On arithmetic properties of Fuchsian groups and Riemann surfaces

Dissertation

zur

Erlangung des Doktorgrades (Dr. rer. nat.)

der

Mathematisch-Naturwissenschaftlichen Fakultät

der

Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt von

Robert Anselm Kucharczyk

aus

Essen

Bonn, im Oktober 2014

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät
der Rheinischen Friedrich-Wilhelms-Universität Bonn

1. Gutachterin: Prof. Dr. Ursula Hamenstädt
2. Gutachter: Prof. Dr. Jakob Stix (Goethe-Universität Frankfurt)

Tag der Promotion: 12. Januar 2015

Erscheinungsjahr: 2015

On arithmetic properties of Fuchsian groups and Riemann surfaces

Contents

1 Introduction **7**

1.1 Three ways to be arithmetic 7

1.1.1 Riemann 7

1.1.2 Jacobi 8

1.1.3 Fuchs 8

1.2 Interaction 9

1.2.1 A simple example 9

1.2.2 Belyĭ's theorem, dessins d'enfants and triangle groups 11

1.2.3 Arithmetic and semi-arithmetic Fuchsian groups 13

1.3 A summary of our results 13

1.4 Acknowledgements 15

2 On copies of the absolute Galois group in $\operatorname{Out}\hat{F}_2$ **17**

2.1 Introduction 17

2.2 Some anabelian geometry 18

2.3 The Galois actions 20

2.4 Concluding remarks 23

3 Jarden's property and Hurwitz curves **25**

3.1 Introduction and statement of results 25

3.1.1 Hurwitz curves and translation surfaces. 25

3.1.2 Jarden's property. 26

3.2 Jarden's property: the proof 27

3.3 Galois actions 33

4 Modular embeddings and rigidity for Fuchsian groups **37**

4.1 Introduction 37

4.2 Traces on PSL(2) and Möbius transformations 41

4.3 The finite groups $\mathrm{PSL}(2, q)$ 41

4.4 Semi-arithmetic groups and their congruence subgroups 43

4.5 Congruence quotients of semi-arithmetic groups 47

4.6 Characters for Fuchsian groups 49

4.7 Modular embeddings 51

4.8 Congruence rigidity 52

4.9 An example 56

4.10 Concluding remarks 56

5 Prym varieties and triangle groups 59

5.1 Introduction 59

5.2 Triangle groups 62

5.3 Hypergeometric curves and their moduli 65

5.3.1 Cohomology of hypergeometric curves 65

5.3.2 The family of simple hypergeometric curves over $\mathrm{Conf}_3(\mathbb{C})$ and its period map 68

5.3.3 The mapping-class group as a braid group 69

5.3.4 Descending to moduli space 72

5.4 Congruence subgroups 77

5.4.1 The Prym lattice 77

5.4.2 Skew-Hermitian forms over finite fields 80

5.4.3 Reduction modulo a prime ideal 82

5.4.4 Prym level structures 85

5.4.5 The braid group action on the Prym lattice 87

5.5 Moduli 88

5.5.1 Moduli spaces of simple hypergeometric curves as sets 88

5.5.2 Algebraic structures on moduli spaces 92

5.5.3 Belyĭ maps and Galois actions 93

5.5.4 Hurwitz curves 96

5.5.5 Shimura varieties 96

Bibliography 99

Chapter 1

Introduction

In this thesis we investigate some special classes of Riemann surfaces from a number-theoretic perspective. The arithmetic theory of Riemann surfaces is rich in examples and special phenomena, and as yet rather poor in overall organising principles (at least when compared to other fields of pure mathematics with a comparable history). We follow Lochak's point of view expressed in [50, p. 444] that distinguishes between "three types of arithmetics at work which one might call modular (Riemann), period (Jacobi) and hyperbolic (Fuchs) arithmetics". In that work curves in the moduli space of curves are considered, but we think the classification works as well for abstract curves or Riemann surfaces. We give a short introduction to the three types.

1.1 Three ways to be arithmetic

1.1.1 Riemann

The starting point here is Riemann's existence theorem: every compact Riemann surface can be embedded as a smooth closed subvariety of some $\mathbb{P}^n(\mathbb{C})$, hence as a smooth projective algebraic curve over $\mathbb{C}$. Moreover, this algebraic structure is unique: any complex submanifold of $\mathbb{P}^n(\mathbb{C})$ is automatically algebraic by Chow's theorem, and holomorphic maps between projective varieties are always regular, i.e. given by rational maps in the standard homogeneous coordinates on projective space. This defines an identification (in modern terms, an equivalence of categories) between compact Riemann surfaces and smooth projective complex curves, and we use the terms interchangeably.

With this preparation, a compact Riemann surface X is *defined over a number field in Riemann's sense* if one of the following equivalent conditions hold:

(i) There exists a holomorphic embedding $f\colon X \to \mathbb{P}^n(\mathbb{C})$ whose image is an algebraic curve cut out by equations with coefficients in a number field $L \subset \mathbb{C}$.

(ii) There exists a smooth projective algebraic curve X_0 over some number field $L \subset \mathbb{C}$ with $X_0(\mathbb{C}) \simeq X$.

(iii) There exists a subfield K of the field $\mathscr{M}(X)$ of meromorphic functions on X

such that K is finitely generated over $\mathbb{Q}$, furthermore $L = K \cap \mathbb{C}$ is a number field and the canonical map $K \otimes_L \mathbb{C} \to \mathscr{M}(X)$ is an isomorphism.

The diffiulty of determining whether a Riemann surface satisfies these conditions increases with the genus: in genus zero there is only $X = \mathbb{P}^1(\mathbb{C})$ for which we can clearly take $L = \mathbb{Q}$. In genus one the j-invariant for elliptic curves does the job: an elliptic curve X is defined over a number field if and only if $j(X)$ is algebraic, in which case we may take $L = \mathbb{Q}(j(X))$. Curves of genus two are all hyperelliptic, hence they can be defined by an affine equation of the form

$$X \colon w^2 = z(z-1)(z-a)(z-b)(z-c);$$

here a, b, c are called *Rosenhain parameters*, and X can be defined over a number field if and only if $a, b, c \in \overline{\mathbb{Q}}$. More generally, the (coarse) moduli space of smooth projective curves of genus g has the structure of an algebraic variety M_g over $\mathbb{Q}$, and a complex curve X can be defined over a number field if and only if its moduli point lies in the dense countable subset $M_g(\overline{\mathbb{Q}}) \subset M_g(\mathbb{C})$.

1.1.2 Jacobi

This point of view deals with pairs (X, ω), where X is a compact Riemann surface and ω is a nonzero meromorphic differential form on X. Let $S_\omega \subset X$ be the union of zeros and poles of ω. For a relative cycle $\gamma \in H_1(X, S_\omega; \mathbb{Z})$ we may form the *period*

$$\int_\gamma \omega \in \mathbb{C}$$

(convergence assumed). We may ask whether one particular period is algebraic, or whether all periods of ω are algebraic; the latter question can be reformulated as follows: can (X, ω) be glued from polygons with only algebraic vertices?

Again this can be phrased as the algebraicity of certain coordinates on some moduli space: for some combinatorial data π prescribing the orders of the zeros and poles of ω, there is a moduli space $\Omega\mathscr{M}_g(\pi)$ of pairs (X, ω) with X a compact Riemann surface of genus g and ω a meromorphic one-form of type π. It is a complex orbifold, and on some manifold cover of it we can define local coordinates by the periods $\int_\gamma \omega$ for a fixed finite collection of cycles ω. Again one finds that the pairs (X, ω) with all periods algebraic form a dense countable subset of $\Omega\mathscr{M}_g(\pi)$.

1.1.3 Fuchs

The third approach to Riemann surfaces is to view them as quotients by discrete groups of Möbius transformations; here we concentrate on the class of *Fuchsian groups*, i.e. discrete subgroups of $\mathrm{SL}(2, \mathbb{R})$ acting on the upper half plane $\mathfrak{H}$. By the uniformisation theorem, any Riemann surface can be written as $\Gamma\backslash\mathfrak{H}$ for some Fuchsian group Γ and hence inherits a hyperbolic metric (with singularities if Γ has fixed points). The most interesting case for us is when Γ is a lattice in G – this is equivalent to $\Gamma\backslash\Omega$ being the Riemann surface underlying a (not necessarily projective) smooth algebraic curve. The question for arithmeticity in this case becomes: can Γ be chosen to have only elements with algebraic matrix entries?

1.2 Interaction

It is an easy and rather unproductive exercise to produce examples of curves satisfying *one* of these three arithmeticity conditions; a much deeper question, which is very far from being answered outside some rather restricted families of special examples, is this: when can a curve be arithmetically defined in two of these ways, or even all three? When it can, other questions naturally come up: are the number fields (or other arithmetic invariants) appearing in the two descriptions somehow related to each other? If we apply a Galois automorphism on one side, can we foresee what happens on the other side?

1.2.1 A simple example

We give an example of a curve X in genus 2 where all three types of arithmetic are present:

(i) X is the smooth projective curve defined by the affine equation $w^2 = 1 - z^5$, so it is defined over $\mathbb{Q}$ in Riemann's sense. In other words, X is the hyperelliptic curve with ramification locus $\mu_5 \cup \{\infty\}$.

(ii) A basis of the space $\Omega^1(X)$ of holomorphic one-forms on X is given by

$$\omega_1 = \frac{\mathrm{d}z}{w} \text{ and } \omega_2 = \frac{z\,\mathrm{d}z}{w}.$$

The translation surface (X, ω_1) can be obtained by glueing two regular pentagons in the complex plane along parallel sides, as indicated by the numbering in Figure 1.1. Similarly, (X, ω_2) can be obtained by glueing opposite sides in a regular decagon, see Figure 1.2. The periods $\int_\gamma \omega_j$ for $\gamma \in H_1(X, S_{\omega_j}; \mathbb{Z})$ are then algebraic up to an easily determined constant factor:

Consider first ω_1. The grey points in Figure 1.1 are all identified, and they form the one point above $z = \infty$. The full black points are identified in pairs and are given by $z \in \mu_5$; we may assume that the point marked by i has coordinates $(z, w) = (\zeta_5^{i-1}, 0)$. Finally the two white points with a black circle around it have coordinates $(z, w) = (0, \pm 1)$. The vector from, say, the left white point P to the black point Q at its right is the complex number

$$\int_P^Q \omega_1 = \int_0^1 \frac{\mathrm{d}z}{\sqrt{1 - z^5}} = \frac{1}{5} \int_0^1 x^{-4/5} (1 - x)^{-1/2}\, \mathrm{d}x = \frac{1}{5} \mathrm{B}\Big(\frac{1}{2}, \frac{1}{5}\Big)$$

where B is Euler's beta function. By [77] this number is transcendental. Still, a glance at Figure 1.1 tells us that

$$\frac{1}{\mathrm{B}\big(\frac{1}{2}, \frac{1}{5}\big)} \int_\gamma \omega_1 \in \mathbb{Q}(\zeta_5) \text{ for all } \gamma \in H_1(X, S_{\omega_1}; \mathbb{Z}).$$

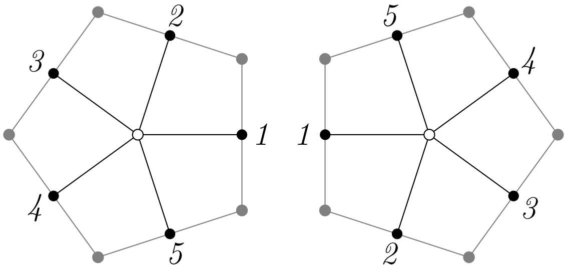

Figure 1.1: The translation surface (X, ω_1)

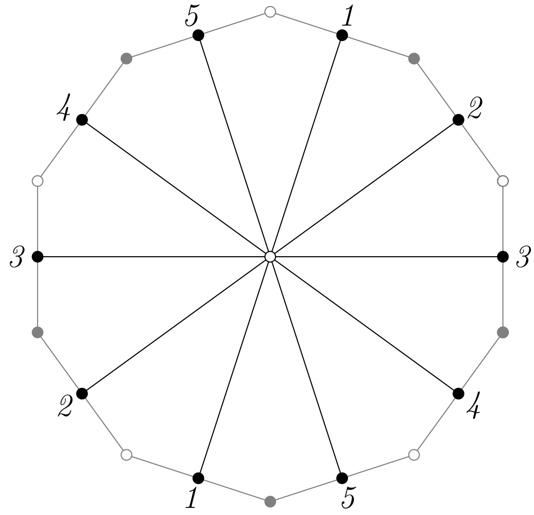

Figure 1.2: The translation surface (X, ω_2)

For ω_2 similar considerations lead to

$$\frac{1}{\mathrm{B}\left(\frac{1}{2}, \frac{2}{5}\right)} \int_\gamma \omega_1 \in \mathbb{Q}(\zeta_{20}) \text{ for all } \gamma \in H_1(X, S_{\omega_2}; \mathbb{Z}).$$

(iii) Apart from finitely many points X can be uniformised by a subgroup of the *Hecke triangle group* H_5. This is the discrete subgroup of $\mathrm{SL}(2, \mathbb{R})$ generated by

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T_5 = \begin{pmatrix} 1 & \varphi \\ 0 & 1 \end{pmatrix},$$

where $\varphi = (1 + \sqrt{5})/2$ is the golden ratio. There is a unique group homomorphism $\alpha \colon H_5 \to \mathbb{Z}/10\mathbb{Z}$ with $\alpha(S) = 5$ and $\alpha(T_5) = 1$, and we set $\Gamma = \ker \alpha$. Then if $P \in X$ is the point above $z = \infty$ the complement $X \setminus \{P\}$ is biholomorphic to $\Gamma \backslash \mathfrak{H}$.

We omit the proof that these three constructions really define the same Riemann surface; it is an application of the constructions behind Theorem 1.3. This surface provides an example for one of the two major unifying principles for relating two or more types of arithmetic:

1.2.2 Belyĭ's theorem, dessins d'enfants and triangle groups

Although being defined over a number field depends on subtle algebraic properties of a Riemann surface it is entirely equivalent to being defined by a *dessin d'enfant*, a purely combinatorial (and, with a suitable encoding, even finite) object. Before we formally introduce dessins we state the truly remarkable theorem that establishes this improbable link:

Theorem 1.1 (Belyĭ 1979)**.** *Let X be a smooth projective complex curve. Then X can be defined over a number field in Riemann's sense if and only if there exists a finite holomorphic map $f\colon X \to \mathbb{P}^1(\mathbb{C})$, unramified outside three points of $\mathbb{P}^1(\mathbb{C})$. Equivalently, there exists a nonconstant meromorphic function on X with at most three critical values.*

The proof of this theorem consists of two arguments of entirely different character. The "if" argument was essentially known before and follows by a routine application of rather deep results from SGA. Not just X can be defined over a number field, but f becomes a morphism of algebraic curves, defined over a finite extension of L. In any case, both are defined over $\overline{\mathbb{Q}}$ in an essentially unique way. The "only if" argument was Belyĭ's surprising contribution, and it is proved in a completely elementary and constructive fashion.

Let us call a pair (X, f) with X a smooth projective curve over $\overline{\mathbb{Q}}$ and $f\colon X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ a nonconstant regular map unramified outside $\{0, 1, \infty\} \subset \mathbb{P}^1$ a *Belyĭ pair*. Since every three points in $\mathbb{P}^1$ can be moved simultaneously to 0, 1, ∞ by a Möbius transformation, the new part of Belyĭ's Theorem says that every smooth projective curve over $\overline{\mathbb{Q}}$ can be completed to a Belyĭ pair. Now a Belyĭ pair (X, f) gives rise to a graph embedded in $X(\mathbb{C})$ by taking the preimage of the closed interval $[0, 1]$ as the union of all edges and the preimages of $\{0, 1\}$ as the vertices. We give this graph a bipartite structure by colouring the preimages of 0 white, those of 1 black. So what we obtain is this:

Definition 1.2. *A* dessin d'enfant *is a finite bipartite graph Γ embedded in an oriented compact (topological) surface S such that the complemenet $S \smallsetminus |\Gamma|$ consists of finitely many simply connected regions.*

There is an obvious notion of isomorphism for both Belyĭ pairs and dessins d'enfants, and it is not hard to see that the procedure just described defines a bijection between the set of isomorphism classes of Belyĭ pairs and that of isomorphism classes of dessins d'enfants. In particular, every dessin d'enfant, a purely topological object, gives rise to a Belyĭ pair (X, f).

We have already seen two examples: take the curve $X\colon w^2 = 1 - z^5$ from section 1.2.1. The two maps $f_1, f_2 \colon X \to \mathbb{P}^1$ given by

$$f_1(z,w) = z^5, \quad f_2(z,w) = \frac{1}{z^5}$$

are Belyĭ maps. The black skeleton in Figure 1.1 is the dessin for (X, f_1), that in Figure 1.2 is the dessin for (X, f_2).

Belyĭ's Theorem can also be reformulated in two more ways closer to Fuchsian groups, see [15]:

Theorem 1.3. *Let X be a compact Riemann surface. The following are equivalent:*

(i) X can be defined over a number field as an algebraic curve.

(ii) There exists a finite index subgroup $\Gamma \subseteq \mathrm{SL}(2,\mathbb{Z})$ such that $X \simeq \Gamma\backslash\mathfrak{H}^*$, where $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$, with the usual construction for the topology and the analytic structure on the quotient.

(iii) There exists a finite index subgroup Γ in a cocompact Fuchsian triangle group $\Delta \subset \mathrm{PSL}(2,\mathbb{R})$ with $X \simeq \Gamma\backslash\mathfrak{H}$.

Alexander Grothendieck describes his amazement at these elementary yet surprising connections in his famous essay "Esquisse d'un programme" [32] (originally a research proposal, and probably "the best rejected proposal ever" [49]):

> Cette découverte, qui techniquement se réduit à si peu de choses, a fait sur moi une impression très forte, et elle représente un tournant décisif dans le cours de mes réflexions, un déplacement notamment de mon centre d'intérêt en mathématique, qui soudain s'est trouvé fortement localisé. Je ne crois pas qu'un fait mathématique m'ait jamais autant frappé que celui-là, et ait eu un impact psychologique comparable.[1] Cela tient sûrement à la nature tellement familière, non technique, des objets considérés, dont tout dessin d'enfant griffonné sur un bout de papier (pour peu que le graphisme soit d'un seul tenant) donne un exemple parfaitement explicite. A un tel dessin se trouvent associés des invariants arithmétiques subtils, qui seront chamboulés complètement dès qu'on y rajoute un trait de plus. [. . .]
>
> Toute carte finie orientée donne lieu à une courbe algébrique projective et lisse définie sur $\overline{\mathbb{Q}}$, et il se pose alors immédiatement la question : quelles sont les courbes algébriques sur $\overline{\mathbb{Q}}$ obtenues ainsi — les obtiendrait-on toutes, qui sait ? En termes plus savants, serait-il vrai que toute courbe algébrique projective et lisse définie sur un corps de

[1] Je puis faire exception pourtant d'un autre « fait », du temps où, vers l'âge de douze ans, j'étais interné au camp de concentration de Rieucros (près de Mende). C'est là que j'ai appris, par une détenue, Maria, qui me donnait des leçons particulières bénévoles, la définition du cercle. Celle-ci m'avait impressionné par sa simplicité et son évidence, alors que la propriété de « rotondité parfaite » du cercle m'apparaissait auparavant comme une réalité mystérieuse au-delà des mots. C'est à ce moment, je crois, que j'ai entrevu pour la première fois (sans bien sûr me le formuler en ces termes) la puissance créatrice d'une « bonne » définition mathématique, d'une formulation qui décrit l'essence. Aujourd'hui encore, il semble que la fascination qu'a exercé sur moi cette puissance-là n'a rien perdu de sa force. *[Original footnote]*

> nombres interviendrait comme une « courbe modulaire » possible pour paramétriser les courbes elliptiques munies d'une rigidification convenable ? Une telle supposition avait l'air à tel point dingue que j'étais presque gêné de la soumettre aux compétences en la matière. Deligne consulté trouvait la supposition dingue en effet, mais sans avoir un contre-exemple dans ses manches. Moins d'un an après, au Congrès International de Helsinki, le mathématicien soviétique Bielyi annonce justement ce résultat, avec une démonstration d'une simplicité déconcertante tenant en deux petites pages d'une lettre de Deligne — jamais sans doute un résultat profond et déroutant ne fut démontré en si peu de lignes !

1.2.3 Arithmetic and semi-arithmetic Fuchsian groups

The second class of special Riemann surfaces which are arithmetically significant both in Riemann's and in Fuchs's sense are those uniformised by *arithmetic groups*. If K is a totally real number field and A is a quaternion algebra over K unramified over the identity embedding $K \hookrightarrow \mathbb{R}$ and ramified over all other infinite places of K, let $\mathcal{O}$ be some order in A and let $\mathcal{O}^1$ be the group of elements in A of reduced norm one. Then via an isomorphism $A \otimes_K \mathbb{R} \simeq \mathrm{M}(2,\mathbb{R})$ the group $\mathcal{O}^1$ embeds as a lattice in $\mathrm{SL}(2,\mathbb{R})$, and any lattice in $\mathrm{SL}(2,\mathbb{R})$ commensurable to some such $\mathcal{O}^1$ is called an arithmetic (Fuchsian) group. The algebraic curves they uniformise are also defined over $\overline{\mathbb{Q}}$ since they either are themselves, or are closely related to, moduli spaces of abelian varieties with certain PEL structures, see [87]. Because of this moduli interpretation, much more is known in terms of general statements about the intertwining of Riemann and Fuchs arithmetics for these curves. Then again, they are much less intuitive and easy to define than dessins d'enfants.

The simplest example of an arithmetic Fuchsian group is $\mathrm{SL}(2,\mathbb{Z})$, obtained from $K = \mathbb{Q}$ and $A = \mathrm{M}(2,\mathbb{Q})$, which already occurred in Theorem 1.3 above. Also precisely 85 of the hyperbolic triangle groups $\Delta(p,q,r)$ are arithmetic by [91]. However, many Fuchsian lattices that appear in nature fall short of being arithmetic and yet share many important properties with arithmetic groups, such as their traces being algebraic integers. A convenient class of such groups is given by the *semi-arithmetic groups with modular embeddings* which are disussed in Chapter 4: they contain not only all hyperbolic triangle groups, but also the *Veech groups* uniformising *Teichmüller curves* which are totally geodesic algebraic curves in moduli spaces of curves. We refer to the introduction of Chapter 4 for a closer discussion of (semi-)arithmetic groups.

1.3 A summary of our results

In four independent chapters we prove some results on algebraic curves and Fuchsian groups which are arithmetic in at least one, and often more, of the senses discussed above. We shortly summarise their main results; each chapter contains a more detailed individual introduction.

In the second chapter we prove a result that can be interpreted as comparing distinct Galois actions on combinatorial objects called *origamis*, which are similar to dessins d'enfants; see [34]. The Galois action on these objects is obtained from an elliptic curve over a number field minus its origin, which plays the same rôle as $\mathbb{P}^1 \smallsetminus \{0,1,\infty\}$ for dessins d'enfants. The Galois action on dessins d'enfants can be encoded in one injective homomorphism

$$\varrho_{01\infty}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \hookrightarrow \mathrm{Out}\,\hat{F}_2,$$

where $\hat{F}_2$ is the profinite completion of a free group on two letters, and Out denotes the outer automorphism group. This homomorphism is obtained from an isomorphism between $\hat{F}_2$ and the étale fundamental group of $\mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0,1,\infty\}$. Similarly for every elliptic curve E over a number field $K \subset \mathbb{C}$ and every basis $\mathfrak{B}$ of $H_1(E(\mathbb{C}),\mathbb{Z})$ we obtain an injective group homomorphism

$$\varrho_{E,\mathfrak{B}}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}|K) \hookrightarrow \mathrm{Out}\,\hat{F}_2.$$

The main result in Chapter 2 is that, under the mild and necessary condition that the bases are positively oriented for the intersection pairings, $\varrho_{E_1,\mathfrak{B}_1}$ and $\varrho_{E_2,\mathfrak{B}_2}$ have equal images only in the obvious case where the number fields agree and there is an isomorphism $E_1 \simeq E_2$ taking $\mathfrak{B}_1$ to $\mathfrak{B}_2$. Simple consequences for the commensurability classes in $\hat{F}_2$ of these images are drawn, in particular no image of $\varrho_{E,\mathfrak{B}}$ for any elliptic curve is widely commensurable with the image of $\varrho_{01\infty}$. These results are drawn from previous deep results in anabelian geometry by Neukirch, Uchida and Tamagawa, combined with an elementary trick and an application of Belyĭ's Theorem.

In the third chapter we prove that the absolute Galois group acts faithfully on certain rather small classes of dessins d'enfants and origamis. The first main result in that chapter is faithfulness of the Galois action on normal dessins of given ramification type, which had essentially been proved (but not stated explicitly) before in [30]. We translate their rather complicated proof, which mixes complex-analytic and étale considerations, entirely into the language of ℓ-adic sheaves. This way we can circumvent the explicit calculations in [30] and prove more generally that if $\mathscr{X}$ is a Deligne–Mumford stack over a number field K which is finitely covered by a hyperbolic curve, then $\mathrm{Gal}(\overline{\mathbb{Q}}|K)$ operates faithfully on the set of isomorphism classes of normal étale coverings of $\mathscr{X}$ by curves. For $\mathscr{X}$ over $\mathbb{Q}$ with $\mathscr{X}(\mathbb{C}) = \Delta(p,q,r)\backslash\mathfrak{H}$ (as an orbifold quotient) we obtain the already mentioned result on normal dessins, and for $(p,q,r) = (2,3,7)$ we get that $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ operates faithfully on Hurwitz curves, i.e. smooth projective curves X realising Hurwitz's bound $|\operatorname{Aut} X| \leq 84(g-1)$ with $g \geq 2$ the genus of X. A similar result holds for origamis attaining a similar bound for the automorphism group.

In the fourth chapter we switch from Riemann to Fuchs arithmetics. Mostow's rigidity theorem, which means that a lattice in the isometry group of hyperbolic n-space ($n \geq 3$) is uniquely determined up to conjugacy by its isomorphism class, does not hold for $n = 2$. Still, for semi-arithmetic groups admitting a modular embedding (in particular for arithmetic groups, lattice Veech groups, and finite index subgroups of triangle groups) we obtain a rigidity statement for the topology defined by congruence subgroups.

In the fifth chapter, all three types of arithmetics come together. We give a moduli interpretation for prime level principal congruence subgroups of triangle groups $\Delta = \Delta(2,3,r)$ with $r \geq 7$ coprime to 6. The main result is that for a prime $\mathfrak{p}$ in the trace field $\mathbb{Q}(\zeta_r + \zeta_r^{-1})$, the quotient $\Delta(\mathfrak{p})\backslash\mathbb{D}$ is birational to a moduli space of what we call simple hypergeometric curves, i.e. curves of the form

$$w^{2r} = f(z),$$

f a monic separable cubic polynomial, together with a level-$\mathfrak{p}$ structure for generalised complex multiplication by $\mathbb{Q}(\zeta_r)$ on the Prym variety, a summand of the Jacobian. Passing from the curve to its Jacobian defines the modular embedding for $\Delta(\mathfrak{p})$. This identification of moduli spaces is constructed explicitly with rather classical complex-analytic methods applied to suitable period maps. It provides a comparatively elementary way of proving that the absolute Galois group acts on the curves $\Delta(\mathfrak{p})\backslash\mathfrak{H}$ by permuting the ideals $\mathfrak{p}$ in the obvious way, and we derive consequences about the fields of definition and moduli fields of $\Delta(\mathfrak{p})\backslash\mathfrak{H}$. Again these results specialise to Hurwitz curves: for $r = 7$ the curves $\Delta(\mathfrak{p})\backslash\mathfrak{H}$ are Hurwitz curves, and our results in this special case reprove and reconcile older results on Hurwitz curves by Džambić, Macbeath and Streit.

1.4 Acknowledgements

First and foremost I wish to thank my supervisor, Ursula Hamenstädt, who taught me a great amount of mathematics and supported me throughout the four years of my existence as a PhD student which are now coming to an end. Particularly in those difficult phases when things did not go as smoothly as one might wish she always took the time to listen to my problems and helped me to find a way. Thank you!

I also would like to thank Jakob Stix for agreeing to serve as a second referee for this thesis; many colleagues from the mathematical community for interesting and helpful mathematical conversations; my fellow graduate students, friends and family for support in various ways that made these four years so much richer than they would have been without them.

Chapter 2

On copies of the absolute Galois group in $\operatorname{Out}\hat{F}_2$

2.1 Introduction

One of the most important consequences of Belyĭ's three points theorem [7] is the existence of a continuous injective homomorphism

$$\varrho_{01\infty}\colon G_{\mathbb{Q}} \hookrightarrow \operatorname{Out}\hat{F}_2, \tag{2.1}$$

where $G_{\mathbb{Q}} = \operatorname{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ is the absolute Galois group of the rational numbers, $\hat{F}_2$ is the profinite completion of a free group on two letters and Out denotes the outer isomorphism group. This map is obtained from the short exact sequence of étale fundamental groups

$$1 \to \pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0,1,\infty\}, *) \to \pi_1(\mathbb{P}^1_{\mathbb{Q}} \smallsetminus \{0,1,\infty\}, *) \to G_k \to 1 \tag{2.2}$$

in which the kernel can be identified with the profinite completion of

$$\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \smallsetminus \{0,1,\infty\}, *) \simeq F_2.$$

Choosing a base point $*$ defined over $\mathbb{Q}$ we obtain a splitting of the sequence (2.2) and hence a lift of (2.1) to an injection

$$G_{\mathbb{Q}} \hookrightarrow \operatorname{Aut}\hat{F}_2; \tag{2.3}$$

the most popular base point is the tangential base point $* = \overrightarrow{01}$ as defined in [22]. Alexander Grothendieck urged his fellow mathematicians in [32] to study the image of (2.1) or (2.3) with the hope of arriving at a purely combinatorial description of $G_{\mathbb{Q}}$. He gave a candidate for the image, known today as the (profinite) Grothendieck–Teichmüller group $\widehat{\mathrm{GT}} \subset \operatorname{Aut}\hat{F}_2$ (see [78] for an overview). By construction $G_{\mathbb{Q}} \hookrightarrow \widehat{\mathrm{GT}}$, but the other inclusion remains an open conjecture.

There are, however, still other embeddings $G_K \hookrightarrow \operatorname{Out}\hat{F}_2$ for each number field $K \subset \mathbb{C}$. For each elliptic curve E over K we set $E^* = E \smallsetminus \{0\}$ and obtain a short exact sequence

$$1 \to \pi_1(E^*_{\overline{\mathbb{Q}}}) \to \pi_1(E^*) \to G_K \to 1$$

analogous to (2.2). Choosing a basis $\mathfrak{B}$ of $H_1(E(\mathbb{C}),\mathbb{Z})$ we construct an identification $\pi_1(E^*_{\overline{\mathbb{Q}}}) \simeq \hat{F}_2$ below, and hence an injection

$$\varrho_E = \varrho_{E,\mathfrak{B}} \colon G_K \hookrightarrow \operatorname{Out}\hat{F}_2.$$

We will actually require this basis to be positive, i.e. positively oriented for the intersection pairing.

Theorem A. *For $j = 1,2$ let $K_j \subset \mathbb{C}$ be a number field, E_j an elliptic curve over K_j and $\mathfrak{B}_j$ a positive basis of $H_1(E_j(\mathbb{C}),\mathbb{Z})$. Assume that*

$$\varrho_{E_1,\mathfrak{B}_1}(G_{K_1}) = \varrho_{E_2,\mathfrak{B}_2}(G_{K_2})$$

as subgroups of $\operatorname{Out}\hat{F}_2$*. Then $K_1 = K_2$ and there exists an isomorphism $E_1 \simeq E_2$ over K_1 sending $\mathfrak{B}_1$ to $\mathfrak{B}_2$.*

It is necessary to assume that the bases are positive: let τ denote complex conjugation, let K be a non-real number field with $\tau(K) = K$ and let E be an elliptic curve over K with E not isomorphic to $\tau(E)$. Then complex conjugation defines a real diffeomorphism $E(\mathbb{C}) \to \tau(E)(\mathbb{C})$ sending each positive basis $\mathfrak{B}$ of $H_1(E(\mathbb{C}),\mathbb{Z})$ to a negative basis $\tau(\mathfrak{B})$ of $H_1(\tau(E)(\mathbb{C}),\mathbb{Z})$, and $\varrho_{E,\mathfrak{B}}$ and $\varrho_{\tau(E),\tau(\mathfrak{B})}$ have the same image.

2.2 Some anabelian geometry

We recall some facts about étale fundamental groups of hyperbolic curves over number fields.

Definition 2.1. *Let k be a field and Y a smooth curve over k. Let X be the smooth projective completion of Y and $S = X(\overline{k}) \smallsetminus Y(\overline{k})$; let g be the genus of X and n the cardinality of S. Then Y is called* hyperbolic *if $\chi(Y) = 2 - 2g - n < 0$.*

If $k \subseteq \mathbb{C}$ then Y is hyperbolic if and only if the universal covering space of $Y(\mathbb{C})$ is biholomorphic to the unit disk. Both $\mathbb{P}^1$ minus three points and an elliptic curve minus its origin are hyperbolic.

Now assume that $k = K \subset \mathbb{C}$ is a number field. By [1, XIII 4.3] the sequence

$$1 \to \pi_1(Y_{\overline{\mathbb{Q}}},*) \to \pi_1(Y,*) \to G_K \to 1 \tag{2.4}$$

induced by the “fibration” $Y_{\overline{\mathbb{Q}}} \to Y \to \operatorname{Spec} K$ is exact. By the usual group-theoretic constructions this sequence defines a homomorphism

$$G_K \to \operatorname{Out}\pi_1(Y_{\overline{\mathbb{Q}}},*), \tag{2.5}$$

and the group $\pi_1(Y_{\overline{\mathbb{Q}}},*)$ is the profinite completion of $\pi_1^{\mathrm{top}}(Y(\mathbb{C}),*)$, which is either a free group (in the affine case) or can be presented as

$$\langle a_1,\dots,a_g,b_1,\dots,b_g \mid [a_1,b_1]\cdots[a_g,b_g] = 1\rangle.$$

Proposition 2.2. *The homomorphism (2.5) is injective.*

Proof. This is [36, Theorem C]. □

We also note for later use that the sequence (2.4) can be reconstructed from (2.5):

Lemma 2.3. *Let G be a profinite group, and let π be a profinite group which is isomorphic to the étale fundamental group of a hyperbolic curve over $\mathbb{C}$. Let $\varphi\colon G \to \operatorname{Out}\pi$ be a continuous group homomorphism. Then there exists a short exact sequence*

$$1 \to \pi \to H \to G \to 1$$

inducing φ, and it is unique in the sense that if another such sequence is given with H' in the middle, then there exists an isomorphism $H' \to H$ such that the diagram

$$\begin{tikzcd}
1 \arrow[r] & \pi \arrow[r] \arrow[d, equal] & H \arrow[r] \arrow[d, "\simeq"] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \pi \arrow[r] & H' \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

commutes.

Proof. Let $\mathscr{Z}(\pi)$ denote the centre of π. The obstruction to the existence of such a sequence is a class in $H^3(G, \mathscr{Z}(\pi))$ by [51, Chapter IV, Theorem 8.7], but since $\mathscr{Z}(\pi)$ is trivial by [4, Proposition 18], the obstruction is automatically zero. Given the existence of one such sequence, the isomorphism classes of all such sequences are in bijection with $H^2(G, \mathscr{Z}(\pi)) = 0$ by [51, Chapter IV, Theorem 8.8]. □

We may safely ignore basepoints for the following reason: if $y, y' \in Y(\overline{\mathbb{Q}})$ then there exists an isomorphism $\pi_1(Y_{\mathbb{Q}}, y) \simeq \pi_1(Y_{\mathbb{Q}}, y')$, canonical up to inner automorphisms. Hence the outer automophism groups of both are canonically identified. Furthermore, since both basepoints map to the same tautological base point of $\operatorname{Spec} k$, the whole sequence (2.4) is changed only by inner automorphisms of the kernel when basepoints are changed within $Y(\overline{\mathbb{Q}})$. So we drop basepoints from the notation in the sequel.

If X and Y are hyperbolic curves over a number field K and $f\colon X \to Y$ is an isomorphism, we obtain a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(X_{\overline{\mathbb{Q}}}) \arrow[r] \arrow[d, "\simeq"] & \pi_1(X) \arrow[r] \arrow[d, "\simeq"] & G_K \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \pi_1(Y_{\overline{\mathbb{Q}}}) \arrow[r] & \pi_1(Y) \arrow[r] & G_K \arrow[r] & 1.
\end{tikzcd} \tag{2.6}$$

Theorem 2.4. *Let K be a number field and X, Y hyperbolic curves over K. Let $f\colon \pi_1(X) \to \pi_1(Y)$ be an isomorphism of fundamental groups commuting with the projections to G_K. Then f is induced by a unique isomorphism of K-varieties $X \to Y$, and can be inserted into a commutative diagram of the form (2.6).*

Proof. This holds more generally for K finitely generated over $\mathbb{Q}$. It was conjectured by Grothendieck in [31], proved in the affine case by Tamagawa in [93, Theorem 0.3] and in the projective case by Mochizuki in [61]. □

2.3 The Galois actions

Let F_2 be the free group on two letters a, b and let $\hat{F}_2$ be its profinite completion. Consider the following objects:

(i) a number field $K \subset \mathbb{C}$,
(ii) an elliptic curve E over K and
(iii) a basis $\mathfrak{B}$ of the homology group $H_1(E(\mathbb{C}), \mathbb{Z})$.

Let $E^* = E \smallsetminus \{0\}$, then $\pi_1^{\mathrm{top}}(E^*(\mathbb{C}))$ is a free group of rank two whose maximal abelian quotient can be identified with $H_1(E(\mathbb{C}), \mathbb{Z})$. By the following lemma, the group isomorphism

$$\mathbb{Z}^2 \to H_1(E(\mathbb{C}), \mathbb{Z}), \quad (m, n) \mapsto mx + ny \text{ where } \mathfrak{B} = (x, y)$$

can be lifted uniquely to an outer isomorphism class

$$F_2 \dashrightarrow \pi_1^{\mathrm{top}}(E^*(\mathbb{C})), \tag{2.7}$$

i.e. a group isomorphism which is well-defined up to inner automorphisms (which allows us to drop the basepoint for the fundamental group).

Lemma 2.5. *Let F and G be free groups of rank two, and let $f\colon F^{\mathrm{ab}} \to G^{\mathrm{ab}}$ be an isomorphism between their maximal abelian quotients. Then there exists an isomorphism $\tilde{f}\colon F \to G$ inducing F; it is uniquely determined by f up to inner automorphisms of F.*

Proof. It is enough to prove this lemma in the case where $F = G = F_2$; but this is a reformulation of the well-known result that the natural map

$$\operatorname{Out} F_2 \to \operatorname{Aut}(\mathbb{Z}^2) = \mathrm{GL}(2, \mathbb{Z})$$

is an isomorphism. □

Since the profinite completion of $\pi_1^{\mathrm{top}}(E^*(\mathbb{C}))$ can be identified with $\pi_1(E^*_{\overline{\mathbb{Q}}})$ we obtain an outer isomorphism class

$$\iota_{\mathfrak{B}}\colon \hat{F}_2 \dashrightarrow \pi_1(E^*_{\overline{\mathbb{Q}}}). \tag{2.8}$$

Hence pulling back the Galois action on $\pi_1(E^*_{\overline{\mathbb{Q}}})$ along (2.8) defines an injective homomorphism

$$\varrho_{E,\mathfrak{B}}\colon G_K \hookrightarrow \operatorname{Out} \hat{F}_2. \tag{2.9}$$

Lemma 2.6. *Let E be an elliptic curve over $\overline{\mathbb{Q}}$ and let $\sigma \in G_{\mathbb{Q}}$. Let $f\colon \pi_1(E^*) \dashrightarrow \pi_1(\sigma(E^*))$ be an outer isomorphism class of profinite groups which can be obtained in each of the following ways:*

(i) it is the map of étale fundamental groups induced via functoriality by the tautological isomorphism of schemes $t\colon E^* \to \sigma(E^*)$;

(ii) it is the profinite completion of an outer isomorphism class

$$\pi_1^{\mathrm{top}}(E^*(\mathbb{C})) \dashrightarrow \pi_1^{\mathrm{top}}(\sigma(E^*)(\mathbb{C}))$$

induced by an orientation-preserving isomorphism of real Lie groups $h\colon E(\mathbb{C}) \to \sigma(E)(\mathbb{C})$.

Then σ is the identity, and so is the group isomorphism in (ii).

Proof. We write $E^\dagger = E \smallsetminus E[2]$; the multiplication-by-2 map is a normal étale covering $E^\dagger \to E^*$, therefore $\pi_1(E^\dagger)$ is a normal open subgroup of $\pi_1(E^*)$. From assumption (i) we see that f maps $\pi_1(E^\dagger)$ isomorphically to $\pi_1(\sigma(E^\dagger))$. Similarly h maps $E[2]$ to $\sigma(E)[2]$, hence (i) and (ii) hold with every $*$ replaced by $\dagger$.

The quotient of $E^\dagger$ by the identification $x \sim -x$ is isomorphic over $\overline{\mathbb{Q}}$ to a scheme of the form $\mathbb{P}^1 \smallsetminus \{0,1,\infty,\lambda\}$, and we obtain a commutative diagram of schemes

$$\begin{tikzcd}
E^\dagger \arrow[r, "\wp"] \arrow[d, "t"'] & \mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0,1,\infty,\lambda\} \arrow[r, "\iota"] \arrow[d, "t"'] & \mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0,1,\infty\} \arrow[d, "t"'] \\
\sigma(E^\dagger) \arrow[r, "\wp"'] & \mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0,1,\infty,\sigma(\lambda)\} \arrow[r, "\iota"'] & \mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0,1,\infty\}
\end{tikzcd} \tag{2.10}$$

where the horizontal maps are morphisms of $\overline{\mathbb{Q}}$-schemes and the vertical maps are all base change morphisms along $\sigma\colon \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$. (The maps $\wp$ are not necessarily Weierstraß $\wp$-functions, but up to Möbius transformations on $\mathbb{P}^1$ they are, whence our sloppy notation.)

There is a very similar commutative diagram of topological spaces:

$$\begin{tikzcd}
E^\dagger(\mathbb{C}) \arrow[r, "\wp"] \arrow[d, "h"'] & \mathbb{P}^1(\mathbb{C}) \smallsetminus \{0,1,\infty,\lambda\} \arrow[r, "\iota"] \arrow[d, "H"'] & \mathbb{P}^1(\mathbb{C}) \smallsetminus \{0,1,\infty\} \arrow[d, "H"'] \\
\sigma(E^\dagger)(\mathbb{C}) \arrow[r, "\wp"'] & \mathbb{P}^1(\mathbb{C}) \smallsetminus \{0,1,\infty,\sigma(\lambda)\} \arrow[r, "\iota"'] & \mathbb{P}^1(\mathbb{C}) \smallsetminus \{0,1,\infty\}
\end{tikzcd} \tag{2.11}$$

where the horizontal maps are isomorphisms of Riemann surfaces and the vertical maps are orientation-preserving homeomorphisms. We claim that two diagrams (2.10) and (2.11) induce the same commutative diagrams of outer homomorphisms between the étale fundamental groups: the groups are clearly the same, and so are the homomorphisms induced by the horizontal maps and by the leftmost vertical maps. But since the composition

$$E^\dagger \xrightarrow{\wp} \mathbb{P}^1 \smallsetminus \{0,1,\infty,\lambda\} \xrightarrow{\iota} \mathbb{P}^1 \smallsetminus \{0,1,\infty\}$$

induces a surjection on fundamental groups (which is easily checked in the topological case), the other vertical maps also have to induce the same homomorphisms.

In particular the base change map t induced by $\sigma\colon \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ and the orientation-preserving homeomorphism H define the same element in $\operatorname{Out} \pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0,1,\infty\})$. But H is homotopic to the identity, hence this element has to be trivial; and by Proposition 2.2 for $Y = \mathbb{P}^1 \smallsetminus \{0,1,\infty\}$ the automorphism σ has to be trivial, too. □

We note a result closely related to Lemma 2.6:

Theorem 2.7 (Matsumoto–Tamagawa). *Let E be an elliptic curve defined over a number field $K \subset \mathbb{C}$. Then the images of the outer Galois representation*

$$\operatorname{Gal}(\overline{\mathbb{Q}}|K) \to \operatorname{Out} \pi_1(\overline{E}^*)$$

and the profinite closure of the topological monodromy

$$\widehat{\mathrm{SL}(2,\mathbb{Z})} \to \operatorname{Out}\pi_1(\overline{E}^*)$$

intersect trivially.

We also need one more result on isomorphisms, this time between Galois groups. Let K and L be number fields in $\mathbb{C}$, and assume that $\sigma \in G_{\mathbb{Q}}$ satisfies $\sigma(K) = L$. Then we can define a group isomorphism

$$\Phi_\sigma \colon G_K \to G_L, \quad \tau \mapsto \sigma\tau\sigma^{-1}.$$

Theorem 2.8 (Neukirch–Uchida)**.** *Let $K, L \subset \mathbb{C}$ be number fields and let $\Phi\colon G_K \to G_L$ be a continuous group isomorphism. Then there exists a unique $\sigma \in G_{\mathbb{Q}}$ with $\sigma(K) = L$ and $\Phi = \Phi_\sigma$.*

For the proof see [94].

Proof of Theorem A. The bases $\mathfrak{B}_j$ of $H_1(E_j(\mathbb{C}), \mathbb{Z})$ define an orientation-preserving isomorphism between these two cohomology groups, hence an orientation-preserving isomorphism of *real* Lie groups $h\colon E_1(\mathbb{C}) \to E_2(\mathbb{C})$ and an isomorphism of profinite fundamental groups

$$h_* = \iota_{\mathfrak{B}_2}^{-1} \circ \iota_{\mathfrak{B}_1} \colon \pi_1(E^*_{1,\overline{\mathbb{Q}}}) \to \pi_1(E^*_{2,\overline{\mathbb{Q}}}).$$

Since the representations ϱ_{E_j} are injective there is a unique isomorphism of profinite groups $\Phi\colon G_{K_1} \to G_{K_2}$ such that $\varrho_{E_1} = \varrho_{E_2} \circ \Phi$. By Theorem 2.8 this has to be of the form Φ_σ for a unique isomorphism $\sigma \in G_{\mathbb{Q}}$ with $\sigma(K_1) = K_2$. We shall construct an isomorphism $\sigma(E_1) \to E_2$ of elliptic curves over K_2.

Consider the short exact homotopy sequences for the three varieties $\sigma(E_1)$, E_1, E_2 over their respective base fields; they can be completed to the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(\sigma(\overline{E}_1^*)) \arrow[r] \arrow[d, "m_*"', "\simeq"] & \pi_1(\sigma(E_1^*)) \arrow[r] \arrow[d, "m_*"', "\simeq"] & G_{K_2} \arrow[r] \arrow[d, "\Phi_\sigma^{-1}"'] & 1 \\
1 \arrow[r] & \pi_1(\overline{E}_1^*) \arrow[r] \arrow[d, "h_*"', "\simeq"] & \pi_1(E_1^*) \arrow[r] & G_{K_1} \arrow[r] \arrow[d, "\Phi_\sigma"'] & 1 \\
1 \arrow[r] & \pi_1(\overline{E}_2^*) \arrow[r] & \pi_1(E_2^*) \arrow[r] & G_{K_2} \arrow[r] & 1.
\end{tikzcd}$$

Here the lower rectangle commutes trivially by exactness of the rows, and the upper two squares commute by functoriality of the fundamental group. From Lemma 2.3 we obtain an isomorphism $F\colon \pi_1(E_1^*)\pi_1(E_2^*)$ that makes the resulting diagram commute:

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(\sigma(E^*_{1,\overline{\mathbb{Q}}})) \arrow[r] \arrow[d, "m_*"', "\simeq"] & \pi_1(\sigma(E^*_1)) \arrow[r] \arrow[d, "m_*"', "\simeq"] & G_{K_2} \arrow[r] \arrow[d, "\Phi_\sigma^{-1}"'] & 1 \\
1 \arrow[r] & \pi_1(E^*_{1,\overline{\mathbb{Q}}}) \arrow[r] \arrow[d, "h_*"', "\simeq"] & \pi_1(E^*_1) \arrow[r] \arrow[d, "F"'] & G_{K_1} \arrow[r] \arrow[d, "\Phi_\sigma"'] & 1 \\
1 \arrow[r] & \pi_1(E^*_{2,\overline{\mathbb{Q}}}) \arrow[r] & \pi_1(E^*_2) \arrow[r] & G_{K_2} \arrow[r] & 1.
\end{tikzcd}$$

By Theorem 2.4 the group isomorphism $F \circ m_* \colon \pi_1(\sigma(E^*_1)) \to \pi_1(E^*_2)$ must be induced by a unique isomorphism $g \colon \sigma(E_1) \to E_2$ of K_2-schemes. But this means that

$$m_* \colon \pi_1(\sigma(E^*_{1,\overline{\mathbb{Q}}})) \to \pi_1(E^*_{1,\overline{\mathbb{Q}}})$$

is induced by the orientation-preserving homeomorphism

$$h^{-1} \circ g^{\mathrm{an}};$$

by Lemma 2.6 we find that σ must be the identity, so $K_1 = K_2$ and g is the desired isomorphism. □

2.4 Concluding remarks

From Theorem A we can easily deduce several analogous statements. To state the first corollary, recall that two subgroups H', H'' of a group G are called directly commensurable if $H' \cap H''$ has finite index both in H' and in H''; they are called widely commensurable if $gH'g^{-1}$ and H'' are directly commensurable for some $g \in G$.

Corollary 2.9. *For $j = 1, 2$ let $K_j \subset \mathbb{C}$ be a number field, E_j an elliptic curve over K_j and $\mathfrak{B}_j$ a positive basis of $H_1(E_j(\mathbb{C}), \mathbb{Z})$. Let I_j be the image of $\varrho_{E_j,\mathfrak{B}_j} \colon G_{K_j} \to \operatorname{Out} \hat{F}_2$.*

(i) $I_1 = I_2$ if and only if $K_1 = K_2$ and there exists an isomorphism $E_1 \simeq E_2$ over K_1 sending $\mathfrak{B}_1$ to $\mathfrak{B}_2$.

(ii) I_1 and I_2 are conjugate in $\operatorname{Out} \hat{F}_2$ if and only if $K_1 = K_2$ and $E_1 \simeq E_2$ as elliptic curves over K_1.

(iii) I_1 and I_2 are directly commensurable if and only if there exists an isomorphism $E_{1,\mathbb{C}} \to E_{2,\mathbb{C}}$ sending $\mathfrak{B}_1$ to $\mathfrak{B}_2$.

(iv) I_1 and I_2 are widely commensurable if and only if $E_{1,\mathbb{C}} \simeq E_{2,\mathbb{C}}$.

Proof. (i) is Theorem A and (ii) is Theorem 2.4. For (iii) we can find an open subgroup G_{L_j} of each G_{K_j} such that these two subgroups have the same image; we can then apply (i) to $E_i \otimes_{K_i} L_i$. Vice versa any isomorphism between two elliptic curves over $\mathbb{C}$ that admit models over number fields must already be defined over some number field. (iv) follows similarly from (ii). □

Corollary 2.10. *Let K be a number field, E an elliptic curve over K and $\mathfrak{B}$ a basis of $H_1(E_j(\mathbb{C}), \mathbb{Z})$. Then $\varrho_{E,\mathfrak{B}}(G_K)$ and $\varrho_{01\infty}(G_{\mathbb{Q}})$ are not widely commensurable in* $\operatorname{Out} \hat{F}_2$.

Proof. Assume they were widely commensurable; after enlarging the fields of definition K and $\mathbb{Q}$ to some suitable number fields L_1, L_2 the two Galois images would actually be conjugate in $\operatorname{Out} \hat{F}_2$. As in the proof of Theorem A we would obtain an isomorphism $\sigma \in G_{\mathbb{Q}}$ with $\sigma(L_1) = L_2$ and a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(\sigma(E^*_{\overline{\mathbb{Q}}})) \arrow[r] \arrow[d, "\simeq"] & \pi_1(\sigma(E)_{L_2}) \arrow[r] \arrow[d, "\simeq"] & G_{L_2} \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0,1,\infty\}) \arrow[r] & \pi_1(\mathbb{P}^1_{L_2} \smallsetminus \{0,1,\infty\}) \arrow[r] & G_{L_2} \arrow[r] & 1,
\end{tikzcd}$$

hence by Theorem 2.4 an isomorphism $\sigma(E^*_{\overline{\mathbb{Q}}}) \to \mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0, 1, \infty\}$ which is absurd. □

Chapter 3

Jarden's property and Hurwitz curves

3.1 Introduction and statement of results

In this introduction we first present the two main themes of this chapter and then explain how they go together. Proofs will be provided in the later sections.

3.1.1 Hurwitz curves and translation surfaces.

By a well-known theorem of Hurwitz [38] a (smooth projective) curve of genus $g \geq 2$ over $\mathbb{C}$ has no more than $84(g-1)$ automorphisms. Curves which attain this bound are called *Hurwitz curves.* They are relatively rare: Conder computed [16] that there are only 92 Hurwitz curves of genus less than one million, with only 32 different genera occurring. Furthermore, the series $\sum_X g(X)^{-s}$, where X runs over all Hurwitz curves, converges precisely for $\Re(s) > \frac{1}{3}$, see [48]. And yet:

Theorem 3.1. *The absolute Galois group $\Gamma_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ operates faithfully on the set of isomorphism classes of Hurwitz curves.*

This is to be understood as follows: every Hurwitz curve has a unique model over $\overline{\mathbb{Q}}$, and conjugating it by an automorphism of $\overline{\mathbb{Q}}$ will yield another, possibly different, Hurwitz curve.

Theorem 3.1 can be understood as a special case of a more general result about the Galois action on dessins d'enfants[1]:

Theorem 3.2. *Let $p, q, r \in \mathbb{N}$ with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. Then $\Gamma_{\mathbb{Q}}$ acts faithfully on the set of all regular*[2] *dessins d'enfants where the white vertices have degree dividing p, the black vertices degree dividing q and the cells are $2r'$-gons with $r' \mid r$.*

One can ask similar questions for translation surfaces[3]; this has been initiated

[1] For dessins d'enfants see [84].

[2] A dessin is called regular if the canonical morphism to $\mathbb{CP}^1$ is a Galois covering.

[3] A translation surface is a closed Riemann surface with a nonzero holomorphic one-form; for more geometric descriptions, see [37].

in [75]. There it is shown that a translation surface of genus $g \geq 2$ has at most $4(g-1)$ automorphisms, and surfaces achieving this bound are named *Hurwitz translation surfaces.* They are more common than Hurwitz curves; for example, a Hurwitz translation surface exists in genus g if and only if $g \equiv 1, 3, 4, 5 \bmod 6$, see [75, Theorem 2]. We show similarly:

Theorem 3.3. *The absolute Galois group $\Gamma_{\mathbb{Q}}$ operates faithfully on the set of isomorphism classes of Hurwitz translation surfaces.*

For the precise definition of this operation see below.

Finally we can deduce consequences for the mod ℓ Galois representations associated with Hurwitz curves:

Theorem 3.4. *Fix an element $\sigma \in \Gamma_{\mathbb{Q}}$ other than the identity. Then there exists a Hurwitz curve Y with moduli field $\mathbb{Q}$ such that for any model*[4] *$\mathscr{Y}$ of Y over $\mathbb{Q}$ and for every odd prime ℓ, the image of σ under the representation $\varrho_{\mathscr{Y},\ell} \colon \Gamma_{\mathbb{Q}} \to \mathrm{GL}(2g, \mathbb{F}_\ell)$ is not the identity.*

Here $\varrho_{\mathscr{Y},\ell}$ is the usual Galois representation on the ℓ-torsion of the Jacobian, $(\operatorname{Jac} Y)[\ell] \cong \mathbb{F}_\ell^{2g}$. A similar statement holds for Hurwitz translation surfaces, where "with moduli field $\mathbb{Q}$" must be replaced by "admitting a model over $\mathbb{Q}$".

Theorems 1 to 4 are proved, in this order, from page 34 onwards. To obtain these results we use Jarden's property for certain étale fundamental groups. Since we believe this to be of independent interest, we now give a short introduction to Jarden's property.

3.1.2 Jarden's property.

Let G be a profinite group and let F be an open normal subgroup of G. An automorphism[5] φ of G is called *F-normal* if $\varphi(N) = N$ for every open subgroup $N \subseteq F \subseteq G$ which is normal in G (not necessarily in F). Inner automorphisms are evidently F-normal. Instead of "G-normal", we simply say "normal".[6]

Definition 3.5. *A pair of profinite groups (G, F) with $F \subseteq G$ an open subgroup has* Jarden's property *if every F-normal automorphism of G is inner. A profinite group G has* Jarden's property *if every normal automorphism of G is inner.*

The first discussion of this property is in [39]: free profinite groups on at least two (possibly infinitely many) generators have Jarden's property. In [40], two further results were shown: [40, Theorem A] states that the absolute Galois group G_K has Jarden's property for every finite extension K of $\mathbb{Q}_p$, and [40, Theorem B] contains as a special case:

[4] Every Hurwitz curve admits a model over its moduli field, see [28].

[5] In this work, homomorphisms between profinite groups are always tacitly assumed to be continuous.

[6] The notion of a normal automorphism dates back to [6] and is used throughout the literature; the more general notion of an F-normal automorphism is introduced explicitly for the first time in this work, but was used implicitly in [30].

Theorem 3.6 (Jarden–Ritter). *Let Γ be a finitely presented group on e generators and d relations, with $e \geq d + 2$. Then the profinite completion of Γ has Jarden's property.*

The technical heart of the present chapter is Jarden's property for étale fundamental groups of projective hyperbolic curves and a slight generalisation:

Definition 3.7. *Let k be a field. A* closed Fuchsian orbifold *over k is a smooth Deligne-Mumford stack $\mathscr{X}$ over k with trivial generic stabilisers, admitting a finite étale covering $Y \to \mathscr{X}$ with Y a smooth projective geometrically connected curve of genus at least two over k.*

For such Deligne-Mumford stacks we can define an étale fundamental group in the usual way, and on page 33 we prove after a sequence of lemmas:

Theorem 3.8. *Let k be a separably closed field and let $\mathscr{X}_1 \to \mathscr{X}$ be an étale covering map between closed Fuchsian orbifolds over k. Then the pair of étale fundamental groups $(\pi_1^{\text{ét}}(\mathscr{X}), \pi_1^{\text{ét}}(\mathscr{X}_1))$ has Jarden's property.*

For instance for $k = \mathbb{C}$ we get Jarden's property for any pair $(\hat{\Gamma}, \hat{\Gamma}_1)$ where $\Gamma_1 \subseteq \Gamma$ are cocompact lattices in $\mathrm{PSL}(2, \mathbb{R})$ (with $\mathscr{X}(\mathbb{C}) = \Gamma \backslash \mathbb{H}$). But Theorem 3.8 is more general since it also holds in positive characteristic where the isomorphism types of such fundamental groups vary wildly, see [74].

Theorem 3.8 was proved in [30, Theorem 27] for the following special case: $k = \mathbb{C}$ and the analytification of $\mathscr{X}$ is the orbifold quotient of the upper half plane by a triangle group; in particular, $\pi_1^{\text{ét}}(\mathscr{X})$ is the profinite completion of that triangle group. Our proof of Theorem 3.8 basically follows [30], but we translate their methods, which work partly with the profinite group and partly with the discrete triangle group, into the language of ℓ-adic cohomology, thereby simplifying and generalising the argument.

3.2 Jarden's property: the proof

Let $\mathscr{X}$ and $\mathscr{X}_1$ be as in the statement of Theorem 3.8, and choose some basepoints with trivial stabilisers $\bar{x} \in \mathscr{X}(k)$ and $\bar{x}_1 \in \mathscr{X}_1(k)$ such that $\bar{x}_1$ maps to $\bar{x}$. Set $G = \pi_1^{\text{ét}}(\mathscr{X}, \bar{x})$ and $G_1 = \pi_1^{\text{ét}}(\mathscr{X}_1, \bar{x}_1)$. Finally let $\varphi\colon G \to G$ be a G_1-normal automorphism; we have to show that φ is an inner automorphism.

This is done by character theory of profinite groups with special consideration of those characters of G that appear in the ℓ-adic cohomology of finite Galois covers of $\mathscr{X}$. We begin by explaining the required notions from character theory.

Unless otherwise noted, we fix a rational prime $\ell \neq p = \operatorname{char} k$ and an algebraic closure $\overline{\mathbb{Q}}_\ell$ of the field $\mathbb{Q}_\ell$ of ℓ-adic numbers.

Definition 3.9. *Let Γ be a profinite group. A* finite representation *of Γ is a continuous group homomorphism $\varrho\colon \Gamma \to \mathrm{GL}(V)$ with finite image, where V is a finite-dimensional $\overline{\mathbb{Q}}_\ell$-vector space.*

The function $\chi\colon \Gamma \to \overline{\mathbb{Q}}_\ell$, $\gamma \mapsto \operatorname{tr} \varrho(\gamma)$, is called the character *associated with ϱ; every function arising this way for some finite representation is called a* finite character *of* Γ.

Note that the definition of finite representations and characters makes no use of the ℓ-adic topology on $\overline{\mathbb{Q}}_\ell$; we arrive at exactly the same notion if we endow it with the discrete topology — or in fact choose a field isomorphism $\overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ and demand that ϱ be continuous for the complex topology on $\mathbb{C}$. From this we deduce that the category of finite representations of Γ is semi-simple.

Lemma 3.10. *Let* $\varrho\colon \Gamma \to \mathrm{GL}(V)$ *and* $\varrho'\colon \Gamma \to \mathrm{GL}(V')$ *be two finite representations whose associated characters agree as functions on* Γ*. Then* $\varrho \cong \varrho'$*.*

Proof. There exists an open normal subgroup $\Delta \subseteq \Gamma$ such that both ϱ and ϱ' factor through the quotient Γ/Δ. They induce the same characters of Γ/Δ, hence the two representations of Γ/Δ are isomorphic[7], hence also those of Γ. □

By virtue of this lemma we may speak of the representation V_χ associated with a finite character $\chi\colon \Gamma \to \overline{\mathbb{Q}}_\ell$.

Lemma 3.11. *Let* Δ *be an open normal subgroup of a profinite group* Γ *and let* $\chi\colon \Gamma \to \overline{\mathbb{Q}}_\ell$ *and* $\psi\colon \Delta \to \overline{\mathbb{Q}}_\ell$ *be irreducible characters. Then the following are equivalent:*

(i) V_ψ *is a subrepresentation of* $V_\chi|_\Delta$ *(i.e. of* V_χ *regarded as a finite representation of* Δ*);*

(ii) the induced representation $\mathrm{Ind}_\Delta^\Gamma V_\psi$ *of* Γ *(defined as usual) contains* V_χ *as a subrepresentation.*

If these conditions are fulfilled, we say that χ lies above ψ *and that* ψ lies below χ*.*

Proof. By definition of the induced representation,

$$\mathrm{Hom}_\Delta(V_\psi, V_\chi) \cong \mathrm{Hom}_\Gamma(\mathrm{Ind}_\Delta^\Gamma V_\psi, V_\chi);$$

but as ψ and χ are irreducible, the left hand side is nozero if and only if (i) is satisfied; the right hand side is nonzero if and only if (ii) is satisfied. □

In this case Γ operates on the set $\mathrm{Irr}(\Delta)$ of irreducible finite characters of Δ: if $\psi \in \mathrm{Irr}(\Delta)$ and $\gamma \in \Gamma$, then

$$\psi^\gamma\colon \Delta \to \overline{\mathbb{Q}}_\ell, \quad \delta \mapsto \psi(\gamma\delta\gamma^{-1})$$

is again an irreducible finite character of Δ.

Theorem 3.12 (Clifford)**.** *Let* $\chi\colon \Gamma \to \overline{\mathbb{Q}}_\ell$ *be an irreducible finite character. Then the set of irreducible characters* $\Delta \to \overline{\mathbb{Q}}_\ell$ *lying below* χ *is precisely one* Γ*-orbit in* $\mathrm{Irr}(\Delta)$*.*

Proof. The corresponding statement for finite groups, from which our generalisation directly follows, is proved in [13, Theorem 1]. □

[7] see [21, Corollary 30.14]

We shall apply these concepts for $\Gamma = G = \pi_1^{\text{ét}}(\mathscr{X}, \bar{x})$ as in the beginning of this section. For this, recall that continuous finite-dimensional $\overline{\mathbb{Q}}_\ell$-representations of an étale fundamental group are equivalent to smooth $\overline{\mathbb{Q}}_\ell$-sheaves on the corresponding variety. We will not apply this to G directly but to its open normal torsion-free subgroups which are fundamental groups of honest algebraic curves.

To be more technical, let S be a connected noetherian scheme over k and $\bar{s}$ a geometric point of S. The fibre functor at $\bar{s}$ then provides an equivalence of categories

$$\left\{\begin{matrix}\text{locally constant sheaves of}\\ \text{finite abelian groups on } S\end{matrix}\right\} \xrightarrow{\sim} \left\{\begin{matrix}\text{finite abelian groups with}\\ \text{continuous } \pi_1^{\text{ét}}(S,\bar{s})\text{-action}\end{matrix}\right\} \tag{3.1}$$

and its more elaborate version

$$\{\text{smooth } \overline{\mathbb{Q}}_\ell\text{-sheaves on } S\} \xrightarrow{\sim} \left\{\begin{matrix}\text{finite-dim. cont. representations}\\ \text{of } \pi_1^{\text{ét}}(S,\bar{s}) \text{ over } \overline{\mathbb{Q}}_\ell\end{matrix}\right\}. \tag{3.2}$$

for the notion of $\overline{\mathbb{Q}}_\ell$-sheaves and the proof of this equivalence see [42, Appendix A]. A finite representation in our sense then corresponds to a smooth $\overline{\mathbb{Q}}_\ell$-sheaf which becomes trivialised on some finite étale cover of S.

In the case relevant for us, these correspondences extend to cohomology:

Proposition 3.13. *Let Y be a smooth curve of genus at least two over a separably closed field k of characteristic $p \geq 0$, and let $\mathscr{F}$ be a locally constant sheaf of finite abelian groups on X without p-torsion. Let $\mathscr{F}_{\bar{y}}$ be its fibre at $\bar{y}$. Then there is a natural isomorphism*

$$H^1(Y, \mathscr{F}) \cong H^1(\pi_1^{\text{ét}}(Y, \bar{y}), \mathscr{F}_{\bar{y}})$$

(continuous group cohomology). Similarly, let $\mathscr{F}$ be a smooth $\overline{\mathbb{Q}}_\ell$-sheaf on Y corresponding via (3.2) to the representation V of $\pi_1^{\text{ét}}(Y, \bar{y})$. Then there is a natural isomorphism of $\overline{\mathbb{Q}}_\ell$-vector spaces

$$H^1(Y, \mathscr{F}) \cong H^1(\pi_1^{\text{ét}}(Y, \bar{y}), V).$$

Proof. This is a folklore result, see e.g. [95, p. 510]. □

Now we have all technical ingredients at hand to begin with the proof of Theorem 3.8.

Consider the following scenario: $Y \to \mathscr{X}$ is an étale covering which is also normal and which factors over $\mathscr{X}_1$, and such that Y is a curve (and not merely a stack). This corresponds to an open normal subgroup $F \subseteq G$ which is torsion-free and contained in G_1. (To see that such an F exists, recall that by definition of a Fuchsian orbifold there exists a torsion-free open subgroup of G; by intersecting it with its conjugates and with G_1 we arrive at a suitable subgroup.) Then G operates via its quotient G/F on Y and therefore on its étale cohomology.

Lemma 3.14. *Let $q \neq p$ be an odd prime. Then G/F operates faithfully on the étale cohomology group $H^1(Y, \mu_q)$.*

Proof. This follows from the main result of [82], noting that G/F operates faithfully on Y. □

Similarly, G operates on $H^1(Y, \overline{\mathbb{Q}}_\ell) = H^1(F, \overline{\mathbb{Q}}_\ell)$ which is the dual of $F^{\mathrm{ab}} \otimes_{\hat{\mathbb{Z}}} \overline{\mathbb{Q}}_\ell$; the action of G can be understood as derived from that on F^{ab} via conjugation on F.

Recall that φ is a G_1-normal automorphism of G, hence $\varphi(F) = F$, and φ induces a linear automorphism of $H^1(Y, \overline{\mathbb{Q}}_\ell)$ which we denote by φ_ℓ.

Lemma 3.15. *Let $\chi\colon G \to \overline{\mathbb{Q}}_\ell$ be a finite irreducible character contained in $H^1(Y, \overline{\mathbb{Q}}_\ell)$. Then $\chi \circ \varphi = \chi$.*

To prove this lemma we need to modify ℓ conveniently, making use of:

Theorem 3.16. *Let Y be a smooth proper curve over a separably closed field of characteristic $p \geq 0$ and f an automorphism of Y. Then the trace of f acting on $H^1(Y, \overline{\mathbb{Q}}_\ell)$ is a rational integer independent of $\ell \neq p$.*

Proof of Theorem 3.16. On the other nonzero cohomology groups H^0 and H^2, f acts as the identity. Therefore our statement follows from the well-known corresponding facts for the Lefschetz number $\sum_{m=0}^{2}(-1)^m \operatorname{tr}(f^*, H^m)$, see e.g. [43, 1.3.6.(ii)c]. □

Proof of Lemma 3.15. [8] By Theorem 3.16, this statement is independent of ℓ. By this we mean the following:

Let $\ell' \neq p$ be some other prime, and choose a field isomorphism $\overline{\mathbb{Q}}_\ell \cong \overline{\mathbb{Q}}_{\ell'}$. This isomorphism induces a bijection between finite characters (i.e. between isomorphism classes of finite representations, see Lemma 3.10) of G with values in these two fields. We identify these two sets of characters by this bijection. Then by Theorem 3.16 the characters of G operating on $H^1(Y, \overline{\mathbb{Q}}_\ell)$ and $H^1(Y, \overline{\mathbb{Q}}_{\ell'})$ agree, hence an irreducible character occurs in the former if and only if it occurs in the latter. So the statement of the lemma is independent of ℓ.

Now assume that χ is defined on a finite quotient of G of order m; then for $\ell' \equiv 1 \bmod m$, which can always be found by Dirichlet's theorem on primes in arithmetic progressions, $\mathbb{Q}_{\ell'}$ contains all m-th roots of unity, hence all values of χ. To sum up, χ can be assumed to have values in $\mathbb{Q}_\ell$.

Hence χ occurs in $H^1(Y, \mathbb{Q}_\ell)$ and therefore also in its dual $F^{\mathrm{ab}} \otimes_{\hat{\mathbb{Z}}} \mathbb{Q}_\ell$. Write $F_\ell = F^{\mathrm{ab}} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell$, which is then a finitely generated free $\mathbb{Z}_\ell$-module on which G acts via G/F, and on which φ again defines a linear automorphism φ_ℓ. We claim that $\varphi_\ell(M) = M$ for every $\mathbb{Z}_\ell[G]$-submodule $M \subseteq F_\ell$.

Namely, $M = N/[F, F]$ with some closed normal subgroup N of G; since φ is normal and N is the intersection of the finite normal subgroups it is contained in, we find that $\varphi(N) = N$, whence $\varphi_\ell(M) = M$.

Now we use a trick from [39]: let $M \subseteq F_\ell$ be a $\mathbb{Z}_\ell[G]$-submodule with $M \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong V_\chi$. Then φ_ℓ is an automorphism of this module, but also G operates on M by conjugation (denoted, as usual, by exponentiation). Now unravelling of definitions yields that

$$(\varphi_\ell(m))^{\varphi(g)} = \varphi_\ell(m^g)$$

[8] following the proof of [30, Lemma 25]

for $m \in M$ and $g \in G$. That is, $\varphi(g) \circ \varphi_\ell = \varphi_\ell \circ g$ as automorphisms of M; in other words, g and $\varphi(g)$ as automorphisms of M are conjugate. Therefore they have the same trace, i.e. $\chi(g) = \chi(\varphi(g))$. □

Lemma 3.17. *Let $F \subseteq G$ as before, corresponding to $Y \to \mathscr{X}$. Let furthermore $E \subseteq F$ be another open subgroup which is normal both in F and in G; this corresponds to $Z \to Y \to \mathscr{X}$. Let $\psi \colon F \to \overline{\mathbb{Q}}_\ell$ be an irreducible finite character factoring through F/E. Then there exists an irreducible finite character $\chi \colon G \to \overline{\mathbb{Q}}_\ell$ lying above ψ with χ contained in $H^1(Z, \overline{\mathbb{Q}}_\ell)$.*

Proof. [9] Let V_ψ be the F-module corresponding to ψ, and

$$W = \operatorname{Ind}_F^G V_\psi$$

the associated G-module. Now, χ lies above ψ if and only if it is contained in W. So what we have to show is that some irreducible G-submodule of W is also contained in $H^1(Z, \overline{\mathbb{Q}}_\ell)$ or, equivalently, in its dual $E_\ell \otimes \overline{\mathbb{Q}}_\ell$; since the category of finite G-representations is semi-simple, this amounts to showing that

$$\operatorname{Hom}_G(E_\ell \otimes \overline{\mathbb{Q}}_\ell, W) \neq 0.$$

We can rewrite the left hand side:

$$\operatorname{Hom}_G(E_\ell \otimes \overline{\mathbb{Q}}_\ell, W) \cong H^1(E, W)^G \cong H^1(G, W)$$

(continuous cohomology). The second identification is justified by the inflation-restriction exact sequence

$$H^1(G/E, W^E) \longrightarrow H^1(G, W) \longrightarrow H^1(E, W)^G \longrightarrow H^2(G/E, W^E)$$

and the observation that G/E is a finite group and W^E a $\overline{\mathbb{Q}}_\ell$-vector space, so the first and the last cohomology groups vanish. Now by Shapiro's lemma (see e.g. [99, p. 172]), $H^1(G, W) \cong H^1(F, V_\psi)$ since W is induced from V and F has finite index in G. Now let $\mathscr{V}$ be the $\overline{\mathbb{Q}}_\ell$-sheaf on Z corresponding to V_ψ; we can then identify $H^1(F, V_\psi)$ with $H^1(Y, \mathscr{V})$. Finally by Theorem 3.18 below,

$$h^0(Y, \mathscr{V}) - h^1(Y, \mathscr{V}) + h^2(Y, \mathscr{V}) = e(Y, \mathscr{V}) = e(Y) \cdot \operatorname{rank} \mathscr{V} < 0,$$

whence $h^1(F, V_\psi) = h^1(Y, \mathscr{V}) > 0$. □

Theorem 3.18 (Raynaud)**.** *Let Y be a proper smooth algebraic curve over an algebraically closed base field. Let $\mathscr{F}$ be a lisse $\overline{\mathbb{Q}}_\ell$-sheaf over Y of rank d. Then the following relation holds for the Euler–Poincaré characteristics:*

$$e(Y, \mathscr{F}) = e(Y) \cdot \operatorname{rank} \mathscr{F}.$$

Proof. See [73]. □

[9] following the proof of [30, Lemma 26]

Lemma 3.19. *Let F, G and G_1 as above and let φ be a G_1-normal automorphism of G. Then φ induces an inner automorphism of G/F.*

Proof. [10] Choose some odd prime q larger than both $(G : F)$ and p. Recall that G acts on $H^1(Y, \mu_q)$. By Proposition 3.13 this cohomology group can be identified with $H^1(F, \mu_q) = \mathrm{Hom}(F, \mu_q)$. Thus interpreting cohomology classes in $H^1(F, \mu_q)$ as irreducible characters $F \to \mu_q \subset \overline{\mathbb{Q}}_\ell$, we set for every $g \in G$:

$$M^{\varphi,g} = \{\psi \in H^1(F, \mu_q) \mid \psi \circ \varphi = \psi^g\}.$$

We claim that

$$H^1(F, \mu_q) = \bigcup_{g \in G} M^{\varphi,g} : \tag{3.3}$$

let $\psi \colon F \to \mu_q$ be an element of this cohomology group, then by Lemmas 3.15 and 3.17 there exists an irreducible finite character $\chi \colon G \to \overline{\mathbb{Q}}_\ell$ of G above F with $\chi \circ \varphi = \chi$. By Theorem 3.12 this means that there exists a $g \in G$ with $\psi \circ \varphi = \psi^g$, since both ψ and $\psi \circ \varphi$ lie below χ. This proves (3.3).

Now $M^{\varphi,g}$ only depends on the residue class of g modulo F, and therefore there are at most $(G : F)$ distinct subspaces on the right hand side in (3.3). But all these spaces are finite-dimensional $\mathbb{F}_q$-vector spaces, and $q > (G : F)$. So there must be at least one of them which is already equal to $H^1(F, \mu_q)$; let us assume that $H^1(F, \mu_q) = M^{\varphi,g_0}$, i.e.

$$\psi \circ \varphi = \psi^{g_0} \text{ for all } \psi \in H^1(F, \mu_q). \tag{3.4}$$

Next, set for every $g \in G$:

$$M^g = \{\psi \in H^1(F, \mu_q) \mid \psi = \psi^g\}.$$

Since G/F operates faithfully on $H^1(F, \mu_q)$ by Lemma 3.14, M^g must be a proper $\mathbb{F}_q$-subspace of $H^1(F, \mu_q)$ whenever $g \in G \smallsetminus F$. Again, M^g only depends on the coset of g modulo F, so there are only $(G : F) - 1 < q$ distinct subspaces M^g for $g \in G \smallsetminus F$; hence they cannot cover the entire space, and there exists a $\psi_0 \in H^1(F, \mu_q)$ not contained in any of them, i.e. satisfying

$$\psi_0 \neq \psi_0^g \text{ for all } g \in G \smallsetminus F. \tag{3.5}$$

Combining (3.4) and (3.5), we obtain

$$(\psi_0)^{gg_0} = (\psi_0^g)^{g_0} = \psi_0^g \circ \varphi = (\psi_0 \circ \varphi)^{\varphi(g)} = (\psi_0^{g_0})^{\varphi(g)} = \psi_0^{g_0\varphi(g)},$$

whence $(\psi_0)^{gg_0\varphi(g)^{-1}g_0^{-1}} = \psi_0$, and by (3.5) this yields $gg_0\varphi(g)^{-1}g_0^{-1} \in F$. That is, φ operates as conjugation by g_0 on G/F. □

[10] following the proof of [30, Theorem 27]

Proof of Theorem 3.8. Recall that $G = \pi_1^{\text{ét}}(\mathscr{X}, \bar{x})$ and $G_1 = \pi_1^{\text{ét}}(\mathscr{X}_1, \bar{x}_1)$. The set $\mathscr{N}$ of those open normal subgroups $F \subseteq G$ that are contained in G_1 is cofinal in the directed set of all open normal subgroups of G, that is

$$G = \varprojlim_{F \in \mathscr{N}} G/F.$$

Now by assumption $\varphi(F) = F$ for every $F \in \mathscr{N}$, and φ operates as an inner automorphism on each G/F. Choose, for every $F \in \mathscr{N}$, an element $g_F \in G$ such that φ acts as conjugation by $g_F F$ on G/F. Since G is compact, the net $(g_F)_{F \in \mathscr{N}}$ must have a convergent subnet $(g_F)_{F \in \mathscr{M}}$. By definition of "subnet", $\mathscr{M}$ is again cofinal in all open normal subgroups, so that

$$G = \varprojlim_{F \in \mathscr{M}} G/F.$$

Let $g = \lim_{F \in \mathscr{M}} g_F \in G$. This means that for every $F \in \mathscr{M}$ there exists some $E \in \mathscr{M}$ with φ operating as conjugation by g_E on G/E; taking the limit over all these E we see that φ is indeed conjugation by g on G. □

3.3 Galois actions

Let k be a number field and let $\mathscr{X}$ be a closed Fuchsian orbifold over k. Denote the base change $\mathscr{X} \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{\mathbb{Q}}$ by $\mathscr{X}_{\overline{\mathbb{Q}}}$. Then for a geometric point $\bar{x}$ of $\mathscr{X}$ with trivial stabiliser, for simplicity assumed to lie over some point $x \in \mathscr{X}(k)$, we obtain a natural split short exact sequence of profinite groups (see [1, IX.6.1]):

$$1 \longrightarrow \pi_1^{\text{ét}}(\mathscr{X}_{\overline{\mathbb{Q}}}, \bar{x}) \longrightarrow \pi_1^{\text{ét}}(\mathscr{X}, \bar{x}) \longrightarrow \Gamma_k \longrightarrow 1. \tag{3.6}$$

This yields an action of Γ_k the "geometric fundamental group" $\pi_1^{\text{ét}}(\mathscr{X}_{\overline{\mathbb{Q}}}, \bar{x})$ and hence, after forgetting the basepoint, an outer action of Γ_k on $\pi_1^{\text{ét}}(\mathscr{X}_{\overline{\mathbb{Q}}})$. The latter action also exists if $\mathscr{X}(k) = \varnothing$ and can be constructed by Galois descent.

Proposition 3.20. *The exterior Galois action of* Γ_k *on* $\pi_1^{\text{ét}}(\mathscr{X}_{\overline{\mathbb{Q}}})$ *is faithful.*

Proof. Choose a normal étale covering $f\colon Y \to \mathscr{X}$ where Y is a geometrically connected curve (i.e. an "honest" curve and not merely a stack) over k. Choose further a point $\bar{y} \in Y(\overline{\mathbb{Q}})$ which is mapped to a point with trivial stabiliser under f, and consider the corresponding action of Γ_k on $\pi_1^{\text{ét}}(\mathscr{X}_{\overline{\mathbb{Q}}}, f(\bar{y}))$; denote the latter group by G and the subgroup $\pi_1^{\text{ét}}(Y_{\overline{\mathbb{Q}}}, \bar{y})$ by F.

Now consider the closed subgroup

$$\Delta = \{\sigma \in \Gamma_k \mid \sigma \text{ operates by an inner automorphism on } G\} \tag{3.7}$$

of Γ_k. Let $\mathscr{Z}(G)$ be the centre of G; it is a closed normal subgroup of G.[11] So we obtain a continuous group homomorphism $\varphi\colon \Delta \to G/\mathscr{Z}(G)$ defined by $\delta \in \Delta$

[11] In fact it is finite since it cannot meet F: F is centrefree by [4, Proposition 18]. We conjecture that it is trivial.

operating on G as conjugation by any element of the $\mathscr{Z}(G)$-coset $\varphi(\delta)$. Now every $\delta \in \Delta$ operates also on F as conjugation (within G) by $\varphi(\delta)$. The outer Galois action on F is faithful by [36, Theorem C], so $\varphi(\delta)$ can only be in $F \cdot \mathscr{Z}(G)$ if $\delta = \mathrm{id}$. Therefore the induced map

$$\bar{\varphi}\colon \Delta \longrightarrow G/(\mathscr{Z}(G) \cdot F) \tag{3.8}$$

is injective, but the latter group is finite. Therefore, Δ is itself finite. But it is also a normal subgroup of Γ_k; hence, it is trivial. □

With k and $\mathscr{X}$ as before, let $\mathrm{GC}(\mathscr{X}_{\overline{\mathbb{Q}}})$ (for "Galois coverings") be the set of all normal étale coverings $Y \to \mathscr{X}_{\overline{\mathbb{Q}}}$ where Y is a connected curve, up to isomorphism. Clearly Γ_k acts on $\mathrm{GC}(\mathscr{X}_{\overline{\mathbb{Q}}})$.

Corollary 3.21. *The action of* Γ_k *on* $\mathrm{GC}(\mathscr{X}_{\overline{\mathbb{Q}}})$ *is faithful.*

Proof. Assume that $\sigma \in \Gamma_k$ operates trivially on $\mathrm{GC}(\mathscr{X}_{\overline{\mathbb{Q}}})$.

Choose some normal étale covering $X_1 \to \mathscr{X}$ where X_1 is a geometrically connected curve over k, and choose convenient basepoints as above (suppressed in the notation). Every open normal subgroup of $\pi_1^{\text{ét}}(\mathscr{X}_{\overline{\mathbb{Q}}})$ contained in $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})$ defines an element of $\mathrm{GC}(\mathscr{X}_{\overline{\mathbb{Q}}})$; this amounts to an Γ_k-equivariant injection from the set of such subgroups to $\mathrm{GC}(\mathscr{X}_{\overline{\mathbb{Q}}})$. Since σ operates trivially on the image, it has to operate trivially on the domain. But by Jarden's property for the pair $(\pi_1^{\text{ét}}(\mathscr{X}_{\overline{\mathbb{Q}}}), \pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}))$ (Theorem 3.8), σ operates on $\pi_1^{\text{ét}}(\mathscr{X}_{\overline{\mathbb{Q}}})$ as an inner automorphism. By Proposition 3.20 this implies $\sigma = \mathrm{id}$. □

We now deduce Theorems 3.1 to 3.3 from Corollary 3.21 by suitable choices of $\mathscr{X}_{\overline{\mathbb{Q}}}$.

Proof of Theorem 3.1. If Y is a Hurwitz curve over $\overline{\mathbb{Q}}$, then $Y/\operatorname{Aut}(Y)$ is isomorphic to the projective line $\mathbb{P}^1$, and the projection map $X \to \mathbb{P}^1$ has precisely three ramification points, which can be taken as $0, 1, \infty$ after a suitable change of coordinates. Further, the orders of ramifications at these points are 2, 3 and 7. Vice versa, if $Y \to \mathbb{P}^1$ is a normal ramified covering with ramification points $0, 1, \infty$ and orders $2, 3, 7$ respectively, then Y is a Hurwitz curve and the Deck transformation group of this covering is the full automorphism group of Y.

That said, we consider the following Fuchsian orbifold $\mathscr{X}$ over $\mathbb{Q}$: its underlying coarse moduli space is $\mathbb{P}^1_{\mathbb{Q}}$, and it has trivial point stabilisers except for the points 0, 1 and ∞ where the stabilisers are $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$, respectively. Then the elements of $\mathrm{GC}(\mathscr{X}_{\overline{\mathbb{Q}}})$ and the isomorphism classes of Hurwitz curves are in canonical $\Gamma_{\mathbb{Q}}$-equivariant bjection, so Theorem 3.1 follows from Corollary 3.21. □

This result should be compared with the relative rarity of Hurwitz curves as mentioned in the introduction. From [16] we read that the only $g \leq 100$ such that there exist Hurwitz curves of genus g are 3, 7, 14 and 17, and the tables in [19] tell us about their behaviour under $\Gamma_{\mathbb{Q}}$:

(i) The only Hurwitz curve in genus three is *Klein's quartic curve* with homogeneous equation $x^3y + y^3z + z^3x = 0$, hence fixed by $\Gamma_\mathbb{Q}$.

(ii) The only Hurwitz curve in genus seven is the *Macbeath curve* which is therefore again fixed by $\Gamma_\mathbb{Q}$. However, no simple defining equations over $\mathbb{Q}$ are known; there is a simple model over $\mathbb{Q}(\zeta_7)$, and in [35] an extremely complicated model over $\mathbb{Q}$ was found.

(iii) In genus fourteen there are three Hurwitz curves known as the *first Hurwitz triplet*. They are defined over $k = \mathbb{Q}(\cos \frac{2\pi}{7})$ and permuted simply transitively by $\mathrm{Gal}(k|\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.

(iv) Finally, in genus seventeen there are two Hurwitz curves, defined over $\mathbb{Q}(\sqrt{-3})$ and exchanged by this field's nontrivial automorphism.

Proof of Theorem 3.2. This is analogous to the proof of Theorem 3.1, with the ramification indices $(2, 3, 7)$ replaced by (p, q, r). □

Proof of Theorem 3.3. Theorem 1 in [75] can be reinterpreted as follows: Hurwitz translation surfaces are precisely the normal translation coverings of a torus with one ramification point and ramification order two at this point. To define a Galois action, we have to fix the algebraic structure on the covered torus (actually a model over $\mathbb{Q}$). It does not matter for our proof which one we take, and the constructions in Chapter 2 define a Galois action on coverings of this torus for every elliptic curve E over $\mathbb{Q}$. Then let $\mathscr{T}$ be the Fuchsian orbifold over $\mathbb{Q}$ which has E as its coarse moduli space and precisely one point with nontrivial stabiliser; that point is the point at infinity, and its stabiliser is $\mathbb{Z}/2\mathbb{Z}$. Then Hurwitz translation surfaces are in canonical $\Gamma_\mathbb{Q}$-equivariant bijection with the elements of $\mathrm{GC}(\mathscr{T}_{\overline{\mathbb{Q}}})$. □

Proof of Theorem 3.4. Let $\mathscr{X}$ be as in the proof of Theorem 3.1, so that Hurwitz curves correspond to elements of $\mathrm{GC}(\mathscr{X}_{\overline{\mathbb{Q}}})$, and set $G = \pi_1(\mathscr{X}_{\overline{\mathbb{Q}}})$. Every open normal subgroup N of G contains one which is stable under $\Gamma_\mathbb{Q}$: the setwise stabiliser of N in $\Gamma_\mathbb{Q}$ has finite index in $\Gamma_\mathbb{Q}$, therefore

$$\tilde{N} = \bigcap_{\sigma \in \Gamma_\mathbb{Q}} \sigma(N)$$

is an open normal subgroup of G contained in N. This means that G can also be described as the projective limit of all G/N with N open, normal and stable under $\Gamma_\mathbb{Q}$. We conclude (using the compactness of G as in the proof of Theorem 3.8) that σ operates by a non-trivial outer automorphism on some such G/N. Now N corresponds to a Hurwitz curve Y with moduli field $\mathbb{Q}$; we claim that Y has the desired properties.

The Hurwitz group $H = G/N = \mathrm{Aut}_{\overline{\mathbb{Q}}} Y$ sits in a short exact sequence:

$$1 \longrightarrow \mathrm{Aut}_{\overline{\mathbb{Q}}} Y \longrightarrow \mathrm{Aut}_{\mathbb{Q}} Y \longrightarrow \Gamma_\mathbb{Q} \longrightarrow 1. \tag{3.9}$$

Here the middle term means the group of all automorphisms of Y as a $\mathbb{Q}$-scheme (or, which amounts to the same, as a scheme without any further structure). A choice of a model $\mathscr{Y}$ over $\mathbb{Q}$ yields a splitting s of this sequence.

Now $\operatorname{Aut}_{\mathbb{Q}} Y$ acts naturally on the étale cohomology group $H^1(Y, \mathbb{F}_\ell)$; by Lemma 3.14 the subgroup $H = \operatorname{Aut}_{\overline{\mathbb{Q}}} Y$ operates faithfully on this cohomology group. But Y was chosen in such a way that $s(\sigma)hs(\sigma)^{-1} \neq h$ for some $h \in H = \operatorname{Aut}_{\overline{\mathbb{Q}}} Y$, hence also these elements operate differently on $H^1(Y, \mathbb{F}_\ell)$. But this means that $s(\sigma)$ has to operate nontrivially on this cohomology group. Finally, the ℓ-torsion points of the Jacobian are canonically identified with the dual of $H^1(Y, \mathbb{F}_\ell)$, so σ also operates nontrivially there. □

Chapter 4

Modular embeddings and rigidity for Fuchsian groups

4.1 Introduction

In 1968 George Mostow published his famous Rigidity Theorem [63]: if M_1 and M_2 are two closed oriented hyperbolic manifolds of dimension $n \geq 3$ and $f\colon \pi_1(M_1) \to \pi_1(M_2)$ is a group isomorphism, then there exists a unique isometry $M_1 \to M_2$ inducing f. This can be reformulated as a statement about lattices in the orientation-preserving isometry groups $\mathrm{PSO}(1,n)$ of hyperbolic n-space $\mathbf{H}^n$:

Theorem (Mostow)**.** *Let $n \geq 3$ and let $\Gamma_1, \Gamma_2 \subset \mathrm{PSO}(1,n)$ be cocompact lattices. Let $f\colon \Gamma_1 \to \Gamma_2$ be an isomorphism of abstract groups. Then f is conjugation by some element of the full isometry group $\mathrm{PO}(1,n)$ of $\mathbf{H}^n$, in particular f extends to an algebraic automorphism of $\mathrm{PSO}(1,n)$.*

This has later been generalised by various authors; in particular, the condition that Γ_j be cocompact can be weakened to having finite covolume, see [72]. The condition that $n \neq 2$, however, is necessary: two-dimensional hyperbolic manifolds are the same as hyperbolic Riemann surfaces, which are well-known to admit deformations.

As a model for the hyperbolic plane take the upper half-plane $\mathfrak{H} = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}$, so its orientation-preserving isometry group becomes identified with $\mathrm{PSL}(2,\mathbb{R})$ via Möbius transformations. In this article we prove that a variant of Mostow Rigidity does hold in $\mathrm{Isom}^+(\mathfrak{H}) = \mathrm{PSL}(2,\mathbb{R})$ if we restrict ourselves to a certain class of lattices, for which congruence subgroups are defined, and demand that the group isomorphism preserves congruence subgroups.

We first state our result in the simpler case of arithmetic groups. Recall that given a totally real number field $k \subset \mathbb{R}$, a quaternion algebra B over k which is split over the identity embedding $k \to \mathbb{R}$ and ramified over all other infinite places of k, an order $\mathcal{O} \subset B$ and an isomorphism $\varphi\colon B \otimes_k \mathbb{R} \to \mathrm{M}(2,\mathbb{R})$ we obtain a group homomorphism $\varphi\colon \mathcal{O}^1 \to \mathrm{PSL}(2,\mathbb{R})$ whose image is a lattice, where $\mathcal{O}^1$ is the group of units in $\mathcal{O}$ with reduced norm one. A lattice $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ is called *arithmetic* if Γ is commensurable to some such $\varphi(\mathcal{O}^1)$.

For a nonzero ideal $\mathfrak{n} \subset \mathfrak{o}_k$ we then define the *principal congruence subgroup*

$$\mathcal{O}^1(\mathfrak{n}) = \{b \in \mathcal{O}^1 \mid b - 1 \in \mathfrak{n} \cdot \mathcal{O}\}.$$

If Γ contains a subgroup of finite index in $\varphi(\mathcal{O}^1)$ we set $\Gamma(\mathfrak{n}) = \Gamma \cap \varphi(\mathcal{O}^1(\mathfrak{n}))$, and a subgroup of Γ is a *congruence subgroup* if it contains some $\Gamma(\mathfrak{n})$.

Theorem (special case of Theorem A below)**.** *Let $\Gamma_1, \Gamma_2 \subset \mathrm{PSL}(2, \mathbb{R})$ be arithmetic Fuchsian groups, and let $f\colon \Gamma_1 \to \Gamma_2$ be an isomorphism of abstract groups such that for every subgroup $\Delta \subseteq \Gamma_1$ of finite index, Δ is a congruence subgroup of Γ_1 if and only if $f(\Delta)$ is a congruence subgroup of Γ_2.*

Then there exists $a \in \mathrm{PGL}(2, \mathbb{R})$ such that f is conjugation by a. In particular, $\Gamma_2 = a\Gamma_1 a^{-1}$.

Now both the notion of congruence subgroup and our result can be extended to a larger class of Fuchsian groups.

For a subgroup $\Gamma \subseteq \mathrm{PSL}(2, \mathbb{R})$ denote the preimage in $\mathrm{SL}(2, \mathbb{R})$ by $\tilde{\Gamma}$. A lattice $\Gamma \subset \mathrm{PSL}(2, \mathbb{R})$ is called *semi-arithmetic* if $\operatorname{tr}^2 \gamma$ is a totally real algebraic integer for each $\gamma \in \tilde{\Gamma}$; this notion is invariant under commensurability. It was introduced in [76], and many classes of Fuchsian groups are semi-arithmetic:

(i) Arithmetic lattices are semi-arithmetic.

(ii) All Fuchsian triangle groups $\Delta(p, q, r)$ are semi-arithmetic. However, they fall into infinitely many commensurability classes, only finitely many of which are arithmetic, see [91].

(iii) In [76] further examples of semi-arithmetic groups which are not arithmetic were constructed by giving explicit generators.

(iv) The theory of flat surfaces provides for another construction of semi-arithmetic groups. If X is a closed Riemann surface and ω is a holomorphic one-form on X which is not identically zero, a simple geometric construction yields the Veech group[1] $\mathrm{SL}(X, \omega)$ which is a discrete subgroup of $\mathrm{SL}(2, \mathbb{R})$. In certain cases the Veech group is a lattice, and then its image in $\mathrm{PSL}(2, \mathbb{R})$ is a semi-arithmetic group by [58, Theorems 5.1, 5.2] and [62, Proposition 2.6]. Veech groups are never cocompact, see [37, p. 509], therefore a Veech group which is a lattice is arithmetic if and only if it is commensurable to $\mathrm{SL}(2, \mathbb{Z})$.[2] In [58] we find, for every real quadratic number field k, the construction of a lattice Veech group contained in $\mathrm{SL}(2, \mathfrak{o}_k)$ which is therefore semi-arithmetic but not arithmetic.

Examples (ii) and (iv) intersect: in [9, Theorem 6.12] it is proved that all non-cocompact triangle groups $\Delta(p, q, \infty)$ are commensurable to some Veech group. On

[1] The name first appeared in [33] but these groups were studied before from different points of view, see [96].

[2] For a complete characterisation of (X, ω) whose Veech group is arithmetic see [33, Theorem 4].

the other hand, cocompact triangle groups can never be Veech groups, and only finitely many of the examples in [58] are commensurable with triangle groups.

The generalisation of the notion of congruence subgroups to semi-arithmetic groups is a bit involved; we refer the reader to section 4.4.

Now the conclusion of Theorem A does not hold for general semi-arithmetic groups; we need to impose one more condition which is the existence of a *modular embedding*: let $\Gamma \subset \mathrm{PSL}(2, \mathbb{R})$ be a semi-arithmetic subgroup and let k be the number field generated by all $\mathrm{tr}^2 \gamma$ with $\gamma \in \tilde{\Gamma}$. Then for every embedding $\sigma \colon k \to \mathbb{R}$ there exists a group embedding $i_\sigma \colon \tilde{\Gamma} \to \mathrm{SL}(2, \mathbb{R})$, unique up to conjugation in $\mathrm{GL}(2, \mathbb{R})$, such that $\mathrm{tr}^2 i_\sigma(\gamma) = \sigma(\mathrm{tr}^2 \gamma)$ for every $\gamma \in \tilde{\Gamma}$, see [76, Remark 4]. The original group Γ is arithmetic precisely if no $i_\sigma(\tilde{\Gamma})$ for σ different from the identity embedding contains a hyperbolic element. In general, let $\sigma_1, \ldots, \sigma_r$ be those embeddings σ for which $i_\sigma(\tilde{\Gamma})$ contains a hyperbolic element. Then the coordinate-wise embedding $(i_{\sigma_1}, \ldots, i_{\sigma_r}) \colon \Gamma \to \mathrm{PSL}(2, \mathbb{R})^r$ maps Γ to an irreducible arithmetic group $\Lambda \subset \mathrm{PSL}(2, \mathbb{R})^r$; for the precise construction see section 4.7.

We note that if Γ is not already arithmetic itself, it is mapped into Λ with Zariski-dense image of infinite index; such groups are called *thin*. This is essentially due to S. Geninska [29, Proposition 2.1 and Corollary 2.2]; we explain it below in Corollary 4.27.

Now Λ acts on $\mathfrak{H}^r$ by coordinate-wise Möbius transformations, and a *modular embedding* for Γ is then a holomorphic map $F \colon \mathfrak{H} \to \mathfrak{H}^r$ equivariant for $\Gamma \to \Lambda$.

(i) If Γ is arithmetic, then $r = 1$ and Λ contains Γ as a finite index subgroup. We may take $F(\tau) = \tau$ as a modular embedding.

(ii) All Fuchsian triangle groups admit modular embeddings, see [14, Theorem p. 96].

(iii) Most of the new examples of semi-arithmetic groups in [76] do not admit modular embeddings, see [76, Corollary 4].

(iv) Veech groups which are lattices always admit modular embeddings, see [62, Corollary 2.11]. This solves [76, Problem 1] which asks whether every Fuchsian group admitting a modular embedding is arithmetic or commensurable with a triangle group: there exist Veech groups which are neither[3], but do admit modular embeddings.

More generally, we say Γ *virtually admits a modular embedding* if some finite index subgroup of Γ admits one.

Theorem A. *For $j = 1, 2$, let $\Gamma_j \subset \mathrm{PSL}(2, \mathbb{R})$ be semi-arithmetic lattices which virtually admit modular embeddings. Let $f \colon \Gamma_1 \to \Gamma_2$ be an isomorphism of abstract*

[3] Almost all of McMullen's genus two examples in [58] do the job: only finitely many real quadratic fields appear as invariant trace fields of triangle groups, so if k is not among them, then any lattice Veech group with trace field k cannot be commensurable to a triangle group, and it cannot be arithmetic either since it is not cocompact.

groups such that for every subgroup $\Delta \subseteq \Gamma_1$ of finite index, Δ is a congruence subgroup of Γ_1 if and only if $f(\Delta)$ is a congruence subgroup of Γ_2.

Then there exists $a \in \mathrm{PGL}(2, \mathbb{R})$ such that f is conjugation by a. In particular, $\Gamma_2 = a\Gamma_1 a^{-1}$.

This theorem will be proved in section 4.8. It rests on the following result on congruence subgroups in semi-arithmetic groups, which may be of independent interest.

Theorem B. *Let $\Gamma \subset \mathrm{PSL}(2, \mathbb{R})$ be a semi-arithmetic lattice satisfying the trace field condition*[4]*, with trace field k. Then there exists a finite set $S(\Gamma)$ of rational primes with the following property:*

(i) If $\mathfrak{p}$ is a prime ideal in k not dividing any element of $S(\Gamma)$, then $\Gamma/\Gamma(\mathfrak{p}) \simeq \mathrm{PSL}(2, \mathfrak{o}_k/\mathfrak{p})$.

(ii) If q is a rational prime power not divisible by any element of $S(\Gamma)$ and Δ is a normal congruence subgroup of Γ with $\Gamma/\Delta \simeq \mathrm{PSL}(2, q)$, then there exists a unique prime ideal $\mathfrak{p}$ of k of norm q with $\Delta = \Gamma(\mathfrak{p})$.

Here, (i) is a combination of Proposition 4.10 and Lemma 4.16; (ii) is Proposition 4.30.

In particular, the information which groups $\mathrm{PSL}(2, q)$ appear how often as congruence quotients determines the splitting behaviour of all but finitely many primes in k (see Remark 4.31). On the other hand, allowing noncongruence quotients we get many more finite groups. The collection of all these finite groups will determine the abstract isomorphism type of a Fuchsian lattice, but of course no more, see [11, Theorem 1.1].

Outline. In sections 2 and 3 we fix notations and recall standard results on the group PSL(2), both over the reals and over finite fields. In sections 4 and 5 we introduce semi-arithmetic subgroups of $\mathrm{PSL}(2, \mathbb{R})$ and study their congruence subgroups. The object of section 6 is the deduction of a statement about PSL(2) from an analogous result for SL(2) by Culler and Shalen [20, Proposition 1.5.2]: a finitely generated subgroup of $\mathrm{PSL}(2, \mathbb{R})$ is determined up to conjugacy by its squared traces. This allows us to work with numbers instead of matrices in the remainder of the article. In section 7 we formally define modular embeddings and discuss some consequences of their existence. Then in section 8 the previous observations are used to prove Theorem A and the hard part of Theorem B. Section 9 presents an example with two arithmetic groups, sharpening the statement of Theorem A considerably in this special case. Finally section 10 discusses some possible and impossible generalisations.

[4] This is a technical condition which is always satisfied after passing to a finite index subgroup, see Definition 4.6.

4.2 Traces on $\mathrm{PSL}(2)$ and Möbius transformations

For every ring A we set $\mathrm{PGL}(2, A) = \mathrm{GL}(2, A)/A^\times$ where $A^\times$ is embedded by means of scalar matrices. We also set $\mathrm{PSL}(2, A) = \mathrm{SL}(2, A)/\{\pm\mathbf{1}\}$. There is an obvious homomorphism $\mathrm{PSL}(2, A) \to \mathrm{PGL}(2, A)$, but in general it is neither injective nor surjective.

Let k be a field. The determinant homomorphism $\mathrm{GL}(2, k) \to k^\times$ descends to a homomorphism $\mathrm{PGL}(2, k) \to k^\times/(k^\times)^2$, and we obtain a short exact sequence

$$1 \longrightarrow \mathrm{PSL}(2, k) \longrightarrow \mathrm{PGL}(2, k) \longrightarrow k^\times/(k^\times)^2 \longrightarrow 1. \tag{4.1}$$

In particular, $\mathrm{PSL}(2, \mathbb{C})$ and $\mathrm{PGL}(2, \mathbb{C})$ are naturally isomorphic whereas for $k = \mathbb{R}$ or a finite field of odd characteristic, $\mathrm{PSL}(2, k)$ becomes identified with an index two normal subgroup of $\mathrm{PGL}(2, k)$.

Note that since $\mathrm{PSL}(2, k)$ is a normal subgroup of $\mathrm{PGL}(2, k)$, the latter operates faithfully on the former by conjugation. Since $\mathrm{tr}(-g) = -\mathrm{tr}\, g$, the squared trace map $\mathrm{tr}^2 \colon \mathrm{SL}(2, k) \to k$ descends to a map

$$\mathrm{tr}^2 \colon \mathrm{PSL}(2, k) \to k, \quad \{g, -g\} \mapsto (\mathrm{tr}\, g)^2.$$

For $k = \mathbb{R}$ we also define

$$|\mathrm{tr}| \colon \mathrm{PSL}(2, \mathbb{R}) \to \mathbb{R}, \quad \{g, -g\} \mapsto |\mathrm{tr}\, g|.$$

Let $\mathfrak{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ be the upper half-plane. The group $\mathrm{SL}(2, \mathbb{R})$ operates on $\mathfrak{H}$ in the well-known way by Möbius transformations, descending to a faithful action by $\mathrm{PSL}(2, \mathbb{R})$. This in fact identifies $\mathrm{PSL}(2, \mathbb{R})$ with both the group of holomorphic automorphisms and that of orientation-preserving isometries (for the Poincaré metric) of $\mathfrak{H}$. Elements of $\mathrm{PSL}(2, \mathbb{R})$ can be categorised by their behaviour on $\mathfrak{H}$, see [41, section 1.3]:

Proposition 4.1. *Let $\pm\mathbf{1} \neq g \in \mathrm{PSL}(2, \mathbb{R})$. Then g belongs to exactly one of the following classes:*

(i) *g is* elliptic: *it has a unique fixed point in $\mathfrak{H}$, and $\mathrm{tr}^2 g < 4$.*

(ii) *g is* parabolic: *it has a unique fixed point in $\mathbb{P}^1(\mathbb{R})$, but not in $\mathfrak{H}$. Its squared trace satisfies $\mathrm{tr}^2 g = 4$.*

(iii) *g is* hyperbolic: *it has two distinct fixed points in $\mathbb{P}^1(\mathbb{R})$, one of them repelling and one of them attracting, but no fixed points in $\mathfrak{H}$. Its squared trace satisfies $\mathrm{tr}^2 g > 4$.*

4.3 The finite groups $\mathrm{PSL}(2, q)$

Next we study $\mathrm{PSL}(2)$ over finite fields. With $\mathbb{F}_q$ being the field of q elements we also write $\mathrm{PSL}(2, q)$ instead of $\mathrm{PSL}(2, \mathbb{F}_q)$.

Proposition 4.2. *If $q > 3$ is an odd prime power,* $\mathrm{PSL}(2,q)$ *is a simple group of order $\frac{1}{2}q(q^2-1)$. Furthermore* $\mathrm{PSL}(2,q) \simeq \mathrm{PSL}(2,q')$ *if and only if $q = q'$.*

Proof. The simplicity of $\mathrm{PSL}(2,q)$ is a well-known fact, see e.g. [100, section 3.3.2]. The order of $\mathrm{PSL}(2,q)$ is easily calculated using (4.1), for instance. The function $q \mapsto \frac{1}{2}q(q^2-1)$ is strictly increasing on $\mathbb{N}$, therefore if $\mathrm{PSL}(2,q)$ and $\mathrm{PSL}(2,q')$ have the same orders, $q = q'$. □

As remarked in section 4.2, $\mathrm{PGL}(2,q)$ operates by conjugation on $\mathrm{PSL}(2,q)$. Furthermore the Frobenius automorphism $\varphi\colon \mathbb{F}_q \to \mathbb{F}_q$ defined by $\varphi(x) = x^p$, where p is the prime of which q is a power, defines an automorphism φ of $\mathrm{PSL}(2,q)$. The following is also well-known, see e.g. [100, Theorem 3.2.(ii)]:

Proposition 4.3. *The automorphism group of* $\mathrm{PSL}(2,q)$ *is generated by* $\mathrm{PGL}(2,q)$ *and φ.*

In particular if $q = p$ is a prime, then every automorphism of $\mathrm{PSL}(2,p)$ is the restriction of an inner automorphism of $\mathrm{PGL}(2,p)$, and the map $\mathrm{tr}^2\colon \mathrm{PSL}(2,p) \to \mathbb{F}_p$ is invariant under all automorphisms. So the following definition works:

Definition 4.4. *Let G be a finite group which is abstractly isomorphic to some* $\mathrm{PSL}(2,p)$ *for an odd prime p. Then the map $\mathrm{tr}^2_G\colon G \to \mathbb{F}_p$ is defined as follows: choose some automorphism $\alpha\colon G \to \mathrm{PSL}(2,p)$, then set $\mathrm{tr}^2_G = \mathrm{tr}^2 \circ \alpha$.*

If p is replaced by a prime power q, the corresponding map on G is only are well-defined up to automorphisms of $\mathbb{F}_q$, i.e. we may define a map $\mathrm{tr}^2_G\colon G \to \mathbb{F}_q/\operatorname{Aut}\mathbb{F}_q$.

Lemma 4.5. *Let $n \in \mathbb{N}$ and let $q_1, \ldots, q_n, q'$ be odd prime powers. Let*

$$\beta\colon G = \mathrm{PSL}(2,q_1) \times \cdots \times \mathrm{PSL}(2,q_n) \to \mathrm{PSL}(2,q')$$

be a group epimorphism. Then there is a $1 \le j \le n$ such that $q' = q_j$ and for some automorphism α of $\mathrm{PSL}(2,q')$ *we can write $\beta = \alpha \circ \mathrm{pr}_j$, where pr_j is the projection on the j-th factor.*

Proof. By the Jordan–Hölder theorem, the only simple quotients of G are the $\mathrm{PSL}(2,q_j)$, so $q' = q_j$ for some j.

We now proceed by induction on n. For $n = 1$ the lemma is trivial, so assume the lemma has been proved for n. Let $\beta\colon G \to \mathrm{PSL}(2,q')$ be an epimorphism where G has $n+1$ factors. For cardinality reasons it cannot be injective, so there exists some $g \in G \smallsetminus \{1\}$ with $\beta(g) = 1$. Write $g = (g_1, \ldots, g_{n+1})$, then $g_j \neq 1$ for some j; for simplicity of notation assume that $j = n+1$. Since $\mathrm{PSL}(2,q_{n+1})$ has trivial centre, there exists some $h_{n+1} \in G$ which does not commute with g_{n+1}. Then set

$$h = (1, \ldots, 1, h_{n+1}) \in G$$

and compute

$$1 = \beta(h)\beta(h^{-1}) = \beta(ghg^{-1}h^{-1}) = \beta(1, \ldots, 1, g_{n+1}h_{n+1}g_{n+1}^{-1}h_{n+1}^{-1})$$

using $\beta(g) = 1$. That is, β restricted to the $(n+1)$-st factor has nontrivial kernel. Since that factor is simple, the restriction of β to the $(n+1)$-st factor has to be trivial, so β factors through the projection onto the first n factors, hence (by induction hypothesis) onto one of them. □

4.4 Semi-arithmetic groups and their congruence subgroups

Let $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a lattice and let $\tilde{\Gamma}$ be its preimage in $\mathrm{SL}(2,\mathbb{R})$. By $\Gamma^{(2)}$ we denote the subgroup of Γ generated by all γ^2 with $\gamma \in \Gamma$. Since Γ is finitely generated, $\Gamma^{(2)}$ is then a normal subgroup of finite index in Γ.

Definition 4.6. *The* trace field *of* Γ *is the field* $\mathbb{Q}(\operatorname{tr}\Gamma) \subset \mathbb{R}$ *generated by all* $\operatorname{tr}\gamma$ *with* $\gamma \in \tilde{\Gamma}$. *The* invariant trace field *of* Γ *is the trace field of* $\Gamma^{(2)}$.

A lattice Γ *satisfies the* trace field condition *if its trace field and its invariant trace field agree.*

Clearly the trace field contains the invariant trace field, but the two are not always equal. As the name suggests, the invariant trace field is the more useful invariant: commensurable lattices have the same invariant trace field, see [54, Theorem 3.3.4], but not necessarily the same trace field. Hence, if Γ is any lattice then $\Gamma^{(2)}$ satisfies the trace field condition. Therefore any lattice has a finite index normal sublattice which satisfies the trace field condition.

Definition 4.7. *A lattice* $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ *is called* semi-arithmetic *if its invariant trace field is a totally real number field and every trace* $\operatorname{tr}\gamma$ *for* $\gamma \in \tilde{\Gamma}$ *is an algebraic integer.*[5]

Being semi-arithmetic is stable under commensurability, therefore every semi-arithmetic lattice contains a semi-arithmetic lattice satisfying the trace field condition. For the following constructions let Γ be a semi-arithmetic lattice satisfying the trace field condition, and let $k = \mathbb{Q}(\operatorname{tr}\gamma)$. Then the sub-$k$-vector space $B = k[\Gamma]$ of $\mathrm{M}(2,\mathbb{R})$ generated by $\tilde{\Gamma}$ is in fact a sub-k-algebra, more precisely a quaternion algebra over k. The sub-$\mathfrak{o}_k$-algebra $\mathfrak{o}_k[\tilde{\Gamma}]$ of B generated by $\tilde{\Gamma}$ is an order in B, though not necessarily a maximal one. We choose a maximal order $\mathcal{O} \supseteq \mathfrak{o}_k[\tilde{\Gamma}]$.

If $\mathcal{O}^1$ denotes the subgroup of $\mathcal{O}^\times$ consisting of elements with reduced norm one, $\tilde{\Gamma}$ becomes a subgroup of $\mathcal{O}^1$. Also write $\mathrm{P}\mathcal{O}^1 = \mathcal{O}^1/\{\pm\mathbf{1}\}$ so that Γ is a subgroup of $\mathrm{P}\mathcal{O}^1$.

Proposition 4.8. *Let* $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ *be a semi-arithmetic lattice satisfying the trace field condition. Then the following are equivalent:*

(i) Γ *is arithmetic.*

(ii) Let $k = \mathbb{Q}(\operatorname{tr}\Gamma) \subset \mathbb{R}$. *Then for every embedding* $\sigma\colon k \to \mathbb{R}$ *other than the identity inclusion and every* $\gamma \in \tilde{\Gamma}$ *one has* $|\sigma(\operatorname{tr}\gamma)| \leq 2$.

[5] It follows from [54, Lemma 3.5.6] that this is equivalent to the definition given in the introduction.

(iii) For every embedding $\sigma\colon k \to \mathbb{R}$ other than the identity inclusion, $B \otimes_{k,\sigma} \mathbb{R}$ is isomorphic to Hamilton's quaternions $\mathbb{H}$.

(iv) $\mathrm{P}\mathcal{O}^1$ is a discrete subgroup of $\mathrm{PSL}(2, \mathbb{R})$.

(v) The index $(\mathrm{P}\mathcal{O}^1 : \Gamma)$ is finite.

Proof. The equivalence (i) $\Leftrightarrow$ (ii) is the main result in [90]; the other equivalences follow from the explicit classification of arithmetic lattices in $\mathrm{PSL}(2, \mathbb{R})$, see e.g. [41, chapter 5] or [54, chapter 8]. □

Now we discuss congruence subgroups. For an elementary definition, let $\Gamma \subset \mathrm{PSL}(2, \mathbb{R})$ be a semi-arithmetic lattice satisfying the trace field condition, and let k and $\mathcal{O}$ be as above. Then every nonzero ideal $\mathfrak{a}$ of $\mathfrak{o}_k$ defines a subgroup

$$\tilde{\Gamma}(\mathfrak{a}) = \{\gamma \in \tilde{\Gamma} \mid \gamma - \mathbf{1} \in \mathfrak{a} \cdot \mathcal{O}\}$$

and its image $\Gamma(\mathfrak{a})$ in Γ, called the *principal congruence subgroup* of level $\mathfrak{a}$. A *congruence subgroup* of Γ is then a subgroup containing some principal congruence subgroup. Similarly we define principal congruence subgroups $\mathcal{O}^1(\mathfrak{a})$ and congruence subgroups of $\mathcal{O}^1$.

These groups can also defined more abstractly using algebraic groups: there is a canonical linear algebraic group H over k with $H(k) = B^1$; we may define it functorially by setting $H(A) = (B \otimes_k A)^1$ for every k-algebra A. Then H is a twisted form of $\mathrm{SL}(2)_k$. By Weil restriction of scalars we obtain an algebraic group $G = \mathrm{Res}_{k|\mathbb{Q}} H$ with a canonical identification $G(\mathbb{Q}) = H(k) = B^1$. Then G is a twisted form of $\mathrm{SL}(2)_{\mathbb{Q}}^d$ where $d = [k : \mathbb{Q}]$; in particular $G(\mathbb{C})$ is isomorphic to $\mathrm{SL}(2, \mathbb{C})^d$.

Choosing a faithful representation $G \to \mathrm{GL}(n)$ we can define a congruence subgroup in $G(\mathbb{Q})$ to be one that contains the preimage of a congruence subgroup of $\mathrm{GL}(n, \mathbb{Z})$ as a finite index subgroup. This notion of congruence subgroup is independent of the representation $G \to \mathrm{GL}(n)$, see [60, Proposition 4.1]; that it is equivalent to the more elementary one given before follows by taking the representation of $G \to \mathrm{GL}(4d)$ by left multiplication on B, the latter considered as a $(4d)$-dimensional $\mathbb{Q}$-vector space with the lattice $\mathcal{O}$.

Let $\mathbb{A}^f$ be the ring of finite adèles of $\mathbb{Q}$ and endow $G(\mathbb{A}^f)$ with the adèlic topology. Similarly let $\mathbb{A}_k^f$ be the ring of finite adèles of k, then there is a canonical isomorphism $\mathbb{A}^f \otimes_{\mathbb{Q}} k = \mathbb{A}_k^f$ inducing $G(\mathbb{A}^f) = H(\mathbb{A}_k^f)$. The closure of $\mathcal{O}^1$ in $G(\mathbb{A}^f)$ can be identified with the completion of $\mathcal{O}^1$ with respect to all congruence subgroups; equivalently, with the group of elements of reduced norm one in the profinite completion of $\mathcal{O}$. Therefore we denote it by $\widehat{\mathcal{O}}^1$. It is a maximal compact open subgroup of $G(\mathbb{A}^f)$.

There is a canonical bijection between open subgroups of $\widehat{\mathcal{O}}^1$ and congruence subgroups of $\mathcal{O}^1$: with a congruence subgroup of $\mathcal{O}^1$ we associate its closure in $G(\mathbb{A}^f)$, and with an open subgroup of $\widehat{\mathcal{O}}^1$ we associate its intersection with $\mathcal{O}^1$. For the proof see again [60, Proposition 4.1].

Proposition 4.9 (Strong Approximation for Semi-Arithmetic Groups)**.** *The closure of* $\tilde{\Gamma}$ *in* $G(\mathbb{A}^f) = H(\mathbb{A}_k^f)$ *is open.*

Proof. First we claim that $\tilde{\Gamma}$ is Zariski-dense in G. It suffices to show that $\tilde{\Gamma}$ is Zariski-dense in $G(\mathbb{C}) \simeq \mathrm{SL}(2,\mathbb{C})^d$, and the proof of an analogous but more complicated statement over the reals [29, Proposition 2.1 and Corollary 2.2] carries over mutatis mutandis.

Then we use a special case of a result of M. Nori [67, Theorem 5.4], see also [57]: if G is an algebraic group over $\mathbb{Q}$ such that $G(\mathbb{C})$ is connected and simply connected (which is the case for our G since $\pi_1(\mathrm{SL}(2,\mathbb{C})) = \pi_1(\mathrm{SU}(2)) = \pi_1(S^3) = 1$) and Γ is a finitely generated Zariski-dense subgroup of $G(\mathbb{Q})$ contained in some arithmetic subgroup of G, then the closure of Γ in $G(\mathbb{A}^f)$ is open. □

Proposition 4.10. *There exists a nonzero ideal* $\mathfrak{m}$ *of* $\mathfrak{o}_k$*, depending on* Γ*, such that for every ideal* $\mathfrak{a}$ *of* $\mathfrak{o}_k$ *prime to* $\mathfrak{m}$ *the homomorphism*

$$\tilde{\Gamma} \hookrightarrow \mathcal{O}^1 \twoheadrightarrow \mathcal{O}^1/\mathcal{O}^1(\mathfrak{a})$$

is surjective, i.e. the canonical homomorphism

$$\Gamma/\Gamma(\mathfrak{a}) \to \mathrm{P}\mathcal{O}^1/\mathrm{P}\mathcal{O}^1(\mathfrak{a})$$

is an isomorphism of finite groups.

The proof uses several results that will be used later on, so we mention them separately.

Theorem 4.11 (Strong Approximation for Quaternion Algebras)**.** $G(\mathbb{Q}) = H(k)$ *is dense in* $G(\mathbb{A}^f) = H(\mathbb{A}_k^f)$.[6]

For the proof see e.g. [71, Theorem 7.12].

We shall now investigate the quotient groups $\mathcal{O}^1/\mathcal{O}^1(\mathfrak{a})$. These are best understood locally: if $\mathfrak{p}$ is a finite prime of k, we set $\mathcal{O}_\mathfrak{p} = \mathcal{O} \otimes_{\mathfrak{o}_k} \mathfrak{o}_\mathfrak{p}$. We can then consider the group $\mathcal{O}_\mathfrak{p}^1$ of its elements of norm one, and its congruence subgroups $\mathcal{O}_\mathfrak{p}^1(\hat{\mathfrak{p}}^r)$. Recall that $\mathcal{O}_\mathfrak{p}$ is a maximal order in $B_\mathfrak{p}$.

Proposition 4.12. *Let* $\mathfrak{a}$ *be an ideal of* k *with prime factorisation* $\mathfrak{a} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\cdots\mathfrak{p}_n^{r_n}$*. Then the canonical homomorphism*

$$\mathcal{O}^1/\mathcal{O}^1(\mathfrak{a}) \to \prod_{j=1}^{n} \mathcal{O}_{\mathfrak{p}_j}^1/\mathcal{O}_{\mathfrak{p}_j}^1(\hat{\mathfrak{p}}_j^{r_j}) \tag{4.2}$$

is an isomorphism of groups.

Proof. Injectivity is easy, so we only show surjectivity.

We use the description of $H(\mathbb{A}_k^f)$ as the restricted direct product of the completions $B_\mathfrak{l}^1 = (B \otimes_k k_\mathfrak{l})^1$, restricted with respect to the compact subgroups $\mathcal{O}_\mathfrak{l}^1$. For $j = 1,\ldots,n$ take an element $x_j \in \mathcal{O}_{\mathfrak{p}_j}^1$. The Strong Approximation Theorem furnishes us with an element $\beta \in H(k) = B^1$ with the following properties:

[6] Usually this result is phrased differently: if $\mathbb{A} = \mathbb{A}^f \times \mathbb{R}$ denotes the full adèle ring, then $G(\mathbb{Q}) \cdot G(\mathbb{R})$ is dense in $G(\mathbb{A})$. But the latter is canonically isomorphic to $G(\mathbb{A}^f) \times G(\mathbb{R})$ which shows the equivalence to our formulation.

- For $j = 1, \ldots, n$, β considered as an element of $B^1_{\mathfrak{p}_j}$ is congruent to x_j modulo $\mathscr{O}^1_{\mathfrak{p}_j}(\hat{\mathfrak{p}_j}^{r_j})$ (note that the latter is an open subgroup of $B^1_{\mathfrak{p}_j}$).

- For each finite prime $\mathfrak{l}$ different from all $\mathfrak{p}_j$'s, β is in $\mathscr{O}^1_{\mathfrak{l}}$.

Then $\beta \in \mathscr{O}^1$, and its class in the left hand side of (4.2) maps to $(x_1, \ldots, x_n)$. □

Note that our proof also shows that the map

$$\mathscr{O}^1/\mathscr{O}^1(\mathfrak{a}) \to \prod_{j=1}^{n} \mathscr{O}^1/\mathscr{O}^1(\mathfrak{p}_j^{r_j})$$

is an isomorphism.

Corollary 4.13. *The canonical homomorphism*

$$\mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{a}) \to \prod_{j=1}^{n} \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{p}_j^{r_j})$$

is an epimorphism whose kernel is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^d$ *for some* $d < n$.

Proof. The homomorphism $\mathscr{O}^1/\mathscr{O}^1(\mathfrak{p}_j^{r_j}) \to \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{p}_j^{r_j})$ is always surjective, and it is injective precisely when $\mathfrak{p}_j^{r_j}$ divides (2), otherwise it has kernel isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Similarly the kernel of $\mathscr{O}^1/\mathscr{O}^1(\mathfrak{a}) \to \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{a})$ is either trivial or $\mathbb{Z}/2\mathbb{Z}$. So the corollary follows from the remark preceding it. □

Corollary 4.14. *Let* $\Delta \subseteq \mathscr{O}^1$ *be a congruence subgroup, containing* $\mathscr{O}^1(\mathfrak{m})$ *for some ideal* $\mathfrak{m}$ *of* k. *Let* $\mathfrak{a}$ *be an ideal of* k *which is coprime to* $\mathfrak{m}$. *Then the composition*

$$\Delta \hookrightarrow \mathscr{O}^1 \twoheadrightarrow \mathscr{O}^1/\mathscr{O}^1(\mathfrak{a})$$

is surjective.

Proof. This is equivalent to the statement $\mathscr{O}^1(\mathfrak{m}) \cdot \mathscr{O}^1(\mathfrak{a}) = \mathscr{O}^1$, and this in turn follows from the isomorphism of finite groups

$$\mathscr{O}^1/(\mathscr{O}^1(\mathfrak{m}) \cap \mathscr{O}^1(\mathfrak{a})) \to \mathscr{O}^1/\mathscr{O}^1(\mathfrak{m}) \times \mathscr{O}^1/\mathscr{O}^1(\mathfrak{a}).$$ □

Proof of Proposition 4.10. By Proposition 4.9 there exists some ideal $\mathfrak{m}$ of k with $\mathscr{O}^1(\mathfrak{m}) \subseteq \overline{\tilde{\Gamma}}$, where the latter denotes the closure of $\tilde{\Gamma}$ in $\widehat{\mathscr{O}}^1 \subset G(\mathbb{A}^f)$. This does the job by Corollary 4.14. □

Corollary 4.15. *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be two coprime ideals of* k *which are both prime to* 2. *Then the canonical homomorphism*

$$\mathrm{P}\mathscr{O}^1(\mathfrak{a})/\mathrm{P}\mathscr{O}^1(\mathfrak{a}\mathfrak{b}) \to \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{b})$$

is an isomorphism. □

4.5 Congruence quotients of semi-arithmetic groups

Our next step is to determine the quotients on the right hand side of (4.2). This is done by distinguishing between the ramified and the unramified case. To simplify notation, let K be a p-adic field with ring of integers $\mathfrak{o}_K$ and prime ideal $\mathfrak{p} = (\pi)$. Let $q = p^f$ be the cardinality of the residue class field $\kappa = \mathfrak{o}_K/\mathfrak{p}$. Let B be an unramified quaternion algebra over K, and let $\mathcal{O} \subset B$ be a maximal order. We may assume that $B = \mathrm{M}(2, K)$ and $\mathcal{O} = \mathrm{M}(2, \mathfrak{o}_K)$; then $\mathcal{O}^1 = \mathrm{SL}(2, \mathfrak{o}_K)$ and $\mathcal{O}^1(\mathfrak{p})$ is the kernel of the reduction map $\mathrm{SL}(2, \mathfrak{o}_K) \to \mathrm{SL}(2, \kappa)$.

Lemma 4.16. *Let $r \geq 1$. The reduction map $\mathrm{SL}(2, \mathfrak{o}_K) \to \mathrm{SL}(2, \mathfrak{o}_K/\mathfrak{p}^r)$ is surjective and thus induces an isomorphism $\mathcal{O}^1/\mathcal{O}^1(\mathfrak{p}^r) \to \mathrm{SL}(2, \mathfrak{o}_K/\mathfrak{p}^r)$. In particular $\mathcal{O}^1/\mathcal{O}^1(\mathfrak{p})$ is isomorphic to $\mathrm{SL}(2, q)$.*

Proof. Let

$$\overline{\gamma} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in \mathrm{SL}(2, \mathfrak{o}_K/\mathfrak{p}^r)$$

and lift $\overline{\gamma}$ arbitrarily to a matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathfrak{o}_K).$$

The determinant $\delta = \det \gamma$ is an element of $1+\mathfrak{p}^r$, hence so is its inverse $\frac{1}{\delta}$. Therefore

$$\gamma' = \begin{pmatrix} \frac{a}{\delta} & \frac{b}{\delta} \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathfrak{o}_K)$$

still reduces to $\overline{\gamma}$. □

Lemma 4.17. *Let $r \geq 1$. Assumptions as before, the quotient $\mathcal{O}^1(\mathfrak{p}^r)/\mathcal{O}^1(\mathfrak{p}^{r+1})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{3f}$.*

Proof. We construct a map

$$(\mathcal{O}/\mathfrak{p}\mathcal{O})_0 \to \mathrm{SL}(2, \mathfrak{o}_K/\mathfrak{p}^{r+1}), \quad [A] \mapsto [1 + \pi^r A].$$

Here the left hand side denotes the subgroup of those elements of $\mathcal{O}/\mathfrak{p}\mathcal{O} = M(2, \kappa)$ that have trace $\equiv 0 \bmod \mathfrak{p}$. Note that $\det(1 + \pi^r A) \equiv 1 + \pi^r \operatorname{tr} A \bmod \mathfrak{p}^{r+1}$, so the map is indeed well-defined. It is an injective group homomorphism, and its image is precisely the image of $\mathcal{O}^1(\mathfrak{p}^r)$ in $\mathrm{SL}(2, \mathfrak{o}_K/\mathfrak{p}^{r+1})$, which is isomorphic to $\mathcal{O}^1(\mathfrak{p}^r)/\mathcal{O}^1(\mathfrak{p}^{r+1})$. □

Now we turn to the ramified case. We use the explicit descritption of B and $\mathcal{O}$ given in [54, section 6.4]. Let $L|K$ be the unique unramified quadratic extension, then B is up to isomorphism given by

$$B = \left\{ \begin{pmatrix} a & b \\ \pi b' & a' \end{pmatrix} \middle| a, b \in L \right\},$$

where $a \mapsto a'$ is the nontrivial element of $\mathrm{Gal}(L|K)$. This contains a unique maximal order,

$$\mathcal{O} = \left\{ \begin{pmatrix} a & b \\ \pi b' & a' \end{pmatrix} \middle| a, b \in \mathfrak{o}_L \right\},$$

and $\mathcal{O}$ has a unique maximal two-sided ideal,

$$\mathcal{M} = \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix} \mathcal{O} = \left\{ \begin{pmatrix} \pi a & b \\ \pi b' & \pi a' \end{pmatrix} \middle| a, b \in \mathfrak{o}_L \right\}.$$

It satisfies $\mathcal{M}^2 = \mathfrak{p}\mathcal{O}$. We define congruence subgroups $\mathcal{O}^1(\mathcal{M}^r) = \mathcal{O}^1 \cap (1 + \mathcal{M}^r)$, so that $\mathcal{O}^1(\mathfrak{p}^r) = \mathcal{O}^1(\mathcal{M}^{2r})$.

Lemma 4.18. *The quotient $\mathcal{O}^1/\mathcal{O}^1(\mathcal{M})$ is a cyclic group of order $q+1$.*

Proof. Since $L|K$ is unramified, the quotient $\lambda = \mathfrak{o}_L/\pi\mathfrak{o}_L$ is a finite field of order q^2. We construct a map

$$\mathcal{O}^1/\mathcal{O}^1(\mathcal{M}) \to \lambda^\times, \qquad \left[\begin{pmatrix} a & b \\ \pi b' & a' \end{pmatrix} \right] \mapsto a \bmod \pi.$$

This is easily seen to be an injective group homomorphism whose image is the kernel of the norm map $N_{\lambda|\kappa}$. That norm map is surjective to $\kappa^\times$, so its kernel has order $(q^2-1)/(q-1) = q+1$. □

Lemma 4.19. *Let $r \geq 1$. Then $\mathcal{O}^1(\mathcal{M}^r)/\mathcal{O}^1(\mathcal{M}^{r+1})$ is isomorphic to the additive group of κ.*

Proof. We construct injective group homomorphisms

$$\mathcal{O}^1(\mathcal{M}^{2r})/\mathcal{O}^1(\mathcal{M}^{2r+1}) \to \lambda, \qquad \left[\begin{pmatrix} a & b \\ \pi b' & a' \end{pmatrix} \right] \mapsto \frac{a-1}{\pi^r} \bmod \pi$$

and

$$\mathcal{O}^1(\mathcal{M}^{2r-1})/\mathcal{O}^1(\mathcal{M}^{2r}) \to \lambda, \qquad \left[\begin{pmatrix} a & b \\ \pi b' & a' \end{pmatrix} \right] \mapsto \frac{b}{\pi^{r-1}} \bmod \pi.$$

The image is in both cases the kernel of the trace map $\mathrm{tr}_{\lambda|\kappa}$. □

We summarise the results, reformulated for number fields:

Corollary 4.20. *Let k be a number field and B a quaternion algebra over k, unramified over at least one infinite place of k. Let $\mathcal{O} \subset B$ be a maximal order and let $\mathfrak{p}$ be a prime of k of norm $q = p^f$. Let $r \geq 1$ and $H = \mathcal{O}^1/\mathcal{O}^1(\mathfrak{p}^r)$.*

(i) If B is ramified at $\mathfrak{p}$, then H is solvable; the prime numbers appearing as orders in its composition series are p and the prime divisors of $q+1$.

(ii) If B is unramified at $\mathfrak{p}$ and $\mathfrak{p} \nmid 6$, then H is not solvable. Its composition factors are: once $\mathbb{Z}/2\mathbb{Z}$, once $\mathrm{PSL}(2,q)$ and $3f(r-1)$ times $\mathbb{Z}/p\mathbb{Z}$.

In case (ii) for $\mathfrak{p} \mid 6$ we have to replace $\mathrm{PSL}(2,q)$, which is not necessarily simple then, by its composition factors.

4.6 Characters for Fuchsian groups

In this section we prove a criterion for two isomorphic lattices in $\mathrm{PSL}(2,\mathbb{R})$ being conjugate:

Theorem 4.21. *Let Γ be a group, and for $j = 1, 2$ let $\varrho_j \colon \Gamma \to \mathrm{PSL}(2,\mathbb{R})$ be an injective group homomorphism such that $\varrho_j(\Gamma)$ is a lattice. Let $\Delta \subseteq \Gamma$ be a finite index subgroup, and assume that*

$$\mathrm{tr}^2\, \varrho_1(\gamma) = \mathrm{tr}^2\, \varrho_2(\gamma) \text{ for all } \gamma \in \Delta. \tag{4.3}$$

Then there exists a unique $a \in \mathrm{PGL}(2,\mathbb{R})$ such that $\varrho_2(\gamma) = a\varrho_1(\gamma)a^{-1}$ for all $\gamma \in \Gamma$.

The proof of Theorem 4.21 rests on the following result, see [20, Proposition 1.5.2], as well as on subsequent elementary lemmas.

Theorem 4.22 (Culler–Shalen). *Let $\varrho_1, \varrho_2 \colon \Gamma \to \mathrm{SL}(2,\mathbb{C})$ be two representations such that*

$$\mathrm{tr}\, \varrho_1(\gamma) = \mathrm{tr}\, \varrho_2(\gamma) \text{ for every } \gamma \in \Gamma, \tag{4.4}$$

and assume that ϱ_1 is irreducible. Then there exists $a \in \mathrm{SL}(2,\mathbb{C})$, unique up to sign, such that $\varrho_2(\gamma) = a\varrho_1(\gamma)a^{-1}$ for every $\gamma \in \Gamma$.

Lemma 4.23. *Let $g \in \mathrm{PSL}(2,\mathbb{R})$ and let $\Sigma \subset \mathrm{PSL}(2,\mathbb{R})$ be a group generated by two hyperbolic elements without common fixed points. Then there exists $s \in \Sigma$ with sg hyperbolic.*

Proof. Lift g to an element $G \in \mathrm{SL}(2,\mathbb{R})$. First we will show that there exists some $S \in \tilde{\Sigma}$ with $\mathrm{tr}(SG) \neq 0$.

Assume, on the contrary, that $\mathrm{tr}(SG) = 0$ for all $S \in \tilde{\Sigma}$. Choose two hyperbolic elements $S_1, S_2 \in \tilde{\Sigma}$ without common fixed points; without loss of generality we may assume that

$$S_1 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \quad S_2 = \begin{pmatrix} w & x \\ y & z \end{pmatrix}, \quad G = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for some $\lambda > 1$ and $xy \neq 0$. Then

$$\lambda a + \lambda^{-1} d = \mathrm{tr}(S_1 G) = 0 = \mathrm{tr}(G) = a + d,$$

hence $a = d = 0$ and

$$G = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, \quad bc = -\det(G) = -1, \text{ so } b, c \neq 0.$$

But then

$$cx + by = \mathrm{tr}(S_2 G) = 0 = \mathrm{tr}(S_1 S_2 G) = \lambda cx + \lambda^{-1} by,$$

hence $cx = by = 0$; but we know that $b, c, x, y \neq 0$, contradiction.

So there exists some $S \in \tilde{\Sigma}$ with $\operatorname{tr}(SG) \neq 0$; without loss of generality we assume that already $\operatorname{tr} G \neq 0$. Take some arbitrary hyperbolic $T \in \tilde{\Sigma}$; by the elementary equation

$$\operatorname{tr}(AB) + \operatorname{tr}(AB^{-1}) = \operatorname{tr}(A) \cdot \operatorname{tr}(B) \text{ for all } A, B \in \mathrm{SL}(2, \mathbb{C}) \tag{4.5}$$

then

$$|\operatorname{tr}(T^N G)| + |\operatorname{tr}(T^{-N} G)| \geq |\operatorname{tr}(T^N G) + \operatorname{tr}(T^{-N} G)| = |\operatorname{tr}(T^N) \operatorname{tr}(G)|.$$

But the right hand side goes to ∞ as $N \to \infty$, so for sufficiently large N, at least one of $|\operatorname{tr}(T^N G)|$ and $|\operatorname{tr}(T^{-N} G)|$ must be larger than 2. □

Lemma 4.24. *Let $\Gamma \subset \mathrm{PSL}(2, \mathbb{R})$ be a lattice. Then there exists a finite generating system of Γ only consisting of hyperbolic elements.*

Proof. Assume that Γ is generated by $g_1, \ldots, g_n$. By [41, Exercise 2.13], Γ contains two hyperbolic elements h_1, h_2 without common fixed points; let them generate the group S. For each $1 \leq j \leq n$ choose some $s_j \in S$ with $s_j g_j$ hyperbolic. Then Γ is generated by the hyperbolic elements $h_1, h_2, s_1 g_1, \ldots, s_n g_n$. □

Lemma 4.25. *Let $a \in \mathrm{SL}(2, \mathbb{C})$ and let $\Gamma \subset \mathrm{SL}(2, \mathbb{R})$ be a lattice with $a \Gamma a^{-1} \subset \mathrm{SL}(2, \mathbb{R})$. Then $a \in \mathbb{C}^\times \cdot \mathrm{GL}(2, \mathbb{R})$.*

Proof. Since Γ is Zariski-dense in $\mathrm{SL}(2, \mathbb{R})$ we may deduce that $a\mathrm{SL}(2, \mathbb{R})a^{-1} \subseteq \mathrm{SL}(2, \mathbb{R})$. The sub-$\mathbb{R}$-vector space of $\mathrm{M}(2, \mathbb{C})$ generated by $\mathrm{SL}(2, \mathbb{R})$ is $\mathrm{M}(2, \mathbb{R})$, so $a\mathrm{M}(2, \mathbb{R})a^{-1} = \mathrm{M}(2, \mathbb{R})$. By the Skolem–Noether Theorem, the automorphism $g \mapsto aga^{-1}$ of $\mathrm{M}(2, \mathbb{R})$ has to be an inner automorphism, i.e. there exists $b \in \mathrm{GL}(2, \mathbb{R})$ with $aga^{-1} = bgb^{-1}$ for all $g \in \mathrm{M}(2, \mathbb{R})$ and hence, by linear extension, also for all $g \in \mathrm{M}(2, \mathbb{C})$. But this means that ba^{-1} is in the centre of $\mathrm{M}(2, \mathbb{C})$ which is $\mathbb{C}^\times$. □

Proof of Theorem 4.21. Without loss of generality we may assume that Δ is torsion-free by Selberg's Lemma [80, Lemma 8], hence it has a presentation

$$\Delta = \langle g_1, \ldots, g_m \mid [g_1, g_{n+1}][g_2, g_{n+2}] \cdots [g_n, g_{2n}] = 1 \rangle \text{ with } m = 2n$$

(in the cocompact case), or is free on some generators $g_1, \ldots, g_m$ (otherwise). By [81, Theorem 4.1] each $\varrho_j|_\Delta$ can be lifted to representations $\tilde{\varrho}_j \colon \Delta \to \mathrm{SL}(2, \mathbb{R})$; furthermore again by that theorem we can arbitrarily prescribe the sign of each lift of $\varrho_j(g_i)$, so we may assume that

$$\operatorname{tr} \tilde{\varrho}_1(g_i) = \operatorname{tr} \tilde{\varrho}_2(g_i) \text{ for all } 1 \leq i \leq m. \tag{4.6}$$

More generally,

$$\operatorname{tr} \tilde{\varrho}_1(\gamma) = \varepsilon(\gamma) \cdot \operatorname{tr} \tilde{\varrho}_2(\gamma) \text{ for all } \gamma \in \Delta,$$

where ε is some function $\Delta \to \{\pm 1\}$. Note that ε is uniquely determined by this equation because the traces cannot be zero since elements of $\varrho_j(\Delta)$ are not elliptic. Furthermore $\varepsilon(g_i) = 1$ for every generator g_i by (4.6).

We now show that ε is identically 1. The crucial step is the following implication:

$$\text{If } \varepsilon(\gamma) = \varepsilon(\delta) = 1, \text{ then } \varepsilon(\gamma\delta) = \varepsilon(\gamma\delta^{-1}) = 1. \tag{4.7}$$

So assume that $\varepsilon(\gamma) = \varepsilon(\delta) = 1$. We deduce from (4.5):

$$\begin{aligned} \varepsilon(\gamma\delta)\operatorname{tr}\tilde{\varrho}_1(\gamma\delta) + \varepsilon(\gamma\delta^{-1})\operatorname{tr}\tilde{\varrho}_1(\gamma\delta^{-1}) &= \operatorname{tr}\tilde{\varrho}_2(\gamma\delta) + \operatorname{tr}\tilde{\varrho}_2(\gamma\delta^{-1}) \\ = (\operatorname{tr}\tilde{\varrho}_2(\gamma))\cdot(\operatorname{tr}\tilde{\varrho}_2(\delta)) = (\operatorname{tr}\tilde{\varrho}_1(\gamma))\cdot(\operatorname{tr}\tilde{\varrho}_1(\delta)) &= \operatorname{tr}\tilde{\varrho}_1(\gamma\delta) + \operatorname{tr}\tilde{\varrho}_1(\gamma\delta^{-1}). \end{aligned} \tag{4.8}$$

If $\varepsilon(\gamma\delta)$ and $\varepsilon(\gamma\delta^{-1})$ were both negative, (4.8) would entail that $(\operatorname{tr}\tilde{\varrho}_2(\gamma))\cdot(\operatorname{tr}\tilde{\varrho}_2(\delta)) = 0$ which is absurd because Δ does not contain elliptic elements. If $\varepsilon(\gamma\delta) = 1$ and $\varepsilon(\gamma\delta^{-1}) = -1$, then $\operatorname{tr}\tilde{\varrho}_2(\gamma\delta^{-1}) = 0$ which is again absurd; the other mixed case is ruled out in an analogous way. This proves (4.7).

Now we can prove that $\varepsilon(\gamma) = 1$ for every $\gamma \in \Delta$ using induction on the word length $\ell(\gamma)$: this is the number of factors $g_j^{\pm 1}$ needed to obtain γ as a product. If $\ell(\gamma) = 1$ then $\gamma = g_j^{\pm 1}$; since $\varepsilon(\gamma) = \varepsilon(\gamma^{-1})$, this must be equal to $\varepsilon(g_j) = 1$. If $\varepsilon(\gamma) = 1$ for all γ with $\ell(\gamma) \leq n$ we may use (4.7) and the trivial identity $\varepsilon(\gamma^{-1}) = \varepsilon(\gamma)$ to show the statement for all γ with $\ell(\gamma) \leq n+1$. Therefore by induction, ε is identically 1, hence

$$\operatorname{tr}\tilde{\varrho}_1(\gamma) = \operatorname{tr}\tilde{\varrho}_2(\gamma) \text{ for all } \gamma \in \Delta.$$

By Theorem 4.22 this means that $\tilde{\varrho}_1$ is conjugate to $\tilde{\varrho}_2$ within $\mathrm{SL}(2,\mathbb{C})$, but since all images are real, the conjugation must be possible within $\mathrm{GL}(2,\mathbb{R})$ by Lemma 4.25. This in turn means that $\varrho_1|_\Delta$ and $\varrho_2|_\Delta$ are conjugate in $\mathrm{PGL}(2,\mathbb{R})$.

We need to extend this to the entire group Γ. Without loss of generality we may assume that $\varrho_1|_\Delta = \varrho_2|_\Delta$. By Lemma 4.24 there exists a generating system $\gamma_1, \ldots, \gamma_m$ of Γ, not necessarily related in any way to that of Δ, such that all $\varrho_1(\gamma_j)$ are hyperbolic. But some power of each γ_j is contained in Δ, and hence $\varrho_1(\gamma_j)^N = \varrho_2(\gamma_j)^N$. Under the assumptions on γ_j this entails $\varrho_1(\gamma_j) = \varrho_2(\gamma_j)$, i.e. $\varrho_1 = \varrho_2$. □

4.7 Modular embeddings

Let once again $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a semi-arithmetic lattice satisfying the trace field property, with trace field k, quaternion algebra B, maximal order $\mathcal{O}$ and algebraic group $G = \operatorname{Res}_{k|\mathbb{Q}} H$. As explained above, Γ is a subgroup of the arithmetic group $\mathrm{P}\mathcal{O}^1$. Now that latter group naturally lives on the symmetric space of G, i.e. on $G(\mathbb{R})/K$ for a maximal compact subgroup K. This space can be described explicitly as $\mathfrak{H}^r$ where $\mathfrak{H}$ is the upper half-plane and $r \leq d = [k : \mathbb{Q}]$. Let $\sigma_1, \ldots, \sigma_d \colon k \to \mathbb{R}$ be the field embeddings, where σ_1 is the identity embedding. We also may assume that the quaternion algebra $B \otimes_{k,\sigma_i} \mathbb{R}$ is isomorphic to $\mathrm{M}(2,\mathbb{R})$ for each $1 \leq i \leq r$ and isomorphic to $\mathbb{H}$ for $r < i \leq d$.

For each $1 \leq i \leq r$ we choose an isomorphism $\alpha_i \colon B \otimes_{k,\sigma_i} \mathbb{R} \to \mathrm{M}(2,\mathbb{R})$. We obtain an embedding

$$\alpha \colon \mathcal{O}^1 \hookrightarrow \mathrm{SL}(2,\mathbb{R})^r, \quad x \mapsto (\alpha_1(x), \ldots, \alpha_r(x))$$

descending to an embedding $\alpha\colon \mathrm{P}\mathcal{O}^1 \hookrightarrow \mathrm{PSL}(2,\mathbb{R})^r$. We denote the image by $\Lambda = \alpha(\mathrm{P}\mathcal{O}^1)$.

Theorem 4.26. *Λ is an irreducible arithmetic lattice in $\mathrm{PSL}(2,\mathbb{R})^r$.*

For the proof see e.g. [87].

Note that $\alpha(\Gamma)$ becomes a subgroup of Λ. It has finite index precisely if Γ is already arithmetic; in every case $\alpha(\Gamma)$ is a Zariski-dense subgroup of Λ by the proof of Proposition 4.9. Zariski-dense subgroups of infinite index in arithmetic groups are called *thin*, and so we have shown:

Corollary 4.27. *If Γ is not arithmetic itself, the embedding $\alpha\colon \Gamma \to \Lambda$ realises Γ as a thin group.*

Let $\mathrm{PSL}(2,\mathbb{R})^r$ operate by component-wise Möbius transformations on $\mathfrak{H}^r$; the induced action of Λ on $\mathfrak{H}^r$ is properly discontinuous and has a quotient of finite volume. This motivates the following definition:

Definition 4.28. *A* modular embedding *of Γ is a holomorphic embedding $F\colon \mathfrak{H} \to \mathfrak{H}^r$ such that*

$$F(\gamma\tau) = \alpha(\gamma)F(\tau)$$

for every $\gamma \in \Gamma$ and every $\tau \in \mathfrak{H}$.

The following result which will be used later on is [76, Corollary 5]:

Proposition 4.29. *Let $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a semi-arithmetic group which satisfies the trace field property and admits a modular embedding, and let $k = \mathbb{Q}(\operatorname{tr}\Gamma)$. Let $\gamma \in \tilde{\Gamma}$ be hyperbolic and let $\sigma\colon k \to \mathbb{R}$ be an embedding which is not the identity inclusion. Then $|\sigma(\operatorname{tr}\gamma)| < |\operatorname{tr}\gamma|$.*

Note that if Γ is an arithmetic group then even $|\sigma(\operatorname{tr}\gamma)| < 2$ by Proposition 4.8.

4.8 Congruence rigidity

Let $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$ be a semi-arithmetic lattice satisfying the trace field condition, with trace field $k = \mathbb{Q}(\operatorname{tr}\Gamma)$. Let $B = k[\tilde{\Gamma}]$ be the associated quaternion algebra and G the algebraic group over $\mathbb{Q}$ with $G(\mathbb{Q}) = B^1$. Let $\mathcal{O} \subset B$ be a maximal order containing $\tilde{\Gamma}$, and let $\mathfrak{m} \subset \mathfrak{o}_k$ be such that a finite index subgroup of Γ is adèlically dense in $\mathrm{P}\mathcal{O}^1(\mathfrak{m})$; in particular, $\mathfrak{m}$ satisfies the conclusion of Proposition 4.10.

For the statement of the next proposition, let $\mathfrak{m} = \mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$ be the prime factorisation of $\mathfrak{m}$. Let ℓ_j be the norm of the prime ideal $\mathfrak{l}_j$. Then $S(\mathfrak{m})$ is the finite set of all rational primes diving some $|\mathrm{PSL}(2,\ell_j)|$ (this includes the primes dividing ℓ_j or $\ell_j + 1$). Note that if $\mathfrak{m}'$ is an ideal which has the same prime divisors as $\mathfrak{m}$ and if ℓ is a rational prime dividing the order of $\mathrm{P}\mathcal{O}^1/\mathrm{P}\mathcal{O}^1(\mathfrak{m}')$, then $\ell \in S(\mathfrak{m})$. Also $S(6)$ is the set consisting of $2, 3$ and all prime divisors of orders of $\mathrm{PSL}(2,q)$ where q is the norm of a prime ideal $\mathfrak{p}$ in k with $\mathfrak{p} \mid 6$. Finally $S(\Gamma)$ is the union of $S(\mathfrak{m}) \cup S(6)$, the primes lying over the ramification divisor of B and the primes that ramify in k. Still, $S(\Gamma)$ is a finite set of rational primes.

Proposition 4.30. *Let Γ as above, and let $q = p^f$ be an odd prime power which is prime to all primes in $S(\Gamma)$. Let $\Delta \subset \Gamma$ be a normal congruence subgroup such that $\Gamma/\Delta \simeq \mathrm{PSL}(2,q)$. Then there exists a unique prime $\mathfrak{p}$ of norm q in k such that $\Delta = \Gamma(\mathfrak{p})$.*

Proof. There exists an ideal $\mathfrak{n}$ such that $\Delta \supseteq \Gamma(\mathfrak{n})$ and a finite index subgroup of Δ is adèlically dense in $\mathrm{P}\mathscr{O}^1(\mathfrak{n})$. We may assume that $\mathfrak{m}$ divides $\mathfrak{n}$. Write $\mathfrak{n} = \mathfrak{n}' \cdot \mathfrak{n}_{\mathfrak{m}}$ with $\mathfrak{n}'$ coprime to $\mathfrak{m}$ and $\mathfrak{n}_{\mathfrak{m}}$ having the same prime divisors as $\mathfrak{m}$; then Γ also contains a subgroup which is adèlically dense in $\mathrm{P}\mathscr{O}^1(\mathfrak{n}_{\mathfrak{m}})$. By Proposition 4.10 this entails that Γ surjects onto $\mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}')$.

Denote the quotient map modulo Δ by

$$\pi\colon \Gamma \to \mathrm{PSL}(2,q).$$

Note that π is continuous in the adèlic topology on Γ since it vanishes on $\Gamma(\mathfrak{n})$.

Now $\Gamma(\mathfrak{n}') = \Gamma \cap \mathrm{P}\mathscr{O}^1(\mathfrak{n}')$ is a normal subgroup of Γ, hence its image under π is a normal subgroup of $\mathrm{PSL}(2,q)$. Since that group is simple, the image can only be $\mathrm{PSL}(2,q)$ or the trivial group. Assume it were the entire group, then in the sequence

$$\mathrm{PSL}(2,q) \twoheadleftarrow \Gamma(\mathfrak{n}')/\Gamma(\mathfrak{n}) \hookrightarrow \mathrm{P}\mathscr{O}^1(\mathfrak{n}')/\mathrm{P}\mathscr{O}^1(\mathfrak{n}) \simeq \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}_{\mathfrak{m}})$$

(where the isomorphism is by Corollary 4.15) the order of the left hand side would divide the order of the right hand side. But the former is divisible by p, the latter only by primes in $S(\Gamma)$. A contradiction, hence the image of $\Gamma(\mathfrak{n}')$ under π is the trivial group. In other words,

$$\Delta \supseteq \Gamma(\mathfrak{n}').$$

This implies that π descends to an epimorphism

$$\pi\colon \Gamma/\Gamma(\mathfrak{n}') \twoheadrightarrow \mathrm{PSL}(2,q).$$

By Proposition 4.10 the inclusion $\Gamma \subseteq \mathrm{P}\mathscr{O}^1$ induces an isomorphism

$$\alpha\colon \Gamma/\Gamma(\mathfrak{n}') \xrightarrow{\simeq} \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}').$$

So by composition we obtain an epimorphism $\pi \circ \alpha^{-1}\colon \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}') \twoheadrightarrow \mathrm{PSL}(2,q)$. Let $\mathfrak{n}' = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$ with distinct prime ideals $\mathfrak{p}_j$, and let $\mathrm{rad}(\mathfrak{n}') = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Then $\mathrm{P}\mathscr{O}^1(\mathrm{rad}(\mathfrak{n}'))/\mathrm{P}\mathscr{O}^1(\mathfrak{n}')$ is a solvable normal subgroup of $\mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}')$ by Lemma 4.17, so its image by $\pi \circ \alpha^{-1}$ has to be a solvable normal subgroup of $\mathrm{PSL}(2,q)$, i.e. trivial. Therefore $\pi \circ \alpha^{-1}$ factors through $\mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathrm{rad}(\mathfrak{n}'))$; we summarise this in a diagram:

$$\begin{tikzcd}
\Gamma/\Gamma(\mathfrak{n}') \arrow[r, "\simeq", "\alpha"'] \arrow[dr, two heads, "\pi"'] & \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{n}') \arrow[r, two heads] \arrow[d, two heads] & \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathrm{rad}(\mathfrak{n}')) \arrow[dl, two heads, dashed] \\
& \mathrm{PSL}(2,q) &
\end{tikzcd} \tag{4.9}$$

Now the rightmost projects onto

$$\mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{p}_1) \times \cdots \times \mathrm{P}\mathscr{O}^1/\mathrm{P}\mathscr{O}^1(\mathfrak{p}_n), \tag{4.10}$$

and by Corollary 4.13 the kernel of this projection is an abelian normal subgroup which is therefore mapped to the identity element by the dashed arrow in (4.9). Hence that dashed arrow is defined on (4.10); by Lemma 4.5 it actually has to factor through the projection onto one of them, composed with an isomorphism. We hence obtain

$$\begin{tikzcd}
\Gamma/\Gamma(\mathfrak{n}') \arrow[r, "\simeq", "\alpha"'] \arrow[dr, two heads, "\pi"'] & \mathrm{P}\mathcal{O}^1/\mathrm{P}\mathcal{O}^1(\mathfrak{n}') \arrow[r, two heads] \arrow[d, two heads] & \mathrm{P}\mathcal{O}^1/\mathrm{P}\mathcal{O}^1(\mathfrak{p}_j) \arrow[dl, dashed, "\simeq"] \\
 & \mathrm{PSL}(2,q) &
\end{tikzcd}$$

for some $1 \leq j \leq n$. We may shorten this to

$$\begin{tikzcd}
\Gamma/\Gamma(\mathfrak{p}_j) \arrow[rr, "\simeq", "\alpha'"'] \arrow[dr, two heads, "\pi'"'] & & \mathrm{P}\mathcal{O}^1/\mathrm{P}\mathcal{O}^1(\mathfrak{p}_j) \arrow[dl, dashed, "\simeq"] \\
 & \mathrm{PSL}(2,q) &
\end{tikzcd} \tag{4.11}$$

with α' again induced by the inclusion $\Gamma \subseteq \mathrm{P}\mathcal{O}^1$. In this diagram π' is obviously an isomorphism, therefore $\Delta = \ker \pi$ is equal to $\Gamma(\mathfrak{p}_j)$. The dashed isomorphism in (4.11) shows that the norm of $\mathfrak{p}_j$ is q. □

Remark 4.31. We note that this proposition enables us to reconstruct the splitting behaviour of almost all primes in k from Γ and its congruence subgroups: Let $p \notin S(\Gamma)$ be a rational prime in Γ. Then there exist only finitely many normal congruence subgroups $\Delta \triangleleft \Gamma$ such that $\Gamma/\Delta \simeq \mathrm{PSL}(2,q)$ for some power q of f. Let these be $\Delta_1, \ldots, \Delta_n$, and let the corresponding quotients be $\mathrm{PSL}(2, p^{f_1}), \ldots, \mathrm{PSL}(2, p^{f_n})$.

On the other hand consider the prime decomposition $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ in k. Then $n = m$, and up to renumeration $\Delta_j = \Gamma(\mathfrak{p}_j)$ and $N(\mathfrak{p}_j) = p^{f_j}$. In particular we can reconstruct $[k\colon \mathbb{Q}] = f_1 + \ldots + f_n$ from the knowledge of Γ and its congruence subgroups.

Proof of Theorem A. By Theorem 4.21 we may replace Γ_j by finite index subgroups corresponding to each other under the isomorphism f. Hence we may assume that each Γ_j is torsion-free and satisfies the trace field condition. Again by Theorem 4.21 it suffices to show that $\mathrm{tr}^2 f(\gamma) = \mathrm{tr}^2 \gamma \in \mathbb{R}$ for each $\gamma \in \Gamma_1$.

Denote the trace field of Γ_j by k_j. Each number $a \in \mathfrak{o}_{k_j}$ has a *characteristic polynomial* $\chi_a(x) \in \mathbb{Z}[x]$ which can be described as follows:

- it is the characteristic polynomial of the map $k_j \to k_j$, $v \mapsto av$ interpreted as a $\mathbb{Q}$-linear map;
- it is equal to $\prod_\sigma (x - \sigma(a))$. Here σ runs through a system of representatives of $\mathrm{Gal}(L_j|\mathbb{Q})$ modulo $\mathrm{Gal}(L_j|k_j)$ where L_j is the Galois closure of k_j.

Now let p be a rational prime not in $S(\Gamma_1) \cup S(\Gamma_2)$. By Remark 4.31 we can decompose $p\mathfrak{o}_{k_j}$ into prime ideals

$$p\mathfrak{o}_{k_1} = \mathfrak{p}_1 \cdots \mathfrak{p}_n, \quad p\mathfrak{o}_{k_2} = \mathfrak{q}_1 \ldots \mathfrak{q}_n$$

in such a way that

$$f(\Gamma_1(\mathfrak{p}_j)) = \Gamma_2(\mathfrak{q}_j) \text{ and } \mathfrak{o}_{k_1}/\mathfrak{p}_j \simeq \mathfrak{o}_{k_2}/\mathfrak{q}_j. \tag{4.12}$$

Then

$$\mathfrak{o}_{k_1}/p\mathfrak{o}_{k_1} \simeq \mathfrak{o}_{k_1}/\mathfrak{p}_1 \times \cdots \times \mathfrak{o}_{k_1}/\mathfrak{p}_d \tag{4.13}$$

is a finite-dimensional $\mathbb{F}_p$-algebra, and we may similarly define the characteristic polynomial $\chi_{\bar{b}}(x) \in \mathbb{F}_p[x]$ of an element $\bar{b} \in \mathfrak{o}_{k_1}/p\mathfrak{o}_{k_1}$ as the characteristic polynomial of the $\mathbb{F}_p$-linear endomorphism of $\mathfrak{o}_{k_1}/p\mathfrak{o}_{k_1}$ given by multiplication by $\bar{b}$. Then for $a \in \mathfrak{o}_{k_1}$ clearly

$$\chi_a(x) \bmod p = \chi_{a \bmod p}(x) \in \mathbb{F}_p[x]. \tag{4.14}$$

We now claim that the characteristic polynomials of $\operatorname{tr}^2\gamma$ and $\operatorname{tr}^2 f(\gamma)$ are congruent modulo p. To see this we use the abstract version of squared traces on finite groups introduced in section 4.3. For each $1 \leq j \leq n$, using (4.12) we obtain an isomorphism of finite groups $\bar{f}\colon \Gamma_1/\Gamma_1(\mathfrak{p}_j) \to \Gamma_2/\Gamma_2(\mathfrak{q}_j)$. By the remark after Definition 4.4, $\operatorname{tr}^2\gamma \bmod \mathfrak{p}_j$ and $\operatorname{tr}^2 f(\gamma) \bmod \mathfrak{q}_j$ are Galois-conjugate elements of the finite field $\mathbb{F}_q \simeq \mathfrak{o}_{k_1}/\mathfrak{p}_j \simeq \mathfrak{o}_{k_2}/\mathfrak{q}_j$. Hence there exists an isomorphism of $\mathbb{F}_p$-algebras

$$\alpha_j\colon \mathfrak{o}_{k_1}/\mathfrak{p}_j \xrightarrow{\simeq} \mathfrak{o}_{k_2}/\mathfrak{q}_j$$

with $\alpha_j(\operatorname{tr}^2\gamma \bmod \mathfrak{p}_j) = \operatorname{tr}^2 f(\gamma) \bmod \mathfrak{q}_j$. Gluing these together component-wise in (4.13) yields an isomorphism of $\mathbb{F}_p$-algebras $\alpha\colon \mathfrak{o}_{k_1}/p\mathfrak{o}_{k_1} \to \mathfrak{o}_{k_2}/p\mathfrak{o}_{k_2}$ with $\alpha(\operatorname{tr}^2\gamma \bmod p) = \operatorname{tr}^2 f(\gamma) \bmod p$. Since characteristic polynomials are stable under algebra isomorphisms, we obtain

$$\chi_{\operatorname{tr}^2\gamma \bmod p}(x) = \chi_{\operatorname{tr}^2 f(\gamma) \bmod p}(x) \in \mathbb{F}_p[x].$$

By (4.14), this means

$$\chi_{\operatorname{tr}^2\gamma}(x) \equiv \chi_{\operatorname{tr}^2 f(\gamma)}(x) \bmod p.$$

But this holds for infinitely many p, so

$$\chi_{\operatorname{tr}^2\gamma}(x) = \chi_{\operatorname{tr}^2 f(\gamma)}(x) \in \mathbb{Z}[x].$$

Since we had assumed Γ_1 to be torsion-free, γ cannot be elliptic. If it is parabolic, then $\operatorname{tr}^2\gamma = 4$ and therefore $\chi_{\operatorname{tr}^2\gamma}(x) = (x-4)^d$. Hence also the characteristic polynomial of $f(\gamma)$ is $(x-4)^d$, and since $\operatorname{tr}^2 f(\gamma)$ is a zero of this polynomial, $\operatorname{tr}^2 f(\gamma) = 4$, hence $f(\gamma)$ is parabolic as well.

Finally assume that γ is hyperbolic. Then $f(\gamma)$ must also be hyperbolic because it cannot be parabolic (else γ would be parabolic by the inverse of the previous argument). By Proposition 4.29, $\operatorname{tr}^2\gamma$ is the largest zero of $\chi_{\operatorname{tr}^2\gamma}(x)$, similarly for $\operatorname{tr}^2 f(\gamma)$. Therefore $\operatorname{tr}^2(\gamma) = \operatorname{tr}^2 f(\gamma)$. □

4.9 An example

In our proof of Theorem A we did not use the full assumption that all congruence subgroups are mapped to congruence subgroups by the given isomorphism. We spell out in a concrete example how far an isomorphism between non-conjugate arithmetic groups can be from preserving congruence subgroups.

In [92] we find a complete list of all arithmetic groups of signature $(1;2)$, i.e. whose associated Riemann surfaces have genus one and which have one conjugacy class of elliptic elements, these elements being of order two. In particular all these groups are abstractly isomorphic, and we may just pick the first two of them: Γ_1' is generated by the two Möbius transformations

$$\alpha_1 = \pm\begin{pmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{-1+\sqrt{5}}{2} \end{pmatrix} \text{ and } \beta_1 = \pm\begin{pmatrix} \sqrt{3} & \sqrt{2} \\ \sqrt{2} & \sqrt{3} \end{pmatrix},$$

Γ_2' by the two Möbius transformations

$$\alpha_2 = \pm\begin{pmatrix} \sqrt{2}+1 & 0 \\ 0 & \sqrt{2}-1 \end{pmatrix} \text{ and } \beta_2 = \pm\frac{1}{2}\begin{pmatrix} \sqrt{6} & \sqrt{2} \\ \sqrt{2} & \sqrt{6} \end{pmatrix}.$$

These are, respectively, generators satisfying the relation $(\alpha_j\beta_j\alpha_j^{-1}\beta_j^{-1})^2 = 1$. So there exists a group isomorphism $f\colon \Gamma_1' \to \Gamma_2'$ with $f(\alpha_1) = \alpha_2$ and $f(\beta_1) = \beta_2$. The Γ_j' do not satisfy the trace field condition, but the $\Gamma_j = (\Gamma_j')^{(2)}$ (between whom f also induces an isomorphism) do; in both cases the invariant trace field is $\mathbb{Q}$.

Then, with finitely many exceptions, $\Gamma_1/\Gamma_1(p) \simeq \mathrm{PSL}(2,p) \simeq \Gamma_2/\Gamma_2(p)$ for rational primes p; nevertheless, the proof of Theorem A shows that there can be only finitely many p such that $f(\Gamma_1(p))$ is a congruence subgroup (and hence only finitely many p with $f(\Gamma_1(p)) = \Gamma_2(p)$).

4.10 Concluding remarks

Remark 4.32. The assumption that both groups admit a modular embedding is crucial although it only enters in the very last step of the proof. If Γ is a semi-arithmetic lattice with invariant trace field k and $\sigma\colon k \to \mathbb{R}$ a field embedding we obtain in a natural way a group $i_\sigma(\Gamma) \subset \mathrm{PSL}(2,\mathbb{R})$, see [76, Remark 4]. There exist semi-arithmetic lattices Γ with nontrivial Galois conjugates $i_\sigma(\Gamma)$ that are again lattices, and then the isomorphism $\Gamma \to i_\sigma(\Gamma)$ preserves congruence subgroups but not traces. For an explicit construction see e.g. [3] referring to [10, Proposition 4.11]. But if Γ admits a modular embedding, then none of the nontrivial Galois conjugates $i_\sigma(\Gamma)$ can be discrete by [76, Theorem 3].

Note that the existence of a modular embedding enters the proof via Proposition 4.29 which is its only genuinely non-algebraic ingredient: it is a consequence of the Schwarz Lemma.

One may still ask whether a weakened version of our main theorem holds in the general case: if $f\colon \Gamma_1 \to \Gamma_2$ is an isomorphism between semi-arithmetic lattices in $\mathrm{PSL}(2, \mathbb{R})$ respecting congruence subgroups, is it the composition of an inner automorphism of $\mathrm{PGL}(2, \mathbb{R})$ with a Galois conjugation of the trace field?

Remark 4.33. There exist arithmetic Fuchsian groups with different trace fields but whose congruence completions are isomorphic away from a finite set of primes. To see this, start with the polynomial in the remark after [56, Theorem 5.1]: the splitting field of this polynomial is a totally real Galois extension of $\mathbb{Q}$ with Galois group $\mathrm{PSL}(2, 7)$. By the discussion in [69, p. 358–359] such a field contains two subfields k_1, k_2 which are not isomorphic but have the same Dedekind zeta function. Then there exists a finite set S of rational primes such that $\mathbb{A}_{k_1}^S \simeq \mathbb{A}_{k_2}^S$. From this we can easily construct arithmetic Fuchsian groups over k_1 and k_2 with isomorphic prime-to-S congruence completion.

There also exist non-isomorphic number fields with isomorphic finite adèle rings (at all primes), see [47]. But no construction seems to be known where these fields are totally real.

Chapter 5

Prym varieties and triangle groups

5.1 Introduction

In this chapter we generalise some well-known facts about principal congruence subgroups from $\mathrm{SL}(2,\mathbb{Z})$ to certain cocompact Fuchsian triangle groups. Recall that for a rational prime p, the principal congruence subgroup $\Gamma(p)$ is the kernel of the natural homomorphism $\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{F}_p)$. Among its properties are the following:

(a) For the natural action of $\Gamma(p)$ on the upper half plane $\mathbb{H} \subset \mathbb{C}$ by Möbius transformations, the quotient $\Gamma(p)\backslash\mathbb{H}$ can be interpreted as a moduli space for elliptic curves with level p structure.

(b) Such a moduli space can also be constructed in a purely algebraic way, leading to an affine curve $Y(p)$ defined over $\mathbb{Q}$ (the naïve moduli interpretation only makes sense over the cyclotomic field $\mathbb{Q}(\zeta_p)$, but there is a way to carefully reformulate it and then descend to $\mathbb{Q}$, see [26, section 4.1]). Then $Y(p)(\mathbb{C}) \simeq \Gamma(p)\backslash\mathbb{H}$.

(c) The compactification $X(p)(\mathbb{C}) \simeq \Gamma(p)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$ is a smooth projective curve, and the forgetful map $X(p) \to X(1) \simeq \mathbb{P}^1$ can be viewed as a Belyĭ map whose dessin is regular and fixed by all Galois automorphisms.

Now $\mathrm{SL}(2,\mathbb{Z})$ acts on $\mathbb{H}$ via its quotient $\mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\{\pm 1\}$, which is geometrically a triangle group of type $(2,3,\infty)$. We shall prove analogues to (a) – (c) above for triangle groups Δ of type $(2,3,r)$ where $r > 6$ is coprime to 6. The most difficult part is the moduli interpretation of congruence subgroups $\Delta(\mathfrak{p})$ where $\mathfrak{p}$ is now a prime ideal in a certain number field. This interpretation uses the fact that Δ appears as a monodromy group for a certain hypergeometric differential equation, see [44, §42]. The curves to be parameterised are such that the associated hypergeometric functions can be interpreted as periods on families of such curves; we call them *simple hypergeometric curves.*

By a simple hypergeometric curve of degree d we mean a smooth projective curve C with affine equation $w^d = f(z)$, where f is a monic separable polynomial of degree 3. Note that for $d = 2$ we obtain elliptic curves in Weierstraß form. There are projections to all simple hypergeometric curves $w^e = f(z)$ with $e|d$, and splitting away the copies of their Jacobians in $\operatorname{Jac} C$ leaves us with the *Prym variety* $\operatorname{Prym} C$, a $\varphi(d)$-dimensional abelian subvariety of $\operatorname{Jac} C$.

The curve C has an automorphism T of order d given by $T(z, w) = (z, \zeta_d w)$, inducing an automorphism T_* of the Jacobian that stabilises $\operatorname{Prym} C$. The minimal polynomial of T_* on $\operatorname{Prym} C$ is the $(2r)$-th cyclotomic polynomial, leading to an embedding

$$\Phi\colon \mathfrak{o}_K \to \operatorname{End} \operatorname{Prym} C$$

where $K = \mathbb{Q}(\zeta_{2r}) = \mathbb{Q}(\zeta_r)$. Now we let $\mathfrak{p}$ be a prime of $F = \mathbb{Q}(\zeta_{2r} + \zeta_{2r}^{-1})$, the maximal real subfield of K, and set

$$(\operatorname{Prym} C)[\mathfrak{p}] = \{x \in \operatorname{Prym} C \mid \Phi(\alpha)x = 0 \text{ for all } \alpha \in \mathfrak{p}\mathfrak{o}_K\}.$$

This is a finite group and a free module of rank two under $\mathbb{K}_\mathfrak{p} = \mathfrak{o}_K/\mathfrak{p}\mathfrak{o}_K$. There is a perfect skew-Hermitian form $\{\cdot,\cdot\}_\mathfrak{p}$ on this module, and we can always find a basis (x_1, x_2) which is orthonormal in the sense that $\{x_1, x_2\}_\mathfrak{p} = 0$ and $\{x_1, x_1\}_\mathfrak{p} = \{x_2, x_2\}_\mathfrak{p}$, where the latter is an invertible element of $\mathbb{K}_\mathfrak{p}$ (which can, however, never be 1). Two orthonormal bases (x_1, x_2) and (y_1, y_2) are declared equivalent if there exists $\alpha \in \mathbb{K}_\mathfrak{p}^\times$ with $\alpha x_1 = y_1$ and $\alpha x_2 = y_2$. An equivalence class of orthonomal bases is called a *Prym level* $\mathfrak{p}$ *structure* on C.

We also define a normal subgroup $\Delta(\mathfrak{p})$ of Δ with $\Delta/\Delta(\mathfrak{p}) \simeq \mathrm{PSL}(2, \mathbb{F}_\mathfrak{p})$ by the usual procedure involving quaternion algebras in section 5.2. Our central result about moduli interpretations is then (for a more precise formulation see Theorem 5.46 and Proposition 5.47 below):

Theorem A. *Let Δ be a hyperbolic triangle group of type $(2,3,r)$ with $r \equiv \pm 1 \bmod 6$, acting on the unit disk $\mathbb{D} \subset \mathbb{C}$. Let $\mathfrak{p}$ be a prime of $F = \mathbb{Q}(\zeta_r + \zeta_r^{-1})$ coprime to r.*

There exists a coarse moduli space for simple hypergeometric curves of degree $2r$ with Prym level $\mathfrak{p}$ structure over $\mathbb{C}$; it has two connected components, each of which is birational to $\Delta(\varepsilon(\mathfrak{p}))\backslash\mathbb{D}$.

Here ε is the unique automorphism of F with $\varepsilon(\zeta_r + \zeta_r^{-1}) = \zeta_r^2 + \zeta_r^{-2}$.

Rather than constructing a model of this moduli space as a scheme over a sufficiently small number field, we construct it analytically over $\mathbb{C}$ and then use some general facts about Galois descent for algebraic curves to deduce rather easily:

Theorem B. *Let r, Δ, F and $\mathfrak{p}$ as in Theorem A, and let $X(\mathfrak{p}) = \Delta(\mathfrak{p})\backslash\mathbb{D}$ as an algebraic curve over $\mathbb{C}$. For a field automorphism σ of $\mathbb{C}$ we get $\sigma(X(\mathfrak{p})) \simeq X(\sigma(\mathfrak{p}))$, where σ acts on the primes via its restriction to F. The minimal field of definition of $X(\mathfrak{p})$, as well as its moduli field, is equal to the decomposition field in F of the rational prime p above $\mathfrak{p}$.*

This also has consequences for the dessins d'enfants defined by $\Delta(\mathfrak{p})$, see Proposition 5.52, and it gives a new proof for a known result on Hurwitz curves. These are algebraic curves of genus $g > 1$ with $84(g-1)$ automorphisms (the maximal possible number); for $r = 7$ and $\mathfrak{p}$ any prime in $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ the curve $X(\mathfrak{p})$ is a Hurwitz curve with automorphism group $\mathrm{PSL}(2, \mathbb{F}_\mathfrak{q})$, with Theorem B explaining the Galois action on these curves, see section 5.5.4 below.

Finally we remark that for the triangle groups Δ of type $(2,3,7)$ and $(2,3,11)$ there is yet another moduli interpretation: these groups are arithmetic groups. Hence for any congruence subgroup Γ of Δ, the quotient $\Gamma\backslash\mathbb{D}$ classifies certain six- or ten-dimensional (depending on whether $r = 7$ or 11) abelian varieties with polarisation, an action of $\mathbb{Z}[\zeta_r]$ by endomorphisms and some level structures; in other words, $\Gamma\backslash\mathbb{D}$ is then a PEL Shimura variety. The link with our apporach is that $\Delta(\mathfrak{p})\backslash\mathbb{H}$ is the Shimura variety parameterising abelian varieties with PEL structure of the type given by the Prym varieties of simple hypergeometric curves and their Prym level structures. In general Δ still admits a modular embedding (see [14, 76]) leading to a closed embedding of $X(\mathfrak{p})$ into a compactified Shimura variety, see Proposition 5.53.

General references. Three works are particularly important to our approach:

(i) In [14] a modular embedding for the full triangle group Δ (see Proposition 5.53 below) is constructed in three different ways: by Schwarz triangle mappings, by hypergeometric differential equations and by considering a certain family of hypergeometric curves and abelian subvarieties of their Jacobians. Up to a slight variation in the choice of the curves, a combination of the first and third methods in [14] is an essential part of our proof of Theorem A.

(ii) The choice of curves is as in [59], that is, the family of simple hypergeometric curves over the configuration space $\mathrm{Conf}_3(\mathbb{C})$. We use the explicit models in [59] for the monodromy action of the braid group on a certain two-dimensional subspace of cohomology, which translates to the monodromy of a certain hypergeometric differential equation in more classical language.

(iii) Finally we use some explicit structure results about congruence subgroups of triangle curves from [12]. To our knowledge that is the first work to systematically study such congruence subgroups.

Apart from these we note that the relation between hypergeometric functions (or related objects) and discrete transformation groups with special geometric properties has been studied for a long time; the interested reader is referred to the textbooks [44, 102], the survey article [64] and the research articles [79, 70, 23, 59, 97]. Hypergeometric curves and their Prym varieties are studied carefully in [5]; other works related to ours where they appear are [101, 86, 85].

Outline. In section 2 we introduce the triangle groups of type $(2,3,r)$ and their associated quaternion orders; we determine these orders and define congruence subgroups. In section 3 we study the family of simple hypergeometric curves over the configuration space, introduce a multi-valued period map on this space and relate it to a Schwarz triangle map, hence identify its monodromy group with a triangle group. In section 4 the arithmetic aspects of this monodromy group are studied: it is related to the monodromy group of the family of Prym varieties, and we show how to reduce the skew-Hermitian pairing on the Prym lattice modulo a prime. In section 5 we first prove Theorem A by tying together results from the previous sections. After that we deduce Theorem B and related statements, and finally we hint how to link our approach with the theories of Hurwitz curves and Shimura varieties.

Notation. Throughout this chapter r will be a positive integer greater than 6 and coprime to 6 (the latter of which is equivalent to $r \equiv \pm 1 \bmod 6$). For a positive integer n we set $\zeta_n = \exp \frac{2\pi\sqrt{-1}}{n} \in \mathbb{C}$, and μ_n is the group of n-th roots of unity in $\mathbb{C}$.

The ring of integers in a number field L is denoted by $\mathfrak{o}_L$. The number fields K and F are defined by $K = \mathbb{Q}(\zeta_r) = \mathbb{Q}(\zeta_{2r})$ and $F = \mathbb{Q}(\zeta_r + \zeta_r^{-1}) = \mathbb{Q}(\zeta_{2r} + \zeta_{2r}^{-1})$. The automorphism ε of K is defined by

$$\varepsilon(\zeta_r) = \zeta_r^2; \text{ equivalently, } \varepsilon(\zeta_{2r}) = -\zeta_r. \tag{5.1}$$

For a subgroup G of some general linear group $\mathrm{GL}(V)$ of a vector space over an arbitrary field, the image of G in $\mathrm{PGL}(V)$ is denoted by $\mathrm{P}G$, leading to notations like $\mathrm{PU}(V)$ which we will not explain individually.

5.2 Triangle groups

We give a slightly unusual construction of the $(2,3,r)$-triangle group. For generalities on Fuchsian triangle groups see [55, section II.5].

Consider the unit disk $\mathbb{D} = \{z \in \mathbb{C} \mid |z| < 1\}$ with its Poincaré metric as a model of the hyperbolic plane. The orientation-preserving isometry group of $\mathbb{D}$, which is equal to the group of biholomorphisms $\mathbb{D} \to \mathbb{D}$, can be identified with $\mathrm{PSU}(1,1)$ via Möbius transformations. In $\mathbb{D}$ there exists a regular geodesic triangle T with interior angles equal to $\frac{\pi}{r}$; this triangle is unique up to hyperbolic motions. Reflecting it along its sides gives three new triangles of this type, and continuing ad infinitum yields a tesselation $\mathscr{C}$ of $\mathbb{D}$ by regular geodesic triangles. This is shown as the dark grey triangles in Figure 5.1[1] for $r = 7$.

The barycentric subdivision $\mathscr{B}$ of $\mathscr{C}$ is again a tesselation of $\mathbb{D}$ by triangles; this time they have internal angles $\frac{\pi}{2}$, $\frac{\pi}{3}$ and $\frac{\pi}{r}$. In Figure 1 it is represented by the lines of all colours. The following is a consequence of elementary facts in hyperbolic geometry:

Lemma 5.1. *Let $g \in \mathrm{PSU}(1,1) = \mathrm{Aut}\,\mathbb{D}$. The following are equivalent:*

(i) g preserves $\mathscr{C}$, i.e. it sends every vertex, edge and face of $\mathscr{C}$ to a vertex, edge or face, respectively.

(ii) g preserves $\mathscr{B}$.

(iii) g preserves the set $V(\mathscr{C})$ of vertices of $\mathscr{C}$. □

The *triangle group of type* $(2,3,r)$ is then the group Δ consisting of all $g \in \mathrm{PSU}(1,1)$ satisfying the equivalent conditions of Lemma 5.1. It can be generated by three elements A, B, C which are rotations of angles π, $\frac{2\pi}{3}$ and $\frac{2\pi}{r}$, respectively, around the corresponding vertices of one triangle in $\mathscr{B}$; they lead to a presentation

$$\Delta = \langle A, B, C \mid A^2 = B^3 = C^r = ABC = 1 \rangle. \tag{5.2}$$

[1] Source `http://commons.wikimedia.org/wiki/File:Hyperbolic_domains_CMY_237.png`, released into public domain by Wikipedia user Tamfang.

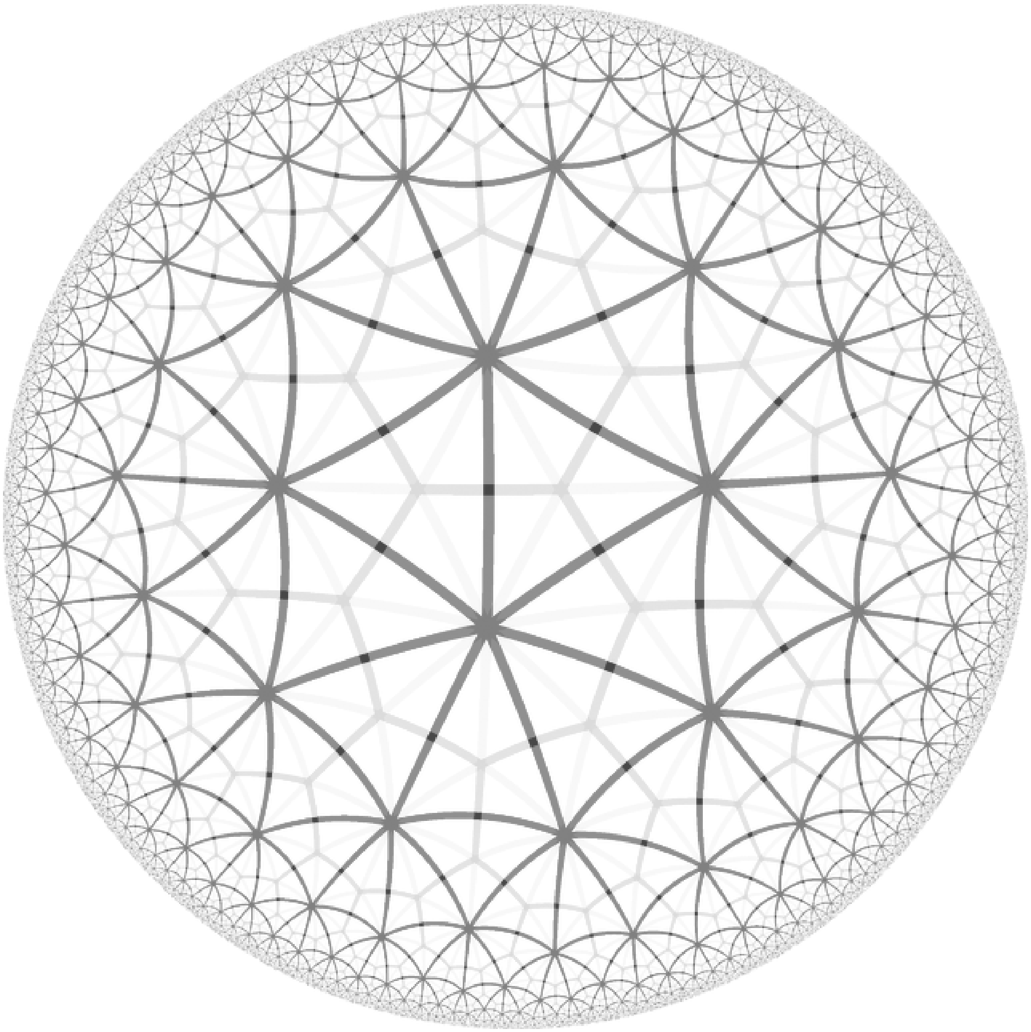

Figure 5.1: A psychedelic pattern in the hyperbolic plane

We note that this characterises Δ uniquely up to conjugation, and this group has two more special properties:

Proposition 5.2. *Let* $6 < r \equiv \pm 1 \bmod 6$*, and let* Δ *be a triangle group of type* $(2, 3, r)$*.*

(i) *Let* $\Gamma \subset \mathrm{PSU}(1, 1)$ *be a subgroup (not necessarily discrete) generated by three elliptic elements* A, B, C *with rotation angles* π, $\frac{2\pi}{3}$ *and* $\frac{2\pi}{r}$*, respectively, satisfying* $ABC = \mathrm{id}$*. Then* Γ *is conjugate to* Δ *in* $\mathrm{PSU}(1, 1)$*.*

(ii) Δ *is a maximal discrete subgroup of* $\mathrm{PSU}(1, 1)$*, i.e. if* $\Gamma \subset \mathrm{PSU}(1, 1)$ *is a discrete subgroup with* $\Delta \subseteq \Gamma$*, then* $\Delta = \Gamma$*.*

(iii) Δ *is perfect, i.e. if* G *is an abelian group and* $f\colon \Delta \to G$ *is a group homomorphism, then* $f = 0$*.*

Proof. (i) is well-known and follows by a lengthy elementary calculation; (ii) is contained in [88, Theorems 1 and 2]. For (iii), note that

$$2f(A) = 3f(B) = rf(C) = f(A) + f(B) + f(C) = 0;$$

multiplying the last equation with $3r$ yields $3rf(A) = 0$; because 2 and $3r$ are coprime, we obtain $f(A) = 0$. Similarly we get $f(B) = f(C) = 0$. □

The preimage $\tilde{\Delta}$ of Δ under the projection $\mathrm{SU}(1, 1) \to \mathrm{PSU}(1, 1)$ is more approachable from an algebraic viewpoint. Lifting the generators to suitable matrices a, b, c, the defining relations (5.2) become

$$a^2 = b^3 = c^r = abc = -\mathbf{1}.$$

All elements of $\tilde{\Delta}$ have traces in $\mathfrak{o}_F = \mathbb{Z}[\zeta_r + \zeta_r^{-1}]$ by [91, Proposition 2], and it makes sense to consider the subring

$$\mathcal{O} = \mathfrak{o}_F[\tilde{\Delta}] \subset \mathrm{M}(2, \mathbb{C}).$$

From standard facts about finitely generated subgroups of $\mathrm{SL}(2, \mathbb{C})$ it follows that $\mathcal{O}$ is an order in a quaternion algebra $A = \mathbb{Q}\mathcal{O} = F[\tilde{\Delta}]$ over F (see e.g. [54, Lemma 8.5.3]).

Proposition 5.3. *The quaternion algebra* A *is unramified at all finite places of* F*. Let* $\sigma\colon F \to \mathbb{R}$ *be an infinite place given by* $\sigma(\zeta_r + \zeta_r^{-1}) = \zeta_r^k + \zeta_r^{-k}$ *with* $0 < k < \frac{r}{2}$ *and* k *coprime to* r*. Then* A *is ramified at* σ *if and only if* $k > \frac{r}{6}$*.*

Furthermore, $\mathcal{O}$ *is a maximal order of* A*.*

Proof. The discriminant of $\mathcal{O}$ is calculated in [12, Lemma 4.4]; in our case, their formula simplifies to

$$d(\mathcal{O}) = \zeta_r + \zeta_r^{-1} - 1 = \zeta_r + \zeta_r^{-1} - \zeta_6 - \zeta_6^{-1} = -\zeta_6^{-1}(1 - \zeta_6\zeta_r)(1 - \zeta_6\zeta_r^{-1}).$$

This is an algebraic unit because $\zeta_6\zeta_r$ and $\zeta_6\zeta_r^{-1}$ are primitive $6r$-th roots of unity, and if n is a positive integer with at least two prime divisors, then $1 - \zeta_n$ is an algebraic unit by [98, Proposition 2.8]. By [54, Theorem 6.6.1], $\mathcal{O}$ has to be a maximal order and A has to be unramified at all finite places of F.

Takeuchi gives a criterion for ramification at the infinite places for general triangle groups in [91, Theorem 1] and its proof. In our case it amounts to this: A is ramified at σ if and only if $\sigma(\zeta_r + \zeta_r^{-1} - 1) < 0$. This is easily seen to be equivalent to the statement to be shown. □

So $\tilde{\Delta}$ is a subgroup of $\mathcal{O}^1$, the group of invertible elements in $\mathcal{O}$ with reduced norm equal to 1. This contains, for every prime $\mathfrak{p}$ of F, the subgroup

$$\mathcal{O}^1(\mathfrak{p}) = \{\gamma \in \mathcal{O}^1 \mid \gamma - 1 \in \mathfrak{p}\mathcal{O}\}$$

which can also be seen as the kernel of the reduction map $\mathcal{O}^1 \to (\mathcal{O}/\mathfrak{p}\mathcal{O})^1$. By Proposition 5.3, $\mathcal{O} \otimes_{\mathfrak{o}_F} \mathfrak{o}_\mathfrak{p} \simeq \mathrm{M}(2, \mathfrak{o}_\mathfrak{p})$, where $\mathfrak{o}_\mathfrak{p}$ is the completion of $\mathfrak{o}_F$ with respect to $\mathfrak{p}$; therefore $(\mathcal{O}/\mathfrak{p}\mathcal{O})^1 \simeq \mathrm{SL}(2, \mathbb{F}_\mathfrak{p})$, where $\mathbb{F}_\mathfrak{p} = \mathfrak{o}_F/\mathfrak{p}$. By strong approximation (see [54, Theorem 7.7.5]) the canonical map $\mathcal{O}^1 \to (\mathcal{O}/\mathfrak{p}\mathcal{O})^1$ is surjective.

We then define the principal congruence subgroup $\tilde{\Delta}(\mathfrak{p}) = \tilde{\Delta} \cap \mathcal{O}^1(\mathfrak{p})$, and we let $\Delta(\mathfrak{p})$ be its image in Δ.

Proposition 5.4. *Assume that $\mathfrak{p}$ does not divide $6r$. Then the composition $\tilde{\Delta} \subseteq \mathcal{O}^1 \to (\mathcal{O}/\mathfrak{p}\mathcal{O})^1$ is surjective. Therefore,*

$$\Delta/\Delta(\mathfrak{p}) \simeq \mathrm{PSL}(2, \mathbb{F}_\mathfrak{p}) \text{ and } \tilde{\Delta}/\tilde{\Delta}(\mathfrak{p}) \simeq \mathrm{SL}(2, \mathbb{F}_\mathfrak{p}).$$

Proof. This is a special case of [12, Theorem B]; note that the construction in the proof of [12, Theorem 9.1], to which the former refers, shows that the subgroup considered in that theorem is equal to our $\Delta(\mathfrak{p})$. □

5.3 Hypergeometric curves and their moduli

5.3.1 Cohomology of hypergeometric curves

We repeat the definition of hypergeometric curves from the introduction, but in a more abstract fashion.

Definition 5.5. *A* hypergeometric curve of degree *d is a smooth projective complex curve C together with a morphism $\pi\colon C \to D$ and a distinguished point $\infty \in D$ such that*

(i) D is a smooth projective curve of genus zero;

(ii) π is a cyclic Galois covering of degree d;

(iii) π is ramified over precisely three points of $D_0 = D \setminus \{\infty\}$, and possibly over ∞.

If $S = \{s_1, s_2, s_3\} \subset C \setminus \{\infty\} \simeq \mathbb{C}$ denotes the set of finite branch points of π, the monodromy of a simple, positively oriented loop around each s_j gives a well-defined element m_j in the Deck group $G \simeq \mathbb{Z}/d\mathbb{Z}$. After choosing a generator T of the Deck group we may identify C as the smooth projective curve birational to the affine curve $w^d = (z - s_1)^{a_1}(z - s_2)^{a_2}(z - s_3)^{a_3}$, where $1 \leq a_j < n$ with $T^{a_j} = m_j$. In this model, $\pi(z, w) = z$ and $T(z, w) = (z, \zeta_d w)$.

We use the term "hypergeometric curve" because the hypergeometric function

$$F(a, b, c; t) = \sum_{n=0}^{\infty} \frac{a(a+1)\cdots(a+n-1)\cdot b(b+1)\cdots(b+n-1)}{c(c+1)\cdots(c+n-1)\cdot n!} t^n$$

has an integral representation

$$F(a, b, c; t) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 z^{b-1}(1-z)^{c-b-1}(1-tz)^{-a} \mathrm{d}z \tag{5.3}$$

discovered by Euler [27, caput X]. If a, b, c are rational numbers this can be written as a relative period on some hypergeometric curve $C \to \mathbb{P}^1$ with finite branch points $0, 1, 1/t$.

Definition 5.6. *A hypergeometric curve $\pi\colon C \to D$ is called* simple *if all finite branch points of π induce the same monodromy element in the deck group.*

Hence a simple hypergeometric curve has an affine model as $w^d = f(z)$ where f is a separable monic polynomial of degree three, with the projection being given by $\pi(z, w) = z$.

Let $\mu_d \subset \mathbb{C}^\times$ be the group of d-th roots of unity. Then there exists a unique group isomorphism

$$\varphi_C\colon \mu_d \to \operatorname{Aut}_D C \tag{5.4}$$

(the deck transformation group of π) such that $\varphi(\xi)$ operates on the tangent space T_bC for each finite branch point b of π as multiplication by ξ. In our model it is given by $\varphi(\xi)(z, w) = (z, \xi w)$.

Proposition 5.7. *Let C be a simple hypergeometric curve with affine equation $w^d = f(z)$ as above, and assume that d is coprime to 3. Then C is a smooth projective curve of genus $d - 1$; a basis of $\Omega^1(C)$ is given by the forms*

$$\omega_k = \begin{cases} z\,\mathrm{d}z/w^{d-k} & \text{for } 0 < k < d/3, \\ \mathrm{d}z/w^k & \text{for } d/3 < k < d. \end{cases}$$

for integer $0 < k < d$.

Proof. That C has genus $d - 1$ follows by applying the Riemann–Hurwitz formula to the covering $\pi\colon C \to \mathbb{P}^1$, $(z, w) \mapsto z$. That the ω_k form a basis of holomorphic one-forms is proved in [59, Theorem 3.1]. □

We fix some notations concerning the homology and cohomology of C. The group $H_1(C, \mathbb{Z})$ is a free abelian group of rank $2(d-1)$, and the intersection form is a perfect skew-symmetric pairing

$$\langle \cdot, \cdot \rangle\colon H_1(C, \mathbb{Z}) \times H_1(C, \mathbb{Z}) \to \mathbb{Z}.$$

Complex singular cohomology $H^*(C,\mathbb{C})$ can be identified with de Rham cohomology, with the cup product being translated to the exterior product. Evaluation on the fundamental class $\alpha([C])$ corresponds to integration $\int_C \alpha$, so we use the latter symbolism even when only integral cohomology classes are considered. Poincaré duality provides an isomorphism

$$(\cdot)^\sharp \colon H_1(C,\mathbb{Z}) \to H^1(C,\mathbb{Z}), \quad x \mapsto x^\sharp \text{ with } \alpha(x) = \int_C \alpha \wedge x^\sharp \text{ for all } \alpha \in H^1(C,\mathbb{Z}).$$

This relates the intersection form with the exterior product in the sense that

$$\langle x, y\rangle = \int_C x^\sharp \wedge y^\sharp \text{ for all } x, y \in H_1(C,\mathbb{Z}).$$

Every homeomorphism $f\colon C \to C$ induces automorphisms f_* and f^* of homology and cohomology, resp.; they are related by

$$f^{*,-1}(x^\sharp) = (f_*(x))^\sharp. \tag{5.5}$$

Via de Rham cohomology $H^1(C,\mathbb{C})$ can be identified with the space of harmonic one-forms on C, and this can be written as $\Omega^1(C) \oplus \overline{\Omega^1(C)}$. On this space there is an Hermitian form

$$(\cdot,\cdot)\colon H^1(C,\mathbb{C}) \times H^1(C,\mathbb{C}) \to \mathbb{C}, \quad (\alpha,\beta) = \frac{\sqrt{-1}}{2}\int_C \alpha \wedge \overline{\beta}.$$

It is positive definite on $\Omega^1(C)$ and negative definite on $\overline{\Omega^1(C)}$.

For each d-th root of unity we obtain automorphisms $\varphi(\xi)_*$ of $H_1(C,\mathbb{Z})$ and $\varphi(\xi)^*$ of $H^1(C,\mathbb{C})$. The latter respects the subspace $\Omega^1(C)$. If $\sigma\colon \mathbb{Q}(\zeta_d) \to \mathbb{C}$ is a field embedding, we set

$$H_1(C)_\sigma = \{x \in H_1(X,\mathbb{C}) \mid \varphi(\xi)_*(x) = \sigma(\xi)x \text{ for every } \xi \in \mu_d\},$$
$$H^1(C)_\sigma = \{\alpha \in H^1(X,\mathbb{C}) \mid \varphi(\xi)^*(\alpha) = \sigma(\xi)\alpha \text{ for every } \xi \in \mu_d\},$$
$$H^{1,0}(C)_\sigma = H^1(C)_\sigma \cap \Omega^1(C) \text{ and } H^{0,1}(C)_\sigma = H^1(C)_\sigma \cap \overline{\Omega^1(C)}.$$

From (5.5) we deduce that the Poincaré duality isomorphism maps $H_1(C)_\sigma$ to $H^1(C)_{\sigma\circ\kappa}$ where κ is complex conjugation.

Proposition 5.8. *Let $d = 2r$. For every embedding $\sigma\colon K = \mathbb{Q}(\zeta_r) \to \mathbb{C}$ the space $H^1(C)_\sigma$ is two-dimensional.*

Let ε be as in (5.1). Then $H^1(C)_\varepsilon$ is the direct sum of its one-dimensional subspaces $H^{1,0}(C)_\varepsilon$ and $H^{0,1}(C)_\varepsilon$. These are generated by

$$\frac{\mathrm{d}z}{w^{r-2}} \text{ and } \overline{\left(\frac{z\,\mathrm{d}z}{w^{r+2}}\right)},$$

respectively. The signature of $(\cdot,\cdot)$ restricted to $H^1(C)_\varepsilon$ is $(1,1)$.

Proof. This is a simple calculation using the basis for $\Omega^1(C)$ given in Proposition 5.7; it is performed in [59, p. 906]. □

Now we study how simple hypergeometric curves vary in families. Since they are essentially determined by their branching loci, their moduli are closely related with those of point configurations in $\mathbb{C}$. Now there are two distinct notions of equivalence for simple hypergeometric curves $\pi\colon C \to \mathbb{P}^1$: we may either demand that their projections to $\mathbb{P}^1$ agree pointwise, or that they are related by an automorphism of $\mathbb{P}^1$ fixing infinity.

5.3.2 The family of simple hypergeometric curves over $\mathrm{Conf}_3(\mathbb{C})$ and its period map

From the first point of view it is most natural to start with the *configuration space* $\mathrm{Conf}_3(\mathbb{C})$ which consists of all three-element subsets $S \subset \mathbb{C}$. This can be seen as an affine complex variety: with $S \in \mathrm{Conf}_3(\mathbb{C})$ we associate the monic polynomial $f_S(z) = \prod_{s\in S}(z-s)$. If

$$\mathfrak{D}(a,b,c) = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$$

denotes the discriminant of the polynomial $z^3 + az^2 + bz + c$, assigning to S the coefficients of f_S defines a biholomorphism from $\mathrm{Conf}_3(\mathbb{C})$ to $\mathbb{C}^3 \smallsetminus \{\mathfrak{D} = 0\}$.

Fix the degree $d = 2r$. Then for every $S \in \mathrm{Conf}_3(\mathbb{C})$ there is a simple hypergeometric curve $C_S \to \mathbb{P}^1$ ramified over $S \cup \infty$, with affine model $w^{2r} = f_S(z)$. These glue to a family of algebraic curves $\mathscr{C} \to \mathrm{Conf}_3(\mathbb{C})$, and the homomorphisms $\varphi_C\colon \mu_d \to \operatorname{Aut} C_S$ glue to $\varphi\colon \mu_d \to \operatorname{Aut}\mathscr{C}$.

We fix some "base configuration" $S_0 \in \mathrm{Conf}_3(\mathbb{C})$ (for symmetry reasons we may think of it as the set of third roots of unity). A *marking* of a point configuration $S \in \mathrm{Conf}_3(\mathbb{C})$ is an isotopy class of compactly supported homeomorphisms $m\colon \mathbb{C} \to \mathbb{C}$ with $m(S_0) = S$; here we only consider isotopies that are constant on S_0, and a homeomorphism is called compactly supported if it agrees with the identity outside a compact subset. The set of all marked configurations is again in a natural way a complex manifold $\mathscr{T}_{\mathrm{Conf}}$ endowed with a forgetful map $\mathscr{T}_{\mathrm{Conf}} \to \mathrm{Conf}_3(\mathbb{C})$; this map turns it into the universal covering space of $\mathrm{Conf}_3(\mathbb{C})$. We call $\mathscr{T}_{\mathrm{Conf}}$ the *Teichmüller space of configurations.*

On this space the mapping-class group $\mathrm{Mod}^c(\mathbb{C}, S_0)$, consisting of isotopy classes of homeomorphisms $(\mathbb{C}, S_0) \to (\mathbb{C}, S_0)$ as in the definition of a marking, acts as the deck transformation group of the universal covering.

For each marked configuration (S, m) we can consider the curve C_S; the marking m gives an isomorphism of cohomology groups $m^*\colon H^1(C_S) \to H^1(C_{S_0})$ respecting the Hermitian forms and the actions of the respective operators $\varphi(\xi)$. In particular m^* sends the $\varphi(\xi)$-eigenspace $H^1(C_S)_\varepsilon$ to $H^1(C_{S_0}, \mathbb{C})_\varepsilon$. Their subspaces $H^{1,0}(C_S)_\varepsilon$ and $H^{1,0}(C_{S_0})_\varepsilon$, however, need not be related by m^*, so the following makes sense:

Definition 5.9. *Let $L \simeq \mathbb{P}^1$ be the space of complex lines in $H^1(C_{S_0})_\varepsilon$, and let $L^+ \subset L$ be the subspace of positive lines for the Hermitian form $(\cdot,\cdot)$ (this is an*

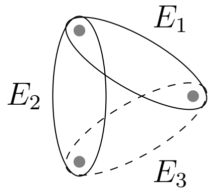

Figure 5.2: Generators of Br_3

open disk in L, hence biholomorphic to the unit disk). The period map at ε *is the map* $p\colon \mathscr{T}_{\mathrm{Conf}} \to L^+$ *that sends a marked point configuration* (S, m) *to the point defined by the subspace* $m^*(H^{1,0}(C_S)_\varepsilon)$.

The mapping-class group $\mathrm{Mod}^c(\mathbb{C}, S_0)$ acts on both domain and target of the period map. As to the target, note that each homeomorphism $(\mathbb{C}, S_0) \to (\mathbb{C}, S_0)$ which is the identity outside a compact set K has a unique lift to C_{S_0} with the property that it is the identity outside $\pi^{-1}(K)$, where $\pi\colon C_{S_0} \to \mathbb{P}^1$ is the projection. This defines a homomorphism $\mathrm{Mod}^c(\mathbb{C}, S_0) \to \mathrm{Mod}(C_{S_0})$, and all elements in the image commute with the mapping-classes of the automorphisms $\varphi(\xi)$. Hence their action on cohomology $H^1(C_{S_0})$ stabilises the $\varphi(\xi)$-eigenspaces. In short, we have a homomorphism $\varrho_\varepsilon\colon \mathrm{Mod}^c(\mathbb{C}, S_0) \to \mathrm{GL}(H^1(C_{S_0})_\varepsilon)$. We denote the composition

$$\mathrm{Mod}^c(\mathbb{C}, S_0) \xrightarrow{\varrho_\varepsilon} \mathrm{GL}(H^1(C_{S_0})_\varepsilon) \to \mathrm{PGL}(H^1(C_{S_0})_\varepsilon) = \mathrm{Aut}\, L$$

by $\mathrm{P}\varrho_\varepsilon$. Since the image of ϱ_σ preserves the Hermitian form on $H^1(C_{S_0})_\varepsilon$, the image of $\mathrm{P}\varrho_\varepsilon$ preserves the set L^+ of positive lines and we may write

$$\mathrm{P}\varrho_\varepsilon\colon \mathrm{Mod}^c(\mathbb{C}, S_0) \to \mathrm{Aut}\, L^+ = \mathrm{PU}(H^1(C_{S_0})_\varepsilon) \simeq \mathrm{PU}(1, 1).$$

Proposition 5.10. *The period map* $p\colon \mathscr{T}_{\mathrm{Conf}} \to L^+$ *is* $\mathrm{Mod}^c(\mathbb{C}, S_0)$*-equivariant for the tautological action on* $\mathscr{T}_{\mathrm{Conf}}$ *and the action defined by* $\mathrm{P}\varrho_\sigma$ *on* L^+. □

In the next subsection we shall show that the image of $\mathrm{P}\varrho_\varepsilon$ is a $(2, 3, r)$ triangle group.

5.3.3 The mapping-class group as a braid group

For the results on braid groups mentioned in this section cf. [8, chapter 1].

The mapping-class group $\mathrm{Mod}^c(\mathbb{C}, S_0)$ can be identified with Artin's braid group Br_3 on three strands: an element of $\mathrm{Mod}^c(\mathbb{C}, S_0)$ is represented by a homeomorphism $\mathbb{C} \to \mathbb{C}$ sending S_0 to S_0; ignoring what happens on S_0, this is isotopic to the identity. Let $h\colon [0, 1] \times \mathbb{C} \to \mathbb{C}$ be such an isotopy, and extend it to a homeomorphism $H\colon [0, 1] \times \mathbb{C} \to [0, 1] \times \mathbb{C}$ by $H(t, z) = (t, h(t, z))$. Then $H([0, 1] \times S_0) \subset [0, 1] \times \mathbb{C}$ is a braid. The thus defined homomorphism $\mathrm{Mod}^c(\mathbb{C}, S_0) \to \mathrm{Br}_3$ is an isomorphism. We shall identify these two groups when no confusion arises.

We give a redundant but symmetric system of generators b_1, b_2, b_3 for Br_3: with ellipses E_i as in Figure 5.2, let b_i be a half Dehn twist around E_i in counter-clockwise direction. Then Br_3 is presented as the group generated by b_1, b_2 modulo the one relation

$$b_1b_2b_1 = b_2b_1b_2;$$

this relation is equivalent to

$$(b_1b_2)^3 = (b_1b_2b_1)^2.$$

The element $R = b_1b_2$ satisfies $Rb_iR^{-1} = b_{i+1}$ (indices interpreted cyclically modulo 3), whence we can express b_3 as a word in b_1 and b_2, and see that all b_i are conjugate. The centre of Br_3 is infinite cyclic generated by $c = R^3 = (b_1b_2)^3 = (b_1b_2b_1)^2$.

Definition 5.11. *Let r be a positive integer.*

(i) $\delta^r\colon \mathrm{Br}_3 \to \mu_r$ is the unique group homomorphism with $\delta^r(b_i) = \zeta_r$ for each i.

(ii) Br_3^r is the kernel of δ^r.

The following observation will be useful:

Lemma 5.12. *Assume that $r \equiv \pm 1 \bmod 6$. Then every element $b \in \mathrm{Br}_3^r$ can be written as a product $b = c^nb'$ with $n \in \mathbb{Z}$ (so that c^n is in the centre of Br_3) and $b' \in \mathrm{Br}_3^r$.*

Proof. Let $\delta^r(b) = \zeta_r^k$. By assumption there exists $n \in \mathbb{Z}$ with $6n \equiv k \bmod r$. If we set $b' = c^{-n}b$, then because of $\delta^r(c) = \zeta_r^6$ we find that $\delta^r(b') = 1$ and $b = c^nb$. □

With this preparation we now turn to the representation $\varrho_\varepsilon\colon \mathrm{Br}_3 \to \mathrm{U}(H^1(C)_\varepsilon)$.

Proposition 5.13. *The two-dimensional $\mathbb{C}$-vector space $H_1(X_0, \mathbb{C})_\varepsilon$ is generated by three vectors e_1, e_2, e_3 with the following properties:*

(i) $e_1 + e_2 + e_3 = 0$.

(ii) $B_i = \varrho_\varepsilon(b_i)$ operates by

$$B_i(e_i) = \zeta_r e_i, \quad B_i(e_{i+1}) = e_{i+1} - \zeta_r e_i, \quad B_i(e_{i+2}) = e_i + e_{i+2},$$

where indices are interpreted cyclically modulo 3.

Proof. McMullen [59, Theorem 4.1] constructs a system of generators e_1, e_2, e_3; we shall show that it satisfies (i) and (ii).

He describes the behaviour of the intersection form on these generators; note that what he calls $\langle x, y\rangle$ is equal to (x, y) in our notation, hence his relations become

$$(e_i, e_i) = -2\sin\frac{2\pi}{r}, \quad (e_i, e_{i+1}) = \sqrt{-1}(1 + \zeta_r^{-1}), \quad (e_i, e_{i+2}) = -\sqrt{-1}(1 + \zeta_r).$$

From these relations we easily compute that $(e_1 + e_2 + e_3, e_i) = 0$ for every i. But the e_i generate the vector space, and the form is nondegenerate by Proposition 5.8. This shows (i).

Finally, formula (4.1) in the proof of [59, Theorem 4.1] gives our statement (ii). □

Lemma 5.14. *(i) The determinant of the representation $\varrho_\sigma\colon \mathrm{Br}_3 \to \mathrm{U}(H_1(C)_\varepsilon)$ is equal to δ^r. In particular we obtain a representation*

$$\varrho_\varepsilon\colon \mathrm{Br}_3^r \to \mathrm{SU}(H_1(C)_\varepsilon).$$

(ii) Recall that $c = (b_1b_2)^3 = (b_1b_2b_1)^2$ generates the centre of Br_3*. Its image $\varrho_\varepsilon(c)$ is scalar multiplication by $-\zeta_r^3$.*

Proof. From Proposition 5.13.(i) we see that e_1, e_2 form a basis of $H_1(C)_\varepsilon$, hence from expressing $\varrho_\varepsilon(b_1)$ in this basis we see that $\det \varrho_\varepsilon(b_1) = \zeta_r = \delta^r(b_1)$. Since the range μ_r of δ^r is commutative and the b_i are conjugate to each other, we see that also $\det \varrho_\varepsilon(b_i) = \zeta_r = \delta^r(b_i)$. Since these elements generate the braid group, we find that $\det \varrho_\varepsilon = \delta^r$.

Claim (ii) follows by explicitly computing $\varrho_\varepsilon(c)$, which we omit. □

For the next proposition we consider the isomorphism $H^1(C)_\varepsilon \simeq \mathbb{C}^2$ defined by the basis e_1, e_2. The form $(\cdot,\cdot)$ on $H^1(C)_\varepsilon$ defines an Hermitian form of signature $(1,1)$ on $\mathbb{C}^2$ whose associated unitary group we denote by $\mathrm{U}(1,1)$. Then $\operatorname{Aut} L^+ = \mathrm{PU}(H^1(C)_\varepsilon)$ becomes identified with $\mathrm{PU}(1,1) \simeq \mathrm{PSU}(1,1)$.

Proposition 5.15. *Under these isomorphisms:*

(i) The braid group Br_3 *and its subgroup* Br_3^r *have the same image under* $\mathrm{P}\varrho_\varepsilon$*, which is a $(2,3,r)$-triangle group $\Delta \subset \mathrm{PSU}(1,1) = \operatorname{Aut} L^+$.*

(ii) $\varrho_\varepsilon(\mathrm{Br}_3^r)$ becomes identified with the preimage $\tilde{\Delta}$ in $\mathrm{SU}(1,1)$ *of the $(2,3,r)$-triangle group $\Delta \subset \mathrm{PSU}(1,1)$.*

Proof. We first determine the image of $\varrho_\varepsilon(\mathrm{Br}_3)$ in $\mathrm{PU}(1,1)$. An alternative system of generators for Br_3 is given by $\alpha = b_1b_2b_1 = b_2b_1b_2$, $\beta = b_1b_2$ and $\gamma = b_1$. In the basis e_1, e_2, the images of these elements under ϱ_ε are represented by the following matrices:

$$\alpha \mapsto \begin{pmatrix} 0 & -\zeta_r^2 \\ \zeta_r & 0 \end{pmatrix}, \quad \beta \mapsto \begin{pmatrix} 0 & -\zeta_r^2 \\ 1 & \zeta_r \end{pmatrix}, \quad \gamma \mapsto \begin{pmatrix} \zeta_r & -\zeta_r \\ 0 & 1 \end{pmatrix}.$$

So by rescaling them in such a way that their determinants become one, we see that the images of the three generators in $\mathrm{PSU}(1,1) \simeq \mathrm{PU}(1,1)$ are

$$\alpha \mapsto \pm\begin{pmatrix} 0 & -\zeta_{2r} \\ \zeta_{2r}^{-1} & 0 \end{pmatrix}, \quad \beta \mapsto \pm\begin{pmatrix} 0 & -\zeta_r \\ \zeta_r^{-1} & 1 \end{pmatrix}, \quad \gamma \mapsto \pm\begin{pmatrix} \zeta_{2r} & -\zeta_{2r} \\ 0 & \zeta_{2r}^{-1} \end{pmatrix}.$$

Then by calculating traces we see that in $\mathrm{PU}(1,1)$, the image A of α is a hyperbolic rotation with angle π, the image B of β is a hyperbolic rotation with angle $\frac{2\pi}{3}$, and the image C of γ is a hyperbolic rotation with angle $\frac{2\pi}{r}$. Furthermore, ABC is the image of $b_2b_1b_2b_1b_2b_1 = c$ which is known to be a scalar multiplication in $\mathrm{U}(1,1)$ by Lemma 5.14, therefore the identity in $\mathrm{PU}(1,1)$. That is, the subgroup of $\mathrm{PU}(1,1)$ generated by A, B, C is the one and only $(2,3,r)$ triangle group Δ by Proposition 5.2.(i).

From Lemma 5.12 and Lemma 5.14.(ii) it follows that the image of Br_3^r in $\mathrm{PU}(1,1)$ is also Δ.

Now we can determine the group $\varrho_\varepsilon(\mathrm{Br}_3^r) \subset \mathrm{SU}(1,1)$: it has to be a subgroup of $\mathrm{SU}(1,1)$ mapping to Δ when dividing by $\{\pm 1\}$. We remember from Lemma 5.14.(ii) that $\varrho_\varepsilon(c)$ is scalar multiplication by $-\zeta_r^3$; this is a primitive $(2r)$-th root of unity. Therefore c^r, which is an element of Br_3^r, acts by multiplication with -1. Hence minus the identity is contained in $\varrho_\varepsilon(\mathrm{Br}_3^r)$, which is therefore the entire preimage of Δ in $\mathrm{SU}(1,1)$. □

This calculation explains why it is necessary to have the automorphism ε in Theorem A. For any embedding $\sigma\colon K \to \mathbb{C}$ we obtain a similar action $\mathrm{P}\varrho_\sigma$ of Br_3 on the space of lines in $H^1(C)_\sigma$; but if σ is neither ε nor its complex conjugate, then $\mathrm{P}\varrho_\sigma(\mathrm{Br}_3)$ will be an indiscrete Galois conjugate of Δ.

5.3.4 Descending to moduli space

Now we explain what happens if we identify simple hypergeometric curves whose branching loci are related by an affine map $z \mapsto az + b$. In this case we consider the moduli space $\mathscr{M}^*_{0,[3]}$ of three unordered points in an affine line (equivalently, of four points, one of which is distinguished, on a complex projective line). This is an orbifold; it can be obtained as the orbifold quotient $\mathscr{M}^*_{0,3}/\mathfrak{S}_3$, where $\mathscr{M}^*_{0,3} \simeq \mathbb{C} \smallsetminus \{0,1\}$ is the moduli space of three ordered points in an affine line (or four ordered points on a projective line) and $\mathfrak{S}_3$ is the symmetric group.

There is again a Teichmüller-theoretic description of the universal covering space of $\mathscr{M}^*_{0,[3]}$:

Let D be a smooth complex projective curve of genus zero with a distinguished point ∞, and let $S \subset D \smallsetminus \{\infty\}$ be a three-element subset. A *marking* of (D, ∞, S) is then an isotopy class of orientation-preserving homeomorphisms $\mathbb{P}^1 \to D$ sending ∞ to ∞ and S_0 to S (isotopies fixing $S_0 \cap \{\infty\}$). The set of all marked curves of this type is in a natural way a complex manifold $\mathscr{T}_{0,4}$, and the forgetful map $\mathscr{T}_{0,4} \to \mathscr{M}^*_{0,[3]}$ is the universal covering of our moduli space.

We have a commutative square of forgetful maps, where the horizontal maps are universal covering maps:

$$\begin{tikzcd}
\mathscr{T}_{\mathrm{Conf}} \arrow[r] \arrow[d] & \mathrm{Conf}_3(\mathbb{C}) \arrow[d] \\
\mathscr{T}_{0,4} \arrow[r] & \mathscr{M}^*_{0,[3]}.
\end{tikzcd}$$

Proposition 5.16. *The period map $p\colon \mathscr{T}_{\mathrm{Conf}} \to L^+$ factors through the forgetful map $\mathscr{T}_{\mathrm{Conf}} \to \mathscr{T}_{0,4}$. The resulting period map $\mathscr{T}_{0,4} \to L^+$ is a local biholomorphism.*

Proof. This is shown in [59, Theorem 6.1]. □

To have a better geometric understanding of the period map, we consider a special holomorphic family $\mathscr{C} \to \mathbb{H}$ of simple hypergeometric curves over the upper half plane: the fibre C_τ over $\tau \in \mathbb{H}$ is the smooth projective curve with affine equation

$$C_\tau\colon w^{2r} = z(z-1)(z-\tau).$$

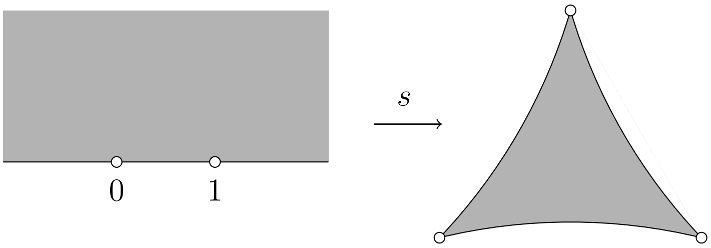

Figure 5.3: A Schwarz triangle map

From Proposition 5.8 we recall that

$$\omega_\tau = \frac{\mathrm{d}z}{w^{r-2}} \text{ and } \eta_\tau = \overline{\left(\frac{z\,\mathrm{d}z}{w^{r+2}}\right)}$$

form a basis of $H^1(C_\tau)_\varepsilon$, the first being holomorphic and the second antiholomorphic, so

$$H^{1,0}(C_\tau)_\varepsilon = \mathbb{C}\omega_\tau \text{ and } H^{0,1}(C_\tau)_\varepsilon = \mathbb{C}\eta_\tau.$$

To find coordinates invariant under parallel transport in $L = \mathbb{P}(H^1(C_\tau)_\varepsilon)$ we consider two paths γ_1 and γ_2 in C_τ that are sent bijectively to the line segments $[0,1]$ and $[1,\infty]$ in $\mathbb{P}^1$ under the projection $C_\tau \to \mathbb{P}^1$, $(z,w) \mapsto z$. It is clearly possible to choose them in a way that depends continuously on τ. Then the two linear forms

$$\int_{\gamma_1}, \int_{\gamma_2} : H^1(C_\tau)_\varepsilon \to \mathbb{C}$$

are invariant under parallel transport. Now either they are linearly dependent, or else they define a biholomorphic map

$$f\colon L = \mathbb{P}(H^1(C_\tau)_\varepsilon) \to \mathbb{P}^1, \quad \mathbb{C}\alpha \mapsto \left[\int_{\gamma_1} \alpha : \int_{\gamma_2} \alpha\right]. \tag{5.6}$$

The period map $p_{\mathbb{H}}\colon \mathbb{H} \to L^+ \subset L$ of the family (X_τ) is then given by $\tau \mapsto \mathbb{C}\omega_\tau$, and its composition with f can be written as

$$\mathbb{H} \to \mathbb{P}^1, \quad \tau \mapsto \left[\int_0^1 \frac{\mathrm{d}z}{(z(z-1)(z-\tau))^{\frac{1}{2}-\frac{1}{r}}} : \int_1^\infty \frac{\mathrm{d}z}{(z(z-1)(z-\tau))^{\frac{1}{2}-\frac{1}{r}}}\right]. \tag{5.7}$$

Proposition 5.17. *The map (5.7) is a* Schwarz triangle map: *it sends the upper half plane biholomorphically to the interior of a triangle in $\mathbb{P}^1$ bounded by three circular arcs, with all three interior angles equal to $\frac{2\pi}{r}$. Its continuous extension to the boundaries sends* 0, 1 *and* ∞ *to the triangle's vertices.*

Proof. We use the following classical result, see e.g. [66, section V.7]: a meromorphic function $s\colon \mathbb{H} \to \mathbb{P}^1$ maps $\mathbb{H}$ biholomorphically to the interior of a triangle bounded by circular arcs with interior angles $\pi\alpha$, $\pi\beta$, $\pi\gamma$ at the vertices $s(0)$, $s(1)$ and $s(\infty)$

if and only if s is a quotient of two linearly independent solutions g_1, g_2 of the hypergeometric differential equation

$$\tau(1-\tau)g''(\tau)+[c-(a+b+1)\tau]g'(\tau)-abg(\tau)=0 \tag{5.8}$$

with

$$a=\frac{1-\alpha+\beta-\gamma}{2},\quad b=\frac{1-\alpha-\beta-\gamma}{2},\quad c=1-\alpha.$$

For $\alpha=\beta=\gamma=\frac{2}{r}$ these parameters become

$$a=\frac{1}{2}-\frac{1}{r},\quad b=\frac{1}{2}-\frac{3}{r},\quad c=1-\frac{2}{r}.$$

One solution of (5.8) is given by the hypergeometric function $F(a,b,c;\tau)$; from Kummer's list of 24 solutions (see [2, equation 15.5.7]) we find that $\tau^{-a}F(a,1+a-c,1+a-b;1/\tau)$ is a second one. That the two solutions are linearly independent can be checked using the transformation formula [2, equation 15.3.7]. We compute using Euler's integral (5.3) and the substitution $x=1/z$, with nonzero constants C_1, C_2:

$$\begin{aligned}C_1F(a,b,c;\tau)&=\int_0^1 x^{-\frac{1}{2}-\frac{3}{r}}(1-x)^{-\frac{1}{2}+\frac{1}{r}}(1-x\tau)^{-\frac{1}{2}+\frac{1}{r}}\mathrm{d}x\\&=-\int_\infty^1 z^{3(\frac{1}{r}-\frac{1}{2})}\left(1-\frac{1}{z}\right)^{\frac{1}{r}-\frac{1}{2}}\left(1-\frac{\tau}{z}\right)^{\frac{1}{r}-\frac{1}{2}}\mathrm{d}z\\&=\int_1^\infty[z(z-1)(z-\tau)]^{\frac{1}{r}-\frac{1}{2}}\mathrm{d}z,\end{aligned}$$

which is the denominator of (5.7), and

$$\begin{aligned}C_2\tau^{-a}F(a,1+a-c,1+a-b;1/\tau)&=C_2\tau^{\frac{1}{r}-\frac{1}{2}}F\left(\frac{1}{2}-\frac{1}{r},\frac{1}{2}+\frac{1}{r},1+\frac{2}{r};\frac{1}{\tau}\right)\\&=\tau^{\frac{1}{r}-\frac{1}{2}}\int_0^1 z^{\frac{1}{r}-\frac{1}{2}}(z-1)^{\frac{1}{r}-\frac{1}{2}}\left(\frac{z}{\tau}-1\right)^{\frac{1}{r}-\frac{1}{2}}\mathrm{d}z\\&=\int_0^1[z(z-1)(z-\tau)]^{\frac{1}{r}-\frac{1}{2}}\mathrm{d}z\end{aligned}$$

which is the numerator of (5.7). □

In particular this map is nonconstant, whence the two integrals are really linearly independent and (5.6) really defines a coordinate on the projective line L.

This calculation has the following significance for our problem: the Teichmüller space $\mathscr{T}_{0,4}$ can be identified with the universal covering space of $\mathbb{C}\setminus\{0,1\}\simeq\mathscr{M}^*_{0,3}$. The last isomorphism identifies $\tau\in\mathbb{C}\setminus\{0,1\}$ with the point configuration $(0,1,\tau)$. The upper half plane $\mathbb{H}\subset\mathscr{M}^*_{0,3}$ is a simply connected open subset, therefore it admits some lift $\tilde{\mathbb{H}}$ to $\mathscr{T}_{0,4}$. Then our calculation means that for some isomorphism $L\simeq\mathbb{P}^1$ the restriction of the period map $p\colon\mathscr{T}_{0,4}\to L\simeq\mathbb{P}^1$ to $\tilde{\mathbb{H}}$ is given by (5.7).

Proposition 5.18. *The image of $\mathscr{T}_{0,4}$ under the period map $p\colon \mathscr{T}_{0,4} \to L^+$ is L^+ minus a discrete countable subset.*

More precisely, the image of $\tilde{\mathbb{H}} \subset \mathscr{T}_{0,4}$ is the interior of a geodesic equilateral triangle with interior angles $\frac{2\pi}{r}$ in L^+. Reflecting this repeatedly along its sides gives a tesselation $\mathscr{C}$ of L^+ by triangles, and the image of the period map is L^+ minus the set $V(\mathscr{C})$ of vertices of $\mathscr{C}$.

Proof. From Proposition 5.17 we see that there exists some disk $D \subset L$ with corresponding Poincaré metric such that p maps $\tilde{\mathbb{H}}$ biholomorphically to the interior of a geodesic equilaretal triangle T in D with interior angles equal to $\frac{2\pi}{r}$. Furthermore it extends to a homeomorphism $\mathbb{H} \cup \mathbb{P}^1(\mathbb{R}) \to \overline{T}$ (the topological closure of T), smooth outside of $0, 1, \infty$ which are mapped to the vertices of T. By the Schwarz reflection principle, all (open) edges and faces of $\mathscr{C}$ are in the image of p.

This shows the statement except for the identification $D = L^+$. But since the image of the period map is contained in L^+ we must have $D \subseteq L^+$. On the other hand all elements of $\Delta(2,3,r) = \mathrm{P}\varrho_\varepsilon(\mathrm{Br}_3)$ have to operate as isometries of L^+, which shows that the boundary of D, which is the limit set of $\Delta(2,3,r)$, has to be contained in the boundary of L^+, so $D = L^+$. □

Again the choice of the embedding ε turns out to be crucial. For $\sigma\colon K \to \mathbb{C}$ which is neither ε nor its complex conjugate we will still obtain a period map and a Schwarz triangle mappping, but the triangles' interior angles will be proper multiples of $\frac{2\pi}{r}$, so continued reflection will lead to overlapping.

In the next lemma an *affine-linear map* is a map $\mathbb{C} \to \mathbb{C}$ of the form $z \mapsto az + b$ with $a, b \in \mathbb{C}$, $a \neq 0$.

Lemma 5.19. *For $i = 1, 2$, let $t_i \in \mathscr{T}_{\mathrm{Conf}}$ be represented by a configuration $S_i \subset \mathbb{C}$ and a homeomorphism $m_i\colon (\mathbb{C}, S_0) \to (\mathbb{C}, S_i)$. The following are equivalent:*

(i) $p(t_1) = p(t_2)$;

(ii) there exists an affine-linear map $\ell\colon \mathbb{C} \to \mathbb{C}$ with $\ell(S_1) = S_2$ such that the class of $m_2^{-1} \circ \ell \circ m_1$ in Br_3 is in the kernel of $\mathrm{P}\varrho_\varepsilon$.

Proof. The implication (ii) ⇒ (i) is clear. For the other direction, we make a case distinction as to the size of

$$\mathrm{Aut}(S) = \{\ell\colon \mathbb{C} \xrightarrow{\sim} \mathbb{C} \text{ affine-linear} \mid \ell(S) = S\} \hookrightarrow \mathfrak{S}_3.$$

For a generic S, the group $\mathrm{Aut}(S)$ is trivial, and we shall assume that $\mathrm{Aut}(S_1) = \mathrm{Aut}(S_2) = \{\mathrm{id}\}$. The other cases can be handled similarly.

Every $S \in \mathrm{Conf}_3(\mathbb{C})$ can be mapped by an affine-linear map to a set of the form $\{0, 1, \tau\}$ with $\tau \in \mathbb{C} \smallsetminus \{0, 1\}$. Then a simple calculation shows that

$$\mathrm{Aut}(S) = \{\mathrm{id}\} \Leftrightarrow \tau \in \mathbb{C} \smallsetminus \mathscr{E} \text{ with } \mathscr{E} = \{0, 1, 2, -1, \frac{1}{2}, \zeta_6, \zeta_6^{-1}\}.$$

Here $\mathscr{E}$ is the set of exceptional orbits for the *anharmonic group*

$$\mathfrak{A} = \left\{\lambda \mapsto \lambda, 1 - \lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, 1 - \frac{1}{\lambda}, \frac{\lambda}{\lambda - 1}\right\} \subset \mathrm{PGL}(2, \mathbb{C})$$

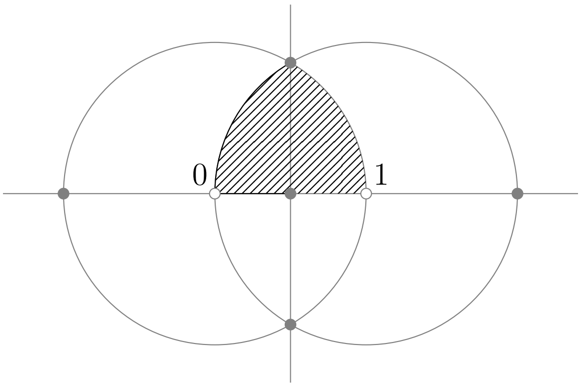

Figure 5.4: A fundamental domain for $\mathfrak{A}$

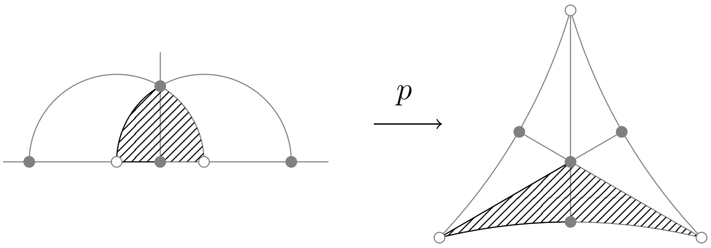

Figure 5.5: The period map on $\tilde{\mathscr{F}}$

(whose action on $\mathbb{C} \smallsetminus \{0, 1\}$ corresponds to the action of $\mathfrak{S}_3 \simeq \mathfrak{A}$ on the elements of S via rescaling). Note that geometrically, $\mathfrak{A}$ is a triangle group of type $(2, 3, 2)$. A fundamental domain for $\mathfrak{A}$ acting on $\mathbb{C} \smallsetminus \mathscr{E}$ is given by

$$\mathscr{F} = \{\tau \in \mathbb{H} \mid |\tau| < 1 \text{ and } |\tau - 1| \leq 1\} \cup \left]0, \frac{1}{2}\right[,$$

the shaded area in Figure 5.4. It is a fundamental domain in the strong sense that for every $\tau \in \mathbb{C} \smallsetminus \mathscr{E}$ there exist precisely one $g \in \mathfrak{A}$ with $g(\tau) \in \mathscr{F}$.

Recall that we have lifted $\mathbb{H}$ to an open subset $\tilde{\mathbb{H}} \subset \mathscr{T}_{0,4}$, and there is a unique extension to a continuous lift $\tilde{\mathscr{F}}$ of $\mathscr{F}$. Symmetry considerations in Figure 5.5 show that the image of $\tilde{\mathscr{F}}$ under the period map is a fundamental domain for the action of $\Delta = \mathrm{P}\varrho_\varepsilon(\mathrm{Br}_3)$ on L^+ minus the fixed points of the elliptic elements, and the map $\mathscr{F} \to p(\tilde{\mathscr{F}})$ is actually a bijection since p operates on $\tilde{\mathbb{H}}$ as a Schwarz triangle map.

Now can prove the implication (i) $\Rightarrow$ (ii): let $t_i \in \mathscr{T}_{\mathrm{Conf}}$ be represented by (S_i, m_i) as in the lemma's statement, and assume that $\mathrm{Aut}(S_i)$ is trivial. Without loss of generality we may assume that $p(t_1) = p(t_2) \in p(\tilde{\mathscr{F}})$. For each i there exists a unique affine-linear map $k_i \colon \mathbb{C} \xrightarrow{\sim} \mathbb{C}$ with $k_i(S) = \{0, 1, \tau_i\}$ such that $\tau_i \in \mathscr{F}$. But then

$$p_{\mathbb{H}}(\tau_1) = p(t_1) = p(t_2) = p_{\mathbb{H}}(\tau_2).$$

But $p_{\mathbb{H}}$ being injective, this means that $\tau_1 = \tau_2$. Setting $\ell = k_2^{-1} \circ k_1$ we get a commutative diagram

$$\begin{tikzcd}
S_0 \arrow[r, "m_1"] \arrow[d, dashed, "m_2^{-1}\circ\ell\circ m_1"'] & S_1 \arrow[r, "k_1"] \arrow[d, "\ell"] & \{0,1,\tau_1\} \arrow[d, equal] \\
S_0 \arrow[r, "m_2"'] & S_2 \arrow[r, "k_2"'] & \{0,1,\tau_2\}.
\end{tikzcd} \tag{5.9}$$

Finally we observe that $\mathrm{P}\varrho_\varepsilon(m_2^{-1}\circ\ell\circ m_1)$ fixes a point of $p(\mathscr{F})$, but $p(\mathscr{F})$ contains no fixed points of nontrivial elements in $\Delta = \mathrm{P}\varrho_\varepsilon(\mathrm{Br}_3)$; hence $\mathrm{P}\varrho_\varepsilon(m_2^{-1}\circ\ell\circ m_1) = \mathrm{id}$. □

5.4 Congruence subgroups

Up to now we have only studied the monodromy action of the braid group on cohomology with complex coefficients. To find out something about its arithmetic properties, we switch to integral homology.

5.4.1 The Prym lattice

As before, let $\pi^d\colon C^d \to D$ be a simple hypergeometric curve of degree d with affine model $w^d = f(z)$. For every divisor e of d there is a unique projection $f\colon C^d \to C^e$ where $\pi^e\colon C^e \to D$ is a simple hypergeometric curve with the same branch locus, compatible with the projections to D and the distinguished monodromy operations $\varphi(\xi)$. It can be constructed by $C^e = C^d/\varphi(\mu_{d/e})$. In coordinates it is given by $f(z,w) = (z, w^{d/e})$.

Definition 5.20. *Let $\pi\colon C^d \to D$ be a simple hypergeometric curve. Its* Prym variety *is the abelian variety*

$$\operatorname{Prym} C^d = \ker^0\left(\operatorname{Jac} C^d \to \prod_{\substack{e\mid d,\\ 1<e<d}} \operatorname{Jac} C^e\right),$$

where the map between Jacobians is induced by the projections $C^d \to C^e$, and $\ker^0$ *denotes the connected component of the kernel containing* 0*.*

As a complex torus the Prym variety is given as

$$\operatorname{Prym} C^d = \Omega^1(C^d)_{\mathrm{old}}^{\perp}/H_1(C^d,\mathbb{Z})_{\mathrm{new}}.$$

Here $\Omega^1(C^d)_{\mathrm{old}}$ is the $\mathbb{C}$-linear subspace of $\Omega^1(C^d)$ generated by the pullbacks of abelian differentials from C^e for proper divisors e of d, and $\Omega^1(C^d)_{\mathrm{old}}^{\perp}$ is the space of linear forms $\Omega^1(C^d) \to \mathbb{C}$ vanishing on $\Omega^1(C^d)_{\mathrm{old}}$. Finally, $H_1(C^d,\mathbb{Z})_{\mathrm{new}}$ is the intersection of the kernels of the maps $H_1(C^d,\mathbb{Z}) \to H_1(C^e,\mathbb{Z})$.

Proposition 5.21. *Assume that d is coprime to* 3*.*

The Prym variety of a simple hypergeometric curve $C = C^d$ is an abelian variety of dimension $\varphi(d)$. The automorphisms $\varphi(\xi)_*$ of $\operatorname{Jac} C$ *induced by $\varphi(\xi)$, where ξ is* *a primitive d-th root of unity, stabilise* $\operatorname{Prym} C$*, and the minimal polynomial of the restriction of each* $\varphi(\xi)_*$ *to* $\operatorname{Prym} C$ *is the d-th cyclotomic polynomial. Consequently we obtain an inclusion of rings* $\Phi_C = \Phi\colon \mathbb{Z}[\zeta_d] \hookrightarrow \operatorname{End} \operatorname{Prym} C$ *with* $\Phi(\xi) = \varphi(\xi)_*$*.*

Proof. Recall the basis $\omega_1, \dots, \omega_{d-1}$ of $\Omega^1(C)$ from Proposition 5.7. A similar basis of course exists for $\Omega^1(C^e)$ with $e|d$, and so we see that $\Omega^1(X)_{\text{old}}$ is generated by the ω_k with k, d *not* coprime. Therefore $\dim \Omega^1(C)_{\text{old}} = d - 1 - \varphi(d)$ (minus one for $d|d$ not occurring) and $\dim \operatorname{Prym} C = \dim \Omega^1(C)^{\perp}_{\text{old}} = \varphi(d)$. The action $\varphi(\xi)^*$ on $\Omega^1(C)$ is given by $\varphi(\xi)^*(\omega_k) = \xi^k \omega_k$ resp. $\xi^{-k}\omega_k$, therefore $\varphi(\xi)$ stabilises $\Omega^1(C)^{\perp}_{\text{old}}$ and operates there as a diagonalisable map all of whose eigenvalues are primitive d-th roots of unity. □

Setting $\Lambda = H_1(C, \mathbb{Z})_{\text{new}} = H_1(\operatorname{Prym} C, \mathbb{Z})$ we can therefore view Λ as an $\mathfrak{o}_K$-module, where $K = \mathbb{Q}(\zeta_r)$. The restriction of the intersection form $\langle \cdot, \cdot \rangle\colon H_1(C, \mathbb{Z}) \times H_1(C, \mathbb{Z}) \to \mathbb{Z}$ defines a skew-symmetric pairing $\Lambda \times \Lambda \to \mathbb{Z}$; we now explain how to lift it to a K-valued pairing.

For every field embedding $\sigma\colon K \to \mathbb{C}$ define a map

$$f_\sigma = \pi_\sigma \circ (\cdot)^\sharp\colon \Lambda \to H_1(C, \mathbb{C}) \overset{(\cdot)^\sharp}{\to} H^1(C, \mathbb{C}) \overset{\pi_\sigma}{\to} H^1(C)_\sigma.$$

Here π_σ is the orthogonal projection for $(\cdot, \cdot)$. We note:

Lemma 5.22. *Let $\kappa\colon K \to K$ be complex conjugation. With the $\mathfrak{o}_K$-module structure on Λ defined by Φ and that on $H^1(C)_\sigma$ defined by the identity inclusion $\mathfrak{o}_K \subset \mathbb{C}$, the map f is $(\mathfrak{o}_K, \sigma \circ \kappa)$-semilinear. That is, $f_\sigma(\alpha x) = \sigma\kappa(\alpha)x$.*

Proof. Let $\alpha \in \mathfrak{o}_K$ and $x \in \Lambda$; we need to show $f(\Phi(\alpha)(x)) = \sigma\kappa(\alpha) f(x)$.

It suffices to check this for $\alpha = \zeta_{2r}$. By definition $\Phi(\zeta_{2r})(x) = \varphi(\zeta_{2r})_*(x)$, so we need to determine $f(\varphi(\zeta_{2r})_*(x))$. Recalling (5.5) we calculate

$$\begin{aligned} f(\Phi(\zeta_{2r})(x)) &= \pi_\sigma((\varphi(\zeta_{2r})_*(x))^\sharp) = \pi_\sigma(\varphi(\zeta_{2r})^{-1,*}(x^\sharp)) \\ &= \sigma(\zeta_{2r}^{-1})\pi_\sigma(x^\sharp) = \sigma\kappa(\zeta_{2r}) f(x). \end{aligned}$$

□

Definition 5.23. *Let $\sigma\colon K \to \mathbb{C}$ be an embedding. For $x, y \in \Lambda$ we set*

$$\{x, y\}_\sigma = \int_C f_\sigma(x) \wedge \overline{f_\sigma(y)} = -2\sqrt{-1}(f_\sigma(x), f_\sigma(y)).$$

For $\varepsilon\colon K \to \mathbb{C}$ as in (5.1) we write $\{x, y\} = \{x, y\}_\varepsilon$.

To state the properties of this pairing, recall that K is a quadratic extension of its totally real subfield $F = \mathbb{Q}(\zeta_r + \zeta_r^{-1})$; the nontrivial Galois automorphism is given by complex conjugation $\alpha \mapsto \overline{\alpha}$. A $K|F$-skew-Hermitian form on an $\mathfrak{o}_K$-module M is a map $H\colon M \times M \to K$ which is sesquilinear in the sense that $H(\alpha x, \beta y) = \alpha\overline{\beta} H(x, y)$, and satisfies $H(x, y) + \overline{H(y, x)} = 0$ for all $x, y \in M$.

Proposition 5.24. *The form $\{\cdot, \cdot\}$ is a $K|F$-skew-Hermitian form on Λ. The intersection form can be retrieved as*

$$\langle x, y \rangle = \operatorname{tr}_{K|\mathbb{Q}}\{x, y\} \text{ for all } x, y \in \Lambda. \tag{5.10}$$

If $x, y \in \Lambda$, then $\{x, y\} \in \mathfrak{o}_K[1/r]$.

Proof. First we note that the image of f_σ lies actually in the subspace $H^1(C,\mathbb{C})_{\mathrm{new}}$ which is the orthogonal complement of $H^1(C,\mathbb{C})_{\mathrm{old}}$: let $x \in \Lambda$ and $\omega \in H^1(C,\mathbb{C})_{\mathrm{old}}$, then ω can be written as a linear combination of pullbacks from simple hypergeometric curves of lower degree. Without loss of generality, $\omega = g^*\eta$ where $g\colon C \to C^e$ and $\eta \in \Omega^1(C^e)$. Then we calculate

$$(f_\sigma(x),\omega) = \frac{\sqrt{-1}}{2}\int_C f_\sigma(x) \wedge \overline{g^*\eta} = \int_x g^*\overline{\eta} = \int_{g_*(x)} \overline{\eta} = 0$$

because $g_*(x) = 0$ by $x \in \Lambda = H_1(C,\mathbb{Z})_{\mathrm{new}}$. Now there is a direct sum decomposition

$$H^1(C,\mathbb{C})_{\mathrm{new}} = \bigoplus_{\sigma\colon K\to\mathbb{C}} H^1(C)_\sigma, \tag{5.11}$$

orthogonal for $(\cdot,\cdot)$ since it is defined by eigenspaces of a self-adjoint map.

Being the $\mathbb{C}$-linear span of the Poincaré dual of Λ, the subspace $H^1(C,\mathbb{C})_{\mathrm{new}}$ is actually defined over $\mathbb{Q}$, and summands $H^1(C)_\sigma$ in (5.11) are defined over K by their construction as eigenspaces. Hence the orthogonal projection π_σ is also defined over K, and we see that $\{\cdot,\cdot\}$ has indeed values in K.

Sesquilinearity follows easily from Lemma 5.22, and that $\{\cdot,\cdot\}$ is skew-Hermitian follows from the fact that the wedge product is skew-symmetric.

Concerning (5.10), note that by (5.11) every $x \in \Lambda$ can be written as

$$x^\sharp = \sum_{\sigma\colon K\to\mathbb{C}} \pi_\sigma(x^\sharp)$$

and for $x, y \in \Lambda$ we compute

$$\begin{aligned}\langle x,y\rangle = \int_C x^\sharp \wedge y^\sharp &= -2\sqrt{-1}(x^\sharp,y^\sharp)\\ &= -2\sqrt{-1}\sum_{\sigma\colon K\to\mathbb{C}}(\pi_\sigma(x^\sharp),\pi_\sigma(y^\sharp))\\ &= \sum_\sigma \int_C \pi_\sigma(x^\sharp)\wedge\pi_\sigma(y^\sharp) = \sum_\sigma \sigma(\{x,y\}) = \mathrm{tr}_{K|\mathbb{Q}}\{x,y\}\end{aligned}$$

which proves (5.10). Here the second equality holds because $y^\sharp$ is a real cohomology class, and the third equality holds because the projections π_σ for different σ are mutually orthogonal.

Finally if $x, y \in \Lambda$ and $\alpha \in \mathfrak{o}_K$ then

$$\mathrm{tr}_{K|\mathbb{Q}}\,\alpha\{x,y\} = \mathrm{tr}_{K|\mathbb{Q}}\{\Phi(\alpha)x,y\} = \langle\Phi(\alpha)x,y\rangle \in \mathbb{Z},$$

so $\{x,y\}$ lies in $\mathfrak{d}^{-1}$, the inverse different of $K|\mathbb{Q}$, which is contained in $\mathfrak{o}_K[1/r]$. □

Proposition 5.25. *The form $\{\cdot,\cdot\}$ on Λ is nondegenerate.*

Proof. Assume that $x \in \Lambda$ is such that $\{x,y\} = 0$ for all $y \in \Lambda$; taking traces to $\mathbb{Q}$ we find that $\langle x,y\rangle = 0$ for all $y \in \Lambda$. This can be expressed in terms of their Poincaré duals as $(x^\sharp,y^\sharp) = 0$ for all $y \in \Lambda$. Now $\Lambda^\sharp \otimes_{\mathbb{Z}} \mathbb{C} = H^1(C,\mathbb{C})_{\mathrm{new}}$, so $\int_x \omega = 0$ for all $\omega \in H^1(C,\mathbb{C})_{\mathrm{new}} = 0$. But also $\int_x \omega = 0$ for all $\omega \in H^1(C,\mathbb{C})_{\mathrm{old}}$, so by the nondegeneracy of $(\cdot,\cdot)$ we find that $x = 0$. □

Lemma 5.26. *The $\mathbb{C}$-linear map $\Lambda \otimes_{\mathfrak{o}_K,\sigma\kappa} \mathbb{C} \to H^1(C)_\sigma$ obtained from f_σ by scalar extension $\sigma\kappa\colon \mathfrak{o}_K \to \mathbb{C}$ is an isomorphism.*

Phrased otherwise, the image $f_\sigma(\Lambda)$ is an $\mathfrak{o}_K$-lattice in $H^1(C)_\sigma$, i.e. the obvious map $f_\sigma(\Lambda) \otimes_{\mathfrak{o}_K} \mathbb{C} \to H^1(C)_\varepsilon$ is an isomorphism.

Proof. The two spaces have the same dimension, so it suffices to show injectivity. Since $\{\cdot,\cdot\}$ is nondegenerate, so is its scalar extension $\{\cdot,\cdot\}_\mathbb{C}$ on $\Lambda \otimes_{\mathfrak{o}_K,\overline{\varepsilon}} \mathbb{C}$, which is a skew-Hermitian form in the usual sense. Since the map in the Lemma relates this form, up to a scalar factor, to the nondegenerate form $(\cdot,\cdot)$, it has to be injective. □

5.4.2 Skew-Hermitian forms over finite fields

Let $\mathbb{F}$ be a finite field of odd characteristic, and let $\mathbb{K}$ be a separable two-dimensional $\mathbb{F}$-algebra; denote the nontrivial $\mathbb{F}$-algebra automorphism of $\mathbb{K}$ by $a \mapsto \overline{a}$. Let V be a finitely generated free $\mathbb{K}$-module.

Recall that a $\mathbb{K}|\mathbb{F}$-*Hermitian form* on V is a map $H\colon V \times V \to \mathbb{K}$ which is linear in the first variable, antilinear in the second variable (meaning $H(x, by) = \overline{b}H(x, y)$) and satisfies $H(x, y) = \overline{H(y, x)}$ for all $x, y \in V$. Such a form is called *nondegenerate* if $H(x, y) = 0$ for all $y \in V$ implies $x = 0$. An *orthonormal basis* for an Hermitian form H is a $\mathbb{K}$-basis $(e_1, \dots, e_n)$ of V such that $H(e_i, e_j) = \delta_{ij}$.

Either $\mathbb{K}$ is itself a field or $\mathbb{K} \simeq \mathbb{F} \times \mathbb{F}$. In the second case, Hermitian forms boil down to something simpler: a free $(\mathbb{F} \times \mathbb{F})$-module V of rank n is of the form $V_1 \times V_2$, where each V_j is an $\mathbb{F}$-vector space of dimension n, and scalar multiplication is of the form $(\lambda_1, \lambda_2) \cdot (v_1, v_2) = (\lambda_1 v_1, \lambda_2 v2)$. An Hermitian form H can be written as (H_1, H_2) with each H_i having values in $\mathbb{F}$. We then define an $\mathbb{F}$-bilinear map $h\colon V_1 \times V_2 \to \mathbb{F}$ by $h(v_1, w_2) = H_1((v_1, 0), (0, w_2))$. The form H is completely determined by h: we find that

$$H((v_1, 0), (w_1, 0)) = H((1, 0) \cdot (v_1, 0), (1, 0) \cdot (w_1, 0)) = (1, 0) \cdot \overline{(1, 0)} \cdot H(\cdots) = 0$$

and similarly

$$H((0, v_2), (0, w_2)) = 0;$$

the first mixed case is simplified as

$$\begin{aligned} H((v_1, 0), (0, w_2)) &= H((1, 0)(v_1, 0), (0, w_2)) \\ &= (1, 0)H(\cdots) = (H_1(\cdots), 0) = (h(v_1, w_2), 0), \end{aligned}$$

and for the second mixed case we conclude

$$\begin{aligned} H((0, v_2), (w_1, 0)) &= \overline{H((w_1, 0), (0, v_2))} \\ &= \overline{(h(w_1, v_2), 0)} = (0, h(w_1, v_2)). \end{aligned}$$

Adding all these together we obtain

$$H((v_1, v_2), (w_1, w_2)) = (h(v_1, w_2), h(w_1, v_2)). \tag{5.12}$$

Vice versa, any $\mathbb{F}$-bilinear form $h\colon V_1 \times V_2 \to \mathbb{F}$ defines an Hermitian form H on V by (5.12); H is nondegenerate if and only if h is a perfect pairing.

Lemma 5.27. *Let H be a nondegenerate $\mathbb{K}|\mathbb{F}$-Hermitian form on V. Then there exists an orthonormal basis for H.*

Proof. The result is well-known if $\mathbb{K}$ is itself a field (an orthonormal basis can be constructed by the Gram–Schmidt procedure, using that the norm map $\mathrm{N}\colon \mathbb{K}^\times \to \mathbb{F}^\times$ is surjective), so we assume $\mathbb{K} = \mathbb{F} \times \mathbb{F}$. Writing $V = V_1 \times V_2$ as above and using the correspondence $H \leftrightarrow h$, we obtain a perfect pairing $h\colon V_1 \times V_2 \to \mathbb{F}$. So we may choose an $\mathbb{F}$-basis $(b_1, \dots, b_n)$ of V_1 and the corresponding dual basis $(b_1^*, \dots, b_n^*)$ of V_2, which is determined by $h(b_i, b_j^*) = \delta_{ij}$. From (5.12) we see that $(e_1, \dots, e_n)$ with $e_i = (b_i, b_i^*)$ is an orthonormal basis of V. □

In practice we need to work with skew-Hermitian forms instead; these are defined precisely like Hermitian forms with the exception that the equation $H(x, y) = \overline{H(y, x)}$ is replaced by $H(x, y) + \overline{H(y, x)} = 0$. If we fix an element $t \in \mathbb{K}^\times$ with $t + \bar{t} = 0$ (these always exist), we obtain a bijection between Hermitian and skew-Hermitian forms by $H \leftrightarrow tH$. Orthonormal bases in the old sense do not exist, but we can instead consider t-orthonormal bases, i.e. bases $(e_1, \dots, e_n)$ satisfying $H(e_i, e_j) = t\delta_{ij}$. Note also that the unitary group

$$\mathrm{U}(tH) = \mathrm{U}(H) = \{g \in \mathrm{GL}(V) \mid H(g(v), g(w)) = H(v, w) \text{ for all } v, w \in V\}$$

acts simply transitively on t-orthonormal bases.

Although the notion of t-orthonormal bases seems to depend on t, this complication can easily be avoided. Suppose that s is another invertible element of $\mathbb{K}$ with $s + \bar{s} = 0$. Then $s = \ell t$ for some $\ell \in \mathbb{F}^\times$, and there exists some element $k \in \mathbb{K}^\times$ with $k\bar{k} = \ell$. Then if $(e_1, \dots, e_n)$ is a t-orthonormal basis, $(ke_1, \dots, ke_n)$ is an s-orthonormal basis. Vice versa, if $(e_1, \dots, e_n)$ is a t-orthonormal basis and $k \in \mathbb{K}^\times$, then $(ke_1, \dots, ke_n)$ is a $(k\bar{k}t)$-orthonormal basis. Hence we can define a *projectivised orthonormal basis* for a skew-Hermitian form H as an equivalence class of n-tuples in V, where $(e_1, \dots, e_n) \sim (\lambda e_1, \dots, \lambda e_n)$ with $\lambda \in \mathbb{K}^\times$, such that some (any) representative defines a t-orthonormal basis for some t.

Let $\mathbb{F}_p$ be the prime field contained in $\mathbb{F}$, and define the $\mathbb{F}_p$-bilinear form $\langle \cdot, \cdot \rangle$ by

$$\langle v, w \rangle = \mathrm{tr}_{\mathbb{K}|\mathbb{F}_p} H(v, w).$$

Lemma 5.28. *Let $(e_1, \dots, e_n)$ be a $\mathbb{K}$-basis of V. The following are equivalent:*

(i) $(e_1, \dots, e_n)$ is a t-orthonormal basis for H, for some $t \in \mathbb{K}^\times$ with $t + \bar{t} = 0$.

(ii) For all $x, y \in \mathbb{K}$ and all i, j, the equation $\langle xe_i, ye_i \rangle = \langle xe_j, ye_j \rangle$ holds, and for $i \neq j$, the equation $\langle xe_i, ye_j \rangle = 0$ holds.

Proof. The implication $(i) \Rightarrow (ii)$ is easy, so let us assume that (ii) holds. Set $t_i = H(e_i, e_i)$, then $\langle xe_i, e_j \rangle = \mathrm{tr}_{\mathbb{K}|\mathbb{F}_p}(xt_i)$. Therefore $\mathrm{tr}(xt_i) = \mathrm{tr}(xt_j) = 0$ for every x, and by Lemma 5.29 below we conclude that $t_i = t_j$, in particular all $H(e_i, e_i)$ are equal to some common $t \in \mathbb{K}$ which must, H being skew-Hermitian, satisfy $t + \bar{t} = 0$, hence be invertible. □

Lemma 5.29. *Let $t \in \mathbb{K}$ be such that $\mathrm{tr}_{\mathbb{K}|\mathbb{F}_p}(tx) = 0$ for every $x \in \mathbb{K}$. Then $t = 0$.*

Proof. Assume first that $\mathbb{K}$ is a field. If $t \neq 0$, then t is invertible, hence the assumption implies that the trace is identically zero on $\mathbb{K}$, which contradicts the fact that extensions between finite fields are always separable. Hence $t = 0$.

Now assume that $\mathbb{K} = \mathbb{F} \times \mathbb{F}$ and $t = (t_1, t_2)$. Then for $x = (x_1, x_2)$ we find that $\operatorname{tr}(xt) = \operatorname{tr}_{\mathbb{F}|\mathbb{F}_p}(x_1 t_1 + x_2 t_2)$. If one of the t_j were nonzero, we would again obtain that the trace $\operatorname{tr}_{\mathbb{F}|\mathbb{F}_p}$ vanishes identically. Hence $t = (0, 0) = 0$. □

Lemma 5.30. *The group* $\mathrm{PSU}(V)$ *operates on the set* $\mathscr{B}(V)$ *of projectivised orthonormal bases for* H *without fixed points; it has precisely two orbits.*

Proof. The group $\mathrm{SU}(V)$ fits into an exact sequence

$$1 \to \mathrm{SU}(V) \to \mathrm{U}(V) \xrightarrow{\det} \mathbb{K}^\times \xrightarrow{\mathrm{N}_{\mathbb{K}|\mathbb{F}}} \mathbb{F}^\times \to 1. \tag{5.13}$$

Let $K \subset \mathbb{K}^\times$ be the kernel of the norm map. This is a finite cyclic group of even order: if $\mathbb{K}^\times$ is a field, we use the fact that every finite subgroup of the multiplicative group of a field is cyclic, see [83, Chapitre I, Théorème 2] and the remark after its proof. If $\mathbb{K} \simeq \mathbb{F} \times \mathbb{F}$, then $K \simeq \mathbb{F}^\times$ which is cyclic by the same theorem. The order is $|\mathbb{F}| + 1$ in the first case, $|\mathbb{F}| - 1$ in the second case.

Now (5.13) gives rise to a short exact sequence

$$1 \to \mathrm{PSU}(V) \to \mathrm{PU}(V) \to K/K^2 \to 1$$

with $K/K^2 \simeq \mathbb{Z}/2\mathbb{Z}$. As $\mathrm{PU}(V)$ operates simply transitively on the projectivised orthonormal bases for H, the lemma follows. □

Proposition 5.31. *Let the rank of* V *be two. Then there are group isomorphisms* $\mathrm{SU}(V) \simeq \mathrm{SL}(2, \mathbb{F})$ *and* $\mathrm{PSU}(V) \simeq \mathrm{PSL}(2, \mathbb{F})$.

Proof. For $\mathbb{K}$ a field this is a classical result, see e.g. the discussion in [100, section 3.6]. If $\mathbb{K} = \mathbb{F} \times \mathbb{F}$, write $V = V_1 \times V_2$ with a perfect pairing $h\colon V_1 \times V_2 \to \mathbb{F}$ as in (5.12). A unitary automorphism g must respect the factorisation $V_1 \times V_2$ by $\mathbb{K}$-linearity, so it can be written as $g = (g_1, g_2)$ with $g_i \in \mathrm{GL}_{\mathbb{F}}(V_i)$. From (5.12) we see that $g \in \mathrm{U}(V)$ if and only if g_2 is the inverse of the h-adjoint of g_1; therefore the map $\mathrm{U}(V) \to \mathrm{GL}_{\mathbb{F}}(V_1)$ given by $g \mapsto g_1$ is an isomorphism. The determinant of g is then $(\det g, \det g^{-1}) \in \mathbb{K}^\times = \mathbb{F}^\times \times \mathbb{F}^\times$, so the subgroup $\mathrm{SU}(V)$ is mapped isomorphically to $\mathrm{SL}_{\mathbb{F}}(V_1)$. Since this isomorphism maps $-\mathbf{1}$ to $-\mathbf{1}$, we obtain $\mathrm{PSU}(V) \simeq \mathrm{PSL}_{\mathbb{F}}(V) \simeq \mathrm{PSL}(2, \mathbb{F})$. □

5.4.3 Reduction modulo a prime ideal

We now study the reduction of Λ under a prime ideal of F.

Proposition 5.32. *Let* p *be a rational prime not dividing* r, *and let* $\Lambda_p = \Lambda/p\Lambda$. *Then the canonical map* $\Lambda_p \to H_1(C, \mathbb{F}_p)$ *is an embedding which identifies the intersection form modulo* p *on* Λ_p *with the intersection form on its image in* $H_1(C, \mathbb{F}_p)$. *The intersection form defines a perfect symplectic pairing* $\langle\cdot,\cdot\rangle_p\colon \Lambda_p \times \Lambda_p \to \mathbb{F}_p$.

Proof. Consider the automorphism $\varphi(\zeta_r)_*$ of $H_1(C,\mathbb{Z})$ (note this time we take a primite r-th root of unity, not a $2r$-th one), and let $f \in \mathbb{Z}[x]$ and D as in Lemma 5.33 below for $d = r$. Since D and p are coprime there exists some $m \in \mathbb{N}$ with $mD \equiv 1 \bmod p$. Set then $P = m \cdot f(\varphi(\zeta_r)_*) \in \operatorname{End} H_1(C,\mathbb{Z})$; from the eigenspace decomposition for $\varphi(\zeta_r)_*$ we see that this endomorphism operates as multiplication by mD on Λ, and as 0 on its orthogonal complement $\Lambda^\perp$. In particular, P is self-adjoint for the intersection form and satisfies $P^2 = mDP$.

Reduction modulo p yields a self-adjoint endomorphism

$$P_p\colon H_1(C,\mathbb{F}_p) \to H_1(C,\mathbb{F}_p)$$

with $P_p^2 = 1$ by $mD \equiv 1 \bmod p$. It is therefore an orthogonal projection onto a symplectic subspace V.

From the properties of P we conclude that

$$p\Lambda \subseteq P(H_1(C,\mathbb{Z})) \subseteq \Lambda,$$

so $V = \operatorname{im} P_p$ is contained in the image of $\Lambda \to H_1(C,\mathbb{F}_p)$. Vice versa, if $x \in \Lambda$ then in $H_1(C,\mathbb{F}_p)$ we get

$$[x] = [mDx] = [P(x)] = P_p([x]) \in V.$$

So V is the image of Λ in $H_1(C,\mathbb{F}_p)$. It remains to be shown that the kernel of the reduction map $\Lambda \to H_1(C,\mathbb{F}_p)$ is $p\Lambda$. So let $x \in \Lambda$ with its reduction $[x] = 0$; then there exists some $y \in H_1(C,\mathbb{Z})$ with $x = py$. But since Λ is the kernel of a homomorphism with torsion-free image, $y \in \Lambda$ and therefore $x \in p\Lambda$. The other inclusion is clear. □

Lemma 5.33. *Let d be a positive integer. Then there exist an integer D and a polynomial $f \in \mathbb{Z}[x]$ such that all the primes dividing D also divide d, and for a d-th root of unity ξ,*

$$f(\xi) = \begin{cases} D & \textit{if } \xi \textit{ is a } \text{primitive } d\textit{-th root of unity;} \\ 0 & \textit{else.} \end{cases}$$

Proof. Let $c_e(x)$ be the e-th cyclotomic polynomial, and set

$$g(x) = \prod_{\substack{e|d,\\ e<d}} c_e(x) = \frac{x^d-1}{c_d(x)} = \prod_{\substack{\xi^d=1\\ \xi \text{ imprimitive}}} (x-\xi).$$

Then $g(x) \in \mathbb{Z}[x]$, and for a d-th root ξ of unity, $g(\xi) \neq 0$ if and only if ξ is primitive.

Now set

$$f(x) = \prod_{\substack{1\le m\le d,\\ \gcd(d,m)=1}} g(x^m).$$

Then $f(\xi) = 0$ for any imprimitive d-root of unity ξ, and for primitive ξ we obtain

$$f(\xi) = \prod_m g(\xi^m) = \mathrm{N}_{\mathbb{Q}(\xi)|\mathbb{Q}}\, g(\xi).$$

This is a nonzero rational integer independent of ξ, so we may denote it by D. It remains to be shown that D has at most the prime divisors of d.

In the ring of integers $\mathbb{Z}[\xi]$ of $\mathbb{Q}(\xi)$ the element

$$g(\xi) = \prod_{\substack{\omega^d=1 \\ \omega \text{ imprimitive}}} (\xi - \omega)$$

is a divisor of

$$\prod_{\substack{\omega^d=1 \\ \omega\neq\xi}} (\xi - \omega) = \lim_{z\to\xi} \prod_{\substack{\omega^d=1 \\ \omega\neq\xi}} (z - \omega) = \lim_{z\to\xi} \frac{z^d-1}{z-\xi} = \frac{\partial}{\partial z}(z^d-1)|_{z=\xi} = d\xi^{d-1}.$$

Taking norms to $\mathbb{Q}$ we find that D is a divisor of $d^{\varphi(d)}$. □

Set $A_p = \mathfrak{o}_K/p\mathfrak{o}_K$ and $B_p = \mathfrak{o}_F/p\mathfrak{o}_F$; then Λ_p is in a natural way an A_p-module.

Lemma 5.34. *The A_p-module Λ_p is free of rank two.*

Proof. Since Λ is a lattice in the K-vector space $\Lambda \otimes \mathbb{Q}$, it has to be a locally free $\mathfrak{o}_K$-module of rank two. This implies that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is a free module of rank two over $\mathfrak{o}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$. □

Let $\mathfrak{p}$ be a prime in $F = \mathbb{Q}(\zeta_r + \zeta_r^{-1})$ not dividing r, and set $\mathbb{F}_{\mathfrak{p}} = \mathfrak{o}_F/\mathfrak{p}$ and $\mathbb{K}_{\mathfrak{p}} = \mathfrak{o}_K/\mathfrak{p}\mathfrak{o}_K$. Then $\mathbb{F}_{\mathfrak{p}}$ is a finite field and $\mathbb{K}_{\mathfrak{p}}$ is a separable $\mathbb{F}_{\mathfrak{p}}$-algebra of dimension two, so it is either a field itself or isomorphic to $\mathbb{F}_{\mathfrak{p}} \times \mathbb{F}_{\mathfrak{p}}$, depending on whether $\mathfrak{p}$ is inert or split in K (it cannot ramify because it does not divide r). Finally recall that Λ has a structure as $\mathfrak{o}_K$-module, and set

$$\Lambda_{\mathfrak{p}} = \Lambda/\mathfrak{p}\Lambda = \Lambda \otimes_{\mathfrak{o}_K} \mathbb{K}_{\mathfrak{p}},$$

which is in a natural way a $\mathbb{K}_{\mathfrak{p}}$-module. We denote the image of an element $x \in \Lambda$ in $\Lambda_{\mathfrak{p}}$ by $[x]_{\mathfrak{p}}$. The $K|F$-skew-Hermitian form $\{\cdot,\cdot\}$ on Λ has values in $\mathfrak{o}_K[1/r]$ by Proposition 5.24, therefore it reduces to a $\mathbb{K}_{\mathfrak{p}}|\mathbb{F}_{\mathfrak{p}}$-skew-Hermitian form

$$\{\cdot,\cdot\}_{\mathfrak{p}} \colon \Lambda_{\mathfrak{p}} \times \Lambda_{\mathfrak{p}} \to \mathbb{K}_{\mathfrak{p}}, \quad \{[x]_{\mathfrak{p}}, [y]_{\mathfrak{p}}\}_{\mathfrak{p}} = \{x, y\} \bmod \mathfrak{p}\mathfrak{o}_K.$$

Proposition 5.35. *The skew-Hermitian form $\{\cdot,\cdot\}_{\mathfrak{p}}$ on $\Lambda_{\mathfrak{p}}$ is perfect, and $\Lambda_{\mathfrak{p}}$ is a free $\mathbb{K}_{\mathfrak{p}}$-module of rank two.*

Proof. The freeness follows from Lemma 5.34 and the observation that $\Lambda_{\mathfrak{p}} = \Lambda_p \otimes_{A_p} \mathbb{K}_{\mathfrak{p}}$.

For the pairing, we first construct an auxiliary form on Λ_p with values in $A_p = \mathfrak{o}_K/p\mathfrak{o}_K$. Set $B_p = \mathfrak{o}_F/p\mathfrak{o}_F$. Since $F|\mathbb{Q}$ is a Galois extension, p splits in F as $p\mathfrak{o}_F = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ where the $\mathfrak{p}_i$ are distinct prime ideals conjugate under the Galois group, and without loss of generality $\mathfrak{p}_1 = \mathfrak{p}$. There is a natural isomorphism

$$B_p \to \mathfrak{o}_F/\mathfrak{p}_1 \times \cdots \mathfrak{o}_F/\mathfrak{p}_g, \quad \alpha \bmod p \mapsto (\alpha \bmod \mathfrak{p}_1, \ldots, \alpha \bmod \mathfrak{p}_g). \tag{5.14}$$

Furthermore, A_p is a B_p-algebra that comes with an involution $a \mapsto \overline{a}$ which is just the reduction of complex conjugation $\mathfrak{o}_K \to \mathfrak{o}_K$. The subring B_p is fixed by this involution, and so it makes sense to speak of $A_p|B_p$-skew-Hermitian forms.

Define such a form $\{\cdot,\cdot\}_p$ on Λ_p by

$$\{[x]_p, [y]_p\}_p = \{x, y\} \bmod p \in A_p.$$

It is related to the intersection form $\langle\cdot,\cdot\rangle_p$ by

$$\langle [x]_p, [y]_p\rangle_p = \operatorname{tr}_{A_p|\mathbb{F}_p}\{[x]_p, [y]_p\}_p,$$

and therefore it is nondegenerate: if $\{[x]_p, [y]_p\}_p = 0$ for all $[y]_p$, then by taking traces to $\mathbb{F}_p$ we see that $\langle [x]_p, [y]_p\rangle = 0$ for all $[y]_p$, and using Proposition 5.32 we see that $[x]_p = 0$. But this means that the homomorphism

$$\Lambda_p \to \operatorname{Hom}_{A_p}(\Lambda_p, A_p), \quad [y]_p \mapsto \{\cdot, [y]_p\}_p \tag{5.15}$$

is injective; but since target and domain are finite groups of the same cardinality by Lemma 5.34, (5.15) has to be bijective, hence the pairing $\{\cdot,\cdot\}_p$ has to be perfect.

To relate this to our form $\{\cdot,\cdot\}_{\mathfrak{p}}$, note that we may define analogous forms $\{\cdot,\cdot\}_{\mathfrak{p}_i}$ having values in $\mathfrak{o}_F/\mathfrak{p}_i$, for each $1 \le i \le g$. Then under the isomorphism (5.14) $\{[x]_p, [y]_p\}_p$ corresponds to

$$(\{[x]_{\mathfrak{p}_1}, [y]_{\mathfrak{p}_1}\}_{\mathfrak{p}_1}, \ldots, \{[x]_{\mathfrak{p}_1}, [y]_{\mathfrak{p}_1}\}_{\mathfrak{p}_1}).$$

Assume that $a \in \Lambda_{\mathfrak{p}_1}$ satisfies $\{a, [y]_{\mathfrak{p}_1}\}_{\mathfrak{p}_1} = 0$ for every $y \in \Lambda$. Then we may find some $x \in \Lambda$ with $[x]_{\mathfrak{p}_1} = a$ and $[x]_{\mathfrak{p}_i} = 0$ for all $i > 1$, and then

$$\{[x]_p, [y]_p\}_p = 0 \text{ for all } y \in \Lambda$$

since it corresponds to

$$(\{a, [y]_{\mathfrak{p}_1}\}_{\mathfrak{p}_1}, \{0, [y]_{\mathfrak{p}_2}\}_{\mathfrak{p}_2}, \cdots) = (0, 0, \cdots)$$

under the isomorphism (5.14). Since we already know that $\{\cdot,\cdot\}_p$ is nondegenerate, $[x]_p = 0$ and therefore $a = [x]_{\mathfrak{p}_1} = 0$. We conclude as for $\{\cdot,\cdot\}_p$ that the pairing actually has to be perfect. □

5.4.4 Prym level structures

Recall that $\operatorname{Prym} C = \Omega^1(C)^{\perp}_{\mathrm{old}}/\Lambda$; therefore we have a canonical identification of finite groups

$$(\operatorname{Prym} C)[\mathfrak{p}] = \mathfrak{p}^{-1}\Lambda/\Lambda \subseteq \frac{1}{p}\Lambda/\Lambda.$$

The latter group is mapped isomorphically to $\Lambda_p = \Lambda/p\Lambda$ by the multiplication-by-p map m_p. Hence we obtain an embedding of finite groups

$$m_p\colon (\operatorname{Prym} C)[\mathfrak{p}] \to \Lambda_p. \tag{5.16}$$

Lemma 5.36. *Under the isomorphism*

$$\Lambda_p \to \Lambda_{\mathfrak{p}_1} \times \cdots \times \Lambda_{\mathfrak{p}_g}, \quad x \bmod p \mapsto (x \bmod \mathfrak{p}_1, \ldots, x \bmod \mathfrak{p}_g)$$

the image of (5.16) is precisely $\Lambda_{\mathfrak{p}_1} \times 0 \times \cdots \times 0$.

Proof. Recall that $p\mathfrak{o}_F = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ with distinct prime ideals $\mathfrak{p}_i$, and with $\mathfrak{p}_1 = \mathfrak{p}$. Then $p\mathfrak{p}^{-1}\Lambda = \mathfrak{p}_2 \cdots \mathfrak{p}_m\Lambda$, which clearly reduces to zero in $\Lambda_{\mathfrak{p}_i}$ with $i > 1$, so the image is contained in the product. The other inclusion then follows by comparing cardinalities. □

Proposition 5.37. *The multiplication-by-p map induces an isomorphism of* $\mathbb{K}_{\mathfrak{p}}$*-modules*

$$(\operatorname{Prym} C)[\mathfrak{p}] \to \Lambda_{\mathfrak{p}}.$$

It relates the Weil pairing on the domain with the skew-Hermitian form $\{\cdot,\cdot\}_{\mathfrak{p}}$ *on the target by*

$$e_p(x,y) = \exp\left(\frac{2\pi\sqrt{-1}}{p} \operatorname{tr}_{\mathbb{K}_{\mathfrak{p}}|\mathbb{F}_p}\{px,py\}_{\mathfrak{p}}\right).$$

Proof. Only the statements about the pairings remains to be shown. The Weil pairing is related to the intersection pairing by

$$e_p(x,y) = \exp\left(\frac{2\pi\sqrt{-1}}{p}\langle px,py\rangle_p\right),$$

see [65, p. 237]. Therefore we need to show that

$$\langle px,py\rangle_p = \operatorname{tr}_{\mathbb{K}_{\mathfrak{p}}|\mathbb{F}_p}\{px,py\}_{\mathfrak{p}}. \tag{5.17}$$

But this follows from applying Lemma 5.38 below to $\alpha = \operatorname{tr}_{K|F}(\{px,py\}) = \{px,py\} - \{py,px\}$, since the left hand side of (5.17) is equal to $\langle px,py\rangle_p = (\operatorname{tr}_{F|\mathbb{Q}}\alpha) \bmod p$ and the right hand side to $\operatorname{tr}_{\mathbb{F}_{\mathfrak{p}}|\mathbb{F}_p}(\alpha \bmod \mathfrak{p})$. □

Lemma 5.38. *Let* $\alpha \in \mathfrak{p}_2 \cdots \mathfrak{p}_g = \mathfrak{p}^{-1}p\mathfrak{o}_K \subset \mathfrak{o}_F$. *Then*

$$\left(\operatorname{tr}_{F|\mathbb{Q}}\alpha\right) \bmod p = \operatorname{tr}_{\mathbb{F}_{\mathfrak{p}}|\mathbb{F}}(\alpha \bmod \mathfrak{p}).$$

Proof. Let F^D be the decomposition field of p in F. This is a subextension $\mathbb{Q} \subseteq F^D \subseteq F$ with $[F^D : \mathbb{Q}] = g$, and p decomposes in this field as $p\mathfrak{o}_{F^D} = \mathfrak{p}_1^D \cdots \mathfrak{p}_g^D$, where $\mathfrak{o}_{F^D}/\mathfrak{p}_i^D = \mathbb{F}_p$ and $\mathfrak{p}_i^D\mathfrak{o}_F = \mathfrak{p}_i$.

Then for any automorphism $\sigma \in \operatorname{Gal}(F|F^D)$ still $\sigma(\alpha) \in \mathfrak{p}_2 \cdots \mathfrak{p}_g$; therefore $\operatorname{tr}_{F|F^D}\alpha \in \mathfrak{p}_2^D \cdots \mathfrak{p}_g^D$. Next, if $\sigma \in \operatorname{Gal}(F^D|\mathbb{Q})$ is different from the identity we obtain $\sigma(\operatorname{tr}_{F|F^D}\alpha) \in \mathfrak{p}_1^D$, so

$$\operatorname{tr}_{F|\mathbb{Q}}(\alpha) = \operatorname{tr}_{F^D|\mathbb{Q}}(\operatorname{tr}_{F|F^D}\alpha) \equiv \operatorname{tr}_{F|F^D}\alpha \bmod \mathfrak{p}_1^D.$$

Since the natural homomorphism $\operatorname{Gal}(F|F^D) \to \operatorname{Gal}(\mathbb{F}|\mathbb{F}_p)$ is an isomorphism, the desired equation follows. □

This comparison suggests to define Prym level structures in a way that only uses the Weil pairing and the $\mathbb{K}_{\mathfrak{p}}$-module structure.

Definition 5.39. *An* orthonormal basis *of* $(\operatorname{Prym} C)[\mathfrak{p}]$ *is a basis* (x_1, x_2) *of that group as a* $\mathbb{K}_{\mathfrak{p}}$*-module, satisfying:*

(i) $e_p(\Phi(\alpha)x_1, \Phi(\beta)x_1) = e_p(\Phi(\alpha)x_2, \Phi(\beta)x_2)$ *for all* $\alpha, \beta \in \mathbb{K}_{\mathfrak{p}}$*;*

(ii) $e_p(\Phi(\alpha)x_1, \Phi(\beta)x_2) = 0$ *for all* $\alpha, \beta \in \mathbb{K}_{\mathfrak{p}}$*.*

Two orthonormal bases (x_1, x_2) *and* (y_1, y_2) *are declared equivalent if there exists* $\alpha \in \mathbb{K}_{\mathfrak{p}}^{\times}$ *with* $\Phi(\alpha)x_1 = y_1$ *and* $\Phi(\alpha)x_2 = y_2$*. An equivalence class of orthonomal bases is called a* Prym level $\mathfrak{p}$ structure *on* C*.*

From Lemma 5.28 and Proposition 5.37 we conclude:

Proposition 5.40. *The multiplication-by-p map provides a bijection between Prym level* $\mathfrak{p}$ *structures and projectivised orthonormal bases of* $\Lambda_{\mathfrak{p}}$*. Every simple hypergeometric curve of degree* $2r$ *admits a Prym level* $\mathfrak{p}$ *structure.* □

5.4.5 The braid group action on the Prym lattice

Recall the family of simple hypergeometric curves $\mathscr{C} \to \operatorname{Conf}_3(\mathbb{C})$ from section 5.3.2. Just like on cohomology the braid group $\mathrm{Br}_3 = \pi_1(\operatorname{Conf}_3(\mathbb{C}), S_0)$ acts on the homology group $H_1(C_{S_0}, \mathbb{Z})$ by monodromy; this action commutes with the automorphisms $\varphi(\xi)_*$ and therefore preserves the Prym lattice $\Lambda \subset H_1(C, \mathbb{Z})$ and its $\mathfrak{o}_K$-module structure. It also preserves the intersection form, the Poincaré duality isomorphism and the various $\varphi(\xi)^*$-eigenspaces in cohomology, so that we obtain a representation

$$\varrho_\Lambda \colon \mathrm{Br}_3 \to \mathrm{U}(\Lambda) = \mathrm{U}(\Lambda, \{\cdot, \cdot\}).$$

The following is straightforward:

Lemma 5.41. *The map* $f_\varepsilon \colon \Lambda \to H^1(C)_\varepsilon$ *is* Br_3*-equivariant for the representations* ϱ_Λ *on the domain and* ϱ_ε *on the target.* □

This lemma allows us to translate results about ϱ_ε to ϱ_Λ:

Proposition 5.42. *The determinant of* $\varrho_\Lambda \colon \mathrm{Br}_3 \to \mathrm{U}(\Lambda)$ *is given by* $\kappa \circ \varepsilon^{-1} \circ \delta^r \colon \mathrm{Br}_3 \to \mu_r$*. In particular* $\varrho_\Lambda(\mathrm{Br}_3^r) \subseteq \mathrm{SU}(\Lambda)$*.*

We write $\Theta = \varrho_\Lambda(\mathrm{Br}_3^r) \subseteq \mathrm{SU}(\Lambda)$.

Definition 5.43. *Let* $\mathfrak{p}$ *be a prime in* $F = \mathbb{Q}(\zeta_r + \zeta_r^{-1})$ *not dividing* $2r$*. The following groups are called* principal congruence subgroups of level $\mathfrak{p}$*:*

(i) $\mathrm{Br}_3^r(\mathfrak{p})$ *is the kernel of the composition* $\mathrm{Br}_3^r \xrightarrow{\varrho_\Lambda} \mathrm{SU}(\Lambda) \to \mathrm{SU}(\Lambda_{\mathfrak{p}})$*.*

(ii) $\Theta(\mathfrak{p})$ *is the kernel of the map* $\Theta \subseteq \mathrm{SU}(\Lambda) \to \mathrm{SU}(\Lambda_{\mathfrak{p}})$*, i.e. the image of* $\mathrm{Br}_3^r(\mathfrak{p})$ *under* ϱ_Λ*.*

Proposition 5.44. *The image of* $\mathrm{Br}_3^r(\mathfrak{p})$ *under* $\mathrm{P}\varrho_\varepsilon$ *is the congruence subgroup* $\Delta(\varepsilon(\mathfrak{p}))$ *of the triangle group* Δ *as defined in section 5.2.*

Proof. The map $f_\varepsilon \colon \Lambda \to H^1(C)_\varepsilon \simeq \mathbb{C}^{1,1}$ induces an $\varepsilon\kappa$-semilinear embedding of algebras

$$\iota \colon \operatorname{End}_K(\Lambda \otimes \mathbb{Q}) \to \operatorname{End} H^1(C)_\varepsilon$$

sending Θ to $\tilde{\Delta}$; it suffices to show that $\iota(\Theta(\mathfrak{p})) = \tilde{\Delta}(\varepsilon(\mathfrak{p}))$. Now Θ is actually contained in a proper subring of $\operatorname{End}_K(\Lambda \otimes \mathbb{Q})$. Recall that the *adjugate* of a (2×2)-matrix is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\dagger = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

and satisfies $A \cdot A^\dagger = (\det A) \cdot \mathbf{1}$. Since this construction is invariant under conjugation, we obtain for every two-dimensional K-vector space V a well-defined involution of K-algebras $(\cdot)^\dagger\colon \operatorname{End}_K(V) \to \operatorname{End}_K(V)$, in particular for $V = \Lambda \otimes \mathbb{Q}$. The *adjoint* for the skew-Hermitian form $\{\cdot,\cdot\}$ defines another involution of $\operatorname{End}_K(\Lambda \otimes \mathbb{Q})$, this time K-antilinear, denoted by $A \mapsto A^*$. By making a base extension to $\mathbb{C}$ we see that the subring

$$B_\Lambda = \{g \in \operatorname{End}_K(\Lambda \otimes \mathbb{Q}) \mid g^\dagger = g^*\}$$

is a quaternion algebra over F. Since it contains $\mathrm{SU}(\Lambda)$, hence also Θ, and its image under ι therefore contains $\iota(\Theta) = \tilde{\Delta}$, for dimension reasons $\iota(B_\Lambda) = B = F[\tilde{\Delta}]$. Furthermore,

$$\mathscr{O}_\Lambda = B_\Lambda \cap \operatorname{End}_{\mathfrak{o}_K}(\Lambda)$$

is an order in B. We claim that

$$\iota(\mathscr{O}_\Lambda) = \mathscr{O} = \mathfrak{o}_F[\tilde{\Delta}]. \tag{5.18}$$

Since $\Theta \subset \mathscr{O}_\Lambda$ and $\iota(\Theta) = \tilde{\Delta}$, the image $\iota(\mathscr{O}_\Lambda)$ has to be an order in $F[\tilde{\Delta}]$ containing $\tilde{\Delta}$, therefore containing $\mathscr{O} = \mathfrak{o}_F[\tilde{\Delta}]$. But $\mathscr{O}$ is a maximal order by Proposition 5.3, which shows (5.18). Since ι is $\varepsilon\kappa$-linear and κ operates trivially on $\mathfrak{o}_F$, the map

$$\iota\colon \mathscr{O}_\Lambda \to \mathscr{O}$$

is an ε-semilinear isomorphism, so it sends $\Theta(\mathfrak{p})$ to $\tilde{\Delta}(\varepsilon(\mathfrak{p}))$. □

Proposition 5.45. *The composition* $\mathrm{Br}_3^r \to \mathrm{SU}(\Lambda) \to \mathrm{SU}(\Lambda_\mathfrak{p})$ *is surjective.*

Proof. The image of this map is isomorphic to $\tilde{\Delta}/\tilde{\Delta}(\varepsilon(\mathfrak{p})) \simeq \mathrm{SL}(2, \mathbb{F}_\mathfrak{p})$ by Proposition 5.4, hence isomorphic to $\mathrm{SU}(\Lambda_\mathfrak{p})$ by Proposition 5.31. Since this is a finite group, the image has to be actually equal to $\mathrm{SU}(\Lambda_\mathfrak{p})$. □

5.5 Moduli

5.5.1 Moduli spaces of simple hypergeometric curves as sets

To have a uniform treatment of the case with level structures and the case ignoring level structures, we make the following conventions in this section: r is as before, an integer > 6 with $r \equiv \pm 1 \bmod 6$, but $\mathfrak{p}$ is now either a prime in F not dividing $6r$, or the ideal (1).

Denote by $\mathscr{X}(\mathfrak{p})$ the set of isomorphism classes of simple hypergeometric curves $\pi\colon C \to D$ of degree $2r$ with a Prym level $\mathfrak{p}$ structure. Here two such objects are declared equivalent if there exists a commutative square

$$\begin{tikzcd}
C_1 \arrow[r, "F", "\simeq"'] \arrow[d, "\pi_1"'] & C_2 \arrow[d, "\pi_2"] \\
D_1 \arrow[r, "\simeq", "f"'] & C_2
\end{tikzcd}$$

with $f(\infty_1) = \infty_2$ and such that the isomorphism $(\operatorname{Prym} C_1)[\mathfrak{p}] \to (\operatorname{Prym} C_2)[\mathfrak{p}]$ relates the two Prym level structures. We fix some three-element subset $S_0 \subset \mathbb{C}$ and consider the corresponding simple hypergeometric curve $C_0 \to \mathbb{P}^1$. The group $\mathrm{PSU}(\Lambda_{\mathfrak{p}})$ acts on the set of Prym level $\mathfrak{p}$ structures on C_0 without fixed points and with one orbit for $\mathfrak{p} = (1)$, two orbits for prime $\mathfrak{p}$ by Lemma 5.30. Assume that $\mathfrak{p}$ is prime and choose representatives $[x_1 : y_1]$ and $[x_2 : y_2]$ for each orbit. Then we can endow the universal family of simple hypergeometric curves over $\mathscr{T}_{\mathrm{Conf}}$, which is a topologically trivial surface bundle, once with the unique continuous extension of $[x_1 : y_1]$, once with that of $[x_2 : y_2]$ and thus obtain a family of simple hypergeometric curves with Prym level $\mathfrak{p}$ structures on $\mathscr{T}_{\mathrm{Conf}} \times \{1, 2\}$. This defines a classifying map

$$c\colon \mathscr{T}_{\mathrm{Conf}} \times \{1, 2\} \to \mathscr{X}(\mathfrak{p}).$$

A similar construction leads to a classifying map

$$c\colon \mathscr{T}_{\mathrm{Conf}} \to \mathscr{X}(1).$$

Furthermore, let L^+ be the period domain with the braid group acting on it via a $(2, 3, r)$-triangle group Δ. Let $E_r \subset L^+$ be the set of all fixed points of elliptic elements of order r in Δ, so that the image of the period map is precisely $\mathbb{D}^* = L^+ \smallsetminus E_r$.

Theorem 5.46. *There exists a unique bijection f making the diagram*

$$\begin{tikzcd}
\mathscr{T}_{\mathrm{Conf}} \arrow[r, "c"] \arrow[dr, "p"'] & \mathscr{X}(1) \arrow[d, dashed, "f"'] \\
& \Delta\backslash\mathbb{D}^*
\end{tikzcd}$$

commutative. If $\mathfrak{p}$ is a prime in F not dividing $6r$, there exists a unique bijection f making the diagram

$$\begin{tikzcd}
\mathscr{T}_{\mathrm{Conf}} \times \{1, 2\} \arrow[r, "c"] \arrow[dr, "p\times\mathrm{id}"'] & \mathscr{X}(\mathfrak{p}) \arrow[d, dashed, "f"'] \\
& \Delta(\varepsilon(\mathfrak{p}))\backslash\mathbb{D}^* \times \{1, 2\}
\end{tikzcd}$$

commutative.

Proof. We only discuss the case of prime $\mathfrak{p}$, the case $\mathfrak{p} = (1)$ being similar but simpler.

For uniqueness to hold, both $p \times \{1,2\}$ and c should be surjective. The surjectivity of $p \times \{1,2\}$ follows from Proposition 5.18; we now show that c is surjective. So take an element of $\mathscr{X}(\mathfrak{p})$, represented by a simple hypergeometric curve which is, without loss of generality, of the form $\pi \colon C \to \mathbb{P}^1$ with $C \colon w^{2r} = f(z)$, where $f(z) = \prod_{s \in S}(z - s)$ with $S \in \mathrm{Conf}_3(\mathbb{C})$, and a Prym level structure $[x_C : y_C]$ on C. Choose an orientation-preserving compactly supported homeomorphism $m \colon (\mathbb{C}, S_0) \to (\mathbb{C}, S)$. This can be lifted to a homeomorphism $M \colon C_0 \to C$ making the diagram

$$\begin{tikzcd} C_0 \arrow[r, "M"] \arrow[d, "\pi_0"'] & C \arrow[d, "\pi"] \\ \mathbb{P}^1 \arrow[r, "m"'] & \mathbb{P}^1 \end{tikzcd}$$

commutative. Now the map M is not unique; there are precisely $2r$ possible choices, and they form one orbit under the action of the Deck group of π, which is the image of μ_{2r} under φ. Luckily, each element of the Deck group operates on Λ, therefore also on $\Lambda_{\mathfrak{p}}$ and hence on $(\mathrm{Prym}\, C)[\mathfrak{p}]$, by scalar multiplication. In particular it fixes all Prym level structures, and hence the pullback of $[x_C : y_C]$ along M is a well-defined Prym level structure on $C_0 \to \mathbb{P}^1$ which only depends on m. It is in the $\mathrm{PSU}(\Lambda_{\mathfrak{p}})$-orbit of $[x_n : y_n]$ for precisely one $n \in \{1, 2\}$. Assume $[x_C : y_C] = g[x_n : y_n]$ for some $g \in \mathrm{PSU}(\Lambda_{\mathfrak{p}})$, and let $b \in \mathrm{Br}_3^r$ be a preimage of g (which exists by Proposition 5.45). Postcomposing the marking of C with b^{-1} gives an element $(t, n) \in \mathscr{T}_{\mathrm{Conf}} \times \{1, 2\}$ which is mapped to the class of $(C, [x_C : y_C])$ in $\mathscr{X}(\mathfrak{p})$ by c.

This shows surjectivity; we now turn to the existence of f. Pick two points $(t_i, n_i) \in \mathscr{T}_{\mathrm{Conf}} \times \{1, 2\}$ for $i = 1, 2$. As before, assume that t_i is represented by a three-element subset $S_i \subset \mathbb{C}$ and an isotopy class of compactly supported homeomorphisms $m_i \colon (\mathbb{C}, S_0) \to (\mathbb{C}, S_i)$ (choose a representative in each case). Let $f_i(z) = \prod_{s \in S_i}(z - s_i)$, so that the fibre of the universal family over t_i is the smooth projective curve $\pi_i \colon C_i \to \mathbb{P}^1$ with affine equation $w^{2r} = f_i(z)$. The homeomorphism m_i can be lifted to a homeomorphism $M_i \colon C_0 \to C_i$ such that the diagram

$$\begin{tikzcd} C_0 \arrow[r, "M_i"] \arrow[d, "\pi_0"'] & C_i \arrow[d, "\pi_i"] \\ \mathbb{P}^1 \arrow[r, "m_i"'] & \mathbb{P}^1 \end{tikzcd}$$

becomes commutative. Again, M_i is unique up to postcomposition with the Deck group of π_i, and the pushforward of the Prym level structure $[x_{n_i} \colon y_{n_i}]$ along M_i does not actually depend on M_i, only on m_i.

We shall show the following are equivalent:

(i) $c(t_1, n_1) = c(t_2, n_2)$;

(ii) $p(t_1, n_1)$ and $p(t_2, n_2)$ lie in the same $\Delta(\varepsilon(\mathfrak{p}))$-orbit.

First assume (i). This means that there exists an affine-linear map $f \colon (\mathbb{C}, S_1) \to (\mathbb{C}, S_2)$ such that any lift $F \colon C_1 \to C_2$ sends the projectivised orthonormal basis

$M_{1,*}[x_{n_1} : y_{n_1}]$ of $(\operatorname{Prym} C_1)[\mathfrak{p}]$ to $M_{2,*}[x_{n_2} : y_{n_2}]$ of $(\operatorname{Prym} C_2)[\mathfrak{p}]$. So setting $B = M_2^{-1} \circ F \circ M_1$ and $b = m_2^{-1} \circ f \circ m_1$ we obtain a commutative diagram

$$\begin{tikzcd}
C_0 \arrow[rrr, dashed, "B", "\approx"'] \arrow[dr] \arrow[ddd, "M_1"', "\approx"] & & & C_0 \arrow[dl] \arrow[ddd, "\approx"', "M_2"] \\
& \mathbb{P}^1 \arrow[r, dashed, "b", "\approx"'] \arrow[d, "m_1"', "\approx"] & \mathbb{P}^1 \arrow[d, "\approx"', "m_2"] & \\
& \mathbb{P}^1 \arrow[r, "\simeq", "f"'] & \mathbb{P}^1 & \\
C_1 \arrow[ur] \arrow[rrr, "\simeq", "F"'] & & & C_2 \arrow[ul]
\end{tikzcd}$$

where the diagonal arrows are cyclic ramified coverings, the maps marked by $\simeq$ are isomorphisms of Riemann surfaces and the maps marked by $\approx$ are orientation-preserving homeomorphisms. The homeomorphism b defines an element of the braid group Br_3, by abuse of notation also called b. This braid satisfies $b(t_2) = t_1$, and we shall show that $\mathrm{P}\varrho_\varepsilon(b) \in \Delta(\mathfrak{p})$, which implies (ii).

The lift B of b differs from the distinguished lift defined in section 5.3.2 at most by an element of the deck transformation group of $\pi_0 \colon C_0 \to \mathbb{P}^1$, so its action on $(\operatorname{Prym} C)[\mathfrak{p}]$ is that of b up to possibly a scalar endomorphism in $\mathbb{K}^\times$. In particular it acts via $\varrho_\Lambda(b)$ on the set of Prym level $\mathfrak{p}$ structures on C_0. Therefore the image of $\varrho_\Lambda(b)$ in $\mathrm{PU}(\Lambda_\mathfrak{p})$ sends $[x_{n_1} : y_{n_1}]$ to $[x_{n_2} : y_{n_2}]$.

By Lemma 5.12, there exists $n \in \mathbb{Z}$ and $b' \in \mathrm{Br}_3^r$ with $b = c^n b'$. Since $\varrho_\Lambda(c)$ is scalar multiplication by some root of unity, $\varrho_\Lambda(b')$ must also operate by some scalar multiplication on $\Lambda_\mathfrak{p}$. But since the determinant of $\varrho_\Lambda(b')$ is one, this scalar has to be ± 1. There exists some $m \in \mathbb{Z}$ such that $\varrho_\Lambda(c^m) = \varrho_\Lambda(b')$ (if the right hand side is the identity, take $m = 0$; if it is minus the identity, take $m = r$). Writing $b'' = c^{-m} b'$ we obtain a decomposition $b = c^{m+n} b''$ with $b'' \in \mathrm{Br}_3^r$ operating trivially on $\Lambda_\mathfrak{p}$, that is, $\varrho_\Lambda(b'') \in \Theta(\mathfrak{p})$. But the image of c under $\mathrm{P}\varrho_\varepsilon$ is trivial, therefore $\mathrm{P}\varrho_\varepsilon(b) = \mathrm{P}\varrho_\varepsilon(b'') \in \Delta(\varepsilon(\mathfrak{p}))$, which shows (ii).

Now assume (ii). Then clearly $n_1 = n_2$ which we denote by $n \in \{1, 2\}$. Choose some $b \in \mathrm{Br}_3^r(\mathfrak{p})$ with

$$\mathrm{P}\varrho_\varepsilon(b) p(t_1) = p(t_2), \tag{5.19}$$

and represent t_i by a configuration $S_i \subset \mathbb{C}$ and a compactly supported homeomorphism $m_i \colon (\mathbb{C}, S_0) \to (\mathbb{C}, S_i)$. Again let $C_i \colon w^{2r} = f_i(z)$ with $f_i(z) = \prod_{s \in S_i}(z - s_i)$ be the corresponding simple hypergeometric curves. Note that (5.19) can also be written as

$$p(b^* t_1) = p(t_2),$$

where b^* is represented by S_1 with the marking $m_1 \circ b^{-1} \colon (\mathbb{C}, S_0) \to (\mathbb{C}, S_1)$. Then by Lemma 5.19 there exists an affine-linear automorphism $\ell \colon \mathbb{C} \to \mathbb{C}$ with $\ell(S_1) = S_2$ such that $\mathrm{P}\varrho_\varepsilon(m_2^{-1} \ell m_1 b^{-1})$ is trivial; therefore also $\mathrm{P}\varrho_\Lambda(m_2^{-1} \ell m_1 b^{-1})$ is trivial. But since $\mathrm{P}\varrho_\Lambda(b) \in \Theta(\mathfrak{p})$, this implies

$$\mathrm{P}\varrho_\Lambda(m_2^{-1} \ell m_1) = \mathrm{P}\varrho_\Lambda(b) \in \Theta(\mathfrak{p}),$$

so

$$m_2^{-1}\ell m_1 \in \mathrm{Br}_3^r(\mathfrak{p}).$$

This means that any lift of this braid to C_0 fixes the Prym level structure $[x_n : y_n]$ on C_0. Now the affine-linear map ℓ can be lifted to an automorphism

$$\begin{tikzcd} C_1 \arrow[r, "L"] \arrow[d, "\pi_1"] & C_2 \arrow[d, "\pi_2"'] \\ \mathbb{P}^1 \arrow[r, "\ell"'] & \mathbb{P}^1 \end{tikzcd}$$

defined by $L(z, w) = (\ell(z), w)$, and a glance at the commutative diagram (5.9) tells us that L sends the Prym level structure $M_{1,*}[x_n : y_n]$ on C_1 to the Prym level structure $M_{2,*}[x_n : y_n]$ on C_2. That is, $c(t_1, n) = c(t_2, n)$, and we have deduced (i).

Finally, the surjectivity of c and $p \times \mathrm{id}$ together with the equivalence (i) $\Leftrightarrow$ (ii) shows the theorem. □

5.5.2 Algebraic structures on moduli spaces

While it is certainly possible to construct a model of $\Delta(\mathfrak{p})\backslash\mathbb{D}$ over a sufficiently small ring using the methods of [24], we prefer a more direct approach in accordance with the function-theoretic focus of this chapter.

Set $X(\mathfrak{p}) = \Delta(\mathfrak{p})\backslash\mathbb{D}$ and $Y(\mathfrak{p}) = \Delta(\mathfrak{p})\backslash(\mathbb{D} \setminus E)$, where E is the set of all fixed points of elliptic elements in Δ. That is, E is the set of all vertices in the tesselation $\mathscr{B}$, cf. section 5.2. By Riemann's correspondence between Riemann surfaces and algebraic curves, $X(\mathfrak{p})$ has a unique structure as a smooth projective algebraic curve over $\mathbb{C}$, and $Y(\mathfrak{p})$ is a Zariski open subset of $X(\mathfrak{p})$. We shall show that $Y(\varepsilon(\mathfrak{p})) \times \{1, 2\}$ classifies *rigid simple hypergeometric curves* with Prym level $\mathfrak{p}$ structure. Here a simple hypergeometric curve $\pi\colon C \to D$ with distinguished point $\infty \in D$ and ramification locus $S \subset D$ is called *rigid* if the only automorphism g of D with $g(\infty) = \infty$ and $g(S) = S$ is the identity.

Proposition 5.47. *Let $\mathfrak{p}$ be a prime of F not dividing $6r$. Then there exists an algebraic family $\mathscr{C}_1 \to \mathbb{P}^1 \times Y(1)$ of simple hypergeometric curves, and an algebraic family $\mathscr{C}_{\mathfrak{p}} \to \mathbb{P}^1 \times Y(\varepsilon(\mathfrak{p})) \times \{1, 2\}$ of simple hypergeometric curves with a continuous family of Prym level $\mathfrak{p}$ structures, satisfying the following properties:*

(i) The classifying map $Y(\varepsilon(\mathfrak{p})) \times \{1, 2\} \to \mathscr{X}(\mathfrak{p})$ is the restriction of the inverse of f in Theorem 5.46 to $Y(\varepsilon(\mathfrak{p})) \times \{1, 2\}$.

(ii) Every rigid simple hypergeometric curve of degree $2r$ with a Prym level $\mathfrak{p}$ structure is isomorphic to precisely one fibre of $\mathscr{C}_{\mathfrak{p}}$.

(iii) If Z is a smooth algebraic curve and $\mathscr{C}_Z \to Z$ is an algebraic family of rigid simple hypergeometric curves of degree $2r$ with Prym level $\mathfrak{p}$ structures, then the classifying map $Z \to Y(\varepsilon(\mathfrak{p})) \times \{1, 2\}$, which is well-defined by (ii), is a regular map of algebraic curves.

Analogous statements hold for $\mathfrak{p} = 1$ with the factors $\{1, 2\}$ removed.

Note that these families cannot be universal in the categorical sense since there are families of hypergeometric curves which are isotrivial but not trivial.

Proof. Recall that $Y(1) \simeq \mathbb{C} \smallsetminus \{0,1\}$; we define a family $\mathscr{C}_1 \to \mathbb{C} \smallsetminus \{0,1\} \times \mathbb{P}^1$ whose fibre over $J \in \mathbb{C} \smallsetminus \{0,1\}$ is the simple hypergeometric curve with equation

$$w^{2r} = z^3 - \frac{27}{4}\frac{J}{J-1}(z+1);$$

this works just as for elliptic curves (see [45, III, Proposition 3.7]), since the j-invariant really is an invariant for configurations in $\mathbb{C}$. The same computation as for elliptic curves proves (i) – (iii) for $\mathfrak{p} = (1)$.

For general $\mathfrak{p}$, the forgetful map $Y(\varepsilon(\mathfrak{p})) \times \{1,2\} \to Y(1)$ is an étale covering, and hence the pullback of $\mathscr{C}_1$ along this projection defines an algebraic family of rigid simple hypergeometric curves $\mathscr{C}_{\mathfrak{p}} \to \mathbb{P}^1 \times Y(\varepsilon(\mathfrak{p})) \times \{1,2\}$; the bijection $Y(\varepsilon(\mathfrak{p})) \times \{1,2\} \to \mathscr{X}^{\mathrm{rigid}}(\mathfrak{p})$ defined by the inverse of f defines a continuous family of Prym level $\mathfrak{p}$ structures on the fibres of this family such that (i) is satisfied. Then (ii) follows from (i), and it remains to show (iii).

So let $\mathscr{C}_Z \to Z$ be a family as in (iii). Since the identification of $Y(\varepsilon(\mathfrak{p})) \times \{1,2\}$ with $\mathscr{X}^{\mathrm{rigid}}(\mathfrak{p})$ is constructed by Teichmüller theory, the classifying map $f\colon Z \to Y(\varepsilon(\mathfrak{p}))$ has to be holomorphic, and its composition with the projection $Y(\varepsilon(\mathfrak{p})) \times \{1,2\} \to Y(1)$ is regular. So either it is a constant map, and then f is constant, too, or it has finite fibres. But then f has finite fibres, too. The curve Z can be embedded into a smooth projective curve $\overline{Z}$ by adding a finite number of points. Around each of these points, f has an inessential singularity by Picard's Great Theorem, so f can be extended to a holomorphic map $\overline{f}\colon \overline{Z} \to X(\varepsilon(\mathfrak{p}))$. But since these are projective curves, $\overline{f}$ has to be regular. This proves (iii). □

The idea used in the last paragraph of the proof is a toy version of Borel's theorem on holomorphic maps to locally symmetric varieties, see the discussion following [60, Theorem 3.14].

5.5.3 Belyĭ maps and Galois actions

Now we study $X(\mathfrak{p})$ as an algebraic curve.

Proposition 5.48. *Let σ be a field automorphism of $\mathbb{C}$. Then $\sigma(X(\mathfrak{p})) \simeq X(\sigma(\mathfrak{p}))$.*

Proof. We use the moduli interpretation of these spaces.

Let $\pi\colon C \to D$ be a simple hypergeometric curve with Prym level $\mathfrak{p}$ structure $[x : y]$. We can then interpret $[\sigma(x) : \sigma(y)]$ as a Prym level $\sigma(\mathfrak{p})$ structure on $\sigma(C) \to \sigma(D)$.

To show this we observe that by its characterisation discussed after (5.4), $\varphi_C\colon \mu_{2r} \to \operatorname{Aut}_D C$ is natural under field automorphisms:

$$\sigma(\varphi_C(\xi)(P)) = \varphi_{\sigma(C)}(\sigma(\xi))(\sigma(P)) \text{ for all } \xi \in \mu_{2r} \text{ and } P \in C.$$

This implies an analogous formula for Φ, hence $\sigma((\operatorname{Prym} C)[\mathfrak{p}]) = (\operatorname{Prym} \sigma(C))[\sigma(\mathfrak{p})]$. Since Prym level structures were defined using only the Weil pairing (which can be constructed in a purely algebraic way) and the map Φ, see Definition 5.39, they are sent to Prym level structures by σ.

Consider the family $\mathscr{C}_\mathfrak{p} \to Y(\varepsilon(\mathfrak{p})) \times \{1, 2\}$; applying the field automorphism σ then yields a family of rigid simple hypergeometric curves with Prym level $\sigma(\mathfrak{p})$ structures

$$\sigma(\mathscr{C}_\mathfrak{p}) \to \sigma(Y(\varepsilon(\mathfrak{p}))) \times \{1, 2\}.$$

In this family every such curve appears exactly once up to automorphism, so by Proposition 5.47.(ii) and (iii) its classifying map

$$f\colon \sigma(Y(\varepsilon(\mathfrak{p}))) \times \{1, 2\} \to Y(\varepsilon\sigma(\mathfrak{p})) \times \{1, 2\}$$

is a regular map between (disconnected) smooth complex algebraic curves, and it is bijective. Hence it is a biholomorphism; by an argument similar to that in the last paragraph of the proof of Proposition 5.47, it must actually be biregular and extend to an isomorphism of (disconnected) smooth projective curves, which on each connected component therefore gives an isomorphism

$$\sigma(X(\varepsilon(\mathfrak{p}))) \simeq X(\varepsilon\sigma(\mathfrak{p})).$$

Replacing $\mathfrak{p}$ by $\varepsilon^{-1}(\mathfrak{p})$ we find that

$$\sigma(X(\mathfrak{p})) \simeq X(\varepsilon\sigma\varepsilon^{-1}(\mathfrak{p})). \tag{5.20}$$

But $\operatorname{Aut} \mathbb{C}$ operates on the prime ideals of F via its quotient $\operatorname{Gal}(F|\mathbb{Q})$, which is abelian; hence the right hand side of (5.20) is equal to $\sigma(X(\mathfrak{p}))$. □

Proposition 5.49. *Let $\mathfrak{p}$ be a prime of F that does not divide $6r$. Then $\Delta(\mathfrak{p})$ is torsion-free.*

Proof. We show that $\tilde{\Delta}(\mathfrak{p})$ is torsion-free: every torsion element in $\tilde{\Delta}$ is conjugate to a power of the generating rotations, hence it has eigenvalues $\xi^{\pm 1}$, where ξ is a $12r$-th root of unity which we can assume to be $\neq 1$. Then ξ is not congruent to 1 modulo $\mathfrak{p}$, for if it were, then $\xi - 1 \in \mathfrak{p}$. But either the order of ξ is a prime power ℓ^n, then ℓ is a divisor of $6r$ and the only primes possibly dividing $\xi - 1$ are those dividing $6r$. Or the order of ξ is composite, then $\xi - 1$ is an algebraic unit by [98, Proposition 2.8]. □

Proposition 5.50. *The only automorphisms of the curve $X(\mathfrak{p})$ are the Deck transformations of the map $X(\mathfrak{p}) \to X(1)$.*

Proof. By Proposition 5.49 the automorphism group of $X(\mathfrak{p})$ is the image of the normaliser

$$N = \{g \in \mathrm{PSU}(1, 1) \mid g\Delta(\mathfrak{p})g^{-1} = \Delta(\mathfrak{p})\}.$$

This normaliser is a discrete subgroup of $\mathrm{PSU}(1, 1)$ containing Δ, therefore it is equal to Δ by Proposition 5.2.(ii). □

Recall that the *moduli field* of an algebraic curve X over $\mathbb{C}$ is the fixed field of $\{\sigma \in \operatorname{Aut}\mathbb{C} \mid \sigma(X) \simeq X\}$. The moduli field is the intersection of all possible fields of definition for X, but it need not be a field of definition itself.

To determine the moduli field of $X(\mathfrak{p})$, note first that it is clearly contained in $F = \mathbb{Q}(\zeta_r + \zeta_r^{-1})$ by Proposition 5.48. The Galois group $\operatorname{Gal}(F|\mathbb{Q})$ can be identified with $(\mathbb{Z}/r\mathbb{Z})^\times/\{\pm 1\}$.

Proposition 5.51. *The moduli field, as well as the unique minimal field of definition, of $X(\mathfrak{p})$ is the fixed field of the subgroup $G \subseteq \operatorname{Gal}(F|\mathbb{Q})$ generated by $\pm p \bmod r$, where p is the rational prime above $\mathfrak{p}$. This is equal to the decomposition field of p in F.*

Proof. We first show that if $X(\mathfrak{p}) \simeq X(\mathfrak{q})$ (with the same r), then $\mathfrak{p} = \mathfrak{q}$:

Using Proposition 5.49 we first conclude that $\Delta(\mathfrak{p})$ and $\Delta(\mathfrak{q})$ are conjugate as subgroups of $\mathrm{PSU}(1,1)$; assume that $g\Delta(\mathfrak{p})g^{-1} = \Delta(\mathfrak{q})$. But as in the proof of Proposition 5.50, Δ is the normaliser of both $\Delta(\mathfrak{p})$ and $\Delta(\mathfrak{q})$ in $\mathrm{PSU}(1,1)$, so $g\Delta g^{-1} = \Delta$; but that means that g is in the normaliser of Δ, which is Δ itself. Hence $\Delta(\mathfrak{p})$ and $\Delta(\mathfrak{q})$ are conjugate in Δ. Since they are normal, they must be equal, hence $\mathfrak{p} = \mathfrak{q}$.

This observation together with Proposition 5.48 implies that the moduli field of $X(\mathfrak{p})$ is the fixed field of the group of $\sigma \in \operatorname{Gal}(F|\mathbb{Q})$ with $\sigma(\mathfrak{p}) = \mathfrak{p}$. This is the subgroup generated by the Frobenius at p, which by class field theory corresponds to $\pm p \bmod r$ under the identification $\operatorname{Gal}(F|\mathbb{Q}) = (\mathbb{Z}/r\mathbb{Z})^\times/\{\pm 1\}$.

Finally, a curve which admits a Galois covering to $\mathbb{P}^1$ can always be defined over its moduli field, see [46, Theorem 2.2]. □

There is a unique isomorphism $J\colon X(1) \to \mathbb{P}^1$ sending the elliptic points of order 2, 3 and r to 1, 0 and ∞, respectively — from the proof of Proposition 5.47 we see that this is the map sending a simple hypergeometric curve $w^{2r} = f(z)$ to the J-invariant of the elliptic curve $w^2 = f(z)$, i.e. the j-invariant divided by 1728. The composition

$$\beta\colon X(\mathfrak{p}) \to X(1) \xrightarrow{J} \mathbb{P}^1 \tag{5.21}$$

is a *Belyĭ map*, i.e. a ramified covering which is unramified outside $0, 1, \infty \in \mathbb{P}^1$. Such maps are famously in one-to-one correspondence with *dessins d'enfants*, i.e. finite bipartite graphs embedded in an oriented closed surface such that the component consists only of simply connected regions; the Galois action on dessins d'enfants defined by this correspondence has been much studied, see [68]. We simply note:

Proposition 5.52. *For each prime $\mathfrak{p}$ in F not dividing $6r$ let $D(\mathfrak{p})$ be the dessin corresponding to (5.21). Then the absolute Galois group $\operatorname{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ acts on these dessins by $\sigma(D(\mathfrak{p})) = D(\sigma(\mathfrak{p}))$, and the moduli field of $D(\mathfrak{p})$, as well as the unique minimal field of definition of the Belyĭ map (5.21), is the decomposition field in F of the rational prime p above $\mathfrak{p}$.*

Proof. Again by [46, Theorem 2.2] the minimal field of definition for β is its moduli field. □

5.5.4 Hurwitz curves

The curves $X(\mathfrak{p})$ for $r = 7$ have received much attention in different disguises since they are *Hurwitz curves*. A smooth projective curve of genus g has a finite automorphism group whose order is at most $84(g-1)$ by a famous theorem of Hurwitz, see [38]. A curve X that realises this bound is called a Hurwitz curve, and this is equivalent to $X \simeq \Gamma\backslash\mathbb{D}$ for some finite index normal subgroup Γ of the $(2,3,7)$ triangle group Δ. The automorphism groups Δ/Γ thus occurring are called *Hurwitz groups*, so Hurwitz groups are precisely the finite quotients of Δ. See the surveys [17, 53, 18] for more information.

In [52] Macbeath proved by purely group-theoretical methods that $\mathrm{PSL}(2,q) = \mathrm{PSL}(2,\mathbb{F}_q)$ is a Hurwitz group if and only if $q = 7$, q is a rational prime with $q \equiv \pm 1 \bmod 7$, or $q = p^2$ for a rational prime $p \equiv \pm 2, \pm 3 \bmod 7$; he also showed that the number of normal subgroups Γ with $\Delta/\Gamma \simeq \mathrm{PSL}(2,q)$ is one in the first and third cases, and three in the second case. In other words, $\mathrm{PSL}(2,q)$ is a Hurwitz group if and only if there is a prime ideal of $F = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ of norm q, and it occurs as often as there are primes of norm q. In [25] it was shown that these are all obtained as quotients by congruence subgroups $\Delta(\mathfrak{p})$. The earlier article [89] describes the Galois action on these Hurwitz curves without using the link to congruence subgroups; its author arrives at the description by group theory and elementary calculations. Our Proposition 5.48 specialised to $r = 7$ thus reconciles [25] with [89].

5.5.5 Shimura varieties

The fact that $\tilde{\Delta}$ generates an order in a quaternion algebra over a totally real number field opens up a connection with Shimura varieties, known under the name *modular embeddings*. We hint how this fits into our discussion, without giving a detailed account.

Let $\mathfrak{p}$ be a prime in F not dividing $6r$, and let C be a simple hypergeometric curve of degree $2r$ equipped with some Prym level $\mathfrak{p}$ structure. Let $V(\mathfrak{p})$ be the connected Shimura variety which classifies polarised abelian varieties A with generalised complex multiplication $\mathfrak{o}_K \to \operatorname{End} A$ and a projectivised orthonormal basis of $A[\varepsilon^{-1}(\mathfrak{p})]$, all of the same type as $\operatorname{Prym} C$.

Proposition 5.53. *The dimension of $V(\mathfrak{p})$ is equal to the number of integers $0 < k < \frac{r}{6}$ which are coprime to r.*

Associating a simple hypergeometric curve with its Prym variety defines a closed embedding of algebraic varieties $X(\mathfrak{p}) \to \overline{V(\mathfrak{p})}$, where the latter denotes the Baily–Borel compactification. If $r = 7$ or 11 this map is an isomorphism, otherwise its image is a proper subvariety not contained in any proper Shimura subvariety.

Sketch of proof. By Shimura's theory of modular varieties for quaternion algebras [87] the variety $V(\mathfrak{p})$ can be constructed as the quotient of $\mathbb{H}^m$ by $\mathcal{O}^1(\varepsilon^{-1}(\mathfrak{p}))$. Here $\mathcal{O} = \mathfrak{o}_F[\tilde{\Delta}]$, m is the number of embeddings $\sigma\colon F \to \mathbb{R}$ with

$$\mathcal{O} \otimes_{\mathfrak{o}_F,\sigma} \mathbb{R} \simeq \mathrm{M}(2,\mathbb{R}), \tag{5.22}$$

and $\mathscr{O}^1(\varepsilon^{-1}(\mathfrak{p}))$ acts on $\mathbb{H}^m$ component-wise by Möbius transformations via the different embeddings (5.22). The dimension m can then be determined using Proposition 5.3; it is one precisely for $r = 7$ or 11. There exists a *modular embedding*, i.e. a holomorphic map $\mathbb{D} \to \mathbb{H}^m$ which is equivariant for the embedding of groups $\tilde{\Delta} \hookrightarrow \mathscr{O}^1$ and whose first coordinate defines a biholomorphic map $\mathbb{D} \to \mathbb{H}$; it is constructed in [14]. In our perspective, the first coordinate of the modular embedding uses the period map for the eigenspace $H^1(C)_\varepsilon$, and similar period maps for other eigenspaces appear analogously in the other coordinates.

That the image of $X(\mathfrak{p}) \to \overline{V(\mathfrak{p})}$ is not contained in a proper Shimura subvariety follows from the fact that $\tilde{\Delta}$ is adèlically, therefore also Zariski, dense in $\mathscr{O}^1$, see [12, Theorem C]. □

Bibliography

[1] *Revêtements étales et groupe fondamental*, Springer-Verlag, Berlin, 1971, Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud, Lecture Notes in Mathematics, Vol. 224. MR 0354651 (50 #7129)

[2] Milton Abramowitz and Irene A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, National Bureau of Standards Applied Mathematics Series, vol. 55, For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 1964. MR 0167642 (29 #4914)

[3] Ian Agol, *mathoverflow answer to: Can Galois conjugates of lattices in* $\mathrm{SL}(2,\mathbb{R})$ *be discrete?*, 2014, http://mathoverflow.net/questions/155798/can-galois-conjugates-of-lattices-in-sl2-r-be-discrete.

[4] Michael P. Anderson, *Exactness properties of profinite completion functors*, Topology **13** (1974), 229–239. MR 0354882 (50 #7359)

[5] Natália Archinard, *Hypergeometric abelian varieties*, Canad. J. Math. **55** (2003), no. 5, 897–932. MR 2005278 (2004i:11056)

[6] Reinhold Baer, *Sylow theorems for infinite groups*, Duke Math. J. **6** (1940), 598–614. MR 0002122 (2,2a)

[7] G. V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 2, 267–276, 479. MR 534593 (80f:12008)

[8] Joan S. Birman, *Braids, links, and mapping class groups*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1974, Annals of Mathematics Studies, No. 82. MR 0375281 (51 #11477)

[9] Irene I. Bouw and Martin Möller, *Teichmüller curves, triangle groups, and Lyapunov exponents*, Ann. of Math. (2) **172** (2010), no. 1, 139–185. MR 2680418 (2012b:32020)

[10] B. H. Bowditch, *Markoff triples and quasi-Fuchsian groups*, Proc. London Math. Soc. (3) **77** (1998), no. 3, 697–736. MR 1643429 (99f:57014)

[11] Martin R. Bridson, Marston D. E. Conder, and Alan Reid, *Determining Fuchsian groups by their finite quotients*, 2014, preprint, arXiv:1401.3645v1.

[12] Pete L. Clark and John Voight, *Algebraic curves uniformized by congruence subgroups of triangle groups*, 2011, preprint, https://math.dartmouth.edu/ jvoight/research.html.

[13] A. H. Clifford, *Representations induced in an invariant subgroup*, Ann. of Math. (2) **38** (1937), no. 3, 533–550. MR 1503352

[14] Paula Cohen and Jürgen Wolfart, *Modular embeddings for some nonarithmetic Fuchsian groups*, Acta Arith. **56** (1990), no. 2, 93–110. MR 1075639 (92d:11039)

[15] Paula Beazley Cohen, Claude Itzykson, and Jürgen Wolfart, *Fuchsian triangle groups and Grothendieck dessins. Variations on a theme of Belyi*, Communications in Mathematical Physics **163** (1994), no. 3, 605–627.

[16] Marston Conder, *The genus of compact Riemann surfaces with maximal automorphism group*, J. Algebra **108** (1987), no. 1, 204–247. MR 887205 (88f:20063)

[17] ______, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 359–370. MR 1041434 (91d:20032)

[18] ______, *An update on Hurwitz groups*, Groups Complex. Cryptol. **2** (2010), no. 1, 35–49. MR 2672551 (2011f:30081)

[19] Marston D. E. Conder, Gareth A. Jones, Manfred Streit, and Jürgen Wolfart, *Galois actions on regular dessins of small genera*, Rev. Mat. Iberoam. **29** (2013), no. 1, 163–181. MR 3010126

[20] Marc Culler and Peter B. Shalen, *Varieties of group representations and splittings of* 3*-manifolds*, Ann. of Math. (2) **117** (1983), no. 1, 109–146. MR 683804 (84k:57005)

[21] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962. MR 0144979 (26 #2519)

[22] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, Galois groups over **Q** (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 79–297. MR 1012168 (90m:14016)

[23] P. Deligne and G. D. Mostow, *Monodromy of hypergeometric functions and nonlattice integral monodromy*, Inst. Hautes Études Sci. Publ. Math. (1986), no. 63, 5–89. MR 849651 (88a:22023a)

[24] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. (1969), no. 36, 75–109. MR 0262240 (41 #6850)

[25] Amir Džambić, *Macbeath's infinite series of Hurwitz groups*, Arithmetic and geometry around hypergeometric functions, Progr. Math., vol. 260, Birkhäuser, Basel, 2007, pp. 101–108. MR 2306150 (2008b:20062)

[26] Noam D. Elkies, *The Klein quartic in number theory*, The eightfold way, Math. Sci. Res. Inst. Publ., vol. 35, Cambridge Univ. Press, Cambridge, 1999, pp. 51–101. MR 1722413 (2001a:11103)

[27] Leonhard Euler, *Institutionum calculi integralis volumen secundum*, Academia Scientiarum Imperialis Petropolitinae, St. Petersburg, 1769, reprinted as Leonhardi Euleri Opera Omnia, ser. 1, vol. 12, Teubner, Leipzig/Berlin, 1914.

[28] M. Fried, *Fields of definition of function fields and Hurwitz families—groups as Galois groups*, Comm. Algebra **5** (1977), no. 1, 17–82. MR 0453746 (56 #12006)

[29] Slavyana Geninska, *Examples of infinite covolume subgroups of* $\mathrm{PSL}(2,\mathbb{R})^r$ *with big limit sets*, Math. Z. **272** (2012), no. 1-2, 389–404. MR 2968231

[30] Gabino González-Diez and Andrei Jaikin-Zapirain, *The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces*, preprint, http://www.uam.es/personal_pdi/ciencias/gabino/Jule03.pdf, 2013.

[31] Alexander Grothendieck, *Brief an G. Faltings*, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, With an English translation on pp. 285–293, pp. 49–58. MR 1483108 (99c:14023)

[32] Alexandre Grothendieck, *Esquisse d'un programme*, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, With an English translation on pp. 243–283, pp. 5–48. MR 1483107 (99c:14034)

[33] Eugene Gutkin and Chris Judge, *The geometry and arithmetic of translation surfaces with applications to polygonal billiards*, Math. Res. Lett. **3** (1996), no. 3, 391–403. MR 1397686 (97c:58116)

[34] Frank Herrlich and Gabriela Schmithüsen, *Dessins d'enfants and origami curves*, Handbook of Teichmüller theory. Vol. II, IRMA Lect. Math. Theor. Phys., vol. 13, Eur. Math. Soc., Zürich, 2009, pp. 767–809. MR 2516744 (2010f:14036)

[35] Ruben A. Hidalgo, *A computational note about Fricke–Macbeath's curve*, preprint, arXiv:1203.6314, 2012.

[36] Yuichiro Hoshi and Shinichi Mochizuki, *On the combinatorial anabelian geometry of nodally nondegenerate outer representations*, Hiroshima Math. J. **41** (2011), no. 3, 275–342. MR 2895284

[37] Pascal Hubert and Thomas A. Schmidt, *An introduction to Veech surfaces*, Handbook of dynamical systems. Vol. 1B, Elsevier B. V., Amsterdam, 2006, pp. 501–526. MR 2186246 (2006i:37099)

[38] A. Hurwitz, *Ueber algebraische Gebilde mit eindeutigen Transformationen in sich*, Math. Ann. **41** (1892), no. 3, 403–442. MR 1510753

[39] Moshe Jarden, *Normal automorphisms of free profinite groups*, J. Algebra **62** (1980), no. 1, 118–123. MR 561120 (81b:20024)

[40] Moshe Jarden and Jürgen Ritter, *Normal automorphisms of absolute Galois groups of* $\mathfrak{p}$*-adic fields*, Duke Math. J. **47** (1980), no. 1, 47–56. MR 563366 (81j:12010)

[41] Svetlana Katok, *Fuchsian groups*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 1992. MR 1177168 (93d:20088)

[42] Reinhardt Kiehl and Rainer Weissauer, *Weil conjectures, perverse sheaves and* ℓ*-adic Fourier transform*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 42, Springer-Verlag, Berlin, 2001. MR 1855066 (2002k:14026)

[43] S. L. Kleiman, *Algebraic cycles and the Weil conjectures*, Dix esposés sur la cohomologie des schémas, North-Holland, Amsterdam, 1968, pp. 359–386. MR 0292838 (45 #1920)

[44] Felix Klein, *Vorlesungen über die hypergeometrische Funktion*, Grundlehren der Mathematischen Wissenschaften, vol. XXXIX, Springer-Verlag, Berlin, 1933.

[45] Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992. MR 1193029 (93j:11032)

[46] Bernhard Köck, *Belyi's theorem revisited*, Beiträge Algebra Geom. **45** (2004), no. 1, 253–265. MR 2070647 (2005j:14036)

[47] Keiichi Komatsu, *On adèle rings of arithmetically equivalent fields*, Acta Arith. **43** (1984), no. 2, 93–95. MR 736723 (85e:11095)

[48] Michael Larsen, *How often is* $84(g-1)$ *achieved?*, Israel J. Math. **126** (2001), 1–16. MR 1882031 (2002m:30056)

[49] Lieven Le Bruyn, *The best rejected proposal ever*, 2007, blog entry, www.neverendingbooks.org/the-best-rejected-proposal-ever.

[50] Pierre Lochak, *On arithmetic curves in the moduli spaces of curves*, Journal of the Institute of Mathematics of Jussieu **4** (2005), 443–508.

[51] Saunders Mac Lane, *Homology*, Die Grundlehren der mathematischen Wissenschaften, Bd. 114, Academic Press, Inc., Publishers, New York; Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963. MR 0156879 (28 #122)

[52] A. M. Macbeath, *Generators of the linear fractional groups*, Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), Amer. Math. Soc., Providence, R.I., 1969, pp. 14–32. MR 0262379 (41 #6987)

[53] A. Murray Macbeath, *Hurwitz groups and surfaces*, The eightfold way, Math. Sci. Res. Inst. Publ., vol. 35, Cambridge Univ. Press, Cambridge, 1999, pp. 103–113. MR 1722414 (2001c:14002)

[54] Colin Maclachlan and Alan W. Reid, *The arithmetic of hyperbolic 3-manifolds*, Graduate Texts in Mathematics, vol. 219, Springer-Verlag, New York, 2003. MR 1937957 (2004i:57021)

[55] Wilhelm Magnus, *Noneuclidean tesselations and their groups*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1974, Pure and Applied Mathematics, Vol. 61. MR 0352287 (50 #4774)

[56] Gunter Malle, *Multi-parameter polynomials with given Galois group*, J. Symbolic Comput. **30** (2000), no. 6, 717–731, Algorithmic methods in Galois theory. MR 1800034 (2002a:12007)

[57] C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler, *Congruence properties of Zariski-dense subgroups. I*, Proc. London Math. Soc. (3) **48** (1984), no. 3, 514–532. MR 735226 (85d:20040)

[58] Curtis T. McMullen, *Billiards and Teichmüller curves on Hilbert modular surfaces*, J. Amer. Math. Soc. **16** (2003), no. 4, 857–885 (electronic). MR 1992827 (2004f:32015)

[59] ———, *Braid groups and Hodge theory*, Math. Ann. **355** (2013), no. 3, 893–946. MR 3020148

[60] J. S. Milne, *Introduction to Shimura varieties*, Harmonic analysis, the trace formula, and Shimura varieties, Clay Math. Proc., vol. 4, Amer. Math. Soc., Providence, RI, 2005, pp. 265–378. MR 2192012 (2006m:11087)

[61] Shinichi Mochizuki, *The local pro-p anabelian geometry of curves*, Invent. Math. **138** (1999), no. 2, 319–423. MR 1720187 (2000j:14037)

[62] Martin Möller, *Variations of Hodge structures of a Teichmüller curve*, J. Amer. Math. Soc. **19** (2006), no. 2, 327–344. MR 2188128 (2007b:32026)

[63] G. D. Mostow, *Quasi-conformal mappings in n-space and the rigidity of hyperbolic space forms*, Inst. Hautes Études Sci. Publ. Math. (1968), no. 34, 53–104. MR 0236383 (38 #4679)

[64] ———, *Braids, hypergeometric functions, and lattices*, Bull. Amer. Math. Soc. (N.S.) **16** (1987), no. 2, 225–246. MR 876959 (88e:22017)

[65] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970. MR 0282985 (44 #219)

[66] Zeev Nehari, *Conformal mapping*, McGraw-Hill Book Co., Inc., New York, Toronto, London, 1952. MR 0045823 (13,640h)

[67] Madhav V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Invent. Math. **88** (1987), no. 2, 257–275. MR 880952 (88d:20068)

[68] Joseph Oesterlé, *Dessins d'enfants*, Astérisque (2003), no. 290, Exp. No. 907, ix, 285–305, Séminaire Bourbaki. Vol. 2001/2002. MR 2074061 (2006c:14031)

[69] Robert Perlis, *On the equation $\zeta_K(s) = \zeta_{K'}(s)$*, J. Number Theory **9** (1977), no. 3, 342–360. MR 0447188 (56 #5503)

[70] Emile Picard, *Sur des fonctions de deux variables indépendantes analogues aux fonctions modulaires*, Acta Math. **2** (1883), no. 1, 114–135. MR 1554595

[71] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen. MR 1278263 (95b:11039)

[72] Gopal Prasad, *Strong rigidity of* $\mathbf{Q}$*-rank* 1 *lattices*, Invent. Math. **21** (1973), 255–286. MR 0385005 (52 #5875)

[73] Michel Raynaud, *Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 286, 129–147. MR 1608794

[74] Mohamed Saïdi, *On complete families of curves with a given fundamental group in positive characteristic*, Manuscripta Math. **118** (2005), no. 4, 425–441. MR 2190105 (2006i:14025)

[75] Jan-Christoph Schlage-Puchta and Gabriela Weitze-Schmithüsen, *Finite translation surfaces with maximal number of translations*, preprint, arXiv:1311.7446v1, 2013.

[76] Paul Schmutz Schaller and Jürgen Wolfart, *Semi-arithmetic Fuchsian groups and modular embeddings*, J. London Math. Soc. (2) **61** (2000), no. 1, 13–24. MR 1745404 (2001a:11071)

[77] Theodor Schneider, *Zur Theorie der Abelschen Funktionen und Integrale*, J. Reine Angew. Math. **183** (1941), 110–128. MR 0006170 (3,266b)

[78] Leila Schneps, *The Grothendieck–Teichmüller group* $\widehat{\mathrm{GT}}$*: a survey*, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, pp. 183–203. MR 1483118 (99a:14043)

[79] H.A. Schwarz, *Ueber diejenigen Fälle, in welchen die Gaussische hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt*, J. Reine Angew. Math. **75** (1873), 292–335.

[80] Atle Selberg, *On discontinuous groups in higher-dimensional symmetric spaces*, Contributions to function theory (internat. Colloq. Function Theory, Bombay, 1960), Tata Institute of Fundamental Research, Bombay, 1960, pp. 147–164. MR 0130324 (24 #A188)

[81] Mika Seppälä and Tuomas Sorvali, *Traces of commutators of Möbius transformations*, Math. Scand. **68** (1991), no. 1, 53–58. MR 1124819 (92k:20093)

[82] Jean-Pierre Serre, *Rigidité du foncteur de Jacobi d'échelon* $n \geq 3$, Séminaire Henri Cartan 1960/61, Appendice à l'Exposé 17, Secrétariat mathématique, Paris 1961.

[83] ———, *Cours d'arithmétique*, Collection SUP: "Le Mathématicien", vol. 2, Presses Universitaires de France, Paris, 1970. MR 0255476 (41 #138)

[84] G. B. Shabat and V. A. Voevodsky, *Drawing curves over number fields*, The Grothendieck Festschrift, Vol. III, Progr. Math., vol. 88, Birkhäuser Boston, Boston, MA, 1990, pp. 199–227. MR 1106916 (92f:11083)

[85] Hironori Shiga, Yoshio Suzuki, and Jürgen Wolfart, *Arithmetic properties of Schwarz maps*, Kyushu J. Math. **63** (2009), no. 1, 167–190. MR 2522930 (2010e:33021)

[86] Hironori Shiga and Jürgen Wolfart, *Algebraic values of Schwarz triangle functions*, Arithmetic and geometry around hypergeometric functions, Progr. Math., vol. 260, Birkhäuser, Basel, 2007, pp. 287–312. MR 2306157 (2008c:14059)

[87] Goro Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85** (1967), 58–159. MR 0204426 (34 #4268)

[88] David Singerman, *Finitely maximal Fuchsian groups*, J. London Math. Soc. (2) **6** (1972), 29–38. MR 0322165 (48 #529)

[89] Manfred Streit, *Field of definition and Galois orbits for the Macbeath-Hurwitz curves*, Arch. Math. (Basel) **74** (2000), no. 5, 342–349. MR 1753011 (2001e:14028)

[90] Kisao Takeuchi, *A characterization of arithmetic Fuchsian groups*, J. Math. Soc. Japan **27** (1975), no. 4, 600–612. MR 0398991 (53 #2842)

[91] ______, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), no. 1, 91–106. MR 0429744 (55 #2754)

[92] ______, *Arithmetic Fuchsian groups with signature* $(1; e)$, J. Math. Soc. Japan **35** (1983), no. 3, 381–407. MR 702765 (84h:10031)

[93] Akio Tamagawa, *The Grothendieck conjecture for affine curves*, Compositio Math. **109** (1997), no. 2, 135–194. MR 1478817 (99a:14035)

[94] Kôji Uchida, *Isomorphisms of Galois groups of solvably closed Galois extensions*, Tôhoku Math. J. (2) **31** (1979), no. 3, 359–362. MR 547650 (81a:12010)

[95] Ravi Vakil and Kirsten Wickelgren, *Universal covering spaces and fundamental groups in algebraic geometry as schemes*, J. Théor. Nombres Bordeaux **23** (2011), no. 2, 489–526. MR 2817942 (2012h:14049)

[96] W. A. Veech, *Teichmüller curves in moduli space, Eisenstein series and an application to triangular billiards*, Invent. Math. **97** (1989), no. 3, 553–583. MR 1005006 (91h:58083a)

[97] T. N. Venkataramana, *Monodromy of cyclic coverings of the projective line*, Invent. Math. **197** (2014), no. 1, 1–45. MR 3219513

[98] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575 (97h:11130)

[99] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR 1269324 (95f:18001)

[100] Robert A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009. MR 2562037 (2011e:20018)

[101] Jürgen Wolfart, *Werte hypergeometrischer Funktionen*, Invent. Math. **92** (1988), no. 1, 187–216. MR 931211 (89g:11063)

[102] Masaaki Yoshida, *Hypergeometric functions, my love. Modular interpretations of configuration spaces*, Aspects of Mathematics, E32, Friedr. Vieweg & Sohn, Braunschweig, 1997. MR 1453580 (98k:33024)

Zusammenfassung

In dieser Arbeit beweisen wir verschiedene Ergebnisse über algebraische Kurven und Fuchssche Gruppen, die in verschiedener Hinsicht, sei es für die definierenden algebraischen Gleichungen, die uniformisierenden Fuchsschen Gruppen oder die Perioden, Verhalten arithmetischer Natur aufweisen.

Das erste Kapitel ist eine kurz gehaltene allgemeine Einführung in dieses Thema mit besonderem Augenmerk auf die Theorie der Kinderzeichnungen. Verbindungen zu arithmetischen Gruppen sowie Fuchsschen Dreiecksgruppen werden erwähnt, dann folgt eine Zusammenfassung der wichtigsten Resultate dieser Arbeit.

Im zweiten Kapitel beweisen wir einen Satz, der als Vergleich verschiedener Galois-Aktionen auf kombinatorischen Objekten, sogenannten Origamis, aufgefasst werden kann. Origamis ähneln Kinderzeichnungen, und die Galois-Aktionen auf diesen Objekten wird aus der étalen Fundamentalgruppe einer punktierten elliptischen Kurve über einem Zahlkörper gewonnen. Diese Kurve spielt die gleiche Rolle für Origamis wie $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ für Kinderzeichnungen. Die Galois-Aktion auf Kinderzeichungen kann durch einen injektiven Homomorphismus

$$\varrho_{01\infty}\colon \operatorname{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \hookrightarrow \operatorname{Out} \hat{F}_2$$

kodiert werden; hierbei ist $\hat{F}_2$ die proendliche Vervollständigung einer freien Gruppe auf zwei Erzeugern, und Out bezeichnet die äußere Automorphismengruppe. Dieser Homomorphismus ist vermittels eines Isomorphismus zwischen $\hat{F}_2$ und der étalen Fundamentalgruppe von $\mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0, 1, \infty\}$ definiert. Analog erhalten wir für jede elliptische Kurve E über einem Zahlkörper $K \subset \mathbb{C}$ und jede Basis $\mathfrak{B}$ von $H_1(E(\mathbb{C}), \mathbb{Z})$ einen injektiven Gruppenhomomorphismus

$$\varrho_{E,\mathfrak{B}}\colon \operatorname{Gal}(\overline{\mathbb{Q}}|K) \hookrightarrow \operatorname{Out} \hat{F}_2.$$

Das Hauptresultat im zweiten Kapitel besagt, dass (unter der milden wie notwendigen Bedingung, dass die Basen positiv orientiert für die jeweilige Schnittpaarung sind) $\varrho_{E_1,\mathfrak{B}_1}$ und $\varrho_{E_2,\mathfrak{B}_2}$ das gleiche Bild nur in dem offensichtlichen Fall haben, in welchem die zwei Zahlkörper gleich sind und es einen Isomorphismus $E_1 \simeq E_2$ gibt, der $\mathfrak{B}_1$ auf $\mathfrak{B}_2$ abbildet. Weiters ziehen wir einfache Folgerungen für die Kommensurabilitätsklassen in $\hat{F}_2$, insbesondere ist kein Bild eines $\varrho_{E,\mathfrak{B}}$ für eine elliptische Kurve kommensurabel im weiteren Sinne mit dem Bild von $\varrho_{01\infty}$. Diese Aussagen werden aus bekannten tiefliegenden Sätzen von Neukirch, Uchida und Tamagawa im Gebiet der anabelschen Geometrie mithilfe eines elementaren Tricks und dem Satz von Belyĭ hergeleitet.

Im dritten Kapitel zeigen wir, dass die absolute Galoisgruppe treu auf bestimmten vergleichsweise kleinen Klassen von Kinderzeichnungen und Origamis operiert. Das erste Hauptresultat in diesem Kapitel ist die Treue der Galois-Aktion auf normalen Kinderzeichnungen von vorgegebenem Verzweigungstyp; dies wurde im Wesentlichen schon vorher in einem Preprint von González-Diez und Jaikin-Zapirain aus dem Jahr 2013 bewiesen, allerdings nicht explizit ausformuliert. Wir übersetzen ihren recht komplizierten Beweis, der zwischen komplex-analytischen und étalen

Erwägungen hin- und herspringt, vollständig in die Sprache der ℓ-adischen Garben. Auf diesem Wege können wir die expliziten Rechnungen dieses Peprints umgehen und deutlich allgemeiner Folgendes beweisen: Wenn $\mathscr{X}$ ein Deligne–Mumford-Stack über einem Zahlkörper ist, der endlich étale von einer hyperbolischen Kurve überlagert wird, dann operiert $\mathrm{Gal}(\overline{\mathbb{Q}}|K)$ treu auf der Menge der Isomorphieklassen von normalen étalen Überlagerungen von $\mathscr{X}$ durch Kurven. Für $\mathscr{X}$ über $\mathbb{Q}$ mit $\mathscr{X}(\mathbb{C}) = \Delta(p,q,r)\backslash\mathfrak{H}$ (als Orbifold-Quotient) erhalten wir den bereits erwähnten Satz über normale Kinderzeichnungen, und für $(p,q,r) = (2,3,7)$ erhalten wir die Treue der Aktion von $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ auf Hurwitzkurven, d.h. auf glatten projektiven Kurven X, die Hurwitz' Schranke $|\operatorname{Aut} X| \leq 84(g-1)$ erreichen, wobei $g \geq 2$ das Geschlecht von X ist. Ein analoger Satz gilt für Origamis, die eine ähnliche obere Schranke für die Größe der Automorphismengruppe erreichen.

Im vierten Kapitel wechseln wir von der Arithmetik algebraischer Kurven zur Arithmetik Fuchsscher Gruppen. Der Mostowsche Starrheitssatz, der besagt, dass ein Gitter in der Isometriegruppe des n-dimensionalen hyperbolischen Raumes für $n \geq 3$ schon durch seine Isomorphieklasse als abstrakte Gruppe eindeutig bis auf Konjugation bestimmt ist, gilt nicht für $n = 2$. Für semi-arithmetische Gruppen, die eine modulare Einbettung zulassen (insbesondere also für arithmetische Gruppen, Veech-Gruppen mit der Gittereigenschaft und Untergruppen von endlichem Index in hyperbolischen Dreiecksgruppen), erhalten wir eine Starrheitsaussage für die durch Kongruenzuntergruppen definierte Topologie.

Im fünften Kapitel kommen schließlich arithmetische Eigenschaften von Kurven, Perioden und Fuchsschen Gruppen zusammen. Wir geben eine Modulrauminterpretation für Hauptkongruenzgruppen primer Stufe in Dreiecksgruppen $\Delta(2,3,r)$ an, wobei $r \geq 7$ teilerfremd zu 6 sein soll. Der zentrale Satz besagt, dass für ein Primideal $\mathfrak{p}$ im Spurkörper $\mathbb{Q}(\zeta_r)$ der Dreiecksgruppe der Quotient $\Delta(\mathfrak{p})\backslash\mathfrak{H}$ birational zu einem Modulraum ist; dieser parametrisiert einfache hypergeometrische Kurven, d.h. Kurven der Form

$$w^{2r} = f(z),$$

f ein normiertes separables Polynom dritten Grades, zusammen mit einer Niveaustruktur der Stufe $\mathfrak{p}$ für verallgemeinerte komplexe Multiplikation durch$\mathbb{Q}(\zeta_r)$ auf der Prym-Varietät, einem Summanden der Jacobischen. Die Zuordnung der Jacobischen zur Kurve definiert die modulare Einbettung für $\Delta(\mathfrak{p})$. Diese Identifikation der Modulräume wird explizit mit klassischen funktionentheoretischen Mitteln über geeignete Periodenabbildungen hergestellt. Sie liefert einen vergleichsweise elementaren Zugang zur Aktion der absoluten Galoisgruppe auf den Kurven $\Delta(\mathfrak{p})\backslash\mathfrak{H}$, die durch die offensichtliche Permutation der Primideale $\mathfrak{p}$ erfolgt. Wir ziehen weitere Schlüsse über die Modul- und Definitionskörper der $\Delta(\mathfrak{p})\backslash\mathfrak{H}$. Auch diese Sätze haben Anwendungen auf Hurwitzkurven: für $r = 7$ sind die $\Delta(\mathfrak{p})\backslash\mathfrak{H}$ Hurwitzkurven, und unsere Sätze für diesen speziellen Fall beweisen erneut ältere Ergebnisse von Džambić, Macbeath und Streit und stellen sie in Beziehung zueinander.