Profinite and residual methods in geometric group theory

Sam Hughes

(S. Hughes) Mathematical Institute, Andrew Wiles Building, Observatory Quarter, University of Oxford, Oxford OX2 6GG, UK

Email address: sam.hughes@maths.ox.ac.uk

Contents

Introduction

Todo 1: Write introduction

For a group G we denote by $\mathcal{F}(G)$ the set of isomorphism classes of finite quotients of G. Two groups G and H are said to have the same finite quotients if $\mathcal{F}(G) = \mathcal{F}(H)$. A group G is called *profinitely rigid relative to a class of groups* $\mathcal{C}$ if $G \in \mathcal{C}$ and for any group H in the class $\mathcal{C}$ whenever $\mathcal{F}(G) = \mathcal{F}(H)$, then $G \cong H$. By definition, a finitely generated residually finite group G is called *profinitely rigid (in the absolute sense)* if G is profinitely rigid relative to the class consisting of all finitely generated residually finite groups. If G is not profinitely rigid then we say G is *profinitely flexible*.

Motivating Question (Profinite rigidity). *Given a finitely generated group G and a class of groups $\mathcal{C}$. To what extent do the isomorphism classes of finite quotients of G determine G amongst groups in $\mathcal{C}$?*

CHAPTER I

Residual finiteness and the profinite topology

I.A. Residual finiteness

I.A.1. Definitions, examples, and basic properties. We will make repeated use of the following lemma of Marshall Hall Jr. [**Hal50**]

Lemma I.A.1.1. *A finitely generated group G has only finitely many subgroups of a given finite index n.*

PROOF. Let H be a subgroup of G of index n and consider the action of G on the set of cosets G/H. Note that $|G/H| = n$. The action defines a homomorphism $\psi\colon G \to \mathrm{Sym}(G/H)$. Now, $g \in H$ if and only if $gH = H$. So $H = \mathrm{Stab}_G(H)$ and this is completely determined by the homomorphism ψ. Let X be a finite generating set for G. The homomorphism ψ is determined by its images $\psi(x)$ for $x \in X$. But $\mathrm{Sym}(n)$ is finite so there can only be finitely many possibilities for ψ and hence only finitely many possibilities for H. □

We now turn to the star of the section: residual properties.

Definition I.A.1.2 (Residually $\mathcal{P}$)**.** Let $\mathcal{P}$ be a property of a group (e.g. finite, nilpotent, soluble, amenable). A group G is *residually* $\mathcal{P}$ if for every non-identity element $g \in G$, there exists a homomorphism $\alpha\colon G \twoheadrightarrow Q$ such that Q has $\mathcal{P}$ and $\alpha(g) \neq 1_Q$.

Note that this is equivalent to the following: for every element $g \in G$ there exists a normal subgroup $N \lhd G$ such that G/N has $\mathcal{P}$ and $g \notin N$.

We will now hone in on residual finiteness.

Examples I.A.1.3. We record a number of groups that are easily seen to be residually finite.

(1) Finite groups are clearly residually finite.
(2) The group $\mathbb{Z}$ is residually finite.
Proof. for each $n \in \mathbb{Z}$ such that $n \neq 0$, there exists a quotient $\alpha_k\colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/k$ with k relatively prime to n. In particular, $n \pmod{k} \not\equiv 0$ so $\alpha_k(n) \neq 0$. ◆
(3) Direct products of residually finite groups are residually finite.
Proof. To see this note that every element has non-trivial image when projected to one of the factors. Now, compose with a finite quotient there. ◆
(4) Free groups are residually finite.
Proof. Let X be the generators of a free group F. Consider a word $x_n \dots x_1$ in reduced form where x_i or x_i^{-1} is in X. We will build a homomorphism $F \twoheadrightarrow \mathrm{Sym}(n+1)$, the group of permutations of

$\Omega := \{1, \ldots, n+1\}$. Define a function $X \to \Omega$ by $f(y) = 1$ if y does not equal any x_i or x_i^{-1}. For the remaining elements we define $f(y)$ as follows:

Let $A \subseteq \Omega$ be the set of consisting of the i such that $x_i = y$ and $B \subseteq \Omega$ be the set of consisting of the j such that $x_j^{-1} = y$. Set $f(y)$ as any permutation σ that sends each $i \in A$ to $i+1$, and for each $j \in B$, sends $j+1$ to j. This is well-defined since an element and its inverse cannot occur adjacently in the reduced form for a word.

The function f extends to a homomorphism $\phi\colon F \to \mathrm{Sym}(n+1)$ by the universal property of F. Moreover, x has non-trivial image since $\phi(x)(1) = n+1$. As x was arbitrary we are done. ◆

(5) An infinite simple group is not residually finite.

lem:rf_int

Lemma I.A.1.4. *A group G is residually finite if and only if the intersection of all finite index normal subgroups of G is trivial.*

Proof. Suppose G is residually finite and let $g \in G$ be non-trivial. By the definition of residual finiteness there is a finite quotient $\alpha_g\colon Q \twoheadrightarrow G$ such that $\alpha_g(g) \neq 1_Q$. Now, $\ker\alpha$ is a finite index normal subgroup of G such that $g \notin \ker\alpha$. Since g was arbitrary it follows the intersection of all finite index normal subgroups of G equals $\{1\}$.

Conversely, suppose that the intersection of all finite index normal subgroups of G is trivial and let $g \in G$ be non-trivial. By hypothesis there exists a finite index normal subgroup $N \trianglelefteq G$ such that $g \notin N$. Thus, g has non-trivial image in the finite quotient G/N. Since g was arbitrary it follows that G is residually finite. □

For a general group G we will denote the intersection of all finite index normal subgroups by $G^{(\infty)}$. We call this subgroup the *finite residual* of G. By the previous lemma G is residually finite if and only if $G^{(\infty)}$ is the trivial group.

Exercise I.A.1.5. Explain how Lemma I.A.1.4 is equivalent to 'the intersection of all finite index subgroups of G is trivial'.

ex.rf_subgroupClosed

Exercise I.A.1.6. Let G be a residually finite group. If $H \leqslant G$, then H is residually finite.

ex.rf_productClosed

Exercise I.A.1.7. Let I be a set and let G_i be a residually finite group for each $i \in I$. Then, $\prod G_i$ is residually finite.

The following style of argument will appear a number of times. The key idea dates back to work of McKinsey on symbolic logic [**McK43**], but we provide an adaptation for groups first noticed independently by Dyson [**H.64**] and Mostowski [**Mos66**]. As well as G. Higman and A. Turing (unpublished).

Theorem I.A.1.8 (McKinsey's Algorithm). *A finitely presented residually finite group G has solvable word problem.*

Proof. Note that finite groups are recursively enumerable. For each positive integer n we can generate all Cayley multiplication tables of size $n \times n$ and check whether both a given table represents a group and if the group is already on the list. Note that the existence of the table gives a solution to the word problem for any given fintie group.

Fix an enumeration of all finite groups $\{Q_i\}$ and presentation $\langle X \mid R\rangle$ of G. The set $\hom(G; Q_i)$ is finite since a homorphism is determined by its images on the generators and Q_i is finite. We need to check whether we can extend a map $f\colon X \to Q_i$ to a homomorphism $\phi\colon G \to Q_i$. This amounts to checking the relations $r \in R$ are satisfied. Fortunately, as R is finite a brute force approach will terminate. Hence, we may list all elements of $\hom(G, Q_i)$ in a finite amount of time. Fix an enumeration of all homomorphism from G to finite groups $\phi_1, \phi_2, \dots$

Let g be a word in X. To solve the word problem we now run two machines:

The machine runs over all homomorphism ϕ_i and checks if $\phi_i(g) \neq 1$ (here we are using the solvability of the word problem in the codomain, a finite group). Since G is residually finite, if $g \neq_G 1$, this process will stop.

The second machine runs over all representatives w_j of 1 in G and checks whether $g \equiv w_i$. If $g =_G 1$ this process will stop.

Since exactly one of the machines must stop we can algorithmically decide if g is the trivial word. □

Remark I.A.1.9. There exists a finitely generated residually finite group with unsolvable word problem. See **[Mes74]**.

A *characteristic subgroup* $K \leqslant G$ is one that is invariant under all automorphisms of G. Note that if G is finitely generated, then then the intersection of all subgroups of index n is both finite index and characteristic in G.

Proposition I.A.1.10 (Baumslag)**.** **[Bau63]** *If G is a finitely generated residually finite group, then* $\mathrm{Aut}(G)$ *is residually finite.*

Proof. Let $a \in \mathrm{Aut}(G)$ be non-trivial. There exists a $g \in G$ such that $a(g) \neq g$. Let $h = a(g)g^{-1}$. Since $h \neq 1 \in G$, by Lemma I.A.1.4, there exists a finite index normal subgroup $N \trianglelefteq G$ such that $h \notin N$. Let K denote the intersection of all subgroups of index $|G : N|$ in G. Since K is characteristic, the sujection $\alpha\colon G \twoheadrightarrow G/K$ induces a homomorphism $\psi\colon \mathrm{Aut}(G) \to \mathrm{Aut}(G/K)$. Moreover, $\psi(a)$ is a non-trivial automorphism of G/K because $\pi(h) \neq 1 \in G/K$. Since a was arbitrary, we have verified that $\mathrm{Aut}(G)$ is residually finite. □

Corollary I.A.1.11. *Let N and Q be a residually finite groups. If N is finitely generated, then any semi-direct product $G = N \rtimes Q$ is residually finite.*

Proof. It is easy to see that elements of the form nq with $n \in N$, $q \in Q$ and $q \neq 1$ are non-trivial in a finite quotient. Indeed, the projection $\pi\colon G \twoheadrightarrow Q$ composed with a finite quotient α of Q where $\alpha(q) \neq 1$ suffices. It remains to find finite quotients for the elements $n \in N$ with $n \neq 1$. Since N is residually finite there is a finite quotient $\beta\colon N \twoheadrightarrow L$ such that $\beta(n) \neq 1_L$. Since N is finitely generated and L is finite there are only finitely many homomorphisms $N \to L$. The intersection of these homomorphisms is a finite index characteristic subgroup C of N and so preserved by Q. The subgroup CQ is normal and has finite index in G. Moreover, n has non-trivial image in the finite group G/CQ. ☐

There is also a set of dynamical criterion for residual finiteness due to Cairns, Davis, Elton, Kolganova, and Perversi.

Definition I.A.1.12. Suppose that a group G acts continuously on a Hausdorff topological space X. Then we say that the action of G on X is *chaotic* if both of the following conditions hold

(1) (*topological transitivity*) for every pair of non-empty open subsets U and V of X, there is an element $g \in G$ such that $g(U) \cap V \neq \emptyset$;
(2) (*finite orbits dense*) the set of points in X whose orbit under G is finite is a dense subset of X.

THEOREM I.A.1.13. [**CDE**$^{+}$**95**, Theorem 1] *For a group G, the following are equivalent:*

(1) G is residually finite;
(2) there is a faithful action of G with finite orbits dense on some Hausdorff topological space X;
(3) there is a faithful action of G with all orbits finite on some Hausdorff topological space X;
(4) there is a faithful chaotic action of G on some Hausdorff topological space X.

PROOF. https://www.e-periodica.ch/cntmng?pid=ens-001:1995:41::68

Todo 2: add proof

☐

I.A.2. Mal'cev's Theorem. In [**Mal65**] Mal'cev proved the following remarkable theorem:

`thm.Mal'cev`

THEOREM I.A.2.1 (Mal'cev's Theorem). *A finitely generated linear group is residually finite.*

To prove Mal'cev's Theorem we will need to recall some basic ring theory.

Let R be a ring. Here a ring is associative and contains a multiplicative unit 1. A ring without a multiplicative identity is a *rng*.

A *zero-divisor* is a non-zero element $z \in R$ such that there exists a non-zero element z' satisfying $zz' = 0$. A ring R is a *domain* if it has no zero-divisors.

We say a ring R is *left Noetherian* if R has the *ascending chain condition* on left ideals, that is, for every chain of left ideals $I_1 \subset I_2 \subset \dots$ has a largest element. Said differently, this means there exists an n such that $I_N = I_{N+1}$ for $N > n$.

Let S be a commutative ring and let R be an S-algebra. We say R is *finitely generated* if there exists a finite set of elements $x_1, \dots, x_n \in R$ such that every element of R can be expressed as a polynomial in the x_i with coefficients in S.

The key examples of a finitely generated $\mathbb{Z}$- or $\mathbb{F}_p$-algebra for us is as follows.

ex.fg_Z-alg

Example I.A.2.2. Let k be a field, let $G \leqslant \mathrm{GL}_n(k)$ be a finitely generated subgroup, and let X be a finite set of matrices (closed under inversion) generating G. The subring R of k generated as a k-algebra by the entries of the matrices in X and the multiplicative identity of k is a finitely generated algebra over $\mathbb{Z}$ if $\operatorname{char} k = 0$ and over $\mathbb{F}_p$ if $\operatorname{char} k = p$ a prime. Moreover, $G \leqslant \mathrm{GL}_n(R)$.

lem.facts_Noetherian

Lemma I.A.2.3. *Let S be a commutative Noetherian ring and let R be a finitely generated S-algebra. The following assertions hold:*

(1) R is Noetherian;
(2) if R is a field, then it is finite;
(3) the intersection of the maximal ideals of R is 0.

Proof of Theorem I.A.2.1. Let G be a finitely generated linear group over some field k. Thus, $G \leqslant \mathrm{GL}_n(k)$ for some $n \geqslant 0$. As in Example I.A.2.2 we find that $G \leqslant \mathrm{GL}_n(R)$ where R is a finitely generated $\mathbb{Z}$-algebra.

For an ideal $I \subseteq R$, let $\Gamma(I)$ to be the *Ith principle congruence subgroup* of $\mathrm{GL}_n(R)$ defined by

$$\Gamma(I) := \ker(\mathrm{GL}_n(R) \to \mathrm{GL}_n(R/I)),$$

where the homomorphism is defined by taking entries of $\mathrm{GL}_n(R)$ modulo I.

Now, since R is Noetherian (Lemma I.A.2.3(i)), if I is a maximal ideal then R/I is a field and by Lemma I.A.2.3(ii) it is finite. Hence, $\mathrm{GL}_n(R/I)$ is finite and so $\Gamma(I)$ is a finite index normal subgroup of $\mathrm{GL}_n(R/I)$. Now, the intersection

$$\bigcap_{I \subset R} \Gamma(I) \quad \text{where } I \text{ ranges over all maximal ideals}$$

is finite by Lemma I.A.2.3(iii). The theorem follows from Lemma I.A.1.4. □

The following example of Druţu and Sapir gives an example of a non-linear residually finite one-relator group.

Example I.A.2.4. **[DS05]** (Druţu–Sapir) The group $\langle a, t \mid t^2 a t^{-2} = a^2 \rangle$ is non-linear but is residually finite. Their proof depends in an essential way on **[Weh73]**.

I.A.3. An aside: Hopficity.

Definition I.A.3.1. A group G is *Hopfian* if every surjection $G \twoheadrightarrow G$ is injective.

Another result of Mal'cev shows that for finitely generated groups the Hopf property follows from residual finiteness.

Proposition I.A.3.2. *Let G be a finitely generated group. If G is residually finite, then G is Hopfian.*

Proof. Suppose $G \cong G/N$ for some normal subgroup N, our aim is to show that N is trivial. As G is finitely generated, that the number of subgroups of index m in G is finite. Moreover, the number of subgroups of index n in G/N is equal to the number of subgroups of index n in G. The bijection is $H_i/N \leftrightarrow H_i$. But then it is clear that $N \leqslant H_i$ for every finite index subgroup of G. Thus, $N \leqslant G^{(\infty)} = \{1\}$ where the equality follows from the fact G is residually finite and Lemma I.A.1.4. □

Example I.A.3.3 (Baumslag–Solitar groups)**.** We define a family of one-relator groups, known as Baumslag–Solitar groups, by

$$\mathrm{BS}(m,n) := \langle a, t \mid ta^m t^{-1} = a^n \rangle.$$

We claim *if* $(|m|,|n|) = 1$*, then* $\mathrm{BS}(m,n)$ *is non-Hopfian.* Let p be a prime dividing m but not n. Define an homomorphism

$$\nu\colon \mathrm{BS}(m,n) \to \mathrm{BS}(m,n) \text{ by } \begin{cases} a \mapsto a^p, \\ t \mapsto t. \end{cases}$$

We first prove that ν is an epimorphism. We have $\nu(t) = t$ and

$$\nu([t, a^{m/p}]) = ta^m t^{-1} a^{-m} = a^n a^{-m} = a^{n-m},$$

now since $\nu(a) = a^p$ and $(p, n-m) = 1$, by Bézout's Identity there exist integers x, y such $a^x p a^{y(n-m)} = a$. It remains to check that $\ker \nu$ is non-empty. Note that the element $[t, a^{m/p}]^p a^{m/p}$ is non-trivial in $\mathrm{BS}(m,n)$, but

$$\nu([t, a^{m/p}]^p a^{m-n}) = (ta^m t^{-1} a^m)^p a^{(m-n)p} = (a^n a^{-m})^p a^{(m-n)p} = 1.$$

Hence, ν is not injective. ◆

In fact a complete study of the residual finiteness and Hopficity of Baumslag–Solitar groups has been completed. The Hopfian property was verfied by Baumslag and Solitar in [**BS62**], however, their claim of which $\mathrm{BS}(m,n)$ are residually finite was incorrect. A correct and complete argument was later given by Meskin [**Mes72**].

THEOREM I.A.3.4 (Baumslag–Solitar, Meskin). *The groups* $\mathrm{BS}(m,n)$ *are*

(1) Hopfian if and only if m and n have the same prime factors;
(2) residually finite if and only if $|m| = |n|$ or at least or of $|m|$ or $|n|$ equals 1.

PROOF. To be added, for now see [**Mes72**, Section 2].

Todo 3: Add proof

□

Definition I.A.3.5. A group G is *co-Hopfian* if every injection $G \rightarrowtail G$ is surjective. We say G is *finitely co-Hopfian* is every injection $G \rightarrowtail G$ whose image has finite index is surjective.

Exercise I.A.3.6. Let G be a finitely generated group. Suppose $X(G)$ is a group invariant taking values in $\mathbb{R}$ which for every finite index subgroup $H \leqslant G$ satisfies $X(H) = |G : H| X(G)$. If $X(G) \neq 0$, then G is finitely co-Hopfian.

Examples of invariants (when they are defined) satisfying the hypothesis of the exercise include: Euler characteristic $\chi(G)$, ℓ^2-Betti numbers $b_i^{(2)}(G)$, and ℓ^2-torsion $\rho^{(2)}(G)$.

I.B. Subgroup separability

I.B.1. The definition. We will now extend the notion of residual finiteness to subgroups.

Definition I.B.1.1 (Separable subgroup)**.** Let G be a group and let $H \leqslant G$. We say H is *separable* in G if for each $g \in G \backslash H$ there exists a finite index subgroup $K_g \leqslant G$ with $H \leqslant K_g$ and $g \notin K_g$.

It is easy to see a subgroup H is separable in G if and only if H is an intersection of finite index subgroups of G. In particular, G is residually finite if and only if the trivial subgroup is separable in G.

Lemma I.B.1.2. *Let G be a finitely generated group and let $H \leqslant G$. Then, H is separable in G if and only if for every $g \in G \backslash H$ there exists a finite quotient $\alpha\colon G \twoheadrightarrow Q$ with $\alpha(g) \notin \alpha(H)$.*

Proof. Let $g \in G \backslash H$. We have a homomorphism $\alpha\colon G \twoheadrightarrow Q$ with Q finite and $\alpha(g) \notin \alpha(H)$. Define $K := \alpha^{-1}(\alpha(H))$ and note that K contains H, but $g \notin K$. Thus, it suffices to show that K is finite index in G, but this is clear since it contains $\ker \alpha$ with has index $|Q|$ in G.

Conversely, suppose H is separable in G and let $g \in G \backslash H$. By hypothesis there exists a finite index subgroup $K_g \leqslant G$ containing H but not g. Let N denote the *core* of K_g, that is the intersection of all of the conjugates of a K_g in G. Since G is finitely generated, N is a finite index normal subgroup of G. Let α denote the quotient $G \twoheadrightarrow G/N$. The claim that $\alpha(g) \notin \alpha(H)$ will follows from $\alpha(H) \leqslant \alpha(K_g)$ once we show $\alpha(g) \notin \alpha(K_g)$. The latter statement follows from the finite index of N, the fourth (or lattice) isomorphism theorem, and the fact that gK_g and K_g are distinct cosets of K_g. □

Exercise I.B.1.3. Let H be a separable subgroup in a finitely generated group K. If K is a finite index subgroup of a group G, then H is separable in G.

Let $H \leqslant G$. We say H has *solvable membership problem* in G if there exists an algorithm which takes as input an element $g \in G$ and decides if $g \in H$.

Theorem I.B.1.4. *Let H be a finitely generated subgroup of a finitely presented group G. If H is separable in G, then H has solvable membership problem in G.*

Proof. Let $g \in G$ and fix a generating set $S = \{h_1, \ldots, h_k\}$ of H. The algorithm consists of two processes run in parallel of which one will stop. The first process enumerates finite quotients of G and checks to see if the image of H contains the image of g. If the image of g is not contained in the image of H, then the algorithm stops since $g \notin H$. The second process works in a finitely generated free group F such that $F \twoheadrightarrow G$ is a finite presentation with relations R. We enumerate the words w_ℓ in the free monoid on $S \cup S^{-1}$ and the products p_k in F of conjugates of relators $r \in R$. We check to see if each $g^{-1}w_\ell$ is freely equal to p_k, it is then the algorithm stops since $g \in H$. □

The following result, due to Mihaĭlova [**Mih58, Mih66**], shows that $F_2 \times F_2$ does not in fact have solvable subgroup membership problem.

THEOREM I.B.1.5 (Mihaĭlova). *The group $F_2 \times F_2$ has unsolvable subgroup membership problem.*

PROOF. Note that F_2^2 contains F_n^2 for every $n \geqslant 1$ so we may work in F_n^2 for some n. Let Q be a finitely presented group with unsolvable word problem and let S generate Q. Let $|S| = n$ and let $\pi \colon F_n^2 \twoheadrightarrow Q^2$ be the natural projection. Let $D = \{(g,g)\} < Q^2$ be the diagonal subgroup and define $\Delta = \pi^{-1}(D) < F_n^2$. Now, $(x,y) \in \Delta$ if and only if x and y project to the same element in Q. But Q has unsolvable word problem so we cannot decide if $(x,y) \in \Delta$.

It remains to check that Δ is finitely generated. Let R be a finite set of relations for Q. We claim that

$$\mathcal{S} := \{(g,g) \colon g \in S\} \cup \{(r,1) \colon r \in R\} \cup \{(1,r) \colon r \in R\}$$

is a generating set. The issue is that R only normally generates the kernel of the map $F_n \twoheadrightarrow Q$, however, if $w \in F_n$ and $r \in R$ we have

$$(wrw^{-1}, 1) = (w,w)(r,1)(w^{-1}, w^{-1})$$

of which each term is in $\mathcal{S}$. □

F2xF2_notLERF

Corollary I.B.1.6. *$F_2 \times F_2$ has inseparable subgroups.*

I.B.2. LERF groups. We say a group G is *extended residually finite* (ERF) if every subgroup of G is separable. We say G is *locally extended residually finite* (LERF) if every finitely generated subgroup of G is separable.

Two groups G and H are *commensurable* if there exists finite index subgroups $K \leqslant G$ and $L \leqslant H$ such that $K \cong L$.

Exercise I.B.2.1. Let G be a finitely generated LERF group. If H is a group commensurable with G, then H is LERF.

Examples I.B.2.2. We record a few examples:

(1) finite groups are trivially LERF;
(2) $\mathbb{Z}$ is also trivially seen to be LERF;
(3) $\mathbb{Z}^n$ is LERF.
Proof. Let $L \leqslant \mathbb{Z}^n$ and let $g \in \mathbb{Z}^n \backslash L$. We may assume L has infinite index since all finite index subgroups are separable by definition. Since $L \lhd \mathbb{Z}^n$ we may consider the quotient $\pi_L \colon \mathbb{Z}^n \twoheadrightarrow A = \mathbb{Z}^n/L$. Note that $\pi_L(g) \neq 0$. Now, A is a finitely generated abelian group and hence residually finite. Thus, there exists a finite (abelian) quotient $\alpha \colon A \twoheadrightarrow Q$ where $\alpha(\pi_L(g)) \neq 0 \in Q$. Moreover, $\ker(\alpha \circ \pi_L)$ contains L. Hence, we have separated L from g in Q. ◆
(4) It follows from Corollary I.B.1.6 that $F_2 \times F_2$ is not LERF.

A particularly famous result due to Marshall Hall Jr. is that free groups are LERF **[Hal49]**. We divert the proof to the next section.

thm.MarshallHall

THEOREM I.B.2.3 (Marshall Hall Jr.'s Theorem). *Free groups are LERF*

It follows from Theorem I.B.2.3 and Corollary I.B.1.6 that direct products of LERF groups are not necessarily LERF.

I.B.3. The connection with covering theory. Separability of subgroups has a particularly powerful interpretation when viewed from a topological lens. The following somewhat miraculous result of Scott allows one to promote immersions to embeddings, at the cost of taking a finite cover, when in the presence of subgroup separability.

Let X and Y be CW complexes. Recall that an *immersion* is map $f: X \looparrowright Y$ such that f is a locally injective combinatorial map. The map f map is *combinatorial* if it maps the interior of each cell homeomorphically onto its image.

thm.Scott_LERF_geometric

THEOREM I.B.3.1. **[Sco78]** *Let G be a finitely generated group and let X be a CW complex with $\pi_1 X = G$. Let $H \leqslant G$ and let $Y \to X$ be the cover corresponding to H. Then, H is separable if and only if for every finite subcomplex $K \subseteq Y$, there exists an intermediate finite sheeted cover $Y \to Z \to X$ such that K embeds as a subcomplex of Z.*

PROOF. Suppose the geometric condition holds for some subgroup H with cover $Y \to X$ and let $g \in G \backslash H$. Pick a basepoint $x \in \widetilde{X}$ in the universal cover of X and let $K = \pi(x \cup gx) \subseteq Y$, where $\pi: \widetilde{X} \to Y$ is the universal covering map. By hypothesis we obtain a finite covering $Z \to X$ with corresponding finite index subgroup G' such that $K \subseteq Z$. But, then $g \notin G'$. Hence, H is separable.

Now, suppose H is a separable subgroup of G with corresponding cover $Y \to X$ and let K be a finite subcomplex of Y. Let $\pi: \widetilde{X} \to Y$ be the universal cover and let $C = \pi^{-1}K$. Pick a finite subcomplex D of C such that $\pi(D) = K$ and note that $S := \{g \in G : gD \cap D \neq \varnothing\}$ is finite. Since H is separable we can find a finite index subgroup G' of G such that $H \leqslant G$ and $G' \cap S \subseteq H$. The cover $\widetilde{X}/G' \to X$ is then the required intermediate finite cover. $\square$

We will also need the following easy lemma.

Graphs_imm_lifts

Lemma I.B.3.2. *Let Δ and Γ be finite graphs and let $f: \Delta \looparrowright \Gamma$ be an immersion. Then extends f to a finite-sheeted covering $\hat{\Gamma} \to \Gamma$ such that Δ embeds in $\hat{\Gamma}$.*

PROOF. Fix an orientation and a colouring on the edges of Γ. This lifts to an orientation and a colouring on Δ. A combinatorial map is an immersion if and only if at each vertex, we see each colour arriving exactly once and leaving exactly once. Let n denote the number of vertices of Δ and for each colour c of Γ let n_c be the number of edges of Δ coloured c. There are $n - n_c$ vertices of Δ missing incoming edges with colour c and the same number of vertices missing outgoing edges with colour c. Pick any bijection between these sets and glue in $n - n_c$ edges coloured c. Repeating this for each colour we eventually obtain a covering space $\hat{\Gamma}$ of Γ such that $\Delta \subset \hat{\Gamma}$. $\square$

We now give Stalling's proof of the Marshall Hall Theorem.

PROOF OF THEOREM I.B.2.3. Now, let Γ be a finite rose and H a finitely generated subgroup of $F = \pi_1\Gamma$. Let $\Delta \to \Gamma$ be the covering corresponding to H, and consider a finite subcomplex $K \subset \Delta$. Since H is finitely generated, we may enlarge K to ensure that K is connected and that $\pi_1 K = H$. But $\Delta \to \Gamma$ is an immersion, so can be completed to a finite-sheeted covering $\hat{\Gamma} \to \Gamma$ by Lemma I.B.3.2. The result now follows from Theorem I.B.3.1. □

I.C. Pro topologies on groups

I.C.1. The definition.

Definition I.C.1.1 (Profinite topology)**.** Let $\mathcal{N}$ be a non-empty collection of finite index normal subgroups of a group G. We say $\mathcal{N}$ is *filtered from below* if whenever $N_1, N_2 \in \mathcal{N}$, there exists $N \in \mathcal{N}$ such that $N \leqslant N_1 \cap N_2$. We make G into a topological group by taking $\mathcal{N}$ as a basis of open neighbourhoods of the identity the collection. We refer to the corresponding topology as a *pro topology* on G.

Let $H_1, \ldots, H_n$ be groups. A *subdirect product* of $H = \prod_{i=1}^n H_i$ is any subgroup G of H such that the projections $\pi_i \colon G \to H_i$ are surjective.

Definition I.C.1.2 (Formation)**.** A class of finite groups $\mathcal{C}$ is called a *formation* if $\mathcal{C}$ is closed under taking quotients and subdirect products.

Examples I.C.1.3. The following are examples of formations:

(1) the class of all finite groups;
(2) the class of all finite abelian groups;
(3) the class of all finite nilpotent groups;
(4) the class of all finite soluble groups;
(5) the class of all finite p-groups for a fixed prime p.

Definition I.C.1.4 (Pro-$\mathcal{C}$ topology)**.** Let $\mathcal{C}$ be a formation of finite groups. The *(full) pro-$\mathcal{C}$ topology* on G is the topology $\tau_{\mathcal{C}}(G)$ on G given by taking as a basis of open neighbourhoods of the identity the collection

$$\mathcal{N}_{\mathcal{C}}(G) := \{N \trianglelefteq G \mid G/N \in \mathcal{C}\}.$$

When $\mathcal{C}$ is the class of all finite groups, we denote the topology by τ_G and refer to it as the *profinite topology* on G.

Lemma I.C.1.5. *Let $\mathcal{C}$ be a formation of finite groups. A group G is residually $\mathcal{C}$ if and only if its pro-$\mathcal{C}$ topology is Hausdorff.*

Proof. Suppose G is residually-$\mathcal{C}$. Let $g \neq h$ be elements of G. Since, gh^{-1} is non-trivial, there exists a finite index subgroup $N < G$ such that $gh^{-1} \notin N$. Hence, $gN \cap hN = \varnothing$. This proves the topology is Hausdorff. Reversing the argument yields the converse. □

Definition I.C.1.6 (Separable subset)**.** Let S be subset of G. We say S is *$\mathcal{C}$-separable* if S is closed in pro-$\mathcal{C}$ topology on G.

Lemma I.C.1.7. *Let $\mathcal{C}$ be a formation of finite groups and let G be a group. Suppose $H \leqslant G$. Then, H is closed in the pro-$\mathcal{C}$ topology on G if and only if H is the intersection of open subgroups of G.*

Proof. An open subgroup in the topology $\tau_{\mathcal{C}}(G)$ has finite index so it is also a closed subgroup. Hence, any intersection of open subgroups is closed.

For the converse suppose H is closed in $\tau_{\mathcal{C}}(G)$ and let $g \in G \backslash H$. There exists some $N \in \mathcal{N}_{\mathcal{C}}(G)$ such that $xN \cap H = \varnothing$. Thus, $g \notin HN$. It follows that $H = \bigcap_{N \in \mathcal{N}_{\mathcal{C}}(G)} HN$. But each HN is open, whence the lemma. □

Exercise I.C.1.8. Let $\mathcal{C}$ be a formation of finite groups and let G be a group. Suppose H is a finite index subgroup of G. Then, H is open in the pro-$\mathcal{C}$ topology on G if and only if $G/\operatorname{Core}_G(H)$ is in $\mathcal{C}$.

In general the subspace topology induced on a subgroup $H \leqslant G$ from the pro-$\mathcal{C}$ topology on G will not be equal to the pro-$\mathcal{C}$ topology on H but instead some mystery pro topology. When the topology induced on H is the pro-$\mathcal{C}$ topology we say that G induces the *full pro-$\mathcal{C}$ topology on H*. A sufficient condition for this to happen is that every finite index subgroup of H is separable in G.

Example I.C.1.9. If G is residually finite and H is a finite index subgroup of G, then the inclusion $H \to G$ is a homemorphism onto its image. That is, G induces the full

I.C.2. Virtual retracts.

Definition I.C.2.1 (Virtual retract)**.** Recall that $H \leqslant G$ is a *retract* if the inclusion $i\colon H \rightarrowtail G$ has a left inverse $r\colon G \twoheadrightarrow H$, that is $r \circ i = \mathrm{id}_H$. Similarly, we call H a *virtual retract*, written $H \leqslant_{\mathrm{vr}} G$, if H is a retract of a finite index subgroup of G.

The following useful lemma is due to Hsu and Wise [**HW99**, Lemma 3.9].

`lem.RetractsClosed`

Lemma I.C.2.2. *Let G be a residually finite group and let $H \leqslant G$. If $r\colon G \twoheadrightarrow H$ is retract, then*

1. *H is closed in the profinite topology on G;*
2. *if K is closed in profinite topology on H, then K is closed in the profinite topology on G;*
3. *the inclusion map $H \to G$ induces a homemorphism onto its image of profinite topologies.*

Proof. We first prove (1). Let $N = \ker r$ and note that $G = NH$ and $N \cap H = 1$ so we may express any element of G uniquely as a product nh with $n \in N$ and $h \in H$. Since G is residually finite we may pick a chain (G_i) of finite index normal subgroups of G such that $\bigcap_i G_i = 1$. Let $N_i = G_i \cap N$ and note that $|G : N_iH| = |NH : N_iH| = |N : N_i| \leqslant |G : G_i|$. Hence, (N_iH) is a sequence of finite index subgroups of H whose intersection is exactly H.

We now prove (2). Let K be a closed subgroup of H. Since $r\colon G \to H$ is continuous with respect to the profinite topologies, the preimage $r^{-1}(K)$ is closed in G. Now, $K = H \cap r^{-1}(K)$ and so is the intersection of closed subgroups and hence closed in G.

The claim (3) follows from (2). □

`lem.virRetractsClosed`

Lemma I.C.2.3. *Let G be a finitely generated residually finite group and let $H \leqslant G$. If $H \leqslant_{\mathrm{vr}} G$, then H is closed in the profinite topology on G.*

Proof. Let $K \leqslant G$ be a finite index subgroup admitting a retract $r\colon K \twoheadrightarrow H$. By Lemma I.C.2.2 we see that H is closed in the profinite topology on K. But K is finite index in G, so every closed subset of K is closed in G. Hence, H ic closed in the profinite topology on G. □

We state some elementary properties of virtual retracts first collected by Minasyan [**Min21**, Lemma 3.2].

Exercise I.C.2.4. Suppose that G and G' are groups.

(1) Let $H \leqslant_{\mathrm{vr}} G$ and $A \leqslant G$ such that $H \leqslant A$. Then, $H \leqslant_{\mathrm{vr}} A$.
(2) Suppose $H \leqslant G$ and that there exists a homomorphism $\phi\colon G \to G'$ such that $\phi|_H$ is injective. If $\phi(H) \leqslant_{\mathrm{vr}} G'$, then $H \leqslant_{\mathrm{vr}} G$.
(3) If $H \leqslant_{\mathrm{vr}} G$ and $\alpha \in \mathrm{Aut}(G)$, then $\alpha(H) \leqslant_{\mathrm{vr}} G$.
(4) If $H \leqslant_{\mathrm{vr}} G$ and $A \leqslant_{\mathrm{vr}} H$, then $A \leqslant_{\mathrm{vr}} G$.
(5) If $H \leqslant_{\mathrm{vr}} G$ and $H' \leqslant_{\mathrm{vr}} G'$, then $H \times H' \leqslant_{\mathrm{vr}} G \times G'$.
(6) If G is finitely generated and $H \leqslant_{\mathrm{vr}} G$, then H is undistorted in G.

Let G be finitely generated by a set S and $H \leqslant G$ be finitely generated by a set T. We say H is *undistorted* if there exists a $C > 0$ such that for all $h \in H$ we have $|h|_T \leqslant C \cdot |h|_S$. Where $|\cdot|_S$ and $|\cdot|_T$ are the word metrics in G and H with respect to T and S respectively.

Undistorted subgroup

CHAPTER II

Profinite groups and completions

II.A. Profinite groups

II.A.1. Inverse limits and profinite spaces.

Definition II.A.1.1 (Directed poset)**.** A pair $I = (I, \leqslant)$ where I is a set and $\leqslant$ is a binary relation is a *directed poset* if it is a *poset*:

(1) $i \leqslant i$, for $i \in I$;
(2) if $i \leqslant$ and $j \leqslant k$, then $i \leqslant k$, for $i, j, k \in I$;
(3) if $i \leqslant j$ and $j \leqslant i$, then $i = j$, for $i, j \in I$;

satisfying one additional condition

(4) if $i, j \in I$, then there exists some $k \in I$ such that $i, j \leqslant k$.

Definition II.A.1.2 (Inverse system)**.** An *inverse system* of objects in a category $\mathcal{C}$ over a directed poset I consists of a collection $\{X_i \mid i \in I\}$ of objects in $\mathcal{C}$ indexed by I and a collection of morphisms $\varphi_{i,j} \colon X_i \to X_j$ for each $j \leqslant i$ such that

(1) if $i \leqslant j \leqslant k$ we have $\varphi_{i,j} \circ \varphi_{j,k} = \varphi_{i,k}$, that is the following diagram commutes

$$\begin{array}{ccc} X_i & \xrightarrow{\varphi_{i,j}} & X_j \\ & \searrow^{\varphi_{i,k}} & \downarrow{\scriptstyle \varphi_{j,k}} \\ & & X_k; \end{array}$$

(2) and $\varphi_{i,i} = \mathrm{id}_{X_i}$.

Let Y be an object in some category $\mathcal{C}$ and let $\{X_i, \varphi_{i,j}, I\}$ be an inverse system of objects in $\mathcal{C}$ over a directed poset I.

Definition II.A.1.3 (Inverse limit)**.** We say a sequence of morphisms $\psi_i \colon Y \to X_i$ is *compatible* (with I) if $\varphi_{i,j} \circ \psi_i = \psi_j$ for $j \leqslant i$.

Given an object X in $\mathcal{C}$ with compatible morphisms $\nu_i \colon X \to X_i$, we say X is an *inverse limit* of the inverse system $\{X_i, \varphi_{i,j}, I\}$ if the following universal property holds: whenever Y is an object in $\mathcal{C}$ with a set of compatible morphisms $\psi_i \colon Y \to X_i$, then there exists a unique morphism $\psi \colon Y \to X$ such that following diagram commutes

$$\begin{array}{ccc} Y & \overset{\exists! \psi}{\dashrightarrow} & X \\ & \searrow^{\psi_i} & \downarrow{\scriptstyle \nu_i} \\ & & X_i \end{array}$$

for every $i \in I$. We will denote an inverse limit X by $\varprojlim X_i$.

Exercise II.A.1.4. Let $\mathcal{I} = \{X_i, \varphi_{i,j}, I\}$ be an inverse system of objects in a category $\mathcal{C}$ over a directed poset I. If an inverse limit of $\mathcal{I}$ exists, then it is unique up to $\mathcal{C}$-isomorphism.

Proposition II.A.1.5. *Let $\mathcal{I} = \{X_i, \varphi_{i,j}, I\}$ be an inverse system of topological spaces (or topological groups) over a directed poset I. Then, there exists an inverse limit of $\mathcal{I}$.*

Proof. We construct the inverse limit for spaces, the proof for topological groups being near identical. We define a subspace X of $\prod_{i \in I} X_i$ endowed with the Tychonoff topology to consist of the tuples (x_i) that satisfy $\varphi_{i,j}(x_i) = x_j$ if $j \leqslant i$. The projections $\nu_i \colon X \to \prod_{i \in I} X_i \to X_i$ are clearly continuous. It remains to check the universal property. Suppose $\psi_i \colon Y \to X_i$ is a set of compatible continuous functions, we may take the product map $\psi := \prod_{i \in I} \psi_i \colon Y \to \prod_{i \in I} X_i$. But now $\operatorname{im}(\psi) \subseteq X$ and $\nu_i \circ \psi = \psi_i$. □

prop.InvLimProps

Proposition II.A.1.6. *Let $\{X_i, \varphi_{i,j}\}$ be an inverse system of Hausdorff spaces. The following holds:*

(1) $\varprojlim X_i$ is closed subspace of $\prod_{i \in I} X_i$;
(2) if each X_i is compact, then $\varprojlim X_i$ is compact;
(3) if each X_i is compact and non-empty, then $\varprojlim X_i$ is non-empty;
(4) if each X_i is totally disconnected, then $\varprojlim X_i$ is totally disconnected.

Proof. Exercise. □

Definition II.A.1.7 (Profinite space)**.** A topological space X is a *profinite space* if X is an inverse limit of finite sets with the discrete topology.

Theorem II.A.1.8. *Let X be a topological space. The following are equivalent:*

(1) X is a profinite space;
(2) X is a totally disconnected compact Hausdorff space;
(3) X is a compact Hausdorff space and admits a base of clopen sets for its topology.

Definition II.A.1.9 (Morphism of inverse systems)**.** Let $(X_i, \phi_{i,j})_{i \in I}$ and $(Y_i, \psi_{i,j})_{i \in I}$ be inverse systems of objects in a category $\mathcal{C}$ with inverse limits X and Y respectively. A *morphism of inverse systems* $(f_i) \colon X_i \to Y_i$ is a family of morphisms $f_i \colon X_i \to Y_i$ such that for all $i \preceq j$ we have $f_j \circ \phi_{i,j} = \psi_{i,j} \circ f_i$, that is the following diagram commutes

$$\begin{array}{ccc} X_i & \xrightarrow{f_i} & Y_i \\ {\scriptstyle \phi_{i,j}}\big\downarrow & & \big\downarrow{\scriptstyle \psi_{i,j}} \\ X_j & \xrightarrow{f_j} & Y_j. \end{array}$$

It is easy to check that a morphism of inverse systems induces a morphism $f \colon X \to Y$ that is compatible with the projection maps.

Exercise II.A.1.10. In nice situations we can refine the inverse system to ensure a number of extra properties:

(1) Let $(X_i)_{i \in I}$ be an inverse system of finite sets with inverse limit X. If all of the transition maps $X_i \to X_j$ are surjective, then the projection maps $X \to X_i$ are surjective.

(2) Let $(G_i)_{i\in I}$ be an inverse system of finite groups. Then, there is an inverse system $(H_i')_{i\in I}$ with surjective transition maps and an isomorphic inverse limit.

A *cofinal subsystem* J of an inverse system $(I, \preceq)$ is a subset $J \subseteq I$ such that for all $i \in I$ there is some $j \in J$ such that $i \preceq j$.

(3) Let $(G_i)_{i\in I}$ be an inverse system of finite groups. If $J \subseteq I$ is cofinal, then $\varprojlim_{i\in I} G_i \cong \varprojlim_{i\in J} G_j$ as topological groups. [Hint: There is a natural projection $\varprojlim_{i\in I} G_i \to \varprojlim_{i\in J} G_j$.]

An inverse system $(I, \preceq)$ is *linearly ordered* if there exists a bijection $f\colon I \to \mathbb{N}$ such that $i \preceq j$ if and only if $f(i) \geqslant f(j)$. Note there is a reversal of sign. We say I has *no global minimum* if for all $i \in I$, there exists $j \in I$ such that $j \preceq i$ but $i \neq j$.

(4) Let I be a countable inverse system such that I has no global minimum. Then, I has a linearly ordered cofinal subsystem.

II.A.2. Definition and examples.

Lemma II.A.2.1. *Let $\{G_i, \varphi_{i,j}, I\}$ be an inverse system of finite groups G_i, let $\mathbf{G} = \varprojlim G_i$, and let $\varphi_i\colon \mathbf{G} \twoheadrightarrow G_i$ denote the projection maps. The set $\{\ker \varphi_i\}$ forms a basis of open neighbourhoods of the identity in $\mathbf{G}$.*

Exercise II.A.2.2. Let G be a compact topological group. Then, a subgroup $U \leqslant G$ is open if and only if U is closed and finite index.

Definition II.A.2.3 (Pro-$\mathcal{C}$ group)**.** Let $\mathcal{C}$ be a formation of finite groups. A *pro-$\mathcal{C}$ group* is a group which is the inverse limit of groups in $\mathcal{C}$. A *profinite group* is a group which is the inverse limit of finite groups.

`thm.characterise-proCgroups`

THEOREM II.A.2.4. *Let $\mathcal{C}$ be a formation of finite groups and let G be a topological group. The following are equivalent:*

(1) G is a pro-$\mathcal{C}$ group;
(2) G is compact Hausdorff totally disconnected and for each open normal subgroup N of G we have $G/N \in \mathcal{C}$;
(3) the identity of G admits of a basis of open neighbourhoods $\mathcal{N}$ such that each $N \in \mathcal{N}$ is a normal subgroup of G, $G/N \in \mathcal{C}$, and G is an inverse limit of the quotients $\{G/N\}$.

`lem.profiniteDenseSubsets`

Lemma II.A.2.5. *Let $\{G_i, \varphi_{i,j}, I\}$ be an inverse system of finite groups G_i, let $\mathbf{G} = \varprojlim G_i$, and let $\varphi_i\colon \mathbf{G} \twoheadrightarrow G_i$ denote the projection maps. A subset $X \subseteq G$ is dense if and only if $\varphi_i(X) = \varphi_i(G)$ for all $i \in I$.*

The following lemma is an easy consequence of the Tychnoff product topology.

`lem.ContinuityProjectionsToptoProf`

Lemma II.A.2.6. *Let H be a topological group and let $\mathbf{G} = \varprojlim G_j$ be a profinite group with projections $\pi_i\colon \mathbf{G} \to G_i$. A homomorphism $f\colon H \to G$ is continuous if and only if each map $\pi_i \circ f\colon H \to G_i$ is continuous.*

It follows from point (3) and the continuity of the multiplication $G \times G \to G$ that we have a basis of neighbourhoods for every point $g \in G$. Indeed, the neighbourhoods gN suffice.

Examples II.A.2.7. We record a number of examples.

(1) As a first example we have the *p-adic integers*

$$\mathbb{Z}_{\hat{\mathfrak{p}}} = \varprojlim \Big(\cdots \longrightarrow \mathbb{Z}/p^{i+1} \longrightarrow \mathbb{Z}/p^{i} \longrightarrow \cdots \longrightarrow \mathbb{Z}/p \Big)$$

where the homomorphisms are the reduction modulo p^i maps. Thus, $\mathbb{Z}_{\hat{\mathfrak{p}}}$ is a subgroup of $\prod_{i\geqslant 1} \mathbb{Z}/p^i$ and is hence and abelian group. There is a natural map $i\colon \mathbb{Z} \to \mathbb{Z}_{\hat{\mathfrak{p}}}$ by $n \mapsto (n \mod p^i)_{i\geqslant 1}$. The map i is injective since if $n \in \mathbb{Z}$ and $p^n > |z|$, then $z \mod p^n \neq 0$. There is a ring structure on $\mathbb{Z}_{\hat{\mathfrak{p}}}$ inherited from the product ring structure on $\prod_{i\geqslant 1} \mathbb{Z}/p^i$.

Proposition II.A.2.8. *The following statements hold.*

(a) *As a group $\mathbb{Z}_{\hat{\mathfrak{p}}}$ is torsion-free and abelian.*
(b) *As a ring $\mathbb{Z}_{\hat{\mathfrak{p}}}$ is domain.*

Proof. For (a) we have already verified that $\mathbb{Z}_{\hat{\mathfrak{p}}}$ is abelian. Since $\mathbb{Z}_{\hat{\mathfrak{p}}}$ is abelian we will work with additive notation. It remains to check $\mathbb{Z}_{\hat{\mathfrak{p}}}$ is torsion-free. Let $g = (g_i) \in \mathbb{Z}_{\hat{\mathfrak{p}}}$ be non-trivial and suppose there exists some $k \in \mathbb{N}$ such that $kg = 0$. Suppose for contradiction $k \neq 0$, and let $k = p^\ell s$ where $\gcd(s,p) = 1$. Choose i such that $g_i \neq 0$ and consider $g_{i+\ell}$. We have $mg_{i+\ell} \equiv 0 \mod p^{i+\ell}$ so $p^{i+\ell} | p^\ell s g_{i+\ell}$. Hence, $p^i | g_{i+\ell}$ as s is coprime to p. But then $g_{i+\ell} \equiv 0 \mod p^i$ contradicting $g_{i+\ell} \equiv g_i \mod p^i$.

For (b) suppose there exists $g = (g_i), h = (h_i) \in \mathbb{Z}_{\hat{\mathfrak{p}}}$ both non-zero, so say g_k and h_ℓ are non-zero, such that $gh = 0$. Now, $g_{k+\ell}h_{k+\ell} = 0$, so $p^{k+\ell} | g_{k+\ell}h_{k+\ell}$. But then either $p^k | g_{k+\ell}$ or $p^\ell | h_{k+\ell}$ a contradiction. ☐

Without delving into too deep a discussion about attributions, the colloquially named *Chinese Remainder Theorem* was first written down by Suanjing in the 5th century with no proof. In 1247 Jiushao proved the full version for the integers. A detailed historical account can be found here [**She88**]. A more modern formulation, first recorded by Ore [**Ore52**], is as follows:

Two ideals I, J in a ring R are called *coprime* if there exists elements $i \in I$ and $j \in J$ such that $i + j = 1$.

`thm.CoprimeIdeals`

Theorem II.A.2.9 (The Coprime Ideal Theorem). *Let $I_1, \ldots, I_k$ be pairwise coprime ideals in a ring R and let $I = \bigcap_{i=1}^k I_i$. Then, the map*

$$R/I \to \prod_{i=1}^{k} R/I_i \quad by \quad x \mod I \mapsto (x \mod I_1, \ldots, x \mod I_k)$$

is a ring isomorphism.

Note that in a commutative ring $\bigcap_{i=1}^k I_i = \prod_{i=1}^k I_i$ so we recover the usual statement for $\mathbb{Z}$.

With that out of the way we may return to our examples.

(2) Define $\widehat{\mathbb{Z}}$ to be the inverse limit of the system of finite quotients of $\mathbb{Z}$. That is, the system consisting of all groups $\mathbb{Z}/n$ and the projections $\mathbb{Z}/n \twoheadrightarrow \mathbb{Z}/m$ whenever $m|n$.

`prop.CoprimeIdeals_Zhat`

Proposition II.A.2.10. *There is an isomorphism of topological rings*

$$\widehat{\mathbb{Z}} \cong \prod_{p\in\mathfrak{p}} \mathbb{Z}_{\hat{\mathfrak{p}}}$$

where $\mathfrak{p}$ is the set of all prime numbers.

Proof. Let $m \in \mathbb{N}$ and write $m = \prod_{p\in\mathfrak{p}} p^{c_p(m)}$. The Coprime Ideal Theorem (Theorem II.A.2.9) yields an isomorphism $\phi_m \colon \mathbb{Z}/m \to \prod_{p\in\mathfrak{p}} \mathbb{Z}/p^{c_p(m)}$ that is compatible with any projection $\mathbb{Z}/k \twoheadrightarrow \mathbb{Z}/m$ for $m|k$. Thus, $\widehat{\mathbb{Z}} \cong \varprojlim_i \prod_{p\in\mathfrak{p}} \mathbb{Z}/p^{c_p(i)}$. There are natural continuous surjections $\prod_{p\in\mathfrak{p}} \mathbb{Z}_{\hat{\mathfrak{p}}} \twoheadrightarrow \prod_{p\in\mathfrak{p}} \mathbb{Z}/p^{c_p(i)}$ so we get a homomorphism $\psi \prod_{p\in\mathfrak{p}} \mathbb{Z}_p \to \varprojlim_i \prod_{p\in\mathfrak{p}} \mathbb{Z}/p^{c_p(i)}$ which is continuous by Lemma II.A.2.6 and surjective since ψ has dense image (Lemma II.A.2.5) and the codomain is compact. Injectivity is clear so we conclude that ψ is the desired isomorphism. □

(3) *Direct products of profinite groups are profinite groups.*
Proof. Exercise. ◆

(4) We can define

$$\mathrm{GL}_n(\mathbb{Z}_{\hat{\mathfrak{p}}}) = \{M \in \mathbf{M}_{n\times n}(\mathbb{Z}_{\hat{\mathfrak{p}}})\colon \det M \in \mathbb{Z}_{\hat{\mathfrak{p}}}^\times\}$$

it is an exercise to show that

{eqn.GLnZp_invLim}
$$\mathrm{GL}_n(\mathbb{Z}_{\hat{\mathfrak{p}}}) = \varprojlim_i \mathrm{GL}_n(\mathbb{Z}/p^i) \tag{2.7–i}$$

and that

$$\mathrm{GL}_n(\widehat{\mathbb{Z}}) = \prod_p \mathrm{GL}_n(\mathbb{Z}_p).$$

Hint. For (2.7–i) show that there are epimorphisms

$$\pi_i \colon \mathrm{GL}_n(\mathbb{Z}_{\hat{\mathfrak{p}}}) \twoheadrightarrow \mathrm{GL}_n(\mathbb{Z}/p^i)$$

induced by the projections $\mathbb{Z}_{\hat{\mathfrak{p}}} \twoheadrightarrow \mathbb{Z}/p^i$. Now, adapt the proof of Proposition II.A.2.10, for injectivity show that $\bigcap \ker \pi_i = 1$. ◆

(5) One similarly obtains $\mathrm{SL}_n(\mathbb{Z}_{\hat{\mathfrak{p}}}) = \{M \in \mathbf{M}_{n\times n}(\mathbb{Z}_{\hat{\mathfrak{p}}})\colon \det M = 1\}$, $\mathrm{SL}_n(\mathbb{Z}_{\hat{\mathfrak{p}}}) = \varprojlim_i \mathrm{SL}_n(\mathbb{Z}/p^i)$, and that $\mathrm{SL}_n(\widehat{\mathbb{Z}}) = \prod_p \mathrm{SL}_n(\mathbb{Z}_p)$.

II.A.3. Basic properties.

Lemma II.A.3.1. *Let $\mathbf{G}$ be a profinite group and let $X \subseteq \mathbf{G}$. The closure of X in $\mathbf{G}$ is*

$$\overline{X} = \bigcap_{N \trianglelefteq_0 G} XN$$

Proof. Each set XN is clopen since it is a union of cosets of N. Clearly, $X \subseteq XN$ for each N. If $g \notin \overline{X}$, then there is some open set $U \subseteq \mathbf{G}$ such that $g \in U$ and $X \cap U = \varnothing$. Theorem II.A.2.4 yields an open normal subgroup $N \trianglelefteq \mathbf{G}$ such that $g \in gN \subseteq U$. Suppose $g \in XN$, we may write $g = xn$ with $X \in X$ and $n \in N$, then $x = gn^{-1} \in gN \subseteq U$, a contradiction. □

Proposition II.A.3.2. *A closed subgroup of a profinite group is a profinite group.*

Proof. Let $\mathbf{G} = \varprojlim G_i$ with projections $\varphi_i \colon \mathbf{G} \to G_i$ and let H be a closed subgroup of $\mathbf{G}$. We define an inverse system of groups $H_i = \varphi_i(H)$ and transition maps being the restrictions of the transition maps for $\mathbf{G}$. Let $\mathbf{K} = \varprojlim H_i$. It suffices to show $H = \mathbf{K}$. By construction $H \leqslant \mathbf{K}$. Let $g = (g_i) \notin H$. Since H is closed, $\mathbf{G}\backslash H$ is open. By Theorem II.A.2.4 it follows that $\varphi_i(h) \neq g_i$ for all $h \in H$. Hence, $g_i \notin H_i$ and thus, $g \notin \mathbf{K}$. □

Thm.1stIsoProf

THEOREM II.A.3.3 (The First Isomorphism Theorem). *Let* $\mathbf{G}$ *be a profinite groups. The following hold:*

(1) *If* $\mathbf{N}$ *be a closed normal subgroup, then* $\mathbf{G}/\mathbf{N}$ *with the quotient topology is a profinite group.*

Let $\pi\colon \mathbf{G} \twoheadrightarrow \mathbf{Q}$ *be a continuous surjection, let* $K = \ker \pi$*, and let* $q\colon \mathbf{G} \twoheadrightarrow \mathbf{G}/K$ *denote the natural projection. Endow* $\mathbf{G}/K$ *with the quotient topology.*

(2) *There exists a homeomorphism* $f\colon \mathbf{G}/K \to \mathbf{Q}$ *such that* $\pi = f \circ q$*.*

Proposition II.A.3.4. *If* $\mathbf{G}$ *is a profinite group, then* $\mathbf{G}$ *is residually finite.*

PROOF. Since $\mathbf{G}$ is the inverse limit of a directed system of finite groups (G_i) we may view $\mathbf{G}$ as a subgroup of $\prod G_i$. Thus, $\mathbf{G}$ is residually finite by Exercise I.A.1.7 and Exercise I.A.1.6. □

Exercise II.A.3.5. If $\mathbf{G}$ is a profinite group, then $\mathbf{G}$ is either finite or uncountable. [Hint: Use the Baire Category Theorem.]

II.A.4. Generating sets.

Definition II.A.4.1 (Topological generating set)**.** Let G be a topological group and let $S \subset G$. The *closed subgroup of* G *(topologically) generated by* S, denoted $\overline{\langle S\rangle}$ is the smallest closed subgroup of G containing S.

It is easy to see that if $H \leqslant G$, then the closure $\overline{H} \subseteq G$ is also a subgroup. In particular, for $S \subseteq G$, the closure of the subgroup $\langle S\rangle$ and the subgroup topologically generated by S coincide.

Definition II.A.4.2 (Topologically finitely generated)**.** If a topological group G is topologically generated by a finite subset $S \subseteq G$ then we say G is *topologically finitely generated.*

Exercise II.A.4.3. The following hold.

(1) Let $\mathbf{G}$ be a topologically finitely generated profinite group. If U is a open subgroup of $\mathbf{G}$, then U is topologically finitely generated.
(2) Let (G_i) be an inverse system of finite groups with inverse limit $\mathbf{G}$ and projections $\pi_i\colon \mathbf{G} \twoheadrightarrow G_i$. A subset $S \subseteq G$ is a topological generating set for G if and only if $\pi_i S$ generates $\pi_i \mathbf{G}$ for every i.
(3) Let $\mathbf{G}$ be a topologically finitely generated profinite group. Then $\mathbf{G}$ is an inverse limit of a countable inverse system of finite groups.

The following result was proved by Gaschütz for finite groups [**Gas55**] and extended to topologically finitely generated groups by Jarden and Kiehne [**JK75**].

GaschutzLemma

THEOREM II.A.4.4 (Gaschütz's Lemma). *Let* $\mathbf{G}$ *and* $\mathbf{H}$ *be profinite groups and let* $\Psi\colon \mathbf{G} \twoheadrightarrow \mathbf{H}$ *be a continuous epimorphism. Suppose that* $\mathbf{G}$ *is topologically generated by a set of size* d*. Then, for any topological generating set* T *of size* d *of* $\mathbf{H}$*, there exists some generating set* S *of size* d *of* $\mathbf{G}$ *such that* $\Psi|_S$ *is a bijection.*

PROOF. We first prove the result for finite groups. To this end assume $G = \mathbf{G}$ and $H = \mathbf{H}$ are finite.

Extend the map $\Psi\colon G \to H$ to the product map $\psi := (\Psi)^d\colon G^d \to H^d$. Let $\underline{t} = (t_1, \ldots, t_d) \in H^d$ be such that $\{t_1, \ldots, t_d\}$ generates H. For the remainder of the proof we will say that $\underline{t}$ *generates* H.

We will proceed by induction on $|G|$ with H fixed. Our induction hypothesis is that the number $\mathcal{M}(G, \underline{t})$, defined to be the number of ordered tuples $\underline{s} = (s_1 \ldots s_d) \in G^d$ such that

(1) $\{s_1 \ldots, s_d\}$ generate G; and
(2) $(\psi)^d(\underline{s}) = \underline{t}$,

is independent of the tuple $\underline{t}$. That is $\mathcal{M}(G, \underline{t}) = \mathcal{M}(G, \underline{t}')$ for every $\underline{t}, \underline{t}' \in H^d$ that generate H.

Let $\mathcal{P}_d$ denote the set of proper d-generator subgroups of G. Now, every $\underline{s} \in G^d$ generates G or some subgroup in $\mathcal{P}_d$ so we have

$$\{\underline{s}\colon (\psi)^d(\underline{s}) = \underline{t}\} = \mathcal{M}(G, \underline{t}) + \sum_{P \in \mathcal{P}_d} \mathcal{M}(P, \underline{t}).$$

Now, $|\{\underline{s}\colon (\psi)^d(\underline{s}) = \underline{t}\}| = |\ker \psi|^d$ so

$$\mathcal{M}(G, \underline{t}) = |\ker \psi|^d - \sum_{P \in \mathcal{P}_d} \mathcal{M}(P, \underline{t})$$

but by our inductive hypothesis every term on the right hand side is independent of the tuple $\underline{t}$. Hence, $\mathcal{M}(G, \underline{t})$.

To conclude the proof in the case of finite groups observe that since G^d has some tuple $\underline{s}$ which generates G we have $\mathcal{M}(G, (\psi)^d \underline{t}) \geqslant 1$. Hence, $\mathcal{M}(G, \underline{t}) \geqslant 1$ for every tuple $\underline{t} \in H^d$ that generates H.

Now, suppose $\mathbf{G}$ and $\mathbf{H}$ are profinite groups and write them as inverse limits of finite groups $\mathbf{G} = \varprojlim G_i$ and $\mathbf{H} = \varprojlim H_j$ such that the projection maps $\mathbf{G} \to G_i$ and $\mathbf{H} \to H_j$ are surjective. Let $(\psi_i)\colon (G_i) \to (H_i)$ be a morphism of the inverse systems with inverse limit Ψ and such that each ψ_i is surjective.

Let $\underline{t} \in \mathbf{H}^d$ be a tuple that generates H and let $\underline{t}_i$ be its image in H_i. Define X_i to be the set of tuples $\underline{s}_i \in G_i^d$ such that $(\psi_i)^d(\underline{s}_i) = \underline{t}_i$. By the result for finite groups established above these sets are non-non-empty. The transition maps in the inverse system (G_i) map X_i to X_j whenever $i \geqslant j$, so we have an inverse limit of non-empty sets $X = \varprojlim X_i$ which is non-empty by Proposition II.A.1.6(3). Now, an element of $\underline{t} \in X$ generates G and $(\Psi)^d(\underline{t}) = \underline{s}$ as required. □

II.A.5. The Nikolov–Segal Theorem.

Theorem II.A.5.1 (Nikolov–Segal). *If* $\mathbf{G}$ *is a finitely generated profinite group, then every subgroup of finite index in* $\mathbf{G}$ *is open.*

We highlight an important corollary.

Corollary II.A.5.2 (Automatic continuity)**.** *Let* $\mathbf{G}$ *and* $\mathbf{H}$ *be finitely generated profinite groups. If* $\Theta\colon \mathbf{G} \to \mathbf{H}$ *is an abstract group homomorphism, then* Θ *is continuous.*

II.B. Profinite completions

II.B.1. The completion functor.

Definition II.B.1.1 (Pro-$\mathcal{C}$ completion)**.** Let G be a group and let $\mathcal{C}$ be a formation of finite groups. Consider the non-empty set of finite index normal subgroups $\mathcal{N}_{\mathcal{C}} = \{N \trianglelefteq G : G/N \in \mathcal{C}\}$ of G. We form an inverse system by declaring for $M, N \in \mathcal{N}_{\mathcal{C}}$ that $M \preceq N$ if $N \leqslant M$. The maps are given by the natural epimorphisms $\varphi_{NM} : G/N \twoheadrightarrow G/M$. The group

$$G_{\widehat{\mathcal{C}}} := \varprojlim_{n \in \mathcal{N}_{\mathcal{C}}} G/N$$

is the *pro-$\mathcal{C}$ completion* of G.

When $\mathcal{C}$ consists of all finite groups we instead write $\widehat{G}$ and refer to the resulting profinite group as the *profinite completion* of G. When $\mathcal{C}$ consists of all finite p-groups we obtain the *pro-p completion* of G which we denote by $G_{\hat{\mathbf{p}}}$. When $\mathcal{C}$ consist of all nilpotent or soluble groups, we refer to $G_{\widehat{\mathcal{C}}}$ as the *pro-nilpotent completion* and *pro-soluble completion* respectively.

The group G has natural map $\iota_{\mathcal{C}} : G \to G_{\widehat{\mathcal{C}}}$ given by $g \mapsto (gN)_{N \in \mathcal{N}_{\mathcal{C}}}$. By Lemma II.A.2.5, the image $\iota_{\mathcal{C}}(G)$ is dense in $G_{\widehat{\mathcal{C}}}$.

The next exercise clarifies the link to our study of residual finiteness.

`Ex.resC_embedsGhat`

Exercise II.B.1.2. Let $\mathcal{C}$ be a formation of finite groups. A group G is residually-$\mathcal{C}$ if and only if the natural map $G \to G_{\widehat{\mathcal{C}}}$ is injective.

The following theorem is an easy consequence of work on inverse limits.

`thm.proC_univ`

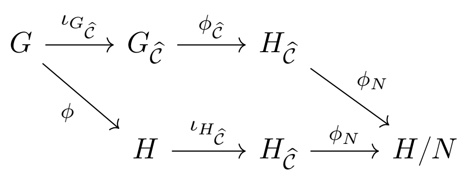
THEOREM II.B.1.3 (Universal property of the pro-$\mathcal{C}$ completion). *Let G be a group and let $\mathbf{H}$ be a pro-$\mathcal{C}$ group. Then, any group homomorphism $G \to \mathbf{H}$ factors uniquely through a continuous homomorphism $\widehat{G} \to \mathbf{H}$.*

Remark II.B.1.4. Note that although pro-$\mathcal{C}$ completion has a universal property, it is not the case that for $\mathbf{G}$ a pro-$\mathcal{C}$ group, the map $\iota_{\widehat{\mathcal{C}}} : \mathbf{G} \to \mathbf{G}_{\widehat{\mathcal{C}}}$ is necessarily an isomorphism.

The next proposition shows that taking pro-$\mathcal{C}$ completions is functorial.

Proposition II.B.1.5. *Let $\mathcal{C}$ be a formation of finite groups. If $\phi : G \to H$ is a group homomorphism, then there exists a unique continuous group homomorphism $\phi_{\widehat{\mathcal{C}}} : G_{\widehat{\mathcal{C}}} \to H_{\widehat{\mathcal{C}}}$ such that $\phi_{\widehat{\mathcal{C}}} \circ \iota_{G_{\widehat{\mathcal{C}}}} = \iota_{H_{\widehat{\mathcal{C}}}} \circ \phi$.*

PROOF. For any $N \trianglelefteq H$ with H/N in $\mathcal{C}$ we have a homomorphism $\phi_N : G \to H/N$ given by the composition. By the universal property of the pro-$\mathcal{C}$ completion we obtain a homomorphism $(\phi_N)_{\widehat{\mathcal{C}}} : G_{\widehat{\mathcal{C}}} \to H/N$. These maps are clearly compatible with the transition maps in the inverse system $\mathcal{N}_{\mathcal{C}}(H)$. So by the definition of a limit, there is a unique continuous homomorphism $\phi_{\widehat{\mathcal{C}}} : G_{\widehat{\mathcal{C}}} \to H_{\widehat{\mathcal{C}}}$. As $\phi_N \phi_{\widehat{\mathcal{C}}} \iota_{G_{\widehat{\mathcal{C}}}} = \phi_N \iota_{H_{\widehat{\mathcal{C}}}} \phi$, that is the following diagram commutes



for every $N \in \mathcal{N}_{\mathcal{C}}(H)$ we have that $\phi_{\hat{\mathcal{C}}} \circ \iota_{G_{\hat{\mathcal{C}}}} = \iota_{H_{\hat{\mathcal{C}}}} \circ \phi$. □

Applying the Nikolov–Segal Theorem and the universal property we obtain the following useful lemma.

`lem:EpisHoms_Ghat_G`

Lemma II.B.1.6. *Let $\mathcal{C}$ be a formation of finite groups and let G be a finitely generated group. For every $Q \in \mathcal{C}$ there are bijections*

$$\hom(G_{\hat{\mathcal{C}}}, Q) \to \hom(G, Q) \text{ and } \operatorname{epi}(G_{\hat{\mathcal{C}}}, Q) \to \operatorname{epi}(G, Q).$$

II.B.2. Finite quotients determine the completion. At this point we have seen the interactions between subgroup separability, the profinite topology, and profinite completions. While developing these abstract theories is certainly interesting it is now time to link everything back to our motivating question from the introduction.

> *Given a finitely generated group G and a class of groups $\mathcal{X}$. To what extent do the isomorphism classes of finite quotients of G determine G amongst groups in $\mathcal{X}$?*

The following theorem was first proved by Dixon, Formanek, Poland and Ribes [**DFPR82**]. Our proof is considerably simplified by applying the Nikolov–Segal Theorem.

`thm.DixonFormanekPolandRibes`

THEOREM II.B.2.1. *Let $\mathbf{G}$ and $\mathbf{H}$ be topologically finite generated profinite groups. If the isomorphism types of continuous finite quotients of $\mathbf{G}$ and $\mathbf{H}$ are equal, then $\mathbf{G} \cong \mathbf{H}$ as profinite groups.*

PROOF. Let G_n denote the intersection of all subgroups of $\mathbf{G}$ of index n and define H_n similarly. We have $\mathbf{G} = \varprojlim \mathbf{G}/G_n$ and similarly $\mathbf{H} = \varprojlim \mathbf{H}/H_n$.

Claim II.B.2.2. $\mathbf{G}/G_n \cong \mathbf{H}/H_n$.

PROOF OF CLAIM. There exists an open subgroup N of $\mathbf{H}$ with $\mathbf{H}/V \cong \mathbf{G}/G_n$. Because the intersection of normal subgroups of $\mathbf{G}/G_n$ whose index is at most n is trivial, we may write N as an intersection of open normal subgroups of $\mathbf{H}$ of index at most n. Now, $|\mathbf{G}/G_n| = |\mathbf{H}/V| \leqslant |\mathbf{H}/H_n|$ and by symmetry we obtain $|\mathbf{G}/G_n| \geqslant |\mathbf{H}/H_n|$. Whence, the claim. ■

It remains to establish that the transition maps in the two inverse systems are compatible. Let $I_n := \operatorname{Iso}(\mathbf{G}/G_n, \mathbf{H}/H_n)$ denote the set of isomorphisms $\mathbf{G}/G_n \to \mathbf{H}/H_n$ and let $\phi_n \in I_n$. Since ϕ_n maps normal subgroups to normal subgroups, it induces a unique isomorphism $\psi_{nm} \colon \mathbf{G}/G_m \to \mathbf{H}/H_m$ such that

$$\begin{array}{ccc}
\mathbf{G}/G_n & \longrightarrow & \mathbf{G}/G_m \\
{\scriptstyle \phi_n}\big\downarrow & & \big\downarrow{\scriptstyle \psi_{nm}} \\
\mathbf{H}/H_n & \longrightarrow & \mathbf{H}/H_m.
\end{array}$$

It follows that $\{I_n, \psi_{nm}\}$ is an inverse system of non-empty finite sets and so the inverse limit $\Psi = \varprojlim I_n$ and defines an isomorphism of inverse systems $\varprojlim \mathbf{G}/G_n \to \varprojlim \mathbf{H}/H_n$. Thus, $\mathbf{G} \cong \mathbf{H}$. □

Corollary II.B.2.3. *Let $\mathcal{C}$ be a formation of finite groups and let G and H be finitely generated groups. If the sets of isomorphism types of finite quotients of G and H in $\mathcal{C}$ are isomorphic, then $G_{\hat{\mathcal{C}}} \cong H_{\hat{\mathcal{C}}}$.*

The following lemma is extraordinarily useful.

Lemma II.B.2.4 (The Promoting Epimorphisms Lemma)**.** *Let $\mathcal{C}$ be a formation of finite groups and let G be a finitely generated residually $\mathcal{C}$ group. If $\varphi\colon G \twoheadrightarrow H$ is an epimorphism, and $G_{\hat{\mathcal{C}}} \cong H_{\hat{\mathcal{C}}}$, then φ is an isomorphism.*

Proof. Let $g \in \ker \varphi$ and note that there is a finite quotient $\alpha\colon G \twoheadrightarrow Q$ such that in $Q \in \mathcal{C}$ and $\alpha(g) \neq 1$. The map α is not in the image of the injection $\hom(H,Q) \to \hom(G,Q)$. Thus, $|\hom(G,Q)| > |\hom(H,Q)|$ contradicting Lemma II.B.1.6. □

II.B.3. Enter profinite rigidity. We are now ready to reformulate our profinite rigidity question from the introduction in terms of profinite completions:

Motivating Question (Profinite rigidity). *Given a finitely generated group G and a class of groups $\mathcal{X}$. To what extent does $\widehat{G}$ determine G amongst groups in $\mathcal{X}$?*

This also raises a second question about group invariants.

Motivating Question (Profinite invariants). *Let $\mathcal{X}$ be a class of finitely generated residually finite groups and let $G, H \in \mathcal{X}$. If $\widehat{G} \cong \widehat{H}$, what properties do G and H share?*

A first straightforward observation is that the lattice of finite index subgroups of G and of $\widehat{G}$ are intimately related.

Proposition II.B.3.1. *Let $\mathcal{C}$ be a formation of finite groups. If G is a finitely generated residually finite group, then there is a bijection*

$$\eta\colon \{N \leqslant_{\mathrm{fi}} G : N \text{ open in } \tau_{\mathcal{C}}(G)\} \to \{U \colon U \leqslant G_{\hat{\mathcal{C}}} \text{ an open subgroup}\}$$

by $N \mapsto \overline{N}$; with inverse given by $U \mapsto U \cap G$. Moreover, if $H, K \in \mathcal{N}_{\mathcal{C}}(G)$ and $H \leqslant K$, then

(1) $|K : H| = |\overline{K} : \overline{H}|$;
(2) $H \trianglelefteqslant K$ if and only if $\overline{H} \trianglelefteqslant \overline{K}$; and in this case $K/H = \overline{K}/\overline{H}$;
(3) if $L \in \mathcal{N}_{\mathcal{C}}(G)$, then $\overline{K \cap L} = \overline{K} \cap \overline{L}$; and $\overline{\langle K, L\rangle} = \langle \overline{K}, \overline{L}\rangle$.

In particular, the topology of $G_{\hat{\mathcal{C}}}$ induces on G the full pro-$\mathcal{C}$ topology.

Proof. Let H be a finite index subgroup of G open in $\tau_{\mathcal{C}}(G)$. Clearly, $H \leqslant G \cap \overline{H}$. Let $g \in G \cap \overline{H}$ and recall that $\overline{H} = \varprojlim_{N \in \mathcal{N}_{\mathcal{C}}(G)} HN/N$. So $g \in HN$. Since $\mathrm{Core}_G(H) \in \mathcal{N}_{\mathcal{C}}(G)$ we have $g \in \mathrm{Core}_G(H)H = H$. Thus $G \cap \overline{H} \leqslant H$.

Let U be an open subgroup of $G_{\hat{\mathcal{C}}}$. Since G is dense in $G_{\hat{\mathcal{C}}}$ if follows that $G \cap U$ is dense in U. Hence, $\overline{U \cap G} = U$. This establishes the bijection η.

We now prove (1). It suffices to establish the result in the case that $K = G$. As G is dense in $G_{\hat{\mathcal{C}}}$ we have $G\overline{H} = G_{\hat{\mathcal{C}}}$. Let $t_1, \dots, t_n$ be a right transversal of $\overline{H}$ in $G_{\hat{\mathcal{C}}}$, so $G = \coprod_{i=1}^n \overline{H}t_i$. Now, if $t \in G$, then $G \cap \overline{H}t = tH$. So,

$$G = G \cap \left(\coprod_{i=1}^n \overline{H}t_i\right) = \coprod_{i=1}^n Ht_i$$

and so $|G_{\widehat{\mathcal{C}}} : \overline{H}| = |G : H|$.

To prove (2) first suppose that $H \trianglelefteq G$. For every $N \in \mathcal{N}_{\mathcal{C}}(G)$ we have $HN/N \trianglelefteq G/N$. Hence, $\overline{H} \trianglelefteq G_{\widehat{\mathcal{C}}}$. Now, suppose U is an open normal subgroup of $G_{\widehat{\mathcal{C}}}$, then $U \cap G \trianglelefteq G$. Hence, normal subgroups map to normal subgroups under η.

Now, suppose $H \trianglelefteq K \leqslant G$ such that $H, K \in \mathcal{N}_{\mathcal{C}}(G)$. The homorphism $K \to \overline{K} \to \overline{K}/\overline{H}$ has kernel $K \cap \overline{H} = H$. Thus, it is an isomorphism since $|H : K| = |\overline{H} : \overline{K}|$ by (1).

Item (3) follows from items (1) and (2) and the fact that η is a bijection as claimed.

We now prove the "in particular". But this follows immediately from the bijection η. □

Let G be finitely generated and residually $\mathcal{C}$. If $H \leqslant G$, then the pro-$\mathcal{C}$ topology on G induces some mystery pro topology on H and so also determines some completion of H. As G is residually $\mathcal{C}$ we have that H embeds into $G_{\widehat{\mathcal{C}}}$ and determines a subgroup $\overline{H}$. This yields an epimorphism $H_{\widehat{\mathcal{C}}} \to \overline{H}$. Clearly, this map is injective exactly when G induces the full pro-$\mathcal{C}$ topology on H. From this we obtain the following easy lemma.

Lemma II.B.3.2. *Let $\mathcal{C}$ be a formation of finite groups, let G be a residually $\mathcal{C}$ group, and let $i\colon H \to G$ be an inclusion. If for every finite index subgroup $H' \leqslant H$, the subgroup H' is $\mathcal{C}$-separable in G, then the natural map $i_{\widehat{\mathcal{C}}}\colon H_{\widehat{\mathcal{C}}} \to G_{\widehat{\mathcal{C}}}$ is an isomorphism.*

We highlight an important consequence for LERF groups.

Corollary II.B.3.3. *Let G be a finitely generated LERF group. If H is a finitely generated subgroup of G, then the natural map $\widehat{H} \to \overline{H} \leqslant \widehat{G}$ is an isomorphism.*

II.B.4. Genus of groups. The *(profinite) genus* $\mathcal{G}(G)$ of a finitely generated residually finite group G is defined to be the set

$$\mathcal{G}(G) = \left\{ H \text{ f. g. residually finite } \mid \widehat{H} \cong \widehat{G} \right\} / \cong .$$

In other words, $\mathcal{G}(G)$ is the set of isomorphisms classes of finitely generated residually finite groups whose profinite completion is isomorphic to that of G.

If $\mathcal{B}$ is a class of residually finite groups, then we denote by $\mathcal{G}_{\mathcal{B}}(G) := \mathcal{G}(G) \cap \mathcal{B}$ the $\mathcal{B}$-*genus* of G. We call a finitely generated residually finite group G *profinitely rigid* (resp. $\mathcal{B}$-profinitely rigid) if $\mathcal{G}(G) = \{G\}$ (resp. $\mathcal{G}_{\mathcal{B}}(G) = \{G\}$). We say that G is *almost profinitely rigid* (resp. almost $\mathcal{B}$-profinitely rigid) if $|\mathcal{G}(G)| < \infty$ (resp. $|\mathcal{G}_{\mathcal{B}}(G)| < \infty$).

Note that these definitions are equivalent to the ones given in the introduction.

II.B.5. Varieties of groups.

Definition II.B.5.1. A non-empty *variety of groups* is a non-empty collection of groups $\mathcal{X}$ such that if $G \in \mathcal{X}$ then G satisfies a given set of equationally defined relations $\{r_i(x_1, \dots, x_n) = 1\colon i \in I\}$ for every $x_1, \dots, x_n \in G$.

The following theorem of Birkhoff classifies when a class of groups forms a variety of groups [**Bir35**].

THEOREM II.B.5.2 (Birkhoff). *A non-empty class of groups is a variety if and only if it is closed under taking subgroups, quotients, and direct products.*

Examples II.B.5.3. The following equations determine varieties of groups:

(1) *Abelian groups:* $r = [x, y]$.
(2) *Nilpotent groups of class at most c:* $r = [[\dots[[x_1, x_2], x_3]\dots], x_c]$
(3) *Soluble groups of derived length at most n:* since this class is closed under subgroups, quotients, and direct products, it forms a variety by Birkhoff's Theorem.
(4) *Burnside varieties:* $r = x^n$. Any variety in which such an equation holds is known as a Burnside variety. All groups in such a variety are torsion and of exponent at most n.

If a variety of groups is defined by only finitely many equations then we may multiply the equations together as $r_1(x_{1_1}, \dots, x_{n_1}) \dots r_k(x_{1_k}, \dots, x_{n_k})$. This new equation alone still defines the variety. In this case we saw that the variety is defined by a *group law*.

Example II.B.5.4. Let $(G_i)_{i \in \mathbb{N}}$ be a sequence of nilpotent groups such that the class of G_i is i. The group $\prod_{i \in \mathbb{N}} G_i$ is not nilpotent. Hence, by Birkhoff's Theorem the class of all nilpotent groups does not form a variety. A similar argument applies to the class of soluble groups.

thm:LawsPassToCompletion

THEOREM II.B.5.5. *Let G be a finitely generated residually finite group and let r be a group law. Then G satisfies r if and only if $\widehat{G}$ satisfies r.*

PROOF. This is essentially a corollary of Birkhoff's Theorem. Suppose $\widehat{G}$ satisfies r. Since G is residually finite, by Exercise II.B.1.2, $G \leqslant \widehat{G}$. As a variety is subgroup closed, it follows that G satisfies r. Conversely, if G satisfies r, then so does every quotient of G. As varieties are closed under direct products, it follows that the product

$$P = \prod_{N \trianglelefteq G,\ |G:N| < \infty} G/N$$

satisfies r. But $\widehat{G} \leqslant P$. Hence $\widehat{G}$ satisfies r. □

II.B.6. Profinite rigidity of finitely generated abelian groups. The first Betti number of a finitely generated group G is

$$b_1(G) := \dim_{\mathbb{Q}}(G^{\mathrm{ab}} \otimes \mathbb{Q})$$

where G^{ab} is the abelianisation of G.

lem:b1_profinite

Lemma II.B.6.1. *Let p be a prime $\mathcal{C}$ be a formation of finite groups containing all abelian p-groups. Let G and H be finitely generated groups. If H is isomorphic to a dense subgroup of $G_{\widehat{\mathcal{C}}}$, then $b_1(H) \geqslant b_1(G)$.*

PROOF. One has that $b_1(G)$ is the greatest integer k such that G sujects onto $(\mathbb{Z}/p^n)^k$ for all $n \geqslant 1$. Now, for every finite group Q, by density, an epimorphism $G_{\widehat{\mathcal{C}}} \twoheadrightarrow A$ restricts to an epimorphism on both G and H. However, the map $\mathrm{epi}(G_{\widehat{\mathcal{C}}}, Q) \to \mathrm{epi}(H, Q)$ need not be surjective. Thus, if G surjects onto $(\mathbb{Z}/p^n)^k$ so does H. □

lem:ab_profinite

Lemma II.B.6.2. *Let $\mathcal{C}$ be a formation of finite groups containing all finite abelian groups. Let G and H be finitely generated groups. If $G_{\widehat{\mathcal{C}}} \cong H_{\widehat{\mathcal{C}}}$, then $G^{\mathrm{ab}} \cong H^{\mathrm{ab}}$.*

Proof. Write $G^{\mathrm{ab}} \cong \mathbb{Z}^r \oplus T_1$ and $H^{\mathrm{ab}} \cong \mathbb{Z}^s \oplus T_2$ where T_i is a finite abelian group. By Lemma II.B.6.1 we have that $b_1(G) = b_1(H)$ so $r = s$. Now, we have quotients $G \twoheadrightarrow T_2$ and $H \twoheadrightarrow T_1$ and hence $T_1 \twoheadrightarrow T_2$ and $T_2 \twoheadrightarrow T_1$ (for these pick a prime $p > |T_1||T_2|$ and map G_i onto $T_j \oplus (\mathbb{Z}/p)^r$ for $i = j+1 \mod 2$). This implies $T_1 \cong T_2$ since they are finite. □

We are now ready to prove are first profinite rigidity result.

Theorem II.B.6.3. *Let G be a finitely generated abelian group. Then, $\mathcal{G}(G) = \{G\}$.*

Proof. Let $H \in \mathcal{G}(G)$. By Theorem II.B.5.5 we see that $\widehat{G}$ is abelian. Since $H \leqslant \widehat{G}$ we have that H is abelian. The result follows from Lemma II.B.6.2 and the classification of finitely generated abelian groups. □

Exercise II.B.6.4. We will investigate profinite rigidity amongst Baumslag–Solitar groups.

(1) Let $n \geqslant 2$. Then, $\mathrm{BS}(1,n) \cong \mathbb{Z}[1/n] \rtimes_n \mathbb{Z}$
(2) If $1 \leqslant |m| < |n|$, then there exists an epimorphism $\nu\colon \mathrm{BS}(m,n) \twoheadrightarrow \mathbb{Z}[1/mn] \rtimes_{n/m} \mathbb{Z}$.
(3) If $\gcd(m,n) = 1$, then $\ker \nu = \mathrm{BS}(m,n)^{(\infty)}$.
(4) For $m \geqslant 2$, the group $\mathrm{BS}(m, \pm m)$ contains a non-abelian free subgroup. [Hint: use the action on the Bass-Serre tree.]
(5) Let $\mathcal{B}$ denote the class of residually finite Baumslag-Solitar groups. Then, $\mathcal{G}_{\mathcal{B}}(\mathrm{BS}(1,n)) = \{\mathrm{BS}(1,n)\}$.

The following exercise studies an interesting one-relator group due to Baumslag [**Bau69**].

Exercise II.B.6.5. Let $G = \langle a, b \mid a = [a, b^{-1}ab]\rangle$.

(1) $a^2 = a^{(a^b)}$.
(2) $\widehat{G} = \widehat{\mathbb{Z}}$. [Hint: show every finite quotient of G is cyclic — you will need to use Fermat's Little Theorem.]
(3) G contains a non-abelian free subgroup.
(4) Conclude G is non-residually finite. [One could appeal to the profinite rigidity of $\mathbb{Z}$ here, although it is overkill to do so.]

The next exercise, first observed by Baumslag [**Bau74**], gives examples of some flexible virtually abelian groups.

Exercise II.B.6.6. We define two groups G and H are isomorphic to split extensions of shape $\mathbb{Z}/_{11} \rtimes \mathbb{Z}$. Here

$$G = \langle a, t \mid a^{11} = 1,\ tat^{-1} = a^4\rangle$$

and

$$H = \langle b, s \mid b^{11} = 1,\ sa^{-1} = a^8\rangle.$$

(1) G is not isomorphic to H. [Hint: Use the fact that $\mathrm{Aut}(\mathbb{Z}/_{11}) = \mathbb{Z}/_{10}$ and that t and s have different images contained in the $\mathbb{Z}/_5$ subgroup.]
(2) Every finite quotient of G is one of $\mathbb{Z}/_n$ or $\mathbb{Z}/_{11} \rtimes \mathbb{Z}/_k$, where $5|k$ and the action in the semi-direct is non-trivial of order 5.
(3) Every finite quotient of H is one of $\mathbb{Z}/_n$ or $\mathbb{Z}/_{11} \rtimes \mathbb{Z}/_k$, where $5|k$ and the action in the semi-direct is non-trivial of order 5.
(4) $\widehat{G} \cong \widehat{H} \cong \mathbb{Z}/_{11} \rtimes \widehat{\mathbb{Z}}$.

II.C. Torsion in the profinite completion

Our goal is to study how torsion in G influences the existence of torsion in $\widehat{G}$. Clearly, if $\widehat{G}$ is torsion-free then so is G. However, G being torsion-free does not guarantee that $\widehat{G}$ is and in fact there are counterexamples.

In particularly nice situations we are able to relate the torsion in $\widehat{G}$ to the torsion in G very concretely. However, the quest to do this will take a rather unusual detour through group cohomology. We quickly outline why one might think to connect these two areas:

(1) In nice situations the cohomological dimension of a torsion-free group is finite;
(2) the cohomological dimension of a finite group is infinite;
(3) the cohomology theory of a finite group is 'seen' by finite modules;
(4) so if we can find reasonable conditions for the profinite completion to see the cohomology of G, then we could try to detect torsion using cohomological dimension.

Our main reference for the next few subsections is Serre's book "Galois Cohomology" [**Ser97**].

II.C.1. Continuous cohomology of profinite groups. Let $\mathbf{G}$ be a profinite group. An abelian group M is a *discrete* $\mathbf{G}$*-module* if M, equipped with the discrete topology, is a $\mathbf{G}$-module such that $\mathbf{G}$ acts continuously.

Let $C_c^n(\mathbf{G}; M)$ be the set of all continuous maps $\mathbf{G}^{n+1} \to M$. One defines a coboundary operator $d_n \colon C_c^n(\mathbf{G}; M) \to C^{n+1}(\mathbf{G}; M)$ in the usual way: for $f \colon \mathbf{G}^n \to M$ we define

$$(d_n f)(g_0, \cdots, g_{n+1}) = \sum_{i=0}^{n+1} (-1)^i f(g_0, g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_{n+1}).$$

Clearly, $d_n f$ is a function in $C_c^{n+1}(\mathbf{G}; M)$ and $d_{n+1} \circ d_n = 0$. Thus, we obtain a chain complex $C_c^\bullet(\mathbf{G}; M)$ and we define, the *continuous cohomology groups of* $\mathbf{G}$ *in* M as

$$H_c^n(\mathbf{G}; M) = \ker d_{n+1} / \operatorname{im} d_n.$$

prop.Devissage_submodules

Proposition II.C.1.1. *Let* $\mathbf{G}$ *be a profinite group written as the inverse limit of finite groups* (G_i) *and let* M *be a discrete* $\mathbf{G}$*-module. Then, for all* $n \geqslant 0$ *we have*

$$H_c^n(G; M) = \varinjlim_{i,\ A \in \mathcal{FG}(M)} H_c^n(G_i; A)$$

where $\mathcal{FG}(M)$ *consists of all finitely generated* $\mathbf{G}$*-submodules of* A.

PROOF. It is an exercise to check that the canonical homomorphism

$$\varinjlim_{i\, A \in \mathcal{FG}(M)} H^n_c(G;A) \to H^n_c(G;M)$$

is an isomorphism. □

Remark II.C.1.2. From here basically everything reduces to the case of finite groups. We highlight a number of facts

(1) the category of discrete $\mathbf{G}$-modules does not in general have enough projectives, but it does have enough injectives;
(2) if M is an injective discrete $\mathbf{G}$-module, then $H^q_c(\mathbf{G};M) = 0$ for all $q \geqslant 1$;
(3) $H^0_c(\mathbf{G};M)$ is the $\mathbf{G}$-fixed points $M^{\mathbf{G}}$ of M;
(4) the functors $M \mapsto H^q_c(\mathbf{G};M)$ are the derived functors of $M \mapsto M^{\mathbf{G}}$;
(5) $H^1_c(\mathbf{G};M)$ is the group of continuous crossed homomorphisms of G to M;
(6) if M is finite, then $H^2_c(\mathbf{G};M)$ is in bijection with equivalence classes of extensions $1 \to M \to \mathbf{E} \to \mathbf{G} \to 1$. For a general M it is in bijection with equivalence classes of factor systems.

II.C.2. Coinduced modules. Let $\mathbf{G}$ be a profinite group and let $H \leqslant \mathbf{G}$ be a closed subgroup. Let M be a discrete H-module. We define the *coinduction of M from H to $\mathbf{G}$* to be the $\mathbf{G}$-module $\mathrm{coind}_H^{\mathbf{G}}(M) = \hom_H(\mathbf{G}, M)$. That is the group of continuous maps $m^*\colon \mathbf{G} \to M$ satisfying

$$m^*(hg) = h \cdot m^*(g)$$

for $h \in H$ and $g \in \mathbf{G}$. The $\mathbf{G}$-module structure is given by

$$(gm^*)(x) = m^*(g^{-1}x)$$

where $g, x \in G$. When $H = 1$ we shall write $\mathrm{coind}(M)$ for the coinduction and say that $\mathrm{coind}(M)$ is a *coinduced module.*

lem:Shapiro

Lemma II.C.2.1 (Shapiro's Lemma)**.** *Let $\mathbf{G}$ be a profinite group and let $H \leqslant \mathbf{G}$ be a closed subgroup. Let M be a discrete H-module. Then,*

(1) there are isomorphisms $H^q_c(\mathbf{G}; \mathrm{coind}_H^{\mathbf{G}} M) \to H^q_c(H;M)$;
(2) $H^q_c(\mathbf{G}; \mathrm{coind} M) = 0$ for $q \geqslant 1$.

PROOF. We define a homomorphism

$$\mathrm{coind}_H^{\mathbf{G}}(M) \to M \text{ by } m^* \mapsto m^*(1)$$

which induces homomorphisms $H^q_c(\mathbf{G}; \mathrm{coind}_H^{\mathbf{G}} M) \to H^q_c(H;M)$. The isomorphism follows from the fact that $\hom^{\mathbf{G}}(N, \mathrm{coind}_H^{\mathbf{G}}(M)) = \hom^H(N, M)$ for every discrete $\mathbf{G}$-module N. The second point also follows since this shows that injective modules are mapped to injective modules under coinduction. □

II.C.3. Cohomological dimension. The *cohomological dimension* of a discrete group G, denoted $\mathrm{cd}(G)$ is the smallest integer n or ∞ such that for every G-module M and every $q > n$ we have that $H^q(G;M) = 0$.

For a prime p, the *p-cohomological dimension* of a profinite group $\mathbf{G}$, denoted $\mathrm{cd}_p(\mathbf{G})$, is the smallest integer n or ∞ such that for every finite discrete G-module M and every $q > n$, the p-primary part of $H_c^q(\mathbf{G}; M)$ is zero. We define the *profinite cohomological dimension* to be

$$\widehat{\mathrm{cd}}(\mathbf{G}) := \sup_{p \in \mathfrak{p}} \{\mathrm{cd}_p(\mathbf{G})\}.$$

The reader may worry that we have restricted ourselves to *finite* modules instead of torsion modules. The next proposition will hopefully un-furrow their brow.

prop:cd_p_equivs

Proposition II.C.3.1. *Let p be a prime and let $\mathbf{G}$ be a profinite group. The following are equivalent*

(1) $\mathrm{cd}_p(\mathbf{G}) \leqslant n$*;*
(2) the p-primary part of $H_c^q(\mathbf{G}; M) = 0$ for all $q > n$ and every discrete torsion $\mathbf{G}$-module M;
(3) $H_c^q(\mathbf{G}; M) = 0$ for all $q > n$ and every discrete p-primary torsion $\mathbf{G}$-module M;
(4) $H_c^{n+1}(\mathbf{G}; M) = 0$ for every simple discrete $\mathbf{G}$-module M killed by p.

Proof. Trivially (2) implies (1). We show that (1) implies (3). Let M be a discrete p-primary torsion $\mathbf{G}$-module. If M is finite we are done trivially. Otherwise we write $M = \varinjlim_{A \in \mathcal{FG}(M)} A$ and note that each A is a finite module. Hence, for each A we have $H_c^q(\mathbf{G}; A) = 0$ for $q > n$. It follows from Proposition II.C.1.1 that $H_c^q(\mathbf{G}; M) = 0$.

The equivalence of (2) and (3) follows immediately from writing $M = \bigoplus M(p)$, the canonical p-primary decomposition of M, and then identifying $H^q(\mathbf{G}; M(p))$ with the p-primary part of $H_c^q(\mathbf{G}; M)$.

Clearly, (3) trivially implies (4). Now, assume (4), we aim to prove (3). Any finite discrete p-primary torsion module N is an iterated extension of simple discrete modules killed by p. From the long exact sequence in cohomology and induction on the length of the composition series we obtain that $H_c^{n+1}(\mathbf{G}; N) = 0$. For a discrete p-primary torsion module A, we write A as a limit of its finitely generated (hence finite) submodules and apply Proposition II.C.1.1.

To conclude we induct on q, the base case $q = n+1$ being complete. Now, embed A into the co-induced module $M = \hom(\mathbf{G}, A)$ by $a \mapsto a(x) = a \cdot x$. We obtain an extension of $\mathbf{G}$-modules $0 \to A \to M \to M/A \to 0$ and so obtain a long exact sequence in cohomology

$$\cdots \to H_c^q(\mathbf{G}; M/A) \to H_c^{q+1}(\mathbf{G}; A) \to H_c^{q+1}(\mathbf{G}; M) \to \cdots$$

where the first and third term of the pictured diagram are 0. Indeed, M/A is a p-torsion module so the inductive hypothesis applies, and M is a coinduced module so all of its cohomology vanishes above degree 0 by Lemma II.C.2.1. □

prop:cdp_closed_subs

Proposition II.C.3.2. *Let p be a prime and let $\mathbf{G}$ be a profinite group. If H is a closed subgroup of G, then $\mathrm{cd}_p(H) \leqslant \mathrm{cd}_p(G)$.*

Proof. Suppose A is a discrete torsion H-module, then $\mathrm{coind}_H^{\mathbf{G}}(M)$ is a discrete torsion $\mathbf{G}$-module and $H_c^q(\mathbf{G}; \mathrm{coind}_H^{\mathbf{G}}(M)) = H_c^q(H; M)$. The result follows from Proposition II.C.3.1. □

II.C.4. The comparison map. Let G be a finitely generated group and let M be a G-module. The map $\iota\colon G \to \widehat{G}$ induces a *comparison map* on cohomology groups

$$\iota_n\colon H^n_c(\mathbf{G}; M) \to H^n(G; M).$$

If M is a finite G-module, then the universal property of the profinite completion makes M a discrete $\mathbf{G}$-module.

Following Serre [**Ser97**, §I.2.6], we say G is *n-good* if for all $k \leqslant n$ and for all finite G-modules M, the comparison map ι_k is an isomorphism. If G is n-good for every n, then we say G is *good.*

lem:good_Serre_equivs

Lemma II.C.4.1. *For a group G the following are equivalent:*

(1) *for every finite discrete $\widehat{G}$-module M the map $\iota_n\colon H^i_c(\widehat{G}; M) \to H^i(G; M)$ is bijective for $0 \leqslant i \leqslant n$ and injective for $i = n+1$;*
(2) *for every finite discrete $\widehat{G}$-module M the map $\iota_n\colon H^i_c(\widehat{G}; M) \to H^i(G; M)$ is surjective for $0 \leqslant i \leqslant n$*
(3) *G is n-good.*

Proof. We have that (1) implies (2) and (3) and that (3) implies (2) so it suffices to show that (2) implies (1) which we leave as an exercise.

[Hint: show that (2) implies *for all $c \in H^q(G; M)$ and $1 \leqslant q \leqslant n$ there exists a subgroup H of G, the preimage of an open subgroup K of $\widehat{G}$ such that x maps to zero under the restriction map $H^q(G; M) \to H^q(H; M)$*. Now, show that the previous statement implies *for all $c \in H^q(G; M)$ and $1 \leqslant q \leqslant n$, there exists a finite G-module N containing M such that the image of c is zero under the induced map $H^q(G; M) \to H^q(G; N)$* taking N to be the coinduced module $\operatorname{coind}^G_H(M)$. Finally, show this last statement implies (1) using induction on n and the long exact sequence in cohomology for the short exact sequence $0 \to M \to N \to M/N \to 0$.] □

lem:1-good_Serre

Lemma II.C.4.2. *All groups are 1-good.*

Proof. Let M be a finite G-module. By the universal property of a profinite completion (Theorem II.B.1.3) we have that the image of G in $\operatorname{Aut}(M)$ is equal to the image of $\widehat{G}$ in $\operatorname{Aut}(M)$. Thus, the fixed point submodules M^G and $M^{\widehat{G}}$ are equal. Recall that $H^1(G; M) \cong \hom^G(G, M)$ which is equal to $\hom^{\widehat{G}}(\widehat{G}; M)$ by Lemma II.B.1.6. But this latter group is isomorphic to $H^1_c(\widehat{G}; M)$. □

Example II.C.4.3. We record a number of examples

(1) Finite groups are good.
(2) Free groups are good. This follows from the fact that free groups have $\operatorname{cd}(G) \leqslant 1$, Lemma II.C.4.1, and Lemma II.C.4.2.

The following extremely useful theorem of Lorensen [**Lor08**] will give us many more examples.

thm.Lorensen_group_ext_good

Theorem II.C.4.4 (Lorensen). *Let N and Q be n-good groups and suppose that N is type FP_{n-1}. If G is an extension $1 \to N \to G \to Q \to 1$, then G is n-good.*

(1) Poly-{finitely generated free} groups are good.

(2) Being good is a commensurability invariant (exercise)
(3) Finitely generated abelian groups are good.

II.C.5. Goodness and separability. The following proposition relates goodness and separability of kernels in group extensions. The forward direction was proven by Serre in [**Ser97**] and the converse was given by Lorensen [**Lor08**, Proposition 2.4].

prop:Good_ResFin_Extensions

Proposition II.C.5.1. *Let G be a group. The following are equivalent:*

(1) G is 2-good;

(2) for every extension $1 \to N \xrightarrow{i} E \to G \to 1$ with N finitely generated, the map $\widehat{i}\colon \widehat{N} \to \widehat{G}$ is injective.

Proof. Assume first N is finite. We may reduce to the case where N is a minimal normal subgroup of E because an extension of a good group with finite kernel is good by Theorem II.C.4.4.

Suppose N is abelian. The action of E on N by conjugation gives N the structure of a G-module with corresponding extension class $c \in H^2(G; N)$. By 2-goodness there is a corresponding class of $H^2_c(\widehat{G}; N)$ mapped to c by the comparison map. In particular, there is a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & N & \longrightarrow & \widehat{E} & \longrightarrow & \widehat{G} & \longrightarrow & 1 \end{array}$$

where the first down arrow is an isomorphism and the third down arrow is injective. Hence, the middle down arrow is injective too.

Suppose N is non-abelian. Observe that the subgroup K defined to be the kernel of the map $E \to \mathrm{Aut}(N)$ is finite index in E. We have $N \cap K = 1$. So the projection $E \to G$ maps K injectively to a subgroup of finite index in G. It follows that K and hence E are residually finite. Hence, the map $N = \widehat{N} \to \widehat{G}$ is injective.

We now suppose N is finitely generated and that K is a finite index subgroup of N. We need to show there is a finite index subgroup E_0 of E such that $E_0 \cap N \leqslant K$. As N is finitely generated there is finite index characteristic subgroup H contained in K that is normal in E. Thus, we obtain a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \pi} & & \downarrow & & \\ 1 & \longrightarrow & N/H & \longrightarrow & \widehat{E}/H & \longrightarrow & \widehat{G} & \longrightarrow & 1 \end{array}$$

where N/H is finite. Now, by the result for the finite case we find $E_0' \leqslant E/H$ such that $E_0' \cap (N/H) = 1$. Thus, $E_0 = \pi^{-1}(E_0')$ satisfies $E_0 \cap N \leqslant H \leqslant K$ as required.

We now prove (2) implies (1) following Lorensen's argument. By Lemma II.C.4.1 it is enough to show the map $H^2_c(\widehat{G}; M) \to H^2(G; M)$ is surjective for all finite discrete $\widehat{G}$-modules M. Let $c \in H^2(G; M)$ and take a corresponding group extension $1 \to M \to E \to G \to 1$. Passing to profinite completions we obtain a short exact sequence of profinite groups $1 \to M \to \widehat{E} \to \widehat{G} \to 1$. The cohomology class of this extension in $H^2_c(\widehat{G}; M)$ is then mapped to c by the homomorphism $H^2_c(\widehat{G}; M) \to H^2(G; M)$. ☐

We record another theorem of Lorensen [**Lor08**, Theorem 2.10], this time relating residual finiteness of group extensions and goodness.

THEOREM II.C.5.2 (Lorensen). *Let G be a group. The following are equivalent*

(1) G is residually finite and 2-good;
(2) for any extension $1 \to N \to E \to G \to 1$, with N a finitely generated residually finite group, the group E is residually finite;
(3) $1 \to N \to E \to G \to 1$, with N a finite group, the group E is residually finite.

PROOF. We leave this as an exercise since the proof is not dissimilar to Proposition II.C.5.1 ☐

II.C.6. Relating cohomology to torsion.

`lem:cd_hat_cd_Z`

Lemma II.C.6.1. *Let G be a good discrete group. If $\mathrm{cd}(G) \leqslant n$, then $\widehat{\mathrm{cd}}(\widehat{G}) \leqslant n$.*

PROOF. Since $\mathrm{cd}(G) \leqslant n$, we have $H^q(G; M) = 0$ for every G-module M and every $q > n$. If M is finite, by goodness we have $H^q_c(\widehat{G}; M) = 0$ for every $q > n$. Whence, the lemma. ☐

We finally attain the goal of the section.

`thm.good.tf`

THEOREM II.C.6.2. *Let G be a residually finite good group. If $\mathrm{cd}(G)$ is finite, then $\widehat{G}$ is torsion-free*

PROOF. Suppose $\widehat{G}$ is not torsion-free. Then, there exists $g \in \widehat{G}$ of prime order p. Now, $H = \langle g \rangle$ is a closed subgroup of $\widehat{G}$ so $\mathrm{cd}_p(H) \leqslant \mathrm{cd}_p(G)$. Since H is discrete, the ordinary and continuous cohomology of H coincides. But then $H^k(H; \mathbb{F}_p) \neq 0$ for all $k \geqslant 0$. So $\mathrm{cd}_p(H)$ is infinite and hence, by Proposition II.C.3.2, so is $\mathrm{cd}_p(\widehat{G})$. Which contradicts Lemma II.C.6.1. ☐

II.C.7. When things go wrong. In this section we will see how being torsion-free does not imply that the profinite completion is. To start we recall a classical result of Mennicke [**Men65**].

`thm.CongrCompl_SLn`

THEOREM II.C.7.1 (Mennicke). *Let $n \geqslant 3$ and let $\leqslant \mathrm{SL}_n(\mathbb{Z})$. If H is a finite index subgroup of $\mathrm{SL}_n(\mathbb{Z})$, then there exists an m such that H contains $\Gamma_m := \ker(\mathrm{SL}_n(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_n(\mathbb{Z}/m))$. In particular, $\mathrm{SL}_n(\widehat{\mathbb{Z}}) = \widehat{\mathrm{SL}_n(\mathbb{Z})}$.*

The 'in particular' conclusion of the previous theorem is known as the *congruence subgroup property*. The groups Γ_m are known as *congruence subgroups*. For a general group A and a subgroup G of its outer automorphism group we may define the *congruence subgroups of G with respect to A* as follows: let $C \trianglelefteq A$ be a characteristic finite index normal subgroup, then we obtain a homomorphism $\phi_C\colon \mathrm{Out}(A) \to \mathrm{Out}(A/C)$; our congruence subgroups are then the groups $\ker \phi_C \cap A$. The congruence subgroups define a pro-topology on G known as the *congruence topology* (with respect to A).

One can take the completion with respect to the congruence topology to obtain a profinite group known as the *congruence completion* (of G with respect to A). Denote the congruence completion by $G_{\widehat{\mathcal{C}(A)}}$. There is a natural surjective map $\widehat{G} \twoheadrightarrow G_{\widehat{\mathcal{C}(A)}}$ of which we call its kernel the *congruence kernel.*

THE CONGRUENCE SUBGROUP PROBLEM. *Let A be residually finite a group. For which residually finite groups $G \leqslant \mathrm{Out}(A)$ is the congruence kernel of G with respect to A finite?*

At the time of writing the congruence subgroup property (CSP) is known for any S-arithmetic lattice in the following algebraic groups: a non-anisotropic group, any group not of type A_n, and any unitary group of a hermitian form. It is conjectured not to hold for lattices in rank one Lie groups. It is known not to hold for lattices in $\mathrm{SO}(n,1)$ except when $n = 7$ where there are some open cases — notably trialitarian lattices. It is open for many lattices in $\mathrm{SU}(n,1)$ — notably type II arithmetic lattices; and it is completely open for lattices in $\mathrm{Sp}(n,1)$ and F_4^{-20}. In higher rank it is open for the cases of inner and outer forms of A_n. In particular, it is open for cocompact lattices in $\mathrm{SL}_3(\mathbb{R})$ and $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$.

The following result of Lubotzky exploits the CSP to produce a lot of torsion in the profinite completion of torsion-free finite index subgroups of $\mathrm{SL}_n(\mathbb{Z})$ for $n \geqslant 3$ [**Lub93**].

Proposition II.C.7.2 (Lubotzky)**.** *For each $r \geqslant 2$ there exists a finitely generated torsion-free linear group G such that $\widehat{G}$ contains uncountably many conjugacy classes of elements of order r.*

PROOF. Let $n \geqslant 3$. The group $\mathrm{SL}_n(\mathbb{Z})$ is virtually torsion-free, let G be any such finite index subgroup. Now, $\widehat{G}$ is a finite index open subgroup of $\widehat{\mathrm{SL}_n(\mathbb{Z})}$ which by Mennicke's theorem Theorem II.C.7.1 is isomorphic to $\prod_{p\in\mathfrak{p}} \mathrm{SL}_n(\mathbb{Z}_{\hat{\mathfrak{p}}})$. Hence, $\widehat{G}$ contains $\prod_{p\in\mathfrak{p}\setminus S} \mathrm{SL}_n(\mathbb{Z}_{\hat{\mathfrak{p}}})$ as a direct factor where S is a finite set of primes. Let $r \geqslant 2$, by Dirichlet's Theorem there is an infinite set of primes $\mathfrak{Q}$ with $r|q-1$ and $\mathfrak{Q} \cap S = \varnothing$. For every $p \in \mathfrak{Q}$ the group $\mathbb{Z}_{\hat{\mathfrak{p}}}$ has a unit of order r and so, $\mathrm{SL}_n(\mathbb{Z}_{\hat{\mathfrak{p}}})$ has an element g_r of order r. Let $A \subseteq \mathfrak{Q}$. We define an element $\alpha_A = (a_i)$ of $\mathrm{SL}_n(\widehat{\mathbb{Z}})$ by $a_i = g_r$ if $p \in A$ and $a_i = 1$ otherwise. It is easy to see this gives an element of order r in G. Moreover, if A and A' are different subsets of $\mathfrak{Q}$, the elements α_A and $\alpha_{A'}$ are not conjugate. □

II.D. Rigidity of virtually abelian groups

Todo 4: Write chapter

II.D.1. Background on crystallographic groups.

II.D.2. Almost rigidity.

II.D.3. Examples.

CHAPTER III

Profinite rigidity and nilpotent groups

III.A. Background on nilpotent groups

III.A.1. Central series and structure theorems. Given a group G we define a series of subgroups

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n = G$$

to be a *central series* if each $G_i \trianglelefteq G$ and G_{i+1}/G_i is contained in $Z(G/G_i)$ for all i. The *lower central series* of G is defined to be the series of subgroups

$$G = \gamma_1 G \geqslant \gamma_2 G \geqslant \dots$$

where $\gamma_1 G = G$ and $\gamma_{n+1} G = [\gamma_n G, G]$. The *upper central series* of G is defined to be the series of subgroups

$$1 = \zeta_0 G \leqslant \zeta_1 G = Z(G) \leqslant \zeta_2 G \leqslant \dots$$

where $\zeta_{n+1} G/\zeta_n G = Z(G/\zeta_n G)$ and $\zeta_1 G = Z(G)$.

A group G is *nilpotent* if it admits a finite length central series terminating in G. The length of the shortest central series of G is the *nilpotency class* of G.

Exercise III.A.1.1. Let G be a nilpotent group. The nilpotent class of G is equal to the length of the upper and lower central series.

Lemma III.A.1.2. *If G is a nilpotent group and $N \trianglelefteq G$ is non-trivial, then $N \cap Z(G)$ is non-trivial.*

Proof. We have $G = \zeta_c G$ for some c. Thus, there exists a smallest positive integer i such that $N \cap \zeta_i G \neq 1$. So, $[N \cap \zeta_i G, G] \leqslant N \cap \zeta_{i-1} G = 1$. Now, $[G, N \cap \zeta_i G] \leqslant [G, N] \cap [G, \zeta_i G] \leqslant N \cap \zeta_{i-1} G$ where the last inclusion follows from $[G, \zeta_i G] \leqslant \zeta_{i-1} G$. But $N \cap \zeta_{i-1} G = 1$ by our choice of i. Hence, $i = 1$ and so $N \cap \zeta_1 G = N \cap Z(G)$ is non-trivial. □

There are homomorphisms

$$\epsilon_i \colon (\gamma_i G/\gamma_{i+1} G) \otimes G^{\mathrm{ab}} \twoheadrightarrow \gamma_{i+1} G/\gamma_{i+2} G$$

by

$$a\gamma_{i+1} G \otimes g[G, G] \mapsto [a, g]\gamma_{i+2} G.$$

The maps ϵ_i are surjective because $\gamma_{i+1} G = [\gamma_i G, G]$.

Exercise III.A.1.3. The maps ϵ_i are well defined group homomorphisms.

`lem:nilp_induct_otimes_ext`

Lemma III.A.1.4. *Let $\mathcal{P}$ be a group theoretic property which is closed under*

(1) extensions; and

(2) homomorphic images of tensor products of abelian groups.

If G is a nilpotent group such that G^{ab} has $\mathcal{P}$, then G has $\mathcal{P}$.

PROOF. Let $F_i = \gamma_i G/\gamma_{i+1} G$. Suppose F_i has $\mathcal{P}$, then F_{i+1} has $\mathcal{P}$ because it is a homomorphic image of $F_i \otimes G^{\mathrm{ab}}$. Thus, by induction every lower central factor of G has $\mathcal{P}$. Since some $\gamma_{c+1}G = 1$ and $\mathcal{P}$ is clsoed under extensions, it follows that G has $\mathcal{P}$. □

Corollary III.A.1.5. *Let G be a nilpotent group. G is finite if and only if G^{ab} is finite.*

A group G is *polycyclic* if G admits a series

$$1 \trianglelefteq G_0 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that G_i/G_{i-1} is a (possibly infinite) cyclic group. If each G_i is isomorphic to $\mathbb{Z}$, then we say G is *poly-$\mathbb{Z}$*.

`ex.tf_nilp_poly_Z`

Exercise III.A.1.6. Let G be a finitely generated torsion-free nilpotent group. Then, G is poly-$\mathbb{Z}$.

Let $\pi \subseteq \mathfrak{p}$ be a non-empty set of prime powers. We call a group whose elements are finite order and have prime power divisors in π a *π-group*, such a number is a *π-number*.

A crafty application of the previous lemma gives us a huge amount of control over the torsion in nilpotent groups.

Lemma III.A.1.7. *Let G be a nilpotent group. The torsion elements of G form a normal subgroup T such that G/T is torsion-free. Moreover, $T = \prod_{p \in \mathfrak{p}} T_p$ where T_p is the maximal p-subgroup of G.*

PROOF. Let $\pi \subseteq \mathfrak{p}$ be a non-empty set of primes. Let T_π denote the subgroup generated by all elements of order whose prime divisors are in π. Now, T_π^{ab} is generated by elements whose prime divisors are in π too. Moreover, it is actually equal to the set of such elements. Now, since T_π^{ab} is a π-group, it follows from Lemma III.A.1.4 is also a π-group.

If $\pi = \mathfrak{p}$, then $T = T_{\mathfrak{p}}$ consists of all elements of finite order. Hence, T is torsion. Taking $\pi = p$ we obtain that T_p is a p-group. It is now easy to see that $T_p \trianglelefteq G$, that $T = \prod_{p \in \mathfrak{p}} T_p$, and that G/T is torsion-free. □

Exercise III.A.1.8. Finitely generated nilpotent groups are residually finite.

A group G is *periodic* if it has a finite *exponent* k, that is, $g^k = 1$ for every $g \in G$.

`lem:fg_nilp_periodic`

Lemma III.A.1.9. *If G is a finitely generated periodic nilpotent group, then G is finite.*

PROOF. We induct on the nilpotency class c. If $c = 1$, then G is a finitely generated periodic abelian group and so obviously finite. Suppose $c > 1$, and note that $[G, G]$ is of nilpotency class $c - 1$. By the inductive hypothesis, $[G, G]$ is finite. Thus, G is an extension of finite groups and hence finite. □

III.A.2. Dimension subgroups. Let G be a group and denote its integral group ring by $\mathbb{Z}G$. The *augmentation* $\epsilon \colon \mathbb{Z}G \to \mathbb{Z}$ by $\sum n_g g \mapsto \sum n_g$. The kernel $\mathfrak{I}$ of ϵ is the *augmentation ideal* of $\mathbb{Z}G$.

For a positive integer n, the *nth dimension subgroup of* G is the subgroup

$$\Delta_n(G) = (1 + \mathfrak{I}^n) \cap G.$$

Note that this is the kernel of the action by right multiplication of G on $\mathbb{Z}G/\mathfrak{I}^n$. Hence, we obtain a sequence of G-modules

$$0 = \mathfrak{I}^n/\mathfrak{I}^n \subseteq \mathfrak{I}^{n-1}/\mathfrak{I} \cdots \subseteq \mathfrak{I}^i/\mathfrak{I}^n \subseteq \cdots \subseteq \mathbb{Z}G/\mathfrak{I}^n$$

Since $\mathfrak{I}^{i-1}(G-1) \subseteq \mathfrak{I}^i$ for each i, we see that G acts trivially on each of the factors. Hence, $G/\Delta_n(G)$ is nilpotent of class at most $n-1$ and $\gamma_n(G) \leqslant \Delta_n(G)$.

Lemma III.A.2.1. *If G is a finitely generated group, then $\mathfrak{I}^n/\mathfrak{I}^{n+1}$ is a finitely generated abelian group.*

Proof. We first show that $\mathfrak{I}/\mathfrak{I}^2$ is finitely generated (in fact isomorphic to G^{ab}.

Define $G \to \mathfrak{I}/\mathfrak{I}^2$ by $g \mapsto (g-1) + \mathfrak{I}^2$. This is a homomorphism since for $g, h \in G$ we have $gh - 1 = (g-1) + (h-1) + (g-1)(h-1)$. As the latter group is abelian we obtain a homomorphism

$$\alpha \colon G^{\mathrm{ab}} \to \mathfrak{I}/\mathfrak{I}^2 \text{ by } g[G,G] \mapsto (g-1) + \mathfrak{I}^2.$$

As $\mathfrak{I}$ is a free abelian group with basis $\{g - 1 : 1 \neq g \in G\}$ we may define a homomorphism

$$\nu \colon \mathfrak{I} \to G^{\mathrm{ab}} \text{ by } (g-1) \mapsto g[G,G].$$

Now, for $g, h \in G$ non-trivial we have

$$\begin{aligned} \nu((g-1)(h-1)) &= \nu((gh-1) - (g-1) - (h-1)) \\ &= gh[G,G] \cdot (g[G,G])^{-1} \cdot (h[G,G])^{-1} \\ &= 1. \end{aligned}$$

Since $\mathfrak{I}^2$ is generated by elements of the form $(g-1)(h-1)$ we see that $\mathfrak{I}^2 \leqslant \ker \nu$ and that ν induces a homomorphism $\mu \colon \mathfrak{I}/\mathfrak{I}^2 \to G^{\mathrm{ab}}$. It is easy to check that $\alpha \circ \mu = \mathrm{id}_{\mathfrak{I}/\mathfrak{I}^2}$ and that $\mu \circ \alpha = \mathrm{id}_{G^{\mathrm{ab}}}$.

Now, if $n \geqslant 1$ there is a surjective homomorphism of abelian groups

$$\beta_n \colon \mathfrak{I}/\mathfrak{I}^2 \otimes \mathfrak{I}^{n-1}/\mathfrak{I}^n \to \mathfrak{I}^n/\mathfrak{I}^{n+1} \text{ by } (a + \mathfrak{I}^n)(b + \mathfrak{I}^2) \mapsto ab + \mathfrak{I}^{n+1}.$$

Hence, the result follows from induction on n. □

thm.Jennings.DimSub

Theorem III.A.2.2 (Jennings). *If G is a finitely generated torsion-free nilpotent group of class c, then $\Delta_{c+1}(G) = 1$.*

III.A.3. Nilpotent actions. Let G and A be groups and suppose G acts on A by automorphisms. We say G acts *nilpotently* on A if there exists a composition series

$$0 \leqslant A_0 \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_n = A$$

such that A_i is a G-invariant normal subgroup and the induced G-action on A_i/A_{i-1} is trivial. We call the series a *G-series* of length n.

lem:nilp_actions

Lemma III.A.3.1. *Suppose a group G acts faithfully on a group A. If A admits a nilpotent G-series of length n, then G is nilpotent of class at most $n-1$.*

Proof. Exercise. □

lem:nilp_PID_actions

Lemma III.A.3.2. *Let R be a commutative principal ideal domain, let M be a finitely generated free R-module, and suppose G acts nilpotently and R-linearly on M. Then, M has an R-basis such that the G-action may be represented by unitriangular matrices.*

Proof. Define a chain of submodules $0 = M_0 \subset M_1 \subset \cdots \subset M_k = M$, where $M_i/M_{i-1} = (M/M_{i-1})^G$. Then, each M_i is an R-submodule of M. Moreover, M/M_{i-1} is R-torsion-free and hence a free R-module because R is a PID. We may write $M_i = M_{i-1} \oplus \left(\bigoplus_{j=1}^{r_i} x_{i,j}R\right)$ and the union of these bases $\{x_{i,j} : 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant r_i\}$ suffices. □

III.A.4. Canonical representations.

Definition III.A.4.1 (Representation ideal)**.** Let G be a finitely generated torsion-free nilpotent group of class c. Define an ideal $J = J(G) \subseteq \mathbb{Z}G$ by $J/\mathfrak{I}^{c+1} = (\mathbb{Z}G/\mathfrak{I}^{c+1})_{\mathrm{tors}}$. We call J the *representation ideal of G*. The reason for this will quickly become apparent.

lem:nilp_rep_J_cap_G

Lemma III.A.4.2. *Let G be a finitely generated torsion-free nilpotent group of class c. Then, $(J+1) \cap G = 1$.*

Proof. Let $H = (J+1) \cap G$. Let N denote the kernel of the G-action on $J/\mathfrak{I}^{c+1}$ by right multiplication. By Theorem III.A.2.2, G acts faithfully on $\mathbb{Z}G/\mathfrak{I}^{c+1}$, so $H \cap N$ is a subgroup of $\hom(\mathbb{Z}G/\mathfrak{I}, J/\mathfrak{I}^{c+1})$ and hence finite. But G is torsion free, so $H \cap N$ is trivial. □

lem:nilp_rep_J_faithful

Lemma III.A.4.3. *Let G be a finitely generated torsion-free nilpotent group of class c. The group $G \rtimes \mathrm{Aut}(G)$ acts on $\mathbb{Z}G$ faithfully extending the action of G, and the ideal J is invariant under this action. Moreover, $G \rtimes \mathrm{Aut}(G)$ acts faithfully on $\mathbb{Z}G/J$.*

Proof. Let $A = G \rtimes \mathrm{Aut}(G)$. We have that G acts by left translation on $\mathbb{Z}G$ and $a \in \mathrm{Aut}(G)$ acts on elements by $a(c_g \cdot g) = c_g \cdot g^a$ and then extending linearly. We leave it to the reader to check this is a well-defined action. It is easy to see that J is invariant under the action of A by its definition.

We now show the action on the quotient is faithful. Consider an element $ga \in A$ that acts trivially on $\mathbb{Z}G/J$. We will show the element is trivial. In J we have $g^a - 1 = 1^{g^a} - 1$. So $g^a = 1$ by Lemma III.A.4.2. Hence $g = 1$. Let $h \in G$ and observe that $h^a h^{-1} - 1 = hh^a h^{-1} - h \in hJ \subseteq J$. Applying Lemma III.A.4.2 we obtain $h^a h^{-1} = 1$ for all $h \in G$. Thus, $a = 1 \in \mathrm{Aut}(G)$. □

thm:nilp_canonical_rep

Theorem III.A.4.4. *Let G be a finitely generated torsion-free nilpotent group of class c. There exists an injective homomorphism $\alpha_G \colon G \rtimes \mathrm{Aut}(G) \to \mathrm{GL}_n(\mathbb{Z})$, where $n = \mathrm{rank}_{\mathbb{Z}}(\mathbb{Z}G/J)$ and image of G is unitriangular. Moreover, the homomorphism is canonical in the following sense: any isomorphism $\beta \colon G \to H$ may be realised by conjugating $\mathrm{im}\,\alpha_G$ to $\mathrm{im}\,\alpha_H$ in $\mathrm{GL}_n(\mathbb{Z})$.*

Proof. By Lemma III.A.4.3 we see that $A = G \rtimes \mathrm{Aut}(G)$ acts faithfully on the free abelian group $\mathbb{Z}G/J$ and so the associated homomorphism $\alpha \colon A \to \mathrm{GL}(\mathbb{Z}G/J) = \mathrm{GL}_n(\mathbb{Z})$ is injective. Since G acts nilpotently on

$\mathbb{Z}G/J$, by Lemma III.A.3.2, we may choose a basis such that G is contained in the upper unitriangular matrices of $\mathrm{GL}_n(\mathbb{Z})$.

It remains to verify the canonicity of the homomorphism. An isomorphism $\beta\colon G \to H$ induces an isomorphism $b\colon \mathbb{Z}G/J(G) \to \mathbb{Z}H/J(H)$. Clearly, b can represented by an element of $\mathrm{GL}_n(\mathbb{Z})$ and we have $(\operatorname{im}\alpha_G)^b = \operatorname{im}\alpha_H = \operatorname{im}(\alpha_H \circ \beta)$ as required. □

III.B. Almost rigidity of nilpotent groups

The goal of this section is to prove a splendid result of Pickel [**Pic71**] that the genus of a finitely generated torsion-free nilpotent group is finite. Our proof follows the line of argument in D. Segal's book [**Seg83**] and we provide a very loose sketch of Pickel's argument in a latter section. Segal's argument more readily generalises to the class of polycyclic-by-finite groups, see [**GPS80**]. But the reader should note this is a *highly* non-trivial result depending on a number of other results of Grunewald and Segal [**Seg78, GS78, GS79, GS82**].

III.B.1. Some sledgehammers involving algebraic groups. Let $\mathbf{G}$ be a algebraic $\mathbb{Q}$-group with a representation $\rho\colon \mathbf{G} \to \mathrm{GL}_n(\mathbb{Q})$ and denote by $\pi_k\colon \mathbf{G}(\mathbb{Z}) \to \mathbf{G}(\mathbb{Z}/_k)$ the congruence quotients of $\mathbf{G}(\mathbb{Z})$. Given two elements $a, b \in \mathbb{Z}^n$ we say that they $\mathbf{G}$-*equivalent* modulo k if there exists an element $g \in \mathbf{G}(\mathbb{Z}/_k)$ such that $g \cdot \overline{a} = \overline{b}$ where $\overline{a}, \overline{b}$ are the images of a and b under the map $\mathbb{Z}^n \twoheadrightarrow (\mathbb{Z}/_k)^n$. If a and b are $\mathbf{G}$-equivalent for every positive integer k, then we say that a and b are in the same *local orbit* of $\mathbf{G}$.

The following theorem of Borel and Serre [**BS64**], which goes far beyond the scope of this text, is the key result in an extremely useful sledgehammer we will need later.

thm:BorelSerre_local_orbits

THEOREM III.B.1.1 (Borel–Serre). *Let $\mathbf{G}$ be a algebraic $\mathbb{Q}$-group with a representation $\rho\colon \mathbf{G} \to \mathrm{GL}_n(\mathbb{Q})$. Every local orbit of $\mathbf{G}$ in $\mathbb{Q}^m$ is a union of finitely many orbits of $\mathbf{G}(\mathbb{Z})$.*

We say two subgroups H and K of $\mathbf{G}(\mathbb{Z})$ are $\mathbf{G}(\mathbb{Z})$-*congruent* if their images in $\mathbf{G}(\mathbb{Z}/_k)$ are conjugate for all positive integers k.

We arrive at our sledgehammer, due to Grunewald and Segal [**GS82**]. The proof again goes far beyond what we will cover here.

thm:GL_congruence_soluble

THEOREM III.B.1.2 (Grunewald–Segal). *Let $\mathbf{G}$ be a algebraic $\mathbb{Q}$-group. Then every $\mathbf{G}(\mathbb{Z})$-congruence class of soluble-by-finite subgroups of $\mathbf{G}(\mathbb{Z})$ is the union of finitely many conjugacy classes of subgroups of $\mathbf{G}(\mathbb{Z})$.*

Todo 5: Add sketch of proof

III.B.2. Proving almost rigidity.

lem:Segal_canonical_rep_profinite

Lemma III.B.2.1 (Segal)**.** *Let G and H be finitely generated torsion-free nilpotent groups. If $\widehat{G} \cong \widehat{H}$, then*

$$n := \operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}G/J(G)) = \operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}H/J(H)),$$

and the images of the canonical representations of G and H are $\mathrm{GL}_n(\mathbb{Z})$-congruent.

PROOF. Throughout this proof we let G^k denote the subgroup of G generated by kth powers of elements, that is by the set $\{g^k \mid g \in G\}$. We note that G/G^k has exponent k and so is a finite group by Lemma III.A.1.9.

Let G be of nilpotency class c and let $J(G)$ be the representation ideal of $\mathbb{Z}G$ and let $V_G = \mathbb{Z}G/J$. Denote by $\alpha_G \colon G \to \mathrm{GL}(V_G) = \mathrm{GL}_n(\mathbb{Z})$ the canonical representation G given by Theorem III.A.4.4.

By Theorem II.B.5.5 we have that H is nilpotent of class c. Let $0 < m \in \mathbb{Z}$ and choose q such that $qJ(G) \subseteq \mathfrak{I}^{c+1}$. Since $\mathbb{Z}G/\mathfrak{I}^{c+1}$ is a finitely generated abelian group, the quotient $R_G = \mathbb{Z}G/(qm\mathbb{Z}G + \mathfrak{I}^{c+1})$ is a finite ring. Thus, the kernel K of the map $G \to R_G^\times$ (the unit group) has finite index in G. In particular, G^k is contained in K for some $k > 0$.

Let $G_k = G/G^k$ and and note that the induced ring hommorphism $\mathbb{Z}G \to \mathbb{Z}G_k$ is surjective with kernel $(G^k - 1)\mathbb{Z}G$. Thus, there is an isomorphism

$$r \colon R_G = \mathbb{Z}G/(qm\mathbb{Z}G + \mathfrak{I}^{c+1}) \to \mathbb{Z}G_k/(qm\mathbb{Z}G_k + \mathfrak{I}_{G_k}^{c+1})$$

where $r(q\mathbb{Z}G + \mathfrak{I}^{c+1}) = q\mathbb{Z}G_k + \mathfrak{I}_{G_k}^{c+1}$.

Our choice of q implies that $V_G/mV_G = (q\mathbb{Z}G + \mathfrak{I}^{c+1})/(qm\mathbb{Z}G + \mathfrak{I}^{c+1})$. Indeed, $V_G = \mathbb{Z}G/J$ and $qJ \subseteq \mathfrak{I}^{c+1}$, so $V_G = q\mathbb{Z}G + \mathfrak{I}^{c+1}$. Thus, by the isomorphism r we have

$$V_G/mV_G \cong (q\mathbb{Z}G_k + \mathfrak{I}_{G_k}^{c+1})(qm\mathbb{Z}G_k + \mathfrak{I}_{G_k}^{c+1}).$$

We now choose q, k such that $qJ_H \subseteq \mathfrak{I}_H^{c+1}$ and $H^k - 1 = qm\mathbb{Z}H + \mathfrak{I}_H^{c+1}$. Let $H_k = H/H^k$. Note that G_k the largest quotient of G of exponent k and similarly for H_k and H. Since $\widehat{H} \cong \widehat{G}$ we have an isomorphism $f_m \colon G_k \to H_k$, which induces an isomorphism

$$(q\mathbb{Z}G_k + \mathfrak{I}_{G_k}^{c+1})/(qm\mathbb{Z}G_k + \mathfrak{I}_{G_k}^{c+1}) \to (q\mathbb{Z}H_k + \mathfrak{I}_{H_k}^{c+1})/(qm\mathbb{Z}H_k + \mathfrak{I}_{H_k}^{c+1}).$$

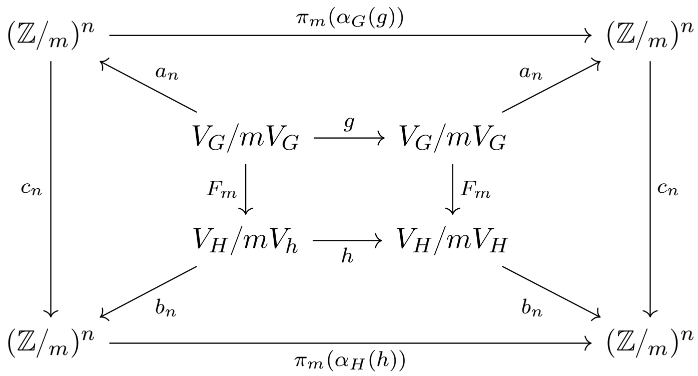
Hence, we get an isomorphism $F_m \colon V_G/mV_G \to V_H/mV_H$. Note that this implies the canonical representation $\alpha_H \colon H \to \mathrm{GL}(V_H)$ of H has image in $\mathrm{GL}_n(\mathbb{Z})$. Indeed, V_G/mV_G has order m^n and similarly for V_H/mV_H (here we take $m > 1$).

We fix isomorphisms $a \colon V_G \to \mathbb{Z}^n$ and $b \colon V_H \to \mathbb{Z}^n$ inducing α_G and α_H. We have a commutative square of isomorphism

$$\begin{array}{ccc} V_G/mV_G & \xrightarrow{a_m} & (\mathbb{Z}/_m)^n \\ {\scriptstyle F_m}\downarrow & & \downarrow{\scriptstyle c_m} \\ V_H/mV_H & \xrightarrow{b_m} & (\mathbb{Z}/_m)^n \end{array}$$

where $c_m = b_m \circ F_m \circ a_m^{-1}$ is an element of $\mathrm{GL}_n(\mathbb{Z}/_m)$. Let $\pi_m \colon \mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}_m)$ denote the congruence map. Our goal now is to show the equality $\pi_m(\alpha_G(G))^{c_m} = \pi_M(\alpha_H(H))$.

Let $g \in G$ and $h \in h$ and denote there images in G_k and H_k by $\overline{g}$ and $\overline{h}$. Suppose $f_m(\overline{g}) = \overline{h}$. We claim the following diagram commutes



but this is clear from the definitions of the maps involved. Thus it follows that $\pi_m(\alpha_H(h)) = c_n^{-1}\pi_m(\alpha_G(g))c_n$ as required. As m was arbitrary, we conclude that G and H are $\mathrm{GL}_n(\mathbb{Z})$-congruent. □

`PickelsTheorem`

THEOREM III.B.2.2 (Pickel). *Let G be a finitely generated torsion-free nilpotent group. Then, $\mathcal{G}(G)$ is finite and all such groups are torsion-free nilpotent.*

PROOF. Let $H \in \mathcal{G}(G)$. By Theorem II.B.5.5 we see that H is nilpotent. By Theorem II.C.4.4 and Exercise III.A.1.6 we conclude that H is good. By Theorem II.C.6.2 we see that H is torsion-free. Thus, we are in the setting of Lemma III.B.2.1 and so conclude that H is $\mathrm{GL}_n(\mathbb{Z})$-congruent to G for some n. But by Theorem III.B.1.2 H is contained in one of finitely many conjugacy classes of subgroups of $\mathrm{GL}_n(\mathbb{Z})$. Hence, there are only finitely many choices for H. □

III.B.3. Pickel's original argument. We summarise the original argument of Pickel [**Pic71**] in the following steps:

(1) Reduce to studying the pro-p completion.
(2) Relate the Mal'cev completions of the pro-p completions of G to rational Lie algebra of G tensored with the p-adic rationals. Specifically, the group given by the non-zero elements with multiplication the lie bracket is isomorphic to the Mal'cev completion of the pro-p completion of G.
(3) The deep result of Borel–Serre (Theorem III.B.1.1) implies the finiteness of the number of isomorphism classes rational Lie algebras which become isomorphic when tensored with the p-adic rationals.
(4) We apply the result of Borel–Serre to show that $\mathcal{G}(G)$ consists of finitely many commensurability classes of torsion-free nilpotent groups.
(5) We now show that the isomorphism classes in each commensurability class $[C]$ of the groups in $\mathcal{G}(G)$ is in bijection with a set of double cosets in some algebraic group.
(6) A deep result of Borel [**Bor63**] implies that the number of double cosets is finite.

III.B.4. Extension to polycyclic groups.

Todo 6: Write section

Todo 7: Prove Jennings theorem

Todo 8: Prove the Borel–Serre finiteness theorem

Todo 9: Better account of Galois cohomology

Bibliography

[Bau63] Gilbert Baumslag. Automorphism groups of residually finite groups. *J. London Math. Soc.*, 38:117–118, 1963. 10.1112/jlms/s1-38.1.117. Cited on Page 4.

[Bau69] Gilbert Baumslag. A non-cyclic one-relator group all of whose finite quotients are cyclic. *J. Austral. Math. Soc.*, 10:497–498, 1969. Cited on Page 26.

[Bau74] Gilbert Baumslag. Residually finite groups with the same finite images. *Compositio Math.*, 29:249–252, 1974. Cited on Page 26.

[Bir35] Garrett Birkhoff. On the structure of abstract algebras. *Proc. Camb. Philos. Soc.*, 31:433–454, 1935. Cited on Page 25.

[Bor63] Armand Borel. Some finiteness properties of adele groups over number fields. *Inst. Hautes Études Sci. Publ. Math.*, (16):5–30, 1963. Cited on Page 40.

[BS62] Gilbert Baumslag and Donald Solitar. Some two-generator one-relator non-Hopfian groups. *Bull. Amer. Math. Soc.*, 68:199–201, 1962. 10.1090/S0002-9904-1962-10745-9. Cited on Page 7.

[BS64] A. Borel and J.-P. Serre. Théorèmes de finitude en cohomologie galoisienne. *Comment. Math. Helv.*, 39:111–164, 1964. 10.1007/BF02566948. Cited on Page 38.

[CDE+95] G. Cairns, G. Davis, D. Elton, A. Kolganova, and P. Perversi. Chaotic group actions. *Enseign. Math. (2)*, 41(1-2):123–133, 1995. Cited on Page 5.

[DFPR82] John D. Dixon, Edward W. Formanek, John C. Poland, and Luis Ribes. Profinite completions and isomorphic finite quotients. *J. Pure Appl. Algebra*, 23(3):227–231, 1982. 10.1016/0022-4049(82)90098-6. Cited on Page 22.

[DS05] Cornelia Druţu and Mark Sapir. Non-linear residually finite groups. *J. Algebra*, 284(1):174–178, 2005. 10.1016/j.jalgebra.2004.06.025. Cited on Page 6.

[Gas55] Wolfgang Gaschütz. Zu einem von B. H. und H. Neumann gestellten Problem. *Math. Nachr.*, 14:249–252 (1956), 1955. 10.1002/mana.19550140406. Cited on Page 19.

[GPS80] F. J. Grunewald, P. F. Pickel, and D. Segal. Polycyclic groups with isomorphic finite quotients. *Ann. of Math. (2)*, 111(1):155–195, 1980. 10.2307/1971220. Cited on Page 38.

[GS78] Fritz J. Grunewald and Daniel Segal. A note on arithmetic groups. *Bull. London Math. Soc.*, 10(3):297–302, 1978. 10.1112/blms/10.3.297. Cited on Page 38.

[GS79] Fritz J. Grunewald and Daniel Segal. On congruence topologies in number fields. *J. Reine Angew. Math.*, 311/312:389–396, 1979. 10.1515/crll.1979.311-312.389. Cited on Page 38.

[GS82] Fritz J. Grunewald and Daniel Segal. Conjugacy of subgroups in arithmetic groups. *Proc. London Math. Soc. (3)*, 44(1):47–70, 1982. 10.1112/plms/s3-44.1.47. Cited on Page 38.

[H.64] Dyson. V. H. The word problem and residually finite groups. *Notices Amer. Math. Soc.*, 11:743, 1964. Abstract 616-7. Cited on Page 3.

[Hal49] Marshall Hall, Jr. Subgroups of finite index in free groups. *Canad. J. Math.*, 1:187–190, 1949. 10.4153/cjm-1949-017-2. Cited on Page 9.

[Hal50] Marshall Hall, Jr. A topology for free groups and related groups. *Ann. of Math. (2)*, 52:127–139, 1950. 10.2307/1969513. Cited on Page 2.

[HW99] Tim Hsu and Daniel T. Wise. On linear and residual properties of graph products. *Michigan Math. J.*, 46(2):251–259, 1999. 10.1307/mmj/1030132408. Cited on Page 12.

[JK75] Moshe Jarden and Ursel Kiehne. The elementary theory of algebraic fields of finite corank. *Invent. Math.*, 30(3):275–294, 1975. 10.1007/BF01425568. Cited on Page 19.

[Lor08] Karl Lorensen. Groups with the same cohomology as their profinite completions. *J. Algebra*, 320(4):1704–1722, 2008. 10.1016/j.jalgebra.2008.03.013. Cited on Pages 30, 31, and 32.

[Lub93] Alexander Lubotzky. Torsion in profinite completions of torsion-free groups. *Quart. J. Math. Oxford Ser. (2)*, 44(175):327–332, 1993. 10.1093/qmath/44.3.327. Cited on Page 33.

[Mal65] A. I. Mal'tsev. On the faithful representation of infinite groups by matrices. *Transl., Ser. 2, Am. Math. Soc.*, 45:1–18, 1965. 10.1090/trans2/045/01. Cited on Page 5.

[McK43] J. C. C. McKinsey. The decision problem for some classes of sentences without quantifiers. *J. Symbolic Logic*, 8:61–76, 1943. 10.2307/2268172. Cited on Page 3.

[Men65] Jens L. Mennicke. Finite factor groups of the unimodular group. *Ann. of Math. (2)*, 81:31–37, 1965. 10.2307/1970380. Cited on Page 32.

[Mes72] Stephen Meskin. Nonresidually finite one-relator groups. *Trans. Amer. Math. Soc.*, 164:105–114, 1972. 10.2307/1995962. Cited on Page 7.

[Mes74] Stephen Meskin. A finitely generated residually finite group with an unsolvable word problem. *Proc. Amer. Math. Soc.*, 43:8–10, 1974. 10.2307/2039314. Cited on Page 4.

[Mih58] K. A. Mihaĭlova. The occurrence problem for direct products of groups. *Dokl. Akad. Nauk SSSR*, 119:1103–1105, 1958. Cited on Page 8.

[Mih66] K. A. Mihaĭlova. The occurrence problem for direct products of groups. *Mat. Sb. (N.S.)*, 70(112):241–251, 1966. Cited on Page 8.

[Min21] Ashot Minasyan. Virtual retraction properties in groups. *Int. Math. Res. Not. IMRN*, (17):13434–13477, 2021. 10.1093/imrn/rnz249. Cited on Page 12.

[Mos66] A. Wł odzimierz Mostowski. On the decidability of some problems in special classes of groups. *Fund. Math.*, 59:123–135, 1966. 10.4064/fm-59-2-123-135. Cited on Page 3.

[Ore52] Oystein Ore. The general Chinese remainder theorem. *Amer. Math. Monthly*, 59:365–370, 1952. 10.2307/2306804. Cited on Page 17.

[Pic71] P. F. Pickel. Finitely generated nilpotent groups with isomorphic finite quotients. *Trans. Amer. Math. Soc.*, 160:327–341, 1971. 10.2307/1995809. Cited on Pages 38 and 40.

[Sco78] Peter Scott. Subgroups of surface groups are almost geometric. *J. London Math. Soc. (2)*, 17(3):555–565, 1978. 10.1112/jlms/s2-17.3.555. Cited on Page 10.

[Seg78] Daniel Segal. Two theorems of polycyclic groups. *Math. Z.*, 164(2):185–187, 1978. 10.1007/BF01174824. Cited on Page 38.

[Seg83] Daniel Segal. *Polycyclic groups*, volume 82 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1983. 10.1017/CBO9780511565953. Cited on Page 38.

[Ser97] Jean-Pierre Serre. *Galois cohomology*. Springer-Verlag, Berlin, 1997. 10.1007/978-3-642-59141-9, Translated from the French by Patrick Ion and revised by the author. Cited on Pages 27, 30, and 31.

[She88] Kangsheng Shen. The historical development of the Chinese remainder theorem. *J. Hangzhou Univ. Natur. Sci. Ed.*, 15(3):270–282, 1988. Cited on Page 17.

[Weh73] B. A. F. Wehrfritz. Generalized free products of linear groups. *Proc. London Math. Soc. (3)*, 27:402–424, 1973. 10.1112/plms/s3-27.3.402. Cited on Page 6.

Index

Todo list