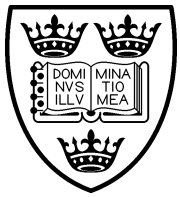
# Homology in Finite Index Subgroups




Liam Wall

Worcester College

University of Oxford

A thesis submitted for the degree of

*Doctor of Philosophy*

Michaelmas 2009

# Abstract

This thesis looks at the following question: If $G$ is a finitely presented group and

$$G > G_1 > G_2 > \dots$$

is a descending sequence of finite index subgroups, then how fast does the rank of $H_1(G_i; \mathbb{F}_p)$ grow compared with the index $|G : G_i|$?

One of our preliminary theorems gives a lower bound on the rank of the first mod-$p$ homology of a normal subgroup $H$ of index a power of $p$, in terms of the mod-$p$ homology of the containing group $G$ and the structure of the quotient $p$-group $G/H$. This bound generalizes a similar result of Lackenby in [Lac09b], and we use it to strengthen a result of that paper from the case $p = 2$ to all primes.

The main result of the thesis concerns the case where $G$ is the fundamental group of a finite-volume hyperbolic 3-manifold, and the subgroups in the descending sequence $\{G_i\}$ are congruence subgroups in $G$. We study the structure of the profinite group $SL(2, R_{\mathcal{P}})$, where $R_{\mathcal{P}}$ is the $\mathcal{P}$-adic completion of a ring of integers in a number field, identifying subgroups of $SL(2, R_{\mathcal{P}})$ which are uniformly powerful. We show that if $G$ is the fundamental group of a finite-volume hyperbolic 3-manifold then it can be approximated by $SL(2, R_{\mathcal{P}})$ for some choices of $R$ and $\mathcal{P}$. More precisely, there is a correspondence between certain congruence subgroups of $G$ and congruence subgroups of $SL(2, R_{\mathcal{P}})$. We use this to prove our most general theorem, Theorem 5.3.1. A simple corollary of Theorem 5.3.1 is that for any $\epsilon > 0$ the group $G$ has a finite index subgroup $G'$ with congruence subgroups $\{G'_i\}$ such that the rank of $H_1(G'_i; \mathbb{F}_p)$ grows at least as fast as $|G' : G'_i|^{\frac{5}{6}-\epsilon}$.

# Acknowledgements

I would like to thank my supervisor Marc Lackenby, for suggesting the direction of my work, and for his persistent encouragement and invaluable help.

I would also like to thank my wife Becky. There are many trials associated with being married to a graduate student, and Becky has coped with all of them graciously.

Finally, thanks go to EPSRC for proving the funding that has allowed me to pursue this study.

# Statement of Originality

This work is my own except where otherwise stated.

To summarize, Chapter 1 provides context and an overview of the thesis. Chapters 2 and 3 are original work, but draw on [Lac09b]. Chapter 4 is purely expository. Chapter 5 is original work, but draws on [DdSMS99], [LS03], and [LR98].

# Contents

# Chapter 1

# Introduction

## 1.1 Why Study Homology Growth?

This thesis is concerned with homology growth in finite index subgroups of hyperbolic 3-manifold groups. To begin with, we look at what *homology growth* is, and why it's worth studying.

Let $G = \pi_1(M)$ where $M$ is a finite-volume hyperbolic 3-manifold. A well-known conjecture is the following:

**Conjecture 1.1.1.** *$G$ is large. That is, $G$ has a finite index subgroup $H < G$ such that $H$ admits a surjective homomorphism to a non-abelian free group.*

One way to investigate this conjecture is to study the homology growth of $G$. Let $G$ be any finitely presented group.

**Definition 1.1.2.** Let $\mathbb{F}$ be a field. The *betti numbers* of $G$ are

$$b_m(G;\mathbb{F}) = \text{rank}(H_m(G;\mathbb{F})).$$

Two questions one might ask are:

1. Given
$$G = G_1 > G_2 > \dots \tag{1.1}$$
where $|G : G_i|$ is finite and strictly increasing with $i$, and a finite field $\mathbb{F}_p$, how fast does $b_1(G_i;\mathbb{F}_p)$ grow compared with $|G : G_i|$?

2. Which such descending sequence has the fastest growth?

These questions are relevant because if a group is large then it has descending sequences with very fast homology growth. As an example consider $F$—the non-abelian free group on $m$ generators. There are normal subgroups of any index, and if $F'$ is index $n$ then $b_1(F';\mathbb{F}_p) = n(m-1)+1$. In this case, for any descending sequence of finite index subgroups

$$F = F_1 > F_2 > \dots \tag{1.2}$$

$b_1(F_i;\mathbb{F}_p)$ grows linearly with $|F : F_i|$. Suppose the group $G$ is large and $H < G$ is of finite index and $f : H \to F$ is a surjective homomorphism to a non-abelian free group. Let $G_i = f^{-1}(F_i)$ for some descending sequence of finite index subgroups as in (1.2). Then $|G : G_i| = |G : H||F : F_i|$ and $b_1(G_i;\mathbb{F}_p) \geq b_1(F_i;\mathbb{F}_p)$, hence

$$b_1(G_i;\mathbb{F}_p) \geq |G : G_i|\frac{(m-1)}{|G : H|} + 1.$$

In particular, $b_1(G_i;\mathbb{F}_p)$ grows linearly with $|G : G_i|$.

For a large group question 2 can easily be answered. We have seen that a large group has a descending sequence of finite index subgroups with linear growth of $\mathbb{F}_p$-homology. In fact linear growth is the fastest one could hope for: Let $G$ be generated by the finite set $X$, let $F$ be the free group on $X$, and let $f : F \to G$ be the induced homomorphism. Given a descending sequence of finite index subgroups as in (1.1) let $F_i = f^{-1}(G_i)$, then $b_1(F_i;\mathbb{F}_p)$ grows linearly with $|F : F_i|$, but also $|G : G_i| = |F : F_i|$ and $b_1(G_i;\mathbb{F}_p) \leq b_1(F_i;\mathbb{F}_p)$.

If $G$ does not have a descending sequence (1.1) where $b_1(G_i;\mathbb{F}_p)$ grows linearly with $|G : G_i|$ then $G$ is not large. The interesting thing is that there are partial converses to this.

A descending series as in (1.1) is called an *abelian p-series* for $G$ if each $G_{i+1}$ is normal in $G_i$ and $G_i/G_{i+1}$ is an elementary abelian $p$-group for all $i \geq 1$. An abelian $p$-series $\{G_i\}$ has *rapid decent* if

$$\inf_i \frac{\operatorname{rank}(G_i/G_{i+1})}{|G : G_i|} > 0.$$

The following is Theorem 1.14 in [Lac].

**Theorem 1.1.3** (Lackenby, [Lac]). *Let $G$ be a finitely presented group, and let $p$ be a prime. Then the following are equivalent:*

1. *$G$ is large; and*

2. *some finite index subgroup of $G$ has an abelian $p$-series with rapid decent.*

If $\{G_i\}$ is an abelian $p$-series for $G$ then $\text{rank}(G_i/G_{i+1}) \leq b_1(G_i; \mathbb{F}_p)$, so the second item of the above theorem immediately implies that $G$ has a sequence (1.1) with linear growth of $\mathbb{F}_p$-homology. However, it is unknown whether a group $G$ which has a descending sequence with linear growth of $\mathbb{F}_p$-homology must have a finite index subgroup with an abelian $p$-series of rapid decent. The following theorem of Lackenby (Theorem 1.1, [Lac09a]) gives a partial answer.

**Theorem 1.1.4** (Lackenby, [Lac09a]). *Let $G$ be a finitely presented group, let $p$ be a prime and suppose that $G \geq G_1 \rhd G_2 \rhd \dots$ is a nested sequence of finite index subgroups, such that each $G_{i+1}$ is normal in $G_i$ and has index a power of $p$. Suppose that $\{G_i\}$ has linear growth of $\mathbb{F}_p$-homology. Then, at least one of the following much hold:*

1. *Some $G_i$ admits a surjective homomorphism onto $(\mathbb{Z}/p\mathbb{Z}) * (\mathbb{Z}/p\mathbb{Z})$ and some normal subgroup of $G_i$ with index a power of $p$ admits a surjective homomorphism onto a non-abelian free group; in particular, $G$ is large; or*

2. *$G$ has Property $(\tau)$ with respect to $\{G_i\}$.*

Property $(\tau)$ will not be considered in this thesis, so we don't define it, but a definition can be found in [Lac09a].

In summary, finding any of the following inside a hyperbolic 3-manifold group would be significant:

1. Abelian $p$-series (such as the derived $p$-series) with rapid decent;

2. descending subgroups with linear homology growth; or

3. descending subgroups without Property $(\tau)$.

## 1.2 Summary of Results and Related Work

A first step to proving results about homology growth is to address the following question: If $G$ is group and $H$ is a finite index normal subgroup, and we know the $\mathbb{F}_p$-homology of $G$ and the structure of $G/H$ what can be said about the $\mathbb{F}_p$-homology of $H$?

There are many previous results in this area. In [SW92] Shalen and Wagreich prove a result for a specific case.

**Definition 1.2.1.** If $p$ is a prime and $G$ is a group then $P_i(G)$ is the $i^{\text{th}}$ term of the lower $p$-central series. That is, $P_i(G)$ is defined inductively by

$$P_i(G) = [G, P_{i-1}(G)]P_{i-1}(G)^{(p)},$$

where $P_1(G) = G$ and for any $H < G$, $[G, H] = \langle ghg^{-1}h^{-1} : g \in G, h \in H\rangle$ and $H^{(p)} = \langle h^p : h \in H\rangle$.

**Lemma 1.2.2** (Shalen and Wagreich)**.** *Let $p$ be a prime and $M$ a closed 3-manifold—orientable if $p$ is odd. Let $\Gamma = \pi_1(M)$ and $\Gamma' = P_2(\Gamma)$ then*

$$b_1(\Gamma'; \mathbb{F}_p) \geq \binom{b_1(\Gamma; \mathbb{F}_p)}{2}.$$

In [Lac09b] Lackenby proves the following theorem:

**Theorem 1.2.3** (Lackenby [Lac09b])**.** *Let $G$ be a group such that $b_1(G; \mathbb{F}_p)$ and $b_2(G; \mathbb{F}_p)$ are finite, for some prime $p$. Let $H$ be a finite index normal subgroup such that $G/H$ is an elementary Abelian $p$-group of rank $n$. Then, for any integer $l$ between 0 and $n$,*

$$b_1(H; \mathbb{F}_p) \geq \sum_{r=2}^{l+1} \binom{n}{r}(r-1) + (b_1(G; \mathbb{F}_p) - n)\sum_{r=0}^{l} \binom{n}{r} - b_2(G; \mathbb{F}_p)\sum_{r=0}^{l-1} \binom{n}{r}.$$

*Moreover, if $p = 2$,*

$$b_1(H; \mathbb{F}_p) \geq b_1(G; \mathbb{F}_p)\sum_{r=0}^{l} \binom{n}{r} - b_2(G; \mathbb{F}_p)\sum_{r=0}^{l-1} \binom{n}{r} - \sum_{r=1}^{l+1} \binom{n}{r}.$$

In chapter 2 we prove:

**Theorem 2.3.1.** *Let $G$ be a finitely generated group and $H$ a normal subgroup such that $G/H$ is a finite $p$-group. Let $M$ be the group ring $\mathbb{F}_p(G/H)$ and $J$ the augmentation ideal in $M$. For each integer $l \geq 1$ the following inequality holds,*

$$b_1(H;\mathbb{F}_p) \geq b_1(G;\mathbb{F}_p)\cdot \dim(M/J^l) - b_2(G;\mathbb{F}_p)\cdot \dim(M/J^{l-1}) \\ - \dim(J/J^{l+1}).$$

This is stronger than previous results as $G/H$ need not be abelian. Moreover, in the abelian case it provides stronger bounds for $p > 2$. Chapter 2 is broken into three parts: In section 2.1 some background on Fox derivatives is set out. In section 2.2 we describe a particular presentation for the group $G$ which has certain nice properties. This presentation was used in [Lac09b], but works just as well for our purposes. Section 2.3 is devoted to proving Theorem 2.3.1.

The first application of Theorem 2.3.1 is in chapter 3. Before stating the theorem of chapter 3 we need two definitions.

**Definition 1.2.4.** A group $G$ has the $b_2 - b_1$ *property* with respect to the prime $p$ if there exists a positive number $N$ such that for all finite index subgroups $H < G$ we have $b_2(H;\mathbb{F}_p) - b_1(H;\mathbb{F}_p) \leq N$.

**Definition 1.2.5.** Let $(x_i)_{i=1}^{\infty}$ and $(y_i)_{i=1}^{\infty}$ be positive real sequences. We write $x_i = \Omega(y_i)$ if $\frac{x_i}{y_i}$ is bounded away from zero.

**Theorem 3.2.2.** *Let $G$ be a finitely generated group that has the $b_2 - b_1$ property with respect to the prime $p$. Suppose that*

$$\sup\{b_1(G_i;\mathbb{F}_p) : G_i \text{ is a finite index subgroup of } G\} = \infty.$$

*Then $G$ has a nested sequence of finite index normal subgroups $\{G_i\}$ such that*

$$b_1(G_i;\mathbb{F}_p) = \Omega\left(\frac{[G:G_i]}{\sqrt{\log[G:G_i]}\log\log[G:G_i]}\right).$$

This was proved in [Lac09b] for the case $p = 2$. It is proved for all primes using the stronger bounds of Theorem 2.3.1. In order to estimate the dimensions of $J^{l-1}/J^l$ we use Jennings' Theorem and the Central Limit Theorem from probability. Jennings' Theorem and dimension subgroups are described in section 3.1. In section 3.2 we do the work of estimating the dimension of $J^{l-1}/J^l$. After making this estimation the proof given in [Lac09b] carries over, so we only provide a summary of it.

In Chapter 4 we present some background on number theory, quaternion algebras, profinite groups, and hyperbolic space. None of this is original work, but it is all used in Chapter 5.

Chapter 5 looks at the congruence subgroups of a hyperbolic 3-manifold group. We start in section 5.1 by studying the structure of $SL(n, R_{\mathcal{P}})$, proving the following:

**Theorem 5.1.1.** *Let $R$ be the ring of integers in a number field, and let $\mathcal{P}$ be a prime ideal lying over the rational prime $p$, with ramification index $e$. For $m \geq 0$ let $G_m$ be the principal congruence subgroup*

$$G_m = \mathrm{Ker}\left(SL(n, R_{\mathcal{P}}) \to SL(n, R/\mathcal{P}^m)\right).$$

*Let $l \geq 2$ if $p = 2$ and $l \geq 1$ if $p > 2$. Then $G_{el}$ is a uniformly powerful pro-$p$ group with $|G_{el} : P_2(G_{el})| = (n^2 - 1) \cdot \mathrm{rank}(R/\mathcal{P}^e)$. Moreover $P_i(G_{el}) = G_{e(l+i-1)}$.*

The proof of this theorem is adapted from the proof of Theorem 5.2 in [DdSMS99], and the lemmas preceding the proof draw heavily on ideas from that same book.

In section 5.2 we prove:

**Theorem 5.2.1.** *Let $\Gamma$ be the fundamental group of a finite-volume hyperbolic 3-manifold. Let $k$ be the trace field of $\Gamma$, and suppose $k$ coincides with the invariant trace field of $\Gamma$. Let $R$ be the ring of integers in $k$ and let $\mathcal{P}$ be a prime ideal in $R$. As long as $\mathcal{P}$ is not in some finite list of ideals there is an injection*

$$\Gamma \hookrightarrow SL(2, R_{\mathcal{P}})$$

*such that the image of $\Gamma$ is dense in $SL(2, R_{\mathcal{P}})$ (where $SL(2, R_{\mathcal{P}})$ has the profinite topology).*

The condition that the trace field and the invariant trace field of $\Gamma$ should coincide is not a strong one. The invariant trace field of $\Gamma$ equals the invariant trace field of $\Gamma^{(2)}$, and the invariant trace field of $\Gamma^{(2)}$ coincides with the trace field of $\Gamma^{(2)}$. So, to satisfy to satisfy the hypothesis, at worst we need to pass to $\Gamma' = \Gamma^{(2)}$.

Theorem 5.2.1 is a kind of strong approximation theorem for hyperbolic 3-manifold groups. There are many versions of the strong approximation theorem in the literature (e.g. [MVW84], [Pin00], [Wei84]). Typically the hypothesis of a strong approximation-type theorem is that $\Gamma$ is a Zariski-dense subgroup in an algebraic group $\mathbb{G}(k)$; the conclusion is that $\Gamma$ (or some finite index subgroup of $\Gamma$) is dense (in the congruence topology) in $\prod \mathbb{G}(R_{\mathcal{P}})$. (The product is taken over all but finitely many prime ideals $\mathcal{P}$ in $R$.) However the strong approximation theorems in the literature seem to split in to two cases: those which restrict to $k = \mathbb{Q}$; or those which require the machinery of group schemes to apply. In all cases the proofs of these theorems are long and use a lot of technology, so it seemed worthwhile to have a simple statement and proof of an approximation theorem for hyperbolic 3-manifold groups.

In section 5.3 we use the knowledge of the structure of $SL(2, R_{\mathcal{P}})$, the approximation theorem, and Theorem 2.3.1 to prove Theorem 5.3.1—our main theorem on the homology growth of congruence subgroups in hyperbolic 3-manifold groups.

**Theorem 5.3.1.** *Let $\Gamma$ be the fundamental group of a finite-volume hyperbolic 3-manifold, and let $R$ be the ring of integers in the invariant trace field of $\Gamma$. For all but finitely many prime ideals $\mathcal{P}$ in $R$ the following holds: $\Gamma$ has a finite index subgroup $\Gamma'$ with the following properties.*

1. *$\Gamma'$ embeds in $SL(2, R_{\mathcal{P}})$, where $R_{\mathcal{P}}$ is the $\mathcal{P}$-adic completion of $R$. Moreover $\Gamma'$ is dense in $SL(2, R_{\mathcal{P}})$.*

2. *Let $r = \operatorname{rank}(R/\mathcal{P})$ and let $\epsilon > 0$. Let $p$ be the characteristic of $R/\mathcal{P}$. Let $\Gamma'_n = \operatorname{Ker}(\Gamma' \to SL(2, R/\mathcal{P}^n))$ (the congruence subgroups), then*

$$b_1(\Gamma'_{n_i}; \mathbb{F}_p) > |\Gamma'_{n_1} : \Gamma'_{n_i}|^{\frac{3r-1}{3r} - \epsilon} b_1(\Gamma'_{n_1}; \mathbb{F}_p),$$

*for some integers* $n_1 < n_2 < \ldots$.

As we see, the larger $r$ is, the closer this is to linear growth.

Finally, we provide a simple corollary to the main theorem, which also demonstrates how it would be applied to specific examples.

**Corollary 5.3.7.** *Let* $\Gamma$ *be the fundamental group of a finite-volume hyperbolic 3-manifold. Then, for infinitely many prime integers* $p$*, and for any* $\epsilon > 0$*,* $\Gamma$ *has a finite index subgroup* $\Gamma'$ *with a sequence of congruence subgroups*

$$\Gamma' = \Gamma'_{n_1} > \Gamma'_{n_2} > \ldots$$

*such that* $b_1(\Gamma'_{n_i}; \mathbb{F}_p) > |\Gamma'_{n_1} : \Gamma'_{n_i}|^{\frac{5}{6}-\epsilon} b_1(\Gamma'_{n_1}; \mathbb{F}_p)$.

# Chapter 2

# Finding Homology in Index $p^n$ Normal Subgroups

The aim of this chapter is to prove Theorem 2.3.1. Given a finitely generated group $G$ and a normal subgroup $H$ of index a power of $p$, Theorem 2.3.1 gives a lower bound for the first mod-$p$ homology of $H$, in terms of the mod-$p$ homology of $G$ and the structure of $G/H$.

In Section 2.1 we describe some background on Fox derivatives and how they are used. In Section 2.2 we describe a group presentation that was used by Lackenby in [Lac09b] and that we will use here. Finally in section 2.3 we prove Theorem 2.3.1.

## 2.1 2-Complexes and Fox Derivatives

Let $\langle X|R\rangle$ be a presentation of a group $G$.

We can make a 2-complex $\mathcal{K}$ which has fundamental group $G$ in the following way. Take a single vertex $v$. For each $x \in X$ add a directed edge $e_x$ which has $v$ as its start and end point. This will be the 1-skeleton $\mathcal{K}^{(1)}$ of $\mathcal{K}$. For each $r \in R$ take a 2-cell $F_r$. The word $r$ spells a closed path in $\mathcal{K}^{(1)}$, where $x$ corresponds to crossing the edge $e_x$ in the forward direction and $x^{-1}$ corresponds to crossing the edge $e_x$ in the reverse direction. Attach the 2-cell $F_r$ to $\mathcal{K}^{(1)}$ such that $\partial R_r$ is the loop spelled by $r$. This 2-complex then has fundamental group $\pi_1(\mathcal{K}, v) \cong G$.

Let $H$ be a subgroup of $G$, and let $\widetilde{\mathcal{K}}$ be the covering space of $\mathcal{K}$ corresponding to $H$. The cover $p : \widetilde{\mathcal{K}} \to \mathcal{K}$ is $|G/H|$-sheeted. In particular, after choosing a base

vertex $b$ in $\widetilde{\mathcal{K}}$ to be labeled by the identity in $G/H$, the 1-skeleton of $\widetilde{\mathcal{K}}$ is a Cayley graph for $G/H$. Then there is a natural bijection from $\widetilde{\mathcal{K}}^{(0)}$ to $G/H$ such that $b$ is mapped to the identity.

We are interested in the homology of $H$. Consider the cellular 1-chains of $H$ with coefficients in $\mathbb{F}_p$. These can be described as elements of $M^{|X|}$, where $M$ is the group ring $\mathbb{F}_p(G/H)$, in the following way: Fix some order on $X$, so $X = \{x_1, x_2, \ldots\}$. If $\gamma \in G/H$ then the element

$$(0, \ldots, 0, \gamma, 0 \ldots, 0) \in M^{|X|},$$

where $\gamma$ appears in the $i^{\text{th}}$ place, corresponds to the cellular 1-chain $1 \cdot e$, where $e$ is the $x_i$ labeled edge emanating from the vertex in $\widetilde{\mathcal{K}}$ labeled by $\gamma$.

Fox derivatives can be used to convert paths in $\widetilde{\mathcal{K}}$ to cellular 1-chains.

**Definition 2.1.1.** Let $F$ be the free group on $X$ and let $x$ be an element of $X$. The *Fox derivative* is a map

$$\frac{\partial}{\partial x} : F \to \mathbb{Z}F$$

defined by:

1. $\frac{\partial}{\partial x} x = 1$ and $\frac{\partial}{\partial x} x^{-1} = -x^{-1}$;
2. for all $y \in X \backslash \{x\}$, $\frac{\partial}{\partial x} y^{\pm 1} = 0$; and
3. if $u, v \in F$ then $\frac{\partial}{\partial x}(uv) = \frac{\partial}{\partial x} u + u \frac{\partial}{\partial x} v$.

It is easy to see that if $w \in F$ then the number of terms in $\frac{\partial w}{\partial x}$ equals the number of occurrences of $x$ and $x^{-1}$ in a reduced word representing $w$. (Reduced means the word does not contain $uu^{-1}$ anywhere as a subword.) For example, if $X = \{x, y, x\}$ then $\frac{\partial}{\partial x}(yx^2zx^{-1}yz^2) = y + yx - yx^2zx^{-1}$.

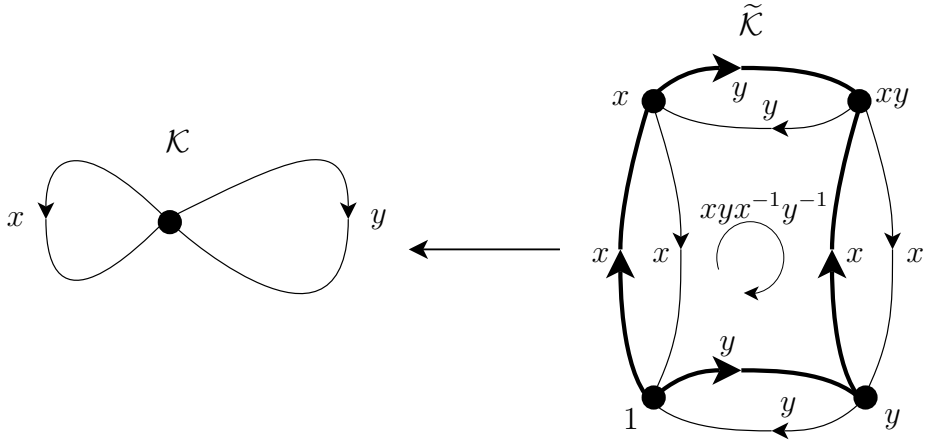
Consider again the situation where $G = \langle X | R \rangle$ with $H \leq G$, and $\mathcal{K}$ is a standard 2-complex with $\pi_1(\mathcal{K}) = G$, and $\widetilde{\mathcal{K}}$ is the covering space corresponding to $H$. There is a natural map $\phi : \mathbb{Z}F \to M$, where $M$ is the group ring $\mathbb{F}_p(G/H)$. Recall that the 1-chains on $\widetilde{\mathcal{K}}$ can be identified with $M^{|X|}$. Consider elements of $F$, the free group

on $X$, as paths in $\widetilde{\mathcal{K}}$ based at the vertex labeled by the identity of $G/H$. Then the map $F \to M^{|X|}$ given by

$$w \mapsto \left( \phi\left(\frac{\partial w}{\partial x_1}\right), \ldots, \phi\left(\frac{\partial w}{\partial x_{|X|}}\right) \right)$$

takes a path based at $b$ and written as a word in elements of $X$ and gives the corresponding 1-chain.

For example, let $X = \{x, y\}$, let $G = F$, let $H = [G, G]G^{(2)}$, and let $w = xyx^{-1}y^{-1}$. Then $w \mapsto (1 - y, x - 1)$, where $G/H = \{1, x, y, xy\}$. This example is shown in the following picture. The path $xyx^{-1}y^{-1}$ based at the vertex labeled 1 is shown in bold.




## 2.2 Choosing a Presentation

Let $G$ be a finitely generated group with a normal subgroup $H$ such that $G/H$ is a finite $p$-group. In this section we describe a group presentation that comes from [Lac09b].

As we have seen, given a presentation $G = \langle X|R\rangle$ there is a 2-complex, whose fundamental group is $G$, with $|X|$ 1-cells and $|R|$ 2-cells. The presentation given here will allow us to only "worry" about $b_1(G; \mathbb{F}_p)$ 1-cells and $b_2(G; \mathbb{F}_p)$ 2-cells.

Let $X_1$ be a subset of $G$ such that its image is a basis in $H_1(G; \mathbb{F}_p)$. Let $X_3$ be a generating set for $H \cap P_2(G)$. Then $X_1 \cup X_3$ is a generating set for $G$, since $X_1$ is a generating set for the finite $p$-group $G/\left(H \cap P_2(G)\right)$. (We do not use $X_2$, in order to maintain some consistency with [Lac09b].)

Lackenby's arguments in [Lac09b] apply in this case, and so $G$ has a presentation

$$G = \langle X_1, X_3 | R_1, R_2, R_3 \rangle$$

with the following properties:

i. $X_1$ forms a basis for $H_1(G; \mathbb{F}_p)$, and for any $x \in X_1$ and for any $r \in R_i$ the total weight of $x$ in $r$ is a multiple of $p$;

ii. every element of $X_3$ is contained in $H$ and is trivial in $H_1(G; \mathbb{F}_p)$;

iii. every element of $R_2$ lies in $P_2(F)$, where $F$ is free on $X_1 \cup X_3$;

iv. $|R_3| = |X_3|$ and for each element $x_3$ in $X_3$ there is a relation in $R_3$ of the form $x_3 = f(x_3)$ where $f(x_3)$ is the product of an element of $P_2(F_-)$ and an element of $P_m(F)$, where $F_-$ is free on $X_1$ and $m$ can be chosen as large as we wish;

v. $R_1$ is a basis for $H_2(G; \mathbb{F}_p)$, where we are using the Hopf formula for $H_2$; and

vi. every element of $R_1$ lies in $P_2(F_-)P_m(F)$.

Let $R_{(1)} = \langle\langle R_1 \cup R_2 \cup R_3 \rangle\rangle$, then inductively define

$$R_{(j+1)} = [F, R_{(j)}] R_{(j)}^p.$$

The following is Lemma 2.2 in [Lac09b].

**Lemma 2.2.1.** *Let $S = \langle\langle R_1 \cup R_3 \rangle\rangle$. Then for each $j \geq 1$, $R_{(1)} = SR_{(j)}$.*

## 2.3 Finding Homology

We work with the presentation $G = \langle X_1, X_3 | R_1, R_2, R_3 \rangle$ described above. Let $K$ be 2-complex corresponding to this presentation, and let $\widetilde{K}$ be the regular cover of $K$ corresponding to the subgroup $H$.

Fix a base vertex $b$ of $\widetilde{K}$. Then each vertex of $\widetilde{K}$ corresponds to an element of $G/H$, where $b$ corresponds to the identity element.

First we consider the mod-$p$ cellular 1-chains supported on edges labeled by $X_1$. Let $M$ be the group ring $\mathbb{F}_p(G/H)$, then the mod-$p$ cellular 1-chains supported on $X_1$ can be identified with $M^{|X_1|}$. The mod-$p$ 1-*co*chains supported on edges labeled by elements of $X_1$ can be identified with $(M^{|X_1|})^*$. (Where $V^* = \mathrm{Hom}(V, \mathbb{F}_p)$.)

An element $w \in F$ is a word in the generating set $X_1 \cup X_3$, and is a path in $\widetilde{K}$ based at the identity vertex $b$. Suppose we have a 1-cochain $\phi \in (M^{|X_1|})^*$. The value of this cochain evaluated on the path $w$ is

$$\phi\left(\left(\frac{\partial w}{\partial x_1}, \frac{\partial w}{\partial x_2}, \ldots\right)\right),$$

where $X_1 = \{x_1, x_2, \ldots\}$, and

$$\frac{\partial}{\partial x_i} : \mathbb{F}_p F \longrightarrow M$$

is the Fox derivative, taken as a map from $\mathbb{F}_p F$ to $M$.

Let $J \subset M$ be the augmentation ideal. That is, the kernel of the augmentation map

$$\epsilon : M \longrightarrow \mathbb{F}_p,$$

given by

$$\sum_{\gamma \in G/H} \lambda_\gamma \gamma \longmapsto \sum_{\gamma \in \Gamma} \lambda_\gamma.$$

It is well known that whenever $G/H$ is a finite $p$-group, powers of $J$ form a filtration of $M$,

$$\{0\} = J^m \subset \ldots \subset J^2 \subset J \subset M.$$

There is a corresponding filtration of $M^*$,

$$M^* \supset (M/J^{m-1})^* \supset \ldots \supset (M/J)^* \supset \{0\}^*.$$

The following theorem relates the first betti number of $H$ to the first two betti numbers of $G$, and the quotient group $G/H$.

**Theorem 2.3.1.** *Let $G$ be a finitely generated group and $H$ a normal subgroup such that $G/H$ is a finite p-group. Let $M$ be the group ring $\mathbb{F}_p(G/H)$ and $J$ the augmentation ideal in $M$. For each integer $l \geq 1$ the following inequality holds,*

$$b_1(H;\mathbb{F}_p) \geq b_1(G;\mathbb{F}_p)\cdot \dim(M/J^l) - b_2(G;\mathbb{F}_p)\cdot \dim(M/J^{l-1}) \\ - \dim(J/J^{l+1}).$$

The rest of this section is devoted to proving this theorem.

The space of cochains on $\widetilde{K}$ supported on $X_1$ labeled edges can be identified with

$$(M^{b_1(G;\mathbb{F}_p)})^* \cong (M^*)^{b_1(G;\mathbb{F}_p)}.$$

Consider the subspace

$$((M/J^l)^*)^{b_1(G;\mathbb{F}_p)},$$

where $l \in \{1,\dots,m-1\}$. This has dimension $b_1(G;\mathbb{F}_p)\cdot\dim(M/J^l)$. Each 2-cell on $\widetilde{K}$ imposes a linear constraint that must be satisfied by any cocycle. The first task is to show that after modifying the cochains slightly, the codimension of the subspace of cocycles is at most $b_2(G;\mathbb{F}_p)\cdot\dim(M/J^{l-1})$.

Let $\beta_1,\dots,\beta_n$ be elements of $M$ whose image is an $\mathbb{F}_p$-basis of $M/J^{l-1}$.

*Claim* 2.3.2. Let $(\phi_1,\dots,\phi_{b_1(G;\mathbb{F}_p)}) \in ((M/J^l)^*)^{b_1(G;\mathbb{F}_p)}$, and let $r \in \langle\langle R_1,R_2,R_3\rangle\rangle$. Suppose that

$$\sum_j \phi_j\left(\beta_i\frac{\partial r}{\partial x_j}\right) = 0$$

for each $i = 1,\dots,n$. Then for any $z \in M$

$$\sum_j \phi_j\left(z\frac{\partial r}{\partial x_j}\right) = 0.$$

*Proof.* Fix $z \in M$, then we can write

$$z = x + \sum_i \lambda_i\beta_i,$$

where $x \in J^{l-1}$ and $\lambda_i \in \mathbb{F}_p$. Then

$$\sum_j \phi_j(z\frac{\partial r}{\partial x_j}) = \sum_j \phi_j(x\frac{\partial r}{\partial x_j}) + \sum_i\left[\lambda_i\sum_j\phi_j\left(\beta_i\frac{\partial r}{\partial x_j}\right)\right].$$

Since $r$ is in $\langle\langle R_1, R_2, R_3\rangle\rangle$, the weight in $r$ of any letter from $X_1$ is a multiple of $p$, hence $\frac{\partial r}{\partial x_j}$ is in $J$ for all $j$. Since $x$ is in $J^{l-1}$ and each $\phi_j$ is in $(M/J^l)^*$, the first summation is zero. The second summation is zero by hypothesis. $\square$

Let $U$ be the subspace of $((M/J^l)^*)^{b_1(G;\mathbb{F}_p)}$ consisting of cochains which evaluate to zero on the boundary of any 2-cell labeled by an element of $R_1$. By the claim $U$ has dimension at least

$$b_1(G;\mathbb{F}_p)\cdot\dim(M/J^l) - b_2(G;\mathbb{F}_p)\cdot\dim(M/J^{l-1}).$$

This is because $|R_1| = b_2(G;\mathbb{F}_p)$, and by the claim, for each $r \in R_1$ the subspace of cochains evaluating to zero on the boundary of all $r$ labeled 2-cells has codimension at most $\dim(M/J^{l-1})$.

We can extend these cochains to cochains supported on $X_1$ and $X_3$ labeled edges in the following way. If $\phi$ is a cochain supported only on $X_1$ labeled edges, let $\varphi(\phi)$ agree with $\phi$ on $X_1$ labeled edges. For each edge $e$ labeled by an element of $X_3$ let $\varphi(\phi)(e)$ be determined as follows: Suppose $e$ is labeled by $x \in X_3$, and is based at the vertex $i(e)$. One of the relations in $R_3$ is of the form $xf(x)^{-1}$. Let $\varphi(\phi)(e) = \phi(f(x))$, where the path $f(x)$ is based at $i(e)$. The map $\varphi$ is linear and injective, hence $\dim(\varphi(U)) = \dim(U)$.

Every element of $R_1$ and $R_3$ is a product of an element of $P_2(F_-)$ and an element of $P_m(F)$ where $m$ can be chosen arbitrarily large. Choose $m$ such that the image of $P_m(F)$ in $G$ is contained in $P_2(H)$. Then, for any cochain $\phi$ the value of $\phi$ evaluated on the boundary of a 2-cell labeled by an element of $R_1$ or $R_3$ depends only on the $P_2(F_-)$ part. Hence, every cochain in $\varphi(U)$ evaluates to zero on the boundary of all 2-cells labeled by elements of $R_1$ and $R_3$. Applying Lemma 2.2.1 with $j = m$ gives

$$\langle\langle R_1, R_2, R_3\rangle\rangle = \langle\langle R_1, R_3\rangle\rangle R_{(m)},$$

where $R_{(m)}$ is contained in $P_m(F)$. Hence every element of $\varphi(U)$ is a cocycle. We have thus proved:

*Claim* 2.3.3. The space of cellular 1-cocycles on $\widetilde{K}$ with coefficients in $\mathbb{F}_p$ has dimension at least

$$b_1(G;\mathbb{F}_p)\cdot\dim(M/J^l) - b_2(G;\mathbb{F}_p)\cdot\dim(M/J^{l-1}).$$

The following claim will complete the proof of Theorem 2.3.1.

*Claim* 2.3.4. The subspace of coboundaries in $\varphi(U)$ has dimension $\dim(J/J^{l+1})$.

*Proof.* Any 1-coboundary is the coboundary of some 0-cochain. Let $f$ be a 0-cochain on $\widetilde{K}$, so $f$ is a linear map $f : M \longrightarrow \mathbb{F}_p$. Let $\partial^*$ be the coboundary map, then we look for conditions on $f$ such that $\partial^* f$ is in $\varphi(U)$.

Recall that $\varphi$ is a map from the space of cochains supported on only $X_1$-labeled edges, to cochains supported on all edges. It has a left inverse $\varphi^{-1}$ given by projection.

The coboundary $\partial^* f$ is in $\varphi(U)$ if and only if $\varphi^{-1}(\partial^* f)$ is in $U$. Since $\varphi^{-1}(\partial^* f)$ is supported only on $X_1$-labeled edges we can take it as an element of $(M^*)^{b_1(G;\mathbb{F}_p)}$. The construction of $\partial^* f$ ensures that $\varphi^{-1}\partial^* f$ will be in $U$ as long as it is in $((M/J^l)^*)^{b_1(G;\mathbb{F}_p)}$.

We can describe $\varphi^{-1}\partial^* f$ as follows: If $w$ is a word in $X_1 \cup X_3$, representing a path in $\widetilde{K}$ based at the identity vertex, then

$$(\varphi^{-1}\partial^* f)(w) = \sum_i \phi_i\left(\frac{\partial w}{\partial x_i}\right),$$

where for each $g \in \Gamma$, $\phi_i(g) = f(gx_i) - f(g)$.

Suppose $(\phi_1, \ldots) \in ((M/J^l)^*)^{b_1(G;\mathbb{F}_p)}$. Let $z_i \in J^l$, then

$$\begin{aligned} 0 = \sum_i \phi_i(z_i) &= \sum_i (f(z_i x_i) - f(z_i)) \\ &= \sum_i f(z_i(x_i - 1)) \\ &= f\left(\sum_i z_i(x_i - 1)\right). \end{aligned}$$

Hence, $f$ is in $(M/J^{l+1})^*$. Finally, if $f$ and $f'$ are maps from $G/H$ to $\mathbb{F}_p$ then $f$ and $f'$ determine the same coboundary if and only if $f - f'$ is a constant function on $G/H$. Thus the space of coboundaries in $\varphi(U)$ had dimension

$$\dim((M/J^{l+1})^*) - 1 = \dim(J/J^{l+1}).$$

□

# Chapter 3

# Lower Bounds on Homology Growth

In this chapter we use Theorem 2.3.1 to strengthen a result of Lackenby in [Lac09b]. Before proving this result in Section 3.2, we introduce dimension subgroups and give Jennings' Theorem in Section 3.1. This is used to calculate dimensions of quotients of the augmentation ideal in group ring.

## 3.1 Dimension Subgroups and Jennings' Theorem

Let $P$ be a finite $p$-group for some prime $p$. Let $J$ be the augmentation ideal in $\mathbb{F}_p P$. The main result of the previous chapter raises the question, how do we determine the order of the quotients $J^l/J^{l+1}$? The answer is that we use Jennings' Theorem.

**Definition 3.1.1.** The *mod-p dimension subgroups* of an arbitrary group $G$ are defined inductively by $D_1(G) = G$ and

$$D_m(G) = D^{(p)}_{\lceil \frac{m}{p} \rceil}(G) \prod_{i+j=m} [D_i(G), D_j(G)],$$

where $\left\lceil \frac{m}{p} \right\rceil$ is the smallest integer greater than or equal to $\frac{m}{p}$.

Two things are immediate from this definition: The dimension subgroups are characteristic; and $D_2(G) = P_2(G)$. The following theorem is 12.9 in [DdSMS99].

**Theorem 3.1.2.** $D_m(G) = \{\gamma \in G : \gamma - 1 \in J^m\}$.

This shows that $D_{m+1}(G) \subseteq D_m(G)$, since $J^{m+1} \subseteq J^m$. The inclusions

$$D_{m+1}(G) \supseteq [D_m(G), G] \supseteq [D_m(G), D_m(G)] \text{ and}$$
$$D_{m+1}(G) \supseteq D^{(p)}_{\lceil \frac{m+1}{p} \rceil} \supseteq D^{(p)}_m(G)$$

show that $D_m(G)/D_{m+1}(G)$ is an elementary abelian $p$-group.

**Theorem 3.1.3** (Jennings [Jen41]). *Let $P$ be a finite $p$-group and $\mathbb{F}$ a field of characteristic $p$. Let $J$ be the augmentation ideal in $\mathbb{F}P$. Then*

$$\sum_{r \geq 0} x^r \cdot \dim(J^r/J^{r+1}) = \prod_{s \geq 1} (1 + x^s + x^{2s} + \cdots + x^{(p-1)s})^{d_s},$$

*where $d_s$ is the rank of $D_s(P)/D_{s+1}(P)$.*

## 3.2 Strengthening [Lac09b]

An interesting application of Theorem 2.3.1 is the case where $G/H$ is an elementary Abelian $p$-group. In [Lac09b] Lackenby proves the following theorem:

**Theorem 3.2.1** (Lackenby [Lac09b]). *Let $G$ be a group such that $b_1(G; \mathbb{F}_p)$ and $b_2(G; \mathbb{F}_p)$ are finite, for some prime $p$. Let $H$ be a finite index normal subgroup such that $G/H$ is an elementary Abelian $p$-group of rank $n$. Then, for any integer $l$ between 0 and $n$,*

$$b_1(H; \mathbb{F}_p) \geq \sum_{r=2}^{l+1} \binom{n}{r} (r-1) + (b_1(G; \mathbb{F}_p) - n) \sum_{r=0}^{l} \binom{n}{r} - b_2(G; \mathbb{F}_p) \sum_{r=0}^{l-1} \binom{n}{r}.$$

*Moreover, if $p = 2$,*

$$b_1(H; \mathbb{F}_p) \geq b_1(G; \mathbb{F}_p) \sum_{r=0}^{l} \binom{n}{r} - b_2(G; \mathbb{F}_p) \sum_{r=0}^{l-1} \binom{n}{r} - \sum_{r=1}^{l+1} \binom{n}{r}.$$

Theorem 2.3.1 recovers the case for $p = 2$ exactly, but gives stronger bounds for odd primes. The following theorem was proved in [Lac09b] for the case $p = 2$ (Theorem 1.7). It is proved for all primes using the stronger bounds of Theorem 2.3.1.

**Theorem 3.2.2.** *Let $G$ be a finitely generated group that has the $b_2 - b_1$ property with respect to the prime $p$. Suppose that*

$$\sup\{b_1(G_i; \mathbb{F}_p) : G_i \text{ is a finite index subgroup of } G\} = \infty.$$

*Then $G$ has a nested sequence of finite index normal subgroups $\{G_i\}$ such that*

$$b_1(G_i; \mathbb{F}_p) = \Omega\left(\frac{[G : G_i]}{\sqrt{\log[G : G_i]}\log\log[G : G_i]}\right).$$

To calculate dimensions of quotients of powers of the augmentation ideal we use Jennings' Theorem. Let $P$ be an elementary Abelian $p$-group of rank $n$, and let $d_i$ be the dimension of the quotient $D_i(P)/D_{i+1}(P)$. Then $d_1 = n$, and $d_i = 0$ for $i \geq 2$ since $D_2(P) = [P, P]P^{(p)} = 1$. Hence for $p = 2$ Jennings' Theorem gives

$$\dim(J^r/J^{r+1}) = \binom{n}{r}.$$

Combining this formula with Theorem 2.3.1 recovers the 2nd part of 3.2.1. For other primes $p$ the Jennings polynomial is

$$f(x) = \left(1 + x + \ldots + x^{(p-1)}\right)^n.$$

The strongest bound from Theorem 2.3.1 is obtained by looking at the largest coefficient in this polynomial.

*Claim* 3.2.3. For sufficiently large $n$, at least one of the coefficients in $f(x)$ is greater than or equal to $\frac{p^n k}{\sqrt{n}}$, where $k$ is a fixed positive constant depending only on $p$.

*Proof.* Let $X_i$, where $i = 1, \ldots, n$ be discrete independent identically distributed random variables, taking values in $\{0, \ldots, p-1\}$ with uniform probability. Let

$$S_n = \sum_{i=1}^{n} X_i,$$

then the probability generating function for $S_n$ is

$$\frac{1}{p^n} f(x).$$

Expectation and variance are

$$\mathbb{E}(S_n) = \frac{(p-1)n}{2},$$
$$\mathrm{Var}(S_n) = \frac{(p^2-1)n}{12}.$$

By the Central Limit Theorem

$$\frac{S_n - \frac{(p-1)n}{2}}{\sqrt{\frac{(p^2-1)n}{12}}} \to N(0,1)$$

in distribution, as $n \to \infty$, where $N(0,1)$ is the standard normal distribution. Let $k$ be any number greater than zero and less than $\mathbb{P}\left(-\sqrt{\frac{3}{p^2-1}} < N(0,1) < \sqrt{\frac{3}{p^2-1}}\right)$, then

$$\mathbb{P}\left(\frac{(p-1)n}{2} - \frac{\sqrt{n}}{2} < S_n < \frac{(p-1)n}{2} + \frac{\sqrt{n}}{2}\right)$$
$$= \mathbb{P}\left(-\sqrt{\frac{3}{p^2-1}} < \frac{S_n - \frac{(p-1)n}{2}}{\sqrt{\frac{(p^2-1)n}{12}}} < \sqrt{\frac{3}{p^2-1}}\right) > k$$

for $n$ sufficiently large.

Let $a_i$ be the coefficient of $x^i$ in $f(x)$, then

$$a_i = p^n \cdot \mathbb{P}(S_n = i).$$

Hence,

$$\sum_{i=\left\lceil \left(\frac{(p-1)n}{2} - \frac{\sqrt{n}}{2}\right)\right\rceil}^{\left\lceil \frac{(p-1)n}{2} + \frac{\sqrt{n}}{2}\right\rceil - 1} a_i \geq p^n k,$$

and so for some $i$,

$$a_i \geq \frac{p^n k}{\sqrt{n}}.$$

□

The proof of Theorem 3.2.2 now proceeds along the same lines as in section 6 of [Lac09b]. Given a group $G$ which satisfies the $b_2 - b_1$ condition for the prime $p$, and such that

$$\sup\{b_1(G_i; \mathbb{F}_p) : G_i \text{ is a finite index subgroup of } G\} = \infty,$$

pick a finite index subgroup $G_1$ of $G$ such that $b_1(G_1, \mathbb{F}_p)$ is suitably large. By results from [Lac09b], $G_1$ may be taken to be normal. Let $G_i$ be the derived $p$-series of $G_1$, let $M_i$ be the group ring $\mathbb{F}_p(G_i/G_{i+1})$, let $J_i$ be the augmentation ideal in $M_i$, and let $x_i = b_1(G_i; \mathbb{F}_p)$. By Theorem 2.3.1,

$$x_{i+1} \geq x_i \cdot \dim(M_i/J_i^l) - b_2(G_i; \mathbb{F}_p) \cdot \dim(M_i/J_i^{l-1}) - \dim(J_i/J_i^{l+1}). \tag{3.1}$$

Substituting the following

$$\dim(J_i/J_i^{l+1}) \leq p^{x_i}, \text{ and}$$
$$\dim(M_i/J_i^l) = \dim(M_i/J_i^{l-1}) + \dim(J_i^{l-1}/J_i^l),$$

in to (3.1) we can obtain

$$x_{i+1} \geq x_i \cdot \dim(J_i^{l-1}/J_i^l) - p^{x_i}\max\{1, 1 + b_2(G_i; \mathbb{F}_p) - x_i\}.$$

By Claim 3.2.3 and Jennings' Theorem, if $x_i$ is sufficiently large then

$$x_{i+1} \geq x_i \frac{p^{x_i}k}{\sqrt{x_i}} - p^{x_i}\max\{1, 1 + b_2(G_i; \mathbb{F}_p) - x_i\}.$$

The following three claims are exactly analogous to claims 1, 2, and 3 of section 6 of [Lac09b], so we do not present the proofs.

*Claim* 3.2.4. Let $\lambda$ be any positive real number less than $k$. Provided $x_1$ is sufficiently big, then for all $i \geq 1$,

$$x_{i+1} \geq \lambda p^{x_i}\sqrt{x_i}.$$

*Claim* 3.2.5. Provided $x_1$ is sufficiently big, then for all $i \geq 1$,

$$|G_1 : G_{i+1}| \leq \lambda p^{x_i} x_i (\log x_i)^{2/3}.$$

*Claim* 3.2.6. As $i \to \infty$,

$$x_i = \Omega\left(\frac{[G_1 : G_i]}{\sqrt{\log([G_1 : G_i])}\log\log([G_1 : G_i])}\right).$$

This final claim completes the proof of Theorem 3.2.2.

# Chapter 4

# Preliminaries

This chapter provides some background material that will be used in Chapter 5. None of this is original work.

## 4.1 Number Theory

In this section we present some basic number theory. Proofs of the claims can be found in almost any introductory algebraic number theory textbook. In preparing this section we used [MR03], [Mar77], and [Nar04].

### 4.1.1 Number Fields

**Definition 4.1.1.** A *number field* is a field extension of $\mathbb{Q}$ which is finite dimensional as a vector space over $\mathbb{Q}$. If $k$ is a number field the dimension of $k$ over $\mathbb{Q}$ is called the *degree* and is denoted $|k : \mathbb{Q}|$.

If $k$ is a number field then $k$ can be embedded in $\mathbb{C}$. There are exactly $|k : \mathbb{Q}|$ distinct embeddings $k \hookrightarrow \mathbb{C}$.

**Definition 4.1.2.** A complex number $\alpha$ is called *algebraic* if there is a non-zero polynomial $f(X) \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$.

Let $k$ be a number field. Every element of $k$ is algebraic: If $|k : \mathbb{Q}| = n$ then for any $\alpha \in k$ the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is linearly dependent, and so there exist $\lambda_0, \ldots, \lambda_{n-1} \in \mathbb{Q}$, not all zero, such that

$$\lambda_0 + \lambda_1\alpha + \ldots + \lambda_{n-1}\alpha^{n-1} = 0.$$

If the $N$ is the product of the denominators of the $\lambda_i$ then $f(X) = N(\lambda_0 + \lambda_1 X + \ldots + \lambda_{n-1}X^{n-1})$ is the required polynomial.

**Definition 4.1.3.** A complex number $\alpha$ is called an *algebraic integer* if there is a non-zero monic polynomial $f(X) \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$.

Fix a number field $k$. Let $R$ be the set of algebraic integers in $k$.

**Lemma 4.1.4.** *$R$ is a ring.*

**Definition 4.1.5.** The set of algebraic integers inside a number field $k$ is called the *ring of integers* in $k$.

**Lemma 4.1.6.** *If $|k : \mathbb{Q}| = n$ then, as an additive group, $R \cong \mathbb{Z}^n$.*

This lemma means that it always possible to choose a $\mathbb{Q}$-basis of $k$ consisting or algebraic integers. Moreover, every element of $k$ can be written as a fraction $\frac{x}{y}$ where $x$ and $y$ are in $R$.

**Lemma 4.1.7.** *1. For any non-zero ideal $I \leq R$ the ring $R/I$ is finite.*

*2. Every non-zero prime ideal of $R$ is maximal.*

The simple corollary of the above lemma is that for any non-zero prime ideal $\mathcal{P} \leq R$ the ring $R/\mathcal{P}$ is a finite field. The set $\mathcal{P} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, and so $\mathcal{P} \cap \mathbb{Z} = (p)$ for some prime integer $p$. It is clear that the characteristic of the field $R/\mathcal{P}$ is $p$.

Unlike in $\mathbb{Z}$, in a general number field an element cannot be uniquely expressed as a product of primes. However, ideals do have unique factorisation in to prime ideals.

**Theorem 4.1.8.** *Let $I$ be an ideal in $R$. Then*

$$I = \mathcal{P}_1 \ldots \mathcal{P}_m,$$

*where, for all $i$, the ideal $\mathcal{P}_i$ is prime. Moreover, if $(\mathcal{P}_i)_{i=1}^m$ and $(\mathcal{Q}_i)_{i=1}^n$ are finite sequences of prime ideals and*

$$\mathcal{P}_1 \ldots \mathcal{P}_m = \mathcal{Q}_1 \ldots \mathcal{Q}_n,$$

*then $m = n$ and for some permutation $\pi \in \Sigma_n$, $\mathcal{P}_i = \mathcal{Q}_{\pi i}$ for all $i$.*

A lemma that is often used in the proof of the above theorem, and which we will make use of is:

**Lemma 4.1.9.** *If $I$ and $J$ are ideals in $R$ then $I \supseteq J$ if and only if there is an ideal $I'$ such that $II' = J$.*

Given a prime integer $p$ the ideal $p\mathbb{Z}$ in $\mathbb{Z}$ is prime, but the ideal $pR$ in $R$ may not be prime. By Theorem 4.1.8, we may factor $pR$ in a unique way into prime ideals:

$$pR = \mathcal{P}_1^{e_1} \dots \mathcal{P}_m^{e_m},\ e_i \in \mathbb{Z}_{\geq 1}, \tag{4.1}$$

where each $\mathcal{P}_i$ is prime and $\mathcal{P}_i = \mathcal{P}_j$ if and only $i = j$.

We have already noted that for any prime ideal $\mathcal{P}$ in $R$, $\mathcal{P} \cap \mathbb{Z}$ is a prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$. In this case $p \in \mathcal{P}$, and so $\mathcal{P}$ divides $pR$. This shows that every prime ideal of $R$ divides a unique ideal for the form $pR$.

**Definition 4.1.10.** Where the ideal $pR$ factors as in equation 4.1, we say:

1. $\mathcal{P}$ *lies over* $p$ and $p$ *lies under* $\mathcal{P}$;

2. $e_i$ is the *ramification index* of $\mathcal{P}_i$; and

3. $p$ is *ramified* in $k$ if some $e_i$ is greater than 1, and *unramified* otherwise.

**Theorem 4.1.11.** *Let $k$ be a number field, then only finitely many primes integers are ramified in $k$.*

**Definition 4.1.12.** If the prime ideal $\mathcal{P} \subset R$ lies over the rational prime $p$ then $R/\mathcal{P}$ is finite field of characteristic $p$. The dimension of $R/\mathcal{P}$ over $\mathbb{F}_p$ is called the *inertial degree* of $\mathcal{P}$.

In order to apply the main theorem of this thesis (Theorem 5.3.1) to actual examples it's necessary to know what inertial degrees can occur for a given number field $k$. The following few results help us to do this.

**Theorem 4.1.13.** *Let $R$ be the ring of integers in a number field $k$. If*

$$pR = \mathcal{P}_1^{e_1} \dots \mathcal{P}_m^{e_m}$$

*and the inertial degree of $\mathcal{P}_i$ is $f_i$, then*

$$e_1 f_1 + \ldots + e_m f_m = |k : \mathbb{Q}|.$$

As we have remarked, if $k$ is a finite dimensional extension of $\mathbb{Q}$ then there are multiple embeddings of $k$ in to $\mathbb{C}$. For example, the field $\mathbb{Q}(2^{\frac{1}{3}})$ is isomorphic to $\mathbb{Q}[X]/(X^3 - 2)$, and there are three embeddings of $\mathbb{Q}[X]/(X^3 - 2)$ in to $\mathbb{C}$—one for each root of the polynomial $X^3 - 2$.

**Definition 4.1.14.** The extension $k$ of $\mathbb{Q}$ is called *normal* if all the embeddings of $k$ in to $\mathbb{C}$ have the same image.

The following is the corollary to Theorem 4 , Appendix 2 of [Mar77].

**Proposition 4.1.15.** *Any finite degree extension $k$ of $\mathbb{Q}$ has a normal closure. That is, there exists a field $\overline{k} \geq k$ such that $\overline{k}/\mathbb{Q}$ is a normal finite extension, and $\overline{k}$ is minimal (with respect to inclusion) among normal extensions of $\mathbb{Q}$ containing $k$.*

The following is the corollary to Theorem 23 , Chapter 3 of [Mar77].

**Proposition 4.1.16.** *If $k/\mathbb{Q}$ is normal, and $R$ is the ring of integers in $k$, and $p$ is a prime integer, then there exists prime ideals $\mathcal{P}_i$ and integers $e$ and $f$ such that*

$$pR = (\mathcal{P}_1 \dots \mathcal{P}_m)^e,$$

*where $\mathcal{P}_i = \mathcal{P}_j$ if and only if $i = j$, and the inertial degree of each $\mathcal{P}_i$ is $f$.*

In the case of the above theorem, this gives $efm = |k : \mathbb{Q}|$, by Theorem 4.1.13. By Theorem 4.1.11, there are only finitely many prime integers $p$ with are ramified, so for "most" $p$ we have $e = 1$. Exactly which $m$ and $f$ can occur for a given normal extension $k$ is given by Čebotarev's Theorem. The theorem we present here is a corollary to Čebotarev's Theorem, and is Proposition 7.36 of [Nar04]. First, some definitions:

**Definition 4.1.17.** Given a field extension $k/\mathbb{Q}$ the *Galois group* $\mathrm{Gal}(k/\mathbb{Q})$ is the group of field automorphisms of $k$ (which fix $\mathbb{Q}$).

Note that for a normal extension we have $|\mathrm{Gal}(k/\mathbb{Q})| = |k : \mathbb{Q}|$. (Appendix 2, [Mar77].)

**Definition 4.1.18.** Let $A$ be a possibly infinite set of prime integers. Then the *Dirichlet density* of $A$ is the limit (if it exists) of

$$\frac{\sum_{p \in A} p^{-s}}{\log\left(\frac{1}{s-1}\right)}$$

as $s$ tends to 1 from above.

Crucially, if $A$ is a finite set then the Dirichlet density of $A$ is 0.

Let $k/\mathbb{Q}$ be a finite field extension of degree $n$. Let $\phi_1, \ldots, \phi_n$ be the embeddings of $k$ into $\mathbb{C}$, and let $G = \mathrm{Gal}(\overline{k}/\mathbb{Q})$. Then $G$ acts on the set $\{\phi_1, \ldots, \phi_n\}$, by composition of maps.

**Theorem 4.1.19** (Čebotarev)**.** *Let $R$ be the ring of integers in $k$. The set of all prime integers $p$ which are unramified in $k$ and satisfy*

$$pR = \mathcal{P}_1 \ldots \mathcal{P}_r,$$

*for some $\mathcal{P}_i$ with given inertial degrees $\mathrm{rank}(R/\mathcal{P}_i) = f_i$ has a Dirichlet density, which equals the proportion of $G$ consisting of permutations of $\{\phi_1, \ldots, \phi_n\}$ which have $r$ disjoint cycles of orders $f_i$ respectively.*

### 4.1.2 $\mathcal{P}$-adic Completions

Fix a prime ideal $\mathcal{P}$ in $R$. This gives a filtration of $R$:

$$R \supset \mathcal{P} \supset \mathcal{P}^2 \supset \mathcal{P}^3 \supset \ldots .$$

The intersection of this descending sequence is the zero ideal $\{0\}$: For any non-zero $x$ in $R$ we can form the ideal $(x)$, and by Theorem 4.1.8 there is some positive

integer $m$ such that $\mathcal{P}^m$ does not divide $(x)$. By Lemma 4.1.9 this gives $(x) \not\subseteq \mathcal{P}^m$, and in particular $x \notin \mathcal{P}^m$.

Following the notation of [MR03], for each $x \in R\backslash\{0\}$ let $n_{\mathcal{P}}(x)$ be the largest integer such that $x \in \mathcal{P}^{n_{\mathcal{P}}(x)}$. Fix some $c \in \mathbb{R}$ such that $0 < c < 1$, then for all $x \in R\backslash\{0\}$ let $v_{\mathcal{P}}(x) = c^{n_{\mathcal{P}}(x)}$. Set $v_{\mathcal{P}}(0) = 0$, then we can extend $v_{\mathcal{P}}$ to all of $k$ by setting $v_{\mathcal{P}}(\frac{x}{y}) = v_{\mathcal{P}}(x)/v_{\mathcal{P}}(y)$, where $x \in R$ and $y \in R\backslash\{0\}$. (It is easy to check that this is well defined.)

The map $v_{\mathcal{P}} : k \to \mathbb{R}_{\geq 0}$ satisfies:

1. $v_{\mathcal{P}}(x) \geq 0$ for all $x \in k$, and $v_{\mathcal{P}}(x) = 0$ if and only if $x = 0$;
2. $v_{\mathcal{P}}(xy) = v_{\mathcal{P}}(x)v_{\mathcal{P}}(y)$ for all $x, y \in k$; and
3. $v_{\mathcal{P}}(x + y) \leq \max\{v_{\mathcal{P}}(x), v_{\mathcal{P}}(y)\}$ for all $x, y \in k$.

**Definition 4.1.20.** A map $k \to \mathbb{R}_{\geq 0}$ satisfying the above three properties is called a *non-Archimedean valuation* on $k$.

Using this valuation we can define a metric on $k$ by $d(x, y) = v_{\mathcal{P}}(x - y)$, and then set about forming the field completion in the usual way. Let $\mathcal{C}$ be the set of Cauchy sequences in $k$. Under pointwise addition and multiplication $\mathcal{C}$ is a ring with a unit. Let $\mathcal{N}$ be the subset of sequences which converge to zero. Then $\mathcal{N}$ is an ideal in $\mathcal{C}$ and $\mathcal{C}/\mathcal{N}$ is a field. There is a natural embedding of $k$ as a subfield given by $x \mapsto (x_i = x)_{i=1}^{\infty} + \mathcal{N}$.

**Definition 4.1.21.** Given a number field $k$ and a prime ideal $\mathcal{P}$ in its ring of integers, we denote the field $\mathcal{C}/\mathcal{N}$ constructed above by $k_{\mathcal{P}}$. We call $k_{\mathcal{P}}$ the *completion* of $k$ at $\mathcal{P}$.

The valuation $v_{\mathcal{P}}$ can be extended to all of $k_{\mathcal{P}}$ in the following way: Let $x \in k_{\mathcal{P}}$ and let $x$ be represented by the Cauchy sequence $(x_i)_{i=1}^{\infty}$ in $k$, then $(v_{\mathcal{P}}(x_i))_{i=1}^{\infty}$ is a Cauchy sequence of real numbers. Let

$$v_{\mathcal{P}}(x) = \lim_{i \to \infty} v_{\mathcal{P}}(x_i).$$

This is well defined: If $(x_i)_{i=1}^{\infty} \in \mathcal{N}$ then $\lim_{i\to\infty} v_{\mathcal{P}}(x_i) = 0$.

**Definition 4.1.22.** The *valuation ring* of $k_{\mathcal{P}}$ is $R_{\mathcal{P}} = \{x \in k_{\mathcal{P}} : \ v_{\mathcal{P}}(x) \leq 1\}$.

The valuation ring $R_{\mathcal{P}}$ is indeed a ring. This is because the extension of $v_{\mathcal{P}}$ to $k_{\mathcal{P}}$ has the properties of a non-Archimedean valuation. Since $v_{\mathcal{P}}(ab) = v_{\mathcal{P}}(a)v_{\mathcal{P}}(b)$ and $v_{\mathcal{P}}(a+b) \leq \max\{v_{\mathcal{P}}(a), v_{\mathcal{P}}(b)\}$ for all $a, b \in k_{\mathcal{P}}$, $R_{\mathcal{P}}$ is closed under addition, multiplication, and taking additive inverse.

The definitions of $k_{\mathcal{P}}$ and $R_{\mathcal{P}}$ given above are the definitions found in [MR03], from which we will later quote many results. However we now describe a different construction of $R_{\mathcal{P}}$ which is used in section 5.1.

Consider the sequence of ring homomorphisms:

$$R/\mathcal{P} \xleftarrow{\phi_1} R/\mathcal{P}^2 \xleftarrow{\phi_2} R/\mathcal{P}^3 \xleftarrow{\phi_3} \dots \ . \tag{4.2}$$

Let

$$\widehat{R} = \left\{ (x_1, x_2, \dots) \in \prod_{i=1}^{\infty} R/\mathcal{P}^i : \ x_i = \phi_{i+1}(x_{i+1}) \text{ for all } i \geq 1 \right\}.$$

**Definition 4.1.23.** $\widehat{R}$ is called the *inverse limit* of the system of ring homomorphisms in equation 4.2.

Again, it is easy to check that $\widehat{R}$ is ring.

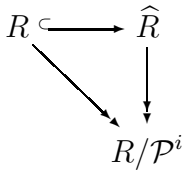
There are natural embedding of $R$ as a subring of $\widehat{R}$ given by

$$r \mapsto (r + \mathcal{P}, r + \mathcal{P}^2, \dots).$$

Moreover, there are obvious maps $\widehat{R} \to R/\mathcal{P}^i$ given by

$$(x_1, x_2, \dots) \mapsto x_i.$$

With these maps the following diagram commutes:




The crucial point about this construction is:

**Lemma 4.1.24.** $\widehat{R} \cong R_{\mathcal{P}}$.

## 4.2 Quaternion Algebras

Again, the background material presented in this section can be found in more detail in [MR03].

Let $\mathbb{F}$ be a field.

**Definition 4.2.1.** A *quaternion algebra* $A$ over $\mathbb{F}$ is a four-dimensional algebra over $\mathbb{F}$ with basis $\{\underline{1}, \underline{i}, \underline{j}, \underline{k}\}$, such that $\underline{1}$ is a multiplicative identity and

$$\underline{i}^2 = a \cdot \underline{1},\ \underline{j}^2 = b \cdot \underline{1}, \text{ and } \underline{ij} = -\underline{ji} = \underline{k},$$

where $a$ and $b$ are some fixed elements of $\mathbb{F} - \{0\}$.

We write

$$A = \left(\frac{a, b}{\mathbb{F}}\right),$$

where the symbol on the right is called a *Hilbert symbol* for $A$.

**Definition 4.2.2.** An $\mathbb{F}$-basis of $A$ is called a *standard basis* if it satisfies the conditions in Definition 4.2.1

Notice that there is not a unique Hilbert symbol for a given quaternion algebra as it depends on the choice of standard basis.

A familiar example is the two-by-two matrix algebra $M(2, \mathbb{F})$. We have

$$M(2, \mathbb{F}) \cong \left(\frac{1, 1}{\mathbb{F}}\right),$$

where

$$\underline{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \underline{i} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \text{ and } \underline{j} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{4.3}$$

Another standard basis of $M(2, \mathbb{F})$ is

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 6 \\ -6 & 0 \end{pmatrix} \right\}.$$

(Assuming the characteristic of $\mathbb{F}$ is not 2 or 3.) This basis shows the isomorphism

$$M(2, \mathbb{F}) \cong \left(\frac{4, 9}{\mathbb{F}}\right).$$

As an example of of an $\mathbb{F}$-basis which is not standard, consider

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

This is not a standard basis as every element squares to zero.

**Definition 4.2.3.** Let $A = \left(\frac{a,b}{\mathbb{F}}\right)$ have a standard basis $\{\underline{1}, \underline{i}, \underline{j}, \underline{k}\}$. Let $A_0$ be the $\mathbb{F}$-span of $\{\underline{i}, \underline{j}, \underline{k}\}$. Then elements of $A_0$ are the *pure quaternions* in $A$.

This definition does not depend on the choice of standard basis. Note that

$$(\lambda_0\underline{1} + \lambda_1\underline{i} + \lambda_2\underline{j} + \lambda_3\underline{k})^2 = (\lambda_0^2 + a\lambda_1^2 + b\lambda_2^2 - ab\lambda_3^3)\underline{1} + 2\lambda_0(\lambda_1\underline{i} + \lambda_2\underline{j} + \lambda_3\underline{k}),$$

and so $x \in A_0 \backslash \{0\}$ if and only if $x \notin \mathbb{F} \cdot \underline{1}$ and $x^2 \in \mathbb{F} \cdot \underline{1}$.

**Definition 4.2.4.** Given any $x \in A$ we can express $x$ in a unique way as $x = \lambda\underline{1} + x_0$ where $x_0 \in A_0$. The *conjugate* of $x$ is

$$\overline{x} = \lambda\underline{1} - x_0.$$

The *trace* of $x$ is

$$\mathrm{tr}(x) = x + \overline{x}.$$

The *norm* of $x$ is

$$\mathrm{n}(x) = x\overline{x}.$$

Both norm and the trace are maps from $A$ to $\mathbb{F} \cdot \underline{1}$, but we typically treat them as maps to $\mathbb{F}$.

For the quaternion algebra $M(2, \mathbb{F})$ the trace and norm coincide with the usual trace and determinant maps.

If $\mathbb{F}$ is a subfield of $\mathbb{K}$ then

$$\left(\frac{a,b}{\mathbb{F}}\right) \otimes_{\mathbb{F}} \mathbb{K} \cong \left(\frac{a,b}{\mathbb{K}}\right).$$

The following result will be crucial in Section 5.2. It is Theorem 2.7.3 of [MR03], combined with Corollary 2.6.4 and Definition 2.7.1 of the same work.

**Theorem 4.2.5** ([MR03]). *Let $A$ be a quaternion algebra over the number field $k$. Let $R$ be the ring of integers in $k$. There is a finite list of prime ideals in $R$ such that if $\mathcal{P}$ is a prime ideal of $R$ not in the list, then*

$$A \otimes_k k_{\mathcal{P}} \cong M(2, k_{\mathcal{P}}).$$

There is one more technical result about quaternion algebras that we record for later use. Let $k$ be a number field, let $R$ be its ring of integers, and let $\mathcal{P}$ be a prime ideal in $R$. Let $A$ be a quaternion algebra over $k_{\mathcal{P}}$.

**Definition 4.2.6.** An *order* $\mathcal{O}$ in $A$ is a finitely-generated $R_{\mathcal{P}}$-submodule of $A$ such that $\underline{1} \in \mathcal{O}$ and $\mathcal{O} \otimes_{R_{\mathcal{P}}} k_{\mathcal{P}} = A$. An order is *maximal* if it is maximal with respect to inclusion.

For example, if $A = \left(\frac{a,b}{k_{\mathcal{P}}}\right)$, where $a$ and $b$ are in $R_{\mathcal{P}}$, then $R_{\mathcal{P}}[\underline{1}, \underline{i}, \underline{j}, \underline{k}]$ is an order in $A$.

The following is Theorem 6.5.3 in [MR03].

**Theorem 4.2.7** ([MR03]). *All maximal orders in $M(2, k_{\mathcal{P}})$ are conjugate to the maximal order $M(2, R_{\mathcal{P}})$.*

## 4.3 Finite Groups

Recall that if $G$ is a finite group then a *composition series* for $G$ is a strictly descending sequence

$$G = G_1 \rhd G_2 \rhd \ldots \rhd G_m = 1$$

such that every $G_i/G_{i+1}$ is a simple group. Every finite group has a composition series, and the resulting simple quotients are called *composition factors*. The Jordan-Hölder Theorem says that if

$$G = G'_1 \rhd G'_2 \rhd \ldots \rhd G'_n = 1$$

is another composition series for $G$ then the composition factors are the same. More precisely, $m = n$ and there is a permutation $\pi \in \Sigma_{m-1}$ such that $G_i/G_{i+1} \cong G'_{\pi i}/G'_{\pi i+1}$.

The following lemma will be used in a later section and is a simple application of the Jordan-Hölder Theorem. It is reminiscent of a theorem of P. Hall [Hal36], for which the clearest statement and proof is Lemma 3.7 in Dunfield and Thurston's paper [DT06]. Our version is slightly different, and is certainly easier to prove.

**Lemma 4.3.1.** *Let $G$ be a group. Let $\{H_i\}_{i=1}^m$ be a finite collection of finite groups such that if $i \neq j$ then $H_i$ and $H_j$ have no composition factors in common. If $\phi : G \to H_1 \times \ldots \times H_m$ is a homomorphism such that every induced map $G \to H_i$ is surjective then $\phi$ is surjective.*

*Proof.* For every $i$ the homomorphism $\mathrm{Im}(\phi) \to H_i$ is surjective, hence for every $i$, every composition factor of $H_i$ is a composition factor of $\mathrm{Im}(\phi)$. Since distinct $H_i$ and $H_j$ have no composition factors in common, $|\mathrm{Im}(\phi)| \geq |H_1| \times \ldots \times |H_m|$, and so $\mathrm{Im}(\phi) = H_1 \times \ldots \times H_m$. □

## 4.4 Profinite and Pro-$p$ Groups

This is a very brief introduction to profinite and pro-$p$ groups. A more extensive treatment of this material can be found in Chapter 1 of [DdSMS99].

Profinite (and pro-$p$) groups are constructed in a similar way to the $\mathcal{P}$-adic completion of a number field $R$ that we saw in section 4.1.

Let $I$ be a directed set. That is, $I$ has a partial order such that whenever $i, j \in I$ there is some $k \in I$ such that $i \leq k$ and $j \leq k$. Let $\{G_i : i \in I\}$ be a collection of finite groups indexed by $I$ with a homomorphism $\phi_{ij} : G_i \to G_j$ for each $i \geq j$, such that for all $i \geq j \geq k$ we have $\phi_{ik} = \phi_{jk} \cdot \phi_{ij}$. The collection of groups $G_i$ together with the homomorphisms $\phi_{ij}$ form an *inverse system*.

The *inverse limit* of this system is a subgroup of $\prod_{i \in I} G_i$. Specifically,

$$\lim_{\leftarrow} G_i = \left\{ (x_i : i \in I) \in \prod_{i \in I} G_i : \text{for all } i \text{ and } j \text{ with } i \geq j,\ \phi_{ij}(x_i) = x_j \right\}.$$

The group $\lim_{\leftarrow} G_i$ can be topologised in the following way: Put the discrete topology on each $G_i$, and put the product topology on $\prod_{i \in I} G_i$. Then give $\lim_{\leftarrow} G_i$ the subspace topology.

**Definition 4.4.1.** The group $\lim_{\leftarrow} G_i$ constructed above, together with the given topology, is called a *profinite group*. If each $G_i$ is a $p$-group for some prime $p$ then the group is called a *pro-p group*.

Starting with a fixed group $G$ it is possible to construct profinite groups from $G$. Let $\{N_i : i \in I\}$ be a collection of finite index normal subgroups in $G$ such that for all $i, j \in I$ there exists $k \in I$ such that $N_i \cap N_j \supseteq N_k$. Then the collection $\{G/N_i : i \in I\}$ naturally forms an inverse system and $\lim_{\leftarrow} G/N_i$ is a profinite group.

**Definition 4.4.2.** If $\{N_i\}$ is taken to be the collection of all finite index normal subgroups of $G$, or the collection of all normal subgroups of index a power of $p$, where $p$ is a fixed prime integer, then the inverse limit of the system $\{G/N_i\}$ is called the *profinite completion* or the *pro-p completion* of $G$.

The main example that we will consider is $SL(2, R_{\mathcal{P}})$. This is a profinite group:

**Lemma 4.4.3.** *If $R$ is the ring of integers in a number field and $\mathcal{P}$ is a prime ideal in $R$, then $SL(2, R_{\mathcal{P}})$ is a profinite group. In particular, $SL(2, R_{\mathcal{P}})$ is isomorphic to the inverse limit of*

$$SL(2, R/\mathcal{P}) \leftarrow SL(2, R/\mathcal{P}^2) \leftarrow SL(2, R/\mathcal{P}^3) \leftarrow \dots \ .$$

*Proof.* The maps $R_{\mathcal{P}} \to R/\mathcal{P}^i$ induce group homomorphisms $SL(2, R_{\mathcal{P}}) \to SL(2, R/\mathcal{P}^i)$. Form the product homomorphism

$$SL(2, R_{\mathcal{P}}) \to \prod_{i \geq 1} SL(2, R/\mathcal{P}^i).$$

It is clear that this is a map to the inverse limit of $\{SL(2, R/\mathcal{P}^i)\}_i$, and injectivity and surjectivity are also clear. □

Here are a few facts about profinite groups, taken from [DdSMS99].

**Proposition 4.4.4.** *Let $G$ be a profinite (or pro-p) group.*

1. *As a topological space $G$ is Hausdorff and compact.*

2. *$G$ is a topological group. That is, the maps $G \to G$ and $G \times G \to G$ given by $g \mapsto g^{-1}$ and $(g, h) \mapsto gh$ are continuous.*

3. *Any open neighborhood around the identity is a union of open subgroups.*

4. *An open subgroup of $G$ is closed, has finite index in $G$, and contains an open normal subgroup of $G$.*

5. *A closed subgroup of $G$ is open if and only if it has finite index in $G$.*

6. *The intersection of all open subgroups of $G$ is the trivial subgroup.*

7. *A sequence $(g_i)_{i=1}^{\infty}$ is convergent in $G$ if and only if it is Cauchy. (The sequence is Cauchy if for each open normal subgroup $N$ in $G$ there exists an integer $m$ such that if $i, j \geq m$ then $g_i g_j^{-1} \in N$.)*

**Definition 4.4.5.** If $G$ is a topological group and $X \subseteq G$ then $X$ *topologically generates* $G$ if $G = \overline{\langle X \rangle}$, where $\overline{\langle X \rangle}$ is the topological closure of the subgroup generated (in the usual group-theoretic way) by $X$.

Given a prime $p$ we have previously defined the lower $p$-central series of a group, denoted by $P_i(\cdot)$. The definition must be changed slightly to accommodate profinite groups. Note that if a finite group is given the discrete topology then it becomes a profinite group, in which case the following two definitions coincide with the usual versions from pure group theory.

**Definition 4.4.6.** Let $G$ be a profinite group, and $p$ a prime integer. Let $P_1(G) = G$ and define the lower $p$-central series for $G$ inductively by

$$P_{i+1}(G) = \overline{[G, P_i(G)] P_i(G)^{(p)}}.$$

**Definition 4.4.7.** Let $G$ be a profinite group. The *Frattini subgroup* of $G$, denoted $\Phi(G)$, is the intersection of all maximal open subgroups of $G$.

**Proposition 4.4.8.** *Let $G$ be a profinite group.*

1. *A subset $X \subseteq G$ generates $G$ topologically if and only if the image of $X$ in $G/\Phi(G)$ is a topological generating set for $G/\Phi(G)$.*

2. *If $G$ is a pro-$p$ group for some prime $p$ then $\Phi(G) = P_2(G)$.*

**Definition 4.4.9.** A pro-$p$ group $G$ is called *powerful* if $p > 2$ and $G/\overline{G^{(p)}}$ is abelian, or if $p = 2$ and $G/\overline{G^{(4)}}$ is abelian.

**Definition 4.4.10.** A pro-$p$ group $G$ is *uniformly powerful* if $G$ is powerful and for all $m$, $|P_m(G) : P_{m+1}(G)| = |G : P_2(G)|$.

Powerful pro-$p$ groups were defined and studied by Lubotzky and Mann in [LM87]. Uniformly powerful pro-$p$ groups were defined and studied by Dixon, Du Sautoy, Mann, and Segal in [DdSMS99]. The following lemma is set as Exercise 11.4 in [DdSMS99].

**Lemma 4.4.11.** *If $G$ is a powerful pro-$p$ group then $P_{n+1}(G) = D_m(G)$ where $p^{n-1} < m \leq p^n$.*

*Proof.* We will prove the result by induction on $m$. For $m = 2$ the equation $p^{n-1} < m \leq p^n$ is satisfied by $n = 1$, and then $P_{n+1}(G) = D_m(G)$ as required. (See section 3.1.)

Suppose the result holds for all positive integers up to and including $m$. We consider two cases.

**Case One**: $p^{n-1} < m < p^n$. In this case $D_m(G) = P_{n+1}(G)$, and we need to show that $D_{m+1}(G) = P_{n+1}(G)$ also. By definition 3.1.1,

$$D_{m+1}(G) = D_{\lceil \frac{m+1}{p} \rceil}(G)^{(p)} \prod_{i+j=m+1} [D_i(G), D_j(G)]. \tag{4.4}$$

Now, $p^{n-2} < \lceil \frac{m+1}{p} \rceil \leq p^{n-1}$, so, by induction, $D_{\lceil \frac{m+1}{p} \rceil} = P_n(G)$. Theorem 3.6 of [DdSMS99] says that as $G$ is a powerful pro-$p$ group we have $P_n(G)^{(p)} = P_{n+1}(G)$ for all $n \geq 1$. Hence

$$D_{m+1}(G) = P_{n+1}(G) \prod_{i+j=m+1} [D_i(G), D_j(G)].$$

If $i$ and $j$ are positive integers with $i + j = m + 1$ then at least one of $i$ or $j$ is greater than $\frac{m}{2}$. Since $\frac{m}{2} > p^{n-2}$ at least on of $i$ or $j$ is greater than $p^{n-2}$. Suppose $i > p^{n-2}$, then by induction $D_i(G) \subseteq P_n(G)$, hence $[D_i(G), D_j(G)] \subseteq P_{n+1}(G)$. This gives $D_{m+1}(G) = P_{n+1}(G)$, which completes Case One.

**Case Two**: $m = p^n$. In this case $D_m(G) = P_{n+1}(G)$ as before, but now we need to show $D_{m+1}(G) = P_{n+2}(G)$. We use the equation 4.4 again. By induction $D_{\lceil \frac{m+1}{p} \rceil}(G) = P_{n+1}(G)$, since $\lceil \frac{m+1}{p} \rceil = p^{n-1} + 1$. By Theorem 3.6 of [DdSMS99], $P_{n+1}(G)^{(p)} = P_{n+2}(G)$, and so

$$D_{m+1}(G) = P_{n+2}(G) \prod_{i+j=m+1} [D_i(G), D_j(G)].$$

As before, if $i + j = m + 1$ then at least one of $i$ or $j$ must be greater than $\frac{m}{2}$. Since $\frac{m}{2} \geq p^{n-1}$, at least one of $i$ of $j$ must be greater than $p^{n-1}$. If $i > p^{n-1}$ then by induction $D_i(G) \subseteq P_{n+1}(G)$, so $[D_i(G), D_j(G)] \subseteq P_{n+2}(G)$. This gives $D_{m+1}(G) = P_{n+2}(G)$, as required. □

## 4.5 Groups of Isometries of Hyperbolic 3-Space

In this section we give a few definitions and assorted facts related to groups of isometries of hyperbolic 3-space. This material can be found in [MR03] and [Thu80].

Let $U = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_3 > 0\}$. At each point $x \in U$ there is a standard Euclidean inner product $\langle \cdot, \cdot \rangle_{\mathbb{E}}$ on $T_xU$, the tangent space to $U$ at $x$. For all points $x = (x_1, x_2, x_3)$ in $U$ and for all vectors $u$ and $v$ in $T_xU$, define

$$\langle u, v \rangle_{\mathbb{H}} = \frac{\langle u, v \rangle_{\mathbb{E}}}{x_3^2}.$$

Then $\langle \cdot, \cdot \rangle_{\mathbb{H}}$ is a Riemannian metric on $U$, and the space $U$ together with this Riemannian metric is called the *upper half-space* model of hyperbolic 3-space. It will be denoted by $\mathbb{H}^3$.

Let $\mathrm{Isom}^+(\mathbb{H}^3)$ be the group of orientation preserving isometries of $\mathbb{H}^3$.

**Theorem 4.5.1.** $\mathrm{Isom}^+(\mathbb{H}^3) \cong PSL(2, \mathbb{C})$.

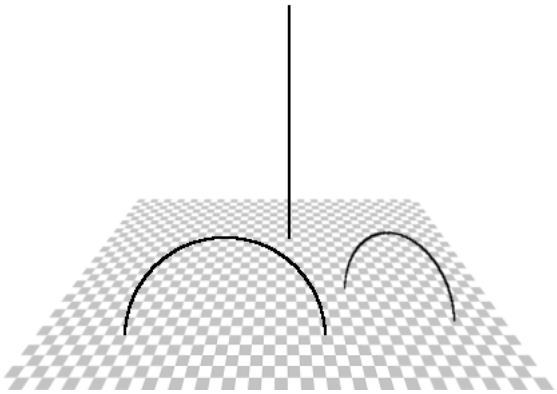


Figure 4.1: Some geodesics in $\mathbb{H}^3$.

The nature of this isomorphism is easy to explain. Let $p^\infty$ be the extra point in the one-point compactification of $\overline{U}$ (where $\overline{U}$ is the closure of $U$ in $\mathbb{R}^3$). Then $S = \partial U \cup \{p^\infty\}$ is called the *sphere at infinity* of $\mathbb{H}^3$. It is topologically a 2-sphere. The isometry group $\mathrm{Isom}^+(\mathbb{H}^3)$ extends in a unique way to act by homeomorphism on $\mathbb{H}^3 \cup S$. Moreover, an element of $\mathrm{Isom}^+(\mathbb{H}^3)$ is determined by its action on $S$. Identify $\partial U = \{(x_1, x_2, 0) : x_1, x_2 \in \mathbb{R}\}$ with $\mathbb{C}$ and $p^\infty$ with $\infty$, then the action of $\mathrm{Isom}^+(\mathbb{H}^3)$ on $S$ corresponds to the action of $PSL(2,\mathbb{C})$ on $\mathbb{C} \cup \{\infty\}$ given by

$$\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d}.$$

The geodesics in $\mathbb{H}^3$ are the Euclidean straight lines and half circles which meet $\partial U$ at right angles (see figure 4.1).

The orientation preserving isometries of $\mathbb{H}^3$ split in to three types:

1. *Elliptic* isometries rotate $\mathbb{H}^3$ around a geodesic. In particular an elliptic isometry has fixed points in $\mathbb{H}^3$. For example, the map $(x_1, x_2, x_3) \mapsto (x_1\cos(\theta) - x_2\sin(\theta), x_1\sin(\theta) + x_2\cos(\theta), x_3)$, where $\theta \in \mathbb{R}$, is an isometry, and is a rotation around the geodesic $\{(0, 0, x_3) : x_3 > 0\}$. Its action on $S = \mathbb{C} \cup \{\infty\}$ is $z \mapsto e^{-i\theta}z$, and so it fixes 0 and $\infty$, but no other points of $S$.

2. *Loxodromic* isometries translate along a geodesic (possibly combined with rotating around the same geodesic). A loxodromic isometry has no fixed points in $\mathbb{H}^3$. For example, the map $(x_1, x_2, x_3) \mapsto (\lambda x_1, \lambda x_2, \lambda x_3)$, where $\lambda > 0$ and $\lambda \neq 1$, is

an isometry, and is a translation along the the geodesic $\{(0,0,x_3) : x_3 > 0\}$. Its action on $S$ is given by $z \mapsto \lambda z$, and so it fixes 0 and $\infty$, but no other points of $S$.

3. *Parabolic* isometries fix a single point in $S$, and no points of $\mathbb{H}^3$. For example, the map $(x_1, x_2, x_3) \mapsto (x_1 + a, x_2 + b, x_3)$, where $a, b \in \mathbb{R}$ and are not both zero, is an isometry. Its action on $S$ is $z \mapsto z + (a + bi)$, and so the only point of $S$ which is fixed is $\infty$.

**Lemma 4.5.2.** *Let $A \in PSL(2,\mathbb{C})\backslash\{\pm\mathbb{1}_2\}$. Then $A$ is parabolic if and only if* $\mathrm{tr}(A) = \pm 2$*, (Note that trace is defined on $PSL(2,\mathbb{C})$ up to sign.)*

*Proof.* Every isometry of $\mathbb{H}^3$ fixes a point in $S$. Since $PSL(2,\mathbb{C})$ acts transitively on $S$, by conjugating if necessary we can assume that $A$ fixes $\infty$. (Note that conjugation does not change the type of isometry, nor the trace.)

Since $A$ fixes $\infty$ it has the form

$$A = \pm \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$$

This corresponds to the map $z \mapsto a^2 z + ab$.

We must show that $A$ fixes a single point in $S$ if and only if $\mathrm{tr}(A) = \pm 2$. The map $z \mapsto a^2 z + ab$ has no fixed points in $\mathbb{C}$ if and only if $a^2 = 1$. That is, if and only if $\mathrm{tr}(A) = a + a^{-1} = \pm 2$. □

**Definition 4.5.3.** Let $\Gamma$ be a discrete group of orientation preserving isometries of $\mathbb{H}^3$. Let $p \in \mathbb{H}^3$. Then the *limit set* of $\Gamma$, denoted $\Lambda(\Gamma)$, is defined to be the set of accumulation points of $\Gamma_p$ in $S \cup \mathbb{H}^3$, where $\Gamma_p = \{\gamma(p) : \gamma \in \Gamma\}$.

Two points to note: $\Lambda(\Gamma)$ does not depend on the choice of $p$; and $\Lambda(\Gamma) \subseteq S$.

**Definition 4.5.4.** A discrete group $\Gamma$ of orientation preserving isometries of $\mathbb{H}^3$ is called *elementary* if $|\Lambda(\Gamma)| = 0$, 1, or 2. Otherwise it is called *non-elementary*.

Here are a few facts related to limit sets and (non-)elementary groups.

**Proposition 4.5.5.** *1. $\Gamma$ is elementary if and only if it is virtually abelian.*

*2. If $\Gamma$ is a non-elementary group and $\Gamma' \trianglelefteq \Gamma$ is a normal subgroup with $\Gamma' \neq 1$ then $\Lambda(\Gamma') = \Lambda(\Gamma)$.*

*3. If $\Gamma$ is a non-elementary group then $\Gamma$ contains a loxodromic element.*

Part 1 is Proposition 8.1.1 and part 2 is Corollary 8.1.3 in [Thu80]. Part 3 is from Theorem 1.2.2 in [MR03].

A standard application of parts 1 and 2 of the above proposition is:

**Proposition 4.5.6.** *Let $\Gamma$ be non-elementary. Then every term in the derived series of $\Gamma$ is non-elementary. (In particular $\Gamma$ is not soluble.)*

*Proof.* Let $\Gamma_1 = \Gamma$ and for $i \geq 2$ let $\Gamma_i = [\Gamma_{i-1}, \Gamma_{i-1}]$, so $\Gamma_i$ is the derived series of $\Gamma$. By induction assume $\Gamma_{i-1}$ is non-elementary. By part 2 of Proposition 4.5.5 either $\Lambda(\Gamma_i) = \Lambda(\Gamma_{i-1})$ and so $\Gamma_i$ is non-elementary, or $\Gamma_i = 1$. However, by part 1 of 4.5.5, the later case cannot occur because $\Gamma_{i-1}$ is non-elementary. □

**Definition 4.5.7.** A 3-manifold (possibly with boundary) is called *hyperbolic* if its interior is homeomorphic to $\mathbb{H}^3/\Gamma$, where $\Gamma$ is a group of orientation preserving isometries of $\mathbb{H}^3$ which acts freely and properly discontinuously on $\mathbb{H}^3$.

In this case $\mathbb{H}^3 \to \mathbb{H}^3/\Gamma$ is a covering map, and so $\Gamma = \pi_1(\mathbb{H}^3/\Gamma)$ since $\mathbb{H}^3$ is simply connected.

**Proposition 4.5.8.** *If $\Gamma$ is the fundamental group of a finite-volume hyperbolic 3-manifold then $\Gamma$ is non-elementary.*

Since $PSL(2,\mathbb{C}) = SL(2,\mathbb{C})/\{\pm \mathbb{1}_2\}$ it is clear that $SL(2,\mathbb{C})$ also has an action by isometries on $\mathbb{H}^3$. We prefer to work with $SL(2,\mathbb{C})$, and so make use of the following theorem:

**Proposition 4.5.9.** *Let $\Gamma$ be the fundamental group of a complete finite-volume hyperbolic 3-manifold $M$. Then there is a representation $\phi : \Gamma \to SL(2,\mathbb{C})$ such that $M = \mathbb{H}^3/\phi(\Gamma)$.*

# Chapter 5

# Congruence Subgroups of Hyperbolic 3-Manifold Groups

In this chapter we prove the main result of this thesis, Theorem 5.3.1, on the homology growth of congruence subgroups in hyperbolic 3-manifold groups. We start in Section 5.1 by studying the group $SL(n, R_{\mathcal{P}})$. In Section 5.2 we show that a hyperbolic 3-manifold group virtually embeds as a dense subgroup in $SL(2, R_{\mathcal{P}})$, for a particular $R$ and good choices of $\mathcal{P}$. In Section 5.3 we prove Theorem 5.3.1 and a simple corollary.

## 5.1 The Structure of $SL(n, R_{\mathcal{P}})$

The aim of this section is to prove the following theorem.

**Theorem 5.1.1.** *Let $R$ be the ring of integers in a number field, and let $\mathcal{P}$ be a prime ideal lying over the rational prime $p$, with ramification index $e$. For $m \geq 0$ let $G_m$ be the principal congruence subgroup*

$$G_m = \mathrm{Ker}\left(SL(n, R_{\mathcal{P}}) \to SL(n, R/\mathcal{P}^m)\right).$$

*Let $l \geq 2$ if $p = 2$ and $l \geq 1$ if $p > 2$. Then $G_{el}$ is a uniformly powerful pro-$p$ group with $|G_{el} : P_2(G_{el})| = (n^2 - 1) \cdot \mathrm{rank}(R/\mathcal{P}^e)$. Moreover $P_i(G_{el}) = G_{e(l+i-1)}$.*

This theorem is analogous to Theorem 5.2 of [DdSMS99] where the group $GL(n, \widehat{\mathbb{Z}_p})$ is considered. The proofs of all lemmas in this section use the methods of that book, and in some cases closely follow proofs given there.

Fix $R$ and $\mathcal{P}$ for the rest of this section.

**Lemma 5.1.2.** *For any $m$ the map $SL(n, R_{\mathcal{P}}) \to SL(n, R/\mathcal{P}^m)$ is surjective.*

*Proof.* Let $A$ be an $n \times n$ matrix with entries in $R$ such that $det(A) = 1 + x$, where $x$ is in $\mathcal{P}^m$. (That is, the image of $A$ is in $SL(n, R/\mathcal{P}^m)$.) Let $r$ be the element of $R_{\mathcal{P}}$ given by the series

$$r = 1 - x + x^2 - x^3 + \dots.$$

The matrix

$$\begin{pmatrix} r & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} A$$

is in $SL(n, R_{\mathcal{P}})$ and has the same image in $SL(n, R/\mathcal{P}^m)$ as $A$. □

**Lemma 5.1.3.** *Let $e$ be the ramification index of $\mathcal{P}$. For all $m \geq 1$ the map $x \mapsto px$ induces an additive group isomorphism $\mathcal{P}^{e(m-1)}/\mathcal{P}^{em} \to \mathcal{P}^{em}/\mathcal{P}^{e(m+1)}$. (Note that $\mathcal{P}^0 = R$.)*

*Proof.* Let $\phi : \mathcal{P}^{e(m-1)} \to \mathcal{P}^{em}/\mathcal{P}^{e(m+1)}$ be the map induced by $x \mapsto px$. This is clearly a group homomorphism. Let $y \in \mathcal{P}^{em}$. Since $\mathcal{P}^{em} = (p)^m + \mathcal{P}^{e(m+1)}$ there exist $y' \in (p)^m$ and $z \in \mathcal{P}^{e(m+1)}$ such that $y = y' + z$. For some $r \in R$, $y' = p^m r$. Set $x = p^{m-1}r$, then $x \in \mathcal{P}^{e(m-1)}$ and $\phi(x) = y + \mathcal{P}^{e(m+1)}$. Hence $\phi$ is surjective. Finally,

$$x \in \ker(\phi) \Leftrightarrow px \in \mathcal{P}^{e(m+1)} \Leftrightarrow \mathcal{P}^{e(m+1)} | (p)(x)$$
$$\Leftrightarrow \mathcal{P}^{em} | (x) \Leftrightarrow x \in \mathcal{P}^{em},$$

hence $\phi$ induces a group isomorphism $\mathcal{P}^{e(m-1)}/\mathcal{P}^{em} \to \mathcal{P}^{em}/\mathcal{P}^{e(m+1)}$. □

Notice that $R/\mathcal{P}^e$ is a quotient of $R/(p)$, and hence is an elementary abelian $p$-group. Thus every $\mathcal{P}^{em}/\mathcal{P}^{e(m+1)}$ is an elementary abelian $p$-group, and they all have the same rank.

**Theorem 5.1.4.** *For all $m \geq 1$ the quotient $G_{em}/G_{e(m+1)}$ is an elementary abelian $p$-group of rank $(n^2 - 1) \cdot \text{rank}(R/\mathcal{P}^e)$.*

*Proof.* Viewing $G_{em}/G_{e(m+1)}$ as a subgroup of $SL(n, R/\mathcal{P}^{e(m+1)})$, elements of $G_{em}/G_{e(m+1)}$ are $n \times n$ matrices $A$ with entries in $R/\mathcal{P}^{e(m+1)}$, such that $A \equiv \mathbb{1}_n \bmod \mathcal{P}^{em}$ and $\det(A) = 1$. By Lemma 5.1.2, $G_{em}/G_{e(m+1)}$ consists of all such matrices. Every element of $G_{em}/G_{e(m+1)}$ can be written as

$$\mathbb{1}_n + X,$$

where $X$ is an $n \times n$ matrix with entries in $\mathcal{P}^{em}/\mathcal{P}^{e(m+1)}$.

Conversely, any such matrix is in $SL(n, R/\mathcal{P}^{e(m+1)})$ as long it has determinant 1. Since the product of any two elements of $\mathcal{P}^{em}/\mathcal{P}^{e(m+1)}$ is zero,

$$\det(\mathbb{1}_n + X) = 1 + \mathrm{tr}(X).$$

Let $M^0\left(n, \mathcal{P}^{em}/\mathcal{P}^{e(m+1)}\right)$ be the additive group of $n \times n$ matrices over $\mathcal{P}^{em}/\mathcal{P}^{e(m+1)}$ with trace 0.

Define $\phi : M^0\left(n, \mathcal{P}^{em}/\mathcal{P}^{e(m+1)}\right) \to G_{em}/G_{e(m+1)}$ by $X \mapsto \mathbb{1}_n + X$. Then $\phi$ is a bijection and for all $X, Y \in M^0\left(n, \mathcal{P}^{em}/\mathcal{P}^{e(m+1)}\right)$,

$$\phi(X)\phi(Y) = (\mathbb{1}_n + X)(\mathbb{1}_n + Y) = \mathbb{1}_n + X + Y = \phi(X + Y).$$

Notice that $(\mathbb{1}_n + X)^{-1} = (\mathbb{1}_n - X)$, and so

$$\phi(-X) = \mathbb{1}_n - X = \phi(X)^{-1}.$$

Hence,

$$M^0\left(n, \mathcal{P}^{em}/\mathcal{P}^{e(m+1)}\right) \cong G_{em}/G_{e(m+1)}.$$

We have already noted that $\mathcal{P}^{em}/\mathcal{P}^{e(m+1)}$ is an elementary abelian $p$-group of rank $\mathrm{rank}(R/\mathcal{P}^e)$, and so the proof is complete. □

**Corollary 5.1.5.** *For all $m \geq 1$, $G_{em}$ is a pro-$p$ group.*

*Proof.* Recall (Lemma 4.4.3) that $SL(2, R_{\mathcal{P}})$ is isomorphic to the inverse limit of

$$SL(2, R/\mathcal{P}) \leftarrow SL(R/\mathcal{P}^2) \leftarrow \dots \ .$$

By Lemma 5.1.2 this is the same as

$$SL(2, R_{\mathcal{P}})/G_1 \leftarrow SL(R_{\mathcal{P}})/G_2 \leftarrow \dots \ .$$

Thus the subgroup $G_{em}$ corresponds to the inverse limit of

$$G_{em}/G_{em+1} \leftarrow G_{em}/G_{em+2} \leftarrow \dots .$$

By Theorem 5.1.4 these are all finite $p$-groups, and so $G_{em}$ is a pro-$p$ group. □

**Lemma 5.1.6.** *Let $m \geq 2$, then the map $x \mapsto x^p$ induces an isomorphism $G_{e(m-1)}/G_{em} \to G_{em}/G_{e(m+1)}$.*

*Proof.* We can string together the following natural isomorphisms:

$$G_{e(m-1)}/G_{em} \to M^0(n, \mathcal{P}^{e(m-1)}/\mathcal{P}^{em}) \to M^0(n, \mathcal{P}^{em}/\mathcal{P}^{e(m+1)}) \to G_{em}/G_{e(m+1)}.$$

Let $\mathbb{1}_n + X$, where $X$ is an $n \times n$ matrix over $\mathcal{P}^{e(m-1)}$, be an element of $G_{e(m-1)}$. Its image in $G_{e(m-1)}/G_{em}$ is mapped by the above isomorphisms in the following way,

$$\mathbb{1}_n + X \mapsto X \mapsto pX \mapsto \mathbb{1}_n + pX.$$

Now,

$$\begin{aligned}(\mathbb{1}_n + X)^p &= \mathbb{1}_n + pX + X^2(\dots) \\ &\cong \mathbb{1}_n + pX \bmod G_{e(m+1)}.\end{aligned}$$

□

**Proposition 5.1.7.** *For $m \geq 2$ and $s \geq 1$ the map $x \mapsto x^{p^s}$ induces an isomorphism $G_{e(m-1)}/G_{em} \to G_{e(m+s-1)}/G_{e(m+s)}$.*

*Proof.* By induction. □

**Lemma 5.1.8.**

$$[G_l, G_m] \leq G_{l+m}.$$

*Proof.* Let $\mathbb{1}_n + A \in G_l$ and $\mathbb{1}_n + B \in G_m$. Note that

$$(\mathbb{1}_n + A)^{-1} \equiv \mathbb{1}_n - A + A^2 - A^3 + \ldots, \text{ and}$$
$$(\mathbb{1}_n + B)^{-1} \equiv \mathbb{1}_n - B + B^2 - B^3 + \ldots.$$

The following calculation shows the result,

$$\begin{aligned}
&[\mathbb{1}_n + A, \mathbb{1}_n + B] \\
=&(\mathbb{1}_n + A)(\mathbb{1}_n + B)(\mathbb{1}_n - A + A^2 - \ldots)(\mathbb{1}_n - B + B^2 - \ldots) \\
=&(\mathbb{1}_n + (A+B) + AB)((\mathbb{1}_n - (A+B) + (A^2+B^2) - (A^3+B^3) + \ldots) + AB(\ldots)) \\
=&\mathbb{1} + AB(\ldots) \in G_{l+m}.
\end{aligned}$$

□

**Lemma 5.1.9.** *If $p > 2$ and if $A \in G_{el}$ and $B \in G_{em}$ where $l \geq 1$ and $m \geq 1$ then $(AB)^p \equiv A^p B^p$ modulo $G_{e(l+m+1)}$.*

*Proof.* Since $[B^{-1}, A^{-1}]$ is in $G_{e(l+m)}$ it commutes with $A$ and $B$ modulo $G_{e(l+m+1)}$. Hence

$$(AB)^p \equiv A^p B^p [B^{-1}, A^{-1}]^{\frac{p(p-1)}{2}} \bmod G_{e(l+m+1)}.$$

Since $p$ divides $\frac{p(p-1)}{2}$ and $G_{e(l+m)}/G_{e(l+m+1)}$ is an elementary abelian $p$-group,

$$[B^{-1}, A^{-1}]^{\frac{p(p-1)}{2}} \equiv \mathbb{1}_n \bmod G_{e(l+m+1)}.$$

□

The proof of the next proposition follows the proof of Lemma 5.1 of [DdSMS99] where the same result is proved in the case of $GL(n, \widehat{\mathbb{Z}_p})$

**Proposition 5.1.10.** *Let $l \geq 2$ if $p = 2$ and $l \geq 1$ if $p > 2$. Then every element of $G_{e(l+1)}$ is a $p^{th}$ power of some element of $G_{el}$.*

*Proof.* The proof is by successive approximation.

Let $Y$ be an element of $G_{e(l+1)}$. Choose any $X_1$ in $G_{el}$, then $X_1^p \equiv Y \bmod G_{e(l+1)}$, since $G_{el}/G_{e(l+1)}$ is an elementary abelian $p$-group.

For the inductive step, suppose $X_m$ is in $G_{el}$ and $X_m^p \equiv Y \bmod G_{e(l+m)}$. Then $X_m^{-p}Y \in G_{e(l+m)}$, and by Proposition 5.1.7 there exists $A$ in $G_{el}$ such that $A^{p^m} \equiv X_m^{-p}Y \bmod G_{e(l+m+1)}$. Rearranging gives $X_m^p A^{p^m} \equiv Y \bmod G_{e(l+m+1)}$. The element $A^{p^{m-1}}$ is in $G_{e(l+m-1)}$, so by Lemma 5.1.8 if $l > 1$ and by Lemma 5.1.9 if $l = 1$,

$$(X_m A^{p^{m-1}})^p \equiv X_m^p A^{p^m} \bmod G_{e(l+m+1)}.$$

Let $X_{m+1} = X_m A^{p^{m-1}}$. In this way we construct a sequence $X_1, X_2, \ldots$ such that $X_m^p \equiv Y \bmod G_{e(l+m)}$ for all $m \geq 1$. For all $m$, $X_m^{-1}X_{m+1}$ is in $G_{e(l+m-1)}$, hence the sequence $\{X_m\}_{m=1}^{\infty}$ is convergent to some $X$ such that $X^p = Y$. □

We are now in a position to prove Theorem 5.1.1. Again, now that all the appropriate lemmas are in place the proof is the same as that of Theorem 5.2 in [DdSMS99], where the equivalent result is proved for $GL(n, \widehat{\mathbb{Z}_p})$.

*Proof of Theorem 5.1.1.* By definition $P_1(G_{el}) = G_{el}$. Suppose that $P_i(G_{el}) = G_{e(l+i-1)}$ for some fixed $i$. Then by Lemma 5.1.8 and Theorem 5.1.4

$$[P_i(G_{el}), G_{el}]P_i(G_{el})^p \leq G_{e(l+i)}.$$

But by the previous proposition $G_{e(l+i)} \leq (P_i(G_{el}))^p$, hence $P_{i+1}(G_{el}) = G_{e(l+i)}$. By induction $P_i(G_{el}) = G_{e(l+i-1)}$ for all $i$.

This also shows that $P_{i+1}(G_{el}) = P_i(G_{el})^p$, in particular $P_2(G_{el}) = (G_{el})^p$, hence $G_{el}$ is powerful for $p > 2$. For $p = 2$ we have $(G_{el})^{2^2} = G_{e(l+2)} \geq [G_{el}, G_{el}]$ since $l \geq 2$, hence $G_{el}/G_{el}^4$ is abelian and again $G_{el}$ is powerful.

By Theorem 5.1.4 $G_{el}$ is uniformly powerful, and $P_i(G_{el})/P_{i+1}(G_{el})$ is of rank $(n^2-1) \cdot \operatorname{rank}(R/I^e)$ for all $i \geq 1$. □

## 5.2 Approximation for Hyperbolic 3-Manifold Groups

In this chapter $\Gamma$ is the fundamental group of a complete finite-volume hyperbolic 3-manifold $M$. Fix an injective homomorphism

$$\Gamma \to SL(2,\mathbb{C})$$

such that $\mathbb{H}^3/\Gamma = M$.

Let $k$ be the trace field of $\Gamma$. That is,

$$k = \mathbb{Q}(\{\mathrm{tr}(\gamma)\colon \gamma \in \Gamma\}).$$

The invariant trace field of $\Gamma$ is defined to be the trace field of $\Gamma^{(2)}$. Theorem 3.1.2 of [MR03] says that $k$ is a number field. Let $R$ be the ring of integers in $k$. The aim of this section is to prove the following theorem.

**Theorem 5.2.1.** *Let $\Gamma$ be the fundamental group of a complete finite-volume hyperbolic 3-manifold. Let $k$ be the trace field of $\Gamma$, and suppose $k$ coincides with the invariant trace field of $\Gamma$. Let $R$ be the ring of integers in $k$ and let $\mathcal{P}$ be a prime ideal in $R$. As long as $\mathcal{P}$ is not in some finite list of ideals there is an injection*

$$\Gamma \hookrightarrow SL(2,R_{\mathcal{P}})$$

*such that the image of $\Gamma$ is dense in $SL(2,R_{\mathcal{P}})$ (where $SL(2,R_{\mathcal{P}})$ has the profinite topology).*

The hypothesis that the trace field and the invariant trace field should coincide is not a strong one. For any $\Gamma$ the subgroup $\Gamma^{(2)}$ has this property. (See the proof of Theorem 3.3.4 of [MR03].)

Theorem 5.2.1 follows easily from the following two propositions. Note that in Proposition 5.2.2 only finitely many prime ideals are excluded since only finitely many rational primes $p$ ramify in $k$ ([MR03], Theorem 0.3.8), and only finitely many primes ideals lie above 2 or 3.

**Proposition 5.2.2.** *Suppose $\mathcal{P}$ has exponent 1 in the ideal $(p)$, and $p \neq 2$ and $p \neq 3$. Let $X \subset SL(2, R_{\mathcal{P}})$ be such that $X$ generates the quotient $SL(2, R/\mathcal{P})$. Then $X$ topologically generates $SL(2, R_{\mathcal{P}})$.*

**Proposition 5.2.3.** *Suppose the trace field of $\Gamma$ equals the invariant trace field of $\Gamma$. As long as $\mathcal{P}$ is not in some finite list of prime ideals then there exists an injective homomorphism*

$$\Gamma \hookrightarrow SL(2, R_{\mathcal{P}})$$

*such that the composition*

$$\Gamma \hookrightarrow SL(2, R_{\mathcal{P}}) \to SL(2, R/\mathcal{P})$$

*is surjective.*

Before proving Proposition 5.2.2 we need a few lemmas. Consider the short exact sequence

$$1 \to K \to SL(2, R/\mathcal{P}^2) \to SL(2, R/\mathcal{P}) \to 1.$$

Assume that $\mathcal{P}$ lies over the rational prime $p$ and has exponent 1 in $(p)$, then $R/\mathcal{P}$ is a finite field of order $p^m$ for some $m \geq 1$. From the previous chapter $K = \{\mathbb{1}_2 + X : X \in M^0(2, \mathcal{P}/\mathcal{P}^2)\}$.

**Lemma 5.2.4.** *If $p \neq 2$ then $K$ is generated by $p^{th}$ powers of elements of $SL(2, R/\mathcal{P}^2)$.*

*Proof.* We will prove this directly by taking a general element of $K$ and expressing it as a product of $p^{\text{th}}$ powers. Let $x_1, x_2, x_3 \in \mathcal{P}/\mathcal{P}^2$, then

$$\begin{pmatrix} 1+x_1 & x_2 \\ x_3 & 1-x_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (1-x_1)x_3 & 1 \end{pmatrix} \begin{pmatrix} 1+x_1 & 0 \\ 0 & 1-x_1 \end{pmatrix} \begin{pmatrix} 1 & (1-x_1)x_2 \\ 0 & 1 \end{pmatrix}.$$

Since $\mathcal{P}^2 + (p) = \operatorname{hcf}(\mathcal{P}^2, (p)) = \mathcal{P}$, for each $i$ we have $x_i = py_i$ for some $y_i \in R/\mathcal{P}^2$. This gives

$$\begin{pmatrix} 1 & 0 \\ (1-x_1)x_3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (1-x_1)y_3 & 1 \end{pmatrix}^p, \text{ and}$$
$$\begin{pmatrix} 1 & (1-x_1)x_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (1-x_1)y_2 \\ 0 & 1 \end{pmatrix}^p.$$

It remains to show that the diagonal matrix is a product of $p^{\text{th}}$ powers.

Since $p \neq 2$ the matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is invertible, and

$$\begin{aligned}
&\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1+x_1 & 0 \\ 0 & 1-x_1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{-1} \\
&\qquad = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1+x_1 & 0 \\ 0 & 1-x_1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \\
&\qquad = \begin{pmatrix} 1 & x_1 \\ x_1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix} \\
&\qquad = \begin{pmatrix} 1 & 0 \\ y_1 & 1 \end{pmatrix}^p \begin{pmatrix} 1 & y_1 \\ 0 & 1 \end{pmatrix}^p,
\end{aligned}$$

hence $\begin{pmatrix} 1+x_1 & 0 \\ 0 & 1-x_1 \end{pmatrix}$ is a product of $p^{\text{th}}$ powers. □

**Lemma 5.2.5.** *Suppose $p \neq 2$ and $p \neq 3$. If $x, y \in SL(2, R/\mathcal{P}^2)$ with $xy^{-1} \in K$ and $x^p \in K$ then $x^p = y^p$.*

*Proof.* The subgroup

$$S = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in R/\mathcal{P} \right\}$$

of $SL(2, R/\mathcal{P})$ has order $p^m$, and $|SL(2, R/\mathcal{P})| = p^m(p^{2m} - 1)$, hence $S$ is a Sylow $p$-subgroup. Assume $x \notin K$, otherwise the result is trivial: If $x$ is in $K$ then $y$ is also in $K$ and so $x^p = y^p = \mathbb{1}_2$. Since $x \notin K$ and $x^p \in K$ the image $\overline{x}$ of $x$ in $SL(2, R/\mathcal{P})$ has order $p$, and so is contained in some Sylow $p$-subgroup of $SL(2, R/\mathcal{P})$. Since all Sylow $p$-subgroups are conjugate there exists $\overline{z} \in SL(2, R/\mathcal{P})$ and $\overline{a} \in R/\mathcal{P}$ such that

$$\overline{z}\,\overline{x}\,\overline{z}^{-1} = \begin{pmatrix} 1 & \overline{a} \\ 0 & 1 \end{pmatrix}.$$

Pick preimages $z$ and $a$ of $\overline{z}$ and $\overline{a}$ in $SL(2, R/\mathcal{P}^2)$ and $R/\mathcal{P}^2$ respectively, then

$$zxz^{-1} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} + X,$$

for some $X \in M(2, \mathcal{P}/\mathcal{P}^2)$. Now,

$$\begin{aligned} zx^p z^{-1} &= \left( \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} + X \right)^p \\ &= \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^p + \sum_{i=0}^{p-1} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^i X \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{p-1-i} \\ &= \begin{pmatrix} 1 & ap \\ 0 & 1 \end{pmatrix} + \sum_{i=0}^{p-1} \begin{pmatrix} 1 & ai \\ 0 & 1 \end{pmatrix} X \begin{pmatrix} 1 & a(p-1-i) \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & ap \\ 0 & 1 \end{pmatrix} + \sum_{i=0}^{p-1} \left( X_1 + iX_2 + i^2 X_3 \right) \text{ (for some } X_i \in M(2, \mathcal{P}/\mathcal{P}^2)) \\ &= \begin{pmatrix} 1 & ap \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

The second equality holds because any term in the expansion in which $X$ occurs more that once is zero. The final equality holds because $p \neq 2$ and $p \neq 3$ so $p$ divides each of

$$\begin{aligned} &\sum_{i=0}^{p-1} 1 = p, \\ &\sum_{i=0}^{p-1} i = p\frac{p-1}{2}, \text{ and} \\ &\sum_{i=0}^{p-1} i^2 = p\frac{(p-1)(2p-1)}{6}. \end{aligned}$$

Finally, if $x \equiv y \bmod K$ then $x$ and $y$ have the same image in $SL(2, R/\mathcal{P})$, hence

$$zyz^{-1} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} + Y$$

for some $Y \in M(2, \mathcal{P}/\mathcal{P}^2)$. As above

$$zy^p z^{-1} = \begin{pmatrix} 1 & ap \\ 0 & 1 \end{pmatrix},$$

so $zy^p z^{-1} = zx^p z^{-1}$, and $x^p = y^p$. □

With these two lemmas Proposition 5.2.2 can be proved. The proof follows that of Lemma 5, Window 9 in [LS03].

*Proof of Proposition 5.2.2.* Recall that for a group $G$ the Frattini Subgroup $\Phi(G)$ of $G$ is the intersection of all the maximal subgroups of $G$.

We start by showing that the Frattini Subgroup $\Phi(SL(2, R/\mathcal{P}^2))$ of $SL(2, R/\mathcal{P}^2)$ contains $K$. Let $M$ be any maximal subgroup of $SL(2, R/\mathcal{P}^2)$. We must show that $K \subseteq M$. Suppose, for a contradiction, that $K$ is not contained in $M$. Let $x \in SL(2, R/\mathcal{P}^2)$ with $x^p \in K$. Since $K \not\subseteq M$ and $M$ is maximal, $KM = SL(2, R/\mathcal{P}^2)$, hence there exists $y \in M$ with $y \equiv x \bmod K$. By Lemma 5.2.5 $x^p = y^p$ and so $x^p$ is contained in $M$. But by Lemma 5.2.4 $K$ is generated by such elements as $x^p$, thus $K \subseteq M$.

As in section 5.1 let

$$G_i = \mathrm{Ker}(SL(2, R_{\mathcal{P}}) \to SL(2, R/\mathcal{P}^i)).$$

Note that $SL(2, R_{\mathcal{P}})/G_2 \cong SL(2, R/\mathcal{P}^2)$ and $G_1/G_2$ corresponds to the subgroup $K$. Hence, by the previous paragraph, $\Phi(SL(2, R_{\mathcal{P}})/G_2) \supseteq G_1/G_2$. By hypothesis the image of $X$ in $SL(2, R_{\mathcal{P}})/G_1$ is a generating set, and so $X$ also generates $(SL(2, R_{\mathcal{P}})/G_2)/\Phi(SL(2, R_{\mathcal{P}})/G_2)$. For any group, a subset which generates the group modulo its Frattini subgroup generates the entire group, thus $X$ generates $SL(2, R_{\mathcal{P}})/G_2$.

By Theorem 5.1.1, $G_1$ is a pro-$p$ group and so the Frattini subgroup of $G_1$ is $P_2(G_1) = G_2$. Hence any generating set for $G_1/G_2$ topologically generates $G_1$. Since every element of $G_1/G_2$ can be written in terms of $X$,

$$G_1 \subset \overline{\langle X \rangle}.$$

So, $X$ generates $SL(2, R_{\mathcal{P}})/G_1$ and $\overline{\langle X \rangle} \supset G_1$, thus $\overline{\langle X \rangle} = SL(2, R_{\mathcal{P}})$. □

Next we turn our attention to proving Proposition 5.2.3. We use the classification of finite subgroups of special linear groups. The classification was given first by Dickson [Dic58], but the statement of the theorem that we use is adapted from Theorem 6.17 of Chapter 3 in [Suz82]:

**Theorem 5.2.6.** *Let $V$ be the two-dimensional vector space over an algebraically closed field $\mathbb{F}$ of characteristic $p$ ($p \geq 0$). Let $L = SL(V)$. Any finite subgroup $G$ of $L$ satisfies one of the following:*

1. *The second derived subgroup of $G$ is trivial.*
2. *$G$ is isomorphic to one of $SL(2,3)$, $SL(2,5)$, or $\overline{\Sigma_4}$ the representation group of symmetric group $\Sigma_4$ in which the transpositions correspond to elements of order 4.*
3. *$G$ is isomorphic to $SL(2,\mathbb{K})$ where $\mathbb{K}$ is a finite subfield of $\mathbb{F}$.*
4. *$G$ is isomorphic to*
$$\left\langle SL(2,\mathbb{K}),\ \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} \right\rangle,$$
*where $\mathbb{K}$ is as above and $|\mathbb{K}(\pi) : \mathbb{K}| = 2$ and $\pi^2$ is a generator of the multiplicative group $\mathbb{K}^*$.*

Assume $p > 2$, and let $\mathbb{E}$ be a finite subfield of $\mathbb{F}$. The following is Lemma 6.18 of chapter 3 of [Suz82].

**Lemma 5.2.7.** *Suppose $G$ is a subgroup of $L$ such that $|G| = iq(q^2-1)$ ($i = 1,\ 2$) where $q$ is a power of $p$. Furthermore suppose that $G \subseteq SL(2,\mathbb{E})$. Then the field $\mathbb{K} = GF(q)$ is contained in $\mathbb{E}$. If $i = 1$ then $G$ is conjugate to the standard $SL(2,\mathbb{K})$ by some element of $GL(2,\mathbb{E})$. If $i = 2$ then $E$ contains $GF(q^2)$ and $G$ can be conjugated by some element of $GL(2,\mathbb{E})$ to*
$$\left\langle SL(2,\mathbb{K}),\ \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} \right\rangle,$$
*where $\pi \in GF(q^2) - \mathbb{K}$ and $\pi^2 \in \mathbb{K}$.*

We can now proceed to the proof of Proposition 5.2.3. This proof is an extension of the methods used in Section 2 and Section 3 of [LR98].

*Proof of Proposition 5.2.3.* Let

$$A = \left\{ \sum_{\gamma \in \Gamma} \lambda_\gamma \gamma \ : \ \lambda_\gamma \in k, \text{ and } \lambda_\gamma = 0 \text{ for all but finitely many } \gamma \right\},$$

then $A$, with the usual matrix addition and multiplication, is $k$-algebra. By Theorem 3.2.1 of [MR03] it is a quaternion algebra over $k$. Recall that an element of $A$ is a pure quaternion if and only if it is non-central, but its square is central. As such, the conjugation on $A$ is just the restriction of the conjugation in the quaternion algebra $M(2, \mathbb{C})$, and the trace and norm on $A$ are induced from the trace and determinant on $M(2, \mathbb{C})$.

Suppose that

$$A = \left( \frac{a, b}{k} \right)$$

where $a, b \in R$. Fix a standard basis $B = \{\underline{1}, \underline{i}, \underline{j}, \underline{k}\}$ of $A$, and a finite generating set $X$ of $\Gamma$, such that if $x \in X$ then $x^{-1} \in X$. Each element of $X$ is in the $k$-span of $B$:

$$x_n = x_{1n}\underline{1} + x_{2n}\underline{i} + x_{3n}\underline{j} + x_{4n}\underline{k}.$$

For each $mn$ there are $y_{mn}, z_{mn} \in R$ such that $x_{mn} = y_{mn}/z_{mn}$. Choose the prime ideal $\mathcal{P}$ in $R$ such that $\mathcal{P}$ does not contain any $z_{mn}$. (This excludes finitely many prime ideals.) If we treat $k$ as a subfield of $k_\mathcal{P}$ then each $x_{mn}$ is contained in the valuation ring $R_\mathcal{P}$,

By Theorem 4.2.5 excluding finitely many more prime ideals gives

$$A \otimes_k k_\mathcal{P} \cong M(2, k_\mathcal{P}).$$

The image of $\Gamma$ in $A \otimes_k k_\mathcal{P}$ is contained in $R_\mathcal{P}[\underline{1}, \underline{i}, \underline{j}, \underline{k}]$, since $\Gamma$ is generated by $X$ and $X \subset R_\mathcal{P}[\underline{1}, \underline{i}, \underline{j}, \underline{k}]$. Since $R_\mathcal{P}[\underline{1}, \underline{i}, \underline{j}, \underline{k}]$ is an order in $A \otimes_k k_\mathcal{P}$ it lives inside some maximal order. Any maximal order in $M(2, k_\mathcal{P})$ can be conjugated to $M(2, R_\mathcal{P})$ (Theorem 4.2.7), so the isomorphism $A \otimes_k k_\mathcal{P} \cong M(2, k_\mathcal{P})$ can be chosen such that $\Gamma$ lies inside $M(2, R_\mathcal{P})$.

All the maps

$$\Gamma \hookrightarrow A \hookrightarrow A \otimes_k k_\mathcal{P} \xrightarrow{\cong} M(2, k_\mathcal{P})$$

preserve norm, so the image of $\Gamma$ in $M(2, k_{\mathcal{P}})$ is contained in $SL(2, R_{\mathcal{P}})$. Moreover all these maps preserve trace.

It remains to show that by excluding finitely many more ideals the induced map $\Gamma \to SL(2, R/\mathcal{P})$ is surjective.

Let $f : R_{\mathcal{P}} \to R/\mathcal{P}$ be the standard map and let $F : \Gamma \to M(2, R/\mathcal{P})$ be the composition of the injection from $\Gamma$ to $M(2, R_{\mathcal{P}})$ with $f$. ($f$ is applied to $M(2, R_{\mathcal{P}})$ by applying $f$ in each entry.) Then $\operatorname{tr}(F(\gamma)) = f(\operatorname{tr}(\gamma))$ for all $\gamma \in \Gamma$.

Let $N$ be the lowest common multiple of $|SL(2,3)|$, $|SL(2,5)|$, and $|\overline{\Sigma_4}|$, and let $\gamma \in \Gamma$ be a non-trivial loxodromic element in the second derived subgroup of $\Gamma$. Such an element $\gamma$ exists because $\Gamma$ is non-elementary (Proposition 4.5.8), and so the second derived subgroup of $\Gamma$ is non-elementary (Proposition 4.5.6) and contains a loxodromic element (Proposition 4.5.5). Since $\gamma$ is loxodromic $\gamma^N$ is loxodromic also, and by Lemma 4.5.2 the trace of $\gamma^N$ is not 2. Hence $\operatorname{tr}(\gamma^N) - 2$ is an element of $k$ and is non-zero. Write $\operatorname{tr}(\gamma^N) - 2 = y/z$ where $y, z \in R$. Suppose both $y$ and $z$ are not in $\mathcal{P}$, then $f(\operatorname{tr}(\gamma^N) - 2) \neq 0$. (This excludes finitely many prime ideals.)

Now,

$$\begin{aligned} 0 \neq f(\operatorname{tr}(\gamma^N) - 2) &= f(\operatorname{tr}(\gamma^N) - \operatorname{tr}(\mathbb{1}_2)) \\ &= \operatorname{tr}(F(\gamma^N)) - \operatorname{tr}(F(\underline{1})) \\ &= \operatorname{tr}(F(\gamma^N)) - 2. \end{aligned}$$

In particular $F(\gamma^N)$ is not the identity matrix.

The second derived subgroup of $F(\Gamma)$ contains $F(\gamma^N)$ and so is non-trivial. Moreover $F(\gamma)^N$ is non-trivial, and so $F(\Gamma)$ and is not isomorphic to any of $SL(2,3)$, $SL(2,5)$ or $\overline{\Sigma_4}$.

By Theorem 5.2.6 and Lemma 5.2.7 the image $F(\Gamma)$ is conjugate (by an element of $GL(2, R/\mathcal{P})$) to either $SL(2, \mathbb{K})$ or $\left\langle SL(2, \mathbb{K}), \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} \right\rangle$ where $\mathbb{K}$ is a subfield

of $R/\mathcal{P}$. It is easy to see that $SL(2,\mathbb{K})$ is normal in $\left\langle SL(2,\mathbb{K}), \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} \right\rangle$ and that

$$\left\langle SL(2,\mathbb{K}), \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} \right\rangle / SL(2,\mathbb{K}) \cong \mathbb{Z}/2\mathbb{Z},$$

hence in either case $F(\Gamma^{(2)})$ is contained in a conjugate of $SL(2,\mathbb{K})$.

By hypothesis the trace field of $\Gamma^{(2)}$ equals $k$, and by Lemma 3.5.1 of [MR03] there is a finite collection $\{\gamma_i\}_{i=1}^m \subset \Gamma^{(2)}$ such that $k = \mathbb{Q}(\{\mathrm{tr}(\gamma_i)\})$. Let $\{q_j\}_{j=1}^n$ be a $\mathbb{Z}$-basis of $R$. Each $q_j$ is a polynomial in the elements of $\{\mathrm{tr}(\gamma_i)\}$, with coefficients in $\mathbb{Q}$. Choose $\mathcal{P}$ such that for each $j$ the denominators of the coefficients of $q_j$ are not in $\mathcal{P}$. (Again, this excludes finitely many prime ideals.) If $\mathcal{P}$ lies over the rational prime $p$ then each $q_j$ is a polynomial in the elements $\{\mathrm{tr}(\gamma_i)\}$ with coefficients in $\mathbb{Z}_{(p)}$, and the image of $q_j$ in $R/\mathcal{P}$ is a polynomial in $\{f(\mathrm{tr}(\gamma_i))\}$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$. In particular the image of each $q_j$ in $R/\mathcal{P}$ is in the ring generated by $\{f(\mathrm{tr}(\gamma_i))\}$, hence the ring generated by $\{f(\mathrm{tr}(\gamma_i))\}$ is the entire of $R/\mathcal{P}$. On the other hand, $f(\mathrm{tr}(\gamma_i)) = \mathrm{tr}(F(\gamma_i))$, and $\mathrm{tr}(F(\gamma_i))$ is contained in $\mathbb{K}$ since $F(\gamma_i)$ is contained in a conjugate of $SL(2,\mathbb{K})$ and trace is invariant under conjugation. Hence $\mathbb{K} = R/\mathcal{P}$ and $F(\Gamma) = SL(2, R/\mathcal{P})$. □

## 5.3 A Lower Bound on Homology Growth of Congruence Subgroups

The aim of this section is to prove the following theorem.

**Theorem 5.3.1.** *Let $\Gamma$ be the fundamental group of a finite-volume hyperbolic 3-manifold, and let $R$ be the ring of integers in the invariant trace field of $\Gamma$. For all but finitely many prime ideals $\mathcal{P}$ in $R$ the following holds: $\Gamma$ has a finite index subgroup $\Gamma'$ with the following properties.*

1. *$\Gamma'$ embeds in $SL(2, R_\mathcal{P})$, where $R_\mathcal{P}$ is the $\mathcal{P}$-adic completion of $R$. Moreover $\Gamma'$ is dense in $SL(2, R_\mathcal{P})$.*

2. *Let* $r = \text{rank}(R/\mathcal{P})$ *and let* $\epsilon > 0$. *Let* $p$ *be the characteristic of* $R/\mathcal{P}$. *Let* $\Gamma'_n = \text{Ker}(\Gamma' \to SL(2, R/\mathcal{P}^n))$ *(the congruence subgroups), then*

$$b_1(\Gamma'_{n_i}; \mathbb{F}_p) > |\Gamma'_{n_1} : \Gamma'_{n_i}|^{\frac{3r-1}{3r}-\epsilon} b_1(\Gamma'_{n_1}; \mathbb{F}_p),$$

*for some integers* $n_1 < n_2 < \ldots$.

For the rest of this section fix $\Gamma$ as in the hypothesis of the theorem. Fix a representation $\Gamma \hookrightarrow SL(2, \mathbb{C})$ such that $\Gamma$ acts as a covering group on $\mathbb{H}^3$.

We assume that the trace field of $\Gamma$ is also the invariant trace field of $\Gamma$, otherwise replace $\Gamma$ by $\Gamma^{(2)}$. Using Theorem 5.2.1, let $\mathcal{P}$ be a prime ideal in $R$ such that there is an injection $f : \Gamma \hookrightarrow SL(2, R_{\mathcal{P}})$ and $f(\Gamma)$ is dense in $SL(2, R_{\mathcal{P}})$. Theorem 5.2.1 ensures that $\mathcal{P}$ can be any prime except for some finite list. Let $p$ be the characteristic of the finite field $R/\mathcal{P}$.

As before the congruence subgroups of $\Gamma$ and $SL(2, R_{\mathcal{P}})$ are

$$G_i = \ker(SL(2, R_{\mathcal{P}}) \to SL(2, R/\mathcal{P})), \text{ and}$$
$$\Gamma_i = \Gamma \cap G_i.$$

The following lemma is proved using a technique that many authors have used.

**Lemma 5.3.2.** *For any* $M \geq 1$ *there is a finite index subgroup* $\Gamma'$ *in* $\Gamma$ *such that* $f(\Gamma')$ *is dense in* $SL(2, R_{\mathcal{P}})$ *and* $b_1(\Gamma'; \mathbb{F}_p) \geq M$.

*Proof.* By Dirichlet's Theorem there are infinitely many primes congruent to 1 modulo $p$. Using Theorem 5.2.1 choose $M$ prime ideals $\mathcal{P}_1, \ldots, \mathcal{P}_M$ in $R$ such that for every $i = 1, \ldots, M$ there is a surjective homomorphism $\Gamma \to SL(2, R/\mathcal{P}_i)$, and such that each $\mathcal{P}_i$ lies over a distinct prime $q_i$ and $q_i$ is congruent to 1 modulo $p$.

Now form the product homomorphism

$$\phi : \Gamma \to SL(2, R/\mathcal{P}) \times PSL(2, R/\mathcal{P}_1) \times \ldots \times PSL(2, R/\mathcal{P}_M),$$

where the map to $SL(2, R/\mathcal{P})$ is induced from $f : \Gamma \to SL(2, R_{\mathcal{P}})$. By Lemma 4.3.1 this map is surjective, since the projection of $\Gamma$ to each factor is surjective, and no two factors share a common composition factor.

For each $i$ there is an element of order $p$ in $PSL(2, R/\mathcal{P}_i)$, since $|PSL(2, R/\mathcal{P}_i)| = \frac{1}{2}q_i^m(q_i^m - 1)(q_i^m + 1)$ (where $|R/\mathcal{P}_i| = q_i^m$) and $p$ divides $(q_i^m - 1)$. Let $C_i$ be a cyclic subgroup of order $p$ in $PSL(2, R/\mathcal{P}_i)$, and let

$$\Gamma' = \phi^{-1}(SL(2, R/\mathcal{P}) \times C_1 \times \ldots \times C_M).$$

Now, $\Gamma'$ has a surjective homomorphism to $C_1 \times \ldots \times C_M$ thus $b_1(\Gamma'; \mathbb{F}_p) \geq M$. Moreover, $f(\Gamma')$ is dense in $SL(2, R_{\mathcal{P}})$ by Proposition 5.2.2, since the map from $f(\Gamma')$ to $SL(2, R/\mathcal{P})$ is surjective. □

Let $\Gamma'$ be a finite index subgroup of $\Gamma$ such that $f(\Gamma')$ is dense in $SL(2, R_{\mathcal{P}})$ and $b_1(\Gamma'; \mathbb{F}_p)$ is very large—exactly how large it needs to be will be seen later in the chapter.

**Lemma 5.3.3.** $b_1(\Gamma'_1; \mathbb{F}_p) \geq b_1(\Gamma'; \mathbb{F}_p)$.

*Proof.* Since $\Gamma'$ is dense in $SL(2, R_{\mathcal{P}})$, $\Gamma'/\Gamma'_1 \cong SL(2, R/\mathcal{P})$—a perfect group. (We assume $|R/\mathcal{P}|$ is not 2 or 3.) Hence $P_2(\Gamma')\Gamma'_1 = \Gamma'$, and so the homomorphism $\Gamma'_1 \to \Gamma'/P_2(\Gamma')$ is surjective. □

**Lemma 5.3.4.** *If $b_1(\Gamma'_1; \mathbb{F}_p)$ is sufficiently large then the sequence*

$$b_1(\Gamma'_1; \mathbb{F}_p),\ b_1(\Gamma'_2; \mathbb{F}_p),\ b_1(\Gamma'_3, \mathbb{F}_p), \ldots$$

*is strictly increasing.*

*Proof.* Since $b_1(H; \mathbb{F}_p) = b_2(H; \mathbb{F}_p)$ for all finite index subgroups $H$ of $\Gamma'$, Theorem 2.3.1 gives

$$b_1(\Gamma'_{(m+1)}; \mathbb{F}_p) \geq \dim(J/J^2) b_1(\Gamma'_m; \mathbb{F}_p) - \dim(J/J^3).$$

Since $\Gamma'_m/\Gamma'_{(m+1)}$ is an elementary abelian $p$-group of rank $3r$ the dimension subgroups $D_i(\Gamma'_m/\Gamma'_{(m+1)})$ are trivial for all $i \geq 2$. By Jennings' Theorem (3.1.3), $\dim(J/J^2) = 3r$ and

$$\dim(J/J^3) = \binom{3r}{2} + 6r.$$

Then $b_1(\Gamma'_{(m+1)}; \mathbb{F}_p) > b_1(\Gamma'_m; \mathbb{F}_p)$ if

$$b_1(\Gamma'_m; \mathbb{F}_p) > \frac{9r(r+1)}{2(3r-1)}.$$

By induction this holds if

$$b_1(\Gamma'_1; \mathbb{F}_p) > \frac{9r(r+1)}{2(3r-1)}.$$

□

**Lemma 5.3.5.** *Let $N$ be a fixed positive integer, and for all positive integers $M$ let*

$$f_M(x) = (1 + x + \ldots + x^M)^N.$$

*Then there exists $\lambda > 0$ (depending only on $N$) such that $f_M(x)$ has a coefficient greater than or equal to $\lambda \left(f_M(1)\right)^{\frac{N-1}{N}}$.*

*Proof.* We will try to estimate the middle coefficient in $f_M(x)$. That is, the coefficient of $x^{\frac{MN}{2}}$ or $x^{\frac{MN+1}{2}}$ depending on whether $MN$ is odd or even.

For $\alpha \in \mathbb{R}$ let $L(\alpha)$ be the plane in $\mathbb{R}^N$ given by

$$x_1 + \ldots + x_N = \alpha.$$

For $\beta \in \mathbb{R}^+$ let $C(\beta)$ be the cube

$$\{(x_1, \ldots, x_N) \in \mathbb{R}^N : 0 \leq x_i \leq \beta \text{ for all } i = 1, \ldots, N\}.$$

Then, if $\alpha$ is a positive integer, the coefficient of $x^\alpha$ in $f_M(x)$ is equal to the number of lattice points on $L(\alpha)$ contained in $C(M)$.

Let $\alpha(M)$ be $\frac{MN}{2}$ when $MN$ is even and $\frac{MN+1}{2}$ otherwise. As $M$ increases the number of lattice points in $L(\alpha(M)) \cap C(M)$ grows linearly with the area of $L(\alpha(M)) \cap C(M)$. This is because for all $M$ the plane $L(\alpha(M))$ is a translation of the plane $x_1 + \ldots + x_n = 0$, so as long as $L(\alpha(M))$ contains a lattice point, which it does, the distribution of lattice points does not change with $M$.

Let $\lambda_1 > 0$ be such that the number of lattice points in $L(\alpha(M)) \cap C(M)$ is greater than or equal to $\lambda_1 \times \text{Area}(L(\alpha(M)) \cap C(M))$, for all $M$.

Since the plane $L(\cdot)$ has dimension $N-1$, scaling down by $M$ gives

$$\text{Area}(L(\alpha(M)) \cap C(M)) = M^{N-1} \times \text{Area}\left(L\left(\frac{\alpha(M)}{M}\right) \cap C(1)\right).$$

The area on the right hand side does depend on $M$ (when $MN$ is odd), however it converges to Area $\left(L\left(\frac{N}{2}\right) \cap C(1)\right)$ as $M$ goes to $\infty$. In particular there exists $\lambda_2 > 0$ such that

$$\text{Area}(L(\alpha(M)) \cap C(M)) \geq M^{N-1}\lambda_2,$$

for all $M$.

Finally, letting $\lambda = \lambda_1\lambda_2$, the coefficient of $x^{\alpha(M)}$, which is the number of lattice points in $L(\alpha(M)) \cap C(M)$, is greater than or equal to

$$\lambda M^{N-1} = \lambda \left(f_M(1)\right)^{\frac{N-1}{N}}.$$

□

**Lemma 5.3.6.** *Let $1 \leq l < m$. Let $r = \text{rank}(R/\mathcal{P})$. Then there exists $\lambda > 0$, depending only on $\mathcal{P}$, such that*

$$b_1(\Gamma'_m; \mathbb{F}_p) > \lambda |\Gamma'_l : \Gamma'_m|^{\frac{3r-1}{3r}} b_1(\Gamma'_l; \mathbb{F}_p) - |\Gamma'_l : \Gamma'_m|.$$

*Proof.* By Theorem 5.1.1 $G_l/G_m$ is powerful and

$$P_i(G_l/G_m) = G_{(l+i-1)}/G_m,$$

where $i$ ranges from 1 to $m-l+1$. By Lemma 4.4.11, since $G_l/G_m$ is powerful

$$D_j(G_l/G_m) = P_{i+1}(G_l/G_m)$$

where $p^{i-1} < j \leq p^i$. Since $\Gamma'$ is dense in $SL(2, R_{\mathcal{P}})$,

$$G_l/G_m \cong \Gamma'_l/\Gamma'_m.$$

Then

$$D_j(\Gamma'_l/\Gamma'_m)/D_{j+1}(\Gamma'_l/\Gamma'_m) = 0$$

when $j$ is not a $p^{\text{th}}$ power, and

$$D_j(\Gamma'_l/\Gamma'_m)/D_{j+1}(\Gamma'_l/\Gamma'_m) = \mathbb{Z}_p^{3r}$$

when $j = p^0, p^1, \ldots, p^{m-l-1}$. Let $J$ be the augmentation ideal in $\mathbb{F}_p(\Gamma'_l/\Gamma'_m)$. By Jennings' Theorem (3.1.3)

$$\sum_{s\geq 0} x^s \cdot \dim J^s/J^{s+1} = \prod_{i=0}^{i=m-l-1} \left(1 + x^{p^i} + x^{2p^i} + \ldots x^{(p-1)p^i}\right)^{3r}.$$

The right hand side of this equation can be expanded to

$$f(x) = \left(1 + x + x^2 + x^3 + \ldots + x^{p^{m-l}-1}\right)^{3r}.$$

Using Lemma 5.3.5 we see that there exists $\lambda > 0$, depending only on $r$, which in turn depends only on $\mathcal{P}$, such that $f(x)$ has a coefficient greater than or equal to

$$\lambda \left(f(1)\right)^{\frac{3r-1}{3r}}.$$

Note that $f(1) = |\Gamma'_l : \Gamma'_m|$, and so Jennings' Theorem says that for some $s$,

$$\dim(J^s/J^{s+1}) \geq \lambda |\Gamma'_l : \Gamma'_m|^{\frac{3r-1}{3r}}. \tag{5.1}$$

A complete finite-volume hyperbolic manifold is a $K(\pi, 1)$ for its fundamental group, and so by Poincaré duality $b_1(\Gamma''; \mathbb{F}_p) = b_2(\Gamma''; \mathbb{F}_p)$ for all finite index subgroups $\Gamma''$ of $\Gamma'$. Hence by Theorem 2.3.1

$$b_1(\Gamma'_m; \mathbb{F}_p) \geq \dim(J^s/J^{s+1}) b_1(\Gamma'_l; \mathbb{F}_p) - \dim(J/J^{s+2}).$$

The bound from equation 5.1 and the inequality $\dim(J/J^{s+2}) < \dim(\mathbb{F}_p\Gamma'_l/\Gamma'_m)$ gives the final result

$$b_1(\Gamma'_m; \mathbb{F}_p) \geq \lambda |\Gamma'_l : \Gamma'_m|^{\frac{3r-1}{3r}} b_1(\Gamma'_l; \mathbb{F}_p) - |\Gamma'_l : \Gamma'_m|.$$

□

We are now in a position to prove Theorem 5.3.1.

*Proof of Theorem 5.3.1.* The result will be proved by induction. Suppose $n_1, \ldots, n_m$ have been found. Let $n_{m+1}$ be determined by the inequality

$$\frac{|\Gamma'_{n_m} : \Gamma'_{n_{m+1}}|^{\frac{1}{3r}}}{b_1(\Gamma'_{n_m}; \mathbb{F}_p)} \leq \frac{1}{2}\lambda < \frac{|\Gamma'_{n_m} : \Gamma'_{(n_{(m+1)}+1)}|^{\frac{1}{3r}}}{b_1(\Gamma'_{n_m}; \mathbb{F}_p)}, \tag{5.2}$$

where $\lambda$ is as in Lemma 5.3.6.

In the following calculation the first inequality is obtained by rearranging Lemma 5.3.6, the second is by equation 5.2, and the third can be ensured by choosing $b_1(\Gamma'_1; \mathbb{F}_p)$ large enough.

$$\begin{aligned}
\frac{\log\left(\frac{b_1(\Gamma'_{n_{m+1}};\mathbb{F}_p)}{b_1(\Gamma'_{n_m};\mathbb{F}_p)}\right)}{\log\left|\Gamma'_{n_m} : \Gamma'_{n_{m+1}}\right|} &\geq \frac{3r-1}{3r} + \frac{\log\left(\lambda - \frac{\left|\Gamma'_{n_m}:\Gamma'_{n_{m+1}}\right|^{\frac{1}{3r}}}{b_1(\Gamma'_{n_m};\mathbb{F}_p)}\right)}{\log\left|\Gamma'_{n_m} : \Gamma'_{n_{m+1}}\right|} \\
&\geq \frac{3r-1}{3r} + \frac{\log\left(\frac{1}{2}\lambda\right)}{\log\left|\Gamma'_{n_m} : \Gamma'_{n_{m+1}}\right|} \geq \frac{3r-1}{3r} - \epsilon.
\end{aligned}$$

Rearranging and applying induction completes the proof:

$$\begin{aligned}
b_1(\Gamma'_{n_{m+1}}; \mathbb{F}_p) &\geq \left|\Gamma'_{n_m} : \Gamma'_{n_{m+1}}\right|^{\frac{3r-1}{3r}-\epsilon} b_1(\Gamma'_{n_m}; \mathbb{F}_p) \\
&\geq \left|\Gamma'_{n_m} : \Gamma'_{n_{m+1}}\right|^{\frac{3r-1}{3r}-\epsilon} \left|\Gamma'_{n_1} : \Gamma'_{n_m}\right|^{\frac{3r-1}{3r}-\epsilon} b_1(\Gamma'_{n_1}; \mathbb{F}_p) \\
&= \left|\Gamma'_{n_1} : \Gamma'_{n_{m+1}}\right|^{\frac{3r-1}{3r}-\epsilon} b_1(\Gamma'_{n_1}; \mathbb{F}_p).
\end{aligned}$$

□

To use Theorem 5.3.1 in actual examples we need to know what inertial degrees can occur in the ring of integers of a given number field. Čebotarev's Theorem (Theorem 4.1.19) gives us this information. We present a basic corollary as an example.

**Corollary 5.3.7.** *Let $\Gamma$ be the fundamental group of a finite-volume hyperbolic 3-manifold. Then, for infinitely many prime integers $p$, and for any $\epsilon > 0$, $\Gamma$ has a finite index subgroup $\Gamma'$ with a sequence of congruence subgroups*

$$\Gamma' = \Gamma'_{n_1} > \Gamma'_{n_2} > \ldots$$

*such that $b_1(\Gamma'_{n_i}; \mathbb{F}_p) > |\Gamma'_{n_1} : \Gamma'_{n_i}|^{\frac{5}{6}-\epsilon} b_1(\Gamma'_{n_1}; \mathbb{F}_p)$.*

*Proof.* Let $k$ be the invariant trace field of $\Gamma$. By Theorem 3.3.7 of [MR03] we have $|k : \mathbb{Q}| \geq 2$, hence $\mathrm{Gal}(\overline{k}/\mathbb{Q})$ is non-trivial and acts non-trivially on the set of embeddings of $k$ in $\mathbb{C}$. Hence, by Čebotarev's Theorem (Theorem 4.1.19) the set of unramified (in $k$) prime integers $p$ which have a prime divisor $\mathcal{P}$ of inertial degree at least 2 has non-zero Dirichlet density. In particular, the set of primes ideals $\mathcal{P}$ with inertial degree at least 2 has infinite order. By Theorem 5.3.1 for all but finitely many of these $\mathcal{P}$ the desired conclusion holds. □

# Bibliography


[DdSMS99] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.

[Dic58] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[DT06] Nathan M. Dunfield and William P. Thurston. Finite covers of random 3-manifolds. *Invent. Math.*, 166(3):457–521, 2006.

[Hal36] P. Hall. The Eulerian Functions of a Group. *Q J Math*, os-7(1):134–151, 1936.

[Jen41] S. A. Jennings. The structure of the group ring of a $p$-group over a modular field. *Trans. Amer. Math. Soc.*, 50:175–185, 1941.

[Lac] Marc Lackenby. Detecting large groups. Preprint. Availible at *http://www.maths.ox.ac.uk/∼lackenby/dl010207.ps*.

[Lac09a] Marc Lackenby. Large groups, property $(\tau)$ and the homology growth of subgroups. *Math. Proc. Cambridge Philos. Soc.*, 146(3):625–648, 2009.

[Lac09b] Marc Lackenby. New lower bounds on subgroup growth and homology growth. *Proc. London Math. Soc.*, 98(2):271–297, 2009.

[LM87] Alexander Lubotzky and Avinoam Mann. Powerful $p$-groups. I. Finite groups. *J. Algebra*, 105(2):484–505, 1987.

[LR98] D. D. Long and A. W. Reid. Simple quotients of hyperbolic 3-manifold groups. *Proc. Amer. Math. Soc.*, 126(3):877–880, 1998.

[LS03] Alexander Lubotzky and Dan Segal. *Subgroup growth*, volume 212 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2003.

[Mar77] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

[MR03] Colin Maclachlan and Alan W. Reid. *The arithmetic of hyperbolic 3-manifolds*, volume 219 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.

[MVW84] C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler. Congruence properties of Zariski-dense subgroups. I. *Proc. London Math. Soc. (3)*, 48(3):514–532, 1984.

[Nar04] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[Pin00] Richard Pink. Strong approximation for Zariski dense subgroups over arbitrary global fields. *Comment. Math. Helv.*, 75(4):608–643, 2000.

[Suz82] Michio Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982. Translated from the Japanese by the author.

[SW92] Peter B. Shalen and Philip Wagreich. Growth rates, $Z_p$-homology, and volumes of hyperbolic 3-manifolds. *Trans. Amer. Math. Soc.*, 331(2):895–917, 1992.

[Thu80] William P. Thurston. The geometry and topology of three-manifolds. Lecture Notes, Princeton University, 1980.

[Wei84] Boris Weisfeiler. Strong approximation for Zariski-dense subgroups of semisimple algebraic groups. *Ann. of Math. (2)*, 120(2):271–315, 1984.