Profinite Groups

Lectures by Gareth Wilkes
Notes by Alexis Marchand

University of Cambridge
Lent 2020
Part III course

Contents

1 Inverse limits

1.1 Categories and limits

Definition 1.1 (Category)**.** *A* category $\mathbf{C}$ *consists of:*

(i) *A collection* $\operatorname{ob}\mathbf{C}$ *of* objects $A, B, C, \ldots,$

(ii) *A collection* $\operatorname{mor}\mathbf{C}$ *of* morphisms $f, g, h, \ldots,$

(iii) *Two operations* dom *and* cod *from* $\operatorname{mor}\mathbf{C}$ *to* $\operatorname{ob}\mathbf{C}$*: we write* $A \xrightarrow{f} B$ *to mean* $f \in \operatorname{mor}\mathbf{C}$, $\operatorname{dom} f = A$ *and* $\operatorname{cod} f = B$,

(iv) *An operation* $A \mapsto \mathrm{id}_A$ *from* $\operatorname{ob}\mathbf{C}$ *to* $\operatorname{mor}\mathbf{C}$ *s.t.* $A \xrightarrow{\mathrm{id}_A} A$,

(v) *A partial binary operation* $(f, g) \mapsto fg$ *on* $\operatorname{mor}\mathbf{C}$ *defined* iff $\operatorname{dom} f = \operatorname{cod} g$ *and satisfying* $\operatorname{dom}(fg) = \operatorname{dom} g$ *and* $\operatorname{cod}(fg) = \operatorname{cod} f$,

satisfying:

(vi) $\mathrm{id}_B f = f = f \mathrm{id}_A$ *for all* $A \xrightarrow{f} B$,

(vii) $f(gh) = (fg)h$ *for all* $A \xrightarrow{h} B \xrightarrow{g} C \xrightarrow{f} D$.

Example 1.2. (i) **Set** *is the category of sets and functions.*

(ii) **Gp** *is the category of groups and group homomorphisms.*

(iii) **TopGp** *is the category of topological groups and continuous group homomorphisms.*

Definition 1.3 (Poset)**.** *A* poset *(or* partially-ordered set*) is a set* J *together with a binary relation* $\preccurlyeq$ *on* J *such that*

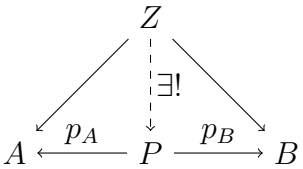
(i) $\forall j \in J,\ j \preccurlyeq j$,

(ii) $\forall i, j \in J,\ (i \preccurlyeq j \text{ and } j \preccurlyeq i) \Longrightarrow i = j$,

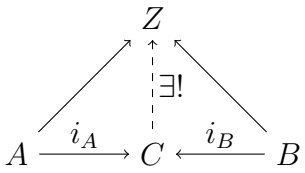
(iii) $\forall i, j, k \in J,\ (i \preccurlyeq j \text{ and } j \preccurlyeq k) \Longrightarrow i \preccurlyeq k$.

A poset can also be seen as a category whose object set is J *and where there is a unique arrow* $i \to j$ *if and only if* $i \preccurlyeq j$.

Definition 1.4 (Product)**.** *In a category* $\mathbf{C}$*, given two objects* A *and* B*, a* product *of* A *and* B *consists of an object* P *together with maps* $A \xleftarrow{p_A} P \xrightarrow{p_B} B$ *satisfying the following universal property: for any object* Z *with arrows* $A \leftarrow Z \rightarrow B$*, there exists a unique arrow* $Z \to P$ *making the following diagram commute:*

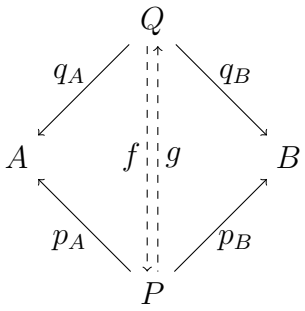


Dually, a coproduct *of A and B consists of an object C together with maps $A \xrightarrow{i_A} C \xleftarrow{j_B} B$ satisfying the following universal property: for any object Z with arrows $A \to Z \leftarrow B$, there exists a unique arrow $C \to Z$ making the following diagram commute:*

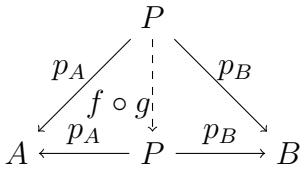


Proposition 1.5. *Products and coproducts, if they exist, are unique up to unique isomorphism.*

Proof. Let $A \xleftarrow{p_A} P \xrightarrow{p_B} B$ and $A \xleftarrow{q_A} Q \xrightarrow{q_B} B$ be two products of A and B. By the universal property of products, there are arrows $Q \xrightarrow{f} P$ and $P \xrightarrow{g} Q$ making the following diagram commute:



Now $f \circ g : P \to P$ makes the following diagram commute:

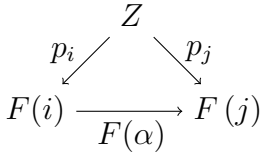


It follows by uniqueness that $f \circ g = \mathrm{id}_P$, and similarly $g \circ f = \mathrm{id}_Q$. Therefore, $P \cong Q$ and f, g are the only isomorphisms between P and Q that make the above diagram commute.

For coproducts, the proof is the same. □

Definition 1.6 (Diagram in a category)**.** *If* $\mathbf{J}$ *and* $\mathbf{C}$ *are categories, a* diagram of shape $\mathbf{J}$ *in* $\mathbf{C}$ *is a functor $F : \mathbf{J} \to \mathbf{C}$, i.e. an assignment of an object $F(X) \in \mathrm{ob}\,\mathbf{C}$ for each $X \in \mathrm{ob}\,\mathbf{J}$ and an assignment of an arrow $F(X) \xrightarrow{F(\alpha)} F(Y)$ for each $X \xrightarrow{\alpha} Y$ in $\mathbf{J}$, such that $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ and $F(\alpha \circ \beta) = F(\alpha) \circ F(\beta)$ whenever the composite is defined.*

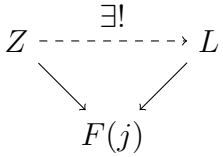
Definition 1.7 (Cones and limits)**.** *Let $F : \mathbf{J} \to \mathbf{C}$ be a diagram of shape $\mathbf{J}$. A* cone *over F is an object Z together with arrows $p_j : Z \to F(j)$ for all $j \in \mathrm{ob}\,\mathbf{J}$, such that the diagram*



commutes for all $i \xrightarrow{\alpha} j$ in $\mathbf{J}$.

Dually, a cocone *has the same definition, with all arrows reversed.*

A limit *of F is a cone L such that, for any other cone Z over F, there is a unique arrow $Z \to L$ such that the diagram*



commutes for all $j \in \operatorname{ob}\mathbf{J}$.

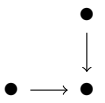
Dually, a colimit *has the same definition, with all arrows reversed.*

Example 1.8.

- *Products are limits of shape*

and coproducts are colimits of the same shape.

- *Pullbacks are limits of the following shape:*



Proposition 1.9. *Limits and colimits, if they exist, are unique up to unique isomorphism.*

Proof. Same proof as for products (Proposition 1.5). □

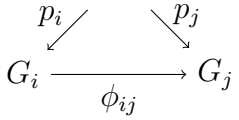
1.2 Inverse limits and profinite groups

Definition 1.10 (Inverse system)**.** *A poset* $(J, \preccurlyeq)$ *is called an* inverse system *if*

$$\forall i, j \in J,\ \exists k \in J,\ k \preccurlyeq i \text{ and } k \preccurlyeq j.$$

Definition 1.11 (Inverse limit of groups)**.** *An* inverse system of groups *(resp. sets) is a functor* $F : \mathbf{J} \to \mathbf{Gp}$ *(resp.* $F : \mathbf{J} \to \mathbf{Set}$*), where* $\mathbf{J}$ *is the poset category of an inverse system. Given such an inverse system* F*, the limit of* F *(if it exists) is called the* inverse limit *of the objects* $(F(j))_{j \in \operatorname{ob}\mathbf{J}}$.

In other words, an inverse system of groups (resp. sets) indexed by an inverse system $(J, \preccurlyeq)$ *consists of groups (resp. sets)* $(G_j)_{j \in J}$ *and transformation maps* $G_i \xrightarrow{\phi_{ij}} G_j$ *for all* $i \preccurlyeq j$ *such that* $\phi_{ii} = \mathrm{id}_{G_i}$ *and* $\phi_{jk} \circ \phi_{ij} = \phi_{ik}$ *for all* $i \preccurlyeq j \preccurlyeq k$*. The inverse limit of the system* $(G_j)_{j \in J}$ *is a group (resp. a set)* $\varprojlim_{j \in J} G_j$ *together with projection maps* $p_j : \varprojlim_{j \in J} G_j \to G_j$ *such that the diagram*



commutes for all $i \preccurlyeq j$*, and that is universal among such cones.*

Proposition 1.12. *Let* $(G_j)_{j \in J}$ *be an inverse system of groups or sets. Then* $\varprojlim_{j \in J} G_j$ *exists, and is given by*

$$\varprojlim_{j \in J} G_j = \left\{ (g_j)_{j \in J} \in \prod_{j \in J} G_j,\ \forall i \preccurlyeq j,\ \phi_{ij}(g_i) = g_j \right\}.$$

Proof. Let L be the above set; if the $(G_j)_{j \in J}$ are groups, then L is a subgroup of $\prod_{j \in J} G_j$ because the maps $\left(G_i \xrightarrow{\phi_{ij}} G_j\right)_{i \preccurlyeq j}$ are homomorphisms. Define $p_j : L \to G_j$ to be the restriction of the projection $\prod_{j \in J} G_j \to G_j$; then $\phi_{ij} \circ p_i = p_j$ holds for all $i \preccurlyeq j$ by choice of L. Now let $\left(Z \xrightarrow{q_i} G_j\right)_{j \in J}$ be a cone over $(G_j)_{j \in J}$. There is a unique map $f : Z \to \prod_{j \in J} G_j$ such that $p_j \circ f = q_j$, and we have $f(Z) \subseteq L$ because of the relations $\phi_{ij} \circ q_i = q_j$. □

Remark 1.13. *The proof of Proposition 1.12 actually shows that* **Gp** *and* **Set** *have all limits.*

Definition 1.14 (Profinite group)**.** *A* profinite group *is an inverse limit (in the category of all groups) of an inverse system of finite groups.*

Example 1.15. *The group* $\mathbb{Z}_p$ *of* p-adic integers *is profinite:*

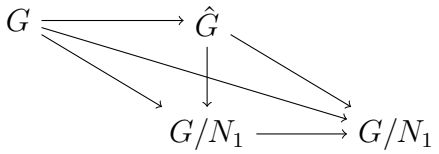
$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}.$$

Definition 1.16 (Profinite completion)**.** *Let* G *be a group. Denote by* $\mathbf{N}$ *the poset (viewed as a category) of finite index normal subgroups of* G*, ordered by inclusion. Then the assignement*

$$(N_1 \subseteq N_2) \longmapsto (G/N_1 \twoheadrightarrow G/N_2)$$

is a diagram $\mathbf{N} \to \mathbf{Gp}$*.*

The limit of this diagram is a group $\hat{G}$ *called the* profinite completion *of* G*. It is equipped with homomorphisms* $\hat{G} \to G/N$ *for all* $N \in \mathbf{N}$*, called* projection maps*. Moreover, the projections* $G \to G/N$ *induce a unique map* $G \to \hat{G}$*, called the* canonical map*, as in the following commutative diagram:*



The profinite completion of a group is a profinite group.

1.3 Topology on a profinite group or set

Definition 1.17 (Topology on a profinite group or set)**.** *Let* $(G_j)_{j\in J}$ *be an inverse system of finite groups or sets. For* $j \in J$*, endow* G_j *with the discrete topology. Then* $\prod_{j\in J} G_j$ *is endowed with the product topology and* $\varprojlim_{j\in J} G_j \subseteq \prod_{j\in J} G_j$ *is endowed with the subspace topology.*

By Tychonoff's Theorem, $\prod_{j\in J} G_j$ *is Hausdorff compact, so* $\varprojlim_{j\in J} G_j$ *is Hausdorff compact because it is closed in* $\prod_{j\in J} G_j$ *(according to the description given by Proposition 1.12).*

Proposition 1.18. *If* $(X_j)_{j\in J}$ *is an inverse system of nonempty finite sets, then*

$$\varprojlim_{j\in J} X_j \neq \varnothing.$$

Proof. Given a finite subset $I \subseteq J$, consider the set

$$Y_I = \left\{ (x_j)_{j\in J} \in \prod_{j\in J} X_j,\ \forall i,j \in I,\ i \preccurlyeq j \Rightarrow \phi_{ij}(g_i) = g_j \right\}.$$

Then Y_I is closed in $\prod_{j\in J} X_j$, and

$$\bigcap_{\substack{I\subseteq J\\ \text{finite}}} Y_I = \varprojlim_{j\in J} X_j.$$

We claim that $Y_I \neq \varnothing$. Indeed, by definition of an inverse system, there exists $k \in J$ such that $k \preccurlyeq i$ for all $i \in I$. Since $X_k \neq \varnothing$ by assumption, we may choose $x_k \in X_k$. Define $(x_j)_{j\in J} \in \prod_{j\in J} X_j$ by $x_j = \phi_{kj}(x_k)$ if $j \in I$, or x_j is any element of X_j if $j \notin I$. Hence, $(x_j)_{j\in J} \in Y_I$, so $Y_I \neq \varnothing$. It follows that if $I_1, \ldots, I_n$ are finite subsets of J, then

$$\bigcap_{\ell=1}^{n} Y_{I_\ell} = Y_{I_1\cup\cdots\cup I_n} \neq \varnothing.$$

Hence $(Y_I)_{\substack{I\subseteq J\\ \text{finite}}}$ is a collection of closed subsets of the compact space $\prod_{j\in J} X_j$ such that any intersection of a finite number of those subsets is nonempty. It follows that $\varprojlim_{j\in J} X_j = \bigcap_{\substack{I\subseteq J\\ \text{finite}}} Y_I \neq \varnothing$. □

Proposition 1.19. *If $(X_i)_{i\in I}$ is a countable family of metrisable spaces, then $\prod_{i\in I} X_i$ is metrisable.*

Proposition 1.20. *If Γ is a finitely generated group, then it has only countably many finite index subgroups.*

Proof. For $n \geqslant 1$, let $\mathcal{A}_n$ be the set of homomorphisms $\Gamma \to \mathfrak{S}_n$; the set $\mathcal{A}_n$ is finite because Γ is finitely generated. Let $\mathcal{A} = \coprod_{n\in\mathbb{N}} \mathcal{A}_n$. If $\mathcal{H}$ is the set of finite index subgroups of Γ, there is a map $\mathcal{A} \to \mathcal{H}$ given by

$$\left(\Gamma \xrightarrow{\phi} \mathfrak{S}_n\right) \in \mathcal{A} \longmapsto \mathrm{Stab}_\phi(1) = \{g \in \Gamma,\ \phi(g)(1) = 1\} \in \mathcal{H}.$$

Now this map is surjective: if H is a subgroup of Γ of index n, then H is the stabiliser of $[1]$ under the (left) action of Γ on Γ/H. Therefore, we have a surjection $\mathcal{A} \twoheadrightarrow \mathcal{H}$, so $\mathcal{H}$ is countable because $\mathcal{A}$ is. □

Corollary 1.21. *If Γ is a finitely generated group, then its profinite completion $\hat{\Gamma}$ is metrisable.*

Proposition 1.22. *Let G be a profinite group. Then the multiplication map $G \times G \to G$ and the inversion $G \to G$ are continuous.*

In other words, G is a topological group*.*

Definition 1.23 (Topological isomorphism)**.** *If G and H are two topological groups, a* topological isomorphism *$G \to H$ is a group isomorphism which is also a homeomorphism.*

Remark 1.24. *From now on, except otherwise specified, all morphisms between profinite groups will be assumed to be continuous.*

Lemma 1.25. *A continuous isomorphism of profinite groups is a homeomorphism and hence a topological isomorphism.*

Proof. Profinite groups are Hausdorff compact, and it is a general fact that any continuous bijection $f : X \to Y$ with X Hausdorff compact is a homeomorphism. □

Lemma 1.26. *Let H be a topological group and let $G = \varprojlim_{j\in J} G_j$ be an inverse limit of finite groups, with projections $p_j : G \to G_j$. Given a group homomorphism $f : H \to G$, the following assertions are equivalent:*

(i) *$f : H \to G$ is continuous.*

(ii) *$p_j \circ f : H \to G_j$ is continuous for all $j \in J$.*

(iii) *$\mathrm{Ker}\,(p_j \circ f)$ is open in H for all $j \in J$.*

Proof. (i) ⇔ (ii) By definition of the product topology.

(ii) ⇒ (iii) If $f_j = p_j \circ f$ is continuous, then $\mathrm{Ker}\, f_j = f_j^{-1}(\{1\})$ is open in H because $\{1\}$ is open in G_j.

(iii) ⇒ (ii) If $\mathrm{Ker}\, f_j$ is open, then for all $g_j \in G_j$, either $f_j^{-1}(\{g_j\}) = \varnothing$ (which is open), or there exists $h \in f_j^{-1}(\{g_j\})$, in which case $f_j^{-1}(\{g_j\}) = h \cdot \mathrm{Ker}\, f_j$ is open. Therefore $f_j^{-1}(U_j)$ is open in H for all $U_j \subseteq G_j$, so that f_j is continuous. □

Proposition 1.27. *Let G be a compact topological group. Then a subgroup $H \leqslant G$ is open* iff *it is closed and of finite index.*

Proposition 1.28. *Let $G = \varprojlim_{j\in J} G_j$ be an inverse limit of finite groups, with projections $p_j : G \to G_j$. Then the open subgroups $H_j = \mathrm{Ker}\, p_j$ form a basis of open neighbourhoods at the identity.*

Proof. Let $V \ni 1$ be open. By definition of the product topology, V contains an open set of the form

$$1 \in p_{j_1}^{-1}(X_{j_1}) \cap \cdots \cap p_{j_m}^{-1}(X_{j_m}) \subseteq V,$$

where $j_1, \ldots, j_m \in J$ and $X_{j_i} \subseteq G_{j_i}$. It follows that $1 = p_{j_i}(1) \in X_{j_i}$ for all i, so we may assume without loss of generality that $X_{j_i} = \{1\}$, so that:

$$1 \in \operatorname{Ker} p_{j_1} \cap \cdots \cap \operatorname{Ker} p_{j_m} \subseteq V.$$

Now there exists $k \in J$ such that $k \preccurlyeq j_1, \ldots, j_m$. Since $p_{j_i} = \phi_{j_i k} \circ p_k$, we have

$$1 \in \operatorname{Ker} p_k \subseteq \operatorname{Ker} p_{j_1} \cap \cdots \cap \operatorname{Ker} p_{j_m} \subseteq V. \qquad \square$$

Corollary 1.29. *Let $G = \varprojlim_{j \in J} G_j$ be an inverse limit of finite groups, with projections $p_j : G \to G_j$.*

(i) $\left\{ p_j^{-1}(g_j),\ j \in J,\ g_j \in G_j \right\}$ *is a basis of open subsets of G.*

(ii) *A subset $S \subseteq G$ is dense* iff $p_j(S) = p_j(G)$ *for all $j \in J$.*

Proof. (i) If U is an open subset of G and $g \in U$, then $g^{-1}U$ is an open neighbourhood of 1, so Proposition 1.28 implies the existence of $j \in J$ such that $\operatorname{Ker} p_j \subseteq g^{-1}U$. It follows that

$$g \in p_j^{-1}(p_j(g)) = g \operatorname{Ker} p_j \subseteq U.$$

(ii)($\Leftarrow$) Assume that $p_j(S) = p_j(G)$ for all $j \in J$. If $U \subseteq G$ is open and nonempty, then by (i), we may assume without loss of generality that $U = p_j^{-1}(g_j)$ for some $j \in J$ and $g_j \in G_j$. Hence $g_j \in p_j(G) = p_j(S)$, so $S \cap U \neq \varnothing$.

(ii)($\Rightarrow$) Assume that there exists $g_j \in p_j(G) \backslash p_j(S)$ for some $j \in J$. If $U = p_j^{-1}(g_j)$, then U is open and nonempty, but $U \cap S = \varnothing$, so S is not dense. $\square$

Example 1.30. *If Γ is a group, $\hat{\Gamma}$ is its profinite completion and $\iota : \Gamma \to \hat{\Gamma}$ is the canonical map, then $\iota(\Gamma)$ is dense in $\hat{\Gamma}$.*

Proof. For all normal subgroup of finite index $N \trianglelefteq_{fi} G$, we have $p_N(\iota(\Gamma)) = \Gamma/N = p_N\left(\hat{\Gamma}\right)$, so Corollary 1.29.(ii) implies the result. $\square$

1.4 Change of inverse system

Definition 1.31 (Surjective inverse system)**.** *An inverse system $(G_j)_{j \in J}$ of groups or sets is said to be* surjective *if the transition maps $\phi_{ij} : G_i \to G_j$ are all surjective.*

Proposition 1.32. *Let $(X_j)_{j \in J}$ be a surjective inverse system of nonempty finite sets. Then all the projection maps $p_j : \varprojlim_{j \in J} X_j \to X_j$ are surjective.*

Proposition 1.33. *Let $(X_j)_{j \in J}$ be an inverse system of finite sets. Then there exists a surjective inverse system of finite sets with the same inverse limit.*

Proof. Recall that

$$\varprojlim_{j \in J} X_j = \left\{ (x_j)_{j \in J} \in \prod_{j \in J} X_j,\ \forall i \preccurlyeq j,\ \phi_{ij}(x_i) = x_j \right\}.$$

Define $Y_j = \operatorname{Im} p_j \subseteq X_j$ for all $j \in J$. Then $(Y_j)_{j \in J}$, together with the transition maps $\left(\phi_{ij_{|Y_i}}\right)_{i \preccurlyeq j}$, forms an inverse system, which is surjective. Finally, $\varprojlim_{j \in J} Y_j = \varprojlim_{j \in J} X_j$. $\square$

Definition 1.34 (Cofinal subsystem)**.** *If J is an inverse system, then a subset $I \subseteq J$ is called* cofinal *if*

$$\forall j \in J,\ \exists i \in I,\ i \preccurlyeq j.$$

This implies that I is also an inverse system.

Example 1.35. *In the inverse system $\{n\mathbb{Z}\}_{n\geqslant 1}$ of finite index subgroups of $\mathbb{Z}$ ordered by inclusion, one cofinal system is $\{(m!)\mathbb{Z}\}_{m\geqslant 0}$, which has the advantage of being linearly ordered.*

Definition 1.36 (Linearly ordered system)**.** *An inverse system J is* linearly ordered *if there is a bijection $f : J \to \mathbb{N}$ such that $i \preccurlyeq j$ if and only if $f(i) \geqslant f(j)$.*

Note that this is equivalent to J being isomorphic to the inverse system $\underline{\mathbb{N}}$ on $\mathbb{N}$ with the wrong-way ordering $\preccurlyeq$ *defined by $i \preccurlyeq j$ if and only if $i \geqslant j$.*

Proposition 1.37. *Let J be a countable inverse system. Then J has a linearly ordered cofinal subsystem.*

Example 1.38. (i) *If J is an inverse system and $k \in J$, then $J_{\preccurlyeq k} = \{j \in J,\ j \preccurlyeq k\}$ is a* principal *cofinal subsystem.*

(ii) *A cofinal subsystem of $\underline{\mathbb{N}}$ is the same as an increasing sequence of integers.*

Proposition 1.39. *Let $(G_j)_{j\in J}$ be an inverse system of groups or sets. Let $I \subseteq J$ be a cofinal subsystem. Then there is a topological isomorphism (or homeomorphism)*

$$\varprojlim_{j\in J} G_j \cong \varprojlim_{i\in I} G_i.$$

Proof. We set $G = \varprojlim_{j\in J} G_j$ and $H = \varprojlim_{i\in I} G_i$. The projection map $\prod_{j\in J} G_j \to \prod_{i\in I} G_i$ is a continuous homomorphism and restricts to a map $f : G \to H$. It remains to show that f is bijective.

- *Injectivity.* Let $g = (g_j)_{j\in J} \in G$ such that $f(g) = 1$. Then for all $i \in I$, $g_i = p_i(g) = 1$. Now, if $j \in J$, then there exists $i \in I$ such that $i \preccurlyeq j$, and therefore $g_j = \phi_{ij}(g_i) = 1$. Hence $g = 1$.
- *Surjectivity.* Let $(g_i)_{i\in I} \in H$. For $j \in J\backslash I$, there exists $i \in I$ such that $i \preccurlyeq j$; define $g_j = \phi_{ij}(g_i)$. Show that $(g_j)_{j\in J}$ is well-defined (independently of the choice of i) and that it is an element of G. □

2 Profinite groups

2.1 The p-adic integers

Definition 2.1 (p-adic integers)**.** *Let p be a prime. Consider the inverse system*

$$\cdots \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z} \twoheadrightarrow \cdots \twoheadrightarrow \mathbb{Z}/p^2\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z} \twoheadrightarrow 1$$

of finite rings. Its inverse limit is the profinite ring

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}.$$

*An element $\alpha \in \mathbb{Z}_p$ (a p-*adic integer*) is a sequence $(a_n)_{n\in\mathbb{N}}$ of elements of $\mathbb{Z}/p^n\mathbb{Z}$ such that $a_n \equiv a_m \mod p^m$ if $n \geqslant m$. The element $a_n = p_n(\alpha)$ will also be denoted by $\alpha \mod p^n$.*

Addition and multiplication are done component-wise.

Definition 2.2 (Pro-p group)**.** *Let p be a prime. A* pro-p group *is an inverse limit of finite p-groups, i.e. finite groups whose order is a power of p.*

The pro-p completion *of a group Γ is*

$$\hat{\Gamma}_{(p)} = \varprojlim_{\substack{N\trianglelefteq\Gamma \\ \Gamma/N \text{ pro-}p}} \Gamma/N.$$

Example 2.3. $\mathbb{Z}_p = \hat{\mathbb{Z}}_{(p)}$.

Remark 2.4. *The projections $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$ induce a map $\iota : \mathbb{Z} \to \mathbb{Z}_p$. This map ι is injective, and we will therefore view $\mathbb{Z}$ as a subring of $\mathbb{Z}_p$.*

Remark 2.5. *The usual profinite topology on $\mathbb{Z}_p$ is induced by the metric d defined as follows: if $\alpha \neq \beta \in \mathbb{Z}_p$, let $n = \min\{m \in \mathbb{N},\ \alpha \not\equiv \beta \mod p^m\}$ and set*

$$d(\alpha, \beta) = p^{-n}.$$

The restriction of this metric to $\mathbb{Z}$ is the p-adic metric *on $\mathbb{Z}$.*

Given $r > 0$, the open ball $B(0, r)$ with centre 0 and radius r in $\mathbb{Z}_p$ is:

$$B(0, r) = \operatorname{Ker}\left(\mathbb{Z}_p \to \mathbb{Z}/p^m\mathbb{Z}\right),$$

with $m = \left\lceil -\log_p r \right\rceil$. Note that this is one of the usual open neighbourhoods of 0 of Proposition 1.28, and that it is also closed.

Proposition 2.6. *The additive group $\mathbb{Z}_p$ is abelian and torsion-free.*

Proof. $\mathbb{Z}_p$ is abelian as a limit of abelian groups. To prove that it is torsion-free, let $\alpha = (a_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p \neq 0$ and assume for contradiction that there exists $m \geqslant 1$ such that $m\alpha = 0$. Write $m = p^r s$ with $r \geqslant 0$ and $s \geqslant 1$ not divisible by p. Since $\alpha \neq 0$, there exists $n \geqslant 0$ such that

$$\alpha \not\equiv 0 \mod p^n.$$

In other words, $p^n \nmid a_n$. But $m\alpha = 0$ implies that $p^{n+r} \mid p^r s a_{n+r} = m a_{n+r}$, so $p^n \mid a_{n+r}$. This is a contradiction because $a_n \equiv a_{n+r} \mod p^n$. □

Proposition 2.7. *The ring $\mathbb{Z}_p$ is an integral domain.*

In particular, it has a field of fraction, which will be denoted by $\mathbb{Q}_p \supseteq \mathbb{Z}_p$.

2.2 The profinite integers

Theorem 2.8 (Chinese Remainder Theorem)**.** *There is an isomorphism of topological groups and of rings,*

$$\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p.$$

Proof. The continuous homomorphisms $\left(\hat{\mathbb{Z}} \to \mathbb{Z}/p^n\mathbb{Z}\right)_{n\geqslant 0}$ are compatible with the transition maps $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, so they induce a homomorphism $\hat{\mathbb{Z}} \to \mathbb{Z}_p$ such that the diagram

$$\begin{array}{ccc} \hat{\mathbb{Z}} & \longrightarrow & \mathbb{Z}_p \\ & \searrow \quad \swarrow & \\ & \mathbb{Z}/p^n\mathbb{Z} & \end{array}$$

commutes for all $n \geqslant 0$. This map is continuous by Lemma 1.26. Now the maps $\left(\hat{\mathbb{Z}} \to \mathbb{Z}_p\right)_{p \text{ prime}}$ induce a continuous homomorphism

$$f : \hat{\mathbb{Z}} \longrightarrow \prod_{p \text{ prime}} \mathbb{Z}_p.$$

By Lemma 1.25, it suffices to show that f is bijective.

Surjectivity. Since $\hat{\mathbb{Z}}$ is compact, $\operatorname{Im} f$ is closed in $\prod_p \mathbb{Z}_p$, so it suffices to show that $\operatorname{Im} f$ is dense in $\prod_p \mathbb{Z}_p$, so it actually suffices to prove that $\operatorname{Im} f$ intersects all basic open sets of $\prod_p \mathbb{Z}_p$ nontrivially. But those basic open sets can be written as

$$U^{(x_1,\ldots,x_r)}_{p_1,\ldots,p_r} = \prod_{i=1}^{r} (x_i + p_i^{n_i}\mathbb{Z}_{p_i}) \times \prod_{p\neq p_1,\ldots,p_r} \mathbb{Z}_p = \phi^{-1}(x_1, \ldots, x_r),$$

where ϕ is the projection $\prod_p \mathbb{Z}_p \longrightarrow \prod_{i=1}^r (\mathbb{Z}/p_i^{n_i}\mathbb{Z})$. Now, if $m = p_1^{n_1} \cdots p_r^{n_r}$, we have a commutative diagram:

$$\begin{array}{ccccc} \mathbb{Z} & \longrightarrow & \hat{\mathbb{Z}} & \xrightarrow{f} & \prod_p \mathbb{Z}_p \\ & \searrow & \downarrow & & \downarrow \phi \\ & & \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\cong} & \prod_{i=1}^r \mathbb{Z}/p_i^{n_i}\mathbb{Z} \end{array}$$

The diagram shows that $(x_1, \ldots, x_r) \in \operatorname{Im}(\phi \circ f)$, so $\operatorname{Im} f \cap \phi^{-1}(x_1, \ldots, x_r) \neq \varnothing$.

Injectivity. Let $g \in \hat{\mathbb{Z}} \backslash \{0\}$. Then there exists $m \geqslant 1$ such that the image of g in $\mathbb{Z}/m\mathbb{Z}$ is nonzero. Writing $m = p_1^{n_1} \cdots p_r^{n_r}$ and considering the above diagram, we have $\phi \circ f(g) \neq 0$, so $f(g) \neq 0$. □

Corollary 2.9. (i) *The additive group $\hat{\mathbb{Z}}$ is abelian and torsion-free.*

(ii) *The ring $\hat{\mathbb{Z}}$ does have zero-divisors.*

2.3 Profinite matrix groups

Notation 2.10. *Let R be a commutative ring with unity.*

- $\operatorname{Mat}_{n,n}(R)$ *is the ring of $n \times n$ matrices with entries in R,*
- $GL_nR = \{A \in \operatorname{Mat}_{n,n}(R),\ \det A \in R^\times\}$,
- $SL_nR = \{A \in \operatorname{Mat}_{n,n}(R),\ \det A = 1\}$.

Proposition 2.11. (i) $\mathbb{Z}_p^\times = \varprojlim_{m \geqslant 0} (\mathbb{Z}/p^m\mathbb{Z})^\times$ *and* $\hat{\mathbb{Z}}^\times = \varprojlim_{m \geqslant 1} (\mathbb{Z}/m\mathbb{Z})^\times$.

(ii) $\mathbb{Z}_p^\times$ *is closed and open in* $\mathbb{Z}_p$.

(iii) $\hat{\mathbb{Z}}^\times$ *is closed but not open in* $\hat{\mathbb{Z}}$.

Proposition 2.12. *Consider the rings* $\operatorname{Mat}_{n,n}(\mathbb{Z}_p)$ *and* $\operatorname{Mat}_{n,n}\left(\hat{\mathbb{Z}}\right)$.

(i) $\operatorname{Mat}_{n,n}(\mathbb{Z}_p) = \varprojlim_{m \geqslant 0} \operatorname{Mat}_{n,n}(\mathbb{Z}/p^m\mathbb{Z})$ *and* $\operatorname{Mat}_{n,n}\left(\hat{\mathbb{Z}}\right) = \varprojlim_{m \geqslant 1} \operatorname{Mat}_{n,n}(\mathbb{Z}/m\mathbb{Z})$.

(ii) $GL_n\mathbb{Z}_p$ *and* $GL_n\hat{\mathbb{Z}}$ *are groups under multiplication (and similarly for* SL_n*).*

(iii) $GL_n\mathbb{Z}_p = \varprojlim_{m \geqslant 0} GL_n(\mathbb{Z}/p^m\mathbb{Z})$ *and* $GL_n\hat{\mathbb{Z}} = \varprojlim_{m \geqslant 1} GL_n(\mathbb{Z}/m\mathbb{Z})$ *(and similarly for* SL_n*).*

(iv) $GL_n\mathbb{Z}_p$ *and* $SL_n\mathbb{Z}_p$ *are closed in* $\operatorname{Mat}_{n,n}(\mathbb{Z}_p)$ *(and similarly for* $\hat{\mathbb{Z}}$*).*

(v) $GL_n\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} GL_n\mathbb{Z}_p$ *(and similarly for* SL_n*).*

2.4 Subgroups, quotients, and homomorphisms

Remark 2.13. *Non-closed subgroups of profinite groups can behave badly, e.g.* $\mathbb{Z}^{\mathbb{N}} \leqslant \prod_p \mathbb{Z}_p \cong \hat{\mathbb{Z}}$.

Proposition 2.14. *Let* $(G_j)_{j \in J}$ *be an inverse system of finite groups,* $G = \varprojlim_{j \in J} G_j$. *If* $X \subseteq G$ *is a subset, then*

$$\overline{X} = \varprojlim_{j \in J} p_j(X) = \bigcap_{j \in J} p_j^{-1}(p_j(X)).$$

Proof. It is clear (by Proposition 1.12) that $\varprojlim_{j \in J} p_j(X) = \bigcap_{j \in J} p_j^{-1}(p_j(X))$; denote this set by X'. We claim that $X' = \overline{X}$. We have $X \subseteq X'$, and X' is closed, so $\overline{X} \subseteq X'$. Now if $g \in G \backslash \overline{X}$, then since $G \backslash \overline{X}$ is open, there is a basic open set $p_j^{-1}(g_j)$ s.t.

$$g \in p_j^{-1}(g_j) \subseteq G \backslash \overline{X}.$$

Therefore, $X \cap p_j^{-1}(g_j) = \varnothing$, so $g_j \notin p_j(X)$ and $g \notin X'$. Hence $G \backslash \overline{X} \subseteq G \backslash X'$. □

Corollary 2.15. *Let $(G_j)_{j\in J}$ be an inverse system of finite groups, $G = \varprojlim_{j\in J} G_j$. If $X \subseteq G$ is a subset, then*

$$\overline{X} = \bigcap_{\substack{N\trianglelefteq G \\ open}} XN.$$

Proof. Note that $\bigcap_{\substack{N\trianglelefteq G \\ \text{open}}} XN = \bigcap_{j\in J} X \operatorname{Ker} p_j = \bigcap_{j\in J} p_j^{-1}(p_j(X))$ and use Proposition 2.14. □

Corollary 2.16. *Closed subgroups of profinite groups are profinite.*

Proposition 2.17. *Let $(G_j)_{j\in J}$ be a surjective inverse system of finite groups, $G = \varprojlim_{j\in J} G_j$. Let $H \leqslant G$ be a closed subgroup. Then H has finite index (or equivalently by Proposition 1.27, H is open) if and only if there is a cofinal subsystem $I \subseteq J$ such that $([G_i : p_i(H)])_{i\in I}$ is constant. In this case, $[G : H] = [G_i : p_i(H)]$ for all $i \in I$.*

Lemma 2.18 (First Isomorphism Theorem for profinite groups)**.** *If $f : G \to Q$ is a surjective continuous homomorphism between profinite groups, then there is a topological isomorphism $\overline{f} : G/\operatorname{Ker} f \xrightarrow{\cong} Q$ such that the following diagram commutes:*

$$\begin{array}{ccc} G & & \\ \downarrow & \searrow^{f} & \\ G/\operatorname{Ker} f & \xrightarrow[\overline{f}]{} & Q \end{array}$$

Proof. The first isomorphism theorem for groups tells us that there exists a group isomorphism $\overline{f}$ making the above diagram commute. Now $\overline{f}$ is continuous as the map on the quotient induced by a continuous map; and it is a homeomorphism by Lemma 1.25. □

Proposition 2.19. *Let G be a profinite group and $N \trianglelefteq G$ a closed normal subgroup. Then G/N, equipped with the quotient topology, is a profinite group.*

Proof. Let $(G_j)_{j\in J}$ be a surjective inverse system such that $G = \varprojlim_{j\in J} G_j$. Define $N_j = p_j(N)$. By surjectivity, $N_j \trianglelefteq G_j$, so we may define $Q_j = G_j/N_j$. Since $\phi_{ij}(N_i) = N_j$, there are maps $\psi_{ij} : Q_i \to Q_j$ induced by $\phi_{ij} : G_i \to G_j$. Now $(Q_j)_{j\in J}$ is an inverse system; we let $Q = \varprojlim_{j\in J} Q_j$, a profinite group. There is a continuous homomorphism $\prod_{j\in J} G_j \to \prod_{j\in J} Q_j$ restricting to $f : G \to Q$. Then, using Proposition 2.14 and the fact that N is closed,

$$\operatorname{Ker} f = \bigcap_{j\in J} p_j^{-1}(N_j) = N.$$

By Lemma 2.18, $G/N \cong Q \cong \varprojlim_{j\in J} Q_j$. □

Corollary 2.20. *Continuous quotients of profinite groups are profinite (with the quotient topology).*

Definition 2.21 (Morphism of inverse systems)**.** *Let $(G_j)_{j\in J}$ and $(H_j)_{j\in J}$ be inverse systems of finite groups indexed over the same poset J. Denote the transition maps by ϕ_{ij}^G and ϕ_{ij}^H respectively. A* morphism of inverse systems *is a family $(f_j : G_j \to H_j)_{j\in J}$ of group homomorphisms such that, for all $i \preccurlyeq j$, the following diagram commutes:*

$$\begin{array}{ccc} G_i & \xrightarrow{f_i} & H_i \\ {\scriptstyle \phi_{ij}^G}\downarrow & & \downarrow{\scriptstyle \phi_{ij}^H} \\ G_j & \xrightarrow{f_j} & H_j \end{array}$$

Proposition 2.22. *Given a morphism between two inverse systems $(G_j)_{j\in J}$ and $(H_j)_{j\in J}$ of finite groups indexed over the same poset J, there is a unique continuous homomorphim $f : G \to H$ such that the following diagram commutes for all $j \in J$:*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle p_j^G}\downarrow & & \downarrow{\scriptstyle p_j^H} \\ G_j & \xrightarrow{f_j} & H_j \end{array}$$

Proof. The maps $\left(f_j \circ p_j^G\right)_{j\in G}$ form a cone over $(H_j)_{j\in J}$. □

Proposition 2.23. *Let $(G_j)_{j\in J}$ and $(H_i)_{i\in I}$ be two inverse systems of finite groups (with I, J countable), $G = \varprojlim_{j\in J} G_j$ and $H = \varprojlim_{i\in I} H_i$. If $f : G \to H$ is a continuous homomorphism, then there are cofinal subsystems $J' \subseteq J$ and $I' \subseteq I$, an order-preserving bijection $\alpha : J' \xrightarrow{\cong} I'$, and a morphism $\left(f_{j'} : G_{j'} \to H_{\alpha(j')}\right)_{j'\in J}$ which induces f as in Proposition 2.22.*

Proof. By Propositions 1.33 and 1.37, we may assume that J and I are linearly ordered, that they are in fact both $\mathbb{N}$ with the wrong-way ordering, and that $(G_j)_{j\in J}$ and $(H_i)_{i\in I}$ are surjective inverse systems. We set $I' = I$. We then construct an increasing sequence $(k_n)_{n\in\mathbb{N}}$ of natural numbers (so that $J' = \{k_n,\ n \in \mathbb{N}\}$ will be cofinal in J) as follows: we have a continuous map $G \xrightarrow{f} H \xrightarrow{p_n^H} H_n$, so its kernel is open and hence it contains a basic open subgroup $\operatorname{Ker} p_{k_n}^G$ of G, i.e.

$$\operatorname{Ker} p_{k_n}^G \subseteq \operatorname{Ker}\left(p_n^H \circ f\right).$$

It follows that there is a quotient map $f_n : G_{k_n} \to H_n$ induced by $f : G \to H$. By increasing k_n, we may assume without loss of generality that $k_n > k_{n-1}$, and hence we have a morphism of inverse systems. □

2.5 Generators of profinite groups

Definition 2.24 (Topological generating set)**.** *Let G be a topological group. Given $S \subseteq G$, the* closed subgroup generated by *S is the smallest closed subgroup of G which contains S. Since the closure of a subgroup is a subgroup, this is equal to $\overline{\langle S\rangle}$.*

We say that S is a topological generating set *for G if $\overline{\langle S\rangle} = G$. We say that G is* topologically finitely generated *if it has a finite topological generating set.*

Proposition 2.25. *Let G be a compact topological group and let $U \leqslant G$ be an open subgroup. Then U is topologically finitely generated if and only if G is.*

Proof. Note first that U has finite index in G by Proposition 1.27.

($\Rightarrow$) Assume that $U = \overline{\langle S\rangle}$ for some finite set S. Let T be a (finite) set of coset representatives for U in G. Then $S \cup T$ is a (finite) topological generating set for G.

($\Leftarrow$) Assume that $G = \overline{\langle S\rangle}$ for some finite set S. Note that $U \cap \langle S\rangle$ has finite index in $\langle S\rangle$, so it is generated by some finite set $T \subseteq \langle S\rangle$. Since U is open and $\langle S\rangle$ is dense in G, $\langle T\rangle = U \cap \langle S\rangle$ is dense in U. □

Proposition 2.26. *Let $G = \varprojlim_{j\in J} G_j$ be an inverse limit of finite groups. Then a subset $S \subseteq G$ is a topological generating set if and only if $p_j(S)$ generates $p_j(G)$ for all $j \in J$.*

Proof. By Corollary 1.29, $\langle S\rangle$ is dense if and only if $\langle p_j(S)\rangle = p_j\left(\langle S\rangle\right) = p_j(G)$ for all $j \in J$. □

Proposition 2.27. *Let $\alpha \in \mathbb{Z}_p$. The following assertions are equivalent:*

(i) *α topologically generates $\mathbb{Z}_p$.*

(ii) $\alpha \not\equiv 0 \mod p$.

(iii) *α is invertible in the ring $\mathbb{Z}_p$.*

The set of $\alpha \in \mathbb{Z}_p$ satisfying the above conditions will be denoted by $\mathbb{Z}_p^\times$.

Moreover, for all $n \in \mathbb{N}$ and for all $a_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, there exists $\alpha \in \mathbb{Z}_p^\times$ such that $\alpha \equiv a_n \mod p^n$.

Proof. (i) $\Rightarrow$ (iii) If α is a topological generator of $\mathbb{Z}_p$, consider the map $f_\alpha : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $x \mapsto \alpha x$. Then $f_\alpha(\mathbb{Z}_p)$ is closed (because f_α is continuous and $\mathbb{Z}_p$ is compact), and contains $\langle\alpha\rangle$, so it contains $\overline{\langle\alpha\rangle} = \mathbb{Z}_p$. In particular, $1 \in f_\alpha(\mathbb{Z}_p)$, i.e. α is invertible.

(iii) $\Rightarrow$ (ii) If α is invertible, then there exists $\beta \in \mathbb{Z}_p$ such that $\alpha\beta = 1$. Therefore, $\alpha\beta \equiv 1 \mod p$, so $\alpha \not\equiv 0 \mod p$ because $\mathbb{Z}/p\mathbb{Z}$ is an integral domain.

(ii) $\Rightarrow$ (i) Write $\alpha = (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$. If $\alpha \not\equiv 0 \mod p$, then for all n, $a_n \not\equiv 0 \mod p$, so a_n generates $\mathbb{Z}/p^n\mathbb{Z}$. By Proposition 2.26, α topologically generates $\mathbb{Z}_p$. □

Proposition 2.28. (i) *An element $\alpha \in \hat{\mathbb{Z}}$ is invertible if and only if $\alpha \not\equiv 0 \mod p$ for all prime numbers p.*

(ii) *$\hat{\mathbb{Z}}^\times$ is a closed subset of $\hat{\mathbb{Z}}$.*

(iii) *For all $n \in \mathbb{N}$ and for all $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, there exists $\kappa \in \hat{\mathbb{Z}}^\times$ such that $\kappa \equiv k \mod n$.*

Proof. Use the Chinese Remainder Theorem (Theorem 2.8). □

Lemma 2.29 (Gaschütz's Lemma for finite groups)**.** *Let $f : G \twoheadrightarrow H$ be a surjective homomorphism of finite groups. Assume that G has a generating set of size d. Then for any generating set $\{z_1, \dots, z_d\}$ of H, there is a generating set $\{x_1, \dots, x_d\}$ of G such that $f(x_i) = z_i$.*

Proof. We shall say that a vector $\underline{x} = (x_1, \dots, x_d) \in G^d$ generates G if $\langle\underline{x}\rangle = \langle x_1, \dots, x_d\rangle = G$. We also extend f to a map $f : G^d \to H^d$ defined by $f(x_1, \dots, x_d) = (f(x_1), \dots, f(x_d))$. Given $\underline{y} \in H^d$ a generating vector for H, we consider

$$N_G\left(\underline{y}\right) = \left|\left\{\underline{x} \in G^d,\ G = \langle\underline{x}\rangle \text{ and } f(\underline{x}) = \underline{y}\right\}\right|.$$

We claim that $N_G\left(\underline{y}\right)$ does not depend on $\underline{y}$. If this is true, then we note that G has a generating vector $\underline{x}'$, so $N_G(f(\underline{x}')) \geqslant 1$ and therefore $N_G\left(\underline{y}\right) \geqslant 1$ for any generating vector $\underline{y}$ for H.

Now we prove the claim by induction on $|G|$. We consider a generating vector $\underline{y}$ for H. We denote by $\mathcal{C}$ the set of proper subgroups of G generated by at most d elements. Given a (not necessarily generating) vector $\underline{x} \in G^d$ such that $f(\underline{x}) = \underline{y}$, we have $\langle\underline{x}\rangle = G$ or $\langle\underline{x}\rangle \in \mathcal{C}$. Therefore,

$$|\operatorname{Ker} f|^d = \left|\left\{\underline{x} \in G^d,\ f(\underline{x}) = \underline{y}\right\}\right| = N_G\left(\underline{y}\right) + \sum_{C\in\mathcal{C}} N_C\left(\underline{y}\right).$$

But $|\operatorname{Ker} f|^d$ does not depend on $\underline{y}$, $N_C\left(\underline{y}\right)$ does not depend on $\underline{y}$ (because either $f_{|C} : C \to H$ is surjective and we can use induction, or $N_C\left(\underline{y}\right) = 0$), so $N_G\left(\underline{y}\right)$ does not depend on $\underline{y}$. □

Lemma 2.30. *Let G be a profinite group and let $\mathcal{U}$ be a collection of open normal subgroups of G which is a basis of open neighbourhoods at 1. Then*

$$G \cong \varprojlim_{U\in\mathcal{U}} G/U.$$

Proof. The projections $G \twoheadrightarrow G/U$ induce a continuous homomorphism $f : G \twoheadrightarrow \varprojlim_{U\in\mathcal{U}} G/U$, which is surjective by surjectivity of $G \twoheadrightarrow G/U$. The morphism f is also injective because $\mathcal{U}$ is a basis of open neighbourhoods: for all $g \in G\backslash\{1\}$, there exists an open neighbourhood $V \subseteq G$ such that $g \notin V$, and therefore there exists $U \in \mathcal{U}$ such that $U \subseteq V$; hence $g \notin U$. □

Corollary 2.31. *If G is a topologically finitely generated profinite group, then G can be written as an inverse limit of a countable inverse system of finite groups.*

Proof. Apply Lemma 2.30 to the set $\mathcal{U} = \{U_n,\, n \in \mathbb{N}\}$ where U_n is the intersection of all open subgroups of index at most n. □

Theorem 2.32 (Gaschütz's Lemma for profinite groups)**.** *Let $f : G \twoheadrightarrow H$ be a continuous surjective homomorphism of profinite groups. Assume that G has a topological generating set of size d. Then for any topological generating set $\{z_1, \ldots, z_d\}$ for H, there is a topological generating set $\{x_1, \ldots, x_d\}$ for G such that $f(x_i) = z_i$.*

Proof. By Corollary 2.31, we may assume that G and H are inverse limits of countable inverse systems of finite groups. By Proposition 2.23, we may assume without loss of generality that $G = \varprojlim_{j\in J} G_j$ and $H = \varprojlim_{j\in J} H_j$, where $(G_j)_{j\in J}$ and $(H_j)_{j\in J}$ are surjective inverse systems and f is induced by a morphism of inverse systems $(f_j : G_j \to H_j)_{j\in J}$. We now consider

$$X_j = \left\{\underline{x}_j \in G_j^d,\, G_j = \left\langle \underline{x}_j \right\rangle,\, f_j\left(\underline{x}_j\right) = p_j\left(\underline{z}\right)\right\}.$$

Then $(X_j)_{j\in J}$ forms an inverse system of nonempty sets (by Lemma 2.29), so $\varprojlim_{j\in J} X_j \neq \varnothing$ by Proposition 1.18. But

$$\varprojlim_{j\in J} X_j = \left\{\underline{x} \in G^d,\, G = \overline{\langle \underline{x} \rangle},\, f\left(\underline{x}\right) = \underline{z}\right\}.$$ □

3 Profinite completion

3.1 Residual finiteness

Notation 3.1. *Given a group Γ, we denote by $\hat{\Gamma}$ its profinite completion and by $\iota_\Gamma : \Gamma \to \hat{\Gamma}$ the canonical map (we may drop the subscript).*

Definition 3.2 (Residual finiteness)**.** *Let Γ be a group. The following assertions are equivalent:*

(i) *For all $\gamma \in \Gamma\backslash\{1\}$, there exists a normal subgroup $N \trianglelefteq_{fi} \Gamma$ of finite index such that $\gamma \notin N$.*

(ii) *The canonical map $\iota_\Gamma : \Gamma \to \hat{\Gamma}$ is injective.*

We then say that Γ is residually finite*.*

Example 3.3. (i) *Any finite group is residually finite.*

(ii) *$\mathbb{Z}$ is residually finite.*

Proposition 3.4. *A subgroup of a residually finite group is residually finite.*

Proof. Let Γ be residually finite, let $\Delta \leqslant \Gamma$. Given $\delta \in \Delta\backslash\{1\}$, there exists $N \trianglelefteq_{fi} \Gamma$ such that $\delta \notin N$. Hence $N \cap \Delta \trianglelefteq_{fi} \Delta$ and $\delta \notin N \cap \Delta$. □

Proposition 3.5. *Let Γ be a group and $\Delta \leqslant_{fi} \Gamma$ be a subgroup of finite index. Then Γ is residually finite if and only if Δ is.*

Proof. ($\Rightarrow$) This is Proposition 3.4.

($\Leftarrow$) Assume that Δ is residually finite. Let $\gamma \in \Gamma\backslash\{1\}$. If $\gamma \notin \Delta$, take

$$\mathrm{Core}_\Gamma(\Delta) = \bigcap_{g\in\Gamma} g\Delta g^{-1}.$$

Note that the above intersection is finite because it can be taken over a set of coset representatives of Δ in Γ; therefore, $\mathrm{Core}_\Gamma(\Delta) \trianglelefteq_{fi} \Gamma$, and $\gamma \notin \mathrm{Core}_\Gamma(\Delta)$. Now if $\gamma \in \Delta$, there exists $M \trianglelefteq_{fi} \Delta$ such that $\gamma \notin M$ because Δ is residually finite. Then $M \leqslant_{fi} \Gamma$, so we have $\mathrm{Core}_\Gamma(M) \trianglelefteq_{fi} \Gamma$ and $\gamma \notin \mathrm{Core}_\Gamma(M)$. □

Proposition 3.6. *A direct product of residually finite groups is residually finite.*

Corollary 3.7. *Finitely generated abelian groups are residually finite.*

Remark 3.8. *Abelian groups are not all residually finite: for instance, $\mathbb{Q}$ has no nontrivial finite quotient, so $\hat{\mathbb{Q}} = 0$ and the canonical map $\iota_{\mathbb{Q}}$ cannot be injective.*

Proposition 3.9. *$SL_n\mathbb{Z}$ and $GL_n\mathbb{Z}$ are residually finite for all n.*

Proof. If $A \in GL_n\mathbb{Z}\backslash\{I\}$, take a prime p greater than some nondiagonal entry of A, so that $A \not\mapsto 1$ under $GL_n\mathbb{Z} \longrightarrow GL_n(\mathbb{Z}/p\mathbb{Z})$. Therefore, $GL_n\mathbb{Z}$ is residually finite, and so is $SL_n\mathbb{Z}$ by Proposition 3.4. □

Corollary 3.10. *Finitely generated free groups are residually finite.*

Proof. Finitely generated free groups embed as subgroups of $SL_n\mathbb{Z}$, so this is a consequence of Propositions 3.4 and 3.9. □

Theorem 3.11 (Maltsev's Theorem)**.** *Let K be a field. Then any finitely generated subgroup of GL_nK or PSL_nK is residually finite.*

Corollary 3.12. *Fundamental groups of closed surfaces are residually finite.*

Proof. The fundamental group of a closed surface embeds as a subgroup of $PSL_2\mathbb{R}$. □

3.2 Profinite completion and finite quotients

Lemma 3.13. *Let Γ be a group. Then the open subgroups of $\hat{\Gamma}$ are exactly the subgroups $\overline{\iota_\Gamma(\Delta)}$ for $\Delta \leqslant_{fi} \Gamma$.*

Proof. If $\Delta \leqslant_{fi} \Gamma$, then $\overline{\iota_\Gamma(\Delta)}$ is closed. Let $g_1, \ldots, g_r$ be coset representatives for Δ in Γ. Hence,

$$\hat{\Gamma} = \overline{\iota_\Gamma(\Gamma)} = \overline{\iota_\Gamma\left(\bigcup_{i=1}^{r} g_i\Delta\right)} = \bigcup_{i=1}^{r} \iota_\Gamma(g_i)\,\overline{\iota_\Gamma(\Delta)},$$

so $\overline{\iota_\Gamma(\Delta)}$ has finite index in $\hat{\Gamma}$ and is therefore open (c.f. Proposition 1.27).

Conversely, let $U \leqslant \hat{\Gamma}$ be an open subgroup. Since $\hat{\Gamma} = \overline{\iota_\Gamma(\Gamma)}$, we have $U = \overline{U \cap \iota_\Gamma(\Gamma)}$. Set $\Delta = \iota_\Gamma^{-1}(U) = \iota_\Gamma^{-1}(U \cap \iota_\Gamma(\Gamma))$. Then $\Delta \leqslant_{fi} \Gamma$ and $\iota_\Gamma(\Delta) = U \cap \iota_\Gamma(\Gamma)$. □

Theorem 3.14. *Let G, H be topologically finitely generated profinite groups. If the sets of isomorphism types of continuous finite quotients of G and H are equal, then $G \cong H$.*

Proof. For $n \in \mathbb{N}$, let G_n (resp. H_n) be the intersection of all open subgroups of G (resp. H) of index at most n. Hence G_n is open in G, H_n is open in H, and by Lemma 2.30,

$$G = \varprojlim_{n\in\mathbb{N}} G/G_n \qquad \text{and} \qquad H = \varprojlim_{n\in\mathbb{N}} H/H_n.$$

Since G/G_n is a continuous finite quotient of G, it is also a continuous finite quotient of H by assumption. Therefore, there exists a normal open subgroup $V \trianglelefteq H$ such that $G/G_n \cong H/V$. The intersection of normal subgroups of index at most n of G/G_n is trivial by choice of G_n, so V can be written as an intersection of some open normal subgroups of H of index at most n (by taking preimages in H). It follows that $H_n \leqslant V$. Therefore,

$$|G/G_n| = |H/V| \leqslant |H/H_n|.$$

But by symmetry, the converse inequality also holds, from which we deduce that $H_n = V$ and

$$G/G_n \cong H/H_n.$$

Now we must construct an isomorphism of inverse systems; we let S_n be the (nonempty) set of isomorphisms $G/G_n \xrightarrow{\cong} H/H_n$. Given $f_n \in S_n$, the image by f_n of a subgroup of G/G_n of index at most $n-1$ is a subgroup of H/H_n of index at most $n-1$; therefore $f_n\left(G_{n-1}/G_n\right) = H_{n-1}/H_n$. Because $G/G_{n-1} \cong \frac{G/G_n}{G_{n-1}/G_n}$, the map f_n induces an isomorphism

$$\psi_{n,n-1}(f_n) : G/G_{n-1} \to H/H_{n-1},$$

such that the diagram

$$\begin{array}{ccc} G/G_n & \xrightarrow{\quad f_n \quad} & H/H_n \\ \downarrow & & \downarrow \\ G/G_{n-1} & \xrightarrow{\psi_{n,n-1}(f_n)} & H/H_{n-1} \end{array}$$

commutes. Thus, S_n is an inverse system of nonempty sets (with the transition maps $\psi_{n,n-1}$), so $\varprojlim_{n\in\mathbb{N}} S_n \neq \varnothing$ by Proposition 1.18. Hence there exist $\left(f_n : G/G_n \xrightarrow{\cong} H/H_n\right)_{n\in\mathbb{N}}$ such that the above diagram commutes for all n. By Proposition 2.22, we obtain an isomorphism $\varprojlim_{n\in\mathbb{N}} G/G_n \xrightarrow{\cong} \varprojlim_{n\in\mathbb{N}} H/H_n$. □

Theorem 3.15. *Let Γ, Δ be finitely generated groups. Then $\hat{\Gamma} \cong \hat{\Delta}$ if and only if the sets of isomorphism types of finite quotients of Γ and Δ are equal.*

Proof. Use Theorem 3.14 together with the fact (Lemma 3.13) that continuous finite quotients of $\hat{\Gamma}$ correspond to finite quotients of Γ. □

3.3 Recovering information about a group from its profinite completion

Proposition 3.16. *Let Γ be a residually finite group. Then Γ is abelian if and only if $\hat{\Gamma}$ is.*

Proof. If Γ is abelian, then all its quotients are abelian, so $\hat{\Gamma}$ is abelian. The converse is clear because $\iota_\Gamma : \Gamma \to \hat{\Gamma}$ is injective. □

Proposition 3.17. *Let G, H be residually finite and finitely generated groups.*

(i) *If G is abelian and $\hat{G} \cong \hat{H}$, then $G \cong H$.*

(ii) *If $\hat{G} \cong \hat{H}$, then $G_{\mathrm{ab}} \cong H_{\mathrm{ab}}$, where $G_{\mathrm{ab}} = G/[G,G]$ is the abelianisation of G.*

Proof. (i) Note that, by Proposition 3.16, both G and H are abelian. Since they are finitely generated, we can write

$$G \cong \mathbb{Z}^r \times T \quad \text{and} \quad H \cong \mathbb{Z}^s \times T',$$

with T, T' finite. We now wish to obtain r, s, T, T' from the set of finite quotients of G and H (so that we can use Theorem 3.15). We have

$$r = \max\left\{k,\ \forall n,\ G \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^k\right\} = \max\left\{k,\ \forall n,\ H \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^k\right\} = s.$$

Similarly, T is the largest finite abelian group such that T surjects to $(\mathbb{Z}/n\mathbb{Z})^r \times T$ for all n; therefore $T \cong T'$ and $G \cong H$.

(ii) If $\hat{G} \cong \hat{H}$, then G and H have the same finite abelian quotients, so the abelianisations G_{ab} and H_{ab} have the same finite quotients, i.e. $\widehat{G_{\mathrm{ab}}} \cong \widehat{H_{\mathrm{ab}}}$. Now (i) implies that $G_{\mathrm{ab}} \cong H_{\mathrm{ab}}$. □

Example 3.18 (Baumslag)**.** *Let $\phi : \mathbb{Z}/25\mathbb{Z} \to \mathbb{Z}/25\mathbb{Z}$ be the automorphism given by $t \mapsto 6t$. The order of ϕ is 5. Form the semidirect products*

$$G_1 = \mathbb{Z}/25\mathbb{Z} \rtimes_\phi \mathbb{Z} \qquad \text{and} \qquad G_2 = \mathbb{Z}/25\mathbb{Z} \rtimes_{\phi^2} \mathbb{Z}.$$

Then $G_1 \ncong G_2$ but $\hat{G}_1 \cong \hat{G}_2$.

Remark 3.19. *The following question is open: if G is finitely generated and residually finite and F is a finitely generated free group, does $\hat{F} \cong \hat{G}$ imply $F \cong G$?*

Equivalently: does there exist a finitely generated and residually finite (non-free) group G, and an integer $n \in \mathbb{N}$, such that a finite group Q is a quotient of G if and only if the minimum number of generators of Q is at most n?

Proposition 3.20. *Let F, F' be finitely generated free groups. If $\hat{F} \cong \hat{F}'$, then $F \cong F'$.*

Proof. Let r (resp. s) be the rank of F (resp. F'). If $\hat{F} \cong \hat{F}'$, then by Proposition 3.17, $\mathbb{Z}^r \cong F_{\mathrm{ab}} \cong F'_{\mathrm{ab}} \cong \mathbb{Z}^s$, so $r = s$ and $F \cong F'$. □

Definition 3.21 (Surface groups)**.** *We denote by S_g the fundamental group of the closed genus g surface. In other words,*

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

Remark 3.22. *Note that $(S_g)_{\mathrm{ab}} \cong \mathbb{Z}^{2g} \cong (F_{2g})_{\mathrm{ab}}$, so Proposition 3.17 is not sufficient to distinguish $\hat{S}_g$ from the profinite completion of a free group.*

Proposition 3.23. *Let G be a finitely generated and residually finite group, viewed as a subgroup of its profinite completion $\hat{G}$. Then there is a bijection*

$$\psi : \{H \leqslant G,\ [G : H] < \infty\} \xrightarrow{\cong} \left\{H \leqslant \hat{G},\ H \text{ is open in } \hat{G}\right\},$$

given by $H \mapsto \overline{H}$, and satisfying, for all $K \leqslant_{fi} H \leqslant_{fi} G$,

(i) $[H : K] = \left[\overline{H} : \overline{K}\right]$,

(ii) $K \trianglelefteq H \iff \overline{K} \trianglelefteq \overline{H}$, *and in that case,* $H/K \cong \overline{H}/\overline{K}$,

(iii) $\hat{H} \cong \overline{H}$.

Proof. The map ψ is well-defined and surjective by Lemma 3.13. To prove that ψ is injective, it suffices to show that $\overline{H} \cap G = H$ for all $H \leqslant_{fi} G$. It is clear that $H \subseteq \overline{H} \cap G$. Now consider the action of G on the set of cosets G/H; since the latter is finite, this action extends to a continuous homomorphism $\alpha : \hat{G} \to \mathfrak{S}_{G/H}$. If $g \in G \backslash H$, consider the set

$$U = \left\{x \in \hat{G},\ \alpha(x)(H) = gH\right\}.$$

This is an open subset of $\hat{G}$ (by continuity of α), and $U \cap H = \varnothing$. It follows that $U \cap \overline{H} = \varnothing$, so $g \in U \subseteq \hat{G} \backslash \overline{H}$. This proves that $\overline{H} \cap G = H$. Now we need to prove (i) − (iii).

(i) The proof of Lemma 3.13 shows that, if $(g_i)_{i \in I}$ is a set of coset representatives for H in G, then it is also a set of coset representatives for $\overline{H}$ in $\hat{G}$. It remains to show that they are distinct. Assume that $g_i \overline{H} = g_j \overline{H}$; then $g_i^{-1} g_j \in \overline{H} \cap G = H$, so $g_i H = g_j H$.

(ii) If $\overline{K} \trianglelefteq \overline{H}$, then $K = \overline{K} \cap G \trianglelefteq \overline{H} \cap G = H$. Conversely, if $K \trianglelefteq H$, then K acts trivially on $H/K \cong \overline{H}/\overline{K}$, so $\overline{K}$ also acts trivially and $\overline{K} \trianglelefteq \overline{H}$. The isomorphism $H/K \cong \overline{H}/\overline{K}$ follows from the proof of (i).

(iii) If $H \twoheadrightarrow H/K$ is any finite quotient, then we have an induced continuous homomorphism $\overline{H} \twoheadrightarrow H/K$. Thus, we have a family of maps $\left(\overline{H} \twoheadrightarrow H/K\right)_{K \leqslant_{fi} H}$, which induces a continuous surjective homomorphism $\overline{H} \twoheadrightarrow \hat{H}$. This morphism is also injective: if $h \in \overline{H} \backslash 1$, then by residual finiteness there is an open normal subgroup $U \trianglelefteq_{fi} \hat{G}$ such that $h \notin U$; therefore $h \not\mapsto 1$ under $\overline{H} \twoheadrightarrow \overline{H}/\overline{H} \cap U$. □

Corollary 3.24 (Basic Correspondence)**.** *Let G_1, G_2 be finitely generated and residually finite groups such that $\hat{G}_1 \cong \hat{G}_2$. Then there is a bijection*

$$\psi : \{H \leqslant G_1,\ [G_1 : H] < \infty\} \xrightarrow{\cong} \{H \leqslant G_2,\ [G_2 : H] < \infty\},$$

such that, for all $K \leqslant_{fi} H \leqslant_{fi} G_1$,

(i) $[H : K] = [\psi(H) : \psi(K)]$,

(ii) $K \trianglelefteq H \iff \psi(K) \trianglelefteq \psi(H)$, *and in that case,* $H/K \cong \psi(H)/\psi(K)$,

(iii) $\hat{H} \cong \widehat{\psi(H)}$.

Corollary 3.25. *$\hat{S}_g \ncong \hat{F}_r$ for any r, g.*

Proof. Every finite-sheeted cover of a surface is a surface, so every finite index subgroup of S_g is also a surface group, and has therefore abelianisation $\mathbb{Z}^{2d}$. However, F_r has an index 2 subgroup, and the Nielsen-Schreier Theorem implies that this subgroup is free of odd rank. The Basic Correspondence (Corollary 3.24) implies that $\hat{S}_g \ncong \hat{F}_r$. □

3.4 The Hopf property

Definition 3.26 (Hopf property)**.** *A (topological) group G has the* Hopf property *(or is* Hopfian*, or* Hopf*), if every (continuous) surjective homomorphism $G \twoheadrightarrow G$ is a (topological) isomorphism.*

Example 3.27. *Finite groups are Hopfian.*

Proposition 3.28. *Let G be a topologically finitely generated profinite group. Then G is Hopfian.*

Proof. For $n \geqslant 1$, let $\mathcal{U}_n$ be the set of open subgroups of G of index at most n and $G_n = \bigcap_{U \in \mathcal{U}_n} U$. Then G_n is open (because $\mathcal{U}_n$ is finite), and by Lemma 2.30,

$$G = \varprojlim_{n \geqslant 1} G/G_n.$$

Now if $U \in \mathcal{U}_n$ and $f : G \to G$ is surjective, we have $[G : U] = [G : f^{-1}(U)]$, so $f^{-1}(U) \in \mathcal{U}_n$. Therefore,

$$f^{-1}(G_n) = f^{-1}\left(\bigcap_{U \in \mathcal{U}_n} U\right) = \bigcap_{U \in \mathcal{U}_n} \underbrace{f^{-1}(U)}_{\in \mathcal{U}_n} \supseteq \bigcap_{V \in \mathcal{U}_n} V = G_n.$$

Therefore, $f(G_n) \subseteq G_n$, so there is a quotient map $f_n : G/G_n \to G/G_n$. The map f_n is surjective because f is, so f_n is an isomorphism because G/G_n is finite. Since this is true for all n, and $G = \varprojlim_{n \geqslant 1} G/G_n$, it follows that f is an isomorphism. □

Corollary 3.29. *If Γ is a finitely generated and residually finite group, then Γ is Hopfian.*

Proof. Let $f : \Gamma \twoheadrightarrow \Gamma$ be a surjective homomorphism. Then f induces a unique map $\hat{f} : \hat{\Gamma} \to \hat{\Gamma}$ making the following diagram commute:

$$\begin{array}{ccc} \Gamma & \xrightarrow{f} & \Gamma \\ {\scriptstyle \iota}\downarrow & & \downarrow{\scriptstyle \iota} \\ \hat{\Gamma} & \xrightarrow{\hat{f}} & \hat{\Gamma} \end{array}$$

Note that ι is injective by residual finiteness. The image of $\hat{f}$ is compact and contains the dense set $\iota(\Gamma)$, so $\hat{f}$ is a surjection, and $\hat{\Gamma}$ is topologically finitely generated, so it is Hopfian by Proposition 3.28, and therefore $\hat{f}$ is an isomorphism. It follows that f is injective, so it is also an isomorphism. □

Proposition 3.30. *Let G be a (topological) group with the Hopf property. Let H be a (topological) group. If there are (continuous) surjections $f : G \twoheadrightarrow H$ and $f' : H \twoheadrightarrow G$, then f and f' are both (topological) isomorphisms.*

Proof. Note that $f' \circ f : G \twoheadrightarrow G$ is a (continuous) surjection, and G is Hopfian, so $f' \circ f$ is a (topological) isomorphism. In particular, f is injective, so it is a (topological) isomorphism. Hence, $f' = (f' \circ f) \circ f^{-1}$ is also a (topological) isomorphism. □

Notation 3.31. *Given a finitely generated group Γ, we denote by $d(\Gamma)$ the minimum number of generators of Γ.*

Note that, if there is a surjection $\Gamma \twoheadrightarrow Q$, then $d(\Gamma) \geqslant d(Q)$.

Proposition 3.32. *Let Γ be a group. Assume that Γ has a finite quotient Q such that $d(\Gamma) = d(Q)$. If F is a free group such that $\hat{F} \cong \hat{\Gamma}$, then $F \cong \Gamma$.*

Proof. If $\hat{F} \cong \hat{\Gamma}$, then Q is also a quotient of F. It follows that

$$d(F) \geqslant d(Q) = d(\Gamma).$$

Therefore, there is a surjection $f : F \twoheadrightarrow \Gamma$, inducing in turn a continuous surjection $\hat{f} : \hat{F} \twoheadrightarrow \hat{\Gamma}$. Since $\hat{F}$ is Hopfian (and $\hat{\Gamma} \cong \hat{F}$), $\hat{f}$ is an isomorphism. It follows that $f : F \to \Gamma$ is injective, so it is an isomorphism. □

Example 3.33. *Let n, m be coprime integers. Then the group*

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

is not Hopfian and therefore not residually finite.

Proof. Consider the map $f : BS(n,m) \to BS(n,m)$ defined by $t \mapsto t$ and $a \mapsto a^n$. This is a surjective homomorphism (because the image contains t, a^n, a^m, and therefore a because n, m are coprime). But f is not injective: indeed, by considering an action on a tree, we can show that a does not commute with tat^{-1}, so $[a, tat^{-1}] \neq 1$, but $f\left([a, tat^{-1}]\right) = [a^n, a^m] = 1$. □

3.5 Finite quotients of free groups

Theorem 3.34. *Let F be a finitely generated free group.*

(i) *F is residually finite.*

(ii) *F is residually p-finite, i.e. for all $g \in F \backslash \{1\}$, there exists a finite p-group Q and a surjection $f : F \twoheadrightarrow Q$ such that $f(g) \neq 1$.*

Proof. (i) Assume that F is freely generated by a finite set S. Let $g \in F \backslash \{1\}$, and write g as a reduced word $s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$, with $s_i \in S$ and $\varepsilon_i \in \{\pm 1\}$.

The idea is to view F as the fundamental group of a bouquet X of $|S|$ circles labelled by elements of S. Write the word g along a line to obtain a labelled graph Y with $n+1$ vertices $v_0, \ldots, v_n$, with an edge labelled by s_i going from v_{i-1} to v_i when $\varepsilon_i = +1$ (or in the other direction if $\varepsilon_i = -1$). There is a natural continuous map $Y \to X$; we would like to make it a covering of X. But we need Y to look locally like X, i.e. every vertex in Y should have exactly one edge labelled by each element of S entering, and one leaving. Note that, in Y, there are the same number of vertices lacking an outgoing s-edge as there are lacking an incoming one. So we can add s-edges to obtain a new graph $\overline{Y}$ in which every vertex has an incoming s-edge and an outgoing one. Now, $\overline{Y}$ is a finite-sheeted covering space of X, so it corresponds to a finite index subgroup $\pi_1\overline{Y} \leqslant_{fi} F$, and $g \notin \pi_1\overline{Y}$. However, $\pi_1\overline{Y}$ may not be normal in F.

We note that following the s-edges induces a permutation of the set V of vertices of $\overline{Y}$. There is therefore a natural action of F on V, i.e. a map $f : F \to \mathfrak{S}_V$. Now g is not in $\operatorname{Ker} f$ because $f(g)$ maps v_0 to v_n, but $\operatorname{Ker} f$ has finite index and is normal in F. □

Theorem 3.35 (Marshall Hall)**.** *Let F be a finitely generated free group. Let $S \subseteq F$ be a finite subset and let $y \in F \backslash \langle S \rangle$. Then there is a finite group Q and a homomorphism $f : F \to Q$ such that $f(y) \notin f\left(\langle S \rangle\right)$.*

Equivalently, in the profinite completion $\hat{F}$,

$$\overline{\langle S \rangle} \cap F = \langle S \rangle .$$

Proof. Assume that F is freely generated by a finite set T. Write $y = t_1^{\varepsilon_1} \cdots t_n^{\varepsilon_n}$, with $t_i \in T$ and $\varepsilon_i \in \{\pm 1\}$. As in Theorem 3.34, start by considering a line graph with $n+1$ vertices $v_0, \ldots, v_n$ with the word y written along the edges $v_i v_{i+1}$. Now from v_0, add one cycle for each element of S, labelling the edges of each cycle by the letters of the corresponding word in S. At this point, v_0 may have several incoming (resp. outgoing) edges labelled by the same generator, so it is not directly possible to proceed as in Theorem 3.34. To solve this problem, perform a number of *Stalling folds*: whenever one vertex has several incoming (resp. outgoing) edges labelled by the same generator, identify all the edges to obtain a new graph. Repeat this process until every vertex has at most one incoming and one outgoing edge labelled by each generator. Then proceed as in Theorem 3.34: add edges to make the given graph Y a covering space for a bouquet of $|T|$ circles, consider the action $f : F \to \mathfrak{S}_V$ on the set of vertices of Y given by following labelled edges, and note that $f(S) \subseteq \mathrm{Stab}\,(v_0) \not\ni f(y)$. □

Remark 3.36. *Note that, if $S = \varnothing$, Theorem 3.35 says that finitely generated free groups are residually finite.*

Corollary 3.37. *Let F be a finitely generated free group. If a finite subset S does not generate F, then there exists a finite group Q and a homomorphism $f : F \to Q$ such that $f(\langle S \rangle) \neq f(F)$.*

Equivalently, $\langle S \rangle = F \iff \overline{\langle S \rangle} = \hat{F}$.

4 Pro-p groups

Definition 4.1 (Pro-p group)**.** *Let p be a prime. A* pro-p group *is an inverse limit of finite p-groups, i.e. finite groups whose order is a power of p.*

The pro-p completion *of a group Γ is*

$$\hat{\Gamma}_{(p)} = \varprojlim_{\substack{N \trianglelefteq \Gamma \\ \Gamma/N \text{ pro-}p}} \Gamma/N.$$

4.1 Frattini subgroup of finite groups

Definition 4.2 (Frattini subgroup)**.** *Let G be a finite group. The* Frattini subgroup $\Phi(G)$ *of G is the intersection of all maximal proper subgroups of G.*

Proposition 4.3. *If $f : G \to H$ is a surjective homomorphism between finite groups, then*

$$f(\Phi(G)) \subseteq \Phi(H).$$

In particular, $\Phi(G)$ is a characteristic normal subgroup of G (i.e. $\Phi(G)$ is stable under every automorphism of G).

Proof. Let M be a maximal proper subgroup of H. Then $f^{-1}(M)$ is a proper subgroup of G (because f is surjective), and it is maximal: if $f^{-1}(M) \subsetneq N \subseteq G$, then $M \subsetneq f(N) \subseteq H$, so $f(N) = H$ as M is maximal, and therefore $G = N \cdot \mathrm{Ker}\, f = N$ because $N \supseteq f^{-1}(M) \supseteq \mathrm{Ker}\, f$. This proves that $f^{-1}(M)$ is maximal. It follows that

$$\Phi(G) \subseteq f^{-1}(M),$$

so $f(\Phi(G)) \subseteq M$. Since this is true for all M, we have $f(\Phi(G)) \subseteq \Phi(H)$. □

Notation 4.4. *Given a group G, a normal subgroup $N \trianglelefteq G$ and a subset $S \subseteq G$, we write SN/N for the image of S under the projection $G \twoheadrightarrow G/N$.*

Proposition 4.5. *Let G be a finite group. Given a subset $S \subseteq G$, the following assertions are equivalent:*

(i) *S generates G.*

(ii) $S\Phi(G)$ *generates* G.

(iii) $S\Phi(G)/\Phi(G)$ *generates* $G/\Phi(G)$.

Intuitively, elements of $\Phi(G)$ *are non-generators.*

Proof. (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) Obvious.

(iii) $\Rightarrow$ (i) Suppose that S does not generate G. Then, since G is finite, S is contained in some maximal proper subgroup M of G. Now $\Phi(G) \subseteq M$, so $M/\Phi(G)$ is a proper subgroup of $G/\Phi(G)$. Therefore,

$$S\Phi(G)/\Phi(G) \subseteq M/\Phi(G) \subsetneq G/\Phi(G),$$

so $S\Phi(G)/\Phi(G)$ does not generate $G/\Phi(G)$. □

Notation 4.6. *Let* G *be a group,* H, K *be subgroups of* G *and* $n \in \mathbb{Z}$.

- $HK = \{hk,\ h \in H,\ k \in K\}$.
  HK *is a subgroup of* G *if* $H \trianglelefteq G$ *or* $K \trianglelefteq G$. *Moreover,* HK *is normal if* H, K *are both normal.*
- $[H, K] = \langle \{[h, k],\ h \in H,\ k \in K\} \rangle$, *where* $[h, k] = h^{-1}k^{-1}hk$.
  $[H, K]$ *is normal if* H, K *are both normal.*
- $G_{\mathrm{ab}} = G/[G, G]$ *is the* abelianisation *of* G.
- $H^n = \langle \{h^n,\ h \in H\} \rangle$.
  H^n *is normal if* H *is.*

Proposition 4.7. *Let* G *be a finite* p*-group. Then*

$$\Phi(G) = [G, G]\, G^p = \mathrm{Ker}\left(G \twoheadrightarrow G_{\mathrm{ab}} \twoheadrightarrow G_{\mathrm{ab}}/pG_{\mathrm{ab}}\right).$$

In particular, $G/\Phi(G) \cong G_{\mathrm{ab}}/pG_{\mathrm{ab}}$ *is a* $\mathbb{F}_p$*-vector space, so*

$$G/\Phi(G) \cong \mathbb{F}_p^{d(G)},$$

where $d(G)$ *is the minimal size of a generating set of* G.

4.2 Generators of pro-p groups

Definition 4.8 (Frattini subgroup of a profinite group)**.** *Let* G *be a profinite group. The* Frattini subgroup $\Phi(G)$ *of* G *is the intersection of all maximal proper closed subgroups of* G *(i.e. closed subgroups* $M \subsetneq G$ *such that, for any proper closed subgroup* $N \supseteq M$*, we have* $N = M$*).*

Lemma 4.9. *Let* G *be a profinite group.*

(i) *Any proper closed subgroup of* G *is contained in a proper open subgroup, and hence in a maximal proper closed subgroup.*

(ii) *Maximal proper closed subgroups are open.*

Proof. Write $G = \varprojlim_{j \in J} G_j$.

(i) If $H \subsetneq G$ is a proper closed subgroup, then H is not dense, so there exists $j \in J$ such that $p_j(H) \subsetneq p_j(G)$. Now $U = p_j^{-1}(p_j(H))$ is a proper open subgroup of G containing H. By Proposition 1.27, the group U has finite index in G, so there is a maximal proper closed subgroup of G containing U (and hence H).

(ii) By (i), any maximal proper closed subgroup M is contained in a proper open subgroup U, which must equal M by maximality, so M is open. □

Proposition 4.10. *If $f : G \to H$ is a surjective continuous homomorphism of profinite groups, then*

$$f(\Phi(G)) \subseteq \Phi(H).$$

Proposition 4.11. *Let G be a profinite group. Given a set $S \subseteq G$, the following assertions are equivalent:*

(i) *S topologically generates G.*

(ii) *$S\Phi(G)$ topologically generates G.*

(iii) *$S\Phi(G)/\Phi(G)$ topologically generates $G/\Phi(G)$.*

Proposition 4.12. *Let $(G_j)_{j\in J}$ be a surjective inverse system of finite groups, let $G = \varprojlim_{j\in J} G_j$. Then*

$$\Phi(G) = \varprojlim_{j\in J} \Phi(G_j).$$

Proof. Denote by $p_j : G \twoheadrightarrow G_j$ the projection maps. By Proposition 4.10, $p_j(\Phi(G)) \subseteq \Phi(G_j)$ for all j (by surjectivity), so $\Phi(G) \subseteq \varprojlim_{j\in J} \Phi(G_j)$.

Now let M be a maximal proper closed subgroup of G. Since M is open (Lemma 4.9), there exists $i_M \in J$ such that $\operatorname{Ker} p_{i_M} \subseteq M$. Therefore, $\operatorname{Ker} p_j \subseteq M$ for all $j \preccurlyeq i_M$. Hence, for $j \preccurlyeq i_M$, $p_j(M)$ is a maximal proper subgroup of G_j, so $p_j(M) \supseteq \Phi(G_j)$. It follows that

$$M \supseteq \varprojlim_{j\preccurlyeq i_M} \Phi(G_j) = \varprojlim_{j\in J} \Phi(G_j).$$

Since this is true for all M, we have $\Phi(G) \supseteq \varprojlim_{j\in J} \Phi(G_j)$. □

Proposition 4.13. *Let G be a topologically finitely generated pro-p group. Then*

$$\Phi(G) = \overline{[G,G]\,G^p},$$

and $G/\Phi(G) \cong \mathbb{F}_p^{d(G)}$, where $d(G)$ is the minimal size of a topological generating set for G.

Proof. Write $G = \varprojlim_{j\in J} G_j$, where $(G_j)_{j\in J}$ is a surjective inverse system of finite p-groups. Then by Propositions 4.7 and 4.12,

$$\Phi(G) = \varprojlim_{j\in J} \Phi(G_j) = \varprojlim_{j\in J} [G_j, G_j]\, G_j^p.$$

Moreover, it is clear that $p_j([G,G]\,G^p) \subseteq [G_j,G_j]\,G_j^p$, so $p_j\left(\overline{[G,G]\,G^p}\right) \subseteq [G_j,G_j]\,G_j^p$. It follows that

$$\overline{[G,G]\,G^p} \subseteq \varprojlim_{j\in J} [G_j,G_j]\,G_j^p = \Phi(G).$$

Now $G/\overline{[G,G]\,G^p}$ is topologically finitely generated by some subset $\{s_1,\dots,s_d\}$ and abelian. It follows that $\{s_1^{n_1}\cdots s_d^{n_d},\ 0 \leqslant n_i < p\}$ is a finite dense subset, so $G/\overline{[G,G]\,G^p}$ is finite and hence isomorphic to $\mathbb{F}_p^d$ for some d. Hence there is a continuous surjection $p : G \twoheadrightarrow G/\overline{[G,G]G^p} \cong \mathbb{F}_p^d$. Since $\Phi\left(\mathbb{F}_p^d\right) = 1$, Proposition 4.10 implies that

$$p(\Phi(G)) \subseteq \Phi\left(\mathbb{F}_p^d\right) = 1,$$

so that $\Phi(G) \subseteq \operatorname{Ker} p = \overline{[G,G]G^p}$. □

Corollary 4.14. *Let $f : G \to H$ be a continuous homomorphism of topologically finitely generated pro-p groups. Then $f(\Phi(G)) \subseteq \Phi(H)$ and hence there is an induced map $f_* : G/\Phi(G) \to H/\Phi(H)$, which is $\mathbb{F}_p$-linear, and such that f is surjective if and only if f_* is.*

Proof. By Proposition 4.13, $\Phi(G) = \overline{[G,G]\,G^p}$. But it is clear that $\Phi\left([G,G]\,G^p\right) \subseteq [H,H]\,H^p$, and so by continuity $\Phi\left(\overline{[G,G]\,G^p}\right) \subseteq \overline{[H,H]\,H^p}$, i.e. $f\left(\Phi(G)\right) \subseteq \Phi(H)$. Now by Proposition 4.11,

$$\begin{aligned} f(G) = H &\iff f(G) \text{ topologically generates } H \\ &\iff f(G)\Phi(H)/\Phi(H) \text{ topologicallly generates } H/\Phi(H) \\ &\iff f\left(G/\Phi(G)\right) \text{ topologically generates } H/\Phi(H) \\ &\iff f\left(G/\Phi(G)\right) = H/\Phi(H). \end{aligned}$$

□

Example 4.15. *Let $F = F(\{a,b\})$ be the free group on two generators. Consider its pro-p completion $G = \hat{F}_{(p)}$. Then $G/\Phi(G) \cong \mathbb{F}_p^2$. If $S = \{a^4b^2a, ba^{-2}b\} \subseteq F$, then S maps to $\{(5,2),(-2,2)\}$ under $G \twoheadrightarrow G/\Phi(G) \cong \mathbb{F}_p^2$. Since*

$$\begin{vmatrix} 5 & -2 \\ 2 & 2 \end{vmatrix} = 14,$$

it follows that $S\Phi(G)/\Phi(G)$ generates $G/\Phi(G)$ if and only if $p \neq 2, 7$.

4.3 Nilpotent groups

Notation 4.16. *If G is a group and $g, h \in G$, we write $g^h = h^{-1}gh$.*

Notation 4.17. *Let G be a group. A* commutator of length 2 *is $[g_1, g_2] = g_1^{-1}g_1^{g_2}$. Iteratively, a* commutator of length n *is defined by $[g_1, \ldots, g_n] = [g_1, [g_2, \ldots, g_n]]$.*

Definition 4.18 (Lower central series)**.** *If G is a group, its* lower central series $\left(\gamma_n(G)\right)_{n\geqslant 1}$ *is the sequence of normal subgroups of G defined by $\gamma_1(G) = G$ and*

$$\gamma_{n+1}(G) = \left[G, \gamma_n(G)\right].$$

We say that G is nilpotent of class c *if $\gamma_{c+1}(G) = 1$ and $\gamma_c(G) \neq 1$. In that case, $\gamma_c(G)$ is central in G.*

Remark 4.19. (i) *A group is nilpotent of class 1 if and only if it is abelian.*

(ii) γ_n *is* fully characteristic *in the sense that if $f : G \to H$ is a group homomorphism, then $f\left(\gamma_n(G)\right) \subseteq \gamma_n(H)$.*

Proposition 4.20. *If a group is nilpotent of class c, then all its subgroups and quotients are nilpotent of class at most c.*

Proposition 4.21. *All finite p-groups are nilpotent.*

Proof. Argue by induction, noting that finite p-groups have a nontrivial centre. □

Example 4.22. *If R is a ring, then the group of upper unitriangular matrices (i.e. upper triangular matrices with 1s on the diagonal) is nilpotent.*

Definition 4.23 (Lower central p-series)**.** *Let G be a topologically finitely generated pro-p group. Its* lower central p-series *is the sequence $\left(\gamma_n^{(p)}(G)\right)_{n\geqslant 1}$ defined by $\gamma_1^{(p)}(G) = G$ and*

$$\gamma_{n+1}^{(p)}(G) = \overline{\left[G, \gamma_n^{(p)}(G)\right]\left(\gamma_n^{(p)}(G)\right)^p}.$$

Remark 4.24. *Let G be a topologically finitely generated pro-p group.*

(i) $\gamma_n(G) \subseteq \gamma_n^{(p)}(G)$ *for all n.*

(ii) $\gamma_n^{(p)}(G)/\gamma_{n+1}^{(p)}(G)$ *is a $\mathbb{F}_p$-vector space for all n.*

(iii) $\gamma_n^{(p)}(G)$ *is open in* G.

(iv) $\left\{\gamma_n^{(p)}(G),\ n \geqslant 1\right\}$ *is a neighbourhood basis at the identity.*

Proof. (iii) Note that $\gamma_{n+1}^{(p)}(G) \supseteq \Phi\left(\gamma_n^{(p)}(G)\right)$. It follows that $\gamma_{n+1}^{(p)}(G)$ has finite index in $\gamma_n^{(p)}(G)$; since it is also closed, $\gamma_{n+1}^{(p)}(G)$ is open in $\gamma_n^{(p)}(G)$ (c.f. Proposition 1.27). The result then follows by induction on n.

(iv) If $N \trianglelefteq G$ is an open normal subgroup of G, then G/N is a finite p-group, so $\gamma_n^{(p)}(G/N)$ vanishes for some n (by Proposition 4.21), and therefore $\gamma_n^{(p)}(G) \subseteq N$. □

4.4 Invariance of topology

Lemma 4.25 (Commutator relations)**.** *Let G be a group, $x, y, z \in G$.*

(i) $[xy, z] = [x, z]^y \cdot [y, z]$.

(ii) $[x, yz] = [x, z] \cdot [x, y]^z$.

Lemma 4.26. *Let G be a nilpotent group generated by $a_1, \ldots, a_d$. Then every $g \in [G, G]$ can be written as*

$$g = [a_1, x_1] \cdots [a_d, x_d]$$

for some $x_1, \ldots, x_d \in G$.

Proof. We argue by induction on the nilpotency class. If $c = 1$, the result is trivial because G is abelian. Assume the result is true for nilpotent groups of class $(c-1)$. In particular, the result is true for $G/\gamma_c(G)$, so we can write

$$g = [a_1, x_1] \cdots [a_d, x_d]\, u,$$

for some $u \in \gamma_c(G)$. Since $u \in \gamma_c(G) = [G, \gamma_{c-1}(G)]$, it can be written as a product $\prod_{i=1}^{N} [g_i, \nu_i]$, with $g_i \in G$ and $\nu_i \in \gamma_{c-1}(G)$. Now let $\nu \in \gamma_{c-1}(G)$ and $w \in G$. Noting that $[h, \nu] \in \gamma_c(G) \subseteq Z(G)$ for all $h \in G$, the commutator relations (Lemma 4.25) imply that,

$$\begin{aligned}
[a_i a_j, \nu] &= [a_i, \nu]\,[a_j, \nu]\,, \\
\left[a_i^{-1}, \nu\right] &= \left[a_i, \nu^{-1}\right] = [a_i, \nu]^{-1}\,, \\
[a_i, \nu]^2 &= \left[a_i, \nu^2\right], \\
[a_i, w]\,[a_i, \nu] &= [a_i, \nu w]\,.
\end{aligned}$$

Since each g_i can be written as a product of elements of $\left\{a_1^{\pm 1}, \ldots, a_d^{\pm 1}\right\}$, we can use the above equalities to rewrite $u = [a_1, \nu_1'] \cdots [a_d, \nu_d']$, so that

$$g = [a_1, x_1] \cdots [a_d, x_d]\,[a_1, \nu_1'] \cdots [a_d, \nu_d'] = [a_1, \nu_1' x_1] \cdots [a_d, \nu_d' x_d]\,. \qquad \square$$

Proposition 4.27. *Let G be a topologically finitely generated pro-p group. Then $[G, G]$ is closed in G.*

Proof. Write $G = \varprojlim_{j \in J} G_j$, where $(G_j)_{j \in J}$ is a surjective inverse system of finite p-groups, with projection maps $p_j : G \to G_j$.

Let $\{a_1, \ldots, a_d\}$ be a topological generating set for G. Let

$$X = \{[a_1, x_1] \cdots [a_d, x_d]\,,\ x_1, \ldots, x_d \in G\}\,.$$

The set X is compact and closed as the image of G^d under a continuous map. It is moreover clear that $X \subseteq [G,G]$. Conversely, if $g \in [G,G]$, then $p_j(g) \in [G_j, G_j]$, and G_j is nilpotent (by Proposition 4.21). By Lemma 4.26, we can write

$$p_j(g) = [p_j(a_1), x_1] \cdots [p_j(a_d), x_d]$$

for some $x_1, \ldots, x_d \in G_j$. Hence $p_j(g) \in p_j(X)$ for all j, so $g \in \overline{X} = X$, completing the proof that $[G,G] = X$. □

Proposition 4.28. *Let G be a pro-p group and let K be a finite index subgroup of G. Then $[G:K]$ is a power of p.*

Proof. We may assume without loss of generality that K is normal in G (otherwise, replace K by $K' = \bigcap_{g \in G} gKg^{-1}$ and note that $[G:K'] = [G:K][K:K']$). Write $[G:K] = m = p^r m'$ with $p \nmid m'$. Consider the set

$$X = \{g^m,\ g \in G\} \subseteq K.$$

Note that X is closed as the image of the compact set G under $g \mapsto g^m$. By Corollary 2.15, it follows that

$$X = \overline{X} = \bigcap_{\substack{N \trianglelefteq G \\ \text{open}}} XN.$$

We claim that $g^{p^r} \in X \subseteq K$ for all $g \in G$. If this is true, then all elements of G/K will have order a power of p, so Cauchy's Theorem will imply that $|G/K|$ is a power of p.

To prove the claim, let $g \in G$ and $N \trianglelefteq G$ be an open normal subgroup. Then G/N is a p-group, so we can write $[G:N] = p^s$ for some s. Let $t = \max\{r,s\}$. Then $g^{p^t} \in N$ for all $g \in G$. Moreover, we have $p^r = \gcd(m, p^t)$, so there exist $a, b \in \mathbb{Z}$ such that $am + bp^t = p^r$. It follows that

$$g^{p^r} = \underbrace{(g^a)^m}_{\in X} \underbrace{\left(g^b\right)^{p^t}}_{\in N} \in XN.$$

Since this is true for all $N \trianglelefteq G$ open, we have $g^{p^r} \in \bigcap_{\substack{N \trianglelefteq G \\ \text{open}}} XN = X \subseteq K$. □

Proposition 4.29. *If G is a topologically finitely generated pro-p group, then $[G,G]\,G^p$ is closed in G, hence equals $\Phi(G)$.*

Proof. Write $G^{\{p\}} = \{g^p,\ g \in G\}$, so that $G^p = \left\langle G^{\{p\}} \right\rangle$. Hence

$$[G,G]\,G^p = [G,G]\,G^{\{p\}},$$

because in $G/[G,G]$ (which is abelian), $a^p b^p = (ab)^p$. Since $[G,G]\,G^{\{p\}}$ is closed (as the image of the compact set $[G,G] \times G$), the result is proved. □

Theorem 4.30. *Let G be a topologically finitely generated pro-p group. Then any finite index subgroup of G is open.*

Proof. As in the proof of Proposition 4.28, it suffices to prove the result for normal subgroups. Assume for contradiction that there is a group G with a normal finite index subgroup $K \trianglelefteq_{fi} G$ such that K is not open in G, and $[G:K]$ is minimal among all such G, K. Consider

$$M = [G,G]\,G^p K,$$

and note that $K \trianglelefteq_{fi} M \trianglelefteq_{fi} G$. Hence G/K is a nontrivial p-group (by Proposition 4.28), and Proposition 4.7 implies that

$$\Phi(G/K) = [G/K, G/K]\,(G/K)^p = M/K,$$

so $M \neq G$ (because the Frattini subgroup is always a proper subgroup). Either $M = K$, so $K \supseteq [G,G]\,G^p = \Phi(G)$ which is open, and thus K is open; or $M \neq K$, so by minimality K is open in M (because $[M:K] < [G:K]$) and similarly M is open in G, so K is open in G. □

Theorem 4.31. *Let G be a topologically finitely generated pro-p group, H a profinite group and $f : G \to H$ a homomorphism. Then f is continuous.*

Proof. Let $U \trianglelefteq H$ be an open normal subgroup. Then U has finite index in H, so $f^{-1}(U)$ has finite index in G. By Theorem 4.30, $f^{-1}(U)$ is open in G. Hence, f is continuous. □

Corollary 4.32. *Let G be a topologically finitely generated pro-p group. There is no other topology on G making it into a profinite group.*

In other words, the group structure determines the topology.

Proof. If $\mathcal{T}_1$ is the given topology on G and $\mathcal{T}_2$ is another topology making G into a profinite group, then the identity $(G, \mathcal{T}_1) \to (G, \mathcal{T}_2)$ is continuous by Theorem 4.31, so it is a homeomorphism: $\mathcal{T}_1 = \mathcal{T}_2$. □

4.5 Hensel's Lemma and p-adic arithmetic

Lemma 4.33. *Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial with coefficients in $\mathbb{Z}_p$. Then f has a root in $\mathbb{Z}_p$ if and only if it has a root in $\mathbb{Z}/p^k\mathbb{Z}$ for all $k \geqslant 0$.*

Proposition 4.34 (Hensel's Lemma for square roots)**.** *Let p be an odd prime. Suppose $\lambda \in \mathbb{Z}_p$ is a nonzero square modulo p, i.e. there exists $r_1 \in \mathbb{Z}$ such that $\lambda \equiv r_1^2 \not\equiv 0 \mod p$. Then there is a unique $\rho \in \mathbb{Z}_p$ such that*

$$\rho^2 = \lambda \qquad \text{and} \qquad \rho \equiv r_1 \mod p.$$

Proof. We construct a sequence $(r_k)_{k\geqslant 1}$ in $\mathbb{Z}$, unique modulo p^k, such that $r_{k+1} \equiv r_k \mod p^k$ and $(r_k)^2 \equiv \lambda \mod p^k$. It will follow that $(r_k)_{k\geqslant 1}$ defines an element $\rho \in \mathbb{Z}_p$ such that $\rho^2 = \lambda$. Suppose we have constructed $r_1, \ldots, r_k$ and consider $r_k + p^k a$ for $0 \leqslant a < p$. Since $r_k^2 \equiv \lambda \mod p^k$, we can write $r_k^2 = \lambda + p^k b_k$ for some $b_k \in \mathbb{Z}_p$. Hence,

$$\left(r_k + p^k a\right)^2 = \lambda + p^k b_k + 2p^k a r_k + p^{2k} a^2 \equiv \lambda + p^k \left(b_k + 2a r_k\right) \mod p^{k+1}.$$

Now, modulo p,

$$b_k + 2a r_k \equiv b_k + 2a r_1 \mod p.$$

Since $2r_1$ is invertible modulo p, there is a unique $0 \leqslant a_k < p$ such that $b_k + 2a_k r_k \equiv 0 \mod p$. Set $r_{k+1} = r_k + p^k a_k$. □

Lemma 4.35. *Let $f(x) \in \mathbb{Z}_p[x]$, $r, a \in \mathbb{Z}_p$ and $k \geqslant 1$. Then*

$$f\left(r + p^k a\right) \equiv f(r) + p^k a f'(r) \mod p^{k+1}.$$

Proof. Since the statement is linear in f, it is enough to show the result when $f(x) = x^n$. The binomial formula then implies that

$$\left(r + p^k a\right)^n = r^n + n p^k a r^{n-1} + \sum_{i=2}^{n} \binom{n}{i} p^{ki} a^i r^{n-i} \equiv r^n + n p^k a r^{n-1} \mod p^{k+1}.$$ □

Proposition 4.36 (Hensel's Lemma)**.** *Let $f(x) \in \mathbb{Z}_p[x]$ and $k \in \mathbb{N}$. Let $r \in \mathbb{Z}_p$ such that*

$$f(r) \equiv 0 \mod p^k \qquad \text{and} \qquad f'(r) \not\equiv 0 \mod p,$$

where f' denotes the formal derivative of f. Then there exists a unique $\rho \in \mathbb{Z}_p$ such that $f(\rho) = 0$ and $\rho \equiv r \mod p^k$.

Proof. Same proof as in the case of square roots (Proposition 4.34), using Lemma 4.35. □

4.6 p-adic matrix groups

Definition 4.37 ($GL_n^{(k)}(\mathbb{Z}_p)$ and $SL_n^{(k)}(\mathbb{Z}_p)$)**.** *We define*

$$GL_n^{(k)}(\mathbb{Z}_p) = \operatorname{Ker}\left(GL_n(\mathbb{Z}_p) \to GL_n\left(\mathbb{Z}/p^k\mathbb{Z}\right)\right) = \left\{I + p^k B,\ B \in \operatorname{Mat}_{n,n}(\mathbb{Z}_p)\right\},$$
$$SL_n^{(k)}(\mathbb{Z}_p) = \operatorname{Ker}\left(SL_n(\mathbb{Z}_p) \to SL_n\left(\mathbb{Z}/p^k\mathbb{Z}\right)\right) = \left\{A \in GL_n^{(k)}(\mathbb{Z}_p),\ \det A = 1\right\}.$$

Proposition 4.38. *Both $GL_n^{(1)}(\mathbb{Z}_p)$ and $SL_n^{(1)}(\mathbb{Z}_p)$ are pro-p groups.*

Proof. Note that

$$GL_n^{(1)}(\mathbb{Z}_p) = \varprojlim_{k\geqslant 0} GL_n^{(1)}\left(\mathbb{Z}/p^k\mathbb{Z}\right) = \varprojlim_{k\geqslant 0}\left\{I + pB,\ B \in \operatorname{Mat}_{n,n}\left(\mathbb{Z}/p^k\mathbb{Z}\right)\right\},$$

and the group $\left\{I + pB,\ B \in \operatorname{Mat}_{n,n}\left(\mathbb{Z}/p^k\mathbb{Z}\right)\right\}$ has order $p^{N^2(k-1)}$. Moreover, $SL_n^{(1)}(\mathbb{Z}_p)$ is a closed subgroup of $GL_n^{(1)}(\mathbb{Z}_p)$, so it is also a pro-p group. □

Notation 4.39. *In this section, the prime p will always be assumed to be odd (i.e. $p \neq 2$).*

Lemma 4.40. *Let $r \geqslant 1$. Then for all $A \in \operatorname{Mat}_{n,n}(\mathbb{Z}_p)$, there exists $E \in \mathbb{Z}[A]$ such that*

$$\begin{aligned}(I + p^r A)^p &= I + p^{r+1}A + p^{r+2}E\\ &\equiv I + p^{r+1}A \mod p^{r+2}.\end{aligned}$$

Proof. Write the binomial expansion of $(I + p^r A)^p$ and note that terms other than I and $p^{r+1}A$ are $\binom{p}{\ell}p^{r\ell}A^\ell$ for $\ell \geqslant 2$, which always has a factor p^{r+2} (because $p \neq 2$). □

Lemma 4.41. *If $p \neq 2$, then $\mathbb{Z}_p^\times \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$.*
In particular, $\mathbb{Z}_p^\times$ has no element of order p.

Proposition 4.42. *The continuous function $A \mapsto A^p$ defines a surjection*

$$GL_n^{(k)}(\mathbb{Z}_p) \twoheadrightarrow GL_n^{(k+1)}(\mathbb{Z}_p).$$

The same is true for SL_n.

Proof. We want to find a p-th root of $I + p^{k+1}A \in GL_n^{(k+1)}(\mathbb{Z}_p)$. By induction on n, we prove that for all $m \geqslant 1$, there are matrices $B_m, E_m \in \mathbb{Z}[A]$, such that

$$B_{m+1} \equiv B_m \mod p^m \qquad \text{and} \qquad \left(I + p^k B_m\right)^p = I + p^{k+1}A + p^{k+m+1}E_m.$$

It will follow that $(B_m)_{m\geqslant 1}$ defines an element $B \in \operatorname{Mat}_{n,n}(\mathbb{Z}_p) = \varprojlim_{m\geqslant 1}\operatorname{Mat}_{n,n}(\mathbb{Z}/p^m\mathbb{Z})$, and that $\left(I + p^k B\right)^p = I + p^{k+1}A$. For $m = 1$, take $B_1 = A$, and use Lemma 4.40 to find $E_1 \in \mathbb{Z}[A]$ such that

$$\left(I + p^k A\right)^p = I + p^{k+1}A + p^{k+2}E_1.$$

For the inductive step, define $B_{m+1} = B_m - p^m E_m$. Then

$$\begin{aligned}\left(I + p^k B_{m+1}\right)^p &= \left(\left(I + p^k B_m\right) - p^{k+m}E_m\right)^p\\ &= \left(I + p^k B_m\right)^p - p^{k+m+1}E_m\left(I + p^k B_m\right) + \mathcal{O}\left(p^{k+m+2}\right)\\ &= I + p^{k+1}A + p^{k+m+1}E_m - p^{k+m+1}E_m\left(I + \mathcal{O}\left(p^k\right)\right) + \mathcal{O}\left(p^{k+m+2}\right)\\ &= I + p^{k+1}A + p^{k+m+2}E_{m+1},\end{aligned}$$

for some $E_{m+1} \in \mathbb{Z}[A]$. This completes the induction and shows that $A \mapsto A^p$ is a surjection $GL_n^{(k)}(\mathbb{Z}_p) \twoheadrightarrow GL_n^{(k+1)}(\mathbb{Z}_p)$.

For SL_n, it suffices to prove that if $\det C^p = 1$, then $\det C = 1$ (for $C \in \operatorname{Mat}_{n,n}(\mathbb{Z}_p)$). This is a consequence of Lemma 4.41. □

Lemma 4.43. *If $A, B \in \mathrm{Mat}_{n,n}(\mathbb{Z}_p)$, then*

$$\begin{aligned}\left(I+p^kA\right)\left(I+p^kB\right) &\equiv I+p^k(A+B) \mod p^{k+1}\\ &\equiv \left(I+p^kB\right)\left(I+p^kA\right) \mod p^{k+1}.\end{aligned}$$

Proposition 4.44. *For all $k \geqslant 1$,*

$$\Phi\left(GL_n^{(k)}(\mathbb{Z}_p)\right) = GL_n^{(k+1)}(\mathbb{Z}_p),$$

and

$$GL_n^{(k)}(\mathbb{Z}_p)/GL_n^{(k+1)}(\mathbb{Z}_p) \cong \mathbb{F}_p^{n^2}.$$

Proof. Note that

$$GL_n^{(k)}(\mathbb{Z}_p)/GL_n^{(k+1)}(\mathbb{Z}_p) = \left\{I+p^kB,\ B \in \mathrm{Mat}_{n,n}(\mathbb{Z}_p)\right\}/p^{k+1}\mathrm{Mat}_{n,n}(\mathbb{Z}_p).$$

Hence $\left|GL_n^{(k)}(\mathbb{Z}_p)/GL_n^{(k+1)}(\mathbb{Z}_p)\right| = p^{n^2}$. Moreover, Lemma 4.43 implies that $GL_n^{(k)}(\mathbb{Z}_p)/GL_n^{(k+1)}(\mathbb{Z}_p)$ is abelian and of exponent p, so it is isomorphic to $\mathbb{F}_p^d$ for some d, and therefore

$$GL_n^{(k)}(\mathbb{Z}_p)/GL_n^{(k+1)}(\mathbb{Z}_p) \cong \mathbb{F}_p^{n^2}.$$

Now Proposition 4.42 implies that

$$GL_n^{(k+1)}(\mathbb{Z}_p) \subseteq \left(GL_n^{(k)}(\mathbb{Z}_p)\right)^p \subseteq \Phi\left(GL_n^{(k)}(\mathbb{Z}_p)\right).$$

Since $\Phi\left(\mathbb{F}_p^{n^2}\right) = 1$, it follows by Proposition 4.10 (applied to the quotient map $GL_n^{(k)}(\mathbb{Z}_p) \twoheadrightarrow \mathbb{F}_p^{n^2}$) that $\Phi\left(GL_n^{(k)}(\mathbb{Z}_p)\right) = GL_n^{(k+1)}(\mathbb{Z}_p)$. □

Corollary 4.45. *For all $k \geqslant 1$, the mapping $A \mapsto A^p$ induces an isomorphism*

$$GL_n^{(k)}(\mathbb{Z}_p)/GL_n^{(k+1)}(\mathbb{Z}_p) \xrightarrow{\cong} GL_n^{(k+1)}(\mathbb{Z}_p)/GL_n^{(k+2)}(\mathbb{Z}_p).$$

Proof. This map is surjective by Proposition 4.42, it is a group homomorphism, and the two groups have the same order by Proposition 4.44. □

Theorem 4.46. *If H is a closed subgroup of $GL_n^{(1)}(\mathbb{Z}_p)$, then*

$$d(H) \leqslant d\left(GL_n^{(1)}(\mathbb{Z}_p)\right) = n^2.$$

Proof. It suffices to show that $d(H) \leqslant n^2$ for all subgroups H of each finite group

$$G = GL_n^{(1)}(\mathbb{Z}_p)/GL_n^{(k+1)}(\mathbb{Z}_p).$$

Let $H \leqslant G$, set

$$G_m = GL_n^{(m)}(\mathbb{Z}_p)/GL_n^{(k+1)}(\mathbb{Z}_p) \qquad \text{and} \qquad H_m = H \cap G_m.$$

We prove by top-down induction that $d(H_m) \leqslant n^2$. This is true for $m = k$ because H_k is a subgroup of $G_k \cong \mathbb{F}_p^{n^2}$. For the inductive step, note that $H_m/H_{m+1} \leqslant G_m/G_{m+1} \cong \mathbb{F}_p^{n^2}$ and let

$$e = \dim_{\mathbb{F}_p}(H_m/H_{m+1}) \leqslant n^2.$$

Take e elements $h_1, \ldots, h_e \in H_m$ whose images generate H_m/H_{m+1}. Corollary 4.45 implies that the p-power map gives an isomorphism $G_m/G_{m+1} \xrightarrow{\cong} G_{m+1}/G_{m+2}$; hence, $h_1^p, \ldots, h_e^p$ are linearly independent in $H_{m+1}/H_{m+2} \leqslant G_{m+1}/G_{m+2} \cong \mathbb{F}_p^{n^2}$, hence they are also linearly independent in $H_{m+1}/\Phi(H_{m+1})$ since there is a surjection $H_{m+1}/\Phi(H_{m+1}) \twoheadrightarrow H_{m+1}/H_{m+2}$. By extending to a basis, we can find $d-e$ elements $y_1, \ldots, y_{d-e} \in H_{m+1}$ (where $d = d(H_{m+1})$) such that

$$H_{m+1} = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{d-e}\rangle.$$

Then

$$H_m = \langle h_1, \ldots, h_e\rangle H_{m+1} = \langle h_1, \ldots, h_e, y_1, \ldots, y_{d-e}\rangle,$$

so $d(H_m) \leqslant d(H_{m+1}) \leqslant n^2$ as required. □

Corollary 4.47. *There is no closed nonabelian free pro-p subgroup $\hat{F}_{(p)} \subseteq GL_n(\mathbb{Z}_p)$.*

Sketch of proof. Note that $\hat{F}_{(p)}$ has a normal subgroup of index p^n for all n. These are free pro-p groups by a form of the Basic Correspondence, and they have rank $p^{n(r-1)}+1$ by Nielsen-Schreier. □

Remark 4.48. *Compare Corollary 4.47 with the fact that $SL_2(\mathbb{Z})$ has a free subgroup of rank 2 (and therefore of every finite rank).*

Theorem 4.49. *Let G be a pro-p group. Assume that there exists $R \geqslant 0$ such that $d(H) \leqslant R$ for all closed subgroups $H \leqslant G$. Then there is an abelian normal subgroup $A \cong \mathbb{Z}_p^e$ of G for some $e \leqslant R$ such that G/A injects into the direct product of $GL_r(\mathbb{Z}_p)$ with a finite group.*

5 Cohomology of groups

5.1 Group rings and chain complexes

Definition 5.1 (Group ring)**.** *Given a group G, its* group ring *is the free abelian group $\mathbb{Z}G$ (sometimes denoted by $\mathbb{Z}[G]$) with basis G, with multiplication defined on basis elements by $g \cdot h = gh$. There is a multiplicative identity $1e$, which we denote by 1.*

Note that $\mathbb{Z}G$ is not commutative, except if G is abelian. Moreover, $\mathbb{Z}G$ may not be an integral domain (e.g. if G has finite order elements).

Definition 5.2 (G-module)**.** *Given a group G, a (left) G-*module *is a (left) $\mathbb{Z}G$-module, i.e. an abelian group M equipped with a function $(r, m) \in \mathbb{Z}G \times M \mapsto r \cdot m \in M$ satisfying*

(i) *$r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ for all $r \in \mathbb{Z}G$ and $m_1, m_2 \in M$,*

(ii) *$r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$ for all $r_1, r_2 \in \mathbb{Z}G$ and $m \in M$,*

(iii) *$(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$ for all $r_1, r_2 \in \mathbb{Z}G$ and $m \in M$.*

Note that we only need to think about the action of basis elements. Hence, a G-module can be defined equivalently as an abelian group M together with a map $G \to \mathrm{Aut}(M)$.

A G-module is trivial *(or has trivial G-action) if $g \cdot m = m$ for all $g \in G$ and $m \in M$.*

A morphism of G-modules *(or G-*linear map*) is a group homomorphism $f : M_1 \to M_2$ such that $f(r \cdot m) = r \cdot f(m)$ for all $r \in \mathbb{Z}G$ and $m \in M$.*

Given G-modules M_1, M_2, the Hom-group $\mathrm{Hom}_G(M_1, M_2)$ *is the set of G-linear maps $M_1 \to M_2$ with a structure of abelian group given by pointwise addition.*

Definition 5.3 (Dual and induced maps)**.** *Let A, B, M, N be G-modules.*

(i) *A G-linear map $f : A \to B$ gives a* dual map

$$f^* : \begin{vmatrix} \mathrm{Hom}_G(B, M) \longrightarrow \mathrm{Hom}_G(A, M) \\ \phi \longmapsto \phi \circ f \end{vmatrix}.$$

(ii) *Similarly, a G-linear map $h : M \to N$ gives an* induced map

$$h_* : \begin{vmatrix} \mathrm{Hom}_G(A, M) \longrightarrow \mathrm{Hom}_G(A, N) \\ \phi \longmapsto h \circ \phi \end{vmatrix}.$$

Definition 5.4 (Chain complex)**.** *A* chain complex $M_\bullet$ *of G-modules is a (finite or infinite) sequence of G-modules and G-linear maps*

$$\cdots \xrightarrow{d_{n+2}} M_{n+1} \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \xrightarrow{d_{n-1}} \cdots,$$

such that $d_n \circ d_{n+1} = 0$*, or equivalently* $\operatorname{Im} d_{n+1} \subseteq \operatorname{Ker} d_n$.

The complex is exact at M_n *if* $\operatorname{Im} d_{n+1} = \operatorname{Ker} d_n$*. The complex is* exact *if it is exact at every* M_n*.*

The homology *of the complex is the sequence of abelian groups defined by*

$$H_n(M_\bullet) = \operatorname{Ker} d_n / \operatorname{Im} d_{n+1}.$$

Example 5.5. (i) *A complex* $0 \to M \xrightarrow{d} N$ *is exact* iff d *is injective.*

(ii) *A complex* $M \xrightarrow{d} N \to 0$ *is exact* iff d *is surjective.*

(iii) *A* short exact sequence *is an exact complex*

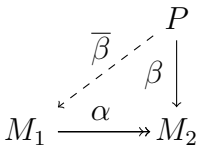
$$0 \to M_2 \xrightarrow{d_2} M_1 \xrightarrow{d_1} M_0 \to 0.$$

5.2 Projective resolutions and cohomology

Definition 5.6 (Free G-modules)**.** *Given a set* X*, the* free G-module *on* X *is the set* $\mathbb{Z}G\{X\}$ *of finite formal sums* $\sum_{x\in X} r_x x$*, with* $r_x \in \mathbb{Z}G$*, with* G*-action given by* $r \cdot \sum_{x\in X} r_x x = \sum_{x\in X} (rr_x)\, x$*.*

Note that, as abelian groups, $\mathbb{Z}G = \mathbb{Z}1\{G\}$*.*

Definition 5.7 (Projective G-module)**.** *A* G*-module* P *is* projective *if for every surjective* G*-linear map* $\alpha : M_1 \twoheadrightarrow M_2$*, and for every* G*-linear map* $\beta : P \to M_2$*, there exists* $\overline{\beta} : P \to M_1$ *such that the following diagram commutes:*



Proposition 5.8. *Free modules are projective.*

Proof. Given $\alpha : M_1 \twoheadrightarrow M_2$ and $\beta : \mathbb{Z}G\{X\} \to M_2$, choose for each $x \in X$ an element $m_x \in M_1$ such that $\alpha(m_x) = \beta(x)$, and define $\overline{\beta} : \mathbb{Z}G\{X\} \to M_1$ by $\overline{\beta}\left(\sum_{x\in X} r_x x\right) = \sum_{x\in X} r_x m_x$. □

Definition 5.9 (Projective resolution)**.** *A* projective resolution *(resp.* free resolution*) of* $\mathbb{Z}$ *by* G*-modules is an exact sequence*

$$\cdots \to F_{n+1} \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} \cdots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} \mathbb{Z} \to 0,$$

where $\mathbb{Z}$ *has trivial* G*-action and each* F_n *is projective (resp. free).*

Example 5.10. *Let* X *be a connected simplicial complex whose universal cover* $\widetilde{X}$ *is contractible. Let* $G = \pi_1 X$ *and let* X_n *be the set of* n*-simplices of* X*. Hence,* G *acts on* $\widetilde{X}$ *with quotient* X *and without fixed point, so the set of* n*-simplices of* $\widetilde{X}$ *is in bijection with* $G \times X_n$*. The* reduced simplicial chain complex *of* $\widetilde{X}$ *takes the form*

$$\cdots \to \mathbb{Z}G\{X_2\} \to \mathbb{Z}G\{X_1\} \to \mathbb{Z}G\{X_0\} \to \mathbb{Z} \to 0;$$

this is a free resolution of $\mathbb{Z}$ *by* G*-modules.*

Definition 5.11 (Group cohomology)**.** *Let* $F_\bullet$ *be a projective resolution of* $\mathbb{Z}$ *by* G*-modules, and let* M *be a* G*-module. Take* Hom*-groups to get a cochain complex*

$$\cdots \xleftarrow{d^3} \operatorname{Hom}_G(F_2, M) \xleftarrow{d^2} \operatorname{Hom}_G(F_1, M) \xleftarrow{d^1} \operatorname{Hom}_G(F_0, M).$$

The n*-th* cohomology group *of* G *with coefficients in* M *is*

$$H^n(G, M) = \operatorname{Ker} d^{n+1} / \operatorname{Im} d^n.$$

Elements of $\operatorname{Ker} d^{n+1}$ *are called* n-cocycles*, elements of* $\operatorname{Im} d^{n+1}$ *are called* n-coboundaries*.*

Example 5.12. *Consider the group $G = \mathbb{Z}$, written multiplicatively as $\mathbb{Z} = \langle t \rangle$. Then the chain complex*

$$0 \to \mathbb{Z}G \xrightarrow{d_1} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

is a free resolution of $\mathbb{Z}$ by G-modules, where $\varepsilon\left(\sum_{g\in G} n_g g\right) = \sum_{g\in G} n_g$ and $d_1(x) = x(t-1)$. To compute $H^n(\mathbb{Z}, M)$ for a G-module M, we apply $\mathrm{Hom}_G(-, M)$, yielding

$$0 \leftarrow \mathrm{Hom}_G(\mathbb{Z}G, M) \xleftarrow{d^1} \mathrm{Hom}_G(\mathbb{Z}G, M).$$

Now it is a general fact that there is an isomorphism of abelian groups $\mathrm{Hom}_G(\mathbb{Z}G, M) \cong M$ given by $\phi \mapsto \phi(1)$, and under this identification, $d^1 : M \to M$ is multiplication by $(t-1)$. It follows that

$$\begin{aligned} H^0(\mathbb{Z}, M) &= \operatorname{Ker} d^1 = \{m \in M,\ (t-1)m = 0\} \\ &= \{m \in M,\ \forall g \in G,\ gm = m\} = M^G, \\ H^1(\mathbb{Z}, M) &= M/\langle (t-1)M \rangle = M_G, \\ H^n(\mathbb{Z}, M) &= 0 \quad \text{for } n \geqslant 2. \end{aligned}$$

Definition 5.13 ((Co-)invariants)**.** *Given a G-module M, the module of* invariants *of M is*

$$M^G = \{m \in M,\ \forall g \in G,\ gm = m\},$$

and the module of co-invariants *of M is*

$$M_G = M/\langle \{gm - m,\ g \in G,\ m \in M\} \rangle.$$

Proposition 5.14. *If G is a free group, then $H^n(G, M) = 0$ for all $n \geqslant 2$.*

Proof. Let X be a wedge of circles with $\pi_1 X = G$. The universal cover $\widetilde{X}$ is a tree – so it is contractible. By Example 5.10, the chain complex of $\widetilde{X}$ gives a free resolution of $\mathbb{Z}$ by G-modules, and it has no n-cells for $n \geqslant 2$. □

Definition 5.15 (Cohomological dimension)**.** *A group G has* cohomological dimension *n (and we write $\mathrm{cd}(G) = n$) if $H^m(G, M) = 0$ for all G-modules M and for all $m > n$, and if there exists a G-module M such that $H^n(G, M) \neq 0$.*

If no such n exists, we set $\mathrm{cd}(G) = \infty$.

Remark 5.16. *It was proved by Stallings and Swan that free finitely generated groups are the only (finitely generated) groups of cohomological dimension 1.*

5.3 Chain maps and induced maps on cohomology

Definition 5.17 (Chain map)**.** *Let $(A_\bullet, \alpha_\bullet)$ and $(B_\bullet, \beta_\bullet)$ be two chain complexes of G-modules. A chain map $f_\bullet : A_\bullet \to B_\bullet$ is a sequence of G-linear maps $f_n : A_n \to B_n$ such that $f_{n-1} \circ \alpha_n = \beta_n \circ f_n$ for all n.*

Proposition 5.18. *A chain map $f_\bullet : A_\bullet \to B_\bullet$ induces maps $f_* : H_n(A_\bullet) \to H_n(B_\bullet)$.*

Proof. We have $f_n(\operatorname{Ker} \alpha_n) \subseteq \operatorname{Ker} \beta_n$ and $f_n(\operatorname{Im} \alpha_{n+1}) \subseteq \operatorname{Im} \beta_{n+1}$ for all n because of the identity $f_{n-1} \circ \alpha_n = \beta_n \circ f_n$. It follows that f_n induces a map

$$f_* : H_n(A_\bullet) = \operatorname{Ker} \alpha_n / \operatorname{Im} \alpha_{n+1} \longrightarrow \operatorname{Ker} \beta_n / \operatorname{Im} \beta_{n+1} = H_n(B_\bullet).$$ □

Corollary 5.19. *If $f : M \to N$ is a G-linear map, then there are induced maps*

$$f_* : H^n(G, M) \to H^n(G, N).$$

Proof. Let $F_\bullet$ be a projective resolution of $\mathbb{Z}$ by G-modules, and note that there is a chain map $\mathrm{Hom}_G(F_\bullet, M) \to \mathrm{Hom}_G(F_\bullet, N)$. □

Lemma 5.20 (Snake Lemma)**.** *If*

$$0 \to A_\bullet \xrightarrow{f_\bullet} B_\bullet \xrightarrow{g_\bullet} C_\bullet \to 0$$

is a short exact sequence of chain complexes, then there are natural maps $\delta_n : H_{n+1}(C_\bullet) \to H_n(A_\bullet)$ such that the sequence

$$\cdots \to H_n(A_\bullet) \xrightarrow{f_*} H_n(B_\bullet) \xrightarrow{g_*} H_n(C_\bullet) \xrightarrow{\delta_{n-1}} H_{n-1}(A_\bullet) \to \cdots$$

is exact.

Lemma 5.21. *Let*

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

be a short exact sequence of G-modules, and let F be projective. Then the sequence of abelian groups

$$0 \to \mathrm{Hom}_G(F, M_1) \xrightarrow{f_*} \mathrm{Hom}_G(F, M_2) \xrightarrow{g_*} \mathrm{Hom}_G(F, M_3) \to 0$$

is exact.

Proof. $\operatorname{Ker} f_* = 0$: if $f_*\phi = f \circ \phi = 0$, then $\operatorname{Im}\phi \subseteq \operatorname{Ker} f = 0$, so $\phi = 0$.

$\operatorname{Ker} g_* = \operatorname{Im} f_*$: we have $g_* f_* \phi = g \circ f \circ \phi = 0$ because $g \circ f = 0$, so $\operatorname{Ker} g_* \supseteq \operatorname{Im} f_*$. Conversely, let $\psi \in \operatorname{Ker} g_* \subseteq \mathrm{Hom}_G(F, M_2)$. For $x \in F$, we have $g(\psi(x)) = (g_*\psi)(x) = 0$, so $\psi(x) \in \operatorname{Ker} g = \operatorname{Im} f$, hence there exists $y \in M_1$ such that $x = f(y)$. Set $y = \phi(x)$, so that ϕ is G-linear and $\psi = f_*\phi \in \operatorname{Im} f_*$.

$\operatorname{Im} g_* = \mathrm{Hom}(F, M_3)$: this is by definition of projectivity. □

Proposition 5.22. *If*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

is a short exact sequence of G-modules, then there is a long exact sequence

$$\cdots \to H^n(G, M_1) \to H^n(G, M_2) \to H^n(G, M_3) \to H^{n+1}(G, M_1) \to \cdots.$$

Proof. If $F_\bullet$ is a projective resolution of $\mathbb{Z}$ by G-modules, then $\mathrm{Hom}_G(F_\bullet, M_i)$ give a short exact sequence of chain complexes by Lemma 5.21; it then suffices to apply the Snake Lemma (Lemma 5.20). □

5.4 Different projective resolutions

Theorem 5.23. *Given a G-module M, the definition of $H^n(G, M)$ does not depend on the choice of projective resolutions.*

Proof. Let $(F_\bullet, d_\bullet)$ and $(F'_\bullet, d'_\bullet)$ be two projective resolutions of $\mathbb{Z}$ by G-modules. We will construct:

- Chain maps $f_\bullet : F_\bullet \to F'_\bullet$ and $g_\bullet : F'_\bullet \to F_\bullet$,
- Maps $s_n : F_n \to F_{n+1}$ such that $d_{n+1}s_n + s_{n-1}d_n = g_n f_n - \mathrm{id}_{F_n}$,
- Maps $s'_n : F'_n \to F'_{n+1}$ such that $d'_{n+1}s'_n + s'_{n-1}d'_n = f_n g_n - \mathrm{id}_{F'_n}$,

Then $f_\bullet$ and $g_\bullet$ will give dual chain maps $f^*_\bullet : \mathrm{Hom}_G(F'_\bullet, M) \to \mathrm{Hom}_G(F_\bullet, M)$, inducing maps on cohomology $f^*_n : H^n_{F'}(G, M) \to H^n_F(G, M)$, and similarly $g^*_n : H^n_F(G, M) \to H^n_{F'}(G, M)$. The existence of the maps s_n and s'_n will imply that

$$f^*_n g^*_n = \mathrm{id}_{H^n_F(G,M)} \qquad \text{and} \qquad g^*_n f^*_n = \mathrm{id}_{H^n_{F'}(G,M)},$$

i.e. $H^n_F(G, M) \cong H^n_{F'}(G, M)$.

Construction of $f_\bullet$. Set $f_{-1} = \mathrm{id}_\mathbb{Z} : \mathbb{Z} \to \mathbb{Z}$. Since $d'_0 : F'_0 \to \mathbb{Z}$ is onto and F_0 is projective, there exists $f_0 : F_0 \to F'_0$ such that $d'_0 f_0 = f_{-1} d_0$. Then continue inductively: if f_{n-1} and f_n have been constructed so that the diagram

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & F_{n+1} & \xrightarrow{d_{n+1}} & F_n & \xrightarrow{d_n} & F_{n-1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\ \cdots & \longrightarrow & F'_{n+1} & \xrightarrow{d'_{n+1}} & F'_n & \xrightarrow{d'_n} & F'_{n-1} & \longrightarrow & \cdots \end{array}$$

commutes, then $d'_n f_n d_{n+1} = f_{n-1} d_n d_{n+1} = 0$, so

$$\operatorname{Im}(f_n d_{n+1}) \subseteq \operatorname{Ker} d'_n = \operatorname{Im} d'_{n+1},$$

and by projectivity of F_{n+1}, there exists $f_{n+1} : F_{n+1} \to F'_{n+1}$ such that $f_n d_{n+1} = d'_{n+1} f_{n+1}$.

Construction of s_n. Set $h_n = g_n f_n - \mathrm{id}$, and perform a similar inductive construction so that $d_{n+1} s_n = h_n - s_{n-1} d_n$. □

Definition 5.24 (Bar resolution)**.** *Denote by $G^{(n)}$ the set of symbols $[g_1 \mid \cdots \mid g_n]$ for $g_1, \ldots, g_n \in G$ (and $G^{(0)} = \{[]\}$). The* bar resolution *of G is the chain complex*

$$\cdots \to F_{n+1} \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} \cdots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} \mathbb{Z} \to 0,$$

defined by

$$F_n = \mathbb{Z}G\left\{G^{(n)}\right\},$$

and with transition map $d_n : F_n \to F_{n-1}$ given by

$$\begin{aligned} d_n([g_1 \mid \cdots \mid g_n]) = g_1[g_2 \mid \cdots \mid g_n] - [g_1 g_2 \mid g_3 \mid \cdots \mid g_n] + [g_1 \mid g_2 g_3 \mid \cdots \mid g_n] \\ - \cdots + (-1)^{n-1}[g_1 \mid \cdots \mid g_{n-2} \mid g_{n-1} g_n] + (-1)^n [g_1 \mid \cdots \mid g_{n-1}], \end{aligned}$$

and $d_0([]) = 1 \in \mathbb{Z}$.

Proposition 5.25. *The bar resolution is a free resolution of $\mathbb{Z}$ by G-modules.*

Proof. First compute $d_n d_{n+1} = 0$ to show that $F_\bullet$ is a chain complex. To prove exactness, we use a "chain homotopy": forget the G-action and define $s_n : F_n \to F_{n+1}$ by

$$s_n(g_0[g_1 \mid \cdots \mid g_n]) = [g_0 \mid g_1 \mid \cdots \mid g_n].$$

Note that this is a homomorphism of abelian groups (but not a G-linear map). Show that $\mathrm{id}_{F_n} = d_{n+1} s_n + s_{n-1} d_n$; this implies that $F_\bullet$ is exact. □

Definition 5.26 (Group of n-cochains)**.** *The group of n-*cochains *of G with coefficients in M is*

$$C^n(G, M) = \{\textit{functions } G^n \to M\} \cong \operatorname{Hom}_G(F_n, M),$$

*where $F_\bullet$ is the bar resolution. The n-*th coboundary map *is $d^n : C^{n-1}(G, M) \to C^n(G, M)$ given by*

$$\begin{aligned} d^n\phi(g_1, \ldots, g_n) = g_1 \phi(g_2, \ldots, g_n) - \phi(g_1 g_2, g_3, \ldots, g_n) + \phi(g_1, g_2 g_3, \ldots, g_n) \\ - \cdots + (-1)^{n-1} \phi(g_1, \ldots, g_{n-2}, g_{n-1} g_n) + (-1)^n \phi(g_1, \ldots, g_{n-1}) \end{aligned}$$

for $\phi : G^{n-1} \to M$.

*The group of n-*cocyles *is $Z^n(G, M) = \operatorname{Ker} d^{n+1}$ and the group of n-*coboundaries *is $B^n(G, M) = \operatorname{Im} d^n$. Since the bar resolution is a free resolution of $\mathbb{Z}$ by G-modules, we have*

$$H^n(G, M) = \frac{Z^n(G, M)}{B^n(G, M)}.$$

Example 5.27. (i) $H^0(G, M) \cong M^G$.

(ii) $H^1(G,M) \cong \frac{\text{crossed homomorphisms}}{\text{principal crossed homorphisms}}$, *where a* crossed homomorphism *is a map* $\phi : G \to M$ *such that*

$$\phi(gh) = g\phi(h) + \phi(g),$$

and a principal crossed homorphism *is one of the form* $\phi(g) = (g-1)m$ *for some* $m \in M$.

Proof. (i) Consider the map $d^1 : C^0(G,M) \to C^1(G,M)$; it is given by $d^1\phi(g) = (g-1)\phi(\cdot)$, so $H^0(G,M) = \operatorname{Ker} d^1 \cong M^G$ under the isomorphism $C^0(G,M) \cong M$.

(ii) Note that d^2 is given by

$$d^2\phi(g,h) = g\phi(h) - \phi(gh) + \phi(g),$$

so $\operatorname{Ker} d^2$ is the set of crossed homomorphisms, and the above shows that $\operatorname{Im} d^1$ is the set of principal crossed homomorphisms. □

5.5 Maps induced by group homomorphisms

Proposition 5.28. *Let* $\alpha : G_1 \to G_2$ *be a group homomorphism. Let* M *be a* G_2*-module, and let* G_1 *act on* M via α. *Then there is a natural homomorphism*

$$\alpha^* : H^n(G_2, M) \to H^n(G_1, M).$$

Proof. Consider the chain groups $C^n(G_2, M)$. Given $f \in C^n(G_2, M)$, set

$$\alpha^* f = \left(G_1^n \xrightarrow{\alpha^n} G_2^n \xrightarrow{f} M \right) \in C^n(G_1, M).$$

These maps α^* form a chain map, so they give maps on cohomology groups. □

Remark 5.29. *Suppose we have a short exact sequence of groups*

$$1 \to H \to G \to Q \to 1.$$

In general, there is no long exact sequence of cohomology groups in the style of the Snake Lemma. For instance, take $H = Q = \mathbb{Z}$ *and* $G = \mathbb{Z}^2$. *A long exact sequence of cohomology groups would have to contain* $0 = H^2(\mathbb{Z},\mathbb{Z}) \to H^2(\mathbb{Z}^2,\mathbb{Z}) \to H^2(\mathbb{Z},\mathbb{Z}) = 0$, *which is impossible because we will prove that* $H^2(\mathbb{Z}^2,\mathbb{Z}) = \mathbb{Z}$.

However, there is some relation to be studied in low dimension (for more on this, see "spectral sequences").

Lemma 5.30. *Let* $H \trianglelefteq G$ *and let* M *be a* G*-module. Let* G *act on* $C^n(H,M)$ via

$$(g \cdot \phi)(h_1, \ldots, h_n) = g\left(\phi\left(g^{-1}h_1 g, \ldots, g^{-1}h_n g\right)\right)$$

for $\phi \in C^n(H,M)$. *This gives an action of* G *on* $H^n(H,M)$. *Moreover,* H *acts trivially, so we can think of it as a* G/H*-action.*

Proof. There is an induced action on cohomology because each g acts as a chain map, i.e.

$$d^n(g \cdot \phi) = g \cdot d^n\phi$$

for $\phi \in C^{n-1}(H,M)$. Moreover, H acts trivially because if $\phi \in Z^n(G,M)$, then $h \cdot \phi - \phi \in \operatorname{Im} d^n$ for all $h \in H$. □

Remark 5.31. *Assume that* M *has trivial* G*-action. Then* $H^1(H,M)$ *is the set of crossed homomorphisms* $\phi : H \to M$, *with* G*-action given by*

$$(g \cdot \phi)(h) = \phi\left(g^{-1}hg\right).$$

An element of $H^1(H,M)^G$ *is called a* G-invariant homomorphism $H \to M$.

Theorem 5.32 (Five term exact sequence)**.** *Suppose we have an exact sequence*

$$1 \to H \to G \to Q \to 1,$$

and let M be a G-module. Then there is an exact sequence

$$0 \to H^1\left(Q, M^H\right) \to H^1(G, M) \to H^1(H, M)^G \to H^2\left(Q, M^H\right) \to H^2(G, M).$$

Sketch of proof. The maps in the exact sequence are constructed as follows:

- Restriction maps $H^n(G, M) \to H^n(H, M)^G$ are given by $\phi \mapsto \phi_{|H}$.
- Inflation maps $H^n\left(Q, M^H\right) \to H^n(G, M)$ are given by $\phi \longmapsto \left(G^n \xrightarrow{\pi^n} Q^n \xrightarrow{\phi} M^H \subseteq M\right)$.
- For the transgression map $Tg : H^1(H, M)^G \to H^2\left(Q, M^H\right)$, choose a set-theoretic section $s : Q \to G$ (this amounts to choosing a set of coset representatives for H), assuming that $s(1) = 1$. Define $\rho : G \to H$ by
$$\rho(g) = g \cdot s(gH)^{-1}.$$
Now if $\phi : H \to M$ is a (Q-invariant) cocycle, define $Tg(\phi) : G^2 \to M$ by
$$Tg(\phi)(g_1, g_2) = \phi(\rho(g_1)\rho(g_2)) - \phi(\rho(g_1 g_2)).$$
In fact, $Tg(\phi)$ induces a map $Q^2 \to M$. □

Corollary 5.33 (Hopf's Formula)**.** *Let F be a free group, $R \trianglelefteq F$ and $Q = F/R$. If A is an abelian group with trivial F-action, then*

$$H^2(Q, A) \cong \frac{\mathrm{Hom}(R, A)^F}{\mathrm{Hom}(F, A)} = \frac{\{f \in \mathrm{Hom}(R, A),\ \forall w \in F,\ \forall r \in R,\ f(w^{-1}rw) = f(r)\}}{\left\{f_{|R},\ f \in \mathrm{Hom}(F, A)\right\}}.$$

Proof. The five-term exact sequence of $1 \to R \to F \to Q \to 1$ can be written as

$$0 \to \mathrm{Hom}(Q, A) \to \mathrm{Hom}(F, A) \to \mathrm{Hom}(R, A)^F \to H^2(Q, A) \to 0.$$ □

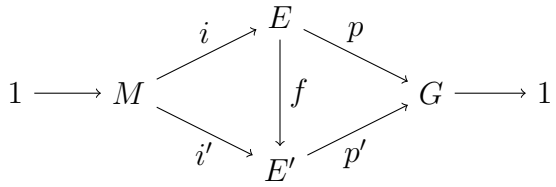
Example 5.34. *Let $Q = \langle x_1, \ldots, x_d \mid r_1, \ldots, r_n \rangle$ be a finitely presented group. Then*

$$\mathrm{rk}\, H^1(Q, \mathbb{Z}) \leqslant d \qquad \text{and} \qquad \mathrm{rk}\, H^2(Q, \mathbb{Z}) \leqslant n.$$

5.6 Cohomology and group extensions

Definition 5.35 (Group extension)**.** *Let E be a group with an abelian normal subgroup M. If $G = E/M$, we say that E is an* extension of G by M.

Two extensions E, E' of G by M are equivalent *if there is a commutative diagram of homomorphisms:*



Lemma 5.36. *Equivalent extensions are isomorphic as groups.*

Proof. We show that the map f of the diagram of Definition 5.35 is an isomorphism.

Injectivity. If $f(e) = 1$, then $p(e) = p'f(e) = 1$, so $e \in \operatorname{Ker} p = \operatorname{Im} i$, and $e = i(m)$ for some $m \in M$. Then $i'(m) = f(i(m)) = f(e) = 1$, so $m = 1$ by injectivity of i' and therefore $e = 1$.

Surjectivity. Let $e' \in E'$. By surjectivity of p, there exists $e \in E$ such that $p(e) = p'(e')$. Hence $p'(f(e)^{-1}e') = p(e)^{-1}p'(e') = 1$, so $f(e)^{-1}e' \in \operatorname{Ker} p' = \operatorname{Im} i'$, and there exists $m \in M$ such that $i'(m') = f(e)^{-1}e'$. Therefore, $e' = f(ei(m)) \in \operatorname{Im} f$ as required. □

Remark 5.37. *Let E be an extension of G by M. Then the conjugation action of E on M reduces to a G-action, so M comes with the structure of a G-module. If the G-action on M is trivial, the extension is called* central.

Definition 5.38 (Split extension)**.** *Let E be an extension of G by M. We say that the extension is* split *if there is a group homomorphism $s : G \to E$ such that $\left(G \xrightarrow{s} E \xrightarrow{p} G\right) = \mathrm{id}_G$.*

Remark 5.39. *Given a G-module M, the semidirect product $E = M \rtimes G$ is an extension of G by M. The underlying set is $M \times G$, and the group operation is defined by*

$$(m_1, g_1)(m_2, g_2) = (m_1 + g_1 \cdot m_2, g_1 g_2).$$

This is a split extension.

Proposition 5.40. *Let M be a G-module. Any extension E of G by M which splits is equivalent to $M \rtimes G$.*

Definition 5.41 (Normalised cocycle)**.** *Let M be a G-module. A cocycle $\phi \in Z^2(G, M)$ is said to be* normalised *if $\phi(1, g) = \phi(g, 1) = 0_M$ for all $g \in G$.*

Lemma 5.42. *Let E be an extension of G by M.*

(i) *Let $s : G \to E$ be a (set-theoretic) section, i.e. a function such that $\left(G \xrightarrow{s} E \xrightarrow{p} G\right) = \mathrm{id}_G$ and $s(1) = 1$. Consider $\phi \in C^2(G, M)$ defined by*

$$\phi(g_1, g_2) = s(g_1)\, s(g_2)\, s(g_1 g_2)^{-1} \in M.$$

Then $\phi \in Z^2(G, M)$. Moreover, ϕ is a normalised cocycle.

(ii) *If $s' : G \to E$ is another section and ϕ' is the corresponding cocycle, then*

$$\phi - \phi' \in B^2(G, M).$$

Proof. (i) The definition of ϕ can be rewritten as

$$\phi(g_1, g_2)\, s(g_1 g_2) = s(g_1)\, s(g_2).$$

Using this, we compute $s(g_1)\, s(g_2)\, s(g_3)$ in two different ways:

$$s(g_1)\, s(g_2)\, s(g_3) = \phi(g_1, g_2)\, s(g_1 g_2)\, s(g_3) = \phi(g_1, g_2)\, \phi(g_1 g_2, g_3)\, s(g_1 g_2 g_3),$$

and

$$\begin{aligned} s(g_1)\, s(g_2)\, s(g_3) &= s(g_1)\, \phi(g_2, g_3)\, s(g_2 g_3) = s(g_1)\, \phi(g_2, g_3)\, s(g_1)^{-1}\, s(g_1)\, s(g_2 g_3) \\ &= s(g_1)\, \phi(g_2, g_3)\, s(g_1)^{-1}\, \phi(g_1, g_2 g_3)\, s(g_1 g_2 g_3). \end{aligned}$$

Comparing these two equalities yields

$$\phi(g_1, g_2)\, \phi(g_1 g_2, g_3) = s(g_1)\, \phi(g_2, g_3)\, s(g_1)^{-1}\, \phi(g_1, g_2 g_3),$$

or in additive notation in $(M,+)$,

$$\phi(g_1,g_2)+\phi(g_1g_2,g_3)=g_1\cdot\phi(g_2,g_3)+\phi(g_1,g_2g_3),$$

i.e. $d^3\phi=0$.

(ii) Define $\psi\in C^1(G,M)$ by

$$\psi(g)=s'(g)s(g)^{-1}\in M.$$

Then

$$\begin{aligned}s'(g_1)s'(g_2)&=\psi(g_1)s(g_1)\psi(g_2)s(g_2)=\psi(g_1)s(g_1)\psi(g_2)s(g_1)^{-1}s(g_1)s(g_2)\\&=\psi(g_1)s(g_1)\psi(g_2)s(g_1)^{-1}\phi(g_1,g_2)s(g_1g_2)\\&=\psi(g_1)s(g_1)\psi(g_2)s(g_1)^{-1}\phi(g_1,g_2)\psi(g_1g_2)^{-1}s'(g_1g_2).\end{aligned}$$

Therefore, in additive notation in $(M,+)$,

$$\phi'(g_1,g_2)=\psi(g_1)+g_1\cdot\psi(g_2)+\phi(g_1,g_2)-\psi(g_1,g_2)=\phi(g_1g_2)+d^2\psi(g_1,g_2).$$ □

Lemma 5.43. *Let M be a G-module. Then every cohomology class in $H^2(G,M)$ is represented by some normalised cocycle.*

Proof. Let $\phi\in Z^2(G,M)$ and define $\psi\in C^1(G,M)$ by $\psi(g)=\phi(1,g)$. We claim that $\phi-d^2\psi$ is normalised. Indeed,

$$\begin{aligned}\left(\phi-d^2\psi\right)(1,g)&=\phi(1,g)-(1\cdot\phi(1,g)-\phi(1,1g)+\phi(1,1))=\phi(1,g)-\phi(1,1),\\\left(\phi-d^2\psi\right)(g,1)&=\phi(g,1)-g\cdot\phi(1,1).\end{aligned}$$

These two are both zero because $\phi\in Z^2(G,M)$, so we have for instance,

$$0=d^3\phi(1,1,g)=1\cdot\phi(1,g)-\phi(1,g)+\phi(1,g)-\phi(1,1)=\phi(1,g)-\phi(1,1).$$ □

Theorem 5.44. *Let M be a G-module. Then the set of equivalence classes of extensions of G by M is in bijection with $H^2(G,M)$.*

Proof. By Lemma 5.42, we can associate an element of $H^2(G,M)$ to each extension of G by M; moreover, equivalent extensions give the same element of $H^2(G,M)$. We now need to construct an inverse map.

Let $[\phi]\in H^2(G,M)$, where ϕ is a normalised cocycle. Define a group structure on the set $M\times G$ by

$$(m_1,g_1)(m_2,g_2)=(m_1+g_1\cdot m_2+\phi(g_1,g_2),g_1g_2).$$

Using the facts that $d^3\phi=0$ and ϕ is normalised, we check that this is a well-defined group operation on $M\times G$. Moreover, this is an extension E_ϕ of G by M. Now if ϕ' is a normalised cocycle such that $\phi-\phi'=d^2\psi$, then the map

$$(m,g)\in E_\phi\longmapsto(m+\psi(g),g)\in E_{\phi'}$$

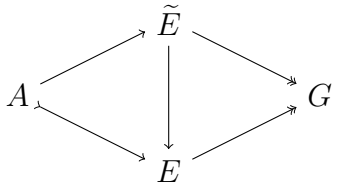
is an equivalence of extensions. □

Remark 5.45. *Suppose that G has a presentation $G=\langle x_1,\dots,x_n\mid r_1,\dots,r_m\rangle$. Let A be an abelian group with trivial G-action. Let F be the free group on $\{x_1,\dots,x_n\}$ and $R=\operatorname{Ker}(F\twoheadrightarrow G)$.*

Let E be a central extension of G by A. Choose some preimage $\overline{x}_i\in E$ of each generator x_i of G. Let $\overline{r}_i$ be the element of E given by replacing each occurrence of x_i in r_i with $\overline{r}_i$. Then $\overline{r}_i\in A=\operatorname{Ker}(E\twoheadrightarrow G)$. Consider the group

$$\widetilde{E}=\langle\overline{x}_1,\dots,\overline{x}_n,A\mid\overline{r}_1,\dots,\overline{r}_m,A\text{ central, relations of }A\rangle.$$

Then there is a commutative diagram:



It follows that $\widetilde{E} \cong E$, so we have a group presentation for E.

Now we define an F-invariant homomorphism $R \to A$ by $r_i \mapsto \overline{r}_i$. We check that this is well-defined. We made a choice of preimages $\overline{x}_i$; had we made a different choice, the resulting homomorphisms $R \to A$ would have differed by a homomorphism $F \to A$.

This gives a correspondance between equivalence classes of extensions of G by A and elements of $\frac{\mathrm{Hom}(R,A)^F}{\mathrm{Hom}(F,A)}$, in agreement with Hopf's Formula (Corollary 5.33).

Example 5.46. *Let $G = \left\langle x_1, x_2 \mid x_1 x_2 x_1^{-1} x_2^{-1} x_1 \right\rangle$. Then $H^2(G, \mathbb{Z}) = 0$.*

Proof. Consider a central extension E of G by $\mathbb{Z}$. Following the argument of Remark 5.45, E has a presentation of the form

$$E = \left\langle \overline{x}_1, \overline{x}_2, t \mid \overline{x}_1 \overline{x}_2 \overline{x}_1^{-1} \overline{x}_2^{-1} \overline{x}_1 t^{-k}, t \text{ central} \right\rangle$$

for some $k \in \mathbb{Z}$. By substituting $\overline{x}_1 \mapsto \overline{x}_1 t^{-k} = \widetilde{x}_1$, we obtain

$$\begin{aligned} E &\cong \left\langle \widetilde{x}_1, \overline{x}_2, t \mid \widetilde{x}_1 t^k \overline{x}_2 t^{-k} \widetilde{x}_1 \overline{x}_2^{-1} \widetilde{x}_1 t^k t^{-k}, t \text{ central} \right\rangle \\ &\cong \left\langle \widetilde{x}_1, \overline{x}_2, t \mid \widetilde{x}_1 \overline{x}_2 \widetilde{x}_1^{-1} \overline{x}_2^{-1} \widetilde{x}_1^{-1}, t \text{ central} \right\rangle \\ &\cong \mathbb{Z} \times G. \end{aligned}$$

Hence all extensions of G by $\mathbb{Z}$ are split, so $H^2(G, \mathbb{Z}) = 0$ by Theorem 5.44. □

5.7 Worked example: central extensions of $\mathbb{Z}^2$

Example 5.47. *All central extensions of $\mathbb{Z}^2$ by $\mathbb{Z}$ are equivalent to a group*

$$\left\{ \begin{pmatrix} 1 & pr & m \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix}, \ r, s, m \in \mathbb{Z} \right\},$$

where the chosen central copy of $\mathbb{Z}$ is generated by the above matrix for $r = s = 0$ and $m = 1$.

Proof. Write $T = \mathbb{Z}^2 = \langle a, b \rangle$ with multiplicative notation. We begin with the free resolution

$$0 \to \mathbb{Z}T \xrightarrow{\beta} (\mathbb{Z}T)^2 \xrightarrow{\alpha} \mathbb{Z}T \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

where ε is the augmentation map, given by $1 \mapsto 1$; $\alpha(x, y) = x(a-1) + y(b-1)$, and $\beta(z) = (z(1-b), z(a-1))$. We check that this is indeed exact. Hence, to compute $H^*(T, \mathbb{Z})$, we apply $\mathrm{Hom}_T(-, \mathbb{Z})$:

$$0 \leftarrow \mathrm{Hom}_T(\mathbb{Z}T, \mathbb{Z}) \xleftarrow{\beta^*} \mathrm{Hom}_T\left((\mathbb{Z}T)^2, \mathbb{Z}\right) \xleftarrow{\alpha^*} \mathrm{Hom}_T(\mathbb{Z}T, \mathbb{Z}).$$

We check that $\alpha^* = 0$ and $\beta^* = 0$ (using the fact that the T-action on $\mathbb{Z}$ is trivial). It follows that

$$H^2(T, \mathbb{Z}) \cong \mathbb{Z} \quad \text{and} \quad H^1(T, \mathbb{Z}) \cong \mathbb{Z}^2 \quad \text{and} \quad H^0(T, \mathbb{Z}) \cong \mathbb{Z}.$$

Next, we compare the above free resolution with the bar resolution, using the method of Theorem 5.23. We want to construct maps f_1, f_2 such that the following diagram commutes:

$$\begin{array}{ccccccccc}
\mathbb{Z}T\{T^{(2)}\} & \xrightarrow{d_2} & \mathbb{Z}T\{T^{(1)}\} & \xrightarrow{d_1} & \mathbb{Z}T\{T^{(0)}\} & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0 \\
\downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
\mathbb{Z}T & \xrightarrow{\beta} & (\mathbb{Z}T)^2 & \xrightarrow{\alpha} & \mathbb{Z}T & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

Introduce the notation

$$S(c,r) = \begin{cases} 1 + c + \cdots + c^{r-1} & \text{if } r \geqslant 0 \\ -c^{-1} - \cdots - c^{r} & \text{if } r < 0 \end{cases} \in \mathbb{Z}T$$

for $c \in \{a, b\}$, so that $(c-1)S(c,r) = c^r - 1$. Now define f_1, f_2 by

$$\begin{aligned} f_1 : [a^r b^s] &\longmapsto (b^s S(a,r), S(b,s)) \\ f_2 : \left[a^r b^s \mid a^t b^u\right] &\longmapsto S(a,r) b^s S(b,u). \end{aligned}$$

Now, let us find a cocycle $\phi \in Z^2(T, \mathbb{Z})$ representing a cohomology class $p \in \mathbb{Z} \cong \mathrm{Hom}_T(\mathbb{Z}T, \mathbb{Z}) \cong H^2(T, \mathbb{Z})$. Such a cocycle is given by the composition $\left(T^2 \xrightarrow{f_2} \mathbb{Z}T \xrightarrow{p\cdot\varepsilon} \mathbb{Z}\right)$. We find

$$\phi\left(a^r b^s, a^t b^u\right) = pru.$$

The group structure on $\mathbb{Z} \times T$ corresponding to this cocycle is given by

$$(m, a^r b^s) \star \left(n, a^t b^u\right) = \left(m + n + pru, a^{r+t} b^{s+u}\right).$$

This is isomorphic to the given matrix group. □

5.8 Cohomology of profinite groups

Definition 5.48 (Finite G-module)**.** *Let G be a profinite group. A* finite G-module *is a finite abelian group M with a continuous G-action $G \times M \to M$.*

Definition 5.49 (Cohomology of profinite groups)**.** *Let G be a profinite group and let M be a finite G-module. We define $C^n(G, M)$ to be the set of continuous functions $G^n \to M$, and $d^n : C^{n-1}(G, M) \to C^n(G, M)$ with the same formula as in Definition 5.26. We can then define*

$$H^n(G, M) = \operatorname{Ker} d^{n+1} / \operatorname{Im} d^n.$$

Remark 5.50. *All general results about the cohomology of abstract groups will remain true for profinite groups, where all groups are assumed to be profinite, all functions are assumed to be continuous, and all G-modules are assumed to be finite.*

Remark 5.51. (i) *We restrict our attention to continuous maps, because for instance* $\mathrm{Hom}\left(\hat{\mathbb{Z}}, M\right)$ *is nice only when homomorphisms are assumed to be continuous.*

(ii) *We restrict our attention to finite G-modules, because otherwise bad things may happen: writing the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ with trivial $\hat{\mathbb{Z}}$-action, computing the cohomology groups and writing the induced long exact sequence yields $H^2\left(\hat{\mathbb{Z}}, \mathbb{Z}\right) \neq 0$. This is bad: free profinite groups should have cohomological dimension* 1.

5.9 Cohomological dimension of pro-p groups

Definition 5.52 (Cohomological dimension)**.** *A profinite group G has cohomological dimension n, and we write* $\mathrm{cd}(G) = n$*, if $H^m(G, M) = 0$ for all $m > n$ and for all finite G-modules M, but there exists a finite G-module M such that $H^n(G, M) \neq 0$.*

Example 5.53. *The only pro-p group G such that $H^1(G, \mathbb{F}_p) = 0$ is the trivial group.*

Therefore, non-trivial pro-p groups have cohomological dimension at least 1.

Definition 5.54 (Simple G-module)**.** *A G-module M is* simple *if its only G-submodules are* 0 *and M.*

Proposition 5.55. *Let G be a profinite group such that $H^n(G, S) = 0$ for all simple finite G-modules S. Then $H^n(G, M) = 0$ for all finite G-modules M.*

Proof. Suppose the result is not true and take M of minimal size such that $H^n(G, M) \neq 0$. Then M is not simple, so there exists a proper non-trivial submodule $N \leqslant M$. We have a short exact sequence

$$0 \to N \to M \to M/N \to 0$$

of G-modules. Proposition 5.22 gives a long exact sequence in cohomology:

$$\cdots \to H^n(G, N) \to H^n(G, M) \to H^n(G, M/N) \to \cdots .$$

But $H^n(G, N) = H^n(G, M/N) = 0$, and therefore $H^n(G, M) = 0$, a contradiction. □

Definition 5.56 (p-primary component)**.** *Given a finite G-module M and a prime p, the* p-primary component *of M is its p-Sylow subgroup M_p. Hence*

$$M = \bigoplus_{p \text{ prime}} M_p.$$

Proposition 5.57. *Let G be a pro-p group and let M be a finite G-module. Then for $n \geqslant 1$,*

$$H^n(G, M) = H^n(G, M_p).$$

Proof. We have $M = M_p \oplus M'$ where $M' = \bigoplus_{q \neq p} M_q$. Therefore

$$H^n(G, M) = H^n(G, M_p) \oplus H^n(G, M').$$

We will prove that $H^n(G, M') = 0$. We first note that this is true if G is a finite p-group. Then we take a continuous function $\phi : G^n \to M'$.

We claim that ϕ factors as $G^n \to (G/K)^n \xrightarrow{\phi_K} M$ for some open normal subgroup $K \trianglelefteq G$. To prove this claim, we need to find K such that $\phi^{-1}(m)$ is a union of cosets of K^n for all $m \in M$. But for $m \in M$, $\phi^{-1}(m)$ is open and closed in G, so it is a union of cosets of open subgroups of G^n. By compactness, we need only finitely many such cosets $\left(g_{i,m} + K_{i,m}^n\right)_{1 \leqslant i \leqslant r_m}$ to cover $\phi^{-1}(m)$. It now suffices to take $K = \bigcap_{m,i} K_{i,m}$. This proves the claim.

But G/K is a finite p-group so $H^n(G/K, M') = 0$. Hence there exists $\psi_K : (G/K)^{n-1} \to M$ such that $\phi_K = d^n \psi_K$. Now set $\psi : G^{n-1} \to (G/K)^{n-1} \xrightarrow{\psi_K} M'$, so that $\phi = d^n \psi$. □

Remark 5.58. *The middle section of the proof of Proposition 5.57 actually shows that*

$$H^n\left(\varprojlim G/K, M\right) = \varinjlim H^n(G/K, M).$$

Proposition 5.59. *If G is a pro-p group, then the only simple p-primary G-module is $\mathbb{F}_p$.*

Proposition 5.60. *If G is a pro-p group such that $H^n(G, \mathbb{F}_p) = 0$, then $H^n(G, M) = 0$ for all finite G-modules M.*

Proposition 5.61. *Suppose that there exists $N \geqslant 0$ such that $H^N(G, M) = 0$ for all G-modules M. Then* $\mathrm{cd}(G) \leqslant N - 1$.

Proof. We prove the result for abstract groups G. If M is a G-module, consider $\mathrm{Hom}(\mathbb{Z}G, M)$. This is a G-module (called the *conduced module*) with

$$(g \cdot f)(x) = f(xg)$$

for $f \in \mathrm{Hom}(\mathbb{Z}G, M)$ and $x \in \mathbb{Z}G$. We can prove that $H^n(G, \mathrm{Hom}(\mathbb{Z}G, M)) = H^n(1, M) = 0$ for $n \geqslant 1$.

Now there is an injective map

$$\alpha : m \in M \longmapsto (x \mapsto xm) \in \mathrm{Hom}(\mathbb{Z}G, M).$$

If $M' = \mathrm{Hom}(\mathbb{Z}G, M)/M$, we have a short exact sequence $0 \to M \to \mathrm{Hom}(\mathbb{Z}G, M) \to M' \to 0$, inducing a long exact sequence in cohomology

$$\cdots \to H^N(G, \mathrm{Hom}(\mathbb{Z}G, M)) \to H^N(G, M') \to H^{N+1}(G, M) \to H^{N+1}(G, \mathrm{Hom}(\mathbb{Z}G, M)) \to \cdots.$$

Hence $H^{N+1}(G, M) = 0$ for all M. □

Theorem 5.62. *Let G be a pro-p group. Then*

$$\mathrm{cd}(G) = \max\{n \geqslant 0,\ H^n(G, \mathbb{F}_p) \neq 0\}.$$

5.10 Pro-p groups of cohomological dimension 1

Notation 5.63. *From now on, all pro-p groups will be assumed to be topologically finitely generated.*

Corollary 5.64. *Free topologically finitely generated pro-p groups have cohomological dimension 1.*

Proof. Let $G = F(X)$ be the free pro-p group on the finite set X. By Theorem 5.62, it suffices to prove that $H^2(F(X), \mathbb{F}_p) = 0$ – i.e. every extension of $F(X)$ by $\mathbb{F}_p$ splits. Hence, consider an extension

$$1 \to \mathbb{F}_p \to E \to F(X) \to 1.$$

E must be a pro-p group. For each $x \in X$, choose a preimage $e_x \in E$ of x by $E \to F(X)$; then define $F(X) \to E$ by $x \mapsto e_x$ (this is possible by the universal property of free pro-p groups). Hence, E splits. □

Remark 5.65. *The proof of Corollary 5.64 can be used to show that free (abstract) groups have cohomological dimension 1 (c.f. Proposition 5.14).*

Theorem 5.66. *Let $f : G \to G'$ be a continuous homomorphism between topologically finitely generated pro-p groups. Assume that:*

(i) *$f^* : H^1(G', \mathbb{F}_p) \to H^1(G, \mathbb{F}_p)$ is an isomorphism,*

(ii) *$f^* : H^2(G', \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ is injective.*

Then f is an isomorphism.

Proof. Consider the lower central p-series $(G_n)_{n\geqslant 1}$ of G and $(G'_n)_{n\geqslant 1}$ of G' – recall that this is defined by $G_1 = G$ and $G_{n+1} = \overline{[G_n, G]\, G_n^p}$. The subgroups $(G_n)_{n\geqslant 1}$ are open in G and

$$G = \varprojlim_{n\geqslant 0} G/G_n,$$

and similarly for G' (by Remark 4.24.(iv) and Lemma 2.30). This is fully characteristic, in particular $f(G_n) \subseteq G'_n$ for all n. It follows that there are quotient maps $f_n : G/G_n \to G'/G'_n$. It is enough to show that f_n is an isomorphism for all n (hence, f will also be an isomorphism).

We prove by induction on n that f_n is an isomorphism. For $n = 2$, we have $G/G_2 = G/\Phi(G)$, and

$$H^1(G, \mathbb{F}_p) \cong \mathrm{Hom}(G, \mathbb{F}_p) \cong \mathrm{Hom}(G/\Phi(G), \mathbb{F}_p);$$

hence, $f_2 : G/G_2 \to G'/G'_2$ is a map of $\mathbb{F}_p$-vectors spaces whose dual is $f^* : H^1(G', \mathbb{F}_p) \to H^1(G, \mathbb{F}_p)$. Since the latter is an isomorphism, so is f_2. Now assume that f_n is an isomorphism. Note that G_n/G_{n+1} is a finite-dimensional vector space over $\mathbb{F}_p$. Therefore, the induced map $G_n/G_{n+1} \to G'_n/G'_{n+1}$ is an isomorphism if and only if its dual $H^1\left(G'_n/G'_{n+1}, \mathbb{F}_p\right) = \mathrm{Hom}\left(G'_n/G'_{n+1}, \mathbb{F}_p\right) \to \mathrm{Hom}(G_n/G_{n+1}, \mathbb{F}_p) = H^1(G_n/G_{n+1}, \mathbb{F}_p)$ is an isomorphism. Now note that a homomorphism $\phi : G_n \to \mathbb{F}_p$ factors through G_n/G_{n+1} if and only if $\phi([g, g']) = 0$ for all $g \in G$ and $g' \in G_n$, or equivalently

$$0 = \phi\left(g^{-1}(g')^{-1}gg'\right) = -\phi\left(g^{-1}g'g\right) + \phi(g'),$$

i.e. if and only if ϕ is G-invariant. Therefore,

$$H^1(G_n/G_{n+1}, \mathbb{F}_p) = H^1(G_n, \mathbb{F}_p)^G.$$

But Theorem 5.32 (applied to the short exact sequence $1 \to G_n \to G \to G/G_n \to 1$) implies that there is a commutative diagram with exact rows (all cohomology groups are with $\mathbb{F}_p$-coefficients):

$$\begin{array}{ccccccccc}
H^1(G/G_n) & \longrightarrow & H^1(G) & \longrightarrow & H^1(G_n)^G & \longrightarrow & H^2(G/G_n) & \longrightarrow & H^2(G) \\
f^*\uparrow\cong & & f^*\uparrow\cong & & f^*\uparrow & & f^*\uparrow\cong & & f^*\uparrow\hookrightarrow \\
H^1(G'/G'_n) & \longrightarrow & H^1(G') & \longrightarrow & H^1(G'_n)^{G'} & \longrightarrow & H^2(G'/G'_n) & \longrightarrow & H^2(G')
\end{array}$$

The red arrows are isomorphisms by induction, and the blue ones are an isomorphism and a monomorphism by assumption. The Five Lemma implies that $f^* : H^1(G'_n, \mathbb{F}_p)^{G'} \to H^1(G_n, \mathbb{F}_p)^G$ is an isomorphism. But we have seen that this map is dual to the map $G_n/G_{n+1} \to G'_n/G'_{n+1}$ induced by f, so the latter is also an isomorphism. Finally, we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & G_n/G_{n+1} & \longrightarrow & G/G_{n+1} & \longrightarrow & G/G_n & \longrightarrow & 1 \\
 & & \uparrow\cong & & f_{n+1}\uparrow & & f_n\uparrow\cong & & \\
1 & \longrightarrow & G'_n/G'_{n+1} & \longrightarrow & G'/G'_{n+1} & \longrightarrow & G'/G'_n & \longrightarrow & 1
\end{array}$$

It follows that f_{n+1} is an isomorphism. □

Theorem 5.67. *Let $f : \Gamma \to \Gamma'$ be a homomorphism between finitely generated abstract groups. Assume that:*

(i) *$f^* : H^1(\Gamma', \mathbb{F}_p) \to H^1(\Gamma, \mathbb{F}_p)$ is an isomorphism,*

(ii) *$f^* : H^2(\Gamma', \mathbb{F}_p) \to H^2(\Gamma, \mathbb{F}_p)$ is injective.*

Then $\hat{f} : \hat{\Gamma}_{(p)} \to \hat{\Gamma}'_{(p)}$ is an isomorphism of pro-p completions.

Proof. Consider the lower central p-series $(\Gamma_n)_{n \geqslant 0}$ of Γ, so that $\hat{\Gamma}_{(p)} = \varprojlim_{n \geqslant 0} \Gamma/\Gamma_n$ and proceed as in Theorem 5.66. □

Corollary 5.68. *If G is a topologically finitely generated pro-p group with $H^2(G, \mathbb{F}_p) = 0$, then G is free.*

Proof. Let $d = d(G)$ and take a topological generating set $X = \{x_1, \ldots, x_d\}$ for G. Let F be the free pro-p group on X. Consider the map $f : F \to G$ given by $x_i \mapsto x_i$. Note that the map

$$\mathbb{F}_p^d \cong F/\Phi(F) \longrightarrow G/\Phi(G) \cong \mathbb{F}_p^d$$

is an isomorphism, so the dual map $H^1(G, \mathbb{F}_p) \to H^1(F, \mathbb{F}_p)$ is an isomorphism. Moreover, $0 = H^2(G, \mathbb{F}_p) \hookrightarrow H^2(F, \mathbb{F}_p)$ is injective, so Theorem 5.66 implies that f is an isomorphism. □

Example 5.69. *Consider* $G = \left\langle x_1, x_2 \mid x_1 x_2 x_1^{-1} x_2^{-1} x_1 \right\rangle$ *as in Example 5.46. Then* $\hat{G}_{(p)} \cong \mathbb{Z}_p$.

Proof. The argument of Example 5.46 also shows that $H^2(G, \mathbb{F}_p) = 0$. Let us determine $H^1(G, \mathbb{F}_p) = \mathrm{Hom}(G, \mathbb{F}_p)$: if $\phi : G \to \mathbb{F}_p$ is a homomorphism, then $0 = \phi\left(x_1 x_2 x_1^{-1} x_2^{-1} x_1\right) = \phi(x_1)$. It follows that $H^1(G, \mathbb{F}_p) \cong \mathbb{F}_p$, with generator given by $x_1 \mapsto 0$ and $x_2 \mapsto 1$.

Now consider the homomorphism $f : \mathbb{Z} \to G$ given by $1 \mapsto x_2$. Then $f^* : H^1(G, \mathbb{F}_p) \to H^1(\mathbb{Z}, \mathbb{F}_p)$ is an isomorphism, $f^* : 0 = H^2(G, \mathbb{F}_p) \to H^2(\mathbb{Z}, \mathbb{F}_p)$ is injective, so Theorem 5.67 implies that $\hat{f} : \mathbb{Z}_p \to \hat{G}_{(p)}$ is an isomorphism of pro-p completions. □

5.11 Presentations of pro-p groups

Definition 5.70 (Presentation for a pro-p group)**.** *Let X be a finite set and let F be the free pro-p group on X. Let $R \subseteq F$. The pro-p group with presentation $\lfloor X \mid R \rfloor_p$ is defined by*

$$\lfloor X \mid R \rfloor_p = F / \overline{\langle\langle R \rangle\rangle}.$$

Lemma 5.71. *Let F_{abs} (resp. F) be the free abstract (resp. pro-p) group on a finite set X and let $R \subseteq F_{\mathrm{abs}} \subseteq F$. If $\Gamma = \langle X \mid R \rangle$ and $G = \lfloor X \mid R \rfloor_p$, then*

$$G = \hat{\Gamma}_{(p)}.$$

Proof. We show that G and Γ have the same p-quotients:

- A quotient $\Gamma \to P$ (where P is a finite p-group) corresponds to a function $X \to P$ such that $f(r) = 1$ for all $r \in R$ after extending to $f : F_{\mathrm{abs}} \to P$.
- A quotient $G \to P$ (where P is a finite p-group) corresponds to a function $X \to P$ such that $\hat{f}(r) = 1$ for all $r \in R$ after extending to $f : F \to P$.

The two groups have the same quotients, so the pro-p version of Theorem 3.14 implies the result. □

Lemma 5.72. *Let G and L be profinite groups with $G \neq 1$. Assume that $L \curvearrowright G$ continuously by automorphisms. Then there is a proper open (normal) subgroup of G which is L-invariant.*

Proof. Denote by $\rho : L \times G \to G$ the (continuous) map corresponding to the action $L \curvearrowright G$. Consider a proper open (normal) subgroup U of G (which exists because G is profinite so it has a finite quotient) and set

$$\widetilde{L} = \{\ell \in L,\ \ell \cdot U = U\} = \{\ell \in L,\ \ell \cdot U \subseteq U\}.$$

We claim that $\widetilde{L}$ is open in L. If this is true, then the Orbit-Stabiliser Theorem implies that the set $\{\ell \cdot U,\ \ell \in L\}$ is finite, so $\bigcap_{\ell \in L} \ell \cdot U$ is an L-invariant open (normal) subgroup.

To prove the claim, let $\ell \in \widetilde{L}$. For each $u \in U$, we have $\ell \cdot u \in U$, i.e. $(\ell, u) \in \rho^{-1}(U)$. Since $\rho^{-1}(U)$ is open in $L \times U$, there exists A_u open in L and B_u open in U such that

$$(\ell, u) \in A_u \times B_u \subseteq \rho^{-1}(U).$$

Since U is compact and $U = \bigcup_{u \in U} B_u$, there is a finite subset $J \subseteq U$ such that $U = \bigcup_{u \in J} B_u$. Consider the open set $A = \bigcap_{u \in J} A_u \ni \ell$ and note that $A \subseteq \widetilde{L}$: if $a \in A$ and $u \in U$, then there exists $v \in J$ such that $u \in B_v$, so $(a, u) \in A_v \times B_v \subseteq \rho^{-1}(U)$, i.e. $a \cdot u \in U$. □

Lemma 5.73. *Let F be a free pro-p group and $N \trianglelefteq F$ be a closed proper normal subgroup of F. Then the following assertions are equivalent.*

(i) *There is a set $R \subseteq N$ of size r s.t. $N = \overline{\langle\langle R \rangle\rangle}$.*

(ii) $\dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^F \leqslant r$.

Proof. Observe first that $H^1(N,\mathbb{F}_p)^F = \mathrm{Hom}(N,\mathbb{F}_p)^F$ is the set of homomorphisms $\phi : N \to \mathbb{F}_p$ such that

$$\phi\left(f^{-1}nf\right) = \phi(n)$$

for all $n \in N$ and $f \in F$; this is in bijection with the set of homomorphisms $N/N^p[N,F] \to \mathbb{F}_p$.

(i) $\Rightarrow$ (ii) Assume that $N = \overline{\langle\langle R\rangle\rangle}$. Note that an F-invariant map $\phi : N \to \mathbb{F}_p$ is determined by what it does to R; hence there is an injection $H^1(N,\mathbb{F}_p)^F \hookrightarrow \mathbb{F}_p^{|R|}$, so $\dim_{\mathbb{F}_p} H^1(N,\mathbb{F}_p)^F \leqslant |R|$.

(ii) $\Rightarrow$ (i) Suppose that $\dim_{\mathbb{F}_p} H^1(N,\mathbb{F}_p)^F = r$. Since the $\mathbb{F}_p$-vector space $H^1(N,\mathbb{F}_p)^F$ is dual to $N/N^p[N,F]$ by the above observation, it follows that $N/N^p[N,F]$ has dimension r as well. Therefore, we may choose a subset $R \subseteq N$ of size r whose image is a basis of $N/N^p[N,F]$. Note that R has the property that every homomorphism $N \to \mathbb{F}_p$ which kills R is the trivial homomorphism. Now suppose for contradiction that $N' = \overline{\langle\langle R\rangle\rangle} \subsetneq N$. Then $N'\Phi(N) \subsetneq N$, so $M = N/N'\Phi(N) \neq 0$. But M is an abelian pro-p group with a continuous action of F, so Lemma 5.72 implies that M has an F-invariant proper open subgroup U. Hence, M/U is a finite F-module which is an abelian p-group. It follows that there is an F-invariant map $M/U \to \mathbb{F}_p$, inducing a nontrivial map $N \to \mathbb{F}_p$ which kills all of R. This is a contradiction. □

Theorem 5.74. *Let G be a pro-p group with a finite topological generating set X. Let r_X be the minimal size of a set $R \subseteq F(X)$ such that $G = \lfloor X \mid R\rfloor_p$. Then*

$$|X| - r_X = \dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p) - \dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p).$$

In particular, if X is of minimal size, then

$$r_X = \dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p).$$

Proof. Let $N = \mathrm{Ker}(F \twoheadrightarrow G)$, where F is the free pro-p group on X. By Theorem 5.32, the short exact sequence $1 \to N \to F \to G \to 1$ induces a five-term exact sequence

$$0 \to H^1(G,\mathbb{F}_p) \to \underbrace{H^1(F,\mathbb{F}_p)}_{\dim=|X|} \xrightarrow{\alpha} \underbrace{H^1(N,\mathbb{F}_p)^F}_{\dim=r_X} \xrightarrow{\beta} H^2(G,\mathbb{F}_p) \to H^2(F,\mathbb{F}_p) = 0.$$

Therefore,

$$|X| - \dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p) = \dim \mathrm{Im}\,\alpha = \dim \mathrm{Ker}\,\beta = r_X - \dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p).$$

For the second assertion, note that if X is of minimal size, then

$$|X| = \dim_{\mathbb{F}_p} G/\Phi(G) = \dim_{\mathbb{F}_p} \mathrm{Hom}(G/\Phi(G),\mathbb{F}_p) = \dim_{\mathbb{F}_p} \mathrm{Hom}(G,\mathbb{F}_p) = \dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p). \quad \square$$

Remark 5.75. *For an abstract group Γ with a generating set X, we may consider the minimal size ρ_X of a set $R \subseteq F(X)$ such that $\Gamma = \langle X \mid R\rangle$. But we have no result as strong as Theorem 5.74:*

- *The number $|X| - \rho_X$ can depend on X.*
- *For a finite p-group $\Gamma = \langle X\rangle$, we certainly have $r_X \leqslant \rho_X$. But the converse inequality is not known.*

References

[1] K. Brown. *Cohomology of Groups.*

[2] L. Ribes and P. Zalesskii. *Profinite Groups.*

[3] J.-P. Serre. *Cohomologie Galoisienne.*

[4] J.S. Wilson. *Profinite Groups.*