrt{\mu} \begin{pmatrix} 6\mu - 7 & -\frac{1}{5}\mu - 5 \\ -91\mu + 119 & 24\mu - 5 \end{pmatrix}$$

is indeed a normalizer of $\Gamma_{5,\infty,\infty}(7)$. This can be done by finding a list of generators of $\Gamma_{5,\infty,\infty}(7)$ and checking that every generator, when conjugated the above element, remains in $\Gamma_{5,\infty,\infty}(7)$ (that is, its (2,1)-entry is a multiple of 7). Using the same computer algebra system, we can show that this is in fact the only normalizer coming from the normalizer of $\Gamma_{5,\infty,\infty}$ (this is done by finding a list of representatives of the cosets of $\Gamma_{5,\infty,\infty}(7)\backslash\Gamma_{5,\infty,\infty}$).

Now, contrary to the split case, there are other elements that are strong candidates for being in the normalizer but for which we cannot prove one way or another. One such element is the following:

$$\begin{pmatrix} \sqrt{7} & \frac{1}{\mu\sqrt{7}} - \frac{3\sqrt{7}}{\mu} \\ -\mu\sqrt{7} & 3\sqrt{7} \end{pmatrix}.$$

To find this element, we investigated if it would be possible to have an element $h \in N(\Gamma^{(0)}_{5,\infty,\infty}(7))$ such that $h{\cdot}\infty = -1/\mu$ in the same spirit of Lemma 3.3.17. After that, we were not able to show that such normalizers do not exist (as was proved in Lemma 3.3.18 for the split case) and, in fact, found this possible candidate for being in the normalizer.

We would like to make one last observation regarding cusps. As mentioned at the beginning of the previous section, a similar study for the Hecke triangle group $\Gamma_{2,5,\infty}$ was conducted in [LT99]. The results there were proved using the fact that the set of cusps of $\Gamma_{2,5,\infty}$ is known explicitly (cf. [Leu67] and [Leu74]). On the other hand, the results from the previous section were obtained without using any description of the set of cusps of $\Gamma_{5,\infty,\infty}$. In fact, to the best of our knowledge, there is no known explicit description of that set. It would be interesting to study whether the results from the previous section can say something about that set.

Chapter 4

The TTV family of curves

In [Dar00], H. Darmon constructed Frey representations (cf. definition 1.1 in [Dar00] and definition 8 in [Dar04]) associated to the triangle groups $\Gamma_{q,\infty,\infty}$ with the use of two families of hyperelliptic curves:

$$\begin{aligned} C_q^-(t) &\;:\; y^2 = h(x) + 2 - 4t \\ C_q^+(t) &\;:\; y^2 = (x+2)(h(x) + 2 - 4t), \end{aligned} \tag{4.1}$$

where

$$h(x) = xg(x^2-2) = g(-x)^2(x-2) + 2 = g(x)^2(x+2) - 2,$$

$g(x)$ is the minimal polynomial of $-\zeta_q - \zeta_q^{-1}$, for ζ_q a primitive q-th root of unity over $\mathbb{Q}$. These curves were originally studied in [TTV91], where it was shown that their Jacobians have real multiplication by $\mathcal{O}_L$, the ring of integers of $L = \mathbb{Q}(\zeta_q)^+ = \mathbb{Q}(\zeta_q + \zeta_q^{-1})$.

In this chapter we will study the family of curves $C_5^{\pm}(t)$:

$$\begin{aligned} C_5^-(t) &: \quad y^2 = x^5 - 5x^3 + 5x + (2-4t) \\ C_5^+(t) &: \quad y^2 = (x+2)(x^5 - 5x^3 + 5x + (2-4t)). \end{aligned} \tag{4.2}$$

(which will be referred to as $C_t^{\pm}$ to simplify notation). In the first section, we will investigate how they sit in the moduli space of genus 2 curves studied by Igusa (cf. [Igu60]). In the following section, we study the modular embedding defined by them into the moduli space $\mathrm{SL}_2(\mathcal{O}, \mathcal{O}^*)\backslash\mathcal{H}^2$ of Abelian surfaces having RM by an order $\mathcal{O}$ in a totally real quadratic field.

4.1 Invariants

In this section we compute the Igusa-Clebsch invariants of $C_5^{\pm}(t)$. We, then, obtain the degree of the map from $\mathbb{P}^1\backslash\{0, 1, \infty\}$ into the moduli space of genus 2 curves defined by the families defined in (4.2).

4.1.1 Igusa-Clebsch invariants

Following Section 2.2 of [GL12], we recall the definition of the Igusa-Clebsch invariants.

Let

$$y^2 = f(x) = u_0x^6 + u_1x^5 + \cdots + u_5x + u_6$$

be a hyperelliptic curve. Denote by $x_1, x_2, \ldots, x_6$ the roots of $f(x)$. In what follows, (ij) is a notation for $(x_i - x_j)$. The *Igusa-Clebsch invariants* are defined to be

$$\begin{aligned} A &= u_0^2 \sum_{\text{fifteen}} (12)^2(34)^2(56)^2, \\ B &= u_0^4 \sum_{\text{ten}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2, \\ C &= u_0^6 \sum_{\text{sixty}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2, \text{ and} \\ D &= u_0^{10} \sum_{i<j} (ij)^2. \end{aligned} \tag{4.3}$$

The subscript “fifteen” in A refers to the fact that there are 15 ways of partition 6 objects into 3 groups of 2 elements, the subscript “ten” in B refers to the fact that there are 10 ways to partition 6 objects into 2 groups of 3 elements. Finally, the subscript “sixty” refers to partitioning 6 objects into 2 groups and then finding a matching between those 2 groups.

In [GL12], it is explained that those invariants belong to the weighted projective space $\mathbb{P}^3_{2,4,6,10}$ and completely determine the genus 2 curve. In other words, let A_1, B_1, C_1, D_1 and A_2, B_2, C_2, D_2 be the Igusa-Clebsch invariants of two curves, then those two curves are isomorphic if, and only if, there is a non-zero r such that

$$A_1 = r^2 A_2 \ , \ B_1 = r^4 B_2 \ , \ C_1 = r^6 C_2 \ \text{ and } \ D_1 = r^{10} D_2.$$

4.1.2 Computing the Igusa-Clebsch invariants

Proposition 4.1.1. *The Igusa-Clebsch invariants of the hyperelliptic curve*

$$y^2 = x^5 - 5x^3 + 5x + (2 - 4t) \tag{4.4}$$

are

$$\begin{aligned}
A &= 350 = 2 \cdot 5^2 \cdot 7, \\
B &= 2500 = 2^2 \cdot 5^4, \\
C &= -11250(2-4t)^2 + 295000 = -2^4 \cdot 5^4 \cdot (18t^2 - 18t - 25), \ \textit{and} \\
D &= 3125(2-4t)^4 - 25000(2-4t)^2 + 50000 = 2^8 \cdot 5^5 \cdot t^2 \cdot (t-1)^2.
\end{aligned}$$

In particular, the map from $\mathbb{P}^1 \backslash \{0, 1, \infty\}$ to the moduli space of genus 2 curves defined by (4.4) is $2:1$.

Proof. To use the definition of the Igusa-Clebsch invariants given in (4.3), we must have a degree 6 polynomial. For this reason, we first remark that the curve

$$y^2 = x^5 - 5x^3 + 5x + (2 - 4t),$$

is isomorphic to

$$y^2 = f(x) = (2 - 4t)x^6 + 5x^5 - 5x^3 + x,$$

which can be seen, for instance, as a consequence of Proposition 7.4.24 in [LE06].

Now, from (4.3), it is clear that A, B, C, and D are symmetric polynomials in the roots of $f(x)$. Since $f(x)$ is known

$$f(x) = tx^6 + 5x^5 - 5x^3 + x,$$

the elementary symmetric polynomials in the roots of $f(x)$ are also explicitly known:

$$s_1 = -5/(2 - 4 * t), \qquad s_2 = 0, \qquad s_3 = 5/(2 - 4 * t),$$

$$s_4 = 4, \qquad s_5 = -1/(2 - 4 * t), \qquad s_6 = 0.$$

Therefore, by the Fundamental Theorem of Symmetric Polynomials, it is possible to compute the Igusa-Clebsch invariants explicitly.

The values of A, B, C, and D were computed using the computer algebra system Sage [S$^+$12] and an algorithm given in Section 26 of [vdW49]. $\square$

Proposition 4.1.2. *The Igusa-Clebsch invariants of the hyperelliptic curve*

$$y^2 = (x+2)(x^5 - 5x^3 + 5x + (2-4t)) \tag{4.5}$$

are

$$\begin{aligned} A &= 2^3 \cdot 5^2, \\ B &= 2^2 \cdot 5^4 \cdot (4t-5)^2, \\ C &= 2^3 \cdot 5^4 \cdot (4512t^3 - 9712t^2 + 2500t + 3125), \text{ and} \\ D &= 2^{12} \cdot 5^5 \cdot t^4 \cdot (t-1)^2. \end{aligned}$$

In particular, the map from $\mathbb{P}^1 \backslash \{0, 1, \infty\}$ to the moduli space of genus 2 curves defined by (4.5) is $1:1$.

Proof. The invariants A, B, C and D were computed using the same method as in the previous proposition. The fact that it therefore defines a $1:1$ map can be checked manually. □

4.2 Modular embedding

We start with a review the moduli space of Abelian surfaces with Real Multiplication. Then we proceed to the computation of the Jacobians of the TTV curves and study how they sit in that moduli space.

4.2.1 Moduli space of Abelian surfaces with Real Multiplication

Let us start fixing the notation. Throughout this chapter,

$$L = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}) \quad , \quad \mathcal{O} = \mathcal{O}_L = \mathbb{Z}\left[\lambda\right],$$

where

$$\lambda = \frac{1+\sqrt{5}}{2}.$$

Notice that L is a totally real field of degree 2. Given $x \in L$, we denote

$$x^{(i)} = i\text{-th embedding of } x \text{ in } \mathbb{R}.$$

As usual, $\mathcal{O}^*$ will denote the dual of $\mathcal{O}$ with respect to the trace, i.e.,

$$\mathcal{O}^* = \{r \in L \mid \mathrm{Tr}_{L/\mathbb{Q}}(rx) \in \mathbb{Z} \text{ for all } x \in \mathcal{O}\},$$

which in our case is given by

$$\mathcal{O}^* = \frac{1}{\sqrt{5}}\mathcal{O}.$$

Moreover

$$\mathrm{SL}_2(\mathcal{O},\mathcal{O}^*) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(L) \mid a, d \in \mathcal{O}, c \in \mathcal{O}^*, b \in (\mathcal{O}^*)^{-1} \right\}.$$

There is a natural action of $\mathrm{SL}_2(\mathcal{O},\mathcal{O}^*)$ on $\mathcal{H}^2$ as follows: let $z = (z_1, z_2) \in \mathcal{H}^2$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O},\mathcal{O}^*)$, then

$$\gamma \cdot z := \left(\gamma^{(1)} z_1, \gamma^{(2)} z_2\right),$$

where

$$\gamma^{(i)} := \begin{pmatrix} a^{(i)} & b^{(i)} \\ c^{(i)} & d^{(i)} \end{pmatrix}$$

and

$$\gamma^{(i)} z_i := \frac{a^{(i)} z_i + b^{(i)}}{c^{(i)} z_i + d^{(i)}}.$$

In this section we briefly explain how $\mathrm{SL}_2(\mathcal{O},\mathcal{O}^*)\backslash\mathcal{H}^2$ parametrizes Abelian surfaces with real multiplication (RM) by $\mathbb{Z}[(1+\sqrt{5})/2]$. For details, consult [Gor02] and [HvdG81].

We first explain the map

$$\mathrm{SL}_2(\mathcal{O},\mathcal{O}^*)\backslash\mathcal{H}^2 \longrightarrow \{\text{Abelian surfaces with RM by } \mathcal{O}\}.$$

Given $z = (z_1, z_2) \in \mathcal{H}^2$, we can construct

$$\begin{array}{rclc} L_z & : & L \oplus L & \longrightarrow & \mathbb{C}^2 \\ & & (\alpha, \beta) & \longmapsto & \alpha z + \beta := \left(\alpha^{(1)} z_1 + \beta^{(1)}, \alpha^{(2)} z_2 + \beta^{(2)}\right) \end{array}.$$

Taking $M = \mathcal{O} \oplus \mathcal{O}^*$, define the lattice

$$\Lambda_z := L_z(M) \subseteq \mathbb{C}^2.$$

So

$$\begin{array}{ccc} \mathrm{PSL}_2(\mathcal{O}, \mathcal{O}^*)\backslash\mathcal{H}^2 & \longrightarrow & \text{Abelian surfaces with RM by } \mathcal{O} \\ z & \longmapsto & A_z := \mathbb{C}^2/\Lambda_z. \end{array}$$

A few remarks about this construction:

1. $\Lambda_z = \mathbb{Z}\left(\frac{1}{\sqrt{5}}, -\frac{1}{\sqrt{5}}\right) \oplus \mathbb{Z}\left(\frac{\lambda^{(1)}}{\sqrt{5}}, -\frac{\lambda^{(2)}}{\sqrt{5}}\right) \oplus \mathbb{Z}\left(z_1, z_2\right) \oplus \mathbb{Z}\left(\lambda^{(1)} z_1, \lambda^{(2)} z_2\right)$.

2. The RM by $\mathcal{O}$ structure on A_z is given by

$$\begin{array}{ccc} \mathcal{O} & \longrightarrow & \mathrm{End}(A_z) \\ r & \longmapsto & \Bigg((x_1, x_2) \mapsto (r^{(1)} x_1, r^{(2)} x_2)\Bigg). \end{array}$$

   Notice that with this action, $r \cdot \Lambda_z = \Lambda_z$ for all $r \in \mathcal{O}$, as it should.

3. With the action of $\mathcal{O}$ on A_z, we have that

$$\Lambda_z = \mathcal{O} \cdot (z_1, z_2) \oplus \mathcal{O}^* \cdot (1, 1),$$

that is, every element $w \in \Lambda_z$ can be written as

$$w = \left(r^{(1)} z_1 + \frac{s^{(1)}}{\sqrt{5}} \ , \ r^{(2)} z_2 - \frac{s^{(2)}}{\sqrt{5}} \right)$$

for some $r, s \in \mathcal{O}$.

Now we are ready to explain the map in the opposite direction:

$$\{\text{Abelian surfaces with RM by } \mathcal{O}\} \longrightarrow \mathrm{SL}_2(\mathcal{O}, \mathcal{O}^*) \backslash \mathcal{H}^2.$$

Let $A = \mathbb{C}^2/\Lambda$ be an Abelian surface with RM by $\mathcal{O}$. Up to isomorphism, we can assume that the action of $\mathcal{O}$ on A is given by

$$r \cdot (x_1, x_2) = (r^{(1)} x_1, r^{(2)} x_2).$$

Since this action has to send Λ to Λ, we obtain that Λ is an $\mathcal{O}$-module. Since it is a lattice of rank 4 without torsion,

$$\Lambda = \mathcal{O} \cdot (v_1, v_2) \oplus \mathcal{O}^* \cdot (w_1, w_2)$$

for some $(v_1, v_2), (w_1, w_2) \in \mathbb{C}^2$.

Note that we must have $v_1, v_2, w_1, w_2 \neq 0$ because otherwise Λ would not have rank 4.

Now we can consider the linear map

$$\begin{aligned} \varphi \ : \quad \mathbb{C}^2 & \longrightarrow \quad \mathbb{C}^2 \\ (x_1, x_2) & \longmapsto (x_1/w_1, x_2/w_2) \end{aligned}$$

or in matrix form

$$\varphi = \begin{pmatrix} 1/w_1 & 0 \\ 0 & 1/w_2 \end{pmatrix}.$$

This map induces an isomorphism (which we still call φ)

$$\varphi \ : \ \mathbb{C}^2/\left(\mathcal{O}(v_1, v_2) \oplus \mathcal{O}^*(w_1, w_2)\right) \ \longrightarrow \ \mathbb{C}^2/\left(\mathcal{O}(z_1, z_2) \oplus \mathcal{O}^*(1, 1)\right)$$

which preserves the action of $\mathcal{O}$ of both sides, i.e.,

$$\varphi(r(x_1, x_2)) = r \cdot \varphi(x_1, x_2),$$

where $(z_1, z_2) = (v_1/w_1, v_2/w_2)$.

Now we just need to check whether $(z_1, z_2) \in \mathcal{H}^2$. From its construction we just have $z_i \in \mathcal{H}^{\pm}$. If they are both in $\mathcal{H}^+$ or both in $\mathcal{H}^-$, this is not a problem because $\mathcal{O}(z_1, z_2) = \mathcal{O}(-z_1, -z_2)$.

If one of them belongs to $\mathcal{H}^+$ and the other to $\mathcal{H}^-$, we use λ: since $\lambda \in \mathcal{O}^{\times}$,

$$\mathcal{O}(z_1, z_2) = \mathcal{O}(\lambda^{(1)} z_1, \lambda^{(2)} z_2)$$

but λ has the nice property that one of its embeddings in $\mathbb{R}$ is positive and the other one is negative.

4.2.2 Jacobians of the TTV curves

In this section we study the Jacobians of the curves $C_t^{\pm} := C_5^{\pm}(t)$ defined in (4.2). We start with

$$C_t^- : y^2 = x^5 - 5x^3 + 5x + (2 - 4t).$$

First, recall that the Jacobian of C_t^- is defined by

$$J(C_t^-) = \frac{\Omega_1(C_t^-)^*}{\Lambda},$$

where $\Omega_1(C_t^-)^*$ is the space of linear functionals from $\Omega_1(C_t^-)$ to $\mathbb{C}$ and

$$\Lambda = \left\{ \int_\gamma \;\middle|\; \gamma \in H_1(C_t^-, \mathbb{Z}) \right\}.$$

It is well known (cf. Prop. 7.4.26 in [LE06]) that

$$\Omega_1(C_t^-) = \left\langle \frac{dx}{y} \;,\; x\frac{dx}{y} \right\rangle.$$

So, via the identification

$$\begin{array}{ccc} \Omega_1(C_5^-(t))^* & \longrightarrow & \mathbb{C}^2 \\ \psi & \longmapsto & \left(\psi(\frac{dx}{y}) \;,\; \psi(x\frac{dx}{y})\right) \end{array} \tag{4.6}$$

we have that

$$J(C_t^-) = \frac{\mathbb{C}^2}{\Lambda},$$

where

$$\Lambda = \left\{ \left(\int_\gamma \frac{dx}{y}, \int_\gamma x\frac{dx}{y} \right) \;\middle|\; \gamma \in H_1(C_t^-, \mathbb{Z}) \right\}.$$

Let $\alpha := \zeta_5 + \zeta_5^{-1} \in L = \mathbb{Q}(\sqrt{5})$. Recall that $\mathcal{O} = \mathcal{O}_L = \mathbb{Z}[\alpha]$.

Lemma 4.2.1. *The Jacobian $J(C_t^-)$ has RM by $\mathcal{O}$.*

$$\begin{array}{rcl} \alpha \cdot \frac{dx}{y} & = & (e^{2\pi i/5} + e^{-2\pi i/5})\frac{dx}{y}, \\ \alpha \cdot x\frac{dx}{y} & = & (e^{4\pi i/5} + e^{-4\pi i/5})x\frac{dx}{y}. \end{array} \tag{4.7}$$

In particular, using the identification (4.6) and the conventions from the previous section, the action of any $r \in \mathcal{O}$ is given by

$$r \cdot (x_1, x_2) = \left(r^{(1)}x_1 \ , \ r^{(2)}x_2 \right).$$

Proof. Cf. [TTV91] and fact 17 below. □

Our goal in this section is to describe the points

$$(z_1, z_2) \ \in \ \mathrm{SL}_2(\mathcal{O}, \mathcal{O}^*)\backslash\mathcal{H}^2$$

that represent the Jacobians $J(C_t^-)$ of the TTV family. By the previous section, we only need to write

$$\Lambda = \mathcal{O} \cdot (-,-) \oplus \mathcal{O}^* \cdot (-,-).$$

We know that Λ is generated (as a $\mathbb{Z}$-module) by

$$\int_{a_1} \quad , \quad \int_{a_2} \quad , \quad \int_{b_1} \quad , \quad \int_{b_2}$$

where $H_1(C_t^-,\ ZZ) = \langle a_1, a_2, b_1, b_2 \rangle$ (generated as a $\mathbb{Z}$-module).

We now need to understand how $\mathcal{O}$ acts on the elements of Λ (not only how it acts on Λ as a subset of $\Omega^1(C_t^-)^*$), that is, how $\mathcal{O}$ transforms elements of Λ into other elements of Λ. In other words, we want to know how to write

$$\left(\int_\gamma r \cdot \frac{dx}{y} \ , \ \int_\gamma r \cdot x \frac{dx}{y} \right)$$

(for all $\gamma \in \{a_1, a_2, b_1, b_2\}$) as a $\mathbb{Z}$-combination of

$$\left(\int_{a_i} \tfrac{dx}{y} \ , \ \int_{a_i} x \tfrac{dx}{y} \right) \quad \text{and} \quad \left(\int_{b_i} \tfrac{dx}{y} \ , \ \int_{b_i} x \tfrac{dx}{y} \right)$$

for $i = 1, 2$. For this, we need to understand the curves C_t^- in more detail. Let us first recall some facts about C_t^- that were proved in [TTV91].

Fact 14. *The curve C_t^- is a quotient of*

$$D_t^- \quad : \quad y^2 = x(x^{10} + (2 - 4t)x^5 + 1)$$

by the involution

$$\sigma \quad : \quad (x, y) \mapsto \left(\tfrac{1}{x}, \tfrac{y}{x^6} \right)$$

and the projection map is given by

$$\begin{array}{rcccc} \varphi & : & D_t^- & \longrightarrow & C_t^- \\ & & (x,y) & \longmapsto & \left(x+\frac{1}{x}, \frac{y}{x^3}\right). \end{array}$$

Fact 15. *The map φ induces an injection*

$$\varphi^* \;\; : \;\; \Omega^1(C_t^-) \;\; \longrightarrow \;\; \Omega^1(D_t^-).$$

Fact 16. *There is an automorphism ζ_5 of D_t^- defined by:*

$$\zeta_5 \cdot (x,y) = (\zeta x, \zeta^3 y) \quad , \quad \textit{where } \zeta = \exp(2\pi i/5) \in \mathbb{C}$$

that defines an action of $\mathbb{Z}[\zeta_5]$, the ring of integers of the 5-th cyclotomic field, on the Jacobian $J(D_t^-)$.

Fact 17. *Under the injection φ^*, the Jacobian $J(C_t^-)$ inherits multiplication by $\mathbb{Z}[\alpha]$ (where, again, $\alpha = \zeta_5 + \zeta_5^{-1}$). That is, if $\omega \in \Omega^1(C_t^-)$, then*

$$[\alpha] \cdot (\varphi^* \omega) \;\in\; \varphi^*(\Omega^1(C_t^-)),$$

where $[\alpha]$ denotes the action of $\alpha \in O_K$ in $\Omega^1(D_t^-)$. More precisely,

$$[\alpha] \cdot \left(\varphi^* \tfrac{dx}{y}\right) = \alpha^{(1)} \left(\varphi^* \tfrac{dx}{y}\right) \quad \textit{and} \quad [\alpha] \cdot \left(\varphi^* x \tfrac{dx}{y}\right) = \alpha^{(2)} \left(\varphi^* x \tfrac{dx}{y}\right)$$

where

$$\alpha^{(1)} = \exp(2\pi i/5) + \exp(2\pi i/5)^{-1} \;\; \textit{and} \;\; \alpha^{(2)} = \exp(4\pi i/5) + \exp(4\pi i/5)^{-1}.$$

In particular, we obtain that (4.7) holds.

Fact 17 shows how $\mathcal{O}$ acts on $\Omega^1(C_t^-)^*$. In order to understand how it acts on Λ, we need to fix a basis for $H_1(C_t^-, \mathbb{Z})$. To do that, we will first consider a convenient model for the hyperelliptic curves D_t^- and C_t^-. We will then see how to naturally choose a basis for $H_1(D_t^-, \mathbb{Z})$ and $H_1(C_t^-, \mathbb{Z})$.

Note that the ramification points of D_t^- (with respect to the x-projection, i.e., the map $D_t^- \to \mathbb{P}^1$ given by $(x, y) \longmapsto x$) are given by:

$$\infty \ , \ (0,0) \ , \ (\zeta^i c^+, 0) \ , \ (\zeta^i c^-, 0)$$

where $i = 0, 1, \ldots, 4$, $\zeta = \exp(2\pi i/5)$ and c^+ and c^- are complex numbers.

Let us call

$$e_1 = (\zeta c^-, 0) \quad , \quad e_3 = (\zeta^2 c^-, 0) \quad , \quad \ldots \quad , \quad e_9 = (\zeta^5 c^-, 0) = (c^-, 0) \ ,$$

$$e_2 = (\zeta c^+, 0) \quad , \quad e_4 = (\zeta^2 c^+, 0) \quad , \quad \ldots \quad , \quad e_{10} = (\zeta^5 c^+, 0) = (c^+, 0) \ ,$$

and

$$e_{11} = (0,0) \quad , \quad e_{12} = \infty.$$

Following pp. 96-97 of [FK92], we can consider a model for D_t^- consisting of two copies of $\mathbb{P}^1$ connected via "cuts" from e_{2i-1} to e_{2i} and define the following basis for $H_1(D_t)$:

$$a_i = \text{curve around the cut } e_{2i-1}e_{2i}$$

and

b_i = curve starting at the cut $e_{11}e_{12}$, going to the cut $e_{2i-1}e_{2i}$, and going back to the initial cut through the other branch.

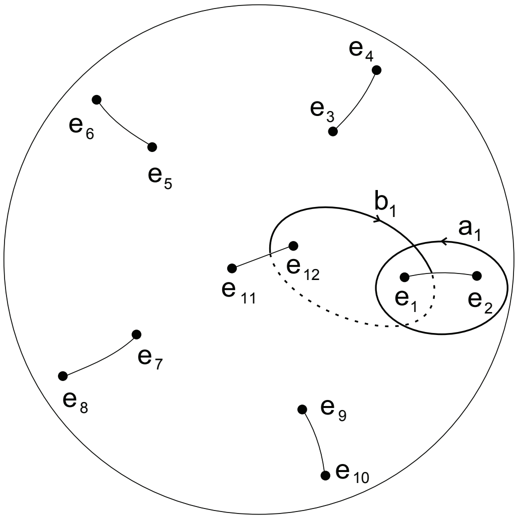

Figure 4.1: Basis for $H_1(D_t^-, \mathbb{Z})$

In figure 4.1, we show a_1 and b_1 drawn on the aforementioned model. It is now clear that the lemma below holds.

Lemma 4.2.2. *The element ζ_5 acts as following on $H_1(D_t^-, \mathbb{Z})$:*

$$(\zeta_5)_* a_1 = a_2 \quad , \quad (\zeta_5)_* a_2 = a_3 \quad , \quad \ldots \quad ,$$

$$(\zeta_5)_* b_1 = b_2 \quad , \quad (\zeta_5)_* b_2 = b_3 \quad , \quad \ldots$$

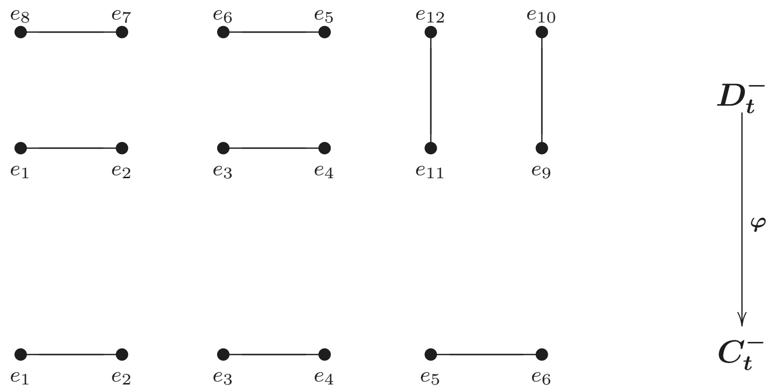

Figure 4.2: Where φ sends the ramification points of D_t^-

It can be easily checked that φ fits in the following commutative diagram

$$\begin{tikzcd}
D_t^- \arrow[r, "\varphi"] \arrow[d] & C_t^- \arrow[d] \\
\mathbb{P}^1 \arrow[r, "x \longmapsto x+1/x"'] & \mathbb{P}^1
\end{tikzcd} \tag{4.8}$$

where the vertical arrows are just the x-projections of D_t^- and C_t^-.

By abuse of notation, we also denote by e_i the ramification points of C_t^- and by a_i and b_i the basis of $H_1(C_t^-, \mathbb{Z})$ analogous to the one constructed for $H_1(D_t^-, \mathbb{Z})$. So the ramification points of D_t^- are mapped to the ramification points of C_t^- as shown in image 4.2. Since the ramification points of C_t^- are away from the branch points of the map $x \mapsto x + 1/x$ (see diagram (4.8)), we obtain the following lemma.

Lemma 4.2.3. *The map* $\varphi_* : H_1(D_t^-, \mathbb{Z}) \to H_1(C_t^-, \mathbb{Z})$ *acts as follows:*

$$\varphi_* a_1 = a_1 \quad , \quad \varphi_* a_2 = a_2 \quad , \quad \varphi_* a_3 = a_2 \ ,$$
$$\varphi_* b_1 = b_1 \quad , \quad \varphi_* b_2 = b_2.$$

We can finally understand how $\mathcal{O}$ acts on Λ. Since $\mathcal{O} = \mathbb{Z}[\alpha]$, it suffices to understand how α acts on Λ. Recall that $\alpha = \zeta_5 + \zeta_5^{-1}$. Let $\omega \in \Omega^1(C_t^-)$. Then, using lemmas 4.2.2 and 4.2.3, we obtain

$$\begin{aligned}
\int_{a_2} [\zeta_5] \cdot \omega &= \int_{a_2} (\varphi^*)^{-1} \circ [\zeta_5] \circ \varphi^* \cdot \omega = \int_{\varphi_* a_2} (\varphi^*)^{-1} \circ [\zeta_5] \circ \varphi^* \cdot \omega \\
&= \int_{(\zeta_5)_* (\varphi_*)^{-1} \varphi_* a_2} \varphi^* \cdot \omega = \int_{(\zeta_5)_* a_2} \varphi^* \cdot \omega = \int_{\varphi_* (\zeta_5)_* a_2} \omega = \int_{\varphi_* a_3} \omega \\
&= \int_{a_2} \omega
\end{aligned}$$

and

$$\begin{aligned}
\int_{a_2} [\zeta_5^{-1}] \cdot \omega &= \cdots = \int_{\varphi_* (\zeta_5^{-1})_* a_2} \omega = \int_{\varphi_* a_1} \omega \\
&= \int_{a_1} \omega.
\end{aligned}$$

Therefore

$$\int_{a_2} [\alpha] \cdot \omega = \int_{a_1} \omega + \int_{a_2} \omega \quad , \quad \text{for any } \omega \in \Omega^1(C_t^-, \mathbb{Z}). \tag{4.9}$$

Similarly,

$$\int_{b_2} [\alpha] \cdot \omega = \int_{b_1} \omega + \int_{b_2} \omega \quad , \quad \text{for any } \omega \in \Omega^1(C_t^-, \mathbb{Z}). \tag{4.10}$$

Combining (4.9) and (4.10), we can conclude that

Theorem 4.2.4. *The action of $\mathcal{O}$ on Λ yields the following decomposition:*

$$\Lambda = \mathcal{O} \cdot \int_{a_2} \;\oplus\; \mathcal{O} \cdot \int_{b_2} .$$

In particular, the point

$$(z_1, z_2) \;\in\; \mathrm{SL}_2(\mathcal{O}, \mathcal{O}^*)\backslash\mathcal{H}^2$$

representing $J(C_t^-)$ is given by

$$\left(\delta^{(1)} \frac{\int_{a_2} \frac{dx}{y}}{\int_{b_2} \frac{dx}{y}} \;,\; \delta^{(2)} \frac{\int_{a_2} x\frac{dx}{y}}{\int_{b_2} x\frac{dx}{y}} \right),$$

where $\delta \in \{\pm 1, \pm\lambda\}$.

A very similar result holds for

$$C_t^+ : y^2 = (x+2)(x^5 - 5x^3 + 5x + (2-4t)).$$

The facts about this curve that are used in order to prove that result are the following:

Fact 18. *The curve C_t^+ is a quotient of*

$$D_t^+ \;:\; y^2 = x^{10} + (2-4t)x^5 + 1$$

by the involution

$$\sigma \;:\; (x,y) \mapsto \left(\tfrac{1}{x}, \tfrac{y}{x^5}\right)$$

and the projection map is given by

$$\begin{array}{rclcl} \varphi & : & D_t^+ & \longrightarrow & C_t^+ \\ & & (x,y) & \longmapsto & \left(x+\frac{1}{x}, \left(\frac{1}{x^2}+\frac{1}{x^3}\right)y\right). \end{array}$$

Fact 19. *The map φ induces an injection*

$$\varphi^* \ : \ \Omega^1(C_t^+) \ \longrightarrow \ \Omega^1(D_t^+).$$

Fact 20. *There is an automorphism ζ_5 of D_t^+ defined by:*

$$\zeta_5 \cdot (x,y) = (\zeta x, y) \quad , \quad \textit{where } \zeta = \exp(2\pi i/5) \in \mathbb{C}$$

that defines an action of $\mathbb{Z}[\zeta_5]$, the ring of integers of the 5-th cyclotomic field, on the Jacobian $J(D_t^+)$.

Fact 21. *Under the injection φ^*, the Jacobian $J(C_t^+)$ inherits multiplication by $\mathbb{Z}[\alpha]$ (where, again, $\alpha = \zeta_5 + \zeta_5^{-1}$). That is, if $\omega \in \Omega^1(C_t^+)$, then*

$$[\alpha] \cdot (\varphi^* \omega) \ \in \ \varphi^*(\Omega^1(C_t^+)),$$

where $[\alpha]$ denotes the action of $\alpha \in O_K$ in $\Omega^1(D_t^+)$. More precisely,

$$\begin{array}{rcl} [\alpha] \cdot \left(\varphi^* \frac{dx}{y}\right) & = & \alpha^{(2)} \left(\varphi^* \frac{dx}{y}\right) \ , \ \textit{and} \\ [\alpha] \cdot \left(\varphi^* x \frac{dx}{y}\right) & = & (\alpha^{(1)} + \alpha^{(2)}) \left(\varphi^* \frac{dx}{y}\right) + \alpha^{(1)} \left(\varphi^* x \frac{dx}{y}\right) \end{array}$$

where

$$\alpha^{(1)} = \exp(2\pi i/5) + \exp(2\pi i/5)^{-1} \quad \textit{and} \quad \alpha^{(2)} = \exp(4\pi i/5) + \exp(4\pi i/5)^{-1}.$$

Hypergeometric periods

We finish this chapter with a more detailed description of the points (z_1, z_2) representing the curves C_t^-. More specifically, we will see that the periods of those curves are hypergeometric functions, i.e., they are solutions to hypergeometric differential equations. For this reason they are sometimes called "hypergeometric curves".

Let us define

$$\pi_1(t) := \int_\gamma \frac{dx}{y} \quad \text{and} \quad \pi_2(t) := \int_\gamma x\frac{dx}{y}$$

where $\gamma = \gamma(t) \in H_1(C_t^-)$ is a family of cycles on C_t^-.

Theorem 4.2.5. *The function $\pi_1(t)$ satisfies a hypergeometric differential equation with parameters*

$$a = 3/10 \quad , \quad b = 7/10 \quad , \quad c = 1.$$

The function $\pi_2(t)$ satisfies a hypergeometric differential equation with parameters

$$a = 9/10 \quad , \quad b = 1/10 \quad , \quad c = 1.$$

Proof. The idea is essentially the one found in [Sch].

We show how to deduce the equation satisfied by $\pi_1(t)$. The proof for $\pi_2(t)$ is analogous. Let

$$\omega(t) = \frac{dx}{y} \in \Omega^1(C_t).$$

We claim that

$$\frac{d^2\omega}{dt^2} + \frac{1-2t}{t(1-t)} \cdot \frac{d\omega}{dt} - \frac{21/100}{t(1-t)} \cdot \omega = d(-),$$

which would imply what was stated (to justify differentiation under the integral sign, cf. Section 9.3, Lemma 12 in [BK86]).

In fact, the right-hand side can be taken to be a linear combination of

$$d\left(\tfrac{x^k}{y^3}\right) \quad \text{for } k = 0, 1, \ldots, 6.$$

This computation was carried out using a computer algebra system. For more details on the computation, cf. Section "Brute-force approach" of [Sch].

□

Remark 4.2.6. Unfortunately the method used in the proof of the previous theorem does not yield a degree 2 differential equation if C_t^- is replaced by C_t^+.

There is at least one other instance in the literature where a modular embedding of the sort obtained here was also studied: in 1990, Cohen and

Wolfart [CW90] constructed modular embeddings for all triangle groups. In their study, the Jacobians also have hypergeometric periods. However, the periods associated to the triangle group $\Gamma_{5,\infty,\infty}$ satisfy a hypergeometric differential equation with different parameters, namely:

$$a = 2/5 \quad , \quad b = 2/5 \quad , \quad c = 4/5$$

and

$$a = 1/5 \quad , \quad b = 1/5 \quad , \quad c = 2/5.$$

Chapter 5

The ordinary locus of the TTV family of curves

In this chapter we continue studying the TTV family of curves $C_t^{\pm} := C_5^{\pm}(t)$ defined in (4.1). More specifically, we study the behavior of the reduction modulo p of these curves (and their Jacobians) via the Cartier-Manin matrix.

The first section recalls the basic about the Cartier-Manin matrix theory. The second section proceeds to the study of those curves and, in particular, finds a relation between the non-ordinary locus of that family of curves and the genus of $X_{5,\infty,\infty}^{(0)}(\mathfrak{p})$.

5.1 The Hasse-Witt and Cartier-Manin matrices

This section is mainly based on Chapters 9 and 10 of [Ser58] and [Yui78].

5.1.1 Hasse-Witt matrix

Let k be a perfect field of characteristic $p > 2$ and C a hyperelliptic curve of genus $g > 0$ defined over k. This notion can be defined in a more general context but we will focus on hyperelliptic curves.

Definition 5.1.1. Fix a basis of $H^1(C, \mathcal{O}_C)$. The *Hasse-Witt matrix* of C is the matrix of the p-linear operator $F : H^1(C, \mathcal{O}_C) \to H^1(C, \mathcal{O}_C)$, where F is the Frobenius operator.

Remark 5.1.2. Notice that the Hasse-Witt matrix is dependent on the basis chosen. Because of the p-linearity of the Frobenius operator, if H and H' are Hasse-Witt matrices with respect to different bases, then there is a matrix U such that

$$H' = U^{-1} H U^{(p)},$$

where $U^{(p)}$ is the matrix obtained from U by raising all its entries to the p-th power.

There is another way to essentially define the Hasse-Witt matrix of a curve. This is done in terms of the so called Cartier operator, which is studied in the next section.

5.1.2 Cartier-Manin Matrix

Suppose C is given by

$$y^2 = f(x) \tag{5.1}$$

where $f(x)$ is a polynomial over k without multiple roots of degree $2g+1$.

Every element of Ω^1_C can be written as

$$\omega = d\varphi + \eta^p x^{p-1} dx$$

for some $\varphi, \eta \in k(C)$.

Definition 5.1.3. The *Cartier operator* $\mathscr{C} : H^0(C, \Omega^1_C) \to H^0(C, \Omega^1_C)$ is defined by

$$\mathscr{C}(d\varphi + \eta^p x^{p-1} dx) = \eta dx.$$

Definition 5.1.4. The *Cartier-Manin matrix* is the matrix of the $1/p$-linear operator $\mathscr{C} : H^0(C, \Omega^1_C) \to H^0(C, \Omega^1_C)$.

Remark 5.1.5. Because of the $1/p$-linearity of the operator $\mathscr{C}$, if M and M' are Cartier-Manin matrices with respect to different bases, then there is a matrix U such that

$$M' = U^{-1} M U^{(1/p)},$$

where $U^{(p)}$ is the matrix obtained from U by raising all its entries to the p-th power.

Remark 5.1.6. The Cartier operator, as defined here, is called the *modified Cartier operator* in [Yui78]. Moreover, the definition of the Cartier-Manin matrix given by N. Yui is slightly different (cf. page 381 of of [Yui78]).

The relation between the Hasse-Witt matrix and the Cartier-Manin matrix arises as follows. It is known that $H^0(C, \Omega^1_C)$ is the dual of $H^1(C, \mathcal{O}_C)$. Under this identification, the following result (cf. Prop. 9, Section 10 in [Ser58]) holds.

Proposition 5.1.7. *The map $\mathscr{C} : H^0(C, \Omega^1_C) \to H^0(C, \Omega^1_C)$ is the dual of $F : H^1(C, \mathcal{O}_C) \to H^1(C, \mathcal{O}_C)$.*

N. Yui (cf. pages 380-381 in [Yui78]) gives a concrete way of computing the Cartier-Manin matrix of a curve:

Proposition 5.1.8. *Let C be given by (5.1). Then the Cartier-Manin matrix of C with respect to the basis*

$$\frac{dx}{y}, x\frac{dx}{y}, \ \ldots\ , \ x^{g-1}\frac{dx}{y}$$

of $H^0(C, \Omega^1_C)$ *is given by*

$$N^{(1/p)},$$

where

$$N = (c_{ip-j}) = \begin{pmatrix} c_{p-1} & c_{p-2} & \cdots & c_{p-g} \\ c_{2p-1} & c_{2p-2} & \cdots & c_{2p-g} \\ \cdots & & & \\ c_{gp-1} & c_{gp-2} & \cdots & c_{gp-g} \end{pmatrix},$$

and

$$f(x)^{(p-1)/2} = \sum c_r x^r.$$

5.1.3 Jacobian of C

From now on, k will be a finite field of characteristic $p > 2$.

Recall the following definitions:

Definition 5.1.9. An abelian variety A of dimension g over k is called

- *ordinary* if its p-rank is g, i.e., $\#(A[p]) = p^g$;
- *supersingular* if A is $\overline{k}$-isogenous to a power of a supersingular elliptic curve.

Remark 5.1.10. As explained in Section 3.2 of [Zhu00], if A is supersingular, then $A[p] = 0$. The converse holds if $g = 1$ or 2 but not necessarily if $g > 2$.

Let $J = J(C)$ be the Jacobian of the curve C.

The results below show the relation between the Cartier-Manin matrix of C and J.

Proposition 5.1.11. *The p-rank of J is bounded above by the rank of the Cartier-Manin matrix, i.e., $\sigma \leq \mathrm{rk}(M)$, where $\#(J[p]) = p^\sigma$ and M denotes the Cartier-Manin matrix.*

Proof. This is a corollary of Proposition 10 in Section 11 of [Ser58]. □

Proposition 5.1.12. *Let M be the Cartier-Manin matrix of C and $N = M^{(p)}$. The following holds:*

(a) $\det(N) \neq 0$ *if and only if J is ordinary.*

(b) $N = 0$ if and only if J is a product of supersingular elliptic curves.

(c) If the genus of C is 2, then $N^{(p)}N = 0$ if and only if J is supersingular.

Proof. Cf. [Yui78] (Theorems 3.1 and 4.1), [Nyg81] (Theorem 4.1) and [Man63] (p. 78). □

5.1.4 Curves with real multiplication

Let L be a totally real number field such that $[L : \mathbb{Q}] = g$ and p a prime number that is unramified in L. In this subsection C will denote a projective algebraic curve of genus g and J its Jacobian, which is assumed to have *real multiplication by* $\mathcal{O}_L$, that is, with an embedding of rings

$$\iota : \mathcal{O}_L \longrightarrow \operatorname{End}(J)$$

as explained in definition 2.2.1 of [Gor02].

In this section, the Cartier operator $\mathscr{C}$ (hence, the Cartier-Manin matrix) is studied via the corresponding operator on the Jacobian of C.

C	J
action of $\mathscr{C}$ on $H^0(C, \Omega^1_C)$ action of F on $H^1(C, \mathcal{O}_C)$	action of V on $H^0(J, \Omega^1_J)$ action of F on $H^1(J, \mathcal{O}_J)$

The vector spaces on the left column are isomorphic to the ones on the right column. Furthermore, the semi-linear operators on the left column coincide (via that isomorphism) to the ones on the right column.

Theorem 5.1.13. *As an $\mathcal{O}_L \otimes k$-module, the space $H^1(J, \mathcal{O}_J)$ decomposes* *as*

$$H^1(J, \mathcal{O}_J) = \bigoplus_{\sigma \in B} W_\sigma,$$

where

$$B = \{\sigma : L \to k \mid \sigma \text{ a ring homomorphism}\} \quad \text{and} \quad \dim_k W_\sigma = 1.$$

Moreover, the action of F commutes with the action of $\mathcal{O}_L \otimes k$ and satisfies the following

$$F(W_\sigma) \subseteq W_{\mathrm{Fr} \circ \sigma}.$$

Proof. Cf. Lemma 2.3.1 and Remark 2.2.8 in [GO00]. □

Remark 5.1.14. Being the dual of F, a similar statement holds for the action of V on $H^0(J, \Omega^1_J)$.

Remark 5.1.15. Consider the factorization of p in $\mathcal{O}_L$ given by

$$p\mathcal{O}_L = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Then, it is not hard to see that, with the notation of Theorem 5.1.13, B decomposes as

$$B = B_1 \sqcup B_2 \sqcup \cdots \sqcup B_r,$$

where $\#B_i = f = f(\mathfrak{p}_i/p) = [\mathcal{O}_l/\mathfrak{p}_i : \mathbb{F}_p]$. Furthermore, Fr acts transitively on each B_i, i.e.,

$$B_i = \{\sigma_i = \mathrm{Fr}^f \circ \sigma_i \ , \ \mathrm{Fr} \circ \sigma_i \ , \ \ldots \ , \ \mathrm{Fr}^{f-1} \circ \sigma_i\}.$$

5.2 Studying $C_q^{\pm}(t)$ for $q = 5$

In this section we return to the families of curves defined in (4.1) for the specific value $q = 5$. These curves have genus $g = 2$ and, as was mentioned in the previous chapter, they have real multiplication by $\mathcal{O}_L$ (where $L = \mathbb{Q}(\sqrt{5})$).

Consider a prime $p > 2$ that is unramified in L.

Lemma 5.2.1. *There are only two possibilities for such a p:*

- *p is a product of two primes in $\mathcal{O}_L$ (when $p \equiv 1, 4 \pmod 5$); or*
- *p is inert in $\mathcal{O}_L$ (when $p \equiv 2, 3 \pmod 5$).*

Proof. Cf. (1.1) in Chapter V of [FT93]. □

In this section, to simplify notation, $C_5^-(t)$ and $C_5^+(t)$ will simply be denoted C_t^- and C_t^+ respectively (or simply C^- and C^+). The equations

(4.1) in this case are:

$$C_t^- \quad : \quad y^2 = x^5 - 5x^3 + 5x + 2 - 4t \ , \ \text{and}$$

$$C_t^+ \quad : \quad y^2 = (x+2)(x^5 - 5x^3 + 5x + 2 - 4t).$$

5.2.1 The Cartier-Manin matrix of the curve C^-

Example 3.5 (or the proof of the main result) in [TTV91] shows that the action of $\mathcal{O}_L$ on $H^0(C^-, \Omega^1)$ has two distinct eigenvectors, namely:

$$\frac{dx}{y}, x\frac{dx}{y}$$

Thus, Lemma 5.2.1, Theorem 5.1.13 and the remarks that follow it yield the result below.

Theorem 5.2.2. *The Cartier-Manin matrix of C^- with respect to the basis $\{\frac{dx}{y}, x\frac{dx}{y}\}$ of $H^0(C^-, \Omega^1)$ is given by*

$$M = \begin{cases} \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, & \textit{if } p \equiv 1, 4 \pmod 5 \\ \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}, & \textit{if } p \equiv 2, 3 \pmod 5). \end{cases},$$

where $*$ are elements of $\mathbb{F}_p[t]$.

Remark 5.2.3. A curious consequence of this fact is the following non-trivial result. Let p be a prime number such that $p \neq 2, 5$, $f(x) = x^5 - 5x^3 + 5x + 2 - 4t \in \mathbb{Z}[t][x]$ and $f(x)^{(p-1)/2} = \sum c_r x^r$. If

- $p \equiv 1, 4 \pmod 5$, then

$$c_{p-1} \equiv c_{2p-2} \equiv 0 \pmod p$$

- $p \equiv 2, 3 \pmod 5$, then

$$c_{p-2} \equiv c_{2p-1} \equiv 0 \pmod p.$$

Proof. Follows from the previous result and Proposition 5.1.8. □

Corollary 5.2.4. *If* $p \equiv 2$ *or* $3 \pmod 5$*, then the Jacobian of the curve* C^- *is either supersingular or ordinary.*

Proof. This is a direct consequence of the previous theorem and of Proposition 5.1.12.

In fact, using Proposition 5.1.12, we have that the Jacobian J^- of C^- is ordinary if and only if $\det(N) \neq 0$, where $N = M^{(p)}$ and M is the Cartier-Manin matrix of C^-. Also, since $r = 5$ (and, thus, the genus of C^- is 2), J^- is supersingular if and only if $N^{(p)}N = 0$. So it suffices to check that $\det(N) = 0$ if and only if $N^{(p)}N = 0$. This follows easily from the previous theorem. □

5.2.2 The Cartier-Manin matrix of the curve C^+

Following the ideas of the proof of the main result of [TTV91], one can compute the action of $\mathcal{O}_L$ on $H^0(C^+, \Omega^1)$.

Proposition 5.2.5. *The Jacobian of the curve C^+ has real multiplication by $\mathcal{O}_L$. Moreover, the action of $\mathcal{O}_L$ on $H^0(C^+, \Omega^1)$ has a basis of eigenvectors, namely:*

$$dx/y\ ,\ dx/y + ydx/y$$

Proof. Tautz-Top-Verberkmoes ([TTV91]) showed that C^+ is the quotient D_t/σ, where

$$D_t : y^2 = x^{10} + tx^5 + 1$$

and $\sigma \in \mathrm{End}(D_t)$ defined by

$$\sigma : (x, y) \mapsto (1/x, y/x^5).$$

Using that

$$X^{2n} + 1 = X^n(X + X^{-1}) \cdot g(X^2 + X^{-2}) \in k[X, X^{-1}]$$

for any odd n, it follows that the map $\varphi : D_t \to C^+$ given by

$$\varphi : (x, y) \mapsto (x + 1/x, y(x + 1)/x^3)$$

is well-defined and corresponds to the natural quotient map $D_t \to D_t/\sigma$. Moreover, it makes the diagram below commutative

$$\begin{tikzcd} D_t \arrow[r, "\varphi"] \arrow[d] & C^+ \arrow[d] \\ \mathbb{P}^1 \arrow[r] & \mathbb{P}^1 \end{tikzcd} ,$$

where

$$\begin{array}{ccc} \mathbb{P}^1 & \to & \mathbb{P}^1 \\ x & \mapsto & x + 1/x \end{array}$$

and the vertical maps are just

$$(x, y) \mapsto x.$$

The curve D_t has multiplication by $\mathcal{O}_{\mathbb{Q}(\zeta_5)}$ coming from the map

$$\zeta : (x, y) \mapsto (\zeta_5 x, y).$$

To prove that the Jacobian of C^+ has multiplication by $\mathcal{O}_L$, it is enough to show that the action of $\zeta^* + (\zeta^{-1})^*$ preserves the space $(\Omega^1_{D_t})^\sigma$ of σ-invariant differentials of D_t. One checks that a basis for $(\Omega^1_{D_t})^\sigma$ is given by

$$\omega_1 = (x^2 - x)dx/y \ , \ \omega_2 = (x^3 - 1)dx/y.$$

Now, by the definition of ζ, one computes that

$$[\zeta^* + (\zeta^{-1})^*]\omega_1 = (\zeta_5^2 + \zeta_5^{-2})\omega_1$$

and

$$[\zeta^* + (\zeta^{-1})^*]\omega_2 = (\zeta_5 + \zeta_5^{-1})\omega_2.$$

Now it remains only to show that

$$dx/y \ , \ dx/y + ydx/y \ \in \Omega^1_{C^+}$$

are eigenvectors for the action of $\mathcal{O}_L$.

Notice that the action on $\Omega^1_{C^+}$ comes from the action on $(\Omega^1_{D_t})^\sigma$ (these spaces are identified via φ). Now, the definition of φ yields

$$\varphi^*(dx/y) = \omega_1$$

$$\varphi^*(dx/y + ydx/y) = \omega_2.$$

From the previous computations, this finishes the proof. □

This result and Lemma 5.2.1 yield

Theorem 5.2.6. *The Cartier-Manin matrix of C^+ with respect to the basis $\{\frac{dx}{y}, x\frac{dx}{y}\}$ of $H^0(C^-, \Omega^1)$ is given by*

$$M = \begin{cases} \begin{pmatrix} a & b-a \\ 0 & b \end{pmatrix}, & \textit{if } p \equiv 1,4 \pmod 5 \\ \begin{pmatrix} a & b \\ a & -a \end{pmatrix}, & \textit{if } p \equiv 2,3 \pmod 5). \end{cases}$$

for some

$$a, b \in \mathbb{F}_p[t].$$

Corollary 5.2.7. *If* $p \equiv 2$ *or* $3 \pmod 5$*, then the Jacobian of the curve* C^+ *is either supersingular or ordinary.*

Proof. This is a direct consequence of the previous theorem and of Proposition 5.1.12. The proof is similar to the proof of corollary 5.2.4. □

5.2.3 A relation between $X^{(0)}_{5,\infty,\infty}(\mathfrak{p})$ and the family C^-

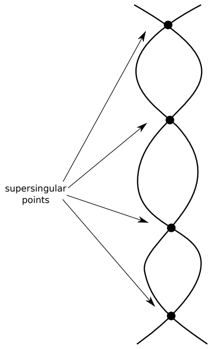

Figure 5.1: Reduction of $X_0(p)$ modulo p

It is known that $X_0(p) = \Gamma_0(p)\backslash\mathcal{H}^*$ admits an integral model for which the reduction modulo p consists of two copies of $X_0(1)_{\mathbb{F}_p} = \mathbb{P}^1_{\mathbb{F}_p}$ crossing transversally at the supersingular points as shown in figure 5.1 (cf. Theorem 6.9, page DeRa-144, in [DR73]). In particular, there is a relation between the genus of $X_0(p)$ and the number of supersingular elliptic curves modulo p.

In this subsection we investigate a similar property for the mock modular curve $X^{(0)}_{5,\infty,\infty}(\mathfrak{p})$: we show that in certain cases, the genus of the curve $X^{(0)}_{5,\infty,\infty}(\mathfrak{p})$ is closely related to the number of non-ordinary elements of the family of curves C^-. More specifically, the following result holds:

Theorem 5.2.8. *Let $p > 5$ be a prime number such that p splits in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ (i.e., $p \equiv 1$ or $4 \pmod 5$) and take $\mathfrak{p}$ a prime ideal above p. Furthermore, let g be the genus of $X^{(0)}_{5,\infty,\infty}(\mathfrak{p})$ and $d(t) = \det(M^{(p)})$, where M is the Cartier-Manin matrix of C^- (as computed in Theorem 5.2.2). Then*

$$g = \deg(d(t)) + \delta,$$

where

$$\delta = \begin{cases} -1, & \text{if } p \equiv 1 \pmod 5 \\ 1, & \text{if } p \equiv 4 \pmod 5). \end{cases}$$

Proof. Since p is assumed to be split, Proposition 1.3.5 implies that the genus of $X^{(0)}_{5,\infty,\infty}(\mathfrak{p})$ is given by

$$g = 2n - 1,$$

where

$$p + 1 = 5n + m$$

with

$$m = \begin{cases} 0, & \text{if } p \equiv -1 \pmod 5 \\ 2, & \text{if } p \equiv 1 \pmod 5). \end{cases}$$

Thus,

$$g = \frac{2}{5}(p+1-m) - 1.$$

It follows from Theorem 5.2.2 that the Cartier-Manin matrix is given by $\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)$, it suffices to compute the degree of the entries of the main diagonal, which is done in the next lemma. □

Lemma 5.2.9. *Let p be as in the statement of the previous proposition and*

$$\begin{pmatrix} a(t) & 0 \\ 0 & b(t) \end{pmatrix}$$

be the Cartier-Manin matrix of C^- with respect to p. Then

$$\deg(a(t)) = \begin{cases} \frac{3}{2}k, & \text{if } p = 5k+1 \\ \frac{3}{2}k - 1, & \text{if } p = 5k-1 \end{cases}$$

and

$$\deg(b(t)) = \begin{cases} \frac{1}{2}k, & \text{if } p = 5k+1 \\ \frac{1}{2}k - 1, & \text{if } p = 5k-1 \end{cases}$$

Proof. By Proposition 5.1.8, $a(t)$ is the $(p-1)$-th coefficient of $f(x)^{(p-1)/2}$, where

$$f(x) = x^5 - 5x^3 + 5x + 2 - 4t.$$

Since this lemma is only concerned about the degree (with respect to t) of a certain coefficient, f can be assumed to be

$$f(x) = x^5 - 5x^3 + 5x + t.$$

By the Multinomial Theorem,

$$f(x)^{(p-1)/2} = \sum_{a,b,c,d} (a,b,c,d)!\ (-1)^b\ 5^{b+c}\ x^{5a+3b+c}\ t^d,$$

where the sum is taken over all integers $a, b, c, d \geq 0$ such that $a+b+c+d = (p-1)/2$ and

$$(a,b,c,d)! = \frac{((p-1)/2)!}{a!\ b!\ c!\ d!}.$$

Therefore the $(p-1)$-th coefficient is given by

$$a(t) = \sum_{5a+3b+c=p-1} (a,b,c,d)!\ (-1)^b\ 5^{b+c}\ t^d.$$

This implies that $\deg(a(t))$, at least over $\mathbb{Z}$, is given (possibly) by the largest d such that

$$d = 4a + 2b - \frac{(p-1)}{2}$$

and

$$\begin{cases} 5a + 3b \leq p - 1 \\ a \geq 0\ ,\ \ b \geq 0. \end{cases}$$

Assume now that that $p = 5k + 1$. One checks (using the graphical method of linear programming) that the solution is

$$d = \frac{3}{2}k$$

attained only once when

$$a = k \quad \text{and} \quad b = 0.$$

Since this is attained only once, $\deg(a(t))$ over $\mathbb{Z}$ is actually $\frac{3}{2}k$. Using the fact that $p > 5$, it follows that the coefficient of the degree $\frac{3}{2}k$ term is not zero modulo p. Hence, $\deg(a(t)) = \frac{3}{2}k$ over $\mathbb{F}_p$.

A similar argument proves all the other cases. The only exception is the last case ($\deg(b(t))$ when $p = 5k-1$), where the maximum d is attained twice. But in this case a straight forward computation shows that the coefficient is still non-zero modulo p. □

Remark 5.2.10. Theorem 5.2.8 presents an interesting relation between the genus of $X^{(0)}_{5,\infty,\infty}(\mathfrak{p})$ and the number of non-ordinary elements in the family C^- modulo p when p is split. Unfortunately when p is inert, the same does not hold. The example below shows that the difference between the degree of $d(t)$ and the genus of $X_{5,\infty,\infty}(\mathfrak{p})$ grows with p when p is inert.

It would be interesting to understand why there is this discrepancy between primes that are split and primes that are inert.

Example 5. Contrary to the split case, the difference between the genus of $X^{(0)}_{5,\infty,\infty}(\mathfrak{p})$ and the degree of $d(t)$ is not ± 1 when p is inert. Here are the first few inert primes and their corresponding data as calculated using the computer algebra system SAGE ([S+12]):

p	genus of $X^{(0)}_{5,\infty,\infty}(\mathfrak{p})$	degree of $d(t)$	genus - degree
7	13	2	11
13	55	4	51
17	99	6	93
23	189	8	181
37	511	14	497
43	697	16	681
47	837	18	819
53	1071	20	1051
67	1729	26	1703

Remark 5.2.11. Note that Theorem 5.2.8 actually describes a relation between the genus of $X^{(0)}_{5,\infty,\infty}(\mathfrak{p})$ and the degree of $d(t)$ (not exactly the number of non-ordinary elements). In our computations, the difference between the degree and the exact number of non-ordinary elements is reasonably small, as the following table shows:

p	degree of $d(t)$	# of non-ordinary curves	difference
11	4	3	1
19	6	5	1
29	10	10	0
31	12	11	1
41	16	16	0
59	22	21	1
61	24	22	2
71	28	25	3
79	30	27	3
89	34	32	2
101	40	38	2
109	42	42	0
131	52	45	7
139	54	53	1
149	58	54	4
151	60	57	3
179	70	69	1

181	72	68	4
191	76	75	1
199	78	75	3
211	84	79	5
229	90	90	0
239	94	91	3
241	96	92	4
251	100	95	5
269	106	106	0
271	108	105	3
281	112	110	2
311	124	123	1
331	132	129	3
349	138	134	4
359	142	139	3
379	150	147	3
389	154	154	0

Chapter 6

Future Directions

As we mentioned in the introduction, the arithmetic of non-congruence modular forms and, especially, those related to triangle groups still present many open questions that require further studies. In this thesis, we have touched on some of those questions. As usual, some of them could only be partially answered and this gives rise to the first category of possible future studies:

1. Chapter 3 completely characterized the normalizers of $\Gamma_{q,\infty,\infty}(\mathfrak{p})$ but only for split primes $\mathfrak{p}$. An understanding of what happens when $\mathfrak{p}$ is inert would be desirable. See Section 3.3.2 for more details.

2. In 4.2, we studied the modular embedding defined by the TTV family of curves. A first comparison between this embedding and the one found

in [CW90] is given via hypergeometric differential equations. Another interesting direction would be to understand more thoroughly their relation.

3. In 5.2, we have found a relation between the genus of $X_{5,\infty,\infty}(\mathfrak{p})$ and the number of non-ordinary curves in the corresponding TTV family of curves. This relation was proved, again, only in the case where $\mathfrak{p}$ is a split prime. A natural problem would, therefore, be to understand the case where $\mathfrak{p}$ is an inert prime.

Secondly, in the process of answering some of the questions tackled in this thesis, other questions naturally arose:

1. The set of cusps of a triangle group is known explicitly in very few cases, one such case being $\Gamma_{2,5,\infty}$. In fact, Lang and Tan ([LT99]) used that knowledge to study the normalizers of $\Gamma_{2,5,\infty}(\mathfrak{p})$. In Chapter 3, we have conducted a similar study about the group $\Gamma_{q,\infty,\infty}(\mathfrak{p})$ but without an explicit knowledge of the set of cusps of $\Gamma_{q,\infty,\infty}$. We wonder whether our study can shed some light on the explicit characterization of the set of cusps of those triangle groups.

2. It is known that $X_0(p)$ admits an integral model containing an inter-

esting connection to supersingular elliptic curves (see Section 5.2.3). Theorem 5.2.8 presents evidence that a similar connection should also exist between $X_{5,\infty,\infty}(\mathfrak{p})$ and non-ordinary TTV curves, at least in the split case.

There are also many interesting questions motivated by the work done for non-congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. For instance:

1. It was shown in [Tho89] (cf. also [Ber94]) that Hecke operators do not give any new information in that case. The same question could be asked about triangle groups: how much new information, if any, can be obtained from “Hecke operators" in the context of triangle groups?

2. There are also the so called Atkin and Swinnerton-Dyer congruences for non-congruence modular forms, which resemble eigenforms in the classical case (see, for instance, [Sch85]). Is there an analogous set of relations in the case of a triangle group?

Bibliography

[ASD71] A. O. L. Atkin and H. P. F. Swinnerton-Dyer. Modular forms on noncongruence subgroups. In *Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968)*, pages 1–25. Amer. Math. Soc., Providence, R.I., 1971.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Bea83] A. F. Beardon. *The geometry of discrete groups*, volume 91 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1983.

[Bel79] G. V. Belyĭ. Galois extensions of a maximal cyclotomic field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(2):267–276, 479, 1979.

[Ber94] G. Berger. Hecke operators on noncongruence subgroups. *C. R. Acad. Sci. Paris Sér. I Math.*, 319(9):915–919, 1994.

[BK86] E. Brieskorn and H. Knörrer. *Plane algebraic curves.* Modern Birkhäuser Classics. Birkhäuser/Springer Basel AG, Basel, 1986. [2012] reprint of the 1986 edition.

[Bor66] I. R. Borevich, A. I.and Shafarevich. *Number theory.* Academic Press, New York, 1966.

[Cox89] D. A. Cox. *Primes of the form $x^2 + ny^2$.* A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[CV] P. Clark and J. Voight. Algebraic curves uniformized by congruence subgroups of triangle groups. (preprint).

[CW34] C. Chevalley and A. Weil. Über das Verhalten der Integrale ersten Gattung bei Automorphismen des Funktionenkörpers. *Abh. math. Sem. Univ. Hamburg*, 10:358–361, 1934.

[CW90] P. Cohen and J. Wolfart. Modular embeddings for some nonarithmetic Fuchsian groups. *Acta Arith.*, 56(2):93–110, 1990.

[Dar97] H. Darmon. Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation. *C. R. Math. Rep. Acad. Sci. Canada*, 19(1):3–14, 1997.

[Dar00] H. Darmon. Rigid local systems, Hilbert modular forms, and Fermat's last theorem. *Duke Math. J.*, 102(3):413–449, 2000.

[Dar04] H. Darmon. A fourteenth lecture on Fermat's last theorem. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 103–115. Amer. Math. Soc., Providence, RI, 2004.

[DG95] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[DGMM] C. F. Doran, T. Gannon, H. Movasati, and Shokri K. M. Automorphic forms for triangle groups.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[DS05] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[EL80] G. Ellingsrud and K. Lønsted. An equivariant Lefschetz formula for finite reductive groups. *Math. Ann.*, 251(3):253–261, 1980.

[FH91] W. Fulton and J. Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[FK92] H. M. Farkas and I. Kra. *Riemann surfaces*, volume 71 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1992.

[FT93] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[GGH91] J. F. Glazebrook, D. R. Grayson, and P. R. Hewitt. Galois representations on holomorphic differentials. *Comm. Algebra*, 19(5):1375–1386, 1991.

[GL12] E. Z. Goren and K. E. Lauter. Genus 2 curves with complex multiplication. *Int. Math. Res. Not. IMRN*, (5):1068–1142, 2012.

[GO00] E. Z. Goren and F. Oort. Stratifications of Hilbert modular varieties. *J. Algebraic Geom.*, 9(1):111–154, 2000.

[Gor02] E. Z. Goren. *Lectures on Hilbert modular varieties and modular forms*, volume 14 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2002. With the assistance of Marc-Hubert Nicole.

[Hec28] E. Hecke. Über ein Fundamentalproblem aus der Theorie der Elliptischen Modulfunktionen. *Abh. Math. Sem. Univ. Hamburg*, 6:235–257, 1928.

[Hec30] E. Hecke. Über das Verhalten der Integrale 1. Gattung bei Abbildungen, insbesondere in der Theorie der elliptischen Modulfunktionen. *Abh. Math. Sem. Univ. Hamburg*, 8:271–281, 1930.

[Hec11] E. Hecke. On modular forms of weight 2 and representations of $\mathrm{PSL}(2, \mathbb{Z}/p\mathbb{Z})$. `http://arxiv.org/abs/1103.3066`, 2011. Translation of "Über das Verhalten der Integrale 1. Gattung bei Abbildungen, insbesondere in der Theorie der elliptischen Modulfunktionen" from the German original by L. K. Takei.

[HvdG81] F. Hirzebruch and G. van der Geer. *Lectures on Hilbert modular surfaces*, volume 77 of *Séminaire de Mathématiques Supérieures.* Presses de l'Université de Montréal, Montreal, Que., 1981. Based on notes taken by W. Hausmann and F. J. Koll.

[Igu60] J. Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960.

[Kat92] S. Katok. *Fuchsian groups.* Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1992.

[LE06] Q. Liu and R. Erné. *Algebraic geometry and arithmetic curves.* Oxford University Press, USA, 2006.

[Leu67] A. Leutbecher. Über die Heckeschen Gruppen $\mathfrak{G}(\lambda)$. *Abh. Math. Sem. Univ. Hamburg*, 31:199–205, 1967.

[Leu74] A. Leutbecher. Über die Heckeschen Gruppen $G(\lambda)$. II. *Math. Ann.*, 211:63–86, 1974.

[LLT00] M. L. Lang, C. H. Lim, and S. P. Tan. Principal congruence subgroups of the Hecke groups. *J. Number Theory*, 85(2):220–230, 2000.

[LLY05a] W. C. W. Li, L. Long, and Z. Yang. Modular forms for noncongruence subgroups. *Q. J. Pure Appl. Math.*, 1(1):205–221, 2005.

[LLY05b] W. C. W. Li, L. Long, and Z. Yang. On Atkin-Swinnerton-Dyer congruence relations. *J. Number Theory*, 113(1):117–148, 2005.

[LT99] M. L. Lang and S. P. Tan. Normalizers of the congruence subgroups of the Hecke group G_5. *Proc. Amer. Math. Soc.*, 127(11):3131–3140, 1999.

[Man63] Y. I. Manin. The theory of commutative formal groups over fields of finite characteristic. *Russian Math. Surveys*, 18:1–83, 1963.

[Mar77] D. A. Marcus. *Number fields.* Springer-Verlag, New York, 1977. Universitext.

[Mar91] G. A. Margulis. *Discrete subgroups of semisimple Lie groups*, volume 17 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3).* Springer-Verlag, Berlin, 1991.

[Miy06] T. Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, English edition, 2006.

[Nyg81] N. O. Nygaard. Slopes of powers of Frobenius on crystalline cohomology. *Ann. Sci. École Norm. Sup. (4)*, 14(4):369–401 (1982), 1981.

[Pet37] H. Petersson. Über die eindeutige bestimmung und die erweiterungsfähigkeit von gewissen grenzkreisgruppen. *Abh. Math. Sem. Univ. Hamburg*, 12(1):180–199, 1937.

[S$^+$12] W. A. Stein et al. *Sage Mathematics Software (Version 4.8)*. The Sage Development Team, 2012. `http://www.sagemath.org`.

[Sch] C. Schnell. On computing picard-fuchs equations. `http://www.math.sunysb.edu/~cschnell/pdf/notes/picardfuchs.pdf`.

[Sch85] A. J. Scholl. Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences. *Invent. Math.*, 79(1):49–77, 1985.

[Sch86] A. J. Scholl. Fourier coefficients of Eisenstein series on noncongruence subgroups. *Math. Proc. Cambridge Philos. Soc.*, 99(1):11–17, 1986.

[Sch03] R. Schoof. Class numbers of real cyclotomic fields of prime conductor. *Math. Comp.*, 72(242):913–937, 2003.

[Ser58] J. P. Serre. Sur la topologie des variétés algébriques en caractéristique p. In *Symposium internacional de topología algebraica International symposium on algebraic topology*, pages 24–53. Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958.

[Shi94] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1994.

[Suz82] M. Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1982.

[Tak77] K. Takeuchi. Arithmetic triangle groups. *J. Math. Soc. Japan*, 29(1):91–106, 1977.

[Tak12] L. K. Takei. On triangle groups and representations of $\mathrm{PSL}_2(\mathbb{F}_{p^{2n+1}})$. *Ann. Sci. Math. Québec*, 36(1):245–258 (2013), 2012.

[Tho89] J. G. Thompson. Hecke operators and noncongruence subgroups. In *Group theory (Singapore, 1987)*, pages 215–224. de Gruyter, Berlin, 1989. Including a letter from J.-P. Serre.

[TTV91] Walter Tautz, Jaap Top, and Alain Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991.

[vdW49] B. L. van der Waerden. *Modern Algebra. Vol. I.* Frederick Ungar Publishing Co., New York, N. Y., 1949.

[Was82] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[Yan] JOURNAL = Compos. Math. FJOURNAL = Compositio Mathematica VOLUME = 149 YEAR = 2013 NUMBER = 1 PAGES = 1–31 ISSN = 0010-437X MRCLASS = 11G18 (11F12 33C05) MRNUMBER = 3011876 MRREVIEWER = Andrea Mori DOI = 10.1112/S0010437X12000371 URL = http://dx.doi.org/10.1112/S0010437X12000371 Yang, Y. TI-

TLE = Schwarzian differential equations and Hecke eigenforms on Shimura curves.

[Yui78] N. Yui. On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. *J. Algebra*, 52(2):378–410, 1978.

[Zhu00] H. J. Zhu. Group structures of elementary supersingular abelian varieties over finite fields. *J. Number Theory*, 81(2):292–309, 2000.