University of
Cambridge

Mathematics Tripos

Part III

Profinite Groups

Lent, 2020

Lectures by
G. R. Wilkes

Notes by
Qiangru Kuang

Contents

0 Introduction

Question: how can we tell when two objects are different? This is in general a difficult question and to answer it we need a variety of techniques.

- $\mathbb{N} \cong \mathbb{Q}$ is easier thatn $\mathbb{Q} \ncong \mathbb{R}$.
- To show two finite dimensional vector spaces are not isomorphic we can compute their dimensions.
- For simplicial complexes, we can compute that homology groups $H_n(X)$. Note that this is a partial invariant, in contrast to dimensiona which is a complete invariant for finite dimensional spaces.
- We can also consider $\pi_1(X)$. However in contrast to $H_1(X)$, $\pi_1(X)$ is not necessarily abelian. The Adian-Rabin theorem says that there can be no algorithm which decides if a finitely presented group is trivial or not. Can we build algorithm which sometimes work? We can solve the problem for finite groups. For infinite groups we can build upon this idea. We can write out the lists of finite quotiesnts of two groups G_1 and G_2 and compare them. The question: when does this work?

  Before we answer this question, note that a list of quotient groups is a very unpleasant object. Instead, we can combine this list into a single "limiting" object, called the profinite completion. This technique works in other situations:

  - p-adic integers $\mathbb{Z}_p$ being the "limit" of $\mathbb{Z}/p^n\mathbb{Z}$,
  - Galois theory: let

    $$\begin{aligned} K &= \mathbb{Q}(n\text{th root of unit for all } n) \\ K_N &= \mathbb{Q}(n\text{th root of unit for } n \leq N) \end{aligned}$$

    Then $K = \bigcup K_N$ and is a Galois extension over $\mathbb{Q}$ so we can consider $\text{Gal}(K/\mathbb{Q})$, which is the "limit" of $\text{Gal}(K_n/\mathbb{Q})$.
  - étale fundamental groups in algebraic geometry.

Aside from profinite groups, we will also study group cohomolgy in this course. It is another invariant of groups. This is related to the homology of a simplicial complex and gives abelian invariants. Among other things, it tells if a group is free. It answers the question: given a group G and an abelian group A, how many groups E exists such that $A \trianglelefteq E$ and $E/A \cong G$?

1 Inverse limits

1.1 Categories & Limits

Recap on categories and limits. Refer to III Category Theory.

1.2 Inverse limits and profinite groups

> **Definition** (profinite completion)**.** Let G be a group. Let $\mathbf{N}$ be the category whose objects are finite index normal subgroups $N \trianglelefteq_f G$ and with an arrow $N_1 \to N_2$ if and only if $N_1 \subseteq N_2$. This is a poset category.
>
> The assignment
>
> $$\begin{aligned} N &\mapsto G/N \\ (N_1 \to N_2) &\mapsto (G/N_1 \to G/N_2) \end{aligned}$$
>
> is a functor $\mathbf{N} \to \mathbf{Grp}$.
>
> The limit of this diagram is a group called the *profinite completion* $\hat{G}$ of G.

Notation. $\hat{G}$ is equipped with homomorphisms making the following diagram commutes:

$$\begin{tikzcd} \hat{G} \arrow[d] \arrow[dr] & \\ G/N_1 \arrow[r] & G/N_2 \end{tikzcd}$$

In this course we refer to them as *projection maps* and the horizontal map as *transition map.* In addition, we have a *canonical map* $i : G \to \hat{G}$ which exists by the definition of limit.

We haven't shown profinite completion exists. We will prove it shortly in a more general context, by showing that it is an exmaple of a particular kind of, in some sense well-behaved, limit.

> **Definition** (inverse system)**.** A poset $(J, \preceq)$ is called an *inverse system* if for all $i, j \in J$ exists $k \in J$ such that $k \preceq i$ and $k \preceq j$.

Example. In $\mathbf{N}$, $N_1 \cap N_2$ is a subgroup of both N_1 and N_2.

> **Definition** (inverse system, inverse limit)**.** An *inverse system* (of groups, sets etc) is a functor $\mathbf{J} \to \mathbf{C}$ where $\mathbf{J}$ is the poset category corresponding to an inverse system.
>
> If $F : \mathbf{J} \to \mathbf{Grp}$ is an inverse system, the limit of F is called the *inverse limit* of the objects $F(j)$.

Since this is the central subject of this course, we spell out this definition explicitly

Definition. An *inverse system of groups*, indexed over an inverse system $(J, \preceq)$, consists of

- a group G_j for all $j \in J$,
- for all $i \preceq j$, a transition map $\phi_{ij} : G_i \to G_j$ such that $\phi_{ii} = \mathrm{id}_{G_i}, \phi_{jk} \circ \phi_{ij} = \phi_{ik}$.

The *inverse limit of the system* $(G_j)_{j\in J}$ is a group $\varprojlim_{j\in J} G_j$ with projection maps $p_j : \varprojlim G_j \to G_j$ such that $\phi_{ij} \circ p_i = p_j$ and such that for any Z with $q_j : Z \to G_j$, a map $q : Z \to \varprojlim G_j$ such that $p_j \circ q = q_j$.

Definition (profinite group)**.** A *profinite group* is the inverse limit of an inverse system of finite groups.

Example.

1. The profinite completion of a group G is a profinite group.
2. $\mathbb{Z}_p$, the p-adic integers, is $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

Proposition 1.1. *Let $(G_j)_{j\in J}$ be an inverse system of groups indexed by an inverse system J. $\varprojlim G_j$ exists and is equal to*

$$L = \{(g_j)_{j\in J} \in \prod_{j\in J} G_j : \varphi_{ij}(g_i) = g_j\}.$$

Proof. Let $p_j : L \to G_j$ be the restriction of the projection $\prod G_j \to G_j$. Then $\varphi_{ij} \circ p_i = p_j$. Now let $q_j : Z \to G_j$ be a cone. There is a unique map $f : Z \to \prod G_j$ such that $p_j \circ f = q_j$ and $f(Z) \subseteq L$. □

Note that we do not use any properties of inverse system or posets. The construction works equally well for sets (except that the resulting inverse limit is not a group). We will see that the finiteness and inverse system requirement ensures that the construction gives a nonempty set. To do so we need to bring in topology.

1.3 Topology on a profinite group/set

Give each finite group G_j in an inverse system the discrete topology. Then give $\prod G_j$ the product topology and $\varprojlim G_j \subseteq \prod G_j$ the subspace topology. $\prod G_j$ is Hausdorff and compact (Tychonoff). It follows that $\varprojlim G_j$ is Hausdorff. Since the conditions defining the subgroup are closed conditions, it is also compact.

Proposition 1.2. *If $(X_j)_{j\in J}$ is an inverse system of nonempty finite sets then $\varprojlim X_j \neq \emptyset$.*

Proof. Consider the set

$$Y_I = \{(x_j) \in \prod X_J : \phi_{ij}(x_i) = x_j \text{ for all } i, j \in I\}$$

where $I \subseteq J$. The Y_I's are closed and $\bigcup_{I \text{ finite}} Y_I = \varprojlim X_j$.

To show for I finite, $Y_I \neq \emptyset$, by definition of inverse system exists $k \in J$ such that $k \leq i$ for all $i \in I$. Now X_k is nonempty so exists $x_k \in X_K$. For $i \in J$, set $X = \varphi_{ki}(x_k)$. For $j \notin I$, set x_j to be arbitrary. Then this gives a sequence $(x_i) \in Y_I$.

Now use finite intersection property: suppose $I_1, \dots, I_m$ are are finite, then

$$Y_{I_1} \cap \dots \cap Y_{I_m} \supseteq Y_{I_1 \cup \dots \cup I_m} \neq \emptyset$$

so $\varprojlim X_j = \bigcup_{I \subseteq J \text{ finite}} Y_I \neq \emptyset$. □

It is perhaps psychologically comforting to point out that the topology on a profinite group is metrisable, thanks to

Proposition 1.3. *If (X_i) is a countable family of metric spaces then $\prod X_i$ is a metric space.*

Proof. IB Metric and Topological Spaces. □

In applications to profinite completions this is often implied by

Proposition 1.4. *If G is a finitely generated group then it has only countably many finite index normal subgroups.*

Proof. Every finite index normal subgroup arises as the kernel of some homomorphism $G \to S_n$. For a fixed n the homomorphism is determined by the image of the generators of G, so finitely many. □

Proposition 1.5. *Let G be a profinite group. Then multiplication $\mu : G \times G \to G$ and inversion $i : G \to G$ are continuous maps.*

Proof. Example sheet 1. □

Thus G is a *topological group.*

Definition. An *isomorphism of topological groups* is an isomorphism $f : G \to H$ which is also a homeomorphism.

From now on we only consider homomorphism between profinite groups which are continuous.

Lemma 1.6. *Let H be a topological group and let $G = \varprojlim G_j$ be an inverse limit of finite groups with projections $p_j : G \to G_j$. Then a homomorphism $f : H \to G$ is continuous if and only if $p_j \circ f : H \to G_j$ is continuous, if and only if* $\ker(p_j \circ f)$ *is an open subgroups of H.*

Proof. The first iff is by definition of the product topology on $\prod G_j$. For the second, let $f_j = p_j \circ f$. If $f_j : H \to G_j$ is continuous then $\ker f_j = f_j^{-1}(1)$ is open. Conversely, if $\ker f_j$ is open then $f_j^{-1}(g_j) = h \cdot \ker(f_j)$, where $h \in f_j^{-1}(g_j)$ if nonempty, is open for all $g_j \in G_j$. Thus $f_j^{-1}(U)$ is open for all $U \subseteq G_j$. □

Proposition 1.7. *Let G be a compact topological group. Then a subgroup $U \subseteq G$ is open if and only if it is closed and has finite index.*

Proof. Example sheet 1. □

Proposition 1.8. *Let $G = \varprojlim G_j$ be an inverse system of finite groups. Then the open subgroups $U_j = \ker p_j$ form a basis of open neighbourhoods of the identity.*

Proof. Let $V \ni 1$ be open. By definition of the product topology, V contains a basic open set of the form $p_{j_1}^{-1}(X_{j_1}) \cap \dots \cap p_{j_m}^{-1}(X_{j_m}) \ni 1$, where $X_{j_i} \subseteq G_{j_i}$ open. Then $1 \in X_{j_i} \subseteq G_{j_i}$ so by shrinking wlog $X_{j_i} = \{1\}$. Thus $1 \in \ker p_{j_1} \cap \dots \cap \ker p_{j_m}$. Now can find $k \in J$ such that $k \le j_i$ for all i. Then $1 \in U_k \subseteq \ker p_{j_1} \cap \dots \cap \ker p_{j_m} \subseteq V$. □

Corollary 1.9. *A basis of open sets in G is $\{p_j^{-1}(g_j) : j \in J, g_j \in G_j\}$.*

Corollary 1.10. *Let $X \subseteq G = \varprojlim G_j$ be a subset. Then X is dense in G if and only if $p_j(X) = p_j(X)$.*

Proof. If X is not dense then exist nonempty open set U such that $U \cap X = \emptyset$. wlog $U = p_j^{-1}(g_j)$. Then $g_j \in p_j(G) \setminus p_j(X)$. Similarly if X is dense and U is nonempty open, wlog $U = p_j^{-1}(g_j)$, then $g_j \in p_j(G) = p_j(X)$ so $X \cap U \neq \emptyset$. □

Proposition 1.11. *Let (G_j) be an inverse system of finite groups and $G = \varprojlim G_j$. Let $X \subseteq G$ be a subset. Then $\overline{X} = \varprojlim X_j$ where $X_j = p_j(X)$.*

Proof. Let

$$\begin{aligned} X' = \varprojlim X_j &= \{(g_i) \in \prod G_j : g_j \in X_j \text{ for all } j, \phi_{ij}(g_i) = g_j\} \\ &= \bigcap p_j^{-1}(X_j) \\ &= \bigcap p_j^{-1}(p_j(X)) \end{aligned}$$

which is closed. $X \subseteq X'$ so $\overline{X} \subseteq X'$. Let $g \in G \setminus \overline{X}$. Then exists a basic open set $p_j^{-1}(g_j) \subseteq G \setminus \overline{X}$. Hence $\overline{X} \cap p_j^{-1}(g_j) = \emptyset$, so $g_j \notin X_j$, so $g \notin X'$. □

Corollary 1.12. *X is closed if and only if $X = \varprojlim X_j$.*

Along the same line

Proposition 1.13. *Let G be a profinite group. Then*

$$\overline{X} = \bigcap_{N \trianglelefteq_o G} XN.$$

Proof. Since $\ker p_j$ form a neighbourhood basis of the identity,

$$\overline{X} = \bigcap p_j^{-1}(p_j(X)) = \bigcap X \cdot \ker p_j \subseteq \bigcap_{N \trianglelefteq_o G} XN.$$

Conversely if $g \notin \overline{X}$ then can find a neighbourhood $p_j^{-1}(g_j)$ of g that is disjoint from X. Then $g \notin X \cdot \ker p_j$. □

Example. If Γ is an abstract group, $\hat{\Gamma}$ its profinite completion with $i : \Gamma \to \hat{\Gamma}$ then $p_j(i(\Gamma)) = \Gamma/N_j = p_j(\hat{\Gamma})$, so $i(\Gamma)$ is dense in $\hat{\Gamma}$.

1.4 Change of inverse system

1.4.1 Surjective inverse system

Let $(G_j)_{j \in J}$ be an inverse system with transition funcitons φ_{ij} and projections p_j.

> **Definition** (surjective inverse system)**.** An inverse system is *surjective* if the transition maps φ_{ij} are all surjective.

> **Proposition 1.14.** *Let (X_j) be a surjective inverse system of nonempty finite sets. Then all projections $p_j : \varprojlim X_j \to X_j$ are surjective.*

Proof. Example sheet 1. □

> **Proposition 1.15.** *Let (X_j) be an inverse system of finite sets. Then there exists a surjective inverse system with the same inverse limit.*

Proof. Recall that

$$\varprojlim X_j = \left\{ (x_j) \in \prod X_j : \varphi_{ij}(x_i) = x_j \right\}.$$

Define $Y_j = p_j(\varprojlim X_j)$. Then Y_j with transition maps $\varphi_{ij}|_{Y_i}$ form an inverse system: if $y_i \in Y_i$ then $\varphi_{ij}(y_i) \in Y_J$. Then $\varprojlim Y_j = \varprojlim X_j$, and this is a surjective inverse system. □

1.4.2 Cofinal subsystems

> **Definition** (cofinal)**.** If J is an inverse system, $I \subseteq J$ is *cofinal* if for all $j \in J$ exists $i \in I$ such that $i \leq j$.

Therefore I is also an inverse system.

Example.

1. In the system of finite index subgroups of $\mathbb{Z}$, one cofinal system is $\{n!\mathbb{Z}\}$.
2. If $k \in J$, then $J_{\leq k} = \{j \in J : j \leq k\}$ is a *principal cofinal system.*
3. A cofinal system of $\mathbb{N}^{\text{op}}$ is the same as an increasing sequence of integers.

Definition (linearly ordered inverse system)**.** An inverse system is *linearly ordered* if it is isomorphic to a subset of $\mathbb{N}^{\mathrm{op}}$.

Proposition 1.16. *Let J be a countable inverse system with no initial element. Then J has a linearly ordered cofinal system.*

Proof. Example sheet 1. □

Proposition 1.17. *Let (X_j) be an inverse system of (finite) sets. Let $I \subseteq J$ be a cofinal system. Then $\varprojlim_{j\in J} X_j \cong \varprojlim_{i\in I} X_i$.*

Proof. We prove the proposition for profinite groups. Let $G = \varprojlim_{j\in J} G_j, H = \varprojlim_{i\in I} G_i$. The map $\prod G_j \to \prod G_i$ is a continuous homomorphism and restricts to a map $f : G \to H$. Remains to check this is a bijection. Suppose $(g_j) \in \ker f$, then $p_i(g) = g_i = 1$ for all $i \in I$. For every $j \in J$ exists $i \in I$ such that $i \leq j$ so $g_j = \varphi_{ij}(g_i) = 1$. Thus $(g_j) = 1$. For surjectivity, let $(g_i) \in H$. For $j \notin I$, let $i \in I$ be such that $i \leq j$ and set $g_j = \varphi_{ij}(g_i)$. It is well-defined and $(g_j) \in G$. □

2 Profinite groups

2.1 $\mathbb{Z}_p$, the p-adic integers

Let p be a prime. Consider the inverse system

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

of finite rings. The inverse limit is the profinite ring *p-adic integers*

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n.$$

An element $\alpha \in \mathbb{Z}_p$ is a sequence (a_n) of elements of $\mathbb{Z}/p^n$ such that $a_n = a_m \bmod p^n$ if $n \geq m$, where $a_n = \alpha \pmod{p^n} = p_n(a)$.

Addition and multiplication are done component-wise. One way to get such α is to take $a \in \mathbb{Z}$ and let a_n be reductions mod p^n of a. This gives $\iota : \mathbb{Z} \to \mathbb{Z}_p$.

> **Definition** (pro-p group, pro-p completion)**.** A *pro-p group* is an inverse limit of p-groups.
>
> The *pro-p completion* of Γ is
>
> $$\hat{\Gamma}_{(p)} = \varprojlim_{\substack{N \trianglelefteq \Gamma \\ \Gamma/N \text{ a } p\text{-group}}} \Gamma/N.$$

Therefore $\mathbb{Z}_p = \hat{\mathbb{Z}}_{(p)}$. Usually we suppress ι and regard $\mathbb{Z} \subseteq \mathbb{Z}_p$.

There is a natural metric on $\mathbb{Z}_p$: let $\alpha = (a_n), \beta = (b_n)$. If $\alpha = \beta$ then $d(\alpha, \beta) = 0$. Otherwise let n be the smallest integer such that $a_n \neq b_n$ and set $d(\alpha, \beta) = p^{-n}$. The restriction of this metric to $\mathbb{Z}$ is the "p-adic metric" on $\mathbb{Z}$.

The open ball is

$$\begin{aligned} B(0, r) &= \{(a_n) : a_m = 0 \text{ for } p^{-m} \geq r\} \\ &= \{(a_n) : a_m = 0 \text{ for } m \leq -\log_p r\} \\ &= \ker(\mathbb{Z}_p \to \mathbb{Z}/p^{\lfloor -\log_p r \rfloor}) \end{aligned}$$

which is an open subgroup of $\mathbb{Z}_p$.

> **Proposition 2.1.** *$\mathbb{Z}_p$ is abelian and torsion-free.*

Proof. Abelian is obvious. For torsion-free, let $\alpha = (a_n) \in \mathbb{Z}_p$ with $\alpha \neq 0$ and $m\alpha = 0$ for some $m > 0$. Write $m = p^r s$ where s is coprime to p. As $\alpha \neq 0$, exists n such that $\alpha \neq 0 \pmod{p^n}$, i.e. $a_n \neq 0 \in \mathbb{Z}/p^n$. As $m \neq 0$, $s \neq 0$. Now consider $ma \pmod{p^{n+r}}$. Claim this is nonzero: if $p^{n+r} \mid ma_{n+r}$ then $p^n \mid a_{n+r}$, hence $a_{n+r} = 0 \pmod{p^n} = a_n \pmod{p^n}$. □

> **Proposition 2.2.** *The ring $\mathbb{Z}_p$ is an integral domain.*

Proof. Example sheet 1. □

2.2 The profinite integers $\hat{\mathbb{Z}}$

Proposition 2.3. *$\hat{\mathbb{Z}}$ is abelian and torsion-free.*

Proposition 2.4. *$\hat{\mathbb{Z}}$ has zero divisors.*

Both follow from

Theorem 2.5 (Chinese remainder theorem)**.** *There is an isomorphism of topological rings*

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

Proof. There is a continuous homomorphism $\hat{\mathbb{Z}} \to \mathbb{Z}_p$ for every p as

$$\begin{tikzcd}
\hat{\mathbb{Z}} \arrow[d] \arrow[dr] & \\
\mathbb{Z}/p^n \arrow[r] & \mathbb{Z}/p^m
\end{tikzcd}$$

We thus have a continuous homomorphism $f : \hat{\mathbb{Z}} \to \prod_{p \text{ prime}} \mathbb{Z}_p$.

f is surjective if and only if $\operatorname{im} f \subseteq \prod \mathbb{Z}_p$ is dense, if and only if $\operatorname{im} f$ intersects all basic open sets of $\prod \mathbb{Z}_p$ non-trivially. A basic open set has the form $\phi^{-1}(x_1, \dots, x_r)$ where $\phi : \prod \mathbb{Z}_p \to \mathbb{Z}/p_1^{n_1} \times \cdots \times \mathbb{Z}/p_r^{n_r}$. Now invoke the classical Chinese remainder theorem: let $m = p_1^{n_1} \cdots p_r^{n_r}$, then we have a commutative diagram

$$\begin{tikzcd}
\hat{\mathbb{Z}} \arrow[r, "f"] \arrow[d, two heads] & \prod \mathbb{Z}_p \arrow[d, "\phi"] \\
\mathbb{Z}/m \arrow[r, "\cong"] & \mathbb{Z}/p_1^{n_1} \times \cdots \times \mathbb{Z}/p_r^{n_r}
\end{tikzcd}$$

As $(x_1, \dots, x_r) \in \operatorname{im}(\phi \circ f)$, have $\operatorname{im} f \cap \phi^{-1}(x_1, \dots, x_r) \neq \emptyset$.

Now suppose $g \in \hat{\mathbb{Z}} \setminus \{0\}$. Then exists m such that the image of g in $\hat{\mathbb{Z}} \to \mathbb{Z}/m$ is nonzero. Now use injectivity of the isomorphism to conclude f must be injective. □

2.3 Profinite matrix group

If R is a commutative ring with 1 then there is a matrix ring $\operatorname{Mat}_n(R)$ of $n \times n$ matrices whose entries are in R. In particular

$$\operatorname{Mat}_n(\mathbb{Z}_p) \cong \varprojlim \operatorname{Mat}_n(\mathbb{Z}/p^m)$$
$$\operatorname{Mat}_n(\hat{\mathbb{Z}}) \cong \varprojlim \operatorname{Mat}_n(\mathbb{Z}/m)$$

for similar argument as above.

Define

$$\operatorname{SL}_n(R) = \{A \in \operatorname{Mat}_n(R) : \det A = 1\}$$
$$\operatorname{GL}_n(R) = \{A \in \operatorname{Mat}_n(R) : \det A \in R^\times\}$$

As $\det : \mathrm{Mat}_n(\mathbb{Z}_p) \to \mathbb{Z}_p$ is a polynomial so continuous, $\mathrm{SL}_n(\mathbb{Z}_p) \subseteq \mathrm{Mat}_n(\mathbb{Z}_p)$ is a closed subset and is a group under multiplication. We will show in example sheet that $\mathbb{Z}_p^\times$ and $\hat{\mathbb{Z}}^\times$ are closed subsets of $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$, and in fact they are isomorphic to $\varprojlim(\mathbb{Z}/p^m)^\times$ and $\varprojlim(\mathbb{Z}/m)^\times$. We have

$$\mathrm{SL}_n(\mathbb{Z}_p) = \varprojlim \mathrm{SL}_n(\mathbb{Z}/p^m)$$

etc. A version of Chinese remainder theorem also holds.

Problem: consider the inclusion $\mathrm{SL}_n(\mathbb{Z}) \subseteq \mathrm{SL}_n(\hat{\mathbb{Z}})$. How does this inclusion look like? For example, is this inclusion dense? (the answer is yes, see example sheet 2). We know from general theory this holds if and only if $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/m)$ is surjecitve. But this is not obvious at all. For example how can we find an element that is mapped to $\left(\begin{smallmatrix} 7 & 9 \\ 4 & 9 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/13)$?

Another question: do we have $\mathrm{SL}_n(\hat{\mathbb{Z}}) = \widehat{\mathrm{SL}_n(\mathbb{Z})}$, i.e. does $\mathrm{SL}_n(\mathbb{Z})$ have any other finite quotients other than $\mathrm{SL}_n(\mathbb{Z}/m)$? The answer is no for $n = 2$ (example sheet 2), and yes for $n \geq 3$ (hard theorem of Bass-Lazard-Serre).

2.4 Subgroups, quotients and homomorphisms

A reminder that we are working in the category of topological groups so subgroups are closed and homomorphisms are continuous (non-closed subgroup can be pretty wild: $\hat{\mathbb{Z}} \supseteq \prod \mathbb{Z}_p \supseteq \prod \mathbb{Z}$).

Proposition 2.6. *A closed subgroup of a profinite group is a profinite group.*

Proposition 2.7. *Let $G = \varprojlim G_j$ be a profinite group of a surjective inverse system, $H \leq G$ a closed subgroup. Let $H_j = p_j(H)$. Then H has finite index (i.e. open) if and only if $[G_j : H_j]$ is constant for $j \in I$ for some cofinal subsystem $I \subseteq J$, in which case $[G : H] = [G_j : H_j]$ for $j \in I$.*

Proof. Exercise. □

Proposition 2.8. *Let G be a profinite group and $N \trianglelefteq_c G$. Then G/N equipped with the quotient topology is a profinite group.*

Proof. Let $G = \varprojlim G_j$ be a surjective inverse system. Define $N_j = p_j(N)$. Then $N_j \trianglelefteq G_j$ and define $Q_j = G_j/N_j$. Exists ψ_{ij} such that the following diagram commutes:

$$\begin{tikzcd}
G_i \arrow[r, "\phi_{ij}"] \arrow[d] & G_j \arrow[d] \\
G_i/N_i \arrow[r, "\psi_{ij}"] & G_j/N_j
\end{tikzcd}$$

Check that (Q_j, ψ_{ij}) is an inverse system. Let $Q = \varprojlim Q_j$. There exists a continuous map $\prod G_j \to \prod Q_j$ restricting to $f : G \to Q$. $(g_j) \in \ker f$ if and only if $g_j \in \ker(G_j \to Q_j) = N_j$ for all j, if and only if $g \in N$. Thus

$\ker f = N$. By first isomorphism theorem for groups, exists group isomorphism $\overline{f} : G/N \to Q$ making the diagram commute

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d] & Q \\
G/N \arrow[ur, dashed, "\overline{f}"'] &
\end{tikzcd}$$

$\overline{f}$ is continuous by definition of quotient topology. $\overline{f}$ is a homeomorphism because G/N is compact and Q is Hausdorff. □

Theorem 2.9 (first isomorphism theorem for profinite groups)**.** *If G and Q are profinite groups, $f : G \to Q$ is a continuous surjective homomorphism, then exists an isomorphism of topological groups $\overline{f} : G/\ker f \to Q$ making the following diagram commute*

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d] & Q \\
G/\ker f \arrow[ur, dashed, "\overline{f}"'] &
\end{tikzcd}$$

Corollary 2.10. *A (closed) quotient of a profinite group is a profinite group when given the quotient topology.*

Definition (morphism of inverse system)**.** Let (G_j) and (H_j) be inverse system of finite groups, indexed over the same poset J. A *morphism of inverse system* is a family of group homomorphisms $f_j : G_j \to H_j$ such that for all $i \leq j$, the following diagram commutes

$$\begin{tikzcd}
G_i \arrow[r, "f_i"] \arrow[d, "\varphi^G_{ij}"] & H_j \arrow[d, "\varphi^H_{ij}"] \\
G_j \arrow[r, "f_j"] & H_j
\end{tikzcd}$$

Proposition 2.11. *Given a morphism of inverse systems as above, exists a unique continuous homomorphism $f : G \to H$ such that*

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "p^G_j"] & H \arrow[d, "p^H_j"] \\
G_j \arrow[r, "f_j"] & H_j
\end{tikzcd}$$

commutes for all j.

Proof. Exercise. □

Proposition 2.12. *Let $(G_j)_{j \in J}, (H_i)_{i \in I}$ be inverse systems of finite groups, $G = \varprojlim G_j, H = \varprojlim H_j$. Let $f : G \to H$ be a continuous homomorphism. Assume J and I are countable. Then there are cofinal subsystems $J' \subseteq J, I' \subseteq I$ with an isomorphism $\alpha : J' \to I'$ and a morphism $f_{j'} : G_{j'} \to H_{\alpha(j')}$ of inverse system which induces f.*

Proof. We may assume J and I are linearly ordered, i.e. isomorphic to $\mathbb{N}^{\text{op}}$. Also we may assume $(G_j)_{j \in J}$ is surjective. Set $J' = J$. Construct an increasing sequence k_n of natural numbers inductively as follows: the composition $G \to H \to H_n$ is continuous so the kernel is open, hence containing a basic open subgroup $\ker p^G_{k_n}$ of G. As $\ker p^G_{k_n} \subseteq \ker p^H_n f$, exists a quotient map $f_n : G_{k_n} \to H_n$. Increase k_n if necessary so $k_n > k_{n-1}$. Set $I' = \{k_n\}$. □

2.5 Generators of profinite groups

Definition (topological generating set)**.** Let G be a topological group. A subset $S \subseteq G$ is a *(topological) generating set* for G if $\langle S \rangle$ is dense in G. G is *(topologically) finitely generated* (tfg) if it has a finite topological generating set.

Definition. Let G be a topological group and $S \subseteq G$. The *closed subgroup generated by* S is the smallest closed subgroup of G which contains S. Equivalently, it is the intersection of all closed subgroups which contain S.

Exercise. The closed subgroup generated by S is $\overline{\langle S \rangle}$. More generally, the closure of a subgroup is a subgroup.

Proposition 2.13. *If G is a profinite group, $U \leq_o G$ then G is tfg if and only if U is tfg.*

Proof. If $G = \overline{\langle S \rangle}$ for some finite S then $U \cap \langle S \rangle$ is finitely generated. As U is open, $U \cap \langle S \rangle$ is dense in U.

Conversely if $U = \overline{\langle S \rangle}$ and T is a set of coset representatives for U in G, then $S \cup T$ is a finite generating set for G. □

Proposition 2.14. *Let $G = \varprojlim G_j$ be an inverse system of finite groups. Then $S \subseteq G$ is a topological generating set if and only if $p_j(S)$ generates $p_j(G)$.*

Proof. $\langle S \rangle$ is dense if and only if $p_j(G) = p_j(\langle S \rangle) = \langle p_j(S) \rangle$ for all j. □

Proposition 2.15. *$\alpha \in \mathbb{Z}_p$ is a generator is and only if $\alpha \not\equiv 0 \pmod{p}$.*

Proof. Let $\alpha = (a_n)$. α is a generator if and only if a_n generates $\mathbb{Z}/p^n$ for all n, if and only if a_n is coprime to p^n, if and only if a_n is coprime to p. □

If α is a generator then consider multiplication by α, $f_\alpha : \mathbb{Z}_p \to \mathbb{Z}_p$. The image of f_α contains $\langle \alpha \rangle$ and hence $\operatorname{im} f_\alpha \supseteq \overline{\langle \alpha \rangle} = \mathbb{Z}_p$ so exists β such that $\alpha\beta = 1$. The converse is also true so we can identify the set of generators of $\mathbb{Z}_p$ with $\mathbb{Z}_p^\times$.

$\mathbb{Z}_p^\times$ is an open subset of $\mathbb{Z}_p$ and for all n the natural map $\mathbb{Z}_p^\times \to (\mathbb{Z}/p^n)^\times$ is surjective. Thus many elements of $\mathbb{Z}$ are invertible in $\mathbb{Z}_p$. For example to compute the inverse of $2 \in \mathbb{Z}_3^\times$, we can compute its inverse in $(\mathbb{Z}/3^n)^\times$ for increasingly large n to get

$$2^{-1} = (\dots, 41, 14, 5, 2) \in \prod \mathbb{Z}/3^n$$

so $2^{-1} = (\dots, 81, 27, 5, 2) \in \mathbb{Z}_3$.

Proposition 2.16. *$\alpha \in \hat{\mathbb{Z}}$ is a generator if and only if $\alpha \neq 0 \pmod{p}$ for all p.*

By Chinese remainder theorem this set is $\prod \mathbb{Z}_p^\times$, and thus can be identified with $\hat{\mathbb{Z}}^\times$. It is a closed subset of $\hat{\mathbb{Z}}$ and just as in the p-adic integer case, $\hat{\mathbb{Z}}^\times \to (\mathbb{Z}/n)^\times$ is surjective for all n.

Theorem 2.17 (Gaschütz's lemma for finite groups)**.** *Let $f : G \to H$ 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 exists a generating set $\{x_1, \dots, x_n\}$ of G such that $f(x_i) = z_i$.*

Proof. We formulate the theorem in terms of *generating vectors*: $(x_1, \dots, x_d) \in G^d$ whose underlying set generates G. f extends to $f^d : G^d \to H^d$. Let y be a generating vector for H and let $N_G(y)$ be the cardinality of the set of generating vectors x for G such that $f^d(x) = y$. We show $N_G(y)$ is independent of y, and then the results follows.

Induction on $|G|$. Let y be a generating vector for H. Let $\mathcal{C}$ be the set of $\leq d$-generated proper subgroups of G. Then for all x such that $f^d(x) = y$, either $\langle x \rangle = G$ or $\langle x \rangle \in \mathcal{C}$. Therefore

$$|\ker f^d| = |\{x \in G^d : f^d(x) = y\}| = N_G(y) + \sum_{C \in \mathcal{C}} N_C(y).$$

As $\ker f^d$ is manifestly independent of y, by induction hypothesis $N_G(y)$ is independent of y. □

Theorem 2.18 (Gaschütz's lemma for profinite groups)**.** *Let $f : G \to H$ be a continuous surjective homomorphism of profinite groups. Assume G has a topological generating set of size d. Then for every generating set $\{z_1, \dots, z_d\}$ of H, exists a generating set $\{x_1, \dots, x_n\}$ of G such that $f(x_i) = z_i$.*

Proof. wlog $G = \varprojlim_{j \in J} G_j, H = \varprojlim_{j \in J} H_j$ and f is induced by a morphism of inverse systems $f_j : G_j \to H_j$ (see lemma below) and the inverse systems are surjective. Let

$$X_j = \{x_j \text{ generating vector for } G_j : f_j(x_j) = p_j^H(z)\}$$

which is nonempty. $(X_j)_{j\in J}$ forms an inverse system so

$$\varprojlim X_j = \{x \in G^d : x \text{ generator of } G : f(x) = z\}$$

is nonempty. □

> **Proposition 2.19.** *Let G be a profinite group and $\mathcal{U}$ be a collection of open normal subgroups of G which form a neighbourhood basis at 1. Then $G = \varprojlim_{U\in\mathcal{U}} G/U$.*

Proof. There exists a homomorphism $f : G \to \varprojlim_{U\in\mathcal{U}} G/U$ which is surjective since G surjects G/U, and injective because $\mathcal{U}$ is a neighbourhood basis: for all $g \in G \setminus \{1\}$ exists $V \trianglelefteq_o G$ such that $g \notin V$ and exists $U \in \mathcal{U}$ such that $U \subseteq V$. □

Example. If G is tfg, take $\mathcal{U} = \{U_n\}$ where

$$U_n = \bigcap \{\text{normal subgroups of } G \text{ of index} \leq n\}$$

which is open since the collection is finite.

As a corollary

> **Lemma 2.20.** *If G is a tfg profinite group then $G = \varprojlim_{j\in J} G_j$ where J is countable.*

3 Profinite completion

3.1 Residual finiteness

Let Γ be an abstract group (usually finitely generated), $\hat{\Gamma} = \varprojlim_{N \trianglelefteq_f \Gamma} \Gamma/N$ its profinite completion, and a canonical map $\iota = \iota_\Gamma : \Gamma \to \hat{\Gamma}$.

We have seen for $\Gamma = \mathbb{Z}$ this canonical map is an injection. This injection is sufficiently important that it deserves its own name.

> **Definition** (residually finite)**.** Let Γ be an abstract group. Γ is called *residually finite* if for every $\gamma \in \Gamma \setminus \{1\}$ there exists $N \trianglelefteq_f \Gamma$ such that $\gamma \notin N$. Equivalently, γ is not in the kernel of $\Gamma \to \Gamma/N$.

> **Proposition 3.1.** *Γ is residually finite if and only if $\iota_\Gamma : \Gamma \to \hat{\Gamma}$ is injective.*

> **Proposition 3.2.** *A subgroup of a residually finite group is residually finite.*

Proof. Suppose $\Delta \leq \Gamma$. If $\gamma \in \Delta \setminus \{1\}$, exists $N \trianglelefteq_f \Gamma$ such that $\gamma \notin N$. Then $N \cap \Delta \trianglelefteq_f \Delta$ and $\gamma \notin N \cap \Delta$. □

A partial converse holds, provided the subgroup has finite index:

> **Proposition 3.3.** *Let Γ be an abstract group, $\Delta \leq \Gamma$ of finite index. Then if Δ is residually finite so is Γ.*

Proof. Let $\gamma \in \Gamma \setminus \{1\}$. If $\gamma \notin \Delta$, take

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

and $\gamma \notin N$. If $\gamma \in \Delta$ then exists $M \trianglelefteq_f \Delta$ such that $\gamma \notin M$. Then $M \leq_f \Gamma$ so $N = \mathrm{Core}_\Gamma(M) \trianglelefteq_f \Gamma$ and $\gamma \notin N$. □

> **Proposition 3.4.** *Direct product of residually finite groups is residually finite.*

Proof. Example sheet 2. □

> **Proposition 3.5.** *All finitely generated abelian groups are residually finite.*

Remark. Finite generation is necessary here. For example $\mathbb{Q}$ has no nontrivial finite quotient.

A source of residually finite groups is matrix group.

> **Proposition 3.6.** $\mathrm{SL}_N(\mathbb{Z})$ *and* $\mathrm{GL}_N(\mathbb{Z})$ *are residually finite for all N.*

Proof. If $A \in \mathrm{GL}_N(\mathbb{Z})$, take a prime p greater than an entry of A. Then A is not in the kernel of $\mathrm{GL}_N(\mathbb{Z}) \to \mathrm{GL}_N(\mathbb{Z}/p)$. □

Proposition 3.7 (Non-examinable). *[Mal'cev's theorem] Let Γ be a finitely generated subgroup of $\mathrm{GL}_N(K)$ (resp. $\mathrm{SL}_N, \mathrm{PSL}_N$) where K is a field. Then Γ is residually finite.*

As a corollary, fundamental groups of surfaces are residually finite (as they are contained in $\mathrm{PSL}_2(\mathbb{R})$ by hyperbolic geometry).

Theorem 3.8. *Let G and H be tfg profinite groups. Then $G \cong H$ if and only if the set of isomorphism types of continuous finite quotients of G and H are equal.*

Proof. Let G_n be the intersection of all open normal subgroups of G of index $\leq n$. Then $G_n \trianglelefteq_o G$ and $G = \varprojlim G/G_n$. Define H_n similarly. Now G/G_n is a continuous finite quotient of G so it is also a continuous finite quotient of H. Thus exists $V \trianglelefteq_o H$ such that $G/G_n \cong H/V$. By definition the intersection of all normal subgroups of G/G_n of index $\leq n$ is trivial, so upon taking their preimages under $H \to H/V$ we have $H_n \subseteq V$. Then

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

By symmetry we have equality so $H_n = V$ and thus $G/G_n \cong H/H_n$.

To show there exists an isomorphism of inverse systems, let S_n be the set of isomorphisms $G/G_n \to H/H_n$, which is nonempty. If $f_n \in S_n$ then it takes normal subgroups of G/G_n of index $\leq n-1$ to those in H/H_n, so defines an isomorphism $G_{n-1}/G_n \to H_{n-1}/H_n$. Thus f_n descends to a map $\phi_{n,n-1}(f_n) : G/G_{n-1} \to H/H_{n-1}$ which makes the following diagram commute

$$\begin{tikzcd} G/G_n \arrow[r, "f_n"] \arrow[d] & H/H_n \arrow[d] \\ G/G_{n-1} \arrow[r, "\phi_{n,n-1}(f_n)"] & H/H_{n-1} \end{tikzcd}$$

$(S_n, \phi_{n,n-1})$ is an inverse system of nonempty sets so $\varprojlim S_n$ is nonempty and its element defines an isomorphism of inverse systems. □

As a corollary

Theorem 3.9. *Let Γ, Δ be finitely generated abstract groups. Then $\hat{\Gamma} \cong \hat{\Delta}$ if and only if the set of isomorphism types of finite quotients of Γ and Δ are the same.*

The following lemma characterises open subgroups of profinite completion

Lemma 3.10. *Let Γ be a finitely generated abstract group. Then the open subgroups of $\hat{\Gamma}$ are precisely the subgroups $\overline{\iota_\Gamma(\Delta)}$ for $\Delta \leq_f \Gamma$.*

Proof. If $\Delta \leq_f \Gamma$ then $\overline{\iota_\Gamma(\Delta)}$ is closed. It also has finite index so open: suppose $\Gamma = \bigcup_{i=r}^r g_i\Delta$ is a finite (disjoint) union, then

$$\hat{\Gamma} = \overline{\iota_\Gamma(\Gamma)} = \overline{\bigcup \iota_\Gamma(g_i\Delta)} = \bigcup \iota_\Gamma(g_i)\overline{\iota_\Gamma(\Delta)}$$

Conversely, let $U \leq_o \hat{\Gamma}$, then $U \cap \iota_\Gamma(\Gamma)$ is dense in U. Let $\Delta = \iota_\Gamma^{-1}(U) = \iota_\Gamma^{-1}(U \cap \iota_\Gamma(\Gamma))$. Then $\Delta \leq_f \Gamma$ and $\iota_\Gamma(\Delta) = U \cap \iota_\Gamma(\Gamma)$. □

Question: how much can we learn about Γ from $\hat{\Gamma}$, if Γ is residually finite?

> **Proposition 3.11.** *If $\hat{\Gamma} \cong \hat{\Delta}$, Δ is abelian and Γ is residually finite then Γ is abelian.*

Proof. If Δ is abelian, all its quotients are abelian, so $\hat{\Delta}$ is abelian. Then $\iota_\Gamma : \Gamma \to \hat{\Gamma} = \hat{\Delta}$ shows Γ is abelian. □

> **Proposition 3.12.** *If G and H are finitely generated and $\hat{G} \cong \hat{H}$ then $G_{\text{ab}} \cong H_{\text{ab}}$. In particular if G is abelian and H is residually finite then $G \cong H$.*

Proof. If G and H have the same finite quotients then they have the same finite abelian quotients, which are precisely the finite quotients of abelianisation. Thus suffices to show we can recover a finitely generated abelian group $G \cong \mathbb{Z}^r \times T$ from its finite quotient. Have

$$r = \max\{k : G \twoheadrightarrow (\mathbb{Z}/n)^k \text{ for all } n\}$$

and T the largest finite abelian group such that $G \twoheadrightarrow (\mathbb{Z}/n)^r \times T$. □

Example (Baumslag)**.** One does not have to go far from abelian groups to show this fails in general. Let $\phi : C_{25} \to C_{25}$ be the automorphism $t \mapsto t^6$ where t is a fixed generator. ϕ has order 5. Form semidirect products $G_1 = C_{25} \rtimes_\phi \mathbb{Z}, G_2 = C_{25} \rtimes_{\phi^2} \mathbb{Z}$. Write $\mathbb{Z} = \langle s \rangle$ multiplicatively. Claim $G_1 \not\cong G_2$ but $\hat{G}_1 \cong \hat{G}_2$.

Proof. Suppose $\psi : G_2 \to G_1$ is an isomorphism. Then $\psi(C_{25}) = C_{25}$ so $\psi(t,1) = (t^a, 1)$ where t^a generates C_{25}. Let $\psi(1,s) = (t^b, s^c)$. As s^c generates $\mathbb{Z}$, $c = \pm 1$. Now compute

$$\psi((1,s) \bullet_2 (t,1) \bullet_2 (1,s^{-1})) = \psi(\phi^2(t), 1) = (\phi^2(t^a), 1).$$

On the other hand

$$\begin{aligned}(t^b, s^c) \bullet_1 (t^a, 1) \bullet_1 (\phi^{-c}(t^{-b}), s^{-c}) &= (t^b \phi^c(t^a), s^c) \bullet_1 (\phi^{-c}(t^{-b}), s^{-c}) \\ &= (t^b \phi^c(t^a) \phi^c \phi^{-c}(t^b), 1) \\ &= (\phi^c(t^a), 1)\end{aligned}$$

so $\phi^2(t^a) = \phi^c(t^a)$ so $2 = c \pmod 5$, absurd.

To show the profinite completions are isomorphic, note $\hat{G}_1 = C_{25} \rtimes_\phi \hat{\mathbb{Z}}, \hat{G}_2 = C_{25} \rtimes_{\phi^2} \hat{\mathbb{Z}}$: let $G_1 \to Q$ be a finite quotient. If the composition $\mathbb{Z} \to G_1 \to Q$ has image of order m, then f factors through the finite quotient $C_{25} \rtimes_\phi (\mathbb{Z}/5m)$, so the quotients $C_{25} \rtimes \mathbb{Z}/5m$ are cofinal in the finite quotients, so

$$\hat{G}_1 = \varprojlim (C_{25} \rtimes \mathbb{Z}/5m) = C_{25} \rtimes \hat{\mathbb{Z}}.$$

Same for G_2. □

It is worth noting that if we try to compute the same expressions in the profinite completions, we can merely conclude c is a topological generator of $\hat{\mathbb{Z}}$ — but $\hat{\mathbb{Z}}$ has many generators! In fact, for any $c \in \hat{\mathbb{Z}}^\times$ such that $c = 2 \pmod 5$ we can define $\psi' : \hat{G}_2 \to \hat{G}_1, (t^a, s^b) \mapsto (t^a, s^{bc})$ which is continuous and injective. As c is a generator, it is also surjective.

Open problem: 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 exists a finitely generated residually finite group G and $n \in \mathbb{N}$ such that a finite group Q is a quotient of G if and only if $d(Q) \leq n$, where d is the minimum number of generators?

Proposition 3.13. *If F_1, F_2 are both finitely generated free and $\hat{F}_1 \cong \hat{F}_2$ then $F_1 \cong F_2$.*

Proof. Immediate. □

What about surface groups? They are fundamental groups of genus g orientable surfaces and has presentation

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

Can we tell them apart from free groups? If $\hat{S}_g = \hat{F}_r$ then $\mathbb{Z}^{2g} \cong \mathbb{Z}^r$ so $r = 2g$. What next?

Proposition 3.14 (basic correspondence)**.** *Let G_1, G_2 be finitely generated residually finite groups. Suppose $\hat{G}_1 \cong \hat{G}_2$. Then there is a bijection*

$$\psi : \{H \leq_f G_1\} \to \{H \leq_f G_2\}$$

such that if $K \leq_f H \leq_f G_1$ then

- $[H : K] = [\psi(H) : \psi(K)]$.
- $K \trianglelefteq H$ *if and only if* $\psi(K) \trianglelefteq \psi(H)$.
- *If* $K \trianglelefteq H$ *then* $H/K \cong \psi(H)/\psi(K)$.
- $\hat{H} \cong \widehat{\psi(H)}$.

Every finite-sheeted cover of a surface is a surface, so every finite index subgroup of S_g is a surface group so has abelianisation $\mathbb{Z}^{2g'}$. However F_r has an index 2 subgroup, which is free of rank $2(r-1)+1$ by Nielsen-Schreier. Thus from the corrspondence we deduce S_g is not free.

The proposition itself follows from the correpondence between subgroups of G and $\hat{G}$.

Proposition 3.15. *Let G be finitely generated residually finite and regard G as a subgroup of $\hat{G}$. Then there is a bijection*

$$\begin{aligned} \{H \leq_f G\} &\to \{U \leq_o \hat{G}\} \\ H &\mapsto \overline{H} \\ U \cap G &\leftarrow\!\shortmid U \end{aligned}$$

Furthermore if $K \leq_f H \leq_f G$ then

- $[H : K] = [\overline{H} : \overline{K}]$,
- $K \trianglelefteq H$ *if and only if* $\overline{K} \trianglelefteq \overline{H}$,

- *If $K \trianglelefteq H$ then $H/K \cong \overline{H}/\overline{K}$,*
- *$\overline{H} \cong \hat{H}$.*

Proof. Surjectivity is done in Lemma 3.10. To show injectivity enough to show $\overline{H} \cap G = H$. Consider the action of G on G/H, inducing a continuous $\alpha : \hat{G} \to \mathrm{Sym}(G/H)$. Then $g \in \mathrm{Stab}_{\hat{G}}(H)$, an open subgroup. If $g \in G \setminus H$ then it is disjoint from H, so $g \notin \overline{H}$.

Let $\{g_i\}$ be a set of coset representatives of H in G. Then $\hat{G} = \bigcup g_i \overline{H}$. This is a disjoint union since $\overline{H} \cap G = H$, so $\{g_i\}$ is also a coset representative of $\overline{H}$ in $\hat{G}$, so there is a natural bijection $G/H \to \hat{G}/\overline{H}$.

If $\overline{K} \trianglelefteq \overline{H}$ then $K = \overline{K} \cap G \trianglelefteq \overline{H} \cap G = H$. H normalises K if and only if K lies in the kernel of the action $H \to \mathrm{Sym}(H/K)$, so $\overline{K} \subseteq \overline{H}$ so $\overline{K} \trianglelefteq \overline{H}$.

Any finite quotient K of H is the quotient of $\overline{H}$ by the open subgroup $\overline{K}$. Thus by universal property there is a continuous homomorphism $\overline{H} \to \hat{H}$. It is injective since for any $1 \neq h \in \overline{H}$, exists U open in $\hat{G}$ such that $h \notin U$. Then h is not mapped to identity under the composition $\overline{H} \to \hat{H} \to \overline{H}/\overline{H} \cap U$. □

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

Usually surjectivity is the easier condition to check — if we know a set of generators then we only have to show that they lie in the image. On the other hand to show injectivity requires understanding the image of each element.

Proposition 3.16. *Let G be a tfg profinite group. Then G has the Hopf property.*

Proof. Let G_n be the intersection of all open normal subgroups of G of index $\leq n$. G_n is open and $G = \varprojlim G/G_n$. If $U \leq_o G$ with $[G : U] \leq n$ then because f is surjective, $[G : U] = [G : f^{-1}(U)] \leq n$ so $G_n \leq f^{-1}(U)$. Thus $G_n \subseteq \bigcap f^{-1}(U) = f^{-1}(G_n)$ so $f(G_n) \subseteq G_n$, inducing a surjective map $f_n : G/G_n \to G/G_n$. Finite groups are Hopfian so f_n is an isomorphism. The result thus follows. □

Corollary 3.17. *If Γ is finitely generated and residually finite then Γ has the Hopf property.*

Proof. Let $f : \Gamma \to \Gamma$ be a surjection. Then f induces a unique map $\hat{f} : \hat{\Gamma} \to \hat{\Gamma}$. $\hat{\Gamma}$ is tfg and $\hat{f}$ is surjective because its image is compact and contains a dense subset. The result then follows from the Hopf property of $\hat{\Gamma}$. □

Proposition 3.18. *Let G, H be (topological respectively) groups, G with Hopf property. If there exists (continuous respectively) surjections $f : G \to H, f' : H \to G$ then both f and f' are isomorphisms.*

Proof. $f' \circ f : G \to G$ is an isomorphism by Hopf property so f is injective and an isomorphism. Then $f' = (f' \circ f) \circ f^{-1}$ is also an isomorphism. □

Proposition 3.19. *Let Γ be a group and suppose exists a finite quotient Q of Γ such that $d(\Gamma) = d(Q)$, where d is the minimum number of generators. Then for a free group F, $\hat{F} \not\cong \hat{\Gamma}$ unless Γ is free, i.e. $\Gamma \cong F$.*

Proof. Let F be a free group with $\hat{F} \cong \hat{\Gamma}$. Then Q is also a quotient of F so $d(F) \geq d(Q) = d(\Gamma)$ so exists a surjection $f : F \to \Gamma$, which induces a continuous surjection $\hat{f} : \hat{F} \to \hat{\Gamma}$. By Hopf property $\hat{f}$ is an isomorphism so f is injective. □

Example. Non-Hopfian groups are not residually finite. For an example of non-Hopfian group, let

$$\mathrm{BS}(n, m) = \langle a, t | a^n t^{-1} = a^m \rangle$$

where n, m coprime. Define

$$\begin{aligned} f : \mathrm{BS}(n, m) &\to \mathrm{BS}(n, m) \\ y &\mapsto t \\ a &\mapsto a^n \end{aligned}$$

f is a surjection as it surjects the generators. But f is not injective: a does not commute with tat^{-1} (which we quote as a fact). But

$$f([a, tat^{-1}]) = [a^n, ta^n t^{-1}] = [a^n, a^m] = 1$$

so $\mathrm{BS}(n, m)$ is not Hopfian. residually finite.

3.2 Finite quotients of free groups

Theorem 3.20. *Free groups are residually finite.*

There are two proofs. The first proof in online notes is non-examinable (and omitted). The proof actually shows that

Corollary 3.21. *For all p, a free group F is residually p-finite. In particular F injects to its pro-p completion.*

We record the second proof here, which is an algorithm to produce finite quotients.

Proof. Let F be free on finite generating set S so $F = \pi_1 \bigvee_S S^1$. Write $g \in F \setminus \{1\}$ as a reduced word $s_1 \cdots s_n$. Write out g "along a line" to get a labelled graph Y and there is a continuous map $Y \to X$. We seek to make Y a covering space of X by adding edges.

For each $s \in S$, the number of vertices having an outgoing s edge is the same as those having an incoming one. Thus we can add s edges so that every vertex has exactly one s edge entering and one leaving. This gives a finite covering $\overline{Y}$ of X so corresponds to a finite index subgroup $\pi_1 \overline{Y}$ of F. $g \notin \pi_1 \overline{Y}$ since it is not a loop.

For each $s \in S$, following the edge s is a permutation of vertices to we have an action of F on vertices of Y. g does not fix the initial vertex of Y as g is not contained in the finite index normal subgroup corresponding to the kernel of the action. □

Theorem 3.22 (Marshall Hall's theorem)**.** *Let $S \subseteq F$ be a finite subset. If $y \notin \langle S \rangle$ then exists a finite group Q and a homomorphism $f : F \to Q$ such that $f(y) \notin f(\langle S \rangle)$.*

Corollary 3.23. *If S does not generate F then exists Q, f such that $f(\langle S \rangle) \neq f(F)$.*

Remark. Marshall Hall's theorem actually says that exists $H \leq_f F$ such that $S \subseteq H$ and $H = \langle S \rangle * H'$.

Corollary 3.24. *S generates F if and only if S (topologically) generates $\hat{F}$.*

Note. As a result $\overline{\langle S \rangle} \cap F = \langle S \rangle$, which generalises the basic correspondence, which holds only for finite index subgroup.

The proof uses monodromy action of the fundamental group. Let X be a wedge of circles whose fundamental group is F. If we can find a finite covering space Y of X such that S is contained in the image of $\pi_1 Y$ then $\langle S \rangle$ is contained in the stabiliser of a vertex of the covering action. Similar to the proof of residually finiteness of free groups, if $y \notin \langle S \rangle$ then we can construct Y so that g does not lie in the stabiliser.

To construct the covering space first let Y be the graph with a distinguished vertex and loops corresponding to words in S going around the vertex. We would like to add edges as before so that Y becomes a covering space. Here we encounter a problem as there might be more than one edge, say a, coming from the distinguished vertex. We need to apply *Stallings' fold* to identify the repeated edges, and it is a fact that this procedure does not change the fundamental group.

The formal proof is non-examinable. A worked example can be found in the lecturer's online notes.

4 Pro-p groups

Recall that a *pro-p group* is an inverse limit of finite p-groups — finite groups of order a power of p. The *pro-p completion* of Γ is

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

For example $\mathbb{Z}_p = \hat{\mathbb{Z}}_{(p)}$.

4.1 Generators of pro-p groups

Definition (Frattini subgroup)**.** Let G be a finite group. The *Frattini subgroup* of G is

$$\Phi(G) = \bigcap \{M : M \text{ maximal proper subgroup of } G\}.$$

Proposition 4.1. *If $f : G \to H$ is a surjective group homomorphism then $f(\Phi(G)) \subseteq \Phi(H)$. In particular $\Phi(G)$ is a characteristic normal subgroup, i.e. if $f : G \to G$ is an automorphism then $f(\Phi(G)) = \Phi(G)$.*

Proof. Let M be a maximal proper subgroup of H. Then $f^{-1}(M)$ is a proper subgroup and it is maximal: if $f^{-1}(M) \subseteq N \subseteq G$, assume $f^{-1}(M) \neq N$. Then $f(N) = H$ as M is maximal. Therefore $G = N \cdot \ker f = N$ as $N \supseteq \ker f$. Therefore $\Phi(G) \subseteq f^{-1}(M)$, hence $f(\Phi(G)) \subseteq M$. Taking intersection to get $f(\Phi(G)) \subseteq \Phi(H)$. □

Note that we did not use finiteness anywhere.

Proposition 4.2. *Let G be a finite group. For $S \subseteq G$ a subset, TFAE:*

1. *S generates G.*
2. *$S\Phi(G)$ generates G.*
3. *$S\Phi(G)/\Phi(G)$, the image of S in $G/\Phi(G)$, generates $G/\Phi(G)$.*

In other words, the elements of $\Phi(G)$ are precisely the non-generators.

Proof. Only $3 \implies 1$ is nonobvious. Suppose S does not generate G. Then $\langle S \rangle$ is contained in some maximal proper subgroup. Here we used the crucial fact that G is finite. Since $\Phi(G) \subseteq M$, $M/\Phi(G)$ is a proper subgroup of $G/\Phi(G)$. Thus $S\Phi(G)/\Phi(G) \subseteq M/\Phi(G) \subsetneq G/\Phi(G)$. □

Definition. Let G be a group, H, K subgroups of G and $m \in \mathbb{Z}$. Define

$$HK = \{hk : h \in H, k \in K\}$$

which is a priori a set, but is a subgroup if either H or K is normal, and is a normal subgroup if both H and G are.

Define the commutator to be

$$[H,K] = \langle [h,k] = h^{-1}k^{-1}hk : h \in H, k \in K\rangle$$

which is a subgroup and is a normal subgroup if both H and K are normal.

Finally define

$$H^m = \langle h^m : h \in H\rangle.$$

which is a subgroup.

Proposition 4.3. *Let G be a p-group. Then*

$$\Phi(G) = [G,G]G^p = \ker(G \to G_{\text{ab}} \to G_{\text{ab}}/pG_{\text{ab}}) = \langle [g_1,g_2]g_3^p\rangle.$$

Note that $G_{\text{ab}}/pG_{\text{ab}}$ is an $\mathbb{F}_p$-vector space, so is isomorphic to $(\mathbb{Z}/p)^d$ for some d. Thus $G/\Phi(G) \cong \mathbb{F}_p^d$ where $d = d(G)$ is the minimum size of a generating set of G.

Proof. Example sheet 2. □

Definition. Let G be a profinite group. Define

$$\Phi(G) = \bigcap \{M : M \text{ maximal proper closed subgroups of } G\},$$

where M maximal proper closed means that if N is a closed subgroup then $M \subseteq N \subseteq G$ implies $N = M$ or $N = G$.

Proposition 4.4. *Any proper closed subgroup of a profinite group G is contained in a proper open subgroup, and hence is contained in a maximal proper closed subgroup, and maximal proper closed subgroups are open.*

Proof. Suppose $H \leq_c G$, $G \neq H$ and $G = \varprojlim G_j$. Since H is not dense, exists j such that $p_j(H) \neq p_j(G)$. Then $p_j^{-1}(p_j(H))$ is open proper and contains H. □

Similar to the finite case we have

Lemma 4.5. *If $f : G \to H$ is a surjective continuous homomorphism of profinite groups then $f(\Phi(G)) \subseteq \Phi(H)$.*

Proposition 4.6. *If $S \subseteq G$ where G is a profinite group then TFAE*

1. *S is a tgs for G.*
2. *$S\Phi(G)$ is a tgs for G.*
3. *$S\Phi(G)/\Phi(G)$ is a tgs for $G/\Phi(G)$.*

Proposition 4.7. *Let $(G_j)_{j\in J}$ be a surjective inverse system of finite* *groups. Let $G = \varprojlim G_j$. Then*

$$\Phi(G) = \varprojlim \Phi(G_j).$$

Proof. Let $p_j : G \to G_j$ be the projection. Then $p_j(\Phi(G)) \subseteq \Phi(G_j)$ for all j. Hence $\Phi(G) \subseteq \varprojlim \Phi(G_j)$.

Now let M be a maximal proper closed subgroup of G. M is open so exists i such that $\ker p_i \subseteq M$. Thus $\ker p_j \subseteq M$ for all $j \leq i$. Then $p_j(M)$ is a maximal proper subgroup of G_j so $p_j(M) \supseteq \Phi(G_j)$ for all $j \leq i$. Thus

$$M \supseteq \varprojlim_{j \leq i} \Phi(G_j) = \varprojlim \Phi(G_j).$$

□

Proposition 4.8. *Let G be a tfg pro-p group. Then*

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

and $G/\Phi(G) \cong \mathbb{F}_p^d$ where $d = d(G)$.

Later we will see that $[G,G]G^p$ is in fact closed.

Note. $G/\Phi(G)$ is also denoted $H_1(G, \mathbb{F}_p)$.

Proof. Write $G = \varprojlim G_j$ as a surjective inverse limit of finite p-groups. Then $\Phi(G) = \varprojlim [G_j, G_j]G_j^p$. If $g_1, g_2, g_3 \in G$ then

$$p_j([g_1, g_2]g_3^p) = [p_j(g_1), p_j(g_2)]p_j(g_3)^p \in [G_j, G_j]G_j^p$$

so $p_j(\overline{[G,G]G^p}) \subseteq [G_j, G_j]G_j^p$ for all j so $\overline{[G,G]G^p} \subseteq \Phi(G)$. Now $G/\overline{[G,G]G^p}$ is tfg abelian and every element has order p. Therefore it is isomorphic to $\mathbb{F}_p^d$ for some d (if $a_1, \dots, a_d$ tgs of $G/\overline{[G,G]G^p}$ then $\{a_1^{n_1} \cdots a_d^{n_d} : n_1, \dots, n_d \in \{0, \dots, p-1\}\}$ is a finite dense subgroup). Then since $\Phi(\mathbb{F}_p^d) = \{0\}$, we find $\Phi(G) \subseteq \overline{[G,G]G^p}$ as required. □

Corollary 4.9. *Let $f : G \to H$ be a continuous homomorphism of tfg 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 a map of vector spaces over $\mathbb{F}_p$. f is surjective if and only if f_* is surjective.*

Proof. If $g_1, g_2, g_3 \in G$ then

$$f([g_1, g_2]g_3^p) = [f(g_1), f(g_2)]f(g_3)^p \in \Phi(H)$$

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

$f(G)$ generates H if and only if $f(G)\Phi(H)/\Phi(H) = f_*(G/\Phi(G))$ generates $H/\Phi(H)$. As the image of both are compact so closed, the result follows. □

Example. Let $F = \langle a, b \rangle$, the free group of rank 2 and $G = \hat{F}_{(p)}$. Then $G/\Phi(G) = \mathbb{F}_p^2$. Let $S = \{a^4b^2a, ba^{-2}b\}$. Map S to $G/\Phi(G)$ to test generation:

$$a^4b^2a \mapsto \left(\begin{smallmatrix} 5 \\ 2 \end{smallmatrix}\right)$$
$$ba^{-2}b \mapsto \left(\begin{smallmatrix} -2 \\ 2 \end{smallmatrix}\right)$$

They generate $\mathbb{F}_p^2$ if and only if $\det\left(\begin{smallmatrix} 5 & -2 \\ 2 & 2 \end{smallmatrix}\right) = 14 \neq 0$, if and only if $p \neq 2, 7$.

4.2 Nilpotent groups

Definition. A commutator of length 2 is a commutator

$$[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2 = g_1^{-1} g_1^{g_2}.$$

Define iteratively a commutator of length n

$$[g_1, g_2, \dots, g_n] = [g_1, [g_2, \dots, g_n]].$$

Definition (lower central series)**.** The *lower central series* of G is the following sequence of subgroups:

$$\begin{aligned} G_1 &= G \\ G_{n+1} &= [G, G_n] = \langle [g, h] : g \in G, h \in G_n \rangle \end{aligned}$$

We sometimes denote G_n by $\gamma_n(G)$.

Definition (nilpotent group)**.** A group G is *nilpotent of class c* if $\gamma_{c+1}(G) = 1$ but $\gamma_c(G) \neq 1$.

For a nilpotent group we have

$$G = \gamma_1 \geq \gamma_2 \geq \dots \geq \gamma_{c+1} = 1.$$

Note. $\gamma_c(G)$ is central in G and nilpotent of class 1 is the same as abelian.

Proposition 4.10. *γ_n is* fully characteristic *in the sense that if $f : G \to H$ is a homomorphism then $f(\gamma_n(G)) \subseteq \gamma_n(H)$.*

Proposition 4.11. *Subgroups and quotients of nilpotent groups of class c are nilpotent of class $\leq c$.*

Proposition 4.12. *A finite p-group is nilpotent.*

Exercise. If R is a ring, then the set of upper trianglular $n \times n$ matrices with 1 on the diagonal is a nilpotent group.

Definition. For G is tfg pro-p group, the *lower central p-series* is defined by

$$\begin{aligned} G_1 &= G \\ G_{n+1} &= \overline{[G, G_n] G_n^p} \end{aligned}$$

$\gamma_n(G) \subseteq G_n = \gamma_n^{(p)}(G)$.

Why are we doing this?

1. G_n/G_{n+1} are vector spaces over $\mathbb{F}_p$.
2. $\gamma_n^{(p)}(G)$ is open in G: inductively $\Phi(G) = \gamma_2^{(p)}(G)$ and $\Phi(G_{n-1}) \leq \gamma_n^{(p)}(G)$, and Frattini subgroup of a tfg pro-p group is open.
3. $\{\gamma_n^{(p)}(G)\}$ forms a neighbourhood basis for the identity: if $N \trianglelefteq_o G$, G/N is a finite p-group so $\gamma_n^{(p)}(G/N)$ vanish for some n. Therefore $\gamma_n^{(p)}(G) \subseteq N$.

4.3 Invariance of topology

Theorem 4.13. *Let G be a tfg pro-p group, H a profinite group and $f : G \to H$ a homomorphism. Then f is continuous.*

Corollary 4.14. *Let G be a tfg pro-p group. There is no other topology on G making it into a profinite group.*

Proof. If τ_1 is our given topology and τ_2 is another topology such that (G, τ_2) is profinite, then the identity homomorphism from τ_1 to τ_2 is continuous so a homeomorphism. □

"The group structure determines the topology".
Theorem 4.13 follows from

Theorem 4.15. *Let G be a tfg pro-p group. Then any finite index subgroup of G is open.*

Proof of Theorem 4.13. Suppose $f : G \to H$ is a homomorphism. Then for all $U \trianglelefteq_o H$, U has finite index so $f^{-1}(H)$ has finite index and hence open in G. Thus f is continuous. □

Lemma 4.16. *Let G be a nilpotent group generated by $a_1, \dots, a_d$. Then every $g \in [G, G]$ can be written as*

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

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

Proof. Induction on nilpotency class. $c = 1$ is trivial. Assume true for nilpotency class $c - 1$. In particular it is true for $G/\gamma_c(G)$ so

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

for some $u \in \gamma_c(G)$. We can write u as a product

$$u = \prod_{i=1}^{N} [g_i, v_i]$$

where $g_i \in G, v_i \in \gamma_{c-1}(G)$. Recall the commutator relations

$$[xy, z] = [x, z]^y [y, z]$$
$$[x, yz] = [x, z][x, y]^z$$

which imply, for $v \in \gamma_{c-1}(G)$

$$\begin{aligned}[a_i a_j, v] &= [a_i, v][a_j v]\\ [a_i^{-1}, v] &= [a_i, v^{-1}] = [a_i, v]^{-1}\\ [a_i, v][a_i, v] &= [a_i, v^2]\\ [a_i, w][a_i, v] &= [a_i, vw]\end{aligned}$$

Now we can rewrite u in the form $[a_1, v_1'] \cdots [a_d, v_d']$ so

$$g = [a_1, x_1] \cdots [a_d, x_d][a_1, v_1'] \cdots [a_d, v_d'] = [a_1, x_1 v_1'] \cdots [a_d, x_d v_d'].$$

□

Proposition 4.17. *Let G be a tfg pro-p group. Then $[G, G]$ is closed in G.*

Proof. Let $a_1, \dots, a_d$ be a tgs for G. Let

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

X is the image of the map

$$\begin{aligned}G^d &\to G\\ (x_1, \dots x_d) &\mapsto [a_1, x_1] \cdots [a_d, x_d]\end{aligned}$$

so is compact so closed. Obviously $X \subseteq [G, G]$. Let $g \in [G, G]$. Let $G = \varprojlim G_j$ where $p_j : G \to G_j$. Then $p_j(g) \in [G_j, G_j]$. G_j is nilpotent as it is a p-group. By the previous lemma

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

for some $x_1, \dots, x_d \in G_j$. Hence $p_j(g) \in p_j(X)$ for all j so $g \in \overline{X} = X$. □

Proposition 4.18. *Let G be a pro-p group and let K be a finite index subgroup. Then $[G : K]$ is a power of p.*

Proof. wlog assume K is normal (otherwise replace K by its core). Let $[G : K] = m = p^r m'$ where m' is coprime to p. Consider $X = \{g^m : g \in G\}$. Then $X \subseteq K$ by Lagrange. X is closed so

$$X = \overline{X} = \bigcap_{N \trianglelefteq_o G} XN.$$

We will show that $g^{p^r} \in X \subseteq K$ for all $g \in G$, and this shows $[G : K]$ divides p^r (?). Let $N \trianglelefteq_o G$ be open normal. Let $[G : N] = p^s$ for some s. Let $t = \max(r, s)$. Then $g^{p^s} \in N$ for all $g \in G$. But $(m, p^t) = p^r$ so exists $a, b \in \mathbb{Z}$ such that $am + bp^t = p^r$. Then

$$g^{p^r} = (g^a)^m \cdot (g^b)^{p^t} \in XN.$$

This holds for all $N \trianglelefteq_o G$ so the result follows. □

> **Proposition 4.19.** *If G is a tfg pro-p group then $[G,G]G^p$ is closed in G, hence equal to $\Phi(G)$.*

Proof. Let $G^{\{p\}} = \{g^p : g \in G\}, G^p = \langle G^{\{p\}}\rangle$. As $G/[G,G]$ is abelian,

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

and $[G,G]G^{\{p\}}$ is closed as it is the image of the map

$$\begin{aligned} [G,G] \times G &\to G \\ (x,g) &\mapsto xg^p \end{aligned}$$

□

Proof of Theorem 4.15. Again wlog look at normal subgroups only. Suppose $K \trianglelefteq_f G$ is a counterexample with $[G:K]$ is minimal. Consider

$$M = [G,G]G^pK \trianglelefteq_f G$$

which contains K as a finite index subgroup.

Now G/K is a non-trivial p-group so

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

which is the image of M in G/K. Hence M is a proper subgroup of G so either $M = K$, so $K \geq [G,G]G^p = \Phi(G)$ open, so K open, or $M \neq K$, therefore by minimality K is open in M and M is open in G so K is open in G. □

4.4 Hensel's lemma & p-adic arithmetic

We saw earlier that solving the equation $ax = 1$ in $\mathbb{Z}_p$ just depends on the image of a in $\mathbb{Z}/p$. Hensel's lemma allows us to do so for all polynomials, and gives an algorithm for finding the root.

> **Lemma 4.20.** *Let $f(x)$ be a polynomial with $\mathbb{Z}_p$ coefficients. Then f has a root in $\mathbb{Z}_p$ if and only if it has a root modulo $\mathbb{Z}/p^k$ for all k.*

The aim is to reduce just to mod p. To do so we use the method of *Hensel lifting*. As an example let $p = 7$ and $f(x) = x^2 - 2$. $f(3) = 0 \pmod 7$ so to find a solution mod 49, consider the element $3 + 7a$, $0 \leq a \leq 6$. Then

$$(3 + 7a)^2 = 9 + 7 \cdot 6a + 49a^2 = 2 + 7(1 + 6a) \pmod{49}$$

so we only have to solve a linear equation since the square term vanishes. $a = 1$, for example, gives a solution so $(3 + 7 \cdot 1)^2 = 100 = 2 \pmod{49}$. Next we can consider $10 + 7^2 \cdot a \in \mathbb{Z}/343$ etc.

> **Proposition 4.21** (Hensel's lemma for square roots)**.** *Let $p \neq 2$ be prime. Suppose $\lambda \in \mathbb{Z}_p$ is congruent to a nonzero square $r_1^2 \pmod p$. Then exists a unique $\rho \in \mathbb{Z}_p$ such that $\rho^2 = \lambda$ and $\rho = r_1 \pmod p$.*

Proof. We construct a sequence $r_k \in \mathbb{Z}$, unique modulo p^k, such that

- $r_{k+1} = r_k \pmod{p^k}$,
- $r_k^2 = \lambda \pmod{p^k}$.

The first condition can be either interpreted as (z_k) forming a Cauchy sequence in $\mathbb{Z}_p$, or as $(r_k) \in \prod \mathbb{Z}/p^k$ compatible with transition functions. In either case it gives an elemnt $\rho \in \mathbb{Z}_p$. The second condition then says $\rho^2 = \lambda$.

Suppose we have constructed r_k. Consider the elements $r_k + ap^k$, $0 \leq a < p$. Since $r_k^2 = \lambda \pmod{p^k}$, we can write $r_k^2 = \lambda + b_k p^k$ for some $b_k \in \mathbb{Z}_p$. Then

$$(r_k + p^k a)^2 = \lambda + p^k b_k + 2p^k a r_k + p^{2k} a^2 = \lambda + p^k (b_k + 2ar_k) \pmod{p^{k+1}}$$

Now modulo p,

$$b_k + 2ar_k = b_k + 2ar_1 \pmod{p}$$

has a unique root for $a \pmod{p}$, since $2r_1 \neq 0 \pmod{p}$. Set $r_{k+1} = r_k + p^k a$. □

Proposition 4.22 (Hensel's lemma)**.** *Let $f(x)$ be a polynomial with $\mathbb{Z}_p$ coefficients and let $K \in \mathbb{N}$. Let $r \in \mathbb{Z}_p$ be such that $f(r) = 0 \pmod{p^K}$, $f'(r) \neq 0 \pmod{p}$. Then exist a unique $\rho \in \mathbb{Z}_p$ such that $f(\rho) = 0$ and $\rho = r \pmod{p^K}$.*

This follows immediately from

Lemma 4.23. *For $r, a \in \mathbb{Z}_p$ and $k \geq 1$,*

$$f(r + p^k a) = f(r) + p^k a f'(r) \pmod{p^{k+1}}.$$

Proof. The statement is linear in f so enough to show for $f(x) = x^n$. By binomial formula,

$$\begin{aligned}(r + p^k a)^n &= r^n + np^k a r^{n-1} + \sum_{i=2}^{n} \binom{n}{i} p^{ki} a^i r^{n-i} \\ &= r^n + np^k a r^{n-1} \pmod{p^{k+1}}\end{aligned}$$

□

We can adapt Hensel's lemma to matrix groups.

Definition. Define filtrations

$$\begin{aligned}\mathrm{GL}_N^{(k)}(\mathbb{Z}_p) &= \ker(\mathrm{GL}_N(\mathbb{Z}_p) \to \mathrm{GL}_N(\mathbb{Z}/p^k)) \\ &= \{I + p^k A : A \in \mathrm{Mat}_{N\times N}(\mathbb{Z}_p)\} \\ \mathrm{SL}_N^{(k)}(\mathbb{Z}_p) &= \ker(\mathrm{SL}_N(\mathbb{Z}_p) \to \mathrm{SL}_N(\mathbb{Z}/p^k)) \\ &= \{I + p^k A : A \in \mathrm{Mat}_{N\times N}(\mathbb{Z}_p), \det(I + p^k A) = 1\}\end{aligned}$$

Proposition 4.24. $\mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$ *and* $\mathrm{SL}_N^{(1)}(\mathbb{Z}_p)$ *are pro-p groups.*

Proof. Write

$$\mathrm{GL}_N^{(1)}(\mathbb{Z}_p) = \varprojlim_{k\in\mathbb{Z}} \mathrm{GL}_N^{(1)}(\mathbb{Z}/p^k)$$

and $\mathrm{GL}_N^{(1)}(\mathbb{Z}/p^k) = \{I+pA : A \in \mathrm{Mat}_{N\times N}(\mathbb{Z}/p^k)\}$ has order $p^{N^2(k-1)}$. $\mathrm{SL}_N^{(1)}(\mathbb{Z}_p)$ is a closed subgroup of $\mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$ and is also a pro-p group. □

For the rest of the section we assume p is an odd prime.

Proposition 4.25. *The continuous function $A \mapsto A^p$ maps $\mathrm{GL}_N^{(k)}(\mathbb{Z}_p)$ onto $\mathrm{GL}_N^{(k+1)}(\mathbb{Z}_p)$. Same for* SL.

Slogan: every element in $\mathrm{GL}_n^{k+1}(\mathbb{Z}_p)$ has a pth root.

Proof. The proof is by Hensel-like successive approximations. Claim for all $r \geq 1$, for all A,

$$(I+p^rA)^p = I + p^{r+1}A + p^{r+2}B = I + p^{r+1}A \pmod{p^{r+2}}$$

where B is some polynomial of A: for $\ell \geq 2$ the term

$$\binom{p}{p-\ell} p^{r\ell}A^\ell$$

always has a factor p^{r+2}.

Let $I+p^{k+1}A \in \mathrm{GL}_N^{(k+1)}(\mathbb{Z}_p)$. We show inductively that: for all $n \geq 1$, exist matrices B_n, E_n both expressible as polynomials in A such that

- $B_{n+1} = B_n \pmod{p^n}$,
- $(I+p^kB_n)^p = I + p^{k+1}A + p^{k+n+1}E_n$.

Note that B_n, E_n's commute and therefore we can apply binomial theorem. For $n = 1$, choose $B_1 = A$. Then

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

Inductively define $B_{n+1} = B_n - p^nE_n$,

$$\begin{aligned}(I+p^kB_{n+1})^p &= (I+p^kB_n - p^{k+n}E_n)^p \\ &= (I+p^kB_n)^p - p\cdot p^{k+n}E_n(I+p^kB_n)^{p-1} + O(p^{k+n+2}) \\ &= I + p^{k+1}A + p^{k+n+1}E_n - p^{k+n+1}E_n(I+O(p^k)) + O(p^{k+n+2}) \\ &= I + p^{k+1}A + p^{k+n+2}E_{n+1}\end{aligned}$$

for some E_{n+1}. Thus the proposition holds for GL.

For SL, suffcies to show $\det C^p = 1$ then $\det C = 1$. See example sheet 3 Q10: $\mathbb{Z}_p^\times = \mathbb{Z}_p \times C_{p-1}$. □

Lemma 4.26.

$$(I+p^kA)(I+p^kB) = (I+p^kB)(I+p^kA) = I + p^k(A+B) \pmod{p^{k+1}}.$$

Proposition 4.27. *For all k,*

$$\Phi(\mathrm{GL}_N^{(k)}(\mathbb{Z}_p)) = \mathrm{GL}_N^{(k+1)}(\mathbb{Z}_p)$$

and

$$\mathrm{GL}_N^{(k)} / \mathrm{GL}_N^{(k+1)} \cong \mathbb{F}_p^{N^2}.$$

Proof. By the previous proposition

$$\mathrm{GL}_N^{(k+1)} \subseteq (\mathrm{GL}_N^{(k)})^p \subseteq \Phi(\mathrm{GL}_n^{(k)}).$$

By the lemma $\mathrm{GL}_N^{(k)} / \mathrm{GL}_N^{(k+1)}$ is abelian and of exponent p so is isomorphic to $\mathbb{F}_p^d$ for some d. But we have already seen that $|\mathrm{GL}_N^{(k)} / \mathrm{GL}_N^{(k+1)}| = p^{N^2}$ so $d = N^2$. As $\Phi(\mathbb{F}_p^{N^2}) = 1$, $\Phi(\mathrm{GL}_N^{(k)}) \subseteq \mathrm{GL}_N^{(k+1)}$. □

Corollary 4.28. *For any k, the continuous map $A \mapsto A^p$ induces an isomorphism*

$$\mathrm{GL}_N^{(k)} / \mathrm{GL}_N^{(k+1)} \to \mathrm{GL}_N^{(k+1)} / \mathrm{GL}_N^{(k+2)}.$$

Theorem 4.29. *If H is a closed subgroup of $\mathrm{GL}_N^{(1)}$ then $d(H) \leq N^2$.*

Proof. Suffices to show $d(H) \leq N^2$ for any subgroup H of each finite group $G = \mathrm{GL}_N^{(1)} / \mathrm{GL}_N^{(k+1)}$ for each k. For each $H \leq G$, for $m \leq k$, set

$$\begin{aligned} G_m &= \mathrm{GL}_N^{(m)} / \mathrm{GL}_N^{(k+1)} \\ H_m &= H \cap G_m \end{aligned}$$

Induction to show $d(H_m) \leq N^2$: for $m = k$

$$H_k \leq G_k = \mathrm{GL}_N^{(k)} / \mathrm{GL}_N^{(k+1)} \cong \mathbb{F}_p^{N^2}.$$

Inductively, let e be the dimension of

$$H_m/H_{m+1} \leq G_m/G_{m+1} \cong \mathbb{F}_p^{N^2}.$$

Have a surjection $H_m/\Phi(H_m) \to H_m/H_{m+1}$ (?). Take e elements $h_1, \dots, h_e$ of H_m which generate H_m/H_{m+1}. The pth-power map gives an isomorphism $G_m/G_{m+1} \cong G_{m+1}/G_{m+2}$ and hence $h_1^p, \cdots, h_e^p$ are linearly independent in G_{m+1}/G_{m+2}, thus linearly independent in $H_{m+1}/\Phi(H_{m+1})$ (?). By extending to a basis, we can find $y_1, \dots, y_{d-e}$ elements of H_{m+1} such that $H_{m+1} = \langle h_1^p, \dots, h_e^p, y_1, \dots, y_{d-e}\rangle$. Then

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

so $d(H_m) \leq d(H_{m+1})$. □

Corollary 4.30 (Non-examinable)**.** *There is no closed nonabelian free pro-p subgroup in* $\mathrm{GL}_N(\mathbb{Z}_p)$*.*

Sketch proof. $\hat{F}_{(p)}$ has normal subgroups of index p^n for all n. These subgroups, by a form of basic correspondence, are free pro-p of rank $p^n(r-1)+1$, absurd. □

Compare this with the result that $\mathrm{SL}_2(\mathbb{Z})$ contains a nonabelian free subgroup.

As a converse we have

Theorem 4.31 (Non-examinable)**.** *If G is a pro-p group and exists R such that $d(H) \leq R$ for all $H \leq_c G$ then there exists an abelian normal subgroup $A \cong \mathbb{Z}_p^e \leq G$ $(e \leq R)$ such that $G/A \hookrightarrow \mathrm{GL}_R(\mathbb{Z}_p) \times F$ where F is a finite p-group.*

5 Cohomology of groups

5.1 Group rings and chain complexes

Let G be an abstract group.

> **Definition** (group ring)**.** The *group ring* $\mathbb{Z}G$ is the free abelian group with basis G, with multiplication given on basis elements by $g \cdot h = gh$.

$\mathbb{Z}G$ is in general noncommutative, but is commutative if G is abelian. The multiplicative identity is $1e = e$. Note that $\mathbb{Z}G$ is not necessarily an integral domain, for example if G has torsion element.

> **Definition** (G-module)**.** A *G-module* is a $\mathbb{Z}G$-module.

Remark.

1. We only need to think about the action of basis elements.
2. A G-module M is trivial if $g \cdot m = m$ for all $g \in G, m \in M$.

> **Definition.** If M_1, M_2 are G-modules, a morphism of G-modules or a G-linear map is a $\mathbb{Z}G$-module homomorphism $M_1 \to M_2$.

> **Definition.** Let M_1, M_2 be G-modules. The Hom-*group* $\operatorname{Hom}_G(M_1, M_2)$ is the set of G-linear maps $M_1 \to G_2$ with the structure of an abelian group.

> **Definition** (chain complex)**.** A *chain complex of G-modules* is a sequence of G-modules and G-module maps
>
> $$M_s \longrightarrow \cdots \longrightarrow M_n \xrightarrow{d_n} \cdots \xrightarrow{d_{t+1}} M_t \longrightarrow \cdots \longrightarrow M_t$$
>
> such that $d_n \circ d_{n+1} = 0$ for all n. Sometimes the chain complex is written as (M_n, d_n).
>
> The complex is *exact at M_n* if $\operatorname{im} d_{n+1} = \ker d_n$. The complex is *exact* if it is exact at M_n for all $t < n < s$.
>
> The *homology* of the complex is the sequence of abelian groups $H_S(M_\bullet) = \ker d_S, H_m(M_\bullet) = \ker d_n / \operatorname{im} d_{n+1}, H_t(M_\bullet) = M_t / \operatorname{im} d_{t+1}$.

Revision on free/projective modules and free/projective resolution.

Example. Let X be a 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. Now G acts on $\widetilde{X}$ with quotient X and no fixed points. Thus 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

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

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

Definition (group cohomology)**.** Let $F_\bullet$ be a projective resolution of $\mathbb{Z}$ by G-modules. Let M be a G-module. Apply the functor $\operatorname{Hom}_G(-, M)$ to get a chain complex

$$\operatorname{Hom}_G(F_0, M) \xrightarrow{d^1} \operatorname{Hom}_G(F_1, M) \xrightarrow{d^2} \cdots$$

The *nth cohomoogy group with coefficients in M* is then

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

Elements of $\ker d^{n+1}$ and $\operatorname{im} d^n$ are called *n-cocycles* and *n-coboundaries* respectively.

Example. Let $G = \mathbb{Z} = \langle t \rangle$ (written multiplicatively). Consider the chain complex

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

where

$$\begin{aligned} \varepsilon(\textstyle\sum n_g g) &= \textstyle\sum n_g \\ d_1(x) &= x(t-1) \end{aligned}$$

It is easy to check this is exact with perhaps the exception $\ker \varepsilon \subseteq \operatorname{im} d_1$. To do so suppose $x = \sum_{k=K}^{L} n_k t^k \in \ker \varepsilon$ so $\sum n_k = 0$. Then

$$\begin{aligned} x &= n_L t^{L-1}(t-1) + n_L t^{L-1} + \sum_{k=K}^{L-1} n_k t^k \\ &= n_L t^{L-1}(t-1) + (n_L + n_{L-1}) t^{L-2}(t-1) + (n_L + n_{L-1}) t^{L-2} + \sum_{k=K}^{L-2} n_k t^k \\ &= \cdots \\ &= \text{ some expression } \cdot (t-1) + \underbrace{(n_L + \cdots + n_K) t^{K-1}}_{=0} \end{aligned}$$

Now let M be a G-module and apply $\operatorname{Hom}_G(-, M)$ to get

$$\operatorname{Hom}_G(\mathbb{Z}G, M) \xrightarrow{d^1} \operatorname{Hom}_G(\mathbb{Z}G, M) \longrightarrow 0$$

Note that $\operatorname{Hom}_G(\mathbb{Z}G, M) \cong M$ as abelian groups so we can rewrite the chain complex as

$$M \xrightarrow{(t-1)\cdot} M \longrightarrow 0$$

so

$$\begin{aligned} H^0(G, M) &= \ker d^1 = \{m \in M : tm = m\} = M^G \\ H^1(G, M) &= M / \operatorname{im} d^1 = M / \langle (t-1) M \rangle = M_G \end{aligned}$$

which are called *invariants* and *coinvariants* of M respectively. $H^n(G, M) = 0$ for $n \geq 2$.

Proposition 5.1. *If G is a free group then $H^n(G, M) = 0$ for all $n \geq 2$.*

Non-examinable. Let X be a wedge of circles with $\pi_1 X = G$. The universal cover $\widetilde{X}$ is a tree so contractible. The simplicial chain complex of $\widetilde{X}$ gives a free resolution of G-modules of length 1. □

Definition (cohomological dimension)**.** A group G has *cohomological dimension n*, written $\operatorname{cd}(G) = n$, if $H^m(G, M) = 0$ for all M for all $m > n$ but exists M such that $H^n(G, M) \neq 0$. If no such n exists then $\operatorname{cd}(G) = \infty$.

Thus free groups have cohomological dimension 1. The converse is a also true, by a deep theorem of Stallings and Swan.

We now investigate morphisms between complexes of G-modules, which should really be done in the context of homological algebra using derived categories. The proofs are omitted.

Definition (chain map)**.** Let (A_n, α_n) and (B_n, β_n) be chain complexes of G-modules. A *chain map* 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 5.2. *A chain map $(f_n) : (A_n) \to (B_n)$ induces maps $f_* : H_n(A_\bullet) \to H_n(B_\bullet)$.*

Corollary 5.3. *A G-linear map $f : M \to N$ induces maps $f_* : H^*(G, M) \to H^*(G, N)$.*

Proposition 5.4. *If*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

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

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

5.2 Different projective resolutions

Theorem 5.5. *The definition of $H^n(G, M)$ does not depend on the choice of projective resolutions.*

This follows from the homological algebra fact that projective resolutions are unique up to quasi-isomorphism. The proof is non-examniable *except* for the definition of the chain map between two complexes.

5.3 Bar resolution

We define the so-called bar resolution for the trivial G-module $\mathbb{Z}$. Let $G^{(n)}$ be the set of symbols $[g_1|g_2|\cdots|g_n]$, $g_i \in G$. Let $F_n = \mathbb{Z}G\{G^{(n)}\}$. Define

$$\begin{aligned} d_0 : F_0 &\to \mathbb{Z} \\ \sum n_g g &\mapsto \sum n_g \end{aligned}$$

i.e. the augmentation map. Define

$$\begin{aligned} d_n : F_n &\to F_{n-1} \\ [g_1|\cdots|g_n] &\mapsto g_1[g_2|\cdots|g_n] \\ &\quad + \sum (-1)^i [g_1|\cdots|g_i g_{i+1}|\cdots|g_n] \\ &\quad + (-1)^n [g_1|\cdots|g_{n-1}] \end{aligned}$$

Proposition 5.6. *The bar resolution is a free resolution of $\mathbb{Z}$ by G-modules.*

Non-examinable. F_n is G-isomorphic to $\mathbb{Z}\{G^{n+1}\}$ (with diagonal G-action) via $[g_1|\cdots|g_n] \mapsto (1, g_1, g_1g_2, \dots, g_1\cdots g_n)$. The latter is a chain complex with boundary maps

$$(g_0, \dots, g_n) \mapsto \sum (-1)^i (g_0, \dots, \hat{g}_i, \dots, g_n)$$

and the complex is acyclic via the obvious chain homotopy

$$(g_0, \dots, g_n) \mapsto (1, g_0, \dots, g_n).$$

□

Since different projective resolutions give the same cohomology groups we might reinterpret group cohomology in terms of bar resolution.

Definition. The group of *nth cochains* of G with coefficients in M is

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

The *nth coboundary map* is

$$\begin{aligned} d^n : C^{n-1}(G, M) &\to C^n(G, M) \\ \phi &\mapsto ((g_1, \dots, g_n) \mapsto g_1 \cdot \phi(g_2, \dots, g_n) \\ &\quad + \sum (-1)^i \phi(g_1 g_2, \dots, g_n) \\ &\quad + (-1)^n \phi(g_1, \dots g_{n-1}) \end{aligned}$$

The *nth cocycle* and *nth coboundary* are

$$\begin{aligned} Z^n(G, M) &= \ker d^{n+1} \\ B^n(G, M) &= \operatorname{im} d^n \end{aligned}$$

The *nth cohomology* is defined to be

$$H^n(G,M) = Z^n(G,M)/B^n(G,M).$$

We can write out the low-dimensional cocyles and coboundaries explicitly.

$$H^0(G,M) = \ker d^1 = \{m \in M : gm = m \text{ for all } g\} = M^G$$

is called the set of *invariants* of M.

$$\begin{aligned} \ker d^2 &= \{\phi : G \to M : \phi(gh) = g\phi(h) + \phi(g)\} \\ \operatorname{im} d^1 &= \{\phi : G \to M : \text{ exists } m \text{ such that } \phi(g) = (g-1)m\} \end{aligned}$$

are called *crossed homomorphisms* and *principal crossed homomorphisms.*

Example. If M has trivial G-action then

$$H^1(G,M) = \operatorname{Hom}(G,M).$$

Proposition 5.7. *Let $\alpha : G_1 \to G_2$ be a group homomorphism and M a G_2-module. Then there is a natural homomorphism $\alpha^* : H^n(G_2,M) \to H^n(G_1,M)$.*

Proof. Given $f \in C^n(G_2,M)$, set $\alpha^* f \in C^n(G_1,M)$ to be the composition $f \circ \alpha^n$. □

Suppose we have a short sequence of groups

$$1 \longrightarrow H \longrightarrow G \longrightarrow Q \longrightarrow 1.$$

There is in general no long exact sequence on cohomologies in the style of the snake lemma.

Example. Let $M = \mathbb{Z}$ (with trivial actions) and a short exact sequence $0 \to \mathbb{Z} \to \mathbb{Z}^2 \to \mathbb{Z} \to 0$. Then the sequence

$$\begin{tikzcd} H^2(\mathbb{Z},\mathbb{Z}) \arrow[r] \arrow[d, equal] & H^2(\mathbb{Z}^2,\mathbb{Z}) \arrow[r] & H^2(\mathbb{Z},\mathbb{Z}) \arrow[d, equal] \\ 0 & & 0 \end{tikzcd}$$

cannot be exact as $H^2(\mathbb{Z}^2,\mathbb{Z}) \neq 0$.

There is, however, *some* exact sequences coming from spectral sequences, namely the five-term exact sequence. In low dimensions they can be described explicitly. We state the result below and sketch the proof.

Lemma 5.8. *Let $H \trianglelefteq G$ and let M be a G-module. Let G act on $C^n(H,M)$ via*

$$(g \cdot \phi)(h_1, \dots, h_n) = g\phi(g^{-1}h_1 g, \dots, g^{-1}h_n g).$$

Then this gives an action of G on $H^n(H,M)$. Moreover H acts trivially.

Proof. The first part is an easy computation:

$$\begin{aligned}(g\cdot d^n\phi)(h_1,\dots,h_n) &= gd^n\phi(g^{-1}h_1g,\dots,g^{-1}h_ng)\\ &= g(g^{-1}h_1g)\phi(g^{-1}h_2g,\dots,g^{-1}h_ng)\\ &+\sum(-1)^i g\phi(g^{-1}h_1g,\dots,g^{-1}h_ih_{i+1}g,\dots,g^{-1}h_ng)\\ &+(-1)^n g\phi(g^{-1}h_1g,\dots,g^{-1}h_{n-1}g)\\ &= h_1(g\cdot\phi)(h_2,\dots,h_n)\\ &+\sum(-1)^i d(g\cdot\phi)(h_1,\dots,h_ih_{i+1},\dots,h_n)\\ &+(-1)^n d(g\cdot\phi)(h_1,\dots,h_{n-1})\\ &= (d^n(g\cdot\phi))(h_1,\dots,h_n)\end{aligned}$$

To show H acts trivially, we show if $h\in H$, $\phi\in Z^n(G,M)$ then $h\cdot\phi-\phi\in\operatorname{im} d^n$. Induction on n. $n=1$,

$$0=(d^2\phi)(h_1,h_2)=h_1\phi(h_2)-\phi(h_1h_2)+\phi(h_1)$$

so

$$\phi(h_1h_2)=h_1\phi(h_2)+\phi(h_1)$$

then

$$\begin{aligned}(h\cdot\phi-\phi)(h_1) &= (h\cdot\phi)(h_1)-\phi(h_1)\\ &= h\phi(h^{-1}h_1h)-\phi(h_1)\\ &= h(h^{-1}\phi(h_1h)+\phi(h^{-1}))-\phi(h_1)\\ &= h_1\phi(h)+\phi(h_1)+h\phi(h^{-1})-\phi(h_1)\\ &= h_1\phi(h)-\phi(h)\\ &= (h_1-1)\phi(h)\in\operatorname{im} d^1\end{aligned}$$

The induction process is another messy calculation and is left as an exercise. □

Note if G has trivial action and $\phi\in C^1(H,M)$ then

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

so $\phi\in H^1(H,M)^G$ if and only if $\phi(h)=\phi(g^{-1}hg)$ for all $g\in G, h\in H$. Such a $\phi: H\to M$ is called a G-invariant homomorphism.

Theorem 5.9 (inflation-restriction exact sequence)**.** *Let $H\trianglelefteq G$ and $Q=G/H$. Let M be a G-module. Then there is an exact sequence*

$$\begin{tikzcd} 0 \arrow[r] & H^1(Q,M^H) \arrow[r] & H^1(G,M) \arrow[r] & H^1(H,M)^G \arrow[dll] \\ & H^2(Q,M^H) \arrow[r] & H^2(G,M) & \end{tikzcd}$$

Note that $H^1(H,M)^G=H^1(H,M)^Q$ by the previous lemma.

Non-examinable. We only define the maps appearing in the sequence. This is done via the restriction map

$$\begin{aligned} H^n(G,M) &\to H^n(H,M)^G \\ \phi &\mapsto \phi|_{H^n} \end{aligned}$$

the inflation map

$$\begin{aligned} H^n(Q,M^H) &\to H^n(G,M) \\ \phi &\mapsto \phi \circ q^n \end{aligned}$$

where $q : G \to Q$, and the transgression map $Tg : H^1(H,M) \to H^2(Q,M^H)$ defined as follow: choose a set-theoretic section $s : Q \to G$, i.e. a transversal, with $s(1) = 1$. Define

$$\begin{aligned} \rho : G &\to H \\ g &\mapsto g \cdot s(gH)^{-1} \end{aligned}$$

If $\phi : H \to M$ is a Q-invariant cocycle, define

$$\begin{aligned} Tg(\phi) : G^2 &\to M \\ (g_1,g_2) &\mapsto \phi(\rho(g_1)\rho(g_2)) - \phi(\rho(g_1g_2)) \end{aligned}$$

$Tg(\phi)$ descends to $Q^2 \to M$. □

> **Corollary 5.10** (Hopf formula)**.** *Let F be free, $R \trianglelefteq F$ and $Q = F/R$. If A is abelian with trivial F-action then*
>
> $$H^2(Q,A) \cong \frac{\{F\text{-invariant homomorphisms } R \to A\}}{\{\text{restrictions of homomorphisms } F \to A\}}.$$

Example. Suppose $Q = \langle x_1,\dots,x_d | r_1,\dots,r_n \rangle$ is a presentation, so $F = F\{x_1,\dots,x_d\}, R = \langle\langle r_1,\dots,r_m \rangle\rangle$. Then

$$\begin{aligned} d(H^1(Q,\mathbb{Z})) &\le d \\ d(H^2(Q,\mathbb{Z})) &\le m \end{aligned}$$

5.4 Cohomology and group extensions

Let E be a group, with an abelian normal subgroup M. Let $G = E/M$. Such an E is called an *extension of G by M*. Two extensions are *equivalent* if there is a commutative diagram of homomorphisms

$$\begin{tikzcd} 1 \arrow[r] & M \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & M \arrow[r] & E' \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

Lemma 5.11. *Equivalent extensions are isomorphic as groups.*

Proof. Same as five lemma. □

Note that M comes with the structure of a G-module: the conjugation action of E on M descends to a G-action. If this action is trivial, the extension is called a *central extension.*

Given a G-module M, the group extension problem is concerned about the classification of the extensions. We can always form the *semidirect product* $E = M \rtimes G$. It is sometimes also called a *split extension.*

Definition (splitting)**.** The *splitting* of an extension E is a group homomorphism $G \to E$ that is a section to $E \to G$.

Proposition 5.12. *Extensions which have a splitting are equivalent to* $M \rtimes G$.

Proof. Set $M \rtimes G \to E, (m, g) \mapsto i(m)s(g)$ where s is a section of $E \to G$. □

Let E be an arbitrary extension of G by M. Let $s : G \to E$ be a set-theoretic section with $s(1) = 1$. To measure how far s is from being a homomorphism, consider the function

$$\phi(g_1, g_2) = s(g_1)s(g_2)s(g_1g_2)^{-1}.$$

Then s is a homomorphism if and only if ϕ is constant. The image of ϕ is in M so $\phi : G^2 \to M$ is an element of $C^2(G, M)$. Claim that in fact $\phi \in Z^2(G, M)$.

Proof. We compute $s(g_1)s(g_2)s(g_3)$ in two ways:

$$\begin{aligned} s(g_1)s(g_2)s(g_3) &= \phi(g_1, g_2)s(g_1g_2)s(g_3) \\ &= \phi(g_1, g_2)\phi(g_1g_2, g_3)s(g_1g_2g_3) \\ s(g_1)s(g_2)s(g_3) &= s(g_1)\phi(g_2, g_3)s(g_2g_3) \\ &= s(g_1)\phi(g_2, g_3)s(g_1)^{-1}s(g_1)s(g_2g_3) \\ &= s(g_1)\phi(g_2, g_3)s(g_1)^{-1}\phi(g_1, g_2g_3)s(g_1g_2g_3) \end{aligned}$$

so

$$\phi(g_1, g_2)\phi(g_1g_2, g_3) = s(g_1)\phi(g_2, g_3)s(g_1)^{-1}\phi(g_1, g_2g_3).$$

Recognising the first three terms on RHS as the action of G on M and convert to additive notation in M, we get

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

□

In addition ϕ is a *normalised cocycle*, i.e.

$$\phi(1, g) = \phi(g, 1) = 0.$$

If we had chosen a different section $s' : G \to E$, consider $\psi(g) = s'(g)s(g)^{-1}$ so $\psi \in C^1(G, M)$. Have

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

and a comparison with $s'(g_1)s'(g_2) = \phi'(g_1, g_2)s'(g_1g_2)$ shows $[\phi] \in H^2(G, M)$ is well-defined. This shows part of

> **Theorem 5.13.** *Let G be a group and M a G-module. There exists a bijection*
>
> $$\{\textit{equivalence classes of extensions of } G \textit{ by } M\} \longleftrightarrow H^2(G, M).$$

Proof. Let to construct the 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

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

By the assumption on ϕ, this defines a group structure with identity $(0, 1)$ and the inverse of (m, g) is $(-g^{-1} \cdot (m + \phi(g, g^{-1})), g^{-1})$. This is an extension.

If we choose a different normalised cocycle ϕ' such that $\phi - \phi' = d^2\psi$, then the obvious map $E_\phi \to E_{\phi'}, (m, g) \mapsto (m + \psi(g), g)$ is an equivalence of extensions.

It is an exercise to check the two maps are inverses to each other. □

One result that is used in the proof is

> **Lemma 5.14.** *Every cohomology class is represented by some normalised cocycle.*

Proof. Let $\phi \in Z^2(G, M)$. Let $\psi(g) = \phi(1, g)$. Then $\phi - d^2\psi$ is normalised:

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

and they both vanish since ϕ is a cocycle. □

We may recover Hopf formula from this identification. Suppose G has presentation $\langle x_1, \dots, x_n | r_1, \dots, r_m \rangle$. Then take F to be the free groups on x_i's and $R = \ker(F \to G)$. Suppose E is a central extension of G by A. Choose some preimages $\overline{x}_i \in E$ of generators 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 $\overline{x}_i$. Then $\overline{r}_i \in A = \ker(E \to G)$, say a_i. Write down a group presentation

$$\overline{E} = \langle \overline{x}_1, \dots, \overline{x}_n, A | \overline{r}_1 = a_1, \dots, \overline{r}_m = a_m, A \text{ central}, \text{relations of A} \rangle$$

There exists a natural diagram of exact rows

$$\begin{tikzcd} & A \arrow[r] \arrow[d, equal] & \overline{E} \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & A \arrow[r] & E \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

It follows that $A \hookrightarrow \overline{E}$ and $\overline{E} \cong E$. Can try to define F-invariant homomorphism $R \to A$ by $r_i \mapsto a_i$. Fact (non-examinable): this is a well-defined F-invariant homomorphism if and only if $A \to \overline{E}$ is an injection. We made a choice of preimages $\overline{x}_i$ of x_i in E. A different choice $\overline{x}_i'$ differ from $\overline{x}_i$ by an element $b_i \in A$. Then $x_i \mapsto b_i$ gives a homomoprhism $f : F \to A$ and $\overline{r}_i' = \overline{r}_i f(b_i)$.

Example. Let $G = \langle x_1, x_2 | x_1 x_2 x_1^{-1} x_2^{-1} x_1 \rangle$. We show $H^2(G, \mathbb{Z}) = 0$. Any central extension of G by $\mathbb{Z}$ has a presentation

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

Now we can make a substitution $\overline{x}_1 \mapsto \overline{x}_1 t^{-k} = \overline{x}_1'$,

$$E \cong \langle \overline{x}_1', \overline{x}_2, t | \overline{x}_1' t^k \cdot \overline{x}_2 (\overline{x}_1' t^k)^{-1} \overline{x}_2^{-1} (\overline{x}_1' t^k) = t^k, t \text{ central} \rangle = E'$$

E and E' are equivalent as extensions and we can simplify E'

$$\langle \overline{x}_1', \overline{x}_2, t | \overline{x}_1' \overline{x}_2 (\overline{x}_1')^{-1} \overline{x}_2^{-1} \overline{x}_1' = 1, t \text{ central} \rangle = \mathbb{Z} \times G$$

It follows that $H^2(G, \mathbb{Z}) = 0$.

5.5 Worked example: $\mathbb{Z}^2$

Let $T = \mathbb{Z}^2 = \langle a, b \rangle$. We will classify all central extensions of T by $\mathbb{Z}$. Start with a free resolution derived from topology

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

where

- ε is the augmentation map.
- $\alpha(x, y) = x(a-1) + y(b-1)$.
- $\beta(z) = (z(1-b), z(a-1))$.

Exactness can either be derived from topology (square tiling of the plane), or direct computation.

Apply $\mathrm{Hom}_{\mathbb{Z}T}(-, \mathbb{Z})$ to get

$$\mathrm{Hom}_{\mathbb{Z}T}(\mathbb{Z}T, \mathbb{Z}) \xrightarrow{\alpha^*} \mathrm{Hom}_{\mathbb{Z}T}((\mathbb{Z}T)^2, \mathbb{Z}) \xrightarrow{\beta^*} \mathrm{Hom}_{\mathbb{Z}T}(\mathbb{Z}T, \mathbb{Z}) \longrightarrow 0$$

where

$$\begin{aligned} \beta^*(f)(z) &= f(z(1-b), z(a-1)) \\ &= f(z - zb, 0) + f(0, za - z) \\ &= (b-1) \cdot f(z, 0) + (1-1) \cdot f(0, z) \\ &= 0 \end{aligned}$$

so $\beta^* = 0$. Similarly $\alpha^* = 0$. Thus

$$H^i(T, \mathbb{Z}) = \begin{cases} \mathbb{Z} & i = 0 \\ \mathbb{Z}^2 & i = 1 \\ \mathbb{Z} & i = 2 \end{cases}$$

To get extensions, we turn to bar resolutions. We seek a chain map

$$\begin{tikzcd}
\dots \arrow[r] & \mathbb{Z}T\{T^2\} \arrow[r, "d_2"] \arrow[d, "f_2"] & \mathbb{Z}T\{T\} \arrow[r, "d_1"] \arrow[d, "f_1"] & \mathbb{Z}T \arrow[r, "\varepsilon"] \arrow[d, "f_0"] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{Z}T \arrow[r, "\beta"] & (\mathbb{Z}T)^2 \arrow[r, "\alpha"] & \mathbb{Z}T \arrow[r, "\varepsilon"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Obviously $f_0 = \mathrm{id}$. f_1 should satisfy $\alpha f_1 = f_0 d_1 = d_1$. Want to find an element $(x_{r,s}, y_{r,s}) \in (\mathbb{Z}T)^2$ such that

$$\alpha(x_{r,s}, y_{r,s}) = d_1([a^r b^s]) = a^r b^s - 1 = (a^r - 1)b^s + (b^s - 1)$$

then define f_1 by $[a^r b^s] \mapsto (x_{r,s}, y_{r,s})$. By commutativity of T,

$$\begin{aligned} x_{r,s} &= \frac{a^r - 1}{a - 1} b^s = S(a, r) b^s \\ y_{r,s} &= \frac{b^s - 1}{b - 1} = S(b, s) \end{aligned}$$

where

$$S(a, r) = \begin{cases} 1 + a + \dots + a^{r-1} & r \geq 0 \\ -(a^{-1} + \dots + a^r) & r < 0 \end{cases}$$

So $f_1([a^r b^s]) = (S(a, r)b^s, S(b, s))$. By a messy calculation we similarly find

$$f_2([a^r b^s | a^t b^u]) = S(a, r) b^s S(b, u).$$

A cohomology class $p \in \mathbb{Z} \cong \mathrm{Hom}_{\mathbb{Z}T}(\mathbb{Z}T, \mathbb{Z})$ is represented by the 2-cochain given by the composition

$$(a^r b^s, a^t b^u) \mapsto S(a, r) b^s S(b, u) \mapsto pru$$

so the group structure on the set $\mathbb{Z} \times T$ corresponding to this cochain is

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

More concretely, this group has a 3-dimensional representation

$$(m, a^r b^s) \mapsto \begin{pmatrix} 1 & pr & m \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix}$$

The group of central extensions of T by $\mathbb{Z}$ is generated by $p = 1$.

5.6 Cohomology of profinite groups

The cohomology theory works for profinite groups.

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

To avoid defining the group ring of a profinite ring, we use the ad hoc definition

Definition. Let G be a profinite group and M a finite G-module. Define

$$C^n(G, M) = \{G^n \to M \text{ continuous}\}$$

and d^n given by the same formula as before. Define $H^n(G, M) = \ker d^{n+1} / \operatorname{im} d^n$.

Course convention: all general results in this chapter and example sheet 4 may be assumed to hold for profinite groups, where all groups are profinite, all functions are continuous and all modules are finite.

Example. An extension of G by M is a profinite group E with $M \trianglelefteq E$ such that $E/M \cong G$. Equivalence of extensions is a continuous homomorphism respecting M and G. Then there exists a bijection between equivalent classes of extensions and $H^2(G, M)$.

One can treat profinite groups as discrete groups, but the resulting cohomology theory is horrid. Another question: why finite modules only? For example consider the exact sequence of $\hat{\mathbb{Z}}$-modules with trivial $\hat{\mathbb{Z}}$-action

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

Have

$$H^1(\hat{\mathbb{Z}}, \mathbb{Z}) = H^1(\hat{\mathbb{Z}}, \mathbb{Q}) = 0$$

as the continuous map from $\hat{\mathbb{Z}} \to \mathbb{Z}$ has compact image. $H^1(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}$. But we should have a long exact sequence, which implies that $H^2(\hat{\mathbb{Z}}, \mathbb{Z})$. Thus free profinite groups $\hat{\mathbb{Z}}$ does not have "cohomologicial dimension" 1.

5.6.1 Pro-p groups of cohomological dimension 1

For simplicity in this section assuming all pro-p groups are tfg. The aim of this section is to prove Stallings-Swan for tfg pro-p groups, i.e. Proposition 5.1 and its converse:

Theorem 5.15. *A tfg pro-p group G is free if and only if* $\operatorname{cd}(G) = 1$*, if and only if* $H^2(G, \mathbb{F}_p) = 0$.

Note that for any non-trivial tfg pro-p group G, in particular free pro-p groups, $\operatorname{cd}(G) \geq 1$ as

$$H^1(G, \mathbb{F}_p) \cong \operatorname{Hom}(G, \mathbb{F}_p) \neq 0.$$

We first show the equivalence of the characterisations

Theorem 5.16. *Let G be a pro-p group. Then*

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

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

Proposition 5.17. *Fix $n \geq 0$. Let G be a profinite group and suppose $H^n(G, S) = 0$ for all simple finite G-modules S. Then $H^n(G, M) = 0$ for all finite M.*

Proof. Suppose for contradiction M of minimal size has nonvanishing $H^n(G, M)$. M is not simple so exists G-submodule $N \leq M$, giving rise to a short exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

of G-modules. By using long exact sequence and minimality of M, $H^n(G, M) = 0$, absurd. □

Definition (p-primary component)**.** Let M be a finite G-module. Let M_p be the Sylow p-subgroup of M, called the *p-primary component* of M. Then $M = \bigoplus_p M_p$.

Proposition 5.18. *Let G be a pro-p group, M a finite G-module. Then*

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

for $n \geq 1$.

Proof. Write $M = M_p \oplus M'$ where M' is the direct sum of other q-primary components. Then

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

(finite p-group case is an exercise in example sheet 4) and we show $H^n(G, M') = 0$. Let $\phi : G^n \to M'$ be a continuous function. Claim ϕ factors as $G^n \to (G/K)^n \to M'$ for some $K \trianglelefteq_o G$.

Proof. We want to find K such that each fibre of ϕ is a union of cosets of K^n. For each $m \in M'$, $\phi^{-1}(m)$ is open and closed, so can be written as $\phi^{-1}(m) = \bigcup (a_i + K_i^n)$ where $K_i \trianglelefteq_o G$. The cover may be taken to be finite and we take K to be the intersection of all the K_i's. □

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

Remark. The argument actually shows that if $G = \varprojlim G/K$ then $H^n(G, M) = \varinjlim H^n(G/K, M)$.

Proposition 5.19. *Let G be a pro-p group. The only simple p-primary G-module is $\mathbb{F}_p$.*

Proof. Example sheet 4. □

Combining these gives

> **Proposition 5.20.** *Let G be a pro-p group. If $H^n(G,\mathbb{F}_p)=0$ then $H^n(G,M)=0$ for all finite modules M.*

> **Proposition 5.21.** *Suppose exists n such that $H^n(G,M)=0$ for all M then $\operatorname{cd}(G)\le n-1$.*

Non-examinable. By course convention we shall prove this for an abstract group G. The main idea is *dimension shifting*: suppose there is a short exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow N \longrightarrow M' \longrightarrow 0$$

where N is cohomologically trivial. Then from the long exact sequence one know $H^i(G,M')\cong H^{i+1}(G,M)$.

Example sheet 4 shows that for $K\le G$, the following holds for the coinduced module $\operatorname{coind}_G^K(M)=\operatorname{Hom}_{\mathbb{Z}K}(\mathbb{Z}G,M)$:

$$H^n(G,\operatorname{coind}_G^K(M))\cong H^n(K,M).$$

So take $K=1$, have $\operatorname{coind}_G^K(M)=\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}G,M)$ cohomologically trivial. Finally the map

$$\begin{aligned}\alpha : M &\to \operatorname{Hom}(\mathbb{Z}G,M)\\ m &\mapsto (x\mapsto xm)\end{aligned}$$

is an injection so gives the required short exact sequence. □

> **Corollary 5.22.** *Free pro-p groups have cohomological dimension 1.*

Proof. Suffice to show $H^2(G,\mathbb{F}_p)=0$, i.e. to show every extension of G by $\mathbb{F}_p$ splits. Let G be free on X for some X finite. Suppose we have an extension

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

E is again a pro-p group. For each $x\in X$ choose a preimage $e_x\in E$. It extends to a unique homomorphism $F(X)\to E$. □

Note that the proof works for free groups as well, so providing an algebraic proof of Proposition 5.1.

> **Theorem 5.23.** *Let G and G' be tfg pro-p groups. Let $f:G\to G'$ be a continuous homomorphism. Assume*
>
> - *$f^*:H^1(G',\mathbb{F}_p)\to H^1(G,\mathbb{F}_p)$ is an isomorphism,*
> - *$f^*:H^2(G',\mathbb{F}_p)\to H^2(G,\mathbb{F}_p)$ is an injection.*
>
> *Then f is an isomorphism.*

Heuristics: $H^1(G,\mathbb{F}_p)=\operatorname{Hom}(G,\mathbb{F}_p)=\operatorname{Hom}(G/\Phi(G),\mathbb{F}_p)$, the dual of the $\mathbb{F}_p$-vector space $G/\Phi(G)$. The first condition tells us something about generators. In particular f is a surjection. H^2 is related to relations, and the second condition says that we impose no additional relations so f is an injection.

Non-examinable. Let $G_n = \gamma_n^{(p)}(G)$, the lower central p-series. Recall that G_n are all open, $G = \varprojlim G/G_n$. G_n's are fully characteristic, therefore inducing maps $f_n : G/G_n \to G'/G'_n$. We will show that they are all isomorphisms and so is f.

Induction on n. For $n = 2$, $f_2 : G/\Phi(G) \to G'/\Phi(G')$. By the remark before the transpose of f_2 is an isomorphism, so is f_2 itself.

Suppose the result holds for n. If we can show $G_n/G_{n+1} \to G'_n/G'_{n+1}$ is an isomorphism then combining the induction hypothesis we deduce the result for $n+1$ from the diagram

$$\begin{tikzcd}
1 \arrow[r] & G_n/G_{n+1} \arrow[r] \arrow[d, "\cong"] & G/G_{n+1} \arrow[r] \arrow[d] & G/G_n \arrow[r] \arrow[d, "\cong"] & 1 \\
1 \arrow[r] & G'_n/G'_{n+1} \arrow[r] & G'/G'_{n+1} \arrow[r] & G'/G'_n \arrow[r] & 1
\end{tikzcd}$$

G_n/G_{n+1} is a finite-dimensional $\mathbb{F}_p$-vector space so $G_n/G_{n+1} \to G'_n/G'_{n+1}$ is an isomorphism if and only if its dual $H^1(G'_n/G'_{n+1}, \mathbb{F}_p) \to H^1(G_n/G_{n+1}, \mathbb{F}_p)$ is. 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 $g \in G, g' \in G_n$, if and only if

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

if and only if ϕ is G-invariant. Thus $H^1(G_n/G_{n+1}, \mathbb{F}_p) = H^1(G_n, \mathbb{F}_p)^G$. The five term exact sequence induced by

$$\begin{tikzcd}
1 \arrow[r] & G_n \arrow[r] & G \arrow[r] & G/G_n \arrow[r] & 1
\end{tikzcd}$$

says we have a commutative diagram of exact sequences

$$\begin{tikzcd}
H^1(G'/G'_n) \arrow[r] \arrow[d, "\cong"] & H^1(G') \arrow[r] \arrow[d, "\cong"] & H^1(G'_n)^{G'} \arrow[r] \arrow[d] & H^2(G'/G'_n) \arrow[r] \arrow[d, "\cong"] & H^2(G') \arrow[d, hook] \\
H^1(G/G_n) \arrow[r] & H^1(G) \arrow[r] & H^1(G_n)^G \arrow[r] & H^2(G/G_n) \arrow[r] & H^2(G)
\end{tikzcd}$$

By induction hypothesis and injectivity on H^2, the middle vertical map is an isomorphism by five lemma. Therefore $G_n/G_{n+1} \cong G'_n/G'_{n+1}$. □

In fact we get for free from the proof

> **Theorem 5.24.** *If Γ and Γ' are finitely generated abstract groups and $f : \Gamma \to \Gamma'$ is a homomorphism and the same conditions hold, then $\hat{f} : \hat{\Gamma}_{(p)} \to \hat{\Gamma}'_{(p)}$ is an isomorphism.*

Proof. Set $\Gamma_n = \gamma_n^{(p)}(\Gamma)$. Then $\hat{\Gamma}_{(p)} = \varprojlim \Gamma/\Gamma_n$. Proceed as before. □

Proof of Theorem 5.15. Suppose $x_1, \dots, x_d$ is a generating set of minimal size. Let F be the free pro-p group on x_i and consider $f : F \to G$. $F/\Phi(F) \to G/\Phi(G)$ is an isomorphism since they are the same $\mathbb{F}_p$-vector space and $H^2(G, \mathbb{F}_p) \to H^2(F, \mathbb{F}_p)$ is an injecition. Thus f is an isomorphism. □

Example. Let $\Gamma = \langle x_1, x_2 | x_1 x_2 x_1^{-1} x_2^{-1} x_1 \rangle$. Recall $H^2(\Gamma, \mathbb{Z}) = 0$. The same argument shows $H^2(\Gamma, \mathbb{F}_p) = 0$. $H^1(\Gamma, \mathbb{F}_p) = \mathrm{Hom}(\Gamma, \mathbb{F}_p)$. Let $\phi : \Gamma \to \mathbb{F}_p$. Then

$$0 = \phi(x_1 x_2 x_1^{-1} x_2^{-1} x_1) = \phi(x_1)$$

and no further relation so $H^1(\Gamma, \mathbb{F}_p) = \mathbb{F}_p$ generated by $x_1 \mapsto 0, x_2 \mapsto 1$. Let $f : \mathbb{Z} \to \Gamma, 1 \mapsto x_2$. Then f induces $\hat{\Gamma}_{(p)} \cong \mathbb{Z}_p$.

5.6.2 Presentation of pro-p groups

> **Definition** (presentation of pro-p group)**.** Let X be a finite set and F a free pro-p group on X. Let $R \subseteq F$. The pro-p group with *presentation* $\lfloor X | R \rfloor_p$ is defined to be $F / \overline{\langle\langle R \rangle\rangle}$.

Note that not all elements in $\lfloor X | R \rfloor_p$ can be written as a product of elements of X.

> **Lemma 5.25.** *Let F_{abs} be the abstract free group on X and let $R \subseteq F_{\text{abs}}$. Let $\Gamma = \langle X | R \rangle, G = \lfloor X | R \rfloor_p$. Then $G = \hat{\Gamma}_{(p)}$.*

Proof. Suffices to look at the p-group quotients of G and Γ. A quotient $\Gamma \to P$, where P is a p-group, is the same as a function $X \to P$ such that its extension to F_{abs} contains R in the kernel. But this is exactly the same as a continuous quotient $G \to P$. □

> **Theorem 5.26.** *Let G be a tfg pro-p group. Let X be a finite tgs of G. Let r_X be the minimal size of a set $R \subseteq F(X)$ such that $G = \lfloor X | R \rfloor_p$. 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 a minimal generating set then $r_X = \dim H^2(G, \mathbb{F}_p)$.*

Remark.

1. One may ask the same question for abstract groups. If Γ is a finitely generated (abstract) group, X a finite generating set, let ρ_X be the minimal size of an R such that $\Gamma = \langle X | R \rangle$. Then what can we say about $|X| - \rho_X$? It is a subtle question and in general the answer depends on X.

2. For G finite p-group, let X be a generating set. One may ask must $\rho_X = r_X$? Certainly $r_X \leq \rho_X$ by the lemma. The other direction is open.

> **Lemma 5.27.** *Let G and L be profinite groups. Assume L acts continuously on G by homomorphism via $\rho : L \times G \to G$. Then there is a proper open normal subgroup of G which is invariant under the action of L.*

Note that if we assume G is tfg then this follows from the old trick of taking all intersections.

Proof. Let U be a proper open normal subgroup of G. Claim $\tilde{L} = \{\ell \in L : \ell \cdot U = U\}$ is open in L. If this claim holds, there are finitely many subgroups of the form $\ell \cdot U$ by orbit-stabiliser. Their intersection is then an L-invariant open normal subgroup.

Let $\ell \in \tilde{L}$. For each $u \in U$ we have $\ell \cdot u \in U$. Can find $A_u \subseteq L, B_u \subseteq U$ open such that

$$(\ell, u) \in A_u \times B_u \subseteq \rho^{-1}(U).$$

B_u's cover U which is compact so we can take a finite subcover $B_{u_1}, \dots, B_{u_k}$. Take $A = A_{u_1} \cap \cdots \cap A_{u_k}$. Left to show $A \subseteq \tilde{L}$: if $a \in A, u \in U$ then exists u_i such that $u \in B_{u_i}$ and $a \in A_{u_i}$, hence $(a, u) \in A_{u_i} \times B_{u_i} \subseteq \rho^{-1}(U)$. Thus $A \cdot U \subseteq U$. □

> **Lemma 5.28.** *Let F be a free pro-p group, $N \trianglelefteq F$ a closed proper normal subgroup of F. Then exists a set $R \subseteq N$ of size r such that $N = \overline{\langle\langle R \rangle\rangle}$ if and only if* $\dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^F \leq r$.

Proof. Recall

$$\begin{aligned} H^1(N, \mathbb{F}_p)^F &= \{\phi : N \to \mathbb{F}_p \text{ homomorphism such that } \phi(f^{-1}nf) = \phi(n)\} \\ &= \{\phi : N/N^p[N, F] \to \mathbb{F}_p\} \end{aligned}$$

If $N = \overline{\langle\langle R \rangle\rangle}$, an F-invariant map $\phi : N \to \mathbb{F}_p$ is determined by the restriction to R, so there is an injection $H^1(N, \mathbb{F}_p)^F \hookrightarrow \mathbb{F}_p^{|R|}$.

Conversely suppose $\dim H^1(N, \mathbb{F}_p)^F = r$, then $\dim N/N^p[N, F] = r$. Let $R \subseteq N$ be a lift of a basis of the vector space. R has the property that every F-invariant homomorphism $N \to \mathbb{F}_p$ which kills R is trivial. Claim $N = \overline{\langle\langle R \rangle\rangle}$: suppose $N' = \overline{\langle\langle R \rangle\rangle} \neq N$. Then $N'\Phi(N) \neq N$ by definition of Frattini subgroup, so $M = N/N'\Phi(N) \neq 0$. M is an abelian pro-p group with a continuous action of F. By the previous lemma M has a F-invariant proper open subgroup U. Now M/U is a finite F-module which is an abelian p-group, so by the characterisation of simple modules there is a map $M/U \to \mathbb{F}_p$. This contradicts

$$N \to N/N'\Phi(N) = M \to M/U \to \mathbb{F}_p$$

which kills all of R. □

Non-examinable proof of Theorem 5.26. This follows from minimal generating set has size equal to $\dim G/\Phi(G) = \dim H^1(G, \mathbb{F}_p)$.

Let $N = \ker(F(X) \to G)$. We obtain the five term exact seqeunce

$$\begin{tikzcd} 0 \arrow[r] & H^1(G) \arrow[r] & H^1(F) \arrow[r] & H^1(N)^F \arrow[r] & H^2(G) \arrow[r] & H^2(F) = 0 \\ & \dim H^1(G) & {|X|} & r_X & \dim H^2(G) & \end{tikzcd}$$

Now take Euler characteristic. □

Index