FINITE QUOTIENTS OF TRIANGLE GROUPS

by

Frankie Chan

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

Department of Mathematics

West Lafayette, Indiana

August 2021

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. David Ben McReynolds, Chair

Department of Mathematics

Dr. Donu Arapura

Department of Mathematics

Dr. Jeremy Miller

Department of Mathematics

Dr. Thomas Sinclair

Department of Mathematics

Approved by:

Dr. Plamen Stefanov

ACKNOWLEDGMENTS

I am extremely grateful for the guidance of my advisor Ben McReynolds. His boundless empathy and enthusiasm is inspiring, and his advice and support was instrumental in my development as a researcher. I only wish I had gotten a hold of him sooner!

I would like to express my appreciation for Ryan Spitler for his immensely patient and insightful discussions. His amazing research ability speaks for itself, but his natural skill to teach and communicate technical ideas makes him a mathematical juggernaut.

Edray Goins is a great mentor. He trained me to be meticulous as a mathematician, and I admire the bank of information he can always draw up on demand.

Joan Ponce merits a special mention for her immense support, emotional and academic, as well as encouragement that made graduate school an incredible time in my life.

My friends have been a constant support system for me, even though they are located all over the map. They have made my time in graduate school an extremely fun and unforgettable experience.

I would also like to thank my family for their support. Their inclination to celebrate my successes throughout my life no matter how big or small drives me to want to win all the time.

TABLE OF CONTENTS

ABSTRACT

Extending an explicit result from Bridson–Conder–Reid [1], this work provides an algorithm for distinguishing finite quotients between cocompact triangle groups Δ and lattices Γ of constant curvature symmetric 2-spaces. Much of our attention will be on when these lattices are Fuchsian groups. We prove that it will suffice to take a finite quotient that is Abelian, dihedral, a subgroup of $\mathrm{PSL}(2, \mathbf{F}_q)$ (for an odd prime power q), or an Abelian extension of one of these 3 groups. For the latter case, we will require and develop an approach for creating group extensions upon a shared finite quotient of Δ and Γ which between them have differing degrees of smoothness. Furthermore, on the order of a finite quotient that distinguishes between Δ and Γ, we are able to establish an effective upperbound that is superexponential depending on the cone orders appearing in each group.

1. INTRODUCTION

1.1 Motivation

Given an object, e.g., a field, group, manifold, variety, etc., one might seek a collection of invariants of the object such that it is essentially determined by this collection. For instance, by the classification of surfaces, a closed, connected, orientable 2–manifold M is uniquely determined up to homeomorphism by its genus.

Unfortunately, such recognition results are rare and require more complicated invariants. As an example, given a number field $K/\mathbf{Q}$, by the Neukirch–Uchida–Pop theorem, K is determined by its collection of finite Galois groups $\mathrm{Gal}(L/K)$. In the same vein, for a finitely generated group Γ, problems of *profinite invariance* (see Section 3.1 for further details) aims in answering the properties of Γ that can be recovered from its collection of finite quotients.

Bridson–Conder–Reid [1] proved that finitely generated Fuchsian groups can be distinguished from lattices of connected Lie groups via their finite quotients (see also [2] [3] regarding the absolute profinite rigidity of certain triangle groups). Furthemore, in Section 8 of [1], an explicit description was detailed for distinguishing finite quotients between two non-isomorphic (cocompact) triangle groups. We are motivated in extending this explicit result, for which we aim to answer the following two main problems.

1. Can we distinguish a triangle group $\Delta := \Delta(r, s, t)$ by a finite quotient Q among the larger class of lattices of constant curvature symmetric 2-spaces $\Gamma := (g; p; \mathbf{m})$?

2. Can we construct an algorithm for distinguishing Δ and Γ via finite quotients? What effective upperbounds can be established on the orders of such quotients?

The first problem is a question of existence (does such a finite quotient Q exist?). Naturally, one wonders if the existence of Q can be proven constructively, which can create more insight towards a proof.

The second problem provides an effective result regarding our finite quotients. Effective upperbounds on the order of Q that differs between Δ and Γ precisely answers how sufficiently large one must pursue quotients before confirming that Δ and Γ must be isomorphic and therefore indistinguishable.

1.2 Main results

Our work will focus on proving the following theorem, which will answer both of the problems listed in the previous section.

Theorem 7.0.2. Let $\Delta := \Delta(r,s,t)$, $\Gamma := (g;p;\mathbf{m})$, and $k := |\mathbf{m}| \geq 0$ such that $\Delta \ncong \Gamma$. Define $N := \max\{\mathrm{lcm}(r,s,t), \mathrm{lcm}(\mathbf{m})\}$. Then there exists a finite group Q having order

$$|Q| \ll N^{(k+3)N^{15}}$$

such that Q is a quotient for one of the groups, but not for the other group.

We are inspired by the methods from [1]; however, generalizing results from triangle groups to lattices is not so straightforward. In addition to producing a list of basic quotients to work with, we also want to qualify certain quotients Q as smooth or non-smooth by considering all of the surjective maps to Q. Another important theorem for this work extends a result from [4], which produces a family of PSL_2 representations that are smooth.

Theorem 5.1.1. Let $q = \ell^d$ be an odd prime power and $\mathbf{m} = (m_1, \ldots, m_k)$, with $k \geq 3$. There exists a subgroup of $\mathrm{PSL}(2,q)$ that is a smooth quotient of $(0;0;\mathbf{m})$ if and only if each of the integers $m_1, \ldots, m_k$ divides one of ℓ, $\frac{q-1}{2}$, or $\frac{q+1}{2}$.

The toughest case that remains is when Δ and Γ share exactly the same basic quotients (there are many examples of this). However, even if Δ and Γ have a common finite quotient G, we have ways of detecting discrepancies in smoothness.

This requires refining the notion on the smoothness of quotients, in the sense that quotients can be considered to be partially smooth or maximally smooth. To this end, for a shared finite quotient G, if G is a smoother quotient for Δ than it is for Γ, then we can construct a group extension G' of G which is a finite quotient of Δ but not for Γ. The following theorem formally states this in terms of first Betti numbers b_1.

Theorem 5.3.1. Let G be a finite group. Fix a surjective homomorphism $\pi\colon (g_1;p_1;\mathbf{m}) \twoheadrightarrow G$ such that $b_1(\ker\pi)$ is maximal among all such surjective maps. If every surjective map

$s\colon (g_2; p_2; \mathbf{n}) \twoheadrightarrow G$ satisfies $b_1(\ker s) < b_1(\ker \pi)$, then there is a finite Abelian extension G' of G such that G' is a finite quotient of $(g_1; p_1; \mathbf{m})$ but not for $(g_2; p_2; \mathbf{n})$.

With these major theorems above utilized in our work, we will be able to show that we can distinguish a triangle group from a lattice by using only dihedral quotients, Abelian quotients, subgroups of $\mathrm{PSL}(2, q)$, or Abelian extensions of the latter three groups. In Section 7.2, we will demonstrate our algorithm with some illustrative examples.

2. SUMMARY

In Chapter 3, we develop the background and conventions necessary for studying the profinite invariants of lattices in constant curvature symmetric 2-spaces. Among the spherical, Euclidean, and hyperbolic lattices, our overwhelming interest will be in the hyperbolic case, for which we can exploit the theory of Fuchsian groups.

The purpose of Chapter 4 is understand Abelian and dihedral quotients. While these quotients are particularly simple to understand, they still are able to provide a wealth of information towards developing rigidity results. These particular concrete quotients represent the least resistant cases towards our proof.

Unfortunately, the quotients studied in Chapter 4 are not enough to prove profinite rigidity. In Chapter 5, we develop a notion of a degree of smoothness of finite quotients, which pays particular attention to the geometry of lattices. Generalizing a result from Macbeath [4], we are able to produce criteria for a lattice to exhibit smooth and non-smooth representations to 2-dimensional projective special linear groups over finite fields.

Chapter 6 provides constructive results for genus 0 lattices. Among the most resistant cases are in distinguishing finite quotients between two triangle groups.

Chapter 7 showcases a full algorithm for distinguishing a triangle group from a lattice via finite quotients. In particular, we are able to produce an effective upperbound on the order of such a distinguishing quotient depending only on the numerical entries of both groups.

3. BACKGROUND AND PRELIMINARIES

We begin with important background on profinite invariants, and then proceed with certain results on finitely generated Fuchsian groups.

3.1 Profinite invariants

For details of much of the profinite results of this section, see [5], and for a further survey on profinite invariants, see [6].

Let Γ be a group, and define the set of *finite quotients* of Γ

$$\mathrm{FQ}(\Gamma) := \{[Q] \mid Q \text{ is a finite quotient of } \Gamma\},$$

where $[Q]$ denotes the isomorphism class of the finite group Q. We can construct a universal object $\widehat{\Gamma}$, called the *profinite completion* of Γ, which is a group that encodes all of the finite quotients $\mathrm{FQ}(\Gamma)$ of Γ.

Definition 1. Let Γ be a group, and let $\mathcal{F}$ be the set of finite index normal subgroups of Γ. Given $M, N \in \mathcal{F}$ such that $M \leq N$, let $\pi_M^N \colon \Gamma/M \twoheadrightarrow \Gamma/N$ be the natural projection map. The *profinite completion* of Γ is the subgroup $\widehat{\Gamma}$ given by

$$\widehat{\Gamma} := \left\{ (x_M)_{M\in\mathcal{F}} \,\middle|\, x_M \in \Gamma/M \text{ and for every } M \leq N,\ \pi_M^N(x_M) = x_N \right\} \leq \prod_{M\in\mathcal{F}} \Gamma/M.$$

A categorical definition of the profinite completion $\widehat{\Gamma}$ as an inverse limit and as a compact topological group is provided in [5]. There is an intimate connection between the profinite completion $\widehat{\Gamma}$ of Γ and the set of finite quotients $\mathrm{FQ}(\Gamma)$. In fact, for finitely generated groups, we can make this connection more precisely.

Theorem 3.1.1. *Let Γ and Λ be finitely generated groups, then $\widehat{\Gamma} \cong \widehat{\Lambda}$ if and only if* $\mathrm{FQ}(\Gamma) = \mathrm{FQ}(\Lambda)$.

We say Γ and Λ are *profinitely equivalent* if $\widehat{\Gamma} \cong \widehat{\Lambda}$. Without the assumption that Γ and Λ are finitely generated, we would require that the isomorphism from above $\widehat{\Gamma} \cong \widehat{\Lambda}$

additionally be a homeomorphism for the theorem to hold. A deep result of Nikolov–Segal [7] implies with this finitely generation assumption that any abstract group isomorphism $\widehat{\Gamma} \cong \widehat{\Lambda}$ is automatically a homeomorphism.

We now assume that the groups Γ and Λ are finitely generated, as is with the case of lattices, see (1). The profinite invariants of a group Γ are the properties that are shared by another profinitely equivalent group Λ, i.e. satisfying $\mathrm{FQ}(\Gamma) = \mathrm{FQ}(\Lambda)$. Notice that if K is the intersection of all of the finite index normal subgroups of Γ, then Γ/K and Γ have exactly the same finite quotients, $\mathrm{FQ}(\Gamma) = \mathrm{FQ}(\Gamma/K)$.

To ensure we are not working with essentially redundant examples such as the one above, we insist on restricting to groups Γ such that its associated subgroup K is the trivial subgroup.

Definition 2. A group Γ is *residually finite*, if the intersection of all of the finite index normal subgroups of Γ is the trivial subgroup $\langle 1_\Gamma \rangle$.

In particular, the group Γ/K constructed above is residually finite. Also, lattices of constant curvature symmetric 2-spaces are residually finite by [8].

The best possible kind of profinite invariant is that of rigidity. We define two different scopes of profinite rigidity.

Definition 3. Let $\mathcal{C}$ denote some subclass of the class of all residually finite groups.

1. A group $\Gamma \in \mathcal{C}$ is *relatively profinitely rigid* in $\mathcal{C}$, if whenever $\widehat{\Gamma} \cong \widehat{\Lambda}$ for some $\Lambda \in \mathcal{C}$, then $\Gamma \cong \Lambda$.

2. A residually finite group Γ is *(absolutely) profinitely rigid*, if Γ is relatively profinitely rigid in the class of all residually finite groups.

One of our main goals will be to prove Theorem 7.0.2 that triangle groups are relatively profinitely rigid in the class of all lattices of constant curvative symmetric 2-spaces.

3.2 Lattices of constant curvature symmetric 2-spaces

Let $\mathbf{X}$ denote any of the following three Riemannian 2-manifolds: the sphere $\mathbf{S}^2$, the Euclidean plane $\mathbf{R}^2$, or the hyperbolic plane $\mathbf{H}^2$. Given a surface $\mathbf{X}$, the isometry group

$\mathrm{Isom}(\mathbf{X})$ is a linear group equipped with an isometric action on the locally compact metric space $\mathbf{X}$. We will concern ourselves with the index two subgroup of orientation-preserving isometries $\mathrm{Isom}^+(\mathbf{X})$. The lattices Γ arising in $\mathrm{Isom}^+(\mathbf{X})$ will be the main objects of our interest.

Definition 4. A *lattice* Γ of $\mathbf{X}$ is a discrete subgroup $\Gamma \leq \mathrm{Isom}^+(\mathbf{X})$ such that Γ has finite co-area, i.e. the quotient $\mathbf{X}/\Gamma$ has finite area.

For a lattice Γ, the metric from $\mathbf{X}$ is inherited by the quotient $\mathcal{O} := \mathbf{X}/\Gamma$ via the natural projection map $\pi_\Gamma \colon \mathbf{X} \twoheadrightarrow \mathbf{X}/\Gamma$ which is a branched covering map. The quotient $\mathcal{O}$ also has the structure of a *2-orbifold*, see [9] and [10] for a treatment on orbifolds. We will often study lattices Γ by understanding its associated orbifold $\mathbf{X}/\Gamma$, and vice versa.

We say that a discrete subgroup $\Gamma \leq \mathrm{Isom}^+(\mathbf{X})$ is *uniform* or *cocompact*, if $\mathbf{X}/\Gamma$ is compact. In this case, Γ automatically has finite co-area.

The most populated examples of lattices Γ as well as the most interesting for this work will be based in the hyperbolic plane $\mathbf{X} = \mathbf{H}^2$. Consequently, Γ is a *Fuchsian group*, and much of the exposition which we will preface about Fuchsian groups can be found in [11].

One objective in this chapter is to provide a combinatorial framework for classifying lattices, via numerical data called the *signature* of the group. We will be able to conclude that every lattice Γ is a finitely presented group whose isomorphism type depends only on the topology and geometry of the orbifold $\mathbf{X}/\Gamma$.

3.2.1 Fuchsian groups

We first describe the action of $\mathrm{PSL}(2,\mathbf{R}) \cong \mathrm{Isom}^+(\mathbf{H}^2)$ on the hyperbolic plane via Möbius transformations. In this case, we will employ the *upper half-plane* model for the hyperbolic plane

$$\mathbf{H}^2 := \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}.$$

For elements $z \in \mathbf{H}^2$ and

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}(2,\mathbf{R}),$$

we define the action

$$Az := \frac{az+b}{cz+d} \in \mathbf{H}^2.$$

This action extends naturally, viewed as a subspace of the Riemann sphere $\mathbf{C} \cup \{\infty\}$, to the boundary $\mathbf{R} \cup \{\infty\}$ of $\mathbf{H}^2$. For a subgroup $\Gamma \leq \mathrm{PSL}(2, \mathbf{R})$, we define the Γ-*orbit* of $z \in \mathbf{H}^2$ by

$$\Gamma z := \{Az \mid A \in \Gamma\}$$

and the Γ-*stabilizer* of z by

$$\mathrm{Stab}_\Gamma(z) := \{A \in \Gamma \mid Az = z\}.$$

In the group $\mathrm{PSL}(2, \mathbf{R})$, the absolute value of the trace function induced by $\mathrm{SL}(2, \mathbf{R})$ is well-defined,

$$|\operatorname{tr}(A)| := |a + d|, \text{ where } A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We say that a non-identity matrix $A \in \mathrm{PSL}(2, \mathbf{R})$ is *elliptic*, *parabolic*, or *hyperbolic*, if $|\operatorname{tr}(A)| < 2$, $|\operatorname{tr}(A)| = 2$, or $|\operatorname{tr}(A)| > 2$, respectively. This can also be characterized in regards to the action of A on $\mathbf{H}^2 \cup (\mathbf{R} \cup \{\infty\})$. Elliptic elements fix only and exactly one point of $\mathbf{H}^2$, parabolic elements fix only and exactly one point of $\mathbf{R} \cup \{\infty\}$, and hyperbolic elements fix only and exactly two points of $\mathbf{R} \cup \{\infty\}$. We say that a subgroup Γ is elliptic, parabolic, or hyperbolic, if all of the non-identity elements in Γ are elliptic, parabolic, or hyperbolic elements, respectively.

A *Fuchsian group* Γ is a discrete subgroup of $\mathrm{PSL}(2, \mathbf{R}) \cong \mathrm{Isom}^+(\mathbf{H}^2)$. In terms of group actions, we will find the following equivalence useful.

Theorem 3.2.1. *A subgroup $\Gamma \leq \mathrm{PSL}(2, \mathbf{R})$ is a Fuchsian group if and only if for every $z \in \mathbf{H}^2$, $\Gamma z \subset \mathbf{H}^2$ is discrete and $\mathrm{Stab}_\Gamma(z)$ is finite.*

Proof. Various characterizations of a Fuchsian group, including the one stated above, can be found in [11]. $\square$

We would like to focus on lattices Γ in $\mathbf{H}^2$, that is, Γ is a Fuchsian group *and* $\mathbf{H}^2/\Gamma$ has finite area. It follows from Theorem 3.2.1 and from [11] that a lattice Γ has up to conjugacy the following: a finite number, say $k \geq 0$, of maximal elliptic cyclic subgroups and a finite number, say $p \geq 0$, of maximal parabolic cyclic subgroups. Sorting by conjugacy classes, each of the k maximal elliptic cyclic subgroups are finite in order and of at least 2, so we can compile a list of those orders into a (possibly empty) unordered tuple $\mathbf{m} := (m_1, \dots, m_k)$, where each $m_i \geq 2$. On the other hand, each of the maximal parabolic cyclic subgroups have infinite order, and on occasion, we will instead treat a conjugacy class of a maximal parabolic cyclic subgroup as an elliptic subgroup of order $m_i = \infty$.

The values p, k, and $\mathbf{m} = (m_1, \dots, m_k)$ coming from the lattice Γ above are witnessed by the quotient orbifold $\mathcal{O} := \mathbf{H}^2/\Gamma$ in a precise way. As a topological space, $\mathcal{O}$ is a *genus g* surface S_g with exactly p points removed, called *punctures* or *cusps*. Additionally, $\mathcal{O}$ has k *cone points* (or *marked points*), one for as many as the size of the tuple $\mathbf{m} = (m_1, \dots, m_k)$, with a *cone order* $m_i \geq 2$ realized at each cone point. All of the points of $\mathcal{O}$ which are not cone points are *smooth points*, locally resembling that of a differentiable 2-manifold. In fact, without any (finite) cone points, $\mathcal{O}$ is globally a differentiable 2-manifold.

We may occasionally view a smooth point of $\mathcal{O}$ as a cone point having cone order 1 and a puncture as a cone point (despite it not even being a point of $\mathcal{O}$) having cone order ∞.

We say the tuple $\mathbf{m} = (m_1, \dots, m_k)$ is *nondegenerate*, if $2 \leq m_i < \infty$, for every i. Unless otherwise mentioned in this work, all tuples will implicitly be considered nondegenerate. As described above, the genus g, number of punctures p, and unordered tuple of cone orders $\mathbf{m} = (m_1, \dots, m_k)$ are all values determined by the lattice Γ.

Definition 5. The *signature* of Γ is the data $(g; p; \mathbf{m})$, where $g \geq 0$ is the genus, $p \geq 0$ is the number of punctures, and $\mathbf{m} = (m_1, \dots, m_k)$, with $k \geq 0$ are the cone orders to each cone point of $\mathcal{O} = \mathbf{H}^2/\Gamma$.

Not every prescription of values $(g; p; \mathbf{m})$ for the signature will admit a Fuchsian group and a hyperbolic orbifold. We will state a theorem of Poincaré, that uses Euler characteristics to quantify which signatures do work.

Definition 6. The *Euler characteristic* of the signature $(g; p; \mathbf{m})$ is the rational number

$$\chi(g; p; \mathbf{m}) := 2 - 2g - p - \sum_{i=0}^{k} \left(1 - \frac{1}{m_i}\right).$$

Without any cone points $\mathbf{m}$, this extends the definition of the Euler characteristic of a 2-manifold of genus g with p punctures. Also, it can be verified that $\chi(g; p; \mathbf{m})$ is well-defined for equivalent degeneracies of the signature $(g; p; \mathbf{m})$.

Theorem 3.2.2. *For $g \geq 0$, $p \geq 0$, and a tuple $\mathbf{m}$, if $\chi(g; p; \mathbf{m}) < 0$, then there exists a Fuchsian group Γ with signature $(g; p; \mathbf{m})$, and the co-area of Γ is finite and equal to $-\chi(g; p; \mathbf{m})$. Otherwise, the 2-orbifold $\mathcal{O}$ corresponding to the signature $(g; p; \mathbf{m})$ is not hyperbolic.*

A proof of this theorem is provided in [11]. Furthermore, it is shown that if Γ has signature $(g; p; \mathbf{m})$, then Γ can be given the following group presentation:

$$\langle a_1, b_1, \ldots, a_g, b_g, y_1, \ldots, y_p, x_1, \ldots, x_k \mid x_i^{m_i} = [a_1, b_1] \ldots [a_g, b_g] y_1 \ldots y_p x_1 \ldots x_k = 1 \rangle. \quad (1)$$

Consequently, lattices in $\mathbf{H}^2$ are finitely presented groups. From now on, we will use context to denote by $(g; p; \mathbf{m})$ either as a signature or as a group with the presentation given by (1). The generators a_i and b_j are hyperbolic, the y_i are parabolic, and the x_i are elliptic (and necessarily torsion). We will refer to these specific generators from (1) as the *canonical generators* for the group $(g; p; \mathbf{m})$.

One collection of groups that we are interested in is the collection of (cocompact) triangle groups.

Definition 7. For integers $r, s, t \geq 1$, the (r, s, t)*-triangle group* is the group

$$\Delta(r, s, t) := (0; 0; r, s, t) \cong \langle x, y, z \mid x^r = y^s = z^t = xyz = 1 \rangle.$$

For this definition, we allow for the possibility for the cone orders to be equal to 1, but not ∞, which would comprise of the non-cocompact triangle groups, see Theorem 3.2.3. We reserve to use the term triangle groups specifically for the cocompact ones. As triangle groups will be a focus for this work, we will find it convenient to denote an operator f (e.g., FQ, χ, or b_1) on a triangle group by $f(r,s,t) := f(\Delta(r,s,t))$.

3.2.2 Signatures

We can extend and redevelop the presentation and signature of the group $\Gamma = (g;p;\mathbf{m})$ given by (1) for the sphere $\mathbf{S}^2$ when $\chi(g;p;\mathbf{m}) > 0$, and for the Euclidean plane $\mathbf{R}^2$ when $\chi(g;p;\mathbf{m}) = 0$. Technically, a few of the non-hyperbolic groups listed below are not finite in co-area, but they can be innocuously subsumed and will be treated as a *lattice*. We now list all of the spherical and Euclidean groups arising as signatures.

Spherical lattices $\chi(g;p;\mathbf{m}) > 0$.

1. $(0;0;m) \cong (0;1;-) \cong \langle 1 \rangle$
2. $(0;0;m,n) \cong \mathrm{C}_{\gcd(m,n)}$
3. $\Delta(1,m,m) \cong (0;1;m) \cong \mathrm{C}_m$
4. $\Delta(2,2,n) \cong \mathrm{D}_{2n}$
5. $\Delta(2,3,3) \cong A_4$
6. $\Delta(2,3,4) \cong S_4$
7. $\Delta(2,3,5) \cong A_5$

Spherical lattices are finite groups and must have genus 0. We denote C_a as the cyclic group of order a and D_{2a} as the dihedral group of order $2a$. We also allowed for the possibility for m and n above to be equal to 1.

Euclidean lattices $\chi(g;p;\mathbf{m}) = 0$.

1. $(0;2;-) \cong \mathbf{Z}$
2. $(1;0;-) \cong \mathbf{Z}^2$
3. $(0;1;2,2) \cong \mathrm{C}_2 * \mathrm{C}_2 \cong \mathrm{D}_\infty \cong \mathbf{Z} \rtimes \mathrm{C}_2$

4. $(0;0;2,2,2,2) \cong \mathbf{Z}^2 \rtimes \mathrm{C}_2$

5. $\Delta(2,3,6) \cong \mathbf{Z}^2 \rtimes \mathrm{C}_6$

6. $\Delta(2,4,4) \cong \mathbf{Z}^2 \rtimes \mathrm{C}_4$

7. $\Delta(3,3,3) \cong \mathbf{Z}^2 \rtimes \mathrm{C}_3$

Euclidean lattices are infinite and solvable groups, and must have genus at most 1. There are only finitely many of them. Each of the groups is isomorphic to some semidirect product of the form $\mathbf{Z}^i \rtimes \mathrm{C}_k$, where $i \in \{1,2\}$ and $k \in \{1,2,3,4,6\}$. We can develop an infinite family of finite quotients $\mathrm{C}_d^i \rtimes \mathrm{C}_k$ by varying $d \geq 1$, each of which are solvable quotients having order kd^i. By taking d large enough, we can distinguish Euclidean lattices from spherical ones. We can use Abelian quotients (see Chapter 4) to be able to distinguish Euclidean lattices from other Euclidean lattices.

Any other signature $(g;p;\mathbf{m})$ provides a hyperbolic group, which are infinite and insolvable groups. We can distinguish a hyperbolic lattice Γ from any non-hyperbolic lattice by finite quotients, for example, [4] shows that Γ has infinitely many finite simple quotients.

We have shown non-hyperbolic lattices are easy cases to deal with, and have fully determined the relative profinite rigidity for these groups. Therefore, in later chapters we will often assume the lattices $(g;p;\mathbf{m})$ are hyperbolic. While for many occasions our results will hold true for even non-hyperbolic lattices, we will only feel the obligation to ensure future results hold for Fuchsian groups.

3.2.3 Punctured and unpunctured lattices

We describe the differences between lattices $(g;p;\mathbf{m})$ for the unpunctured $p=0$ compared to the punctured $p>0$ cases. In Chapter 6, we will dichotomize our analyses in this manner.

Theorem 3.2.3. *The lattice $(g;p;\mathbf{m})$ is cocompact in $\mathbf{X}$ if and only if $p=0$. Furthermore, when $\mathbf{X}=\mathbf{H}^2$, the lattice $(g;p;\mathbf{m})$ is cocompact if and only if it contains no parabolic elements.*

Proof. This is straightforward to verify this for $\mathbf{X}=\mathbf{S}^2$ or $\mathbf{X}=\mathbf{R}^2$, and for $\mathbf{X}=\mathbf{H}^2$, this is Theorems 4.2.1 and 4.2.2 of [11]. $\square$

Whenever $(g;p;\mathbf{m})$ has punctures, it is a virtually free group due to [12], as it can be deduced from the canonical group presentation that

$$(g;p;\mathbf{m}) \cong F_{2g+p-1} * \mathrm{C}_{m_1} * \cdots * \mathrm{C}_{m_k}, \text{ for } p > 0, \tag{2}$$

is a free product of the free group F_r of rank $r := 2g+p-1$ with the cyclic groups C_{m_i} of order m_i.

Since $(g;p;\mathbf{m}) \cong (g-1;p+2;\mathbf{m})$ whenever $p > 0$ (and $g > 0$), we can always find a genus zero representative $(0;p';\mathbf{m})$ isomorphic to $(g;p;\mathbf{m})$ for $p > 0$. It can also be checked that $\chi(g;p;\mathbf{m}) = \chi(g-1;p+2;\mathbf{m})$ in this case. However, as a warning, the associated orbifolds may no longer be isomorphic upon changing the signatures in this way.

If a tuple $\mathbf{n}$ is a permutation of $\mathbf{m}$, then $(g;p;\mathbf{m}) \cong (g;p;\mathbf{n})$, and thus the order of the entries of tuples need no concern. We treat $\mathbf{m} = \mathbf{n}$ as an equality of unordered tuples. Outside of these isomorphisms mentioned above, different hyperbolic signatures produce non-isomorphic lattices.

When $p = 0$, the lattice $(g;0;\mathbf{m})$ is virtually a surface group $\Sigma_{g'} \cong (g';0;-)$. This follows from Selberg's lemma [13], for which we provide an explicit construction in Theorem 5.1.1.

3.2.4 Finite index subgroups of Fuchsian groups

Let $(g;p;\mathbf{m})$ be a Fuchsian group. Every finite index subgroup of $\Gamma = (g;p;\mathbf{m})$ will also be a lattice $\Lambda = (g';p';\mathbf{n})$, and the Riemann–Hurwitz formula will be extremely useful in restricting the possible signatures for Λ.

Riemann–Hurwitz formula. Let Γ be a lattice, and Λ a finite index subgroup of Γ. Then Λ is also a lattice and $\chi(\Lambda) = [\Gamma : \Lambda]\chi(\Gamma)$.

We can use the Riemann–Hurwitz formula to determine the signature of the kernel $K := \ker \pi$ associated to any surjective map $\pi\colon (g;p;\mathbf{m}) \twoheadrightarrow G$ to a finite group G. Suppose that $K := (g';p';\mathbf{n})$, and let $e^{(i)}$ indicate the value of e repeated i times. Take the canonical parabolic and elliptic generators $y_1, \ldots, y_p, x_1, \ldots, x_k \in (g;p;\mathbf{m})$. They map to the elements $\pi(y_1), \dots, \pi(y_p), \pi(x_1), \dots, \pi(x_k) \in G$, and suppose their respective orders in G are $d_1, \dots, d_p, c_1, \dots, c_k$. Denote this tuple of orders by $\mathbf{d} := (d_1, \dots, d_p, c_1, \dots, c_k)$.

By using branched covering space theory, it can be shown that the kernel $K = (g'; p'; \mathbf{n})$ admits the following tuple of (possibly degenerate, if $p > 0$) cone orders:

$$\mathbf{n}' := \left(\infty^{(|G|/d_1)}, \dots, \infty^{(|G|/d_p)}, \frac{m_1}{c_1}^{(|G|/c_1)}, \dots, \frac{m_k}{c_k}^{(|G|/c_k)} \right).$$

With a desire for a nondegenerate $K = (g'; p'; \mathbf{n})$, we apply the data from $\mathbf{n}'$ to let

$$p' := \frac{|G|}{d_1} + \cdots + \frac{|G|}{d_p} \text{ and } \mathbf{n} := \left(\frac{m_1}{c_1}^{(|G|/c_1)}, \dots, \frac{m_k}{c_k}^{(|G|/c_k)} \right).$$

To obtain the value of g', we use the Riemann–Hurwitz formula:

$$\chi(K) = \chi(g'; p'; \mathbf{n}) = |G| \chi(g; p; \mathbf{m}) \tag{3}$$

$$2 - 2g' - \left(\frac{|G|}{d_1} + \cdots + \frac{|G|}{d_p} \right) - \sum_{i=1}^{k} \left(1 - \frac{c_i}{m_i} \right) \frac{|G|}{c_i} = |G| \left(2 - 2g - p - \sum_{j=1}^{k} \left(1 - \frac{1}{m_j} \right) \right) \tag{4}$$

This simplifies to

$$2 - 2g' = |G| \chi(g; 0; \mathbf{d}), \text{ where } \mathbf{d} = (d_1, \dots, d_p, c_1, \dots, c_k). \tag{5}$$

Therefore, for any surjective map $\pi \colon (g; p; \mathbf{m}) \twoheadrightarrow G$ to a finite group G, we are able to determine the signature of the kernel $K = (g'; p'; \mathbf{n})$ that depends only on g, p, $|G|$, and the orders of the images of the canonical parabolic and elliptic generators $\mathbf{d} = (d_1, \dots, d_p, c_1, \dots, c_k)$.

Another consequence from this is that every finite index subgroup $(g'; p'; \mathbf{n}) \leq (g; 0; \mathbf{m})$ remains unpunctured, i.e., $p' = 0$, which reconfirms Theorem 3.2.3. In addition, the analysis provided above shows that every finite index subgroup $(g'; p', \mathbf{n})$ of a punctured lattice $(g; p; \mathbf{m})$ is also punctured, i.e. $p' > 0$ whenever $p > 0$.

4. BASIC QUOTIENTS OF FUCHSIAN GROUPS

This chapter introduces the *dihedral* and *Abelian* quotients of Fuchsian groups arising as lattices. In particular, these quotients will significantly restrict the possible signatures $(g; p; \mathbf{m})$ of profinitely equivalent lattices. However, these quotients alone will not suffice in establishing relative rigidity completely, for which we will require results and techniques described in Chapters 5 and 6.

Many of the results in this chapter are extensions of ideas from [1]. We will also use the convention that the tuples $\mathbf{m}$ and $\mathbf{n}$ with respective sizes k and l have the following entries: $\mathbf{m} := (m_1, \ldots, m_k)$ and $\mathbf{n} := (n_1, \ldots, n_l)$.

4.1 Dihedral quotients

We establish criteria for genus 0 groups $(0; p; \mathbf{m})$ to have dihedral quotients. Let D_{2a} denote the dihedral group of order $2a$, for $a > 0$. Recall that $\Delta(2, 2, a) \cong \mathrm{D}_{2a}$ is a spherical triangle group.

Proposition 4.1.1. *The group $(0; p; \mathbf{m})$ has a dihedral quotient if and only if the number k' of even entries in $\mathbf{m}$ plus the number of punctures p is at least 2, i.e., $k' + p \geq 2$.*

Proof. Let

$$(0; p; \mathbf{m}) \cong \langle y_1, \ldots, y_p, x_1, \ldots, x_k \mid x_i^{m_i} = y_1 \ldots y_p x_1 \ldots x_k = 1 \rangle$$

be the canonical group presentation. Then there is some $a > 0$ with a surjective map $(0; p; \mathbf{m}) \twoheadrightarrow \Delta(2, 2, a)$ if and only if $(0; p; \mathbf{m})$ has two canonical generators of either even or infinite order in $(0; p; \mathbf{m})$. $\square$

Two important cases as a result of Proposition 4.1.1 are that $(0; 0; \mathbf{m})$ admits a dihedral quotient if and only if $\mathbf{m}$ contains at least two even entries, and that $(0; 1; \mathbf{n})$ admits a dihedral quotient if and only if $\mathbf{n}$ contains at least one even entry. We will find these characterizations important for Chapter 6.

4.2 Abelian quotients

The *Abelianization* of Γ is the Abelian group $\Gamma^{\mathrm{Ab}} := \Gamma/[\Gamma,\Gamma]$, where $[\Gamma,\Gamma]$ is the commutator subgroup of Γ. As a universal object, Γ^{Ab} encodes all of the Abelian quotients of Γ. It is clear that the Abelianization of a lattice $(g;p;\mathbf{m})^{\mathrm{Ab}}$ is finitely generated, and we will consider the *invariant factor form* for finitely generated Abelian groups:

$$\mathbf{Z}^r \times \mathrm{C}_{a_1} \times \cdots \times \mathrm{C}_{a_d},$$

where $r \geq 0$, $a_i \neq 0$, and $a_i \mid a_j$ whenever $i < j$. We may remove any instances of the trivial factor C_1 appearing in this decomposition.

To proceed, we generalize the notions of gcd's and lcm's with a definition for the family of operators $\mathrm{mid}_i(\mathbf{m})$, for a k-tuple $\mathbf{m} := (m_1, \ldots, m_k)$. We set

$$\mathbf{L_i} := \{\mathrm{lcm}(\mathbf{m}') \mid \mathbf{m}' \text{ is a projection of the tuple } \mathbf{m} \text{ of size } i\}, \text{ for } 1 \leq i \leq k.$$

Then we define $\mathrm{mid}_i(\mathbf{m}) := \gcd(\mathbf{L_i})$. Equivalently, $\mathrm{mid}_i(\mathbf{m}) = \mathrm{lcm}(\mathbf{G_i})$, where

$$\mathbf{G_i} := \{\gcd(\mathbf{m}') \mid \mathbf{m}' \text{ is a projection of the tuple } \mathbf{m} \text{ of size } k-i+1\}.$$

For another description, $\mathrm{mid}_i(\mathbf{m})$ is the product of each of the i-th lowest prime powers existing among the prime factorizations of the integers $m_1, \ldots, m_k$. In particular we have,

$$\begin{aligned} \mathrm{mid}_1(\mathbf{m}) &= \gcd(\mathbf{m}) \\ \mathrm{mid}_{|\mathbf{m}|}(\mathbf{m}) &= \mathrm{mid}_k(\mathbf{m}) = \mathrm{lcm}(\mathbf{m}) \\ m_1 \ldots m_k &= \prod_{i=1}^{k} \mathrm{mid}_i(\mathbf{m}). \end{aligned}$$

Also worth noting is that $\mathrm{mid}_i(\mathbf{m}) \mid \mathrm{mid}_j(\mathbf{m})$, whenever $i < j$.

We begin with the following piece-wise result for the Abelianizations of lattices.

Proposition 4.2.1. *Written in the invariant factor form (with possible* C_1 *factors),*

$$(g;p;m)^{\mathrm{Ab}} \cong \begin{cases} \mathbf{Z}^{2g+p-1} \times \mathrm{C}_{\mathrm{mid}_1(\mathbf{m})} \times \cdots \times \mathrm{C}_{\mathrm{mid}_k(\mathbf{m})} & \text{if } p > 0 \\ \mathbf{Z}^{2g} \times \mathrm{C}_{\mathrm{mid}_1(\mathbf{m})} \times \cdots \times \mathrm{C}_{\mathrm{mid}_{k-1}(\mathbf{m})} & \text{if } p = 0. \end{cases}$$

Proof. Recall from (2) that when $p > 0$, then

$$(g;p;\mathbf{m}) \cong F_{2g+p-1} * \mathrm{C}_{m_1} * \cdots * \mathrm{C}_{m_k}.$$

Hence this case is the Abelianization of a free product of free and cyclic groups, so that

$$\begin{aligned} (g;p;\mathbf{m})^{\mathrm{Ab}} &\cong \mathbf{Z}^{2g+p-1} \times \mathrm{C}_{m_1} \times \cdots \times \mathrm{C}_{m_k} \\ &\cong \mathbf{Z}^{2g+p-1} \times \mathrm{C}_{\mathrm{mid}_1(\mathbf{m})} \times \cdots \times \mathrm{C}_{\mathrm{mid}_k(\mathbf{m})}, \end{aligned}$$

which is written as a product of its invariant factors.

When $p = 0$, we can further assume that $g = 0$, with the case $g > 0$ following similarly. We write the group presentation of $(0;0;\mathbf{m})^{\mathrm{Ab}}$ additively:

$$(0;0;\mathbf{m})^{\mathrm{Ab}} \cong \langle x_1, \ldots, x_k \mid m_1 x_1 = \cdots = m_k x_k = x_1 + \cdots + x_k = 0 \rangle.$$

This presentation is isomorphic to the quotient of the group $G := \mathbf{Z}^k/(m_1\mathbf{Z} \oplus \cdots \oplus m_k\mathbf{Z})$ by its cyclic subgroup generated by $(1,1,\ldots,1) \in G$ of order $\mathrm{lcm}(\mathbf{m})$. It follows that

$$G \cong H, \text{ where } H := \mathrm{C}_{\mathrm{gcd}(\mathbf{m})} \times \mathrm{C}_{\mathrm{mid}_2(\mathbf{m})} \times \cdots \times \mathrm{C}_{\mathrm{mid}_{k-1}(\mathbf{m})} \times \mathrm{C}_{\mathrm{lcm}(\mathbf{m})}$$

and through this natural isomorphism, the element $(1,1,\ldots,1) \in G$ is mapped to the element $(1,1,\ldots,1) \in H$.

It can be verified that the assignment

$$\begin{aligned} f\colon \mathrm{C}_{\gcd(\mathbf{m})} \times \cdots \times \mathrm{C}_{\mathrm{lcm}(\mathbf{m})} &\to \mathrm{C}_{\gcd(\mathbf{m})} \times \cdots \times \mathrm{C}_{\mathrm{lcm}(\mathbf{m})}, \text{ with} \\ \mathbf{e}_i &\mapsto \mathbf{e}_i, \text{ for } 1 \le i \le k-1, \\ (1, 1, \dots, 1) &\mapsto \mathbf{e}_k, \end{aligned}$$

induces a well-defined group isomorphism. Thus we have the desired result

$$(0; 0; \mathbf{m}) \cong \mathrm{C}_{\gcd(\mathbf{m})} \times \mathrm{C}_{\mathrm{mid}_2(\mathbf{m})} \times \dots \mathrm{C}_{\mathrm{mid}_{k-1}(\mathbf{m})}.$$

□

Remark. Notice that $(g; p; \mathbf{m})^{\mathrm{Ab}}$ is a finite group if and only if $g = 0$ and $p \le 1$. In particular, a triangle group $\Delta(r, s, t)$ has finite Abelianization. Only lattices of the form $(0; 0; \mathbf{m})$ or $(0; 1; \mathbf{m})$ could possibly share all of its Abelian quotients with $\Delta(r, s, t)$. Therefore, our typical and convenient focus will be on lattices of genus 0 with at most one puncture.

Another way to prove the dihedral criterion of Proposition 4.1.1 is to observe that a group $(0; p; \mathbf{m})$ admits a dihedral quotient if and only if $(0; p; \mathbf{m})$ has $\mathrm{C}_2 \cong \mathrm{D}_{2\cdot 1}$ as a quotient, which is also equivalent to having C_2 as a quotient of $(0; p; \mathbf{m})^{\mathrm{Ab}}$. Therefore by Proposition 4.2.1, if $p > 0$, then we require $\mathrm{lcm}(\mathbf{m})$ to be even, and if $p = 0$, then we require $\mathrm{mid}_{k-1}(\mathbf{m})$ to be even.

In the genus 0, unpunctured $(0; 0; \mathbf{m})$ case, the only $\mathrm{mid}_i(\mathbf{m})$, for $1 \le i \le k$, to have no dependence on the Abelianization $(0; 0; \mathbf{m})^{\mathrm{Ab}}$ is the quantity $\mathrm{mid}_k(\mathbf{m}) = \mathrm{lcm}(\mathbf{m})$. Proposition 4.3.2 in the next section will show that the Abelianization and the Euler characteristic of $(0; 0; \mathbf{m})$ determine $\mathrm{lcm}(\mathbf{m})$.

4.3 Euler characteristics

Recall from Section 3.2.4 the Euler characteristic of a signature $(g; p; \mathbf{m})$ is a rational number given by

$$\chi(g; p; \mathbf{m}) = 2 - 2g - p - \sum_{i=1}^{k} \left(1 - \frac{1}{m_i}\right).$$

Also, the Riemann–Hurwitz formula states that if Λ is a finite index subgroup of a lattice Γ, then Λ is also a lattice and

$$\chi(\Lambda) = [\Gamma : \Lambda]\chi(\Gamma).$$

We now consider various results on genus 0, unpunctured lattices, and set notation for the tuples $\mathbf{m} = (m_1, \ldots, m_k)$ and $\mathbf{n} = (n_1, \ldots, n_l)$, and assume $2 \leq k \leq l$.

The following is an immediate corollary to Proposition 4.2.1, since up to reordering, the invariant factor decomposition uniquely determines the isomorphism type for a finitely generated Abelian group.

Corollary 4.3.1. *If* $(0; 0; \mathbf{m})^{\mathrm{Ab}} \cong (0; 0; \mathbf{n})^{\mathrm{Ab}}$*, then*

1. $\mathrm{mid}_i(\mathbf{n}) = 1$*, for* $1 \leq i \leq l - k$*,*
2. $\mathrm{mid}_j(\mathbf{m}) = \mathrm{mid}_{l-k+j}(\mathbf{n})$*, for* $1 \leq j \leq k - 1$*.*

Chapter 5 will show we can distinguish finite quotients between two groups with unequal Euler characteristics $\chi(0; 0; \mathbf{m}) \neq \chi(0; 0; \mathbf{n})$. This provides motivation for allowing the Euler characteristics to be the same for the following proposition. Furthermore, to complement Corollary 4.3.1, appending information about the Euler characteristic will determine the lcm.

Proposition 4.3.2. *If* $(0; 0; \mathbf{m})^{\mathrm{Ab}} \cong (0; 0; \mathbf{n})^{\mathrm{Ab}}$ *and* $\chi(0; 0; \mathbf{m}) = \chi(0; 0; \mathbf{n})$*, then* $\mathrm{lcm}(\mathbf{m}) = \mathrm{lcm}(\mathbf{n})$ *and* $m_1 \ldots m_k = n_1 \ldots n_l$*.*

Proof. The statement $m_1 \ldots m_k = n_1 \ldots n_l$ will hold true, once we show that $\mathrm{lcm}(\mathbf{m}) = \mathrm{lcm}(\mathbf{n})$.

Corollary 4.3.1 determines all of the mid_i's for $\mathbf{m}$ and $\mathbf{n}$, except for their lcm's. In particular, we have that $\mathrm{mid}_i(\mathbf{n}) = 1$, for $1 \leq i \leq l - k$.

Now, for a fixed prime ℓ, let $\nu_\ell(x)$ denote the ℓ-adic valuation of a rational number x. It follows from the *ultrametric property* of ν_ℓ that if $\nu_\ell(x_1) \leq \cdots \leq \nu_\ell(x_r)$, then

$$\nu_\ell(x_1 + \cdots + x_r) \geq \nu_\ell(x_1),$$

with strict inequality only if $\nu_\ell(x_1) = \nu_\ell(x_2)$.

Define $\alpha_j := \nu_\ell(\mathrm{mid}_j(\mathbf{m})) = \nu_\ell(\mathrm{mid}_{l-k+j}(\mathbf{n}))$, for $1 \le j \le k-1$, $\beta := \nu_\ell(\mathrm{lcm}(\mathbf{m}))$, and $\gamma := \nu_\ell(\mathrm{lcm}(\mathbf{n}))$. We have that $0 \le \alpha_1 \le \alpha_2 \le \cdots \le \alpha_{k-1} \le \beta, \gamma$. The Euler characteristic condition $\chi(0;0;\mathbf{m}) = \chi(0;0;\mathbf{n})$ provides the following:

$$\frac{1}{m_1} + \cdots + \frac{1}{m_k} - (k-2) = \frac{1}{n_1} + \cdots + \frac{1}{n_l} - (l-2)$$
$$\frac{S_{\mathbf{m}} - (k-2)m_1 \dots m_k}{m_1 \dots m_k} = \frac{S_{\mathbf{n}} - (l-2)n_1 \dots n_l}{n_1 \dots n_l}$$
$$(S_{\mathbf{m}} - (k-2)m_1 \dots m_k)n_1 \dots n_l = (S_{\mathbf{n}} - (l-2)n_1 \dots n_l)m_1 \dots m_k$$
$$T_{\mathbf{m}}\, n_1 \dots n_l = T_{\mathbf{n}}\, m_1 \dots m_k.$$

The value $S_{\mathbf{m}}$ (resp. $S_{\mathbf{n}}$) is the sum of all k (resp. l) squarefree monomials of $\mathbf{m}$ (resp. $\mathbf{n}$) of size $k-1$ (resp. $l-1$), and we define $T_{\mathbf{m}} := S_{\mathbf{m}} - (k-2)m_1 \dots m_k$ and $T_{\mathbf{n}} := S_{\mathbf{n}} - (l-2)n_1 \dots n_l$. Notice that by ordering each of the individual summands in $T_{\mathbf{m}}$ by their ℓ-adic valuations, the smallest two such ℓ-adic values are $\alpha_1 + \cdots + \alpha_{k-1}$ and $\alpha_1 + \cdots + \alpha_{k-2} + \beta$. Similarly for $T_{\mathbf{n}}$, the smallest two such ℓ-adic values are $\alpha_1 + \cdots + \alpha_{k-1}$ and $\alpha_1 + \cdots + \alpha_{k-2} + \gamma$. Hence, the ultrametric provides the lower bounds on $\nu_\ell(T_m\, n_1 \dots n_l) \ge 2(\alpha_1 + \cdots + \alpha_{k-1}) + \gamma$ and on $\nu_\ell(T_n\, m_1 \dots m_l) \ge 2(\alpha_1 + \cdots + \alpha_{k-1}) + \beta$. Without loss of generality, suppose $\beta < \gamma$, but then $\nu_\ell(T_n\, m_1 \dots m_k)$ cannot take on the value of its ultrametric lower bound. This implies $\alpha_{k-1} = \gamma$; however, $\gamma = \alpha_{k-1} \le \beta$, which is a contradiction.

Therefore, it must be that $\beta = \gamma$, and so $\nu_\ell(\mathrm{lcm}(\mathbf{m})) = \nu_\ell(\mathrm{lcm}(\mathbf{n}))$ for each prime ℓ, which concludes the proof. □

The following lemma provides an explicit way for distinguishing genus 0, unpunctured lattices by dihedral quotients.

Lemma 4.3.3. *Suppose* $(0;0;\mathbf{m})^{\mathrm{Ab}} \cong (0;0;\mathbf{n})^{\mathrm{Ab}}$*, and* $(0;0;\mathbf{m})$ *admits dihedral quotients. If* $\{m_1, \dots, m_k\} \cap \{n_1, \dots, n_l\} = \varnothing$*, then there is a finite dihedral group that is a quotient for one of the groups but not the other.*

Proof. First, observe that the number of even entries in a tuple $\mathbf{x}$ is precisely the number of even integers in the set $\{\mathrm{mid}_i(\mathbf{x}) \mid 1 \le i \le |\mathbf{x}|\}$. By the hypothesis $(0;0;\mathbf{m})^{\mathrm{Ab}} \cong (0;0;\mathbf{n})^{\mathrm{Ab}}$

and by Corollary 4.3.1, $\mathbf{m}$ and $\mathbf{n}$ have exactly the same number of even integers, say a. Applying $\mathbf{m}$ to Proposition 4.1.1, we have that $a \geq 2$, which implies that $(0; 0; \mathbf{n})$ also admits dihedral quotients.

If $a \geq 3$, define t as the largest entry among $\mathbf{m}$ and $\mathbf{n}$, and if $a = 2$, define t as the largest odd entry among $\mathbf{m}$ and $\mathbf{n}$. In either case, since t can only belong to one of $\mathbf{m}$ or $\mathbf{n}$, the dihedral group D_{2t} is a finite quotient for exactly one of $(0; 0; \mathbf{m})$ or $(0; 0; \mathbf{n})$. $\square$

4.4 First Betti numbers

We have encountered an inability to identify $\mathbf{m}$ and $\mathbf{n}$ uniquely in the situation where $(0; 0; \mathbf{m})^{\mathrm{Ab}} \cong (0; 0; \mathbf{n})^{\mathrm{Ab}}$. For example, there are infinitely many groups of the form $(0; 0; \mathbf{m})$ with trivial Abelianization. Developing methods to be able to dismiss these cone orders is one natural way to proceed.

The group $(g; p; \mathbf{m})$ is *torsion-free*, if all of the non-identity elements have infinite order, or equivalently, there are integers g' and p' such that $(g; p; \mathbf{m}) \cong (g', p'; -)$, which precisely accounts for the situation where $\mathbf{m}$ is a degenerate tuple. We define the *first Betti number* of finitely generated groups.

Definition 8. The first Betti number of a finitely generated group Γ is the non-negative integer given by $b_1(\Gamma) := \mathrm{rank}(\Gamma^{\mathrm{Ab}} \otimes_{\mathbf{Z}} \mathbf{Q})$.

Hence for a lattice $(g; p; \mathbf{m})$, by Proposition 4.2.1, we have that

$$b_1(g; p; \mathbf{m}) = \begin{cases} 2g + p - 1 & \text{if } p > 0 \\ 2g & \text{if } p = 0, \end{cases}$$

ignoring any instances of the torsion arising from the tuple $\mathbf{m}$.

Remark. We use b_1 to recast an earlier observation regarding lattices with finite Abelianizations: $b_1(g; p; \mathbf{m}) = 0$ if and only if $g = 0$ and $p \leq 1$.

An important perspective for when $(g; p; -)$ is torsion-free is the following

$$b_1(g; p; -) = \begin{cases} 1 - \chi(g; p; -) & \text{if } p > 0 \\ 2 - \chi(g; 0; -) & \text{if } p = 0. \end{cases}$$

In this case the Euler characteristic and whether or not the lattice is punctured determines the b_1 of the group. More generally, we have the following.

Proposition 4.4.1. *For a nondegenerate tuple* $\mathbf{m}$*, if* $p > 0$*, then*

$$b_1(g; p; \mathbf{m}) \leq 1 - \chi(g; p; \mathbf{m}),$$

with equality if and only if $(g; p; \mathbf{m})$ *is torsion-free. For a nondegenerate tuple* $\mathbf{n}$*, if* $p = 0$*, then*

$$b_1(g; 0; \mathbf{n}) \leq 2 - \chi(g; 0; \mathbf{n}),$$

with equality if and only if $(g; 0; \mathbf{n})$ *is torsion-free.*

Proof. Notice when $p > 0$, then

$$b_1(g; p; \mathbf{m}) = b_1(g; p; -) = 1 - \chi(g; p; -) \leq 1 - \chi(g; p; \mathbf{m}).$$

Similarly for $p = 0$, then

$$b_1(g; 0; \mathbf{n}) = b_1(g; 0; -) = 2 - \chi(g; 0; -) \leq 2 - \chi(g; 0; \mathbf{n}),$$

providing piece-wise upperbounds on the first Betti numbers.

Regarding achieving upperbounds, we will prove the case $p = 0$, with the case $p > 0$ done similarly. When $(g; 0; -)$ is torsion-free, then the observation above shows the upperbound $b_1(g; 0; -) = 2 - \chi(g; 0; -)$ is achieved.

If $b_1(g; 0; \mathbf{n}) = 2 - \chi(g; 0; \mathbf{n})$, then $\chi(g; 0; -) = \chi(g; 0; \mathbf{n})$, and so

$$\sum_{i=1}^{l} \left(1 - \frac{1}{n_i}\right) = 0.$$

This cannot occur for a nondegenerate tuple $\mathbf{n}$ with $|\mathbf{n}| > 0$. Therefore, $|\mathbf{n}| = 0$, and so $(g; 0; \mathbf{n}) = (g; 0; -)$ is torsion-free. $\square$

While it is far from being a unique profinite measurement for any particular lattice, the usage of dihedral and Abelian finite quotients as building blocks for group extensions will be explored in Chapter 5.

5. SMOOTH AND NON-SMOOTH QUOTIENTS

This chapter will introduce the notion of the *degree of smoothness* for a finite quotient G of a lattice $(g; p; \mathbf{m})$, which in light of Chapter 4 aims to detect even smaller differences between two lattices. To apply this theory, we will construct smooth representations to $\mathrm{PSL}(2, q) := \mathrm{PSL}(2, \mathbf{F}_q)$, for $q := \ell^d$ an odd prime power. Extending a result by Macbeath [4], this method of construction will be aiding with computing effective upperbounds and for providing an infinite family of quotients to work with. As with dihedral and Abelian quotients, these PSL_2 representations will append to the list of numerical restrictions for the signatures of profinitely equivalent lattices. By allowing the odd prime powers q to vary, the data associated to the collection of $\mathrm{PSL}(2, q)$'s such that the lattice $(0; 0; \mathbf{m})$ has a smooth representation can be organized with an L_2*-set*, which was initially created in [1].

5.1 Smooth PSL_2 representations

Let G be a finite group. We say that G is a *smooth* quotient of $(g; p; \mathbf{m})$, if there exists a surjective homomorphism $s\colon (g; p; \mathbf{m}) \twoheadrightarrow G$ that preserves the order of torsion elements. In this case, we will also say that the surjective map s is *smooth*. It suffices to check this condition only on the canonical elliptic generators of $(g; p; \mathbf{m})$. Equivalently, G is a smooth quotient of $(g; p; \mathbf{m})$ if there exists a surjective map $s\colon (g; p; \mathbf{m}) \twoheadrightarrow G$ with torsion-free kernel, say $(g'; p'; -)$. In Section 5.3, we will define more generalized degrees of a smooth quotient for lattices of the form $(0; 0; \mathbf{m})$.

To this end, for the remainder of the chapter, we will focus on lattices $(0; 0; \mathbf{m})$ having genus 0 and without punctures. Since every lattice $(g; p; \mathbf{m})$ naturally admits the quotient map $\pi\colon (g; p; \mathbf{m}) \twoheadrightarrow (0; 0; \mathbf{m})$, a finite quotient G of $(0; 0; \mathbf{m})$ is smooth if and only there exists a smooth surjective map $s\colon (g; p; \mathbf{m}) \twoheadrightarrow G$ such that s factors through π. We now set up notation for a theorem that extends a result from Macbeath [4].

For a field $\mathbf{F}_q$ with q elements, we denote the matrix group $\mathrm{SL}(2,q) := \mathrm{SL}(2,\mathbf{F}_q)$, and for $\mathbf{F}_{q^2}$, the unique quadratic extension over $\mathbf{F}_q$, we will be utilizing the isomorphism

$$\mathrm{SL}(2,q) \cong \mathrm{SU}(2,q^2) := \left\{ \begin{pmatrix} a & b \\ -b^q & a^q \end{pmatrix} \,\middle|\, a,b \in \mathbf{F}_{q^2},\ a^{q+1} + b^{q+1} = 1 \right\}. \tag{6}$$

Theorem 5.1.1. *Let $q = \ell^d$ be an odd prime power and $\mathbf{m} = (m_1, \ldots, m_k)$, with $k \geq 3$. There exists a subgroup of $\mathrm{PSL}(2,q)$ that is a smooth quotient of $(0;0;\mathbf{m})$ if and only if each of the integers $m_1, \ldots, m_k$ divides one of ℓ, $\frac{q-1}{2}$, or $\frac{q+1}{2}$.*

Proof. The forward direction holds since the orders of elements in $\mathrm{PSL}(2,q)$ are precisely each of the divisors of ℓ, $\frac{q-1}{2}$, and $\frac{q+1}{2}$.

For the converse, suppose each of the integers $m_1, \ldots, m_k$ divides ℓ, $\frac{q-1}{2}$, or $\frac{q+1}{2}$. Notice by the theory of Jordan canonical forms and that $-1 \neq 1 \in \mathbf{F}_q$, if $A \in \mathrm{SL}(2,q) \cong \mathrm{SU}(2,q^2)$, then $\mathrm{tr}(A) \in \mathbf{F}_q \setminus \{\pm 2\}$ determines the multiplicative order of A. In the case $\mathrm{tr}(A) = \pm 2$, by projecting A to its image in $\mathrm{PSL}(2,q)$, any such non-identity matrix in $\mathrm{PSL}(2,q)$ has the order ℓ.

To this end, we will construct matrices $A_1, \ldots, A_k$ in $\mathrm{PSL}(2,q)$ with corresponding orders $m_1, \ldots, m_k$, such that $A_1 \ldots A_k = I_2$. Therefore, given the canonical elliptic generators $x_1, \ldots, x_k$ with respective orders $m_1, \ldots, m_k$, the following representation will be smooth onto its image

$$\begin{gathered} (0;0;m_1, \ldots, m_k) \to \mathrm{PSL}(2,q) \\ x_i \mapsto A_i. \end{gathered}$$

Let $\mathbf{F}_{q^2} = \mathbf{F}_q(\alpha)$, such that $\alpha^2 \in \mathbf{F}_q$. Such an α always exists, because there are precisely $\frac{q-1}{2}$ non-squares in $\mathbf{F}_q$. Consequently, we have that $\alpha^q = -\alpha$.

We claim that for any $2t \in \mathbf{F}_q$, we can construct a non-identity matrix

$$A := \begin{pmatrix} a & b \\ -b^q & a^q \end{pmatrix} \in \mathrm{SU}(2,q^2)$$

with trace $2t$. Notice that the solutions to the equation given by $a^q + a = \operatorname{tr}(A) = 2t$ are precisely $a = t + u\alpha$, for any $u \in \mathbf{F}_q$. Hence, the condition $\det(A) = 1$ provides, for some $u \in \mathbf{F}_q$, the equation

$$b^{q+1} = 1 - t^2 + u^2\alpha^2 \in \mathbf{F}_q,$$

for which either $b = 0$ or b has $q+1$ distinct non-zero solutions in $\mathbf{F}_{q^2}$ since b^{q+1} is the image of b under the field norm $\mathrm{Nm}\colon \mathbf{F}_{q^2}^\times \twoheadrightarrow \mathbf{F}_q^\times$, which is a $(q+1)$-to-1 surjective homomorphism. This proves the claim, since if $b = 0$, we can choose $u \in \mathbf{F}_q$ so that $a = t + u\alpha \neq 1$, ensuring that A is not the identity matrix.

Now, for each m_i, we will consider the cases where m_i divides one of ℓ, $\frac{q-1}{2}$, or $\frac{q+1}{2}$. We will be using the notation coming from the claim above.

Case $m_i \mid \frac{q\pm1}{2}$.

Take an element $w \in \mathbf{F}_{q^2}$ with multiplicative order $2m_i \mid (q \pm 1)$ and let t be such that $2t = w + w^{-1}$. Thus, for our choices of a and b in the claim above, the matrix

$$A_i := \begin{pmatrix} a & b \\ -b^q & a^q \end{pmatrix} \in \mathrm{SU}(2, q^2)$$

has order $2m_i$, since the eigenvalues of A_i are distinct and equal to w and w^{-1}. Then the projection of A_i to its image in $\mathrm{PSL}(2, q)$, which we also denote by A_i, will have order m_i.

Case $m_i = \ell$.

In the case $m_i = \ell$, it suffices to have the trace $2t$ to be equal to 2, i.e. $a = 1 + s\alpha$, for $s \in \mathbf{F}_q$. If we take $s \neq 0$, we can ensure that the matrix

$$A_i := \begin{pmatrix} a & b \\ -b^q & a^q \end{pmatrix} \in \mathrm{SU}(2, q^2)$$

is not the identity matrix, and therefore A_i has order ℓ. The image of A_i under $\mathrm{PSL}(2, q)$, also denoted A_i, will have order ℓ.

One noted consequence from the cases and the claim is that for any $2t \in \mathbf{F}_q$, there are at least 2 choices for a non-identity A_i such that $\operatorname{tr}(A_i) = 2t$. This will be invoked later when an initial arbitrary choice for A_i causes an undesired coincidence, which is avoided upon any replacement.

For $1 \le i \le k-2$, we define $A_i \in \mathrm{PSL}(2,q)$ with order m_i as in the cases above. An assignment remains for only A_{k-1}, since afterwards the matrix $A_k := (A_1 \ldots A_{k-1})^{-1}$ will be uniquely determined. However, the entries of A_{k-1} must be chosen properly so that both of the orders of A_{k-1} and A_k in $\mathrm{PSL}(2,q)$ are m_{k-1} and m_k, respectively. Exploiting the form (6) of the matrices in $\mathrm{SU}(2,q^2)$, we can set the entries in the following product

$$A_1 \ldots A_{k-2} =: \begin{pmatrix} c & d \\ -d^q & c^q \end{pmatrix}.$$

By possibly varying the matrix entries of one of the factors A_i of this product, we can assume the entry $d \neq 0$. If we establish that

$$A_{k-1} := \begin{pmatrix} e & f \\ -f^q & e^q \end{pmatrix}$$

has order m_{k-1} in $\mathrm{PSL}(2,q)$, then $e^q + e = \mathrm{tr}(A_{k-1}) = 2t_{k-1}$, for an appropriate value of $2t_{k-1}$, corresponding to the case above where m_{k-1} belongs. We can choose some value of e in A_{k-1} so that $f^{q+1} = 1 - e^{q+1} \neq 0$, and therefore f must be nonzero. With the entries c, d, and e now fixed ($d \neq 0$) and with $f \neq 0$ currently left unknown, we have the following matrix product representing A_k^{-1}

$$A_1 \ldots A_{k-2}A_{k-1} = \begin{pmatrix} c & d \\ -d^q & c^q \end{pmatrix} \begin{pmatrix} e & f \\ -f^q & e^q \end{pmatrix} \tag{7}$$

$$= \begin{pmatrix} ce - df^q & cf + de^q \\ -(c^q f^q + d^q e) & c^q e^q - d^q f \end{pmatrix}. \tag{8}$$

We insist the matrix in (8) has order m_k in $\mathrm{PSL}(2, q)$ and has a corresponding trace $2t_k \in \mathbf{F}_q$. It remains to solve for f the following system of equations:

$$ce - df^q + c^q e^q - d^q f = 2t_k \tag{9}$$

$$f^{q+1} = 1 - e^{q+1}, \tag{10}$$

where (9) comes from $\mathrm{tr}(A_1 \dots A_{k-1}) = 2t_k$, and (10) from $\det(A_{k-1}) = 1$. Since we assumed $f \neq 0$, we can substitute (10) into (9) multiplied by f to get

$$d^q f^2 + (2t_k - (ce + c^q e^q))f + d(1 - e^{q+1}) = 0, \tag{11}$$

a quadratic equation in f over $\mathbf{F}_{q^2}$ (recall $d \neq 0$). There is a solution for f to the system in $\mathbf{F}_{q^2}$, because the discriminant (12) of the quadratic is an element of $\mathbf{F}_q$.

$$(2t_k - (ce + c^q e^q))^2 - 4d^{q+1}(1 - e^{q+1}) \in \mathbf{F}_q. \tag{12}$$

After relabelling $A_{k-1} \in \mathrm{SU}(2, q^2)$ by its projection in $\mathrm{PSL}(2, q)$, we have acquired a smooth representation $(0; 0; m_1, \dots, m_k) \to \mathrm{PSL}(2, q)$. $\square$

Retaining the notation above, we will show such a q from Theorem 5.1.1 exists. We show there is an odd prime power q such that all of the m_i divides $\frac{q-1}{2}$. Take any odd prime ℓ that is coprime to $M := 2m_1 m_2 \dots m_k$. Then ℓ is a unit element in the ring $\mathbf{Z}/M\mathbf{Z}$, and so there exists an $n > 0$ such that

$$\ell^d \equiv 1 \pmod{M}. \tag{13}$$

Setting $q := \ell^d$, we have (13) implies that $m_i \mid \frac{q-1}{2}$, for every $1 \leq i \leq k$.

Remark. Theorem 5.1.1 is a constructive version of Selberg's lemma [13], which states that a finitely generated linear group over a field of zero characteristic is virtually torsion-free.

5.2 L_2-sets

Theorem 5.1.1 will allow us to find smooth and non-smooth quotients of $(0;0;\mathbf{m})$, based off simple divisibility conditions. To this end, we will utilize L_2*-sets* in our study of smooth representations to various $\mathrm{PSL}(2,q)$'s. This section repurposes much of the background and results on L_2-sets first introduced in [1].

Definition 9. The L_2-set of $\mathbf{m} = (m_1, \ldots, m_k)$, with $k \geq 3$, denoted $L_2(\mathbf{m})$ is a set $\{M_1, \ldots, M_{k'}\}$ satisfying the following properties:

1. $\gcd(M_i, M_j) = 1$, for every $i \neq j$,
2. $\mathrm{lcm}(M_1, \ldots, M_{k'}) = \mathrm{lcm}(\mathbf{m})$,
3. For each m_i, there exists a unique M_j such that $m_i \mid M_j$.

Notice that $1 \leq |L_2(\mathbf{m})| \leq |\mathbf{m}|$, and we will always implicitly assume $|\mathbf{m}| \geq 3$ in the setting of L_2-sets. In the case where $|L_2(\mathbf{m})| = |\mathbf{m}|$, then as sets we have $L_2(\mathbf{m}) = \mathbf{m}$ precisely when $(0;0;\mathbf{m})$ is a perfect group, i.e., $(0;0;\mathbf{m})^{\mathrm{Ab}}$ is the trivial group. This follows from Proposition 4.2.1. At the other extreme, if $L_2(\mathbf{m})$ is a singleton set, then it must be equal to $\{\mathrm{lcm}(\mathbf{m})\}$. This latter case will be an important focus, particularly for two triangle groups in Proposition 6.2.6.

The L_2-set $L_2(0;0;\mathbf{m})$ disentangles any gcd relations among the pairs of entries of $\mathbf{m}$. An immediate corollary to Theorem 5.1.1 follows from an application of the Chinese remainder theorem.

Corollary 5.2.1. *Let $q = \ell^d$ be an odd prime and $\mathbf{m} = (m_1, \ldots, m_k)$, with $k \geq 3$. Suppose that $L_2(\mathbf{m}) = \{M_1, \ldots, M_{k'}\}$. There exists a subgroup of $\mathrm{PSL}(2,q)$ that is a smooth quotient of $(0;0;\mathbf{m})$ if and only if each of the integers $M_1, \ldots, M_{k'}$ divides one of ℓ, $\frac{q-1}{2}$, or $\frac{q+1}{2}$.*

Remark. It is a priori difficult to tell whether or not the triangle groups $\Delta(15,42,63)$ and $\Delta(21,21,90)$ have smooth representations to exactly the same collection of $\mathrm{PSL}(2,q)$'s. Computing their L_2-sets, we have $L_2(15,42,63) = L_2(21,21,90) = \{630\}$, and Corollary 5.2.1 establishes this is indeed the case.

Corollary 5.2.1 shows that L_2 can be treated as a functor, taking a tuple $\mathbf{m}$ to the collection of all odd prime powers q such that there is a smooth representation from $(0; 0; \mathbf{m})$ to $\mathrm{PSL}(2, q)$. The following proposition (with a condition on the lcm) shows that this association is essentially unique.

Proposition 5.2.2. *Let* $\mathbf{m}$ *and* $\mathbf{n}$ *be tuples such that* $|\mathbf{m}|, |\mathbf{n}| \geq 3$. *If* $L_2(\mathbf{m}) \neq L_2(\mathbf{n})$ *and* $\mathrm{lcm}(\mathbf{m}) = \mathrm{lcm}(\mathbf{n})$, *then by switching* $\mathbf{m}$ *and* $\mathbf{n}$ *if necessary, there exists a finite quotient* G *that is smooth for* $(0; 0; \mathbf{m})$, *but is non-smooth for* $(0; 0; \mathbf{n})$.

Proof. Switching $\mathbf{m}$ and $\mathbf{n}$ if necessary, since $L_2(\mathbf{m}) \neq L_2(\mathbf{n})$, there are distinct maximal prime power factors q_1 and q_2 of $\mathrm{lcm}(\mathbf{m}) = \mathrm{lcm}(\mathbf{n})$ such that for some $N \in L_2(\mathbf{n})$, $q_1 q_2 \mid N$, but $q_1 \mid M_1$ and $q_2 \mid M_2$ for distinct $M_1, M_2 \in L_2(\mathbf{m})$. It suffices to show there exists an odd prime power q satisfying the following system of congruences

$$q \equiv 1 \pmod{2M_1M} \tag{14}$$

$$q \equiv -1 \pmod{2M_2}, \tag{15}$$

where M is the product of each element of $L_2(\mathbf{m}) \setminus \{M_1, M_2\}$ (and with $M = 1$, for the empty product).

From (14), the exhaustive list of integer solutions is given by $q = 1 + i2M_1M$, where $i \in \mathbf{Z}$. Take $1 \leq a < M_2$ such that

$$a \equiv -(M_1M)^{-1} \pmod{M_2},$$

where the inverse exists since by the definition of L_2-sets, $\gcd(M_1M, M_2) = 1$. In addition to being a solution for (14), choosing $i = a$ also provides a solution to (15)

$$1 + a2M_1M \equiv -1 \pmod{2M_2}.$$

Being a unit modulo $2M_2$, we have $\gcd(1 + a2M_1M, 2M_2) = 1$, and therefore,

$$\gcd(1 + a2M_1M, 2M_1M_2) = 1. \tag{16}$$

By the Chinese remainder theorem,

$$q = (1 + a2M_1M) + d2M_1M_2,\ d \in \mathbf{Z} \tag{17}$$

gives the solutions to the system of congruences (14) and (15). By Dirichlet's theorem on arithmetic progressions and (16), there exist infinitely many prime powers q of the form (17).

Now that we have such an odd prime power q as a solution, notice that

$$q_1 \mid M_1M \,\Big|\, \frac{q-1}{2}, \text{ and } q_2 \mid M_2 \,\Big|\, \frac{q+1}{2}. \tag{18}$$

This shows that every element of $L_2(\mathbf{m})$ divides one of $\frac{q-1}{2}$ or $\frac{q+1}{2}$. Since $\frac{q-1}{2}$ and $\frac{q+1}{2}$ are coprime, (18) shows we cannot have $q_1q_2 \,\Big|\, \frac{q\pm1}{2}$, and so $N \in L_2(\mathbf{n})$ cannot exist as an order of any element of $\mathrm{PSL}(2,q)$. By Corollary 5.2.1 applied twice, $(0;0;\mathbf{m})$ has a smooth representation into $\mathrm{PSL}(2,q)$, but for $(0;0;\mathbf{n})$, any representation into $\mathrm{PSL}(2,q)$ must be non-smooth. □

Remark. A natural concern about Proposition 5.2.2 is that its conclusion only provides a smooth finite quotient G for one group $(0;0;\mathbf{m})$ that is non-smooth for the other group $(0;0;\mathbf{n})$, but G may still exist as an outright quotient of $(0;0;\mathbf{n})$. With a few more conditions, Theorem 5.3.1 will put this concern to rest, by producing an appropriate group extension G' of G so that G' is a finite quotient of $(0;0;\mathbf{m})$ but not for $(0;0;\mathbf{n})$.

5.3 Degree of smoothness of quotients

In this section, we state a key theorem for this work. Theorem 5.3.1 and its manifestations will suffice in covering the remaining cases for our relative profinite rigidity problem. We will apply these results in Chapters 6 and 7.

The following theorem generalizes an important observation made in [1].

Theorem 5.3.1. *Let G be a finite group. Fix a surjective homomorphism $\pi\colon (g_1;p_1;\mathbf{m}) \twoheadrightarrow G$ such that $b_1(\ker\pi)$ is maximal among all such surjective maps. If every surjective map $s\colon (g_2;p_2;\mathbf{n}) \twoheadrightarrow G$ satisfies $b_1(\ker s) < b_1(\ker\pi)$, then there is a finite Abelian extension G' of G such that G' is a finite quotient of $(g_1;p_1;\mathbf{m})$ but not for $(g_2;p_2;\mathbf{n})$.*

Proof. Denote $K := \ker \pi$ and $f := b_1(K)$. Let $a > 1$ be such that a is coprime to both $\mathrm{lcm}(\mathbf{m})$ and $\mathrm{lcm}(\mathbf{n})$, or more specifically, the integer $\mathrm{lcm}(\mathbf{m})$ can be replaced with the lcm of all of the cone orders appearing in the signature of K. For our choice of a, we take the subgroup

$$L := K^{(a)}[K, K],$$

which is the join of the commutator subgroup $[K, K]$ with the subgroup $K^{(a)}$ generated by the a-th power elements of K. Since L char $K \trianglelefteq (g_1; p_1; \mathbf{m})$, we see that $L \trianglelefteq (g_1; p_1; \mathbf{m})$. We consider the quotient of $(g_1; p_1; \mathbf{m})$ given by

$$G' := (g_1; p_1; \mathbf{m})/L.$$

By our choice of a, the surjective map $\pi\colon (g_1; p_1; \mathbf{m}) \twoheadrightarrow G$ naturally induces a map $\widetilde{\pi}\colon G' \twoheadrightarrow G$ such that

$$\ker \widetilde{\pi} = K/L \cong (\mathrm{C}_a)^f.$$

This shows that G' is a quotient of $(g_1; p_1; \mathbf{m})$ that is finite.

Suppose by way of contradiction, there is a surjection $t\colon (g_2; p_2; \mathbf{n}) \twoheadrightarrow G'$, and denote $L' := \ker t$. By the hypothesis, we have a composite map $s = \widetilde{\pi} \circ t\colon (g_2; p_2; \mathbf{n}) \twoheadrightarrow G$ with $K' := \ker s$ which satisfies $b_1(K') < f$. It can be seen by the five lemma that there is an isomorphism

$$K'/L' \cong K/L \cong (\mathrm{C}_a)^f.$$

This gives us a surjective map $K' \twoheadrightarrow (\mathrm{C}_a)^f$, implying that (as a result of how a was chosen) that a surjective map $\mathbf{Z}^{b_1(K')} \twoheadrightarrow (\mathrm{C}_a)^f$ exists, which is impossible since $b_1(K') < f$.

We have arrived at a contradiction, and thus, G' cannot be a quotient for $(g_2, p_2; \mathbf{n})$. $\square$

Retaining the notation of Theorem 5.3.1, the hypothesis assumes that the finite group G is a quotient of both groups $(g_1; p_1; \mathbf{m})$ and $(g_2; p_2; \mathbf{n})$. We intuitively think of the maximality conditions on the b_1's as the behavior that G is a quotient that is smoother for the group $(g_1, p_1; \mathbf{m})$ than G is as a quotient for $(g_2, p_2; \mathbf{n})$. For genus 0 lattices, we now aim to formalize some measure of *degree of smoothness* for a quotient G.

Let $\mathbf{c} := (c_1, \ldots, c_k)$ be a tuple that is possibly degenerate. If $c_i \mid m_i$ for every $1 \leq i \leq k$ (which we denote by $\mathbf{c} \mid \mathbf{m}$), then there is the natural projection map

$$p_{\mathbf{c}} \colon (0; 0; m_1, \ldots, m_k) \twoheadrightarrow (0; 0; c_1, \ldots, c_k).$$

In particular, for a finite quotient G of $(0; 0; \mathbf{m})$, there exists a surjection $\pi \colon (0; 0; \mathbf{m}) \twoheadrightarrow G$. If $x_1, \ldots, x_k \in (0; 0; \mathbf{m})$ are the canonical generators with orders $m_1, \ldots, m_k$, respectively, then $\pi(x_i)$ will have some order c_i dividing m_i. This is equivalent to having the map π factor through the map $p_{\mathbf{c}}$.

Definition 10. Let G be a finite group and $\mathbf{c} \mid \mathbf{m}$.

1. G is a $\mathbf{c}$-*smooth quotient* of $(0; 0; \mathbf{m})$, if there exists a surjective map $\pi \colon (0; 0, \mathbf{m}) \twoheadrightarrow G$ that factors through the the natural projection $p_{\mathbf{c}} \colon (0; 0; \mathbf{m}) \twoheadrightarrow (0; 0; \mathbf{c})$. In this case, we say that π is $\mathbf{c}$-*smooth*.

2. G is a $\mathbf{c}$-*maximally smooth quotient* of $(0; 0; \mathbf{m})$, if $\chi(0; 0; \mathbf{c})$ is the smallest such quantity of $\chi(0; 0; \mathbf{c}')$ among all $\mathbf{c}' \mid \mathbf{m}$ and all surjective maps $\pi \colon (0; 0; \mathbf{m}) \twoheadrightarrow G$ such that π factors through $p_{\mathbf{c}'}$. We say that π is $\mathbf{c}$-*maximally smooth*, if G is $\mathbf{c}$-maximally smooth and π is $\mathbf{c}$-smooth.

Remark. Since $\chi(0; 0; \mathbf{m})$ is the lowerbound among the values of $\chi(0; 0; \mathbf{c})$ for $\mathbf{c} \mid \mathbf{m}$, a finite group G is a smooth quotient of $(0; 0; \mathbf{m})$ if and only if G is $\mathbf{m}$-maximally smooth. This observation motivates the above definition as a finer measure on the degree of smoothness for quotients.

We now state important corollaries to Theorem 5.3.1.

Corollary 5.3.2. *Let G be a finite group. Fix surjective homomorphisms*

$$\pi_1 \colon (0; 0; \mathbf{m}) \twoheadrightarrow G \text{ and } \pi_2 \colon (0; 0; \mathbf{n}) \twoheadrightarrow G$$

that are $\mathbf{m}'$-maximally smooth and $\mathbf{n}'$-maximally smooth, respectively. If

$$\chi(0; 0; \mathbf{m}') < \chi(0; 0; \mathbf{n}'),$$

then there exists a finite Abelian extension G' of G such that G' is a finite quotient of $(0; 0; \mathbf{m})$ *but not for* $(0; 0; \mathbf{n})$.

Proof. This follows from Theorem 5.3.1, since (5) and the condition $\chi(0; 0; \mathbf{m}') < \chi(0; 0; \mathbf{n}')$ implies that $b_1(\ker \pi_1) > b_1(\ker \pi_2)$. $\square$

Corollary 5.3.3. *If $\chi(0; 0; \mathbf{m}) \neq \chi(0; 0; \mathbf{n})$, then there exists a group G' that is a finite quotient of one of the groups but not for the other group.*

Proof. Without loss of generality, suppose that $\chi(0; 0; \mathbf{m}) < \chi(0; 0; \mathbf{n})$. Then there exists a finite group G that is a smooth quotient of $(0; 0; \mathbf{m})$ by Theorem 5.1.1. If G is not a quotient of $(0; 0; \mathbf{n})$, then we are done. Otherwise, G is also a quotient of $(0; 0; \mathbf{n})$ and we can directly apply Corollary 5.3.2 to extend G to G' so that G' is a finite quotient of $(0; 0; \mathbf{m})$ but not for $(0; 0; \mathbf{n})$. $\square$

In regards to distinguishing finite quotients between two lattices, we have yet to consider the case when $\chi(0; 0; \mathbf{m}) = \chi(0; 0; \mathbf{n})$, where one of the groups is a triangle group. In this case, we will be finding a way to incorporate Corollary 5.3.2 and will be exploiting features of L_2-sets in Chapter 6.

6. ANALYSIS OF GENUS ZERO CASES

Let $\Delta := \Delta(r, s, t)$ be a triangle group and $\Gamma := (g; p; \mathbf{m})$ be a Fuchsian group. Recall that $b_1(r, s, t) = 0$ and that $b_1(g; p; \mathbf{m}) = 0$ if and only if $g = 0$ and $p \leq 1$. We devote this chapter precisely on these two cases for $(g; p; \mathbf{m})$. Furthermore, we will do so in such a way to accommodate for computations for effective upperbounds performed in Chapter 7, and will closely apply the results from Chapter 5.

Recall that we denote the k-tuple $\mathbf{m} := (m_1, \ldots, m_k)$, where $k \geq 0$.

6.1 Genus 0, Punctures 1

In this section, suppose that $\Delta = \Delta(r, s, t)$ and $\Gamma = (0; 1; \mathbf{m})$, where $\Delta \ncong \Gamma$ and $|\mathbf{m}| \geq 2$. Compared to the next section (where $\Gamma = (0; 0; \mathbf{m})$ will be unpunctured), the punctured case will have a more direct approach.

We now set some notation regarding the kernels of surjective maps coming from our two lattices. Suppose G is a finite quotient that is shared by both groups $\Delta(r, s, t)$ and $(0; 1; \mathbf{m})$. In view of Theorem 5.3.1, we denote K_1 to be the kernel of a surjective map $\Delta(r, s, t) \twoheadrightarrow G$ that maximizes the value of $b_1(K_1)$ among all possible such surjective maps. Similarly, we denote K_2 to be the kernel of a surjective map $(0; 1; \mathbf{m}) \twoheadrightarrow G$ that maximizes the value of $b_1(K_2)$ among all possible such surjective maps. By Riemann-Hurwitz and Proposition 4.4.1, we obtain the following upperbounds on the first Betti numbers

$$b_1(K_1) \leq 2 - |G|\chi(r, s, t) \tag{19}$$

$$b_1(K_2) \leq 1 - |G|\chi(0; 1; \mathbf{m}), \tag{20}$$

where each of the b_1's attain its respective upperbound precisely when G is a smooth quotient for its respective group. By comparing the Euler characteristics of $\Delta(r, s, t)$ and $(0; 1; \mathbf{m})$, we analyze two cases:

Case $\chi(r, s, t) \leq \chi(0; 1; \mathbf{m})$**.**

Suppose that $\chi(r, s, t) \leq \chi(0; 1; \mathbf{m})$. Then for any integer $n > 0$, we have

$$\chi(r, s, t) < \chi(0; 1; \mathbf{m}) + 1/n,$$

and so

$$n\chi(r, s, t) < n\chi(0; 1; \mathbf{m}) + 1,$$

which implies that

$$2 - n\chi(r, s, t) > 1 - n\chi(0; 1; \mathbf{m}), \text{ for every } n.$$

Hence, for a finite smooth quotient G of $\Delta(r, s, t)$ having some order n, we acquire the inequality $b_1(K_1) > b_1(K_2)$, associated to the kernels of each map, see (19) and (20). We can use Theorem 5.1.1 in this case to produce such a G. Then by applying Theorem 5.3.1, we can extend G to G' that is a finite quotient of $\Delta(r, s, t)$ but not for $(0; 1; \mathbf{m})$.

Case $\chi(r, s, t) > \chi(0; 1; \mathbf{m})$**.**

Now suppose that $\chi(r, s, t) > \chi(0; 1; \mathbf{m})$. Since Euler characteristics are rational numbers, we have that $\chi(r, s, t) > \chi(0; 1; \mathbf{m})$, which implies that

$$\chi(r, s, t) - \chi(0; 1; \mathbf{m}) \geq \frac{1}{\operatorname{lcm}(r, s, t, \mathbf{m})}.$$

Hence, for every integer $n > \operatorname{lcm}(r, s, t, \mathbf{m})$, we have the inequality

$$2 - n\chi(r, s, t) < 1 - n\chi(0; 1; \mathbf{m}).$$

If we further assume that $\Delta(r, s, t)^{\mathrm{Ab}} \cong (0; 1; \mathbf{m})^{\mathrm{Ab}}$, then Corollary 4.3.1 shows that $\operatorname{lcm}(\mathbf{m}) = \operatorname{mid}_2(r, s, t)$. Moreover, this implies that $\operatorname{lcm}(\mathbf{m}) \mid \operatorname{lcm}(r, s, t)$, so that

$$\chi(r, s, t) - \chi(0; 1; \mathbf{m}) \geq \frac{1}{\operatorname{lcm}(r, s, t, \mathbf{m})} = \frac{1}{\operatorname{lcm}(r, s, t)}. \tag{21}$$

This then yields

$$2 - n\chi(r, s, t) < 1 - n\chi(0; 1; \mathbf{m}), \tag{22}$$

for every integer $n > \mathrm{lcm}(r, s, t)$.

In either case, we can take G to be a smooth quotient of $(0; 1; \mathbf{m})$ having some order $n > \mathrm{lcm}(r, s, t, \mathbf{m})$. The associated kernels arising from G gives the inequality $b_1(K_1) < b_1(K_2)$. Then by Theorem 5.3.1, we extend G to G' that is a finite quotient of $(0; 1; \mathbf{m})$ but not for $\Delta(r, s, t)$.

What remains to be considered for this case is to be able to construct a smooth finite quotient G of $(0; 1; \mathbf{m})$ having order $n > \mathrm{lcm}(r, s, t, \mathbf{m})$. It suffices to find a group G containing an element of order n. Here, we use Theorem 5.1.1 to generate a smooth representation to $\mathrm{PSL}(2, q)$, where $q := \ell^d$ is an odd prime adhering to the L_2-set $L_2(n, m_1, \ldots, m_k)$, that is, n and each of the m_i divides one of ℓ, $\frac{q-1}{2}$, or $\frac{q+1}{2}$. Consequently, an associated smooth representation $\varphi\colon (0; 1; \mathbf{m}) \to \mathrm{PSL}(2, q)$ will have its image G have order at least n, with φ factoring through the natural projection $(0; 1; \mathbf{m}) \twoheadrightarrow (0; 0; n, m_1, \ldots, m_k)$. Such a smooth representation can be achieved by requiring the sole canonical parabolic generator of $(0; 1; \mathbf{m})$ to map to an order n element in $\mathrm{PSL}(2, q)$.

6.2 Genus 0, Punctures 0

Let $\Delta := \Delta(r, s, t)$ and $\Gamma := (0; 0; m_1, \ldots, m_k)$ such that $\Delta \ncong \Gamma$ and $k \geq 3$.

We will analyze this section with additional assumptions. In light of Proposition 4.3.2 and Corollary 5.3.3, we will aim in restricting to the following

$$\Delta(r, s, t)^{\mathrm{Ab}} \cong (0; 0; \mathbf{m})^{\mathrm{Ab}}, \tag{23}$$

$$\chi(r, s, t) = \chi(0; 0; \mathbf{m}). \tag{24}$$

Given isomorphic Abelianizations (23), we will narrow down the possible sizes $k \geq 3$ for a tuple $\mathbf{m}$ that can satisfy the equality of Euler characteristics (24). The cases when $k = 3$ and $k = 4$ will require most of our attention.

Assume $r, s, t, m_i \geq 2$, for $1 \leq i \leq k$. Every triangle group $\Delta(r, s, t)$ admits the following range of rational values for its Euler characteristic

$$\chi(r, s, t) = \frac{1}{r} + \frac{1}{s} + \frac{1}{t} - 1 \in \left(-1, \frac{1}{2}\right]. \tag{25}$$

On the other hand, notice that the range of values of

$$\chi(0; 0; \mathbf{m}) = \frac{1}{m_1} + \cdots + \frac{1}{m_k} - (k-2) \in \left(-(k-2), \frac{4-k}{2}\right] \tag{26}$$

depends on the size of the k-tuple $\mathbf{m}$. Thus, if $k \geq 6$, then $\chi(0; 0; \mathbf{m}) < \chi(r, s, t)$, regardless of the choice of triangle group $\Delta(r, s, t)$. We can then apply Theorem 5.1.1 to construct some smooth quotient G of $(0; 0; \mathbf{m})$ and Corollary 5.3.3 to obtain the extension G' such that it is a finite quotient of $(0; 0; \mathbf{m})$ but not for $\Delta(r, s, t)$.

The cases that remain are for $k = 3, 4$, and 5. When $k = 4$ or $k = 5$, we compute all of the possible candidates for a tuple $\mathbf{m}$ such that

$$\chi(0; 0; \mathbf{m}) \in \left(-1, \frac{1}{2}\right], \tag{27}$$

as per (24) and (25). Since we are assuming an isomorphism of Abelianizations (23), we will be able to compare $\Delta(r, s, t)$ with each of the candidates $(0; 0; \mathbf{m})$ using either dihedral groups or by Corollary 5.3.3.

Similar methods will not be sufficient for the case when $k = 3$, where both

$$\Delta = \Delta(r, s, t) \text{ and } \Gamma := \Delta(u, v, w)$$

are triangle groups. This will require an analysis of L_2-sets and a result on quotient triangle groups, Lemma 6.2.6. In Section 6.2.4, we will compile a detailed list of numerical restrictions on the profinite invariants of pairs of triangle groups ($k = 3$) that we have observed up to this point.

6.2.1 Case $k = 5$

Let $\Delta := \Delta(r, s, t)$ and $\Gamma := (0; 0; u, v, w, x, y)$, for $r, s, t, u, v, w, x, y \geq 2$, and assume

$$\Delta(r, s, t)^{\mathrm{Ab}} \cong (0; 0; u, v, w, x, y)^{\mathrm{Ab}}.$$

As detailed in (24), we find all the candidate choices of Γ such that

$$\chi(0; 0; u, v, w, x, y) = \chi(r, s, t), \tag{28}$$

and in particular by (27), when

$$\chi(0; 0; u, v, w, x, y) > -1.$$

We will conclude that no such candidates can satisfy (28), and state this as follows.

Proposition 6.2.1. *For any choice of* $\Delta(r, s, t)$ *and* $(0; 0; u, v, w, x, y)$*, if* $\Delta(r, s, t)^{\mathrm{Ab}} \cong (0; 0; u, v, w, x, y)^{\mathrm{Ab}}$*, then* $\chi(r, s, t) \neq \chi(0; 0; u, v, w, x, y)$*.*

Proof. Assume $2 \leq u \leq v \leq w \leq x \leq y$. We will exhaust cases to find u, v, w, x, and y such that

$$\chi(0; 0; u, v, w, x, y) > -1,$$

or equivalently,

$$2 < \frac{1}{u} + \frac{1}{v} + \frac{1}{w} + \frac{1}{x} + \frac{1}{y}. \tag{29}$$

By considering the average value of the summands in the right-hand side of (29), we see that $u < 5/2$. Therefore, $u = 2$ and so

$$\frac{3}{2} < \frac{1}{v} + \frac{1}{w} + \frac{1}{x} + \frac{1}{y}. \tag{30}$$

By applying the average summand argument to the right-hand side of (30), we get $v < 8/3$. Therefore, $v = 2$ and so

$$1 < \frac{1}{w} + \frac{1}{x} + \frac{1}{y}.$$

This gives us $w < 3$ implying that $w = 2$. Thus, we have

$$\frac{1}{2} < \frac{1}{x} + \frac{1}{y},$$

and so $x < 4$ gives us $x = 2$ or $x = 3$.

If $x = 2$, then $0 < \frac{1}{y}$, implying $y \geq 2$ and so we acquire the candidates of the form

$$\Gamma = (0; 0; 2, 2, 2, 2, y). \tag{31}$$

Lastly, if $x = 3$, then $\frac{1}{6} < \frac{1}{y}$, implying $y < 6$, and so we acquire 3 possible candidates

$$\Gamma = (0; 0; 2, 2, 2, 3, 3),\ (0; 0; 2, 2, 2, 3, 4),\ (0; 0; 2, 2, 2, 3, 5). \tag{32}$$

To summarize, only the candidates Γ in (31) and (32) can have the possibility of satisfying $\chi(\Gamma) = \chi(r, s, t)$. We rule out each of these cases from being equal.

Recall our assumption that $\Delta^{\mathrm{Ab}} \cong \Gamma^{\mathrm{Ab}}$. Alongside this, we will also be using Corollary 4.3.1 and Proposition 4.3.2 to finish the proof.

Case $\Gamma = (0; 0; 2, 2, 2, 3, 3)$**.**

If $\chi(0; 0; 2, 2, 2, 3, 3) = \chi(r, s, t)$, then $\frac{1}{6} = \frac{1}{r} + \frac{1}{s} + \frac{1}{t}$. It follows that $r, s, t > 6$, and so $rst > 216$, but after applying Proposition 4.3.2, we have $rst = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 72$, which is a contradiction.

Case $\Gamma = (0; 0; 2, 2, 2, 3, 4)$**.**

If $\chi(0; 0; 2, 2, 2, 3, 4) = \chi(r, s, t)$, then $\frac{1}{12} = \frac{1}{r} + \frac{1}{s} + \frac{1}{t}$. It follows that $r, s, t > 12$, and so $rst > 1728$, but after applying Proposition 4.3.2, we have $rst = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 4 = 96$, which is a contradiction.

Case $\Gamma = (0; 0; 2, 2, 2, 3, 5)$**.**

If $\chi(0; 0; 2, 2, 2, 3, 5) = \chi(r, s, t)$, then $\frac{1}{30} = \frac{1}{r} + \frac{1}{s} + \frac{1}{t}$. It follows that $r, s, t > 30$, and so $rst > 27{,}000$, but after applying Proposition 4.3.2, we have $rst = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 120$, which is a contradiction.

Case $\Gamma = (0; 0; 2, 2, 2, 2, y)$**.**

If $\chi(0; 0; 2, 2, 2, 2, y) = \chi(r, s, t)$, then $\frac{1}{y} = \frac{1}{r} + \frac{1}{s} + \frac{1}{t}$. It follows that $r, s, t > y$, and so $rst > y^3$, but after applying Proposition 4.3.2, we have $rst = 16y$. Hence, $y^3 < 16y$, implying that $y = 2$ or $y = 3$; however, for either case, there are integer solutions $r, s, t \geq 2$ to neither $rst = 32$ nor $rst = 48$.

□

6.2.2 Case $k = 4$

Let $\Delta := \Delta(r, s, t)$ and $\Gamma := (0; 0; u, v, w, x)$, for $r, s, t, u, v, w, x \geq 2$, and assume

$$\Delta(r, s, t)^{\mathrm{Ab}} \cong (0; 0; u, v, w, x)^{\mathrm{Ab}}.$$

Similar to Section 6.2.1, we aim to find all the candidate choices of $\Gamma = (0; 0; u, v, w, x)$ such that

$$\chi(\Gamma) = \chi(r, s, t).$$

In particular, we find u, v, w, x satisfying

$$\chi(0; 0; u, v, w, x) > -1.$$

There will be a glaring difference however: unlike the $k = 5$ case in Proposition 6.2.1, for $k = 4$ there are examples for $\Delta = \Delta(r, s, t)$ and $\Gamma = (0; 0; u, v, w, x)$ such that $\Delta^{\mathrm{Ab}} \cong \Gamma^{\mathrm{Ab}}$ and $\chi(\Delta) = \chi(\Gamma)$. We will handle distinguishing these groups Γ from a triangle group $\Delta(r, s, t)$ later in the section.

Assume $u \leq v \leq w \leq x$. The condition $\chi(0; 0; u, v, w, x) > -1$ is equivalent to

$$1 < \frac{1}{u} + \frac{1}{v} + \frac{1}{w} + \frac{1}{x}. \tag{33}$$

By fixing u, v, and (with one exception) w, we list the finite and infinite families for such candidates $\Gamma = (0; 0; u, v, w, x)$ satisfying (33). We will be applying similar methods to the proof of Proposition 6.2.1.

Finite families.

$$(0;0;2,3,7,\{7 \le x \le 41\})$$
$$(0;0;2,3,8,\{8 \le x \le 23\})$$
$$(0;0;2,3,9,\{9 \le x \le 17\})$$
$$(0;0;2,3,10,\{10,11,12,13,14\})$$
$$(0;0;2,3,11,\{11,12,13\})$$
$$(0;0;2,4,5,\{5 \le x \le 19\})$$
$$(0;0;2,4,6,\{6,7,8,9,10,11\})$$
$$(0;0;2,4,7,\{7,8,9\})$$
$$(0;0;2,4,7,\{7,8,9\})$$
$$(0;0;2,5,5,\{5,6,7,8,9\})$$
$$(0;0;2,5,6,\{6,7\})$$
$$(0;0;3,3,4,\{4 \le x \le 11\})$$
$$(0;0;3,3,5,\{5,6,7\})$$
$$(0;0,3,4,4,\{4,5\})$$

Infinite families.

$$(0;0;2,4,4,\{x \ge 4\})$$
$$(0;0;3,3,3,\{x \ge 3\})$$
$$(0;0;2,3,6,\{x \ge 6\})$$
$$(0;0;2,3,4,\{x \ge 4\})$$
$$(0;0;2,2,\{w \ge 2\},\{x \le w\})$$
$$(0;0;2,3,3,\{x \ge 3\})$$
$$(0;0;2,3,5,\{x \ge 5\})$$

For each of the finite family lattices and as well as for 3 of the infinite family lattices

$$(0;0;2,4,4,\{x\geq 4\}),\ (0;0;3,3,3,\{x\geq 3\}),\ \text{and}\ (0;0;2,3,6,\{x\geq 6\}),$$

we will highlight that the following holds

$$\Delta(r,s,t)^{\mathrm{Ab}}\ncong(0;0;u,v,w,x)^{\mathrm{Ab}}\ \text{or}\ \chi(r,s,t)\neq\chi(0;0;u,v,w,x). \tag{34}$$

Assume that $\chi(r,s,t)=\chi(0;0;u,v,w,x)$, then

$$\frac{1}{u}+\frac{1}{v}+\frac{1}{w}+\frac{1}{x}-1=\frac{1}{r}+\frac{1}{s}+\frac{1}{t},$$

which may be expressed as

$$\frac{1}{\alpha}=\frac{1}{r}+\frac{1}{s}+\frac{1}{t},\ \text{where}\ \alpha:=\frac{1}{\chi(0;0;u,v,w,x)+1}. \tag{35}$$

Notice that $\alpha>0$, since $\chi(0;0;u,v,w,x)>-1$. Equation (35) implies that $r,s,t>\alpha$, and so $rst>\alpha^3$. However, if we also assume that $\Delta(r,s,t)^{\mathrm{Ab}}\cong(0;0;u,v,w,x)^{\mathrm{Ab}}$, then Proposition 4.3.2 provides the equality $rst=uvwx$, but it can be verified that either

1. $uvwx\leq\alpha^3$,
2. $x<w$, or
3. $\mathrm{lcm}(r,s,t)\neq\mathrm{lcm}(u,v,w,x)$,

any one of which would yield a contradiction. This would then confirm that (34) holds.

We are left with 4 remaining lattices Γ, all of which are among the infinite families. We will be able to distinguish Δ and Γ using a dihedral quotient. First, we will require the following proposition.

Proposition 6.2.2. *If $\Delta(r,s,t)^{\mathrm{Ab}}\cong(0;0;u,v,w,x)^{\mathrm{Ab}}$ and $\chi(r,s,t)=\chi(0;0;u,v,w,x)$, then $\{r,s,t\}\cap\{u,v,w,x\}=\varnothing$.*

Proof. The equality of Euler characteristics gives us

$$\frac{1}{u}+\frac{1}{v}+\frac{1}{w}+\frac{1}{x}-1=\frac{1}{r}+\frac{1}{s}+\frac{1}{t},$$

and the hypothesis also ensures that $uvwx = rst$, by Proposition 4.3.2.

Suppose by contradiction that, say, $t = x$. Then it follows that $uvw = rs$ and

$$\frac{1}{u} + \frac{1}{v} + \frac{1}{w} - 1 = \frac{1}{r} + \frac{1}{s}. \tag{36}$$

As with our earlier method for finding our candidate lattices, we can similarly produce candidates (u, v, w) that satisfy (36) for $2 \leq u \leq v \leq w$.

Now since

$$0 < \frac{1}{r} + \frac{1}{s} = \frac{1}{u} + \frac{1}{v} + \frac{1}{w} - 1,$$

we have that

$$1 < \frac{1}{u} + \frac{1}{v} + \frac{1}{w}.$$

This implies that $u < 3$, and so $u = 2$. Therefore,

$$\frac{1}{2} < \frac{1}{v} + \frac{1}{w},$$

and so $v < 4$, which yields $v = 2$ or $v = 3$. If $v = 3$, then $\frac{1}{6} < \frac{1}{w}$, yielding

$$(u, v, w) = (2, 3, \{3, 4, 5\}).$$

Lastly, if $v = 2$, we have $0 < \frac{1}{w}$, yielding

$$(u, v, w) = (2, 2, \{w \geq 2\}).$$

For any of these cases (u, v, w), we have

$$\frac{1}{\alpha} = \frac{1}{r} + \frac{1}{s}, \text{ where } \alpha := \left(\frac{1}{u} + \frac{1}{v} + \frac{1}{w} - 1\right)^{-1} > 0.$$

This implies that $r, s \geq \alpha + 1$, and so $rs \geq (\alpha+1)^2$. Since $rs = uvw$, this implies that $uvw \geq (\alpha+1)^2$. However, it can be verified for each case that $uvw < (\alpha+1)^2$ or $w < v$, which is a contradiction. Thus, we cannot have $t = x$, proving that

$$\{r, s, t\} \cap \{u, v, w, x\} = \varnothing.$$

$\square$

From this proposition, when $\Gamma = (0; 0; 2, 3, 4, \{x \geq 4\})$ or $(0; 0; 2, 2, \{w \geq 2\}, \{x \leq w\})$, we can use Lemma 4.3.3 to distinguish a dihedral quotient between Γ and Δ.

Only the lattices $(0; 0; 2, 3, 3, \{x \geq 3\})$ $(0; 0; 2, 3, 5, \{x' \geq 5\})$ remain. We will let the tuple $\mathbf{n}$ denote either $(2, 3, 3, x)$ or $(2, 3, 5, x')$. We will consider their L_2-sets. Notice if $L_2(\mathbf{n}) \neq L_2(r, s, t)$, then we can apply Proposition 5.2.2 to acquire a smooth finite quotient G for one group that is non-smooth for the other group. Hence, we only need to consider the case when $L_2(\mathbf{n}) = L_2(r, s, t)$.

Lemma 6.2.3. *Suppose that* $(0; 0; \mathbf{n})^{\mathrm{Ab}} \cong \Delta(r, s, t)^{\mathrm{Ab}}$ *and* $\chi(0; 0; \mathbf{n}) = \chi(r, s, t)$. *Then* $L_2(\mathbf{n}) = \{\mathrm{lcm}(\mathbf{n})\}$ *must be a singleton.*

Proof. This follows directly from Proposition 6.2.2 and from the definition of L_2-sets. $\square$

We can characterize that $L_2(2, 3, 3, x) = L_2(r, s, t)$ and $L_2(2, 3, 5, x') = L_2(r, s, t)$ are singletons to precisely the conditions $6 \mid x$ and $30 \mid x'$, respectively. In particular, x and x' are even integers, and therefore we can use Lemma 4.3.3 and Proposition 6.2.2 to distinguish Γ and Δ with a dihedral quotient. This finishes the case $k = 4$.

6.2.3 Case $k = 3$

The last case for this chapter is when $k = 3$, that is, both groups are triangle groups. We let $\Delta := \Delta(r, s, t)$ and $\Gamma := \Delta(u, v, w)$ such that $\Delta \not\cong \Gamma$.

Proposition 6.2.4. *Suppose* $\Delta(r, s, t)^{\mathrm{Ab}} \cong \Delta(u, v, w)^{\mathrm{Ab}}$, $\chi(r, s, t) = \chi(u, v, w)$, *and* $\Delta(r, s, t) \not\cong \Delta(u, v, w)$. *Then*

1. $\gcd(r,s,t) \neq \operatorname{lcm}(r,s,t)$

2. $\{r,s,t\} \cap \{u,v,w\} = \varnothing$.

Proof.

1. By contradiction, suppose that $\gcd(r,s,t) = \operatorname{lcm}(r,s,t)$, which is equivalent to the condition $r = s = t$. By Corollary 4.3.1, this implies that

$$\gcd(u,v,w) = \gcd(r,s,t) = \operatorname{lcm}(r,s,t) = \operatorname{lcm}(u,v,w),$$

and so $r = s = t = u = v = w$, which contradicts that $\Delta(r,s,t) \ncong \Delta(u,v,w)$.

2. The assumptions $\Delta(r,s,t)^{\mathrm{Ab}} \cong \Delta(u,v,w)^{\mathrm{Ab}}$ and $\chi(r,s,t) = \chi(u,v,w)$ provide us with

$$\frac{rs+rt+st}{rst} = \frac{uv+uw+vw}{uvw},$$
$$rst = uvw,$$
$$rs+rt+st = uv+uw+vw,$$

where the second equality comes from Corollary 4.3.2.

Towards a contradiction, assume that $t = w$. This gives

$$rs = uv, \tag{37}$$

and since $rs+rt+st = uv+uw+vw$, we have $rt+st = uw+vw$, and so

$$r+s = u+v. \tag{38}$$

For u and v fixed, the system of equations given by (37) and (38) only has a unique pair of solutions $\{r,s\}$, since they are precisely the roots of the quadratic polynomial $x^2 + (r+s)x + rs$. This contradicts that $\Delta(r,s,t) \ncong \Delta(u,v,w)$.

$\square$

As with Proposition 4.3.3, one suitable situation for the proposition above will be in distinguishing two triangle groups using a dihedral quotient. However, Proposition 6.2.4 will also be important for comparing the L_2-sets $L_2(r,s,t)$ and $L_2(u,v,w)$.

When $L_2(r,s,t) \neq L_2(u,v,w)$, Proposition 5.2.2 showcases a solution as not to warrant further attention for this chapter. It then remains to consider the case when $L_2(r,s,t) = L_2(u,v,w)$.

Lemma 6.2.5. *If $\Delta(r,s,t) \not\cong \Delta(u,v,w)$, $\Delta(r,s,t)^{\mathrm{Ab}} \cong \Delta(u,v,w)^{\mathrm{Ab}}$, and $L_2(r,s,t) = L_2(u,v,w)$, then $L_2(r,s,t) = L_2(u,v,w) = \{\mathrm{lcm}(r,s,t)\}$ is a singleton.*

Proof. Notice when $L_2(r,s,t) = L_2(u,v,w)$ is not a singleton set, then either

$$|L_2(r,s,t)| = 2 \text{ or } |L_2(r,s,t)| = 3.$$

For the case $|L_2(r,s,t)| = 3$, we have

$$\{r,s,t\} = L_2(r,s,t) = L_2(u,v,w) = \{u,v,w\}.$$

When $|L_2(r,s,t)| = 2$, suppose that after possibly permuting the entries of each tuple (r,s,t) and (u,v,w), we have

$$\{r, \mathrm{lcm}(s,t)\} = L_2(r,s,t) = L_2(u,v,w) = \{u, \mathrm{lcm}(v,w)\}, \tag{39}$$

which as a consequence of the definition of L_2-sets we have that

$$\begin{aligned}
\gcd(r,st) &= 1 \\
\gcd(u,vw) &= 1 \\
\gcd(s,t) &> 1 \\
\gcd(v,w) &> 1.
\end{aligned}$$

From (39), if $r = u$, then we are done, so we may assume that

$$r = \mathrm{lcm}(v, w) \text{ and } u = \mathrm{lcm}(s, t). \tag{40}$$

Comparing mid_2's, we have that

$$\mathrm{mid}_2(r, s, t) = \mathrm{lcm}(\gcd(r, s), \gcd(r, t), \gcd(s, t)) = \gcd(s, t)$$
$$\mathrm{mid}_2(u, v, w) = \mathrm{lcm}(\gcd(u, v), \gcd(u, w), \gcd(v, w)) = \gcd(v, w).$$

Furthermore, since by Corollary 4.3.1 we have $\mathrm{mid}_2(r, s, t) = \mathrm{mid}_2(u, v, w)$, this implies that $\gcd(s, t) = \gcd(v, w) > 1$, which contradicts $\gcd(r, st) = 1$ because by (40), $\gcd(v, w) \mid r$.

Therefore, every viable case encountered above results in having $\{r, s, t\} \cap \{u, v, w\} \neq \varnothing$, contradicting Proposition 6.2.4. This proves $|L_2(r, s, t)| = |L_2(u, v, w)| = 1$. □

We conclude this section with the situation when $L_2(r, s, t) = L_2(u, v, w) = \{\mathrm{lcm}(r, s, t)\}$ is a singleton.

Proposition 6.2.6. *Suppose that*

$$\Delta(r, s, t) \ncong \Delta(u, v, w),$$
$$\Delta(r, s, t)^{\mathrm{Ab}} \cong \Delta(u, v, w)^{\mathrm{Ab}},$$
$$\chi(r, s, t) = \chi(u, v, w),$$
$$L_2(r, s, t) = L_2(u, v, w) = \{\mathrm{lcm}(r, s, t)\}.$$

Then there exists a finite group G such that G is a (r', s', t')-maximally smooth quotient of $\Delta(r, s, t)$ and is a (u', v', w')-maximally smooth quotient of $\Delta(u, v, w)$, chosen in such a way so that $\chi(r', s', t') \neq \chi(u', v', w')$.

Proof. Recall from Proposition 6.2.4 that $\gcd(r, s, t) \neq \mathrm{lcm}(r, s, t)$. We define the integers r', s', t', u', v', and w' based on the following two cases. For a prime p, we take $\nu_p \colon \mathbf{Q}^\times \to \mathbf{Z}$ to denote the p-adic valuation.

1. Suppose $\mathrm{mid}_2(r,s,t) \neq \mathrm{lcm}(r,s,t)$. Then there exists a prime p such that

$$\nu_p(\mathrm{mid}_2(r,s,t)) < \nu_p(\mathrm{lcm}(r,s,t)). \tag{41}$$

   By possibly permuting (r,s,t) and (u,v,w), we define

$$(r',s',t') := (r/p, s, t)$$
$$(u',v',w') := (u/p, v, w),$$

   where r and u are taken such that $\nu_p(r) = \nu_p(u) = \nu_p(\mathrm{lcm}(r,s,t))$.

   If one of r,u is equal to p, say $r = p$, then by how p is chosen in (41), we must have $\gcd(p, st) = 1$. This contradicts that $L_2(r,s,t)$ is a singleton, and therefore, we have eliminated the possibility of having $r' = 1$ and $u' = 1$.

2. Suppose $\mathrm{mid}_2(r,s,t) = \mathrm{lcm}(r,s,t)$. Since $\gcd(r,s,t) \neq \mathrm{lcm}(r,s,t)$, there exists a prime p such that

$$\nu_p(\gcd(r,s,t)) < \nu_p(\mathrm{mid}(r,s,t)) = \nu_p(\mathrm{lcm}(r,s,t)). \tag{42}$$

   Then by possibly permuting each tuple, we define

$$(r',s',t') := (r/p, s/p, t)$$
$$(u',v',w') := (u/p, v/p, w),$$

   where $r,s,u,$ and v are taken so that $\nu_p(r) = \nu_p(s) = \nu_p(u) = \nu_p(v) = \nu_p(\mathrm{lcm}(r,s,t))$.

   We show that r,s,u,v cannot be equal to p. Suppose by contradiction that, say, $r = p$. Then by how we chose p in (42), we can assume $p \nmid t$ and $s = pd$ for some d coprime to p. For $L_2(r,s,t)$ to be a singleton set, we must have that $\gcd(d,t) > 1$. Notice also that

$$\mathrm{mid}_2(r,s,t) = \mathrm{lcm}(r,s,t) \implies p \cdot \gcd(d,t) = p \cdot \mathrm{lcm}(d,t).$$

Hence, $d = t$, and so $(r, s, t) = (p, pt, t)$ with $\gcd(p, t) = 1$. However, for u, v, w to satisfy

$$\begin{aligned}\gcd(u, v, w) &= \gcd(p, pt, t) = 1\\ \mathrm{mid}_2(u, v, w) &= \mathrm{mid}_2(p, pt, t) = pt\\ \mathrm{lcm}(u, v, w) &= \mathrm{lcm}(p, pt, t) = pt,\end{aligned}$$

we must have $\Delta(u, v, w) \cong \Delta(r, s, t)$, which is a contradiction. Therefore, none of r', s', u', v' can be equal to 1.

Regarding Euler characteristics, since

$$\chi(r, s, t) = \chi(u, v, w) \text{ and } \{r, s, t\} \cap \{u, v, w\} = \varnothing,$$

where the latter comes from Proposition 6.2.4, it follows that in either case,

$$\chi(r', s', t') \neq \chi(u', v', w').$$

Notice from our construction of the two cases, by setting

$$\begin{aligned}L' &:= \mathrm{lcm}(r', s', t') = \mathrm{lcm}(u', v', w')\\ L &:= \mathrm{lcm}(r, s, t) = \mathrm{lcm}(u, v, w),\end{aligned}$$

then we have $pL' = L \geq 2$. To finish this proof, it remains to show there exists a finite group G that is a (r', s', t')-maximally smooth quotient of $\Delta(r, s, t)$ and is a (u', v', w')-maximally smooth quotient of $\Delta(u, v, w)$, which follows from Theorem 5.1.1 and the ensuing lemma. $\square$

Lemma 6.2.7. *Retain the notation in Proposition 6.2.6. For $pL' = L \geq 2$, there exists an odd prime power q such that* $\mathrm{PSL}(2, q)$ *has an element of order L', but with no element of order L.*

Proof. It suffices to show there is an odd prime power q that solves the following

$$q \equiv 1 \pmod{2L'} \tag{43}$$

$$q \not\equiv \pm 1 \pmod{2L}. \tag{44}$$

The first congruence (43) yields the set of solutions $q = 1 + i2L'$, for $i \in \mathbf{Z}$. Observe that every choice of $1 \leq i \leq p-1$ (recall $pL' = L$) satisfies (44):

$$1 + i2L' \not\equiv \pm 1 \pmod{2L}.$$

In accordance with Dirichlet's theorem, we aim to prove that there exists $1 \leq i \leq p-1$ such that

$$\gcd(1 + i2L', 2L) = 1.$$

It suffices to show that either $i = 1$, i.e, $q = 1 + 2L$, or $i = 2$, i.e., $q = 1 + 4L$, works to complete the proof.

Let ℓ be an arbitrary prime such that $\ell \mid 2L'$. Then also $\ell \mid 2L$ and $\ell \nmid (1 + i2L')$, for any integer i. Specializing to the prime $\ell = p$ for the occasion where $p \mid 2L'$ (recall that $pL' = L$), notice that $2L'$ and $2L$ have an identical list of prime factors. Therefore, $\gcd(1+2L', 2L) = 1$, and we can take $i = 1$ for the case when $p \mid 2L'$. Otherwise, we consider the case where $p \nmid 2L'$, which means the prime p is the only difference between the list of prime factors of $2L'$ and $2L$. Then for this case, either $p \nmid (1 + 2L')$ or $p \nmid (1 + 4L')$. This implies that $\gcd(1 + i2L', 2L) = 1$, where $i = 1$ or $i = 2$, depending on when $p \nmid (1 + i2L')$ holds true.

For our choice of i in either case, we set $q = (1 + i2L') + k2L$, for $k \in \mathbf{Z}$, as a solution to (44). Furthermore, $i = 1$ or $i = 2$ had been chosen so that $\gcd(1 + i2L', 2L) = 1$. This allows us to invoke Dirichlet's theorem that there is an odd prime power of the form $q = (1 + i2L') + k2L$, for some $k \in \mathbf{Z}$ such that it satisfies (43) and (44). Therefore,

$$L' \,\Big|\, \frac{q-1}{2}\,, \text{ but } L \,\not\Big|\, \frac{q \pm 1}{2},$$

and so $\mathrm{PSL}(2, q)$ contains an element of order L', but not an element of order L. $\square$

Remark. We highlight important observations in our constructions of (r', s', t'), (u', v', w'), and q from Proposition 6.2.6 and Lemma 6.2.7.

1. $L' := \operatorname{lcm}(r', s', t') = \operatorname{lcm}(u', v', w')$, $L := \operatorname{lcm}(r, s, t) = \operatorname{lcm}(u, v, w)$, and $pL' = L$. In particular, $L' \neq L$.

2. If $\Delta(r, s, t) \twoheadrightarrow \Delta(a, b, c) \twoheadrightarrow \Delta(r', s', t')$ and $\Delta(a, b, c) \ncong \Delta(r', s', t')$, then

$$L_2(a, b, c) = L_2(r, s, t) = \{L\} \text{ and } \operatorname{lcm}(a, b, c) = L.$$

3. If $\Delta(u, v, w) \twoheadrightarrow \Delta(x, y, z) \twoheadrightarrow \Delta(u', v', w')$ and $\Delta(x, y, z) \ncong \Delta(u', v', w')$, then

$$L_2(x, y, z) = L_2(u, v, w) = \{L\} \text{ and } \operatorname{lcm}(x, y, z) = L.$$

4. For a, b, c as above, there is an odd prime q such that $\Delta(r', s', t')$ has a smooth representation to $\mathrm{PSL}(2, q)$, but $\Delta(a, b, c)$ has no smooth representations to $\mathrm{PSL}(2, q)$.

5. For x, y, z, and q as above, $\Delta(u', v', w')$ has a smooth representation to $\mathrm{PSL}(2, q)$, but $\Delta(x, y, z)$ has no smooth representations to $\mathrm{PSL}(2, q)$.

6. $\chi(r', s', t') \neq \chi(u', v', w')$.

6.2.4 Numerical restrictions for $k = 3$

We now provide a list of numerical restrictions on pairs of triangle groups based on our survey of Abelian quotients, dihedral quotients, and smooth PSL_2 representations.

Proposition 6.2.8. *Assume $\Delta(r, s, t) \ncong \Delta(u, v, w)$ and that both triangle groups have an identical collection of finite quotients. Then we have the (possibly redundant) conditions.*

(1) $\gcd(r, s, t) = \gcd(u, v, w)$,

(2) $\operatorname{mid}_2(r, s, t) = \operatorname{mid}_2(u, v, w)$,

(3) $1/r + 1/s + 1/t = 1/u + 1/v + 1/w < 1$,

(4) $\operatorname{lcm}(r,s,t) = \operatorname{lcm}(u,v,w)$,

(5) $\gcd(r,s,t) \neq \operatorname{lcm}(r,s,t)$ *and* $\gcd(u,v,w) \neq \operatorname{lcm}(u,v,w)$,

(6) $rst = uvw$,

(7) $rs + st + rt = uv + vw + uw$,

(8) $\{r,s,t\} \cap \{u,v,w\} = \varnothing$,

(9) *at most one entry of* (r,s,t) *and at most one entry of* (u,v,w) *are even, and*

(10) $L_2(r,s,t) = L_2(u,v,w) = \{\operatorname{lcm}(r,s,t)\}$.

Using the complexity $N := rst = uvw \leq$ 12,000,000, we computed pairs of distinct hyperbolic triangle groups subjected to these conditions via GAP [14]. We were able to confirm from [1] that there are 3581 pairs of triangle groups exhibiting conditions (1)–(9). Furthermore, we found exactly 1848 pairs of triangle groups under the conditions (1)–(10).

7. ALGORITHM AND EFFECTIVE UPPERBOUNDS

In this chapter, we provide an algorithm for distinguishing a cocompact triangle group $\Delta := \Delta(r, s, t)$ from a Fuchsian group $\Gamma := (g; p; \mathbf{m})$, where $\mathbf{m} = (m_1, \ldots, m_k)$ is an unordered (and possibly empty) tuple. The results from Chapters 4, 5, and 6 will be used to construct these finite quotients.

In finding upperbounds on distinguishing finite quotients, we will require bounds on the odd prime powers q obtained from Theorem 5.1.1. The following result from Linnik [15] [16] and improved by Xylouris [17] is an effective version of Dirichlet's theorem on primes in arithmetic progressions.

Theorem 7.0.1. *Let a and D be coprime positive integers with $a < D$. Then there exists $k \geq 0$ such that $a + kD$ is prime, and if p is the lowest such prime of this form, then $p < cD^5$, where c is an effectively computable constant which is independent of choice of a and D.*

We now state our main result which establishes both the relative profinite rigidity and the effective upperbound on a distinguishing finite quotient. For real valued functions $f(N, k)$ and $g(N, k)$, we denote by $f \ll g$ to mean there exists $M, C > 0$ such that for all $N, k \geq M$, we have $|f(N, k)| \leq C|g(N, k)|$.

Theorem 7.0.2. *Let $\Delta := \Delta(r, s, t)$, $\Gamma := (g; p; \mathbf{m})$, and $k := |\mathbf{m}| \geq 0$ such that $\Delta \not\cong \Gamma$. Define $N := \max\{\mathrm{lcm}(r, s, t), \mathrm{lcm}(\mathbf{m})\}$. Then there exists a finite group Q having order*

$$|Q| \ll N^{(k+3)N^{15}}$$

such that Q is a quotient for one of the groups, but not for the other group.

7.1 Proof of Theorem 7.0.2

Begin with $\Delta := \Delta(r, s, t)$ and $\Gamma := (g; p; \mathbf{m})$ such that $\Delta \not\cong \Gamma$, with $\mathbf{m} := (m_1, \ldots, m_k)$ and $k \geq 0$. We prove Theorem 7.0.2 by showcasing an algorithm broken up into several cases which are not necessarily disjoint.

For ease of readability, we set $L := \mathrm{lcm}(r, s, t)$ and $M := \mathrm{lcm}(\mathbf{m})$.

Both are non-hyperbolic.

For this case, we will relax the restriction of having Δ be a triangle group. Assume both Δ and Γ are non-hyperbolic lattices. We refer to Section 3.2.2 where we listed each of the spherical and Euclidean lattices.

1. **Both are spherical:** When both Δ and Γ are spherical, they are non-isomorphic finite groups, so one of these lattices (denote by G) will suffice as a distinguishing finite quotient. Since a spherical lattice is isomorphic to either C_n, D_{2n}, A_4, S_4, or A_5, we have an upperbound given by

$$|G| \leq \max\{60, 2r, 2s, 2t, 2m_1, \ldots, 2m_k\}.$$

2. **One spherical, one Euclidean:** Without loss of generality, suppose Δ is spherical (hence a finite group) and Γ is Euclidean. Take d to be the smallest positive integer such that there does not exist an element of order d in the group Δ. The Euclidean lattices are of the form

$$\Gamma \cong \mathbf{Z}^i \rtimes \mathrm{C}_k, \text{ where } i \in \{1, 2\} \text{ and } k \in \{1, 2, 3, 4, 6\}.$$

Hence, Γ has a quotient $\mathrm{C}_d^i \rtimes \mathrm{C}_k$ that contains an element of order d and therefore cannot be a quotient of Δ. The group $\mathrm{C}_d^i \rtimes \mathrm{C}_k$ has order $kd^i \leq 6(1 + |\Delta|)^2$.

3. **Both Euclidean:** If Δ and Γ are both Euclidean, we can compare them solely through their Abelianizations:

$$
\begin{aligned}
(0;2;-)^{\mathrm{Ab}} &\cong \mathbf{Z} \\
(1;0;-)^{\mathrm{Ab}} &\cong \mathbf{Z}^2 \\
(0;1;2,2)^{\mathrm{Ab}} &\cong \mathrm{C}_2 \times \mathrm{C}_2 \\
(0;0;2,2,2,2)^{\mathrm{Ab}} &\cong \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2 \\
\Delta(2,3,6)^{\mathrm{Ab}} &\cong \mathrm{C}_2 \\
\Delta(2,4,4)^{\mathrm{Ab}} &\cong \mathrm{C}_2 \times \mathrm{C}_4 \\
\Delta(3,3,3)^{\mathrm{Ab}} &\cong \mathrm{C}_3 \times \mathrm{C}_3.
\end{aligned}
$$

The largest finite Abelianization appearing above has order 9. Notice that when Δ or Γ is one of $(0;2;-)$ or $(1;0;-)$, either the cyclic group C_{10} or the 2-generated group $\mathrm{C}_2 \times \mathrm{C}_2$ will suffice as a distinguishing quotient.

We now assume that at least one of the lattices $\Delta(r,s,t)$ and $(g;p;\mathbf{m})$ is hyperbolic.

Different Abelianizations.

Suppose $\Delta(r,s,t)^{\mathrm{Ab}} \not\cong (g;p;\mathbf{m})^{\mathrm{Ab}}$. We consider the cases for which the Abelianization $(g;p;\mathbf{m})^{\mathrm{Ab}}$ is an infinite or a finite group:

1. **Case $g > 0$ or $p > 1$:** This condition suffices for $\Delta(r,s,t)^{\mathrm{Ab}} \not\cong (g;p;\mathbf{m})^{\mathrm{Ab}}$, since $b_1(g;p;\mathbf{m}) > 0$ but $b_1(r,s,t) = 0$. We can then take the cyclic group $G := \mathrm{C}_{1+\mathrm{mid}_2(r,s,t)}$ which is a finite quotient of $(g;p;\mathbf{m})$, but not for $\Delta(r,s,t)$. The order of the group is $|G| = 1 + \mathrm{mid}_2(r,s,t)$.

2. **Case $g = 0$ and $p \leq 1$:** In this case, both $\Delta(r,s,t)^{\mathrm{Ab}} \not\cong (0;p;\mathbf{m})^{\mathrm{Ab}}$ are finite groups. Take G to be the Abelianization having larger order, or either Abelianization in the case of a tie. We have that G is a finite quotient for one of groups Δ or Γ, but not for the other group. The order of such a G has an upperbound of $|G| \leq \max\{rst, m_1 \ldots m_k\}$.

Same Abelianizations.

Suppose $\Delta(r,s,t)^{\mathrm{Ab}} \cong (g;p;\mathbf{m})^{\mathrm{Ab}}$. Necessarily, we have $g = 0$ and $p \leq 1$. Setting $g = 0$, we will consider the cases for which Γ is unpunctured or 1-punctured. The case $p = 1$ is a relatively straightforward application, but the case $p = 0$ requires considerably more effort.

1. **Case $p = 1$:** Suppose $\Delta(r, s, t)^{\mathrm{Ab}} \cong (0; 1; \mathbf{m})^{\mathrm{Ab}}$. By Proposition 4.2.1, we have that

$$\mathrm{mid}_2(r, s, t) = \mathrm{lcm}(\mathbf{m}),$$

and consequently,

$$M = \mathrm{lcm}(\mathbf{m}) \mid \mathrm{lcm}(r, s, t) = L \text{ and } \mathrm{lcm}(r, s, t, \mathbf{m}) = \mathrm{lcm}(r, s, t).$$

We proceed by comparing Euler characteristics:

(a) $\chi(r, s, t) \leq \chi(0; 1; \mathbf{m})$**:** We take $q := \ell^d$ to be the smallest odd prime power satisfying the following: each of r, s, t divides one of $\ell, \frac{q-1}{2}, \frac{q+1}{2}$. By Theorem 7.0.1, $q \ll L^5$. By Theorem 5.1.1, there exists a group $G \leq \mathrm{PSL}(2, q)$ that is (r, s, t)-smooth. The group G has order $|G| \leq |\,\mathrm{PSL}(2, q)| \leq q^3 \ll L^{15}$. Now, take an integer $a > 1$ such that a and M are coprime, for example, $a = M - 1 < L$. Then using Theorem 5.3.1, we can construct the group G', an extension of G by the group C_a^f, where $f := 2 - |G|\chi(r, s, t)$ from Proposition 4.4.1. We have that $f < 2 + |G| \ll L^{15}$ and that G' is a quotient of $\Delta(r, s, t)$, but not for $(0; 1; \mathbf{m})$. Hence $|G'| = a^f|G| \ll L^{L^{15}}L^{15} \approx L^{L^{15}}$.

(b) $\chi(r, s, t) > \chi(0; 1; \mathbf{m})$**:** We take $q := \ell^d$ to be the smallest odd prime power such that the integer $\mathrm{lcm}(r, s, t)$ divides one of $\ell, \frac{q-1}{2}, \frac{q+1}{2}$. Recall that $\mathrm{lcm}(\mathbf{m})$ divides $\mathrm{lcm}(r, s, t)$, so therefore each of the $m_i \mid \mathrm{lcm}(r, s, t)$. This is useful because in the perspective of Corollary 5.2.1, we want to employ the L_2-set $L_2(m_1, \ldots, m_k, \mathrm{lcm}(r, s, t)) = \{\mathrm{lcm}(r, s, t)\}$. By Theorem 7.0.1, we have $q \ll L^5$. By Corollary 5.2.1, there exists a group $G \leq \mathrm{PSL}(2, q)$ that is a smooth quotient of $(0; 1; \mathbf{m})$, where we map the canonical parabolic generator of $(0; 1; \mathbf{m})$ to an element in $\mathrm{PSL}(2, q)$ having order $\mathrm{lcm}(r, s, t)$. If necessary, we may adjust our smooth representation $(0; 1; \mathbf{m}) \to \mathrm{PSL}(2, q)$, so that the image G is not cyclic, thereby guaranteeing that $|G| > \operatorname{lcm}(r, s, t)$. Recall from Section 6.1, having that $|G| > \operatorname{lcm}(r, s, t)$ ensures that any representation $\Delta(r, s, t) \to \mathrm{PSL}(2, q)$ cannot be smooth. The group G has order $|G| \leq |\mathrm{PSL}(2, q)| \ll L^{15}$. Now, take an integer $a > 1$ such that a and L are coprime, say, $a = L - 1$. By Theorem 5.3.1, we construct the group extension G' of the group G by C_a^f, where $f := 1 - |G|\chi(0; 1; \mathbf{m})$ from Proposition 4.4.1. Notice that $f < 1 + |G|(k-1) \ll kL^{15}$ and that G' is a quotient of $(0; 1; \mathbf{m})$, but not for $\Delta(r, s, t)$. We see that

$$|G'| = a^f |G| \ll L^{kL^{15}} L^{15} \approx L^{kL^{15}}.$$

2. **Case** $p = 0$**:** Suppose $\Delta(r, s, t)^{\mathrm{Ab}} \cong (0; 0; \mathbf{m})^{\mathrm{Ab}}$. In particular, from Proposition 4.2.1, we have

$$\gcd(r, s, t) = \operatorname{mid}_{k-2}(\mathbf{m}) \text{ and } \operatorname{mid}_2(r, s, t) = \operatorname{mid}_{k-1}(\mathbf{m});$$

however, there is generally no relationship between $L := \operatorname{lcm}(r, s, t)$ and $M := \operatorname{lcm}(\mathbf{m})$. We consider some straightforward cases, leaving behind $|\mathbf{m}| = 3, 4$ for further analyses.

   (a) $\chi(r, s, t) < \chi(0; 0; \mathbf{m})$**:** We can precisely mirror the construction and retain the notation of the earlier case $\chi(r, s, t) \leq \chi(0; 1; \mathbf{m})$. The only notable difference is there is in general no relation between the integers L and M, but the groups G and G' as well as the quantities q, a, and f are defined the same way as before. By Corollary 5.3.3, G' is a quotient of $\Delta(r, s, t)$, but not for $(0; 0; \mathbf{m})$. Accounting for the lack of relationship between L and M, the computation of the upperbound for the order of this quotient gives $|G'| \ll M^{L^{15}}$.

   (b) $\chi(r, s, t) > \chi(0; 0; \mathbf{m})$**:** This is the same as the previous case, but with the roles of $\Delta(r, s, t)$ and $(0; 0; \mathbf{m})$ reversed. We take $q := \ell^d$ to be the smallest odd prime power satisfying the following: each of the m_i divides one of $\ell, \frac{q-1}{2}, \frac{q+1}{2}$. By Theorem 7.0.1, $q \ll M^5$. By Theorem 5.1.1, there exists a group $G \leq \mathrm{PSL}(2, q)$ that is $\mathbf{m}$-smooth. The group G has order $|G| \leq |\mathrm{PSL}(2, q)| \leq q^3 \ll M^{15}$. Now, take an integer $a > 1$ such that a and L are coprime, for example, $a = L - 1$. Then by Corollary 5.3.3, we can construct the group G', an extension of G by the group C_a^f, where $f := 2 - |G|\chi(0;0;\mathbf{m})$. Notice that $f < 2 + |G|(k-2) \ll kM^{15}$, and that G' is a quotient of $(0;0;\mathbf{m})$ but not for $\Delta(r,s,t)$. Hence,

$$|G'| = a^f|G| \ll L^{kM^{15}}M^{15} \approx L^{kM^{15}}.$$

(c) $|\mathbf{m}| \geq 6$**:** This case guarantees the inequality $\chi(r,s,t) > \chi(0;0;\mathbf{m})$ above.

(d) $|\mathbf{m}| = 5$**:** This case guarantees the inequality $\chi(r,s,t) \neq \chi(0;0;\mathbf{m})$ above.

(e) $|\mathbf{m}| \leq 2$**:** $(0;0;\mathbf{m}) \cong C_a$ is a finite cyclic group (and a spherical lattice). By Proposition 4.2.1, this forces $\gcd(r,s,t) = 1$ and $\mathrm{mid}_2(r,s,t) = a$. This data specifies that exactly one of r,s,t, say r, is coprime to a. We can use Theorems 5.1.1 and 7.0.1 to produce a group $G \leq \mathrm{PSL}(2,q)$ that is (r,s,t)-smooth with $q \ll L^5$. This construction ensures that G contains an element of order r, so that G cannot be a quotient of $(0;0;\mathbf{m}) \cong C_a$. The upperbound on the order of G is $|G| \ll L^{15}$.

Same Euler characteristics, Same Abelianizations, $g = 0,\ p = 0$**.**

We now append the condition

$$\chi(r,s,t) = \chi(0;0;\mathbf{m}).$$

Since we also have $\Delta(r,s,t)^{\mathrm{Ab}} \cong (0;0;\mathbf{m})^{\mathrm{Ab}}$, Proposition 4.3.2 provides us with

$$L = \mathrm{lcm}(r,s,t) = \mathrm{lcm}(\mathbf{m}) = M \text{ and } rst = m_1 \dots m_k.$$

1. **Different** L_2**-sets:** Suppose $L_2(r,s,t) \neq L_2(0;0;\mathbf{m})$. To proceed, we will highlight the proof of Proposition 5.2.2: switching the roles of (r,s,t) and $\mathbf{m}$ if necessary, there are distinct maximal prime power factors q_1 and q_2 of $\mathrm{lcm}(r,s,t) = \mathrm{lcm}(\mathbf{m})$ such that

for some $R \in L_2(r,s,t)$, $q_1q_2 \mid R$ but $q_1 \mid M_1$ and $q_2 \mid M_2$ for distinct $M_1, M_2 \in L_2(\mathbf{m})$. We take the smallest odd prime power $q = \ell^d$ satisfying

$$q \equiv 1 \pmod{2M_1K}$$
$$q \equiv -1 \pmod{2M_2},$$

where K is the product of each element in $L_2(\mathbf{m})\backslash\{M_1, M_2\}$ (with $K = 1$, for the empty product). By Chinese remainder theorem, the solution to the system of congruences above will be unique modulo

$$2M_1M_2K = 2\operatorname{lcm}(\mathbf{m}) = 2\operatorname{lcm}(r,s,t) = 2L.$$

Therefore, by Theorem 7.0.1, $q \ll L^5$. By our choice of q and by Corollary 5.2.1 (applied twice), there is a smooth representation $(0;0;\mathbf{m}) \to \mathrm{PSL}(2,q)$ such that every map $\Delta(r,s,t) \to \mathrm{PSL}(2,q)$ cannot be smooth. Take G to be the image under the smooth representation, with order $|G| \le |\mathrm{PSL}(2,q)| \ll L^{15}$. We take an integer $a > 1$ that is coprime to L, say $a = L-1$. Now we apply Corollary 5.3.2 to obtain the group extension G' of G by the group C_a^f, where

$$f := 2 - |G|\chi(0;0;\mathbf{m}) = 2 - |G|\chi(r,s,t) < 2 + |G| \ll L^{15}.$$

Then G' is a finite quotient of $(0;0;\mathbf{m})$ but not for $\Delta(r,s,t)$. The upperbound for the order is $|G'| = a^f|G| \ll L^{L^{15}}L^{15} \approx L^{L^{15}}$.

Same L_2-sets, Same χ's, Same Abelianizations, $g = 0$, $p = 0$, and $|\mathbf{m}| = 3, 4$.

We now consider $\Delta = \Delta(r,s,t)$ and $\Gamma = (0;0;\mathbf{m})$, where $|\mathbf{m}| = 3,4$. Additionally, we assume that our L_2-sets are identical: $L_2(r,s,t) = L_2(\mathbf{m})$.

1. **Case $|\mathbf{m}| = 4$:** Let $\Delta = \Delta(r,s,t)$ and $\Gamma = (0;0;u,v,w,x)$, with $u \le v \le w \le x$. We consider the results in Section 6.2.2. We will consider viable choices of tuples (u,v,w,x) that adhere to all of the restrictions above:

(a) **Dihedral groups:** We can use Proposition 6.2.2 to distinguish many of the viable candidates $(0; 0; u, v, w, x)$ from $\Delta(r, s, t)$ by using a dihedral group G. For the purposes of this algorithm, the necessary candidates for Γ to mark that can be distinguished using some dihedral quotient of Δ or Γ are as follows: $(0; 0; 2, 4, 4, x)$, $(0; 0; 2, 2, w, x)$, $(0; 0; 2, 3, 4, x)$, $(0; 0; 2, 3, 6, x)$, $(0; 0; 2, 3, 3, x)$, and $(0; 0; 2, 3, 5, x)$. We determined in Section 6.2.2 that the latter two groups

$$(0; 0; 2, 3, 3, x) \text{ and } (0; 0; 2, 3, 5, x')$$

require that x and x' be even, by the assumption that $L_2(r, s, t) = L_2(\mathbf{m})$. The upperbound on the order for a distinguishing dihedral quotient is

$$|G| \leq 2 \max\{r, s, t, u, v, w, x\}.$$

2. **Case $|\mathbf{m}| = 3$:** Let $\Delta = \Delta(r, s, t)$ and $\Gamma = \Delta(u, v, w)$ be two triangle groups. From Lemma 6.2.5, we have that

$$L_2(r, s, t) = L_2(u, v, w) = \{\mathrm{lcm}(r, s, t)\}$$

is a singleton set. To proceed, we state and apply Lemma 6.2.6, for which we will make effective: there exists

$$r' \mid r,\ \ s' \mid s,\ \ t' \mid t,\ \ u' \mid u,\ \ v' \mid v \text{ and } w' \mid w,$$

such that

$$\chi(r', s', t') \neq \chi(u', v', w') \text{ and } \mathrm{lcm}(r', s', t') = \mathrm{lcm}(u', v', w') \neq \mathrm{lcm}(r, s, t).$$

Moreover, r', s', t' can be chosen so that whenever

$$(r'', s'', t'') \neq (r', s', t') \text{ such that } r' \mid r'' \mid r,\ \ s' \mid s'' \mid s,\ \ t' \mid t'' \mid t,$$

we have an equality of L_2-sets

$$L_2(r'', s'', t'') = L_2(r, s, t = \{\mathrm{lcm}(r, s, t)\}),$$

see the remark at the end of Section 6.2.3. The analogous statement can be made for

$$u' \mid u'' \mid u,\ v' \mid v'' \mid v,\ w' \mid w'' \mid w.$$

Without loss of generality, suppose $\chi(r', s', t') < \chi(u', v', w')$, which follows from Lemma 6.2.6. By Lemma 6.2.7 and Lemma 7.0.1, there exists an odd prime power $q \ll L^5$ such that there are (r', s', t')- and (u', v', w')-smooth representations to $\mathrm{PSL}(2, q)$ but there can never be smooth representations from $\Delta(r'', s'', t'')$ or from $\Delta(u'', v'', w'')$ to $\mathrm{PSL}(2, q)$. Take G to be the image of any (r', s', t')-smooth representation to $\mathrm{PSL}(2, q)$, whose order is bounded by $|G| \ll L^{15}$. From the construction in Corollary 5.3.2, let G' be this group extension of G by C_a^f, where $f := 2 - |G|\chi(r', s', t') < 2 + |G| \ll L^{15}$, and we can take $a = L - 1$. Then G' is a finite quotient of $\Delta(r, s, t)$ but not a finite quotient of $\Delta(u, v, w)$. The upperbound for the order is $|G'| = a^f|G| \ll L^{L^{15}} L^{15} \approx L^{L^{15}}$.

After collecting and comparing the upperbounds produced in each of the cases, we see that the greatest asymptotic bound produced is $N^{(k+3)N^{15}}$, where $N := \max\{\mathrm{lcm}(r, s, t), \mathrm{lcm}(\mathbf{m})\}$.

7.2 Examples

Example 1. Let $\Delta = \Delta(4, 3, 7)$ and $\Gamma = \Delta(2, 3, 7)$. By Proposition 4.2.1, both $\Delta(4, 3, 7)$ and $\Delta(2, 3, 7)$ have trivial Abelianizations, i.e. they are perfect groups. Since naturally the group $\Delta(2, 3, 7)$ is a quotient of $\Delta(4, 3, 7)$, every quotient of $\Delta(2, 3, 7)$ must also be a quotient of $\Delta(4, 3, 7)$. Therefore, we can only use finite quotients from $\Delta(4, 3, 7)$ to distinguish them from $\Delta(2, 3, 7)$. Comparing Euler characteristics yields $-\frac{23}{84} = \chi(4, 3, 7) < \chi(2, 3, 7) = -\frac{1}{42}$. It can be verified that $G = \mathrm{PSL}(2, 7)$ having order 168 is a smooth quotient of $\Delta(4, 3, 7)$, see [4]. Taking $a = 5$ and $f = 2 - |G|\chi(4, 3, 7) = 2 + 168 \cdot \frac{23}{84} = 48$, then there is a group extension G' of G by the Abelian group C_5^{48} such that G' is a quotient of $\Delta(4, 3, 7)$, but not for $\Delta(2,3,7)$. The group G' has order $|G'| = 5^{48} \cdot 168 \approx 5.97 \times 10^{35}$, which is roughly 600 decillion.

Example 2. Let $\Delta = \Delta(15, 42, 63)$ and $\Gamma = \Delta(21, 21, 90)$. These two groups are indistinguishable in many important aspects: both Abelianizations are isomorphic to $\mathrm{C}_3 \times \mathrm{C}_{21}$, both Euler characteristics are equal to $-\frac{563}{630}$, and both L_2-sets are precisely the singleton $\{630\}$ (and so both groups have non-trivial representations to exactly the same list of $\mathrm{PSL}(2,q)$'s, for q an odd prime power). It can be shown that the group $G = \mathrm{PSL}(2,11)$ is a quotient for both groups; however, under $\Delta(15,42,63)$, G is $(5,6,3)$-maximally smooth and under $\Delta(21,21,90)$, G is $(3,3,6)$-maximally smooth. Since $-\frac{3}{10} = \chi(5,6,3) < \chi(3,3,6) = -\frac{1}{6}$, we will consider any $(5,6,3)$-maximally smooth map $\pi\colon \Delta(15,42,63) \twoheadrightarrow \mathrm{PSL}(2,11)$. Notice that the kernel $K := \ker\pi$ is a finitely generated Fuchsian group with signature $(g; 0; 3^{(132)}, 7^{(110)}, 21^{(220)})$, where $g = \frac{1}{2}b_1(K)$, and $d^{(i)}$ is the tuple with all entries d of size i.

Via the Riemann-Hurwitz formula, the kernel $K := \ker\pi$ provides a first Betti number of $f = b_1(K) = 2 - |\mathrm{PSL}(2,11)|\chi(5,6,3) = 200$. Taking $a = 7$, which is coprime to $|\mathrm{PSL}(2,11)| = 660$, we can construct $G' := \Delta(15,42,63)/K^{(7)}[K,K]$, which is a quotient of $\Delta(15,42,63)$ but not for $\Delta(21,21,90)$. The order of G' is $|G'| = a^f|G| = 7^{200} \cdot 660 \approx 6.90 \times 10^{171}$.

Example 3. Let $\Delta = (0;0;2,3,3,315)$ and $\Gamma = \Delta(15,18,21)$. These two groups are have the following properties: both Abelianizations isomorphic to $\mathrm{C}_3 \times \mathrm{C}_3$, their Euler characteristics are both equal to $-\frac{523}{630}$, but $L_2(2,3,3,315) = \{2,315\}$ and $L_2(15,18,21) = \{630\}$. Here, we are able to use Lemma 5.2.2 as an approach to our algorithm: using the notation of Lemma 5.2.2, we can take $q_1 = 3^2$ and $q_2 = 2$ which are maximal prime power divisor of 630 such that the quantity q_1q_2 divides some element of $L_2(15,18,21)$, but two separate elements of $L_2(2,3,3,315)$. We can verify that the prime number $q = 631$ is a solution to the following system of congruences: $q \equiv 1 \pmod{2 \cdot 315}$ and $q \equiv -1 \pmod{2 \cdot 2}$. In this way, we have that $315 \mid \frac{q-1}{2}$, $2 \mid \frac{q+1}{2}$, but $630 \nmid \frac{q\pm1}{2}$. The group G has order 125,619,480. By Theorem 5.1.1, the group $G := \mathrm{PSL}(2,631)$ is a smooth quotient of $(0;0;2,3,3,315)$ but non-smooth for$\Delta(15,18,21)$ (we verified with GAP [14] that G is indeed a quotient). The first Betti number associated to the kernel of a smooth map from $\Delta(15,18,21)$ to G

is precisely $b_1 = 2 - |G|\chi(15, 18, 21) = 104{,}284{,}110$. We mirror the construction given by Theorem 5.3.1 and take $a = 2$ to construct a finite quotient G' that is an extension of G by the Abelian group $\mathrm{C}_a^{b_1}$, which consequently is a quotient of $(0; 0; 2, 3, 3, 315)$, but not for $\Delta(15, 18, 21)$. The order of G' is $|G'| = 2^{104{,}284{,}110} \cdot 125{,}619{,}480 \approx 1.91 \cdot 10^{31{,}392{,}653}$.

We wanted to use the previous example as a proof of concept of Lemma 5.2.2. We now revisit the previous example using a different observation to produce a much smaller distinguishing finite quotient.

Example 4. Let $\Delta = (0; 0; 2, 3, 3, 315)$ and $\Gamma = \Delta(15, 18, 21)$. Both groups have quotients to $G := \Delta(2, 3, 3) \cong A_4$; however, it can be shown that the representations $\pi_1 \colon \Delta \twoheadrightarrow G$ is $(2, 3, 3, 3)$-maximally smooth and that $\pi_2 \colon \Gamma \twoheadrightarrow G$ is $(3, 2, 3)$-maximally smooth. Since $\chi(0; 0; 2, 3, 3, 3) < \chi(0; 0; 3, 2, 3)$, we can ensure that $b_1(\ker \pi_1) > b_1(\ker \pi_2)$. The Riemann-Hurwitz formula gives us $b_1(\ker \pi_1) = 2 - |A_4|\chi(0; 0; 2, 3, 3, 3) = 8$. Take $n = 2$, and let G' be a extension of G by the Abelian group C_2^8. Then G' is a quotient of $(0; 0; 2, 3, 3, 315)$ but not a quotient for $\Delta(15, 18, 21)$. The order of G' is $12 \cdot 2^8 = 3072$, which provides a much better bound than by the previous method.

REFERENCES

[1] M. R. Bridson, M. D. E. Conder, and A. W. Reid, "Determining Fuchsian groups by their finite quotients," *Israel Journal of Mathematics*, vol. 214, no. 1, pp. 1–41, 2016.

[2] M. R. Bridson, D. B. McReynolds, A. W. Reid, and R. Spitler, "On the profinite rigidity of triangle groups," *arXiv preprint arXiv:2004.07137*, 2020.

[3] M. R. Bridson, D. B. McReynolds, A. W. Reid, and R. Spitler, "Absolute profinite rigidity and hyperbolic geometry," *Annals of Mathematics*, vol. 192, no. 3, pp. 679–719, 2020.

[4] A. M. Macbeath, "Generators of the linear fractional groups," in *Proc. Symp. Pure Math*, vol. 12, 1969, pp. 14–32.

[5] J. S. Wilson, "Profinite groups," *Oxford*, vol. 87, p. 90, 1998.

[6] A. W. Reid, "Profinite rigidity," *Proc. Int. Cong. of Math.(Rio de Janeiro)*, vol. 2, pp. 1211–1234, 2018.

[7] N. Nikolov and D. Segal, "On finitely generated profinite groups, I: Strong completeness and uniform bounds," *Annals of mathematics*, pp. 171–238, 2007.

[8] A. Malcev, "On isomorphic matrix representations of infinite groups," *Matematicheskii Sbornik*, vol. 50, no. 3, pp. 405–422, 1940.

[9] W. P. Thurston, *The geometry and topology of three-manifolds*. Princeton University Princeton, NJ, 1979.

[10] P. Scott, "The geometries of 3-manifolds," *Bulletin of the London Mathematical Society*, vol. 15, no. 5, pp. 401–487, 1983.

[11] S. Katok, *Fuchsian groups*. University of Chicago press, 1992.

[12] J. Nielsen, "A basis for subgroups of free groups," *Mathematica Scandinavica*, pp. 31–43, 1955.

[13] A. Selberg, "On discontinuous groups in higher-dimensional symmetric spaces," in *Contributions to function theory*, Tata Institute of Fundamental Research, 1960.

[14] The GAP Group, *GAP – Groups, Algorithms, and Programming*, version 4.11.1, 2021. [Online]. Available: https://www.gap-system.org.

[15] U. V. Linnik, "On the least prime in an arithmetic progression. I. The basic theorem," *Matematicheskii Sbornik*, vol. 15, no. 2, pp. 139–178, 1944.

[16] U. V. Linnik, "On the least prime in an arithmetic progression. II. The Deuring–Heilbronn phenomenon," *Matematicheskii Sbornik*, vol. 15, no. 3, pp. 347–368, 1944.

[17] T. Xylouris, "Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression," 2011.