# Profinite Groups and Group Cohomology

Lectured by Dr Gareth Wilkes
Typed by David Kurniadi Angdinata

Lent 2020

**Syllabus**

# Contents

# 0 Introduction

Lecture 1
Thursday
21/01/21

A question is, when are things different?

- $\mathbb{Z}$ is in bijection with $\mathbb{Q}$, by writing down a bijection.
- $\mathbb{Q}$ is not in bijection with $\mathbb{R}$, by diagonalisation.

A solution is to try to find an invariant, which is

- easier to compute,
- computable, and
- preserved under isomorphism.

**Example 0.0.1.**

- Cardinality of a set.
- Dimension and base field of a vector space, which is complete.
- For an algebraic field extension $K$ over $\mathbb{Q}$, the degree $[K:\mathbb{Q}]$ and the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.
- For a topological space $X$, compactness, connectedness, simplicial homology groups $\mathrm{H}_\bullet(X)$, and the fundamental group $\pi_1(X)$.

**Theorem 0.0.2.** *There is no algorithm that decides whether a finite presentation represents the trivial group.*

Finite groups we can decide.

- List all the finite quotients of a group.
- If you have two such lists, you can compare.
- If two groups have different sets of finite quotients, they are not isomorphic.

How often does this work?

- Combine all the finite quotients into one object to study, the **profinite completion**, which is a limit of the finite groups.
- More generally, a limit of finite groups is called a **profinite group**.

**Example 0.0.3.**

- In Galois theory, let $K = \bigcup_{N\in\mathbb{N}} K_N$ be the extension of $\mathbb{Q}$ adjoining all $p^N$-th roots of unity for $p$ a fixed prime and $N \in \mathbb{N}$, which gives a short exact sequence of Galois groups

$$\mathrm{Gal}(K/K_N) \to \mathrm{Gal}(K/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K_N/\mathbb{Q}).$$

  Then $\mathrm{Gal}(K_N/\mathbb{Q}) = \left(\mathbb{Z}/p^N\mathbb{Z}\right)^\times$ and $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim_N \left(\mathbb{Z}/p^N\mathbb{Z}\right)^\times = \mathbb{Z}_p^\times$.
- In algebraic geometry, étale fundamental groups are profinite groups.

The second part of the course is **group cohomology**, which is another invariant, with the following applications.

- Can tell if a group is free for some profinite groups.
- Given a group $G$ and an abelian group $A$, group cohomology tells us how many groups $E$ exist such that $A \triangleleft E$ and $E/A = G$.

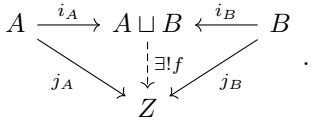
# 1 Inverse limits

## 1.1 Categories and limits

Let $A$ and $B$ be sets. How to combine into one thing? The disjoint union $A \sqcup B$ has inclusion maps $i_A : A \hookrightarrow A \sqcup B$ and $i_B : B \hookrightarrow A \sqcup B$, and for any other set $Z$, with functions $j_A : A \to Z$ and $j_B : B \to Z$ there is a unique function defined by

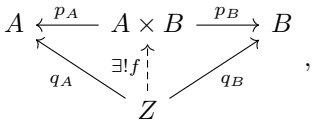
$$\begin{array}{rccc} f & : & A \sqcup B & \longrightarrow & Z \\ & & a & \longmapsto & j_A(a) \\ & & b & \longmapsto & j_B(b) \end{array},$$

such that $f \circ i_A = j_A$ and $f \circ i_B = j_B$, so



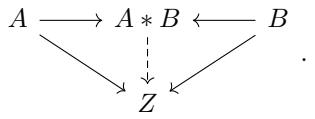

.

The product $A \times B$ comes with $p_A : A \times B \to A$ and $p_B : A \times B \to B$ such that



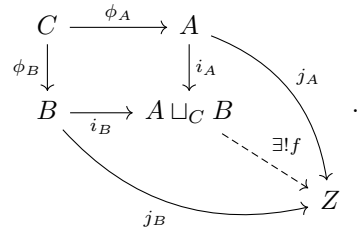

,

where $f(z) = (q_A(z), q_B(z))$. Reversed all arrows, so there is a duality, and disjoint union is a coproduct. What about groups, and group homomorphisms? The product still works, but the disjoint union is not a group. The coproduct is the free product $A * B$ such that




.

More generally is the pushout. Given groups $A$, $B$, and $C$, and homomorphisms $\phi_A : C \to A$ and $\phi_B : C \to B$, the **pushout** $A \sqcup_C B$ is




.

**Definition 1.1.1.** A **category** $\mathcal{C}$ consists of

- a collection of **objects** $\mathrm{Obj}\,\mathcal{C}$,
- a collection of **morphisms** or **arrows** $\mathrm{Mor}\,\mathcal{C}$, such that each $f \in \mathrm{Mor}\,\mathcal{C}$ has a **domain** $X \in \mathrm{Obj}\,\mathcal{C}$ and a **codomain** $Y \in \mathrm{Obj}\,\mathcal{C}$ written as $f : X \to Y$,
- for all objects $X \in \mathrm{Obj}\,\mathcal{C}$, you have $\mathrm{id}_X : X \to X$, and
- if $f : X \to Y$ and $g : Y \to Z$, we have a defined composition $g \circ f : X \to Z$,

such that

- if $f : X \to Y$, then $\mathrm{id}_Y \circ f = f = f \circ \mathrm{id}_X$, and
- if $f : W \to X$, $g : X \to Y$, and $h : Y \to Z$, then $h \circ (g \circ f) = (h \circ g) \circ f$.

**Example 1.1.2.**

- In **Set**, objects are sets and morphisms are functions.
- In **Grp**, objects are groups and morphisms are group homomorphisms.
- In $\mathbf{Grp}_{\text{fin}}$, objects are finite groups.
- In $\mathbf{Grp}_{\text{inj}}$, morphisms are injective group homomorphisms.

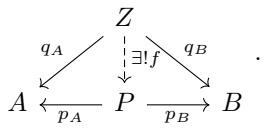
**Definition 1.1.3.** A **partial ordering** on a set $J$ is a binary relation $\leq$ such that

- $i \leq i$,
- if $i \leq j$ and $j \leq i$, then $i = j$, and
- if $i \leq j$ and $j \leq k$, then $i \leq k$.

A **poset** is a pair $(J, \leq)$, which is a **total ordering** if for all $i, j \in J$ either $i \leq j$ or $j \leq i$. The **poset category** $\mathcal{J}$ has objects $\operatorname{Obj}\mathcal{J} = J$ and morphisms $\operatorname{Mor}\mathcal{J} = \{i \to j \mid i \leq j\}$.

Lecture 2
Saturday
23/01/21

**Definition 1.1.4.** Let $\mathcal{C}$ be a category. A **product** of $A, B \in \operatorname{Obj}\mathcal{C}$ is an object $P$, equipped with morphisms $p_A : P \to A$ and $p_B : P \to B$, such that for all $Z \in \operatorname{Obj}\mathcal{C}$ and for all $q_A : Z \to A$ and $q_B : Z \to B$, there exists a unique $f : Z \to P$ such that $p_A \circ f = q_A$ and $p_B \circ f = q_B$, so

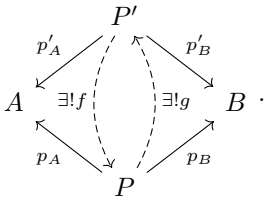



.

**Definition 1.1.5.** Objects $A$ and $B$ in a category $\mathcal{C}$ are **isomorphic** if there exist $f : A \to B$ and $g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

**Proposition 1.1.6.** *If a product of $A$ and $B$ in $\mathcal{C}$ exists, then it is unique up to a unique isomorphism.*

*Proof.* Let $(P, p_A, p_B)$ and $(P', p'_A, p'_B)$ be products. Then

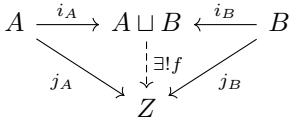



.

Consider $f \circ g : P \to P$. Then $p_A \circ f \circ g = p'_A \circ g = p_A$ and $p_B \circ f \circ g = p'_B \circ g = p_B$. By uniqueness, $f \circ g = \mathrm{id}_P$. Similarly, $g \circ f = \mathrm{id}_{P'}$. □

**Notation 1.1.7.** Define $P = A \times B$.

**Definition 1.1.8.** Let $\mathcal{C}$ be a category and $A, B \in \operatorname{Obj}\mathcal{C}$. Then a **coproduct** is an object $A \sqcup B$, together with maps $i_A : A \to A \sqcup B$ and $i_B : B \to A \sqcup B$, with the universal property




.

Products are examples of limits and coproducts are examples of colimits.

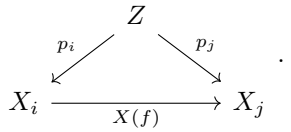
**Definition 1.1.9.** Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A **functor** $F : \mathcal{C} \to \mathcal{D}$ associates an object $F(X) \in \operatorname{Obj}\mathcal{D}$ to each $X \in \operatorname{Obj}\mathcal{C}$, and a morphism $F(f) : F(X) \to F(Y)$ for each $f : X \to Y$ in $\mathcal{C}$, such that

- $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$, and
- $F(g \circ f) = F(g) \circ F(f)$.

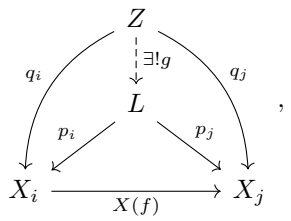
**Definition 1.1.10.** Let $\mathcal{J}$ and $\mathcal{C}$ be categories. A **diagram of shape $\mathcal{J}$ in $\mathcal{C}$** is a functor $X : \mathcal{J} \to \mathcal{C}$. Often write $X(j) = X_j$, for $j \in \operatorname{Obj}\mathcal{J}$.

Very often, $\mathcal{J}$ is a poset category. In that case, if $i \leq j$, there exists a unique arrow $f : i \to j$ and then denote $X(f) = \phi_{ij}$.

**Definition 1.1.11.** A **cone** on a diagram $X : \mathcal{J} \to \mathcal{C}$ is an object $Z \in \operatorname{Obj}\mathcal{C}$, together with maps $p_j : Z \to X_j = X(j)$ for all $j \in \operatorname{Obj}\mathcal{J}$ such that for all $f : i \to j$, $X(f) \circ p_i = p_j$, so




A **limit** of a diagram $X : \mathcal{J} \to \mathcal{C}$ is a cone $L$, with morphisms $p_j$, such that for any cone $Z$, with morphisms $q_j$, there is a unique $g : Z \to L$ such that $p_j \circ f = q_j$, for all $j \in \operatorname{Obj}\mathcal{J}$, so




for $f : i \to j$. **Colimits** are as limits, but arrows are reversed.

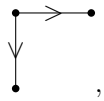
**Example 1.1.12.**

- If $\mathcal{J}$ is the category

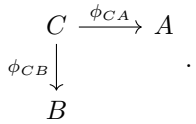
  

  then a diagram of shape $\mathcal{J}$ is a pair of objects. The limit is the product and the colimit is the coproduct.

- If $\mathcal{J}$ is the category

  then a diagram of shape $\mathcal{J}$ in **Grp** would be


  The colimit is the pushout.

**Proposition 1.1.13.** *Limits and colimits are unique up to unique isomorphism.*

## 1.2 Inverse limits and profinite groups

Let $G$ be a group. Let $\mathcal{N}$ be the poset category whose objects are $\{N \lhd_{\mathrm{f}} G\}$, where $N \lhd_{\mathrm{f}} G$ are finite index, with ordering $N_1 \leq N_2$ if and only if $N_1 \subseteq N_2$. There is a diagram of shape $\mathcal{N}$ in **Grp**,

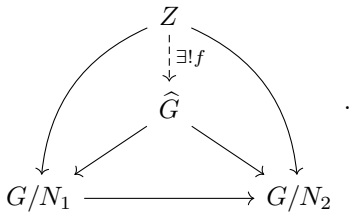
$$\begin{array}{rccc} X & : & \mathcal{N} & \longrightarrow & \mathbf{Grp} \\ & & N & \longmapsto & X_N = G/N \end{array}.$$

If $N_1 \leq N_2$, then $X\left(N_1 \to N_2\right)$ is the quotient map $\phi_{N_1 N_2} : G/N_1 \to G/N_2$, the transition maps.

**Definition 1.2.1.** Let $G$ be a group. The **profinite completion** of $G$ is the limit of this diagram, denoted $\widehat{G}$. Then $G$ comes with **projections** $p_N : \widehat{G} \to G/N$ for all $N \lhd_{\mathrm{f}} G$ such that

- if $N_1 \subseteq N_2$, then $\phi_{N_1 N_2} \circ p_{N_1} = p_{N_2}$, and
- if $Z$ is a group, with $q_N : Z \to G/N$ such that $\phi_{N_1 N_2} \circ q_{N_1} = q_{N_2}$, there exists a unique $f : Z \to \widehat{G}$ such that $p_N \circ f = q_N$ for all $N$.

Thus




.

In particular, $Z = G$ works, so there is a unique morphism $\iota_G : G \to \widehat{G}$, the **canonical morphism**, such that the diagrams commute.

**Definition 1.2.2.** A poset $(J, \leq)$ is an **inverse system** if for all $i, j \in J$ there exists $k \in J$ such that $k \leq i$ and $k \leq j$. An **inverse system of groups** consists of an inverse system $(J, \leq)$ and a diagram of shape $\mathcal{J}$ in **Grp**, so $G : \mathcal{J} \to \mathbf{Grp}$. Thus an inverse system is a group $G_j$ for all $j \in J$ and transition maps $\phi_{ij} : G_i \to G_j$ if $i \leq j$ such that $\phi_{ii} = \mathrm{id}$ and $\phi_{jk} \circ \phi_{ij} = \phi_{ik}$ for all $i \leq j \leq k$. The **inverse limit** of this inverse system of groups $G_j$ is the limit of this diagram, denoted $\varprojlim_j G_j$.

**Definition 1.2.3.** A **profinite group** is the inverse limit of an inverse system of groups, all of which are finite.

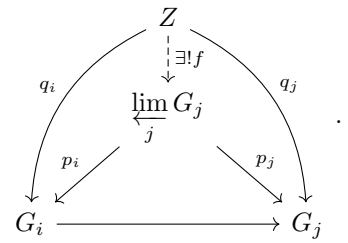
**Proposition 1.2.4.** *Let $\left(G_j\right)_{j \in J}$ be an inverse system of groups. Then the inverse limit exists, and is given by the explicit description*

$$\varprojlim_j G_j = \left\{ \left(g_j\right)_{j \in J} \in \prod_{j \in J} G_j \;\middle|\; \forall i \leq j,\ \phi_{ij}\left(g_i\right) = g_j \right\}.$$

*Proof.* This is a group. We have $p_j : \varprojlim_j G_j \to G_j$, restricted from $\prod_{j \in J} G_j \to G_j$. Take a cone $Z$ on the system. Define

$$\begin{array}{rccc} f & : & Z & \longrightarrow & \varprojlim_j G_j \\ & & z & \longmapsto & \left(q_j\left(z\right)\right)_{j \in J} \end{array}.$$

Then $\phi_{ij}\left(q_i\left(z\right)\right) = q_j\left(z\right)$, so




.

□

Lecture 3
Tuesday
26/01/21

**Definition 1.2.5.** Let $(G_j)_{j\in J}$ be an inverse system of finite groups. Give each $G_j$ the discrete topology. Give $\prod_j G_j$ the product topology. Then $\varprojlim_j G_j \leq \prod_j G_j$ gets the subspace topology.

**Proposition 1.2.6.** *$\varprojlim_j G_j$ is compact Hausdorff.*

*Proof.* $\prod_j G_j$ is Hausdorff and compact, by Tychonoff's theorem. Each condition $\phi_{ij}(g_i) = g_j$ is a closed condition, since $\prod_{j\in J} G_j \to G_i \times G_j$, so $\varprojlim_j G_j$ is closed in $\prod_j G_j$. □

**Proposition 1.2.7.** *Let $(X_j)_{j\in J}$ be an inverse system of non-empty finite sets. Then $\varprojlim_j X_j$ is non-empty.*

*Proof.* Use the finite intersection property. Let $I_1 \subseteq J$ be a finite subset. Define

$$Y_{I_1} = \left\{ (x_j) \in \prod_j X_j \;\middle|\; \forall i,j \in I_1,\ \forall i \leq j,\ \phi_{ij}(x_i) = x_j \right\} \subseteq \prod_j X_j,$$

a closed subset of the product. Since $J$ is an inverse system and $I_1$ is finite, there exists $k \in J$ such that $k \leq i$ for all $i \in I_1$. Choose $x_k \in X_k \neq \emptyset$. Define $x_j = \phi_{kj}(x_k)$ for all $j \geq k$. Choose $x_j$ arbitrarily elsewhere. This gives $x = (x_j) \in \prod_{j\in J} X_j$, which lies in $Y_{I_1}$, since if $i,j \in I_1$ such that $i \leq j$ then

$$x_j = \phi_{kj}(x_k) = \phi_{ij}(\phi_{ki}(x_k)) = \phi_{ij}(x_i).$$

So $Y_{I_1}$ is non-empty. Then $Y_{I_1} \cap \cdots \cap Y_{I_n} \supseteq Y_{I_1 \cup \cdots \cup I_n} \neq \emptyset$. By the finite intersection property, since $\prod_j X_j$ is compact, $\bigcap_{I_1} Y_{I_1} = \varprojlim_j X_j$ is non-empty. □

**Proposition 1.2.8.** *Let $J$ be a countable set and let $(X_j)_{j\in J}$ be a family of finite sets. Then $X = \prod_{j\in J} X_j$ is **metrisable**, so the metric topology equals to the other topology.*

*Proof.* Without loss of generality $J = \mathbb{N}$. Give each $X_n$ the discrete metric $d_n$, where

$$d_n(x_n, y_n) = \begin{cases} 0 & x_n = y_n \\ 1 & x_n \neq y_n \end{cases}, \qquad x_n, y_n \in X_n.$$

Define

$$d((x_n),(y_n)) = \sum_{n=1}^{\infty} \frac{1}{3^n} d_n(x_n, y_n), \qquad (x_n),(y_n) \in \prod_n X_n.$$

We need to show this gives the product topology. Let $f : (X, \tau_{\text{product}}) \to (X, d)$ be the identity function. A basis for the metric topology are open balls $\mathrm{B}(x, 1/3^n)$ for $x \in X$ and $n \in \mathbb{N}$. Then $d((x_n),(y_n)) < 1/3^m$ if and only if $x_n = y_n$ for all $n \leq m$, and

$$f^{-1}\left(\mathrm{B}\left((x_n), \frac{1}{3^m}\right)\right) = \{(y_n) \mid \forall n \leq m,\ y_n = x_n\} = \bigcap_{n=1}^{m} p_n^{-1}(\{x_n\}), \qquad p_n : \prod_n X_n \to X_n$$

is open in the product topology. So $f$ is continuous, so a homeomorphism. □

**Proposition 1.2.9.** *A continuous bijection from a compact space to a Hausdorff space is a homeomorphism.*

**Lemma 1.2.10.** *Let $G$ be a finitely generated group. For each $n \in \mathbb{N}$, there are only finitely many subgroups of index $n$.*

*Proof.* For a subgroup $H \leq G$ of index $n$, we get a homomorphism $G \to \operatorname{Sym} n$, since by labelling cosets $H, \ldots, g_n H$ by symbols $1, \ldots, n$, $G$ permutes these right cosets by $g \cdot g_i H = (gg_i) H$ and $H$ is recovered from this as $\operatorname{Stab} 1$. So there are at most as many subgroups $H$ as homomorphisms to $\operatorname{Sym} n$, and there are only finitely many. □

**Corollary 1.2.11.** *If $G$ is finitely generated, the inverse system $\mathcal{N} = \{N \lhd_{\mathrm{f}} G\}$ is countable.*

**Proposition 1.2.12.** *Let $G$ be a profinite group. Then $G$ is a **topological group**, so*

$$\begin{array}{rccc} \mathrm{m} : & G\times G & \longrightarrow & G \\ & (g,h) & \longmapsto & gh \end{array}, \qquad \begin{array}{rccc} \mathrm{i} : & G & \longrightarrow & G \\ & g & \longmapsto & g^{-1} \end{array}$$

*are continuous.*

**Definition 1.2.13.** Let $G$ and $H$ be topological groups. We say $G$ and $H$ are **isomorphic as topological groups** if and only if there exists $f : G \to H$ which is both an isomorphism of groups and a homeomorphism.

Recall that if $G$ and $H$ are profinite, this is the same as there exists $f$ a continuous isomorphism.

**Proposition 1.2.14.** *Let $H$ be a topological group and $G = \varprojlim_j G_j$ be an inverse limit of finite groups. Let $p_j : G \to G_j$ be the projection maps. A homomorphism $f : H \to G$ is continuous if and only if each map $f_j = p_j \circ f$ is continuous.*

*Proof.* $f : H \to G \leq \prod_j G_j$. This is continuous if and only if all $f_j$ are continuous, by definition of the product topology. □

**Proposition 1.2.15.** *Let $f : H \to G_j$ be a homomorphism from a topological group to a finite group, with the discrete topology. Then $f$ is continuous if and only if* $\ker f$ *is open in $H$.*

*Proof.* If $f$ is continuous then $\ker f = f^{-1}(\{1\})$ is open. Assume $f^{-1}(\{1\})$ is open. Then $f^{-1}(\{g\})$ is open for all $g \in G$, since multiplication is continuous and $f^{-1}(\{g\}) = hf^{-1}(\{1\})$ for some $h \in H$. Taking unions, the preimage of any set in $G_j$ is open in $H$, so $f$ is continuous. □

**Proposition 1.2.16.** *Let $G$ be a compact topological group. A subgroup of $G$ is open if and only if it is closed and of finite index.*

**Proposition 1.2.17.** *Let $(G_j)_{j\in J}$ be an inverse system of finite groups. If $G = \varprojlim_j G_j$, then the open subgroups $U_j = \ker(p_j : G \to G_j)$ form a **basis of open neighbourhoods** of the identity $1 \in G$, so if $V \subseteq G$ is any open set with $1 \in V$, then there exists $j$ such that $U_j \subseteq V$.*

*Proof.* Let $V \ni 1$ be open. By definition of the product topology,

$$V \supseteq p_{j_1}^{-1}(X_{j_1}) \cap \cdots \cap p_{j_n}^{-1}(X_{j_n}) \supseteq p_{j_1}^{-1}(\{1\}) \cap \cdots \cap p_{j_n}^{-1}(\{1\}) = U_{j_1} \cap \cdots \cap U_{j_n}.$$

for $X_{j_i} \subseteq G_{j_i}$. There exists $k$ such that $k \leq j_i$. Since $p_{j_i} = \phi_{kj_i} \circ p_k$, $\ker p_k = U_k \subseteq U_{p_{j_i}} = \ker p_{j_i}$ for all $i$. Thus $V \supseteq U_k$. □

Lecture 4
Thursday
28/01/21

**Corollary 1.2.18.** *If $g = (g_j)_{j\in J} \in G$, then the open cosets $gU_j = p_j^{-1}(\{g_j\})$ form a neighbourhood base at $g$, so for all open set $V \ni g$, there exists $j \in J$ such that $gU_j \subseteq V$.*

*Proof.* Continuity of multiplication. □

**Corollary 1.2.19.** *A subset $X \subseteq G$ is dense if and only if $p_j(X) = p_j(G)$ for all $j \in J$.*

*Proof.* Suppose $X$ is not dense. There exists a non-empty open set $V$ such that $V \cap X = \emptyset$. Pick $g \in V$. There exists $j \in J$ such that $p_j^{-1}(\{g_j\}) = gU_j \subseteq V$, where $g_j = p_j(g)$. Then $g_j \in p_j(G)$. But for any $x \in X$, $p_j(x) \neq g_j$, otherwise $x \in p_j^{-1}(\{g_j\}) = gU_j \subseteq V$, so $p_j(X) \neq p_j(G)$. Assume $X$ is dense. Then $p_j(X) \subseteq p_j(G)$ is obvious. If $g_j \in p_j(G)$, then $p_j^{-1}(\{g_j\})$ is a non-empty open set, so there exists $x \in X \cap p_j^{-1}(\{g_j\})$, then $p_j(x) = g_j$. So $g_j \in p_j(X)$, so $p_j(X) = p_j(G)$. □

**Corollary 1.2.20.** *Let $Y$ be a compact topological space and let $f : Y \to G$ be a continuous function. Then $f$ is surjective if and only if $p_j(f(Y)) = p_j(G)$ for all $j \in J$.*

*Proof.* $p_j(f(Y)) = p_j(G)$ if and only if $f(Y)$ is dense, if and only if $f(Y) = G$, since $f(Y)$ is closed. □

**Proposition 1.2.21.** *Let $G$ be a profinite group and $X \subseteq G$ be a subset. Then the closure of $X$ is*

$$\overline{X} = \bigcap_{N \leq_{\mathrm{o}} G} XN,$$

*where $N \leq_{\mathrm{o}} G$ are open subgroups.*

*Proof.* $XN$ is a union of cosets, hence it is open and closed in $G$. So $\overline{X} \subseteq XN$ for all $N \leq_{\mathrm{o}} G$, so $\overline{X} \subseteq \bigcap_{N \leq_{\mathrm{o}} G} XN$. Take $g \notin \overline{X}$. There exists an open $V \subseteq G$ such that $g \in V$ but $X \cap V = \emptyset$. Then there exists $j \in J$ such that $V \supseteq gU_j$ for $N = U_j = \ker p_j$. Then $g \notin XN$, since if $g = xn$ for $x \in X$ and $n \in N = U_j$ then $x = gn^{-1} \in gN = gU_j \subseteq V$, a contradiction. Thus $g \notin \bigcap_N XN$, so $\bigcap_N XN \subseteq \overline{X}$. □

**Proposition 1.2.22.** *Let $G$ be a profinite group and let $\mathcal{U}$ be a collection of open normal subgroups which form a neighbourhood base at the identity. Then*

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

*as topological groups, where $G/U$ are finite groups.*

*Proof.* The quotient maps $G \twoheadrightarrow G/U$ are a cone on the inverse system, so we get a well-defined homomorphism $f : G \to \varprojlim_U G/U$. Then

- $f$ is continuous, since compositions with projection maps are continuous,
- $f$ is surjective, since $G \twoheadrightarrow G/U$ are surjective, and
- $f$ is injective, since if $g \in G \setminus \{1\}$, there exists an open subset $V$ such that $1 \in V$ and $g \notin V$ and there exists $U \in \mathcal{U}$ such that $1 \in U \subseteq V$, then $g \notin \ker(G \to G/U)$, so $g \notin \ker f$.

□

## 1.3 Change of inverse system

**Definition 1.3.1.** Let $(J, \leq)$ be an inverse system. A **cofinal subsystem** of $J$ is a subset $I \subseteq J$ such that for all $j \in J$ there exists $i \in I$ such that $i \leq j$.

Then $I$ is an inverse system.

**Example 1.3.2.** If $k \in J$, then the set

$$J_{\leq k} = \{j \in J \mid j \leq k\},$$

the **principal cofinal subsystem**, is cofinal in $J$.

**Proposition 1.3.3.** *Let $(G_j)_{j \in J}$ be an inverse system of finite groups, and let $I \subseteq J$ be cofinal. Then $H = \varprojlim_{i \in I} G_i$ is topologically isomorphic to $G = \varprojlim_{j \in J} G_j$.*

*Proof.* The projection map $\prod_{j \in J} G_j \to \prod_{i \in I} G_i$ is a continuous homomorphism, and it restricts to $f : G \to H$. Check that $f$ is bijective.

- Injective. Take $g = (g_j)_{j \in J} \in G$. Assume $f(g) = 1$, so $g_i = p_i(f(g)) = 1$ for all $i \in I$. For any $j \in J$, there exists $i \in I$ such that $i \leq j$. Then $g_j = \phi_{ij}(g_i) = \phi_{ij}(1) = 1$. So $g = 1$.
- Surjective. Let $h = (h_i)_{i \in I} \in H$ for $h_i \in G_i$. Define $g = (g_j) \in \prod_{j \in J} G_j$ by setting $g_j = \phi_{ij}(h_i)$ for some $i \in I$ such that $i \leq j$. If $i_1 \leq j$ and $i_2 \leq j$, there exists $i_0 \in I$ such that $i_0 \leq i_1$ and $i_0 \leq i_2$, then

  $$\phi_{i_1 j}(h_{i_1}) = \phi_{i_1 j}(\phi_{i_0 i_1}(h_{i_0})) = \phi_{i_0 j}(h_{i_0}) = \phi_{i_2 j}(\phi_{i_0 i_2}(h_{i_0})) = \phi_{i_2 j}(h_{i_2}).$$

  It also follows that $g \in G$, since if $j_1 \leq j_2$, choose $i \in I$ such that $i \leq j_1$, then

  $$g_{j_2} = \phi_{ij_2}(h_i) = \phi_{j_1 j_2}(\phi_{ij_1}(h_i)) = \phi_{j_1 j_2}(g_{j_1}).$$

  Finally, $f(g) = h$, since $g_i = \phi_{ii}(h_i) = h_i$ for all $i \in I$.

□

**Definition 1.3.4.** An inverse system of groups is **surjective** if all transition maps are surjective.

**Proposition 1.3.5.** *Let $(X_j)_{j\in J}$ be an inverse system of finite sets where all transition maps are surjective. Then the projection maps $p_j : \varprojlim_j X_j \to X_j$ are surjective.*

**Proposition 1.3.6.** *Let $(G_j)_{j\in J}$ be an inverse system of finite groups. Then there exists an inverse system $\left(G'_j\right)_{j\in J}$ such that $G'_j \leq G_j$, with surjective transition maps, such that $\varprojlim_j G_j = \varprojlim_j G'_j$.*

*Proof.* Let $p_j : G = \varprojlim_j G_j \to G_j$ be the projection. Define $G'_j = p_j(G)$. Since $\phi_{ij} \circ p_i = p_j$, $\left(G'_j\right)$ is an inverse system with $\phi_{ij}|_{G'_i} : G'_i \to G'_j$, and $\phi_{ij}|_{G'_i}$ is surjective. If $g = (g_j) \in G$ then $g_j = p_j(g) \in G'_j$, so $g \in \varprojlim_j G'_j \leq G \leq \prod_j G_j$. Thus $\varprojlim_j G'_j = G$. □

**Definition 1.3.7.** An inverse system $(J, \leq)$ is **linearly ordered** if there exists a bijection $f : J \to \mathbb{N}$ such that $i \leq j$ if and only if $f(i) \geq f(j)$, the **wrong-way ordering** on $\mathbb{N}$.

Thus cofinal if and only if increasing subsequence.

**Proposition 1.3.8.** *If $J$ is a countable inverse system, with no **global minimum**, so there does not exist $m \in J$ such that $m \leq j$ for all $j$, then $J$ has a linearly ordered cofinal subsystem.*

# 2 Profinite groups

## 2.1 The $p$-adic integers

Lecture 5
Saturday
30/01/21

Let $p$ be a prime. Consider

$$\cdots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 1.$$

The **ring of $p$-adic integers** is

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

Thus $\alpha \in \mathbb{Z}_p$ is a sequence $(a_n)_{n\in\mathbb{N}}$ of integers modulo $p^n$ for $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ such that $a_n \equiv a_m \mod p^m$ whenever $n \geq m$, since $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, and

$$\begin{array}{rccl} p_n & : & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} \\ & & \alpha & \longmapsto & a_n = \alpha \mod p^n \end{array}.$$

Given $a \in \mathbb{Z}$, setting $a_n = a \mod p^n$ gives an element $\iota(a) \in \mathbb{Z}_p$ for $\iota : \mathbb{Z} \to \mathbb{Z}_p$. Then $\iota$ is injective, since if $a \in \mathbb{Z}$, and $p^n > |a|$ then $a \not\equiv 0 \mod p^n$, so $\iota(a) \neq 0$ in $\mathbb{Z}_p$. Often $\mathbb{Z} \leq \mathbb{Z}_p$.

**Definition 2.1.1.** Let $\alpha = (a_n), \beta = (b_n) \in \mathbb{Z}_p$. If $\alpha = \beta$ then $\mathrm{d}(\alpha, \beta) = 0$. If $\alpha \neq \beta$, take the smallest $n$ such that $a_n \neq b_n$, and set $\mathrm{d}(\alpha, \beta) = p^{-n}$, the **$p$-adic metric on $\mathbb{Z}_p$**. The restriction of d to $\iota(\mathbb{Z})$ is the **$p$-adic metric on $\mathbb{Z}$**.

Thus $\alpha$ and $\beta$ are close if $(a_n)$ and $(b_n)$ agree modulo $p^n$ for all but large $n$. Since

$$\mathrm{B}(0, r) = \left\{\alpha = (a_n) \;\middle|\; \forall n \leq -\log_p r,\ a_n = 0\right\} = \ker\left(\mathbb{Z}_p \to \mathbb{Z}/p^{\lfloor -\log_p r \rfloor}\mathbb{Z}\right),$$

open balls are the subgroups $p^n\mathbb{Z}_p \leq \mathbb{Z}_p$.

- $\iota(\mathbb{Z})$ is dense in this metric. Let $\alpha = (a_n) \in \mathbb{Z}_p$ and $\epsilon > 0$. Take $n > -\log_p \epsilon$, and choose $a \in \mathbb{Z}$ such that $a \equiv a_n \mod p^n$. Then $\mathrm{d}(\alpha, \iota(a)) \leq p^{-n} < \epsilon$.
- The $p$-adic metric on $\mathbb{Z}$ is not complete, since $a_n = 1 + \cdots + p^n$ does not converge in $\mathbb{Z}$, but does converge in $\mathbb{Z}_p$.
- The $p$-adic metric on $\mathbb{Z}_p$ is complete. Let $\alpha^{(k)} = \left(a_n^{(k)}\right)_{n\in\mathbb{N}}$ be a Cauchy sequence in $\mathbb{Z}_p$. For all $n$ there exists $K_n$ such that for all $k, l \geq K_n$, we have $\mathrm{d}\left(\alpha^{(k)}, \alpha^{(l)}\right) \leq p^{-n}$, so $a_n^{(k)} = a_n^{(l)}$ for all $k, l \geq K_n$ so for fixed $n$, $a_n^{(k)}$ is eventually a constant $b_n$. Then $\beta = (b_n) \in \mathbb{Z}_p$, and $\alpha^{(k)} \to \beta$ in $\mathbb{Z}_p$.

Thus $\mathbb{Z}_p$ is a completion of $\mathbb{Z}$, but is not the profinite completion of $\mathbb{Z}$.

**Definition 2.1.2.** Let $p$ be a prime. A **$p$-group** is a finite group of order $p^n$ for $n \geq 0$. A **pro-$p$ group** is an inverse limit of $p$-groups.

**Definition 2.1.3.** Let $G$ be a group and $p$ prime. The set of normal subgroups $N \triangleleft G$ such that $[G : N] = p^n$ for some $n$ form an inverse system $\mathcal{N}_p$. Since $G/N_1 \times G/N_2$ are $p$-groups, $N_1 \cap N_2 = \ker(G \to G/N_1 \times G/N_2)$ is a $p$-group. The **pro-$p$ completion** is

$$\widehat{G_{(p)}} = \varprojlim_{N\in\mathcal{N}_p} G/N,$$

where $G/N_1 \to G/N_2$ if $N_1 \leq N_2$.

**Proposition 2.1.4.** *The additive group $\mathbb{Z}_p$ is abelian and torsionfree.*

*Proof.* $\mathbb{Z}_p \leq \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ is abelian. Let $\alpha = (a_n) \in \mathbb{Z}_p \setminus \{0\}$. Suppose $m\alpha = 0$ for $m \in \mathbb{Z}$. We want $m = 0$. Assume $m = p^r s$ for $s$ coprime to $p$. Then $\alpha \neq 0$, so there exists $n$ such that $a_n \neq 0$. Consider $a_{n+r}$. Then $0 \equiv m a_{n+r} \equiv p^r a_{n+r} s \mod p^{n+r}$, so $p^n \mid a_{n+r} s$. Thus $p^n \mid a_{n+r}$, so $a_n \equiv a_{n+r} \equiv 0 \mod p^n$, a contradiction. □

**Proposition 2.1.5.** *The ring $\mathbb{Z}_p$ has no zero-divisors.*

*Proof.* Exercise. [1] □

## 2.2 The profinite completion of the integers

The **profinite completion of the integers** is

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z},$$

where $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ whenever $n\mathbb{Z} \leq m\mathbb{Z}$, which is if and only if $m \mid n$, so $n = mr$.

**Theorem 2.2.1** (Chinese remainder theorem)**.** *There is an isomorphism of topological rings*

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

*Proof.* Each natural number $n$ is written as a product of prime powers $n = \prod_{p \text{ prime}} p^{e_p(n)}$. The classical CRT gives natural isomorphisms

$$\begin{array}{rccc} f_n & : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \prod\limits_{p \text{ prime}} \mathbb{Z}/p^{e_p(n)}\mathbb{Z} \\ & & 1 & \longmapsto & (1, \ldots, 1) \end{array},$$

and commutative diagrams

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \xrightarrow[\sim]{f_{mn}} & \prod\limits_p \mathbb{Z}/p^{e_p(mn)}\mathbb{Z} \\ \big\downarrow & & \big\downarrow \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow[f_n]{\sim} & \prod\limits_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z} \end{array}.$$

Passing to inverse limits,

$$\begin{array}{ccc} \widehat{\mathbb{Z}} = \varprojlim\limits_n \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \varprojlim\limits_n \prod\limits_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z} \\ \cap & & \cap \\ \prod\limits_n \mathbb{Z}/n\mathbb{Z} & \xrightarrow[\sim]{} & \prod\limits_n \prod\limits_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z} \end{array}.$$

The natural continuous surjections

$$\prod_p \mathbb{Z}_p \twoheadrightarrow \prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z}$$

form a cone on the inverse system $\left\{\prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z}\right\}$, so there exists

$$f : \prod_p \mathbb{Z}_p \twoheadrightarrow \varprojlim_n \prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z},$$

which is continuous by Proposition 1.2.14, surjective by Corollary 1.2.20, and injective since every non-trivial element of $\prod_p \mathbb{Z}_p$ is non-trivial in some quotient $\mathbb{Z}/p^e\mathbb{Z}$. So $f$ is a topological isomorphism as required. □

**Corollary 2.2.2.** *The abelian group $\widehat{\mathbb{Z}}$ is torsionfree abelian.*

**Corollary 2.2.3.** *The ring $\widehat{\mathbb{Z}}$ is not an integral domain.*

*Proof.* Any product of non-trivial rings $R_1 \times R_2$ has zero-divisors, since $(r_1, 0) \cdot (0, r_2) = (0, 0)$. An element of $\widehat{\mathbb{Z}}$ is a zero-divisor if and only if it is zero in some $\mathbb{Z}_p$-factor. □

Elements of $\iota(\mathbb{Z})$ are not zero divisors in $\widehat{\mathbb{Z}}$.

[1] Exercise

## 2.3 Profinite matrix groups

Lecture 6
Tuesday
02/02/21

For a commutative ring $R$, we have

$$\mathrm{Mat}_{N\times M} R = \{N \times M \text{ matrices with elements in } R\}.$$

If $N = M$, we have a ring structure, where addition and multiplication are given by the usual formula. There exists a determinant function $\det : \mathrm{Mat}_{N\times N} R \to R$. Then

$$\mathbb{Z}_p^{NM} \cong \mathrm{Mat}_{N\times M} \mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathrm{Mat}_{N\times M} \mathbb{Z}/p^n\mathbb{Z}.$$

By continuity of ring operations on $\mathbb{Z}_p$, addition and multiplication on matrices are continuous, and $\det : \mathrm{Mat}_{N\times N} \mathbb{Z}_p \to \mathbb{Z}_p$ is continuous. Since $\mathbb{Z}_p$ is an integral domain, it has a field of fractions $\mathbb{Q}_p$, so you can do linear algebra over $\mathbb{Q}_p$. A matrix over $\mathbb{Q}_p$ has an inverse over $\mathbb{Q}_p$ if and only if its determinant is non-zero, and a matrix over $\mathbb{Z}_p$ has an inverse over $\mathbb{Z}_p$ if and only if its determinant and its inverse are in $\mathbb{Z}_p^\times$. Define

$$\mathrm{GL}_N \mathbb{Z}_p = \left\{A \in \mathrm{Mat}_{N\times N} \mathbb{Z}_p \;\middle|\; \det A \in \mathbb{Z}_p^\times\right\}, \qquad \mathrm{SL}_N \mathbb{Z}_p = \{A \in \mathrm{Mat}_{N\times N} \mathbb{Z}_p \mid \det A = 1\}.$$

Both are profinite groups.

**Lemma 2.3.1.** *For all $N \geq 1$ and $p$ prime,*

$$\mathrm{GL}_N \mathbb{Z}_p = \varprojlim_n \mathrm{GL}_N(\mathbb{Z}/p^n\mathbb{Z}), \qquad \mathrm{SL}_N \mathbb{Z}_p = \varprojlim_n \mathrm{SL}_N(\mathbb{Z}/p^n\mathbb{Z}).$$

*Proof.* The diagrams

$$\begin{array}{ccc} \mathrm{Mat}_{N\times N} \mathbb{Z}_p & \longrightarrow & \mathrm{Mat}_{N\times N} \mathbb{Z}/p^n\mathbb{Z} \\ {\scriptstyle\det}\downarrow & & \downarrow{\scriptstyle\det} \\ \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} \end{array}$$

commute.

- $A \in \mathrm{GL}_N \mathbb{Z}_p$ if and only if $\det A \in \mathbb{Z}_p^\times$, if and only if $\det A_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ for all $n$, if and only if $A_n \in \mathrm{GL}_N(\mathbb{Z}/p^n\mathbb{Z})$ for all $n$.
- $A \in \mathrm{SL}_N \mathbb{Z}_p$ if and only if $\det A = 1$, if and only if $\det A_n = 1$ for all $n$, if and only if $A_n \in \mathrm{SL}_N(\mathbb{Z}/p^n\mathbb{Z})$ for all $n$.

□

Also have matrices over $\widehat{\mathbb{Z}}$. A warning is that $\widehat{\mathbb{Z}}$ is not an integral domain. Analogously,

$$\mathrm{GL}_N \widehat{\mathbb{Z}} = \left\{A \in \mathrm{Mat}_{N\times N} \widehat{\mathbb{Z}} \;\middle|\; \det A \in \widehat{\mathbb{Z}}^\times\right\} = \varprojlim_n \mathrm{GL}_N(\mathbb{Z}/n\mathbb{Z}) = \prod_p \mathrm{GL}_N \mathbb{Z}_p,$$

$$\mathrm{SL}_N \widehat{\mathbb{Z}} = \left\{A \in \mathrm{Mat}_{N\times N} \widehat{\mathbb{Z}} \;\middle|\; \det A = 1\right\} = \varprojlim_n \mathrm{SL}_N(\mathbb{Z}/n\mathbb{Z}) = \prod_p \mathrm{SL}_N \mathbb{Z}_p,$$

since $\mathrm{Mat}_{N\times N} \widehat{\mathbb{Z}} = \prod_p \mathrm{Mat}_{N\times N} \mathbb{Z}_p$, and

$$\mathrm{SL}_N \mathbb{Z} \leq \mathrm{SL}_N \mathbb{Z}_p, \qquad \mathrm{SL}_N \mathbb{Z} \leq \mathrm{SL}_N \widehat{\mathbb{Z}} = \varprojlim_n \mathrm{SL}_N(\mathbb{Z}/n\mathbb{Z})$$

are dense. See problem sheet 2.

**Example 2.3.2.** $\left(\begin{smallmatrix} 7 & 9 \\ 4 & 9 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/13\mathbb{Z})$ is in the image of $\mathrm{SL}_2 \mathbb{Z}$.

## 2.4 Subgroups, quotients, and homomorphisms

**Proposition 2.4.1.** *A closed subgroup of a profinite group is a profinite group.*

*Proof.* Let $G = \varprojlim_{j \in J} G_j$ be a profinite group for $G_j$ finite. Take a closed subgroup $H \leq_{\mathrm{c}} G$ of $G$. Define $H_j = p_j(H) \leq G_j$. Then $H_j$, with transition maps $\phi_{ij}|_{H_i} : H_i \to H_j$, are an inverse system of finite groups. Define

$$H' = \varprojlim_j H_j = \left\{ (g_j) \in \prod_{j \in J} G_j \;\middle|\; \forall i \leq j,\ \phi_{ij}(g_i) = g_j,\ g_j \in H_j \right\}.$$

Show that $H = H'$. If $h = (h_j) \in H$, by definition $h_j = p_j(h) \in H_j$, so $H \leq H'$. Suppose $g = (g_j) \notin H$. Since $H$ is closed, $G \setminus H$ is open, so there exists a basic open set containing $g$, which does not intersect $H$. There exists $j \in J$ such that $gU_j = p_j^{-1}(\{g_j\}) \leq G \setminus H$. Therefore for all $h \in H$, $p_j(h) \neq g_j$, since then $h \in H \cap p_j^{-1}(\{g_j\})$, so $g_j \notin H_j$, so $g \notin H'$. So $H = H'$. □

**Remark 2.4.2.**

- The two topologies on $H$ agree by $\mathrm{id} : (H, \tau_{\text{profinite}}) \to (H, \tau_{\text{subspace}})$, which is continuous by Proposition 1.2.14.
- A better name for $H'$ is $\overline{H}$, the closure. Actually proved that $H' = \overline{H} = H$.

**Proposition 2.4.3.** *Let $G = \varprojlim_j G_j$ and $H \leq G$. Set $H_j = p_j(H) \leq G_j$. Then the closure of $H$ is*

$$\overline{H} = \varprojlim_j H_j.$$

**Lemma 2.4.4.** *Let $f : G_1 \to G_2$ be a surjective homomorphism and $H \leq G_1$. Then $[G_1 : H] \geq [G_2 : f(H)]$.*

**Proposition 2.4.5.** *Let $G = \varprojlim_j G_j$ for $(G_j)$ a surjective inverse system, so $G \twoheadrightarrow G_j$. Let $H \leq_{\mathrm{c}} G$ and set $H_j = p_j(H) \leq G_j$. Then $H$ is finite index if and only if $[G_j : H_j]$ is constant on a cofinal subsystem, if and only if $[G_j : H_j]$ is bounded for all $j$. If this is true, then $[G : H] = [G_i : H_i]$ for $i \in I$.*

*Proof.* $p_j : G \to G_j$ are surjective, so $[G : H] \geq [G_j : H_j]$. Suppose $[G : H] \geq N$. There exist distinct cosets $g_1 H, \ldots, g_N H$ of $H$ in $G$, if and only if $g_n^{-1} g_m \notin H$ if $n \neq m$, so there exists $j_{n,m} \in J$ such that $p_{j_{n,m}}\left(g_n^{-1} g_m\right) \notin H_{j_{n,m}}$. Take $k \leq j_{n,m}$ for all $n$ and $m$. Then $p_k\left(g_n^{-1} g_m\right) \notin H_k$ for all $n \neq m$, so $p_k(g_n) H_k$ are distinct cosets of $H_k$ in $G_k$, so $[G_k : H_k] \geq N$. For any $i$ in the cofinal subsystem $J_{\leq k}$, it follows $[G_i : H_i] \geq N$ for all $i \leq k$. If $[G : H] = N$ is finite, take $k$ as above and $I = J_{\leq k}$. Then $[G : H] \geq [G_i : H_i] \geq N = [G : H]$ for all $i \in I$. If $[G : H]$ is infinite, assume $I$ is cofinal and $[G_i : H_i] = N$ for all $i \in I$. Then there exists $k$ such that $[G_k : H_k] \geq N + 1$. But there exists $i \in I$ such that $i \leq k$, then $[G_i : H_i] \geq [G_k : H_k] \geq N + 1 > N = [G_i : H_i]$, a contradiction. □

**Proposition 2.4.6.** *Let $G$ be a profinite group and $N$ a closed normal subgroup. Then $G/N$, with the quotient topology, is a profinite group.*

*Proof.* Take $G = \varprojlim_j G_j$ for $(G_j)$ a surjective inverse system. Let $N_j = p_j(N) \triangleleft G_j = p_j(G)$. Recall $N = \varprojlim_j N_j$. Define $Q_j = G_j / N_j$. Since $\phi_{ij}(N_i) \leq N_j$, we get quotient homomorphisms $\psi_{ij} : Q_i \to Q_j$, which are transition maps for the $Q_j$. Set $Q = \varprojlim_j Q_j$. The map $\prod_h G_j \to \prod_j Q_j$ is continuous, so there is a continuous surjective group homomorphism $f : G \to Q$. The kernel of this map is $N$, since $f(g) = 1$ if and only if $q_j(f(g)) = 1$ for all $j$, if and only if $g_j \in N_j$ for all $j$, if and only if $g \in \varprojlim_j N_j = N$. By the first isomorphism theorem for groups,

$$\begin{array}{ccc} G & & \\ \downarrow & \searrow & \\ G/N & \xrightarrow[\overline{f}]{\sim} & Q \end{array}.$$

Since $G \to Q$ is continuous and $G \to G/N$ is the quotient map, $\overline{f}$ is continuous. Since $G/N$ is compact and $Q$ is Hausdorff, $\overline{f}$ is a homeomorphism. □

This is the first isomorphism theorem for profinite groups.

Lecture 7
Thursday
04/02/21

**Definition 2.4.7.** Let $(G_j)_{j\in J}$ and $(H_j)_{j\in J}$ be inverse systems of finite groups, over the same poset $J$. A **morphism of inverse systems** $(f_j)$ is a family of homomorphisms $f_j : G_j \to H_j$, such that for all $i \leq j$,

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

commutes, so $\phi_{ij}^H \circ f_i = f_j \circ \phi_{ij}^G$.

**Proposition 2.4.8.** *Let $(f_j) : (G_j) \to (H_j)$ be a morphism of inverse systems. Then there is a unique continuous homomorphism $f : G = \varprojlim_j G_j \to H = \varprojlim_j H_j$ such that*

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

*so $p_j^H \circ f = f_j \circ p_j^G$ for all $j \in J$.*

*Proof.* The maps $f_j \circ p_j^G : G \to H_j$ form a cone on the inverse system $(H_j)$,

$$\begin{array}{ccc} & G & \\ {\scriptstyle f_i\circ p_i^G}\swarrow & & \searrow{\scriptstyle f_j\circ p_j^G} \\ H_i & \xrightarrow[\phi_{ij}^H]{} & H_j \end{array},$$

since

$$\phi_{ij}^H \circ f_i \circ p_i^G = f_j \circ \phi_{ij}^G \circ p_i^G = f_j \circ p_j^G.$$

So by definition of limits, there exists a unique $f : G \to H = \varprojlim_j H_j$ such that $p_j^H \circ f = f_j \circ p_j^G$. □

Thus $f$ is **induced** by the $f_j$ by passing to an inverse limit.

**Proposition 2.4.9.** *Let $G = \varprojlim_{j\in J} G_j$ and $H = \varprojlim_{i\in I} H_i$ be inverse limits of finite groups, where $I$ and $J$ are countable inverse systems with no minimal element. Let $f : G \to H$ be a continuous homomorphism. Then there exist cofinal subsystems $J' \subseteq J$ and $I' \subseteq I$, an order-preserving bijection $J' \cong I'$, and a morphism of inverse systems $(f_j) : (G_j)_{j\in J'} \to (H_i)_{i\in I'}$ inducing $f$.*

*Proof.* Without loss of generality, use Proposition 1.3.8 to assume $J$ and $I$ are linearly ordered. Without loss of generality both are $\mathbb{N}$, with the wrong-way ordering. Construct an increasing sequence $(k_n)$ of natural numbers as follows. Each map $p_n^H \circ f : G \to H \to H_n$ is a continuous homomorphism, so its kernel is open in $G$. By Proposition 1.2.17 there exists $k_n$ such that $\ker(G \to G_{k_n}) \leq \ker(G \to H_n)$, which means there is a quotient homomorphism

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle p_{k_n}^G}\downarrow & \searrow & \downarrow{\scriptstyle p_n^H} \\ G_{k_n} & \xrightarrow[f_n]{} & H_n \end{array}.$$

Then $\ker(G \to G_{n+1}) \leq \ker(G \to G_n)$, so without loss of generality $k_n > k_{n-1}$. Now $J' = \{k_n\}_{n\in\mathbb{N}}$ give a cofinal subsystem of $J = \mathbb{N}$, and the $f_n$ are the required morphisms of inverse systems. □

## 2.5 Generators of profinite groups

**Definition 2.5.1.** Let $G$ be a topological group, and let $S$ be a subset of $G$. Then $S$ is a **topological generating set** for $G$ if the subgroup $\langle S \rangle$ is dense in $G$, and $G$ is **topologically finitely generated** if it has some finite topological generating set $S$.

**Definition 2.5.2.** Let $G$ be a topological group and $S \subseteq G$. The **closed subgroup of $G$ topologically generated by** $S$ is the smallest closed subgroup of $G$ which contains $S$. Denoted $\overline{\langle S \rangle}$.

**Proposition 2.5.3.** *Let $G$ be a topological group and $H$ a subgroup of $G$. Then $\overline{H}$ is a subgroup of $G$. Hence for $S \subseteq G$, the closed subgroup of $G$ generated by $S$ is equal to the closure of $\langle S \rangle$.*

*Proof.* Exercise. [2] □

**Lemma 2.5.4.** *A finite index subgroup of a finitely generated group is finitely generated.*

**Proposition 2.5.5.** *If a profinite group $G$ is topologically finitely generated and $U$ is an open subgroup of $G$ then $U$ is topologically finitely generated.*

*Proof.* Let $S$ be a finite set such that $\langle S \rangle$ is dense in $G$. Then $\Gamma = U \cap \langle S \rangle$ is finite index in $\langle S \rangle$, hence $\Gamma$ is finitely generated, so $\Gamma = \langle S' \rangle$ for $S'$ finite. Since $U$ is open, and $\langle S \rangle$ is dense, $\langle S' \rangle = U \cap \langle S \rangle$ is dense in $U$. So $U$ is topologically finitely generated. □

**Proposition 2.5.6.** *Let $(G_j)$ be a surjective inverse system of finite groups with $G = \varprojlim_j G_j$. Let $S \subseteq G$. Then $S$ is a topological generating set for $G$ if and only if $p_j(S)$ generates $G_j$ for all $j$.*

*Proof.* By Corollary 1.2.19, $\langle S \rangle$ is dense in $G$ if and only if $G_j = p_j(\langle S \rangle) = \langle p_j(S) \rangle$ for all $j$. □

**Lemma 2.5.7.** *Let $G$ be a topologically finitely generated profinite group. Then $G$ may be written as the inverse limit of a countable inverse system of finite groups.*

*Proof.* A continuous homomorphism from $G$ to a finite group is determined by the image of a topological generating set $S$, since a function on $S$ determines all of a homomorphism from $\langle S \rangle$ and continuity gives the behaviour on all of $G$. So there are only countably many continuous homomorphisms from $G$ to $\operatorname{Sym} n$ for $n \in \mathbb{N}$. Every open normal subgroup of $G$ is the kernel of such a continuous homomorphism. So there are only countably many open normal subgroups of $G$. Then $\mathcal{U} = \{U \lhd_{\mathrm{o}} G\}$ is a neighbourhood base of the identity, so by Proposition 1.2.22, $G = \varprojlim_{U \in \mathcal{U}} G/U$. □

**Example 2.5.8.** Let $G$ be a topologically finitely generated profinite group. Then there are only finitely many open subgroups of $G$ of index at most $n$. See Lemma 1.2.10. Define

$$G_n = \bigcap \{U \mid U \leq_{\mathrm{o}} G,\ [G : U] \leq n\}.$$

Then $G_n \lhd G$, and $G_n$ is open in $G$. And $\{G_n\}$ is a neighbourhood base of the identity. So

$$G = \varprojlim_{n \in \mathbb{N}} G/G_n.$$

**Proposition 2.5.9.** *Let $\mathbb{Z}_p^\times$ be the set of elements $\alpha$ of $\mathbb{Z}_p$ which topologically generate $\mathbb{Z}_p$. Then $\alpha \in \mathbb{Z}_p^\times$ if and only if $\alpha \not\equiv 0 \mod p$. Hence $\mathbb{Z}_p^\times$ is a closed uncountable subset of $\mathbb{Z}_p$. For every $n$, and every generator $a_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ there is some $\alpha \in \mathbb{Z}_p^\times$ such that $\alpha \equiv a_n \mod p^n$.*

*Proof.* For the last part, $a_n$ is the image of $\alpha$, since it is a surjective inverse system, and if $a_n$ generates $\mathbb{Z}/p^n\mathbb{Z}$, it is coprime to $p$. If $\alpha = (a_n)$ such that $a_1 \neq 0$, then $p \nmid a_n$ for any $n$. Hence $a_n$ is coprime to $p$, and so generates $\mathbb{Z}/p^n\mathbb{Z}$ for all $n$. So $\langle \alpha \rangle$ is dense in $\mathbb{Z}_p$ by an earlier result. □

Lecture 8
Saturday
06/02/21

**Remark 2.5.10.** $\mathbb{Z}_p^\times$ is the set of units in the ring $\mathbb{Z}_p$.

$\Longleftarrow$ If $\alpha$ is a unit, then $\alpha \mod p^n$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}$, so generates $\mathbb{Z}/p^n\mathbb{Z}$. Then $\alpha$ topologically generates $\mathbb{Z}_p$.

[2] Exercise

$\implies$ Consider the group homomorphism

$$\begin{array}{rccc} f & : & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \\ & & x & \longmapsto & \alpha x \end{array},$$

which is continuous as multiplication in a ring is continuous. So $\operatorname{im} f$ is a closed subgroup of $\mathbb{Z}_p$, containing $\alpha$. Then $\alpha$ generates $\mathbb{Z}_p$, so the only closed subgroup containing $\alpha$ is $\mathbb{Z}_p$ itself. So $1 \in \operatorname{im} f$, so there exists $\beta$ such that $\alpha\beta = 1$.

Thus $\alpha$ is a unit if and only if $\{\alpha\}$ is a topological generating set for $\mathbb{Z}_p$.

**Example 2.5.11.** If $p \neq 2$, then 2 is invertible in $\mathbb{Z}_p$, so $2^{-1}$ exists. If $p = 3$, then $2^{-1} = (\ldots, 5, 2) \in \mathbb{Z}_3 \leq \prod_{n\in\mathbb{N}} \mathbb{Z}/3^n\mathbb{Z}$.

**Proposition 2.5.12.** *$\alpha \in \widehat{\mathbb{Z}}^\times$ if and only if $\alpha \mod n \in (\mathbb{Z}/n\mathbb{Z})^\times$ for all $n$. For any $n$, and every $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ there exists a generator $\alpha \in \widehat{\mathbb{Z}}^\times$ such that $\alpha \equiv k \mod n$.*

*Proof.* Follows from Proposition 2.5.9 via the CRT, since $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. □

**Theorem 2.5.13** (Gaschutz's lemma for finite groups)**.** *Let $f : G \twoheadrightarrow H$ be a surjective homomorphism of finite groups. Suppose $G$ has some generating set of size $d$. For any generating set $\{z_1, \ldots, z_d\} \subseteq H$, there exists a generating set $\{x_1, \ldots, x_d\} \subseteq G$ such that $f(x_i) = z_i$ for all $i$.*

Really, talking about generating vectors $\underline{x} = (x_1, \ldots, x_d) \in G^d$. Extend $f$ to $f : G^d \to H^d$.

*Proof.* We will prove, by induction on $|G|$, for $H$ fixed, the following statement. The number

$$N_G(\underline{y}) = \left|\left\{\text{generating vectors } \underline{x} \text{ of } G \;\middle|\; f(\underline{x}) = \underline{y}\right\}\right|,$$

where $\underline{y} \in H^d$ is a generating vector of $H$, is independent of $\underline{y}$. Want to show $N_G(\underline{z}) > 0$, and $G$ has some generating vector $\underline{x'} \in G^d$ so $N_G(\underline{z}) = N_G(f(\underline{x'})) > 0$. Let $\underline{y} \in H^d$ be a generating vector. Let

$$\mathcal{C} = \{d\text{-generator proper subgroups of } G\}.$$

Every $\underline{x} \in G^d$ such that $f(\underline{x}) = \underline{y}$ either generates $G$ or generates some $C \in \mathcal{C}$. Therefore

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

Thus $N_G(\underline{y}) = |\ker f|^d - \sum_{C\in\mathcal{C}} N_C(\underline{y})$, which is independent of $\underline{y}$ by induction. □

**Theorem 2.5.14** (Gaschutz's lemma for profinite groups)**.** *Let $f : G \to H$ be a continuous surjective homomorphism of profinite groups. Suppose $G$ has a topological generating set of size $d$. Then for any topological generating set $\{z_1, \ldots, z_d\}$ of $H$, there is a topological generating set $\{x_1, \ldots, x_d\}$ of $G$ such that $f(x_i) = z_i$ for all $i$.*

*Proof.* By Proposition 1.3.6 and Proposition 2.4.9 we may assume and write $G = \varprojlim_{j\in J} G_j$ and $H = \varprojlim_{j\in H} H_j$, surjective inverse systems of finite groups, with a morphism of inverse systems $(f_j) : (G_j) \to (H_j)$ such that $f = \varprojlim_j f_j$. It is forced that $f_j$ is surjective, since

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

Let $\underline{z}$ be the given topological generating set of $H$. Set $\underline{z}_j$ for $j \in J$ to be the image of $\underline{z}$ in $H_j$, so $\underline{z}_j = p_j^H(\underline{z})$ is a generating vector of $H_j$. Consider the finite sets

$$X_j = \left\{\text{generating vectors } \underline{x}_j \in G_j^d \;\middle|\; f_j(\underline{x}_j) = \underline{z}_j\right\} \neq \emptyset,$$

by Gaschutz. The $X_j$ form an inverse system, since $\phi_{ij}(X_i) \subseteq X_j$. Therefore $\varprojlim_j X_j$ is non-empty. If $\underline{x} \in \varprojlim_j X_j \subseteq G^d$ such that $p_j^G(\underline{x}) \in X_j$, then $\underline{x}$ is a topological generating set of $G$ and $p_j^H(f(\underline{x})) = \underline{z}_j$ for all $j$, so $f(\underline{x}) = \underline{z}$. □

# 3 Profinite completions

## 3.1 Residual finiteness

**Notation 3.1.1.** Discrete abstract groups will be Greek letters and profinite groups will be Roman letters.

Given an abstract group $\Gamma$ and an inverse system $\mathcal{N} = \{N \triangleleft_{\mathrm{f}} \Gamma\}$, there is an inverse system of finite groups $\Gamma/N$. Then $\widehat{\Gamma} = \varprojlim_{N\in\mathcal{N}} \Gamma/N$, where $\Gamma/N_1 \to \Gamma/N_2$ if $N_1 \leq N_2$. Also had a canonical morphism $\iota_\Gamma = \iota : \Gamma \to \widehat{\Gamma}$. The image of $\iota$ is dense by Corollary 1.2.19. Also implies for any finite generating set $S \subseteq \Gamma$, $\iota(S)$ is a topological generating set of $\widehat{\Gamma}$, so if $\Gamma$ is finitely generated, then $\widehat{\Gamma}$ is topologically finitely generated.

**Proposition 3.1.2.** *Let $f : \Delta \to \Gamma$ be a group homomorphism. Then there exists a unique continuous group homomorphism $\widehat{f} : \widehat{\Delta} \to \widehat{\Gamma}$ such that $\widehat{f} \circ \iota_\Delta = \iota_\Gamma \circ f$, so*

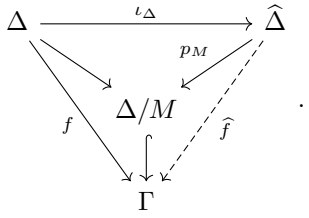
$$\begin{array}{ccc} \Delta & \xrightarrow{f} & \Gamma \\ {\scriptstyle \iota_\Delta}\downarrow & & \downarrow{\scriptstyle \iota_\Gamma} \\ \widehat{\Delta} & \xrightarrow[\widehat{f}]{} & \widehat{\Gamma} \end{array}.$$

*Proof.* Uniqueness will follow from the density of $\iota_\Delta(\Delta)$ in $\widehat{\Delta}$. Take two $\widehat{f_1}$ and $\widehat{f_2}$ satisfying Proposition 3.1.2. Consider

$$S = \left\{ \delta \in \widehat{\Delta} \;\middle|\; \widehat{f_1}(\delta) = \widehat{f_2}(\delta) \right\}.$$

Then $S$ is closed, since it is the preimage of the diagonal in $\widehat{\Gamma}\times\widehat{\Gamma}$ under $\left(\widehat{f_1}, \widehat{f_2}\right) : \widehat{\Delta} \to \widehat{\Gamma}\times\widehat{\Gamma}$, and $S$ contains $\iota_\Delta(\Delta)$, which is dense. So $S = \widehat{\Delta}$.

Case 1. $\Gamma$ is finite, so $\Gamma = \widehat{\Gamma}$. Then $\ker f$ is a finite index normal subgroup $M$ of $\Delta$, so there exists a projection map $p_M : \widehat{\Delta} \to \Delta/M$. So we get a composition

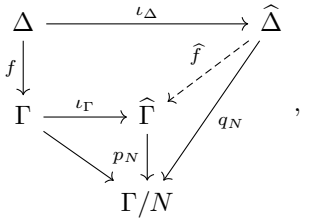



.

Case 2. General case. Take some $N \triangleleft_{\mathrm{f}} \Gamma$. There exists a unique $q_N : \widehat{\Delta} \to \Gamma/N$ such that $q_N \circ \iota_\Delta = p_N \circ \iota_\Gamma \circ f$. Then $(q_N)$ form a cone on the inverse system, since

$$\phi^\Gamma_{N_1N_2} \circ q_{N_1} \circ \iota_\Delta = \phi^\Gamma_{N_1N_2} \circ p_{N_1} \circ \iota_\Gamma \circ f = p_{N_2} \circ \iota_\Gamma \circ f = q_{N_2} \circ \iota_\Delta.$$

Thus there exists a unique $\widehat{f} : \widehat{\Delta} \to \widehat{\Gamma}$ such that $p_N \circ \widehat{f} = q_N$ for all $N$, so




,

and

$$p_N \circ \widehat{f} \circ \iota_\Delta = q_N \circ \iota_\Delta = p_N \circ \iota_\Gamma \circ f.$$

□

**Corollary 3.1.3.** *$\widehat{\cdot}$ is a functor.*

Lecture 9
Tuesday
09/02/21

**Definition 3.1.4.** Let $\Gamma$ be an abstract group. Then $\Gamma$ is **residually finite** if for every $\gamma \in \Gamma \setminus \{1\}$, there exists $N \lhd_{\mathrm{f}} \Gamma$ such that $\gamma \notin N$, if and only if $\gamma N \neq 1$ in $\Gamma/N$, if and only if there exists $\phi : \Gamma \to G$ finite such that $\phi(\gamma) \neq 1$.

**Proposition 3.1.5.** *$\Gamma$ is residually finite if and only if $\iota : \Gamma \to \widehat{\Gamma}$ is injective.*

*Proof.*

$$\begin{array}{ccccc} \iota & : & \Gamma & \longrightarrow & \widehat{\Gamma} \leq \prod\limits_{N} \Gamma/N \\ & & \gamma & \longmapsto & (\gamma N) \end{array}.$$

□

**Proposition 3.1.6.** *Any subgroup of a residually finite group is residually finite.*

**Proposition 3.1.7.** *Let $\Gamma$ be an abstract group, and let $\Delta \leq \Gamma$ be finite index. If $\Delta$ is residually finite, then $\Gamma$ is residually finite.*

*Proof.* Let $\gamma \in \Gamma \setminus \{1\}$.

Case 1. If $\gamma \notin \Delta$, consider

$$\gamma \notin N = \mathrm{Core}_\Gamma \Delta = \bigcap_{g \in \Gamma} g \Delta g^{-1} \lhd_{\mathrm{f}} \Gamma,$$

which has finitely many distinct terms, since if $g\Delta = g'\Delta$ then $g = g'\delta$ so $g\Delta g^{-1} = g'\delta\Delta\delta^{-1}g'^{-1} = g'\Delta g'^{-1}$.

Case 2. If $\gamma \in \Delta$, there exists $N \lhd_{\mathrm{f}} \Delta$ such that $\gamma \notin N$. Now $\gamma \notin \mathrm{Core}_\Gamma N \lhd_{\mathrm{f}} \Gamma$.

□

**Proposition 3.1.8.** *Finitely generated abelian groups are residually finite.*

*Proof.* Exercise. [3] □

**Proposition 3.1.9.** *The groups $\mathrm{SL}_N \mathbb{Z} \leq_{\mathrm{f}} \mathrm{GL}_N \mathbb{Z}$ are residually finite for all $N$.*

*Proof.* For $A \in \mathrm{GL}_N \mathbb{Z} \setminus \{\mathrm{I}\}$. Take a prime $p$ larger than the absolute value of all entries of $A$. Then we have the homomorphism

$$\begin{array}{ccc} \mathrm{GL}_N \mathbb{Z} & \longrightarrow & \mathrm{GL}_N (\mathbb{Z}/p\mathbb{Z}) \\ A & \longmapsto & A_p \neq \mathrm{I} \end{array}.$$

□

These linear groups have as subgroups many important groups, such as free groups in $\mathrm{SL}_2 \mathbb{Z}$.

**Theorem 3.1.10** (Malcev's theorem)**.** *Let $\Gamma$ be a finitely generated subgroup of $\mathrm{GL}_N K$ where $K$ is a field. Then $\Gamma$ is residually finite.*

*Proof (non-examinable).* The entries of a generating set of $\Gamma$ generate a finitely generated subring $R$ of $K$. Commutative algebra says that $R$ has many maximal ideals $\mathfrak{p} \subseteq R$, such that $R/\mathfrak{p}$ is a finite field. Use maps $\mathrm{GL}_N R \to \mathrm{GL}_N (R/\mathfrak{p})$ to show residual finiteness. □

**Proposition 3.1.11.** *The fundamental group of a surface is residually finite.*

*Proof.* Surface groups, via geometry, are subgroups of $\mathrm{Isom}\, \mathbb{H}^2 \cong \mathrm{PSL}_2 \mathbb{R}$. □

[3] Exercise: classification of finitely generated abelian groups

**Lemma 3.1.12.** *Let $\Gamma$ be an abstract group. The open subgroups of $\widehat{\Gamma}$ are exactly $\overline{\iota(\Delta)}$ for $\Delta \leq_{\mathrm{f}} \Gamma$.*

*Proof.* If $\Delta \leq_{\mathrm{f}} \Gamma$ is finite index, take a finite set of coset representatives $\{\gamma_i\}$ of $\Delta$ in $\Gamma$, so $\Gamma = \bigcup_i \gamma_i \Delta$. Then

$$\widehat{\Gamma} = \overline{\iota(\Gamma)} = \overline{\bigcup_i \iota(\gamma_i \Delta)} = \bigcup_i \iota(\gamma_i)\, \overline{\iota(\Delta)},$$

so $\overline{\iota(\Delta)}$ is closed, and finite index, if and only if open. If $U \leq_{\mathrm{o}} \widehat{\Gamma}$, then $\iota(\Gamma)$ is dense, so $U = \overline{\iota(\Gamma) \cap U}$. Set $\Delta = \iota^{-1}(U) \leq_{\mathrm{f}} \Gamma$, and $\iota(\Delta) = \iota(\Gamma) \cap U$. Thus $U = \overline{\iota(\Delta)}$. □

**Theorem 3.1.13.** *Let $G$ and $H$ be topologically finitely generated profinite groups. Suppose the sets of isomorphism types of continuous finite quotients of $G$ and $H$ are equal. Then $G$ and $H$ are isomorphic profinite groups.*

Topologically finitely generated is necessary since $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \ncong (\mathbb{Z}/2\mathbb{Z})^{\mathbb{R}}$. Continuous is not actually necessary by a hard theorem by Nikolov and Segal.

*Proof.* Let $G_n$ be the intersection of all open subgroups of $G$ of index at most $n$. Similarly, $H_n$. By Example 2.5.8, $G = \varprojlim_n G/G_n$ and $H = \varprojlim_n H/H_n$. By assumption there exists $V \lhd_{\mathrm{o}} H$, such that $G/G_n \cong H/V$. The intersection of index at most $n$ subgroups of $G/G_n$ is trivial, and the intersection of index at most $n$ subgroups of $H/V$ is trivial. Taking preimages, there exist index at most $n$ open subgroups of $H$ whose intersection is contained in $V$. Then $H_n \leq V$, so $|G/G_n| = |H/V| \leq |H/H_n|$. By symmetry, $|G/G_n| \geq |H/H_n|$, so equality holds and $V = H_n$. So $G/G_n \cong H/H_n$ for all $n$. We want a morphism of inverse systems, so commuting diagrams

$$\begin{array}{ccc} G/G_n & \longrightarrow & H/H_n \\ \downarrow & & \downarrow \\ G/G_{n-1} & \longrightarrow & H/H_{n-1} \end{array}.$$

Let

$$S_n = \{\text{isomorphisms } f_n : G/G_n \to H/H_n\} \neq \emptyset.$$

If $f_n \in S_n$, then $f_n$ takes an index at most $n-1$ subgroup of $G/G_n$ to an index at most $n-1$ subgroup of $H/H_n$. The intersection of such subgroups is $G_{n-1}/G_n$. So $f_n$ maps $G_{n-1}/G_n$ to $H_{n-1}/H_n$. So there is a well-defined quotient map such that the diagram

$$\begin{array}{ccc} G/G_{n-1} & \xrightarrow[\sim]{\phi_{n,n-1}(f_n)} & H/H_{n-1} \\ \uparrow & & \uparrow \\ G/G_n & \xrightarrow[f_n]{\sim} & H/H_n \end{array}$$

commutes. The $\phi_{n,n-1} : S_n \to S_{n-1}$ make $(S_n)$ into an inverse system. Then $\varprojlim_n S_n$ is non-empty, and an element of $\varprojlim_n S_n \leq \prod_n S_n$ is a sequence of $f_n$ such that all diagrams commute. Thus there is an isomorphism of inverse systems, so $G \cong H$. □

**Theorem 3.1.14.** *Let $\Gamma$ and $\Delta$ be finitely generated abstract groups. Suppose the sets of isomorphism types of finite quotients of $\Gamma$ and $\Delta$ are equal. Then $\widehat{\Gamma} \cong \widehat{\Delta}$.*

Lecture 10
Thursday
11/02/21

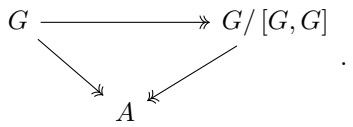
**Definition 3.1.15.** A property $\mathcal{P}$ of groups is a **profinite invariant** if, whenever two finitely generated residually finite groups $G$ and $H$ have $\widehat{G} \cong \widehat{H}$, $G$ has $\mathcal{P}$ if and only if $H$ has $\mathcal{P}$.

**Proposition 3.1.16.** *Being abelian is a profinite invariant.*

*Proof.* Let $G$ and $H$ be finitely generated residually finite groups such that $\widehat{G} \cong \widehat{H}$, with $H$ abelian. Every quotient group of $H$ is abelian, so every finite quotient of $G$ is abelian. Suppose $G$ is not abelian. There exist $g_1, g_2 \in G$ such that $[g_1, g_2] \neq 1$. Since $G$ is residually finite, there exists a finite quotient $Q$ of $G$ and $\phi : G \twoheadrightarrow Q$, such that $[\phi(g_1), \phi(g_2)] = \phi([g_1, g_2]) \neq 1$. But $Q$ is abelian, a contradiction. □

**Proposition 3.1.17.** *Let $G$ and $H$ be finitely generated groups with $\widehat{G} \cong \widehat{H}$. Then the abelianisations $G_{\mathrm{ab}} = G/[G,G]$ and $H_{\mathrm{ab}} = H/[H,H]$ are isomorphic.*

*Proof.* Suppose $\widehat{G} \cong \widehat{H}$. We claim $\widehat{G_{\mathrm{ab}}} \cong \widehat{H_{\mathrm{ab}}}$. Since $G$ and $H$ have the same finite quotients they have the same abelian finite quotients, which are the finite quotients of $G_{\mathrm{ab}}$ and $H_{\mathrm{ab}}$, since




It remains to show, if $A$ and $A'$ are finitely generated abelian groups with $\widehat{A} \cong \widehat{A'}$ then $A \cong A'$. By the classification, $A = \mathbb{Z}^r \times T$ and $A' \cong \mathbb{Z}^s \times T'$ for $r, s \in \mathbb{N}$ and $T$ and $T'$ finite. We can see $r$ and $T$ from finite quotients, since

$$r = \max\left\{k \;\middle|\; \forall n,\ A \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^k\right\} = \max\left\{k \;\middle|\; \forall n,\ A' \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^k\right\} = s.$$

Having found $r$, $T$ is the largest finite group such that $A \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^r \times T$ for all $n$, which is $T'$. □

**Corollary 3.1.18.** *If $G$ is abelian, the property of being isomorphic to $G$ is a profinite invariant.*

**Example 3.1.19.** Let

$$\begin{array}{rccc} \phi & : & \mathcal{C}_{25} & \longrightarrow & \mathcal{C}_{25} \\ & & t & \longmapsto & t^6 \end{array}$$

be an automorphism, where $\mathcal{C}_{25} = \mathbb{Z}/25\mathbb{Z} = \langle t \rangle$. Form semidirect products

$$G_1 = \mathcal{C}_{25} \rtimes_\phi \mathbb{Z}, \qquad \left(t^a, s^b\right) *_1 \left(t^c, s^d\right) = \left(t^a \phi^b\left(t^c\right), s^{b+d}\right),$$

$$G_2 = \mathcal{C}_{25} \rtimes_{\phi^2} \mathbb{Z}, \qquad \left(t^a, s^b\right) *_2 \left(t^c, s^d\right) = \left(t^a \phi^{2b}\left(t^c\right), s^{b+d}\right),$$

where $\mathbb{Z} = \langle s \rangle$. Note that $\phi$ is of order five, so $\phi^5 = \mathrm{id}$ and $\phi^k = \phi^l$ if and only if $k \equiv l \mod 5$.

- Claim that $G_1$ is not isomorphic to $G_2$. Suppose $\Phi : G_2 \to G_1$ is an isomorphism. Each $G_i$ has a unique order 25 subgroup. So $\Phi(\mathcal{C}_{25}) = \mathcal{C}_{25}$ and $\Phi(t, 1) = (t^a, 1)$ for some $a$ coprime to 25. Set $\Phi(1, s) = \left(t^b, s^c\right)$, and $s^c$ generates $\mathbb{Z}$, so $c = \pm 1$. A contradiction comes from the computation of

$$\begin{aligned} \left(\phi^2(t)^a, 1\right) &= \Phi\left(\phi^2(t), 1\right) = \Phi\left((1,s) *_2 (t,1) *_2 \left(1, s^{-1}\right)\right) = \Phi(1,s) *_1 \Phi(t,1) *_1 \Phi\left(1, s^{-1}\right) \\ &= \left(t^b, s^c\right) *_1 (t^a, 1) *_1 \left(\phi^{-c}\left(t^{-b}\right), s^{-c}\right) = \left(\phi^c(t^a), 1\right), \end{aligned}$$

  and since $\phi^2(t^a) = \phi^c(t^a)$, $\phi^2 = \phi^c$, so $c \equiv 2 \mod 5$.

- Consider finite quotients of $G_1$. Let $f : G_1 \to Q$ be a finite quotient map. If $\mathrm{im}(\mathbb{Z} \to G_1 \to Q)$ has order $m$, then $\ker f \geq 5m\mathbb{Z}$. Then $f$ factors through the quotient $\mathcal{C}_{25} \rtimes_\phi \mathbb{Z}/5m\mathbb{Z}$, which is cofinal, so

$$\widehat{G_1} = \varprojlim_m \mathcal{C}_{25} \rtimes_\phi \mathbb{Z}/5m\mathbb{Z} = \mathcal{C}_{25} \rtimes_\phi \widehat{\mathbb{Z}}.$$

  By Gaschutz lemma, there exists $\kappa \in \widehat{\mathbb{Z}}^\times$ such that $\kappa \equiv 2 \mod 5$. We may now build an isomorphism defined by

$$\begin{array}{rccc} \Omega & : & \widehat{G_2} & \longrightarrow & \widehat{G_1} \\ & & \left(t^b, s^\lambda\right) & \longmapsto & \left(t^b, s^{\lambda\kappa}\right) \end{array}.$$

  This is a continuous bijection, and can compute it is a group homomorphism.

**Question 3.1.20** (Remeslennikov's question)**.** Let $F$ be a finitely generated free group, and $G$ a finitely generated residually finite group. Is it true that $\widehat{F} \cong \widehat{G}$ implies that $F \cong G$?

**Question 3.1.21.** Does there exist $G$ a finitely generated residually finite group, other than a free group, and an integer $n$ such that a finite group $Q$ is a quotient of $G$ if and only if $Q$ has a generating set with $n$ elements?

**Proposition 3.1.22.** *Let $F$ and $F'$ be finitely generated free groups. If $\widehat{F} \cong \widehat{F'}$ then $F \cong F'$.*

*Proof.* From earlier, if $\widehat{F} \cong \widehat{F'}$ then $\mathbb{Z}^{\operatorname{rk} F} = F_{\mathrm{ab}} \cong F'_{\mathrm{ab}} = \mathbb{Z}^{\operatorname{rk} F'}$. Thus $\operatorname{rk} F = \operatorname{rk} F'$, so $F \cong F'$. □

How about surface groups? If $\mathrm{S}_g$ is the fundamental group of an orientable surface of genus $g$, then

$$\mathrm{S}_g = \langle a_1, b_1, \ldots, a_g, b_g \mid [a_1, b_1] \ldots [a_g, b_g] = 1 \rangle .$$

Then the abelianisation of $\mathrm{S}_g$ is $\mathbb{Z}^{2g}$. Hence $\widehat{\mathrm{S}_g} \ncong \widehat{\mathrm{F}_r}$, unless possibly $r = 2g$.

**Theorem 3.1.23** (Basic correspondence)**.** *Let $G_1$ and $G_2$ be finitely generated residually finite groups, and suppose $\phi : \widehat{G_1} \cong \widehat{G_2}$. Then there is a bijection*

$$\psi : \{\textit{finite index subgroups of } G_1\} \to \{\textit{finite index subgroups of } G_2\},$$

*such that, if $K \leq_{\mathrm{f}} H \leq_{\mathrm{f}} G_1$, then*

- *$\psi(K) \leq \psi(H)$ and $[H : K] = [\psi(H) : \psi(K)]$,*
- *$K \lhd H$ if and only if $\psi(K) \lhd \psi(H)$,*
- *if $K \lhd H$, then $H/K \cong \psi(H)/\psi(K)$, and*
- *$\widehat{H} \cong \widehat{\psi(H)}$.*

By the Nielsen-Schreier theorem, $\mathrm{F}_{2g}$ has an index two subgroup, which is free of rank $4g - 1$, so has abelianisation odd rank. Any finite index subgroup of a surface group is a surface group, so it has even rank abelianisation, contradicting the basic correspondence, so $\widehat{\mathrm{F}_{2g}} \ncong \widehat{\mathrm{S}_g}$.

Lecture 11
Saturday
13/02/21

**Remark 3.1.24.**

- Residually finite is not actually necessary, by replacing $G_1$ by $G_1/\ker \iota_{G_1}$ for $\iota : G_1 \to \widehat{G_1}$.
- $\phi$ and $\psi$ do not depend on any homomorphism $G_1 \to G_2$.

**Proposition 3.1.25.** *Let $G$ be a finitely generated residually finite group. Let $\psi$ be the function*

$$\begin{array}{rcccc} \psi & : & \{\textit{finite index subgroups } H \leq G\} & \longrightarrow & \left\{\textit{open subgroups of } \widehat{G}\right\} \\ & & H & \longmapsto & \overline{H} \end{array} .$$

*Then, if $K \leq_{\mathrm{f}} H \leq_{\mathrm{f}} G$,*

1. *$\psi$ is a bijection,*
2. *$[H : K] = \left[\overline{H} : \overline{K}\right]$,*
3. *$K \lhd H$ if and only if $\overline{K} \lhd \overline{H}$,*
4. *if $K \lhd H$, then $H/K \cong \overline{H}/\overline{K}$, and*
5. *$\overline{H} \cong \widehat{H}$.*

*Proof.*

1. Let $H \leq_{\mathrm{f}} G$ and take coset representatives $\{g_i\}$ of $H$ in $G$. Since $\widehat{G} = \overline{\bigcup_i g_i H} = \bigcup_i g_i \overline{H}$, $\overline{H}$ is finite index, so open. Conversely, if $U \leq_{\mathrm{o}} \widehat{G}$ then $U = \overline{G \cap U}$, since $G$ is dense and $U$ is open and closed, so let $H = G \cap U$. So $\psi$ is surjective. To show $\psi$ is injective, we show $\overline{H} \cap G = H$. Considering the action of $G$ on $G/H$, gives a continuous homomorphism

$$\begin{array}{ccc} G & \longrightarrow & \operatorname{Sym}(G/H) \\ \cap & \nearrow & \\ \widehat{G} & & \end{array} .$$

   Then $H$ fixes the coset $1H$. By continuity of the action, $\overline{H}$ fixes $1H$. But if $g \in G \setminus H$, then $g \cdot 1H = gH \neq 1H$, so $g \notin \overline{H}$. So $\overline{H} \cap G = H$.

2. Let $\{g_i\}$ be a set of coset representatives. We know that the $g_i\overline{H}$ cover $\widehat{G}$. They are distinct cosets, since if $g_i\overline{H} = g_j\overline{H}$, then $g_i^{-1}g_j \in \overline{H} \cap G = H$. So $g_iH = g_jH$, so $g_i = g_j$, so $\left[\widehat{G} : \overline{H}\right] = [G : H]$. Also, there is a natural bijection of coset spaces $G/H \to \widehat{G}/\overline{H}$.

3. If $\overline{K} \triangleleft \overline{H}$ then $K = \overline{K} \cap G \triangleleft \overline{H} \cap G = H$. Conversely, if $K \triangleleft H$, consider the action of $\overline{H}$ on $\mathrm{Sym}\left(\overline{H}/\overline{K}\right) = \mathrm{Sym}\left(H/K\right) \leq \mathrm{Sym}\left(G/K\right)$. Then $K \triangleleft H$ if and only if $K$ acts trivially on $H/K$, since $k \cdot hK = hK$ if and only if $h^{-1}kh \in K$. By continuity of the action, $\overline{K}$ acts trivially, so $\overline{K} \triangleleft \overline{H}$.

4. If $K \triangleleft H$, we already have our bijection $H/K \to \overline{H}/\overline{K}$, and this is an isomorphism of groups.

5. $\overline{H}$ maps onto all finite quotients $H/K$ in a natural way, so we get a continuous homomorphism $\overline{H} \to \widehat{H}$. This is surjective because $H$ is dense in $\widehat{H}$. For injectivity, if $h \in \overline{H} \setminus \{1\}$, then there is $U \triangleleft_{\mathrm{o}} \widehat{G}$ such that $h \notin U$, and the map

$$\begin{array}{ccc} \overline{H} & \longrightarrow & H/\left(U \cap H\right) \\ & \searrow \quad \nearrow & \\ & \widehat{H} & \end{array}$$

shows that $h \not\mapsto 1 \in \widehat{H}$.

□

**Remark 3.1.26.** $\overline{H} \cap G = H$ and $\overline{H} \cong \widehat{H}$ are not always true if $H$ is not of finite index.

**Definition 3.1.27.** A topological group $G$ is **Hopfian**, or **has the Hopf property**, if every continuous surjection from $G$ to itself is an isomorphism of topological groups.

**Example 3.1.28.** Finite groups, by the pigeonhole principle.

**Proposition 3.1.29.** *Let $G$ be a topologically finitely generated profinite group. Let $f : G \to G$ be a continuous surjection. Then $f$ is an isomorphism.*

*Proof.* Let $G_n$ be the intersection of open subgroups of $G$ of index at most $n$. Then $G_n \triangleleft_{\mathrm{o}} G$, and $G \cong \varprojlim_n G/G_n$. Since $f$ is a surjection, $\left[G : f^{-1}\left(U\right)\right] = [G : U]$ for all $U \leq_{\mathrm{o}} G$. If $U$ has index at most $n$, then $f^{-1}\left(U\right)$ has index at most $n$, so $f^{-1}\left(U\right) \geq G_n$, so $f^{-1}\left(G_n\right) \geq G_n$, so $f\left(G_n\right) \leq G_n$. So we have a quotient map $f_n : G/G_n \twoheadrightarrow G/G_n$, which are surjections, hence isomorphisms. So $(f_n)$ are a morphism of inverse systems giving $f$, so $f = \varprojlim_n f_n$ is an isomorphism. Or, if $g \in G \setminus \{1\}$, then $g \notin G_n$ for some $n$ and then $p_n\left(f\left(g\right)\right) = f_n\left(p_n\left(g\right)\right) \neq 1$ so $g \notin \ker f$. □

**Corollary 3.1.30.** *Finitely generated residually finite groups are Hopfian.*

*Proof.* Let $f : G \to G$ be a surjection where $G$ is finitely generated residually finite. By Proposition 3.1.2, we get an induced map

$$\begin{array}{ccc} \widehat{G} & \xrightarrow{\widehat{f}} & \widehat{G} \\ \uparrow & & \uparrow \\ G & \xrightarrow[f]{} & G \end{array}.$$

Then $\widehat{f}$ is surjective, so it is an isomorphism. Thus $f$ is injective. □

**Proposition 3.1.31.** *Let $G$ be a Hopfian topological group and let $H$ be a topological group. Suppose there exist continuous surjections $f : G \to H$ and $f' : H \to G$. Then $f$ and $f'$ are isomorphisms of topological groups.*

*Proof.* $f' \circ f : G \to G$ is a surjection, hence an isomorphism, and a homeomorphism. So $f$ is injective and $f'$ is injective, because $f$ is a surjection, so isomorphisms. Also $f^{-1} = \left(f' \circ f\right)^{-1} \circ f'$ and $f'^{-1} = f \circ \left(f' \circ f\right)^{-1}$ are continuous. □

Let d be the minimal size of a generating set.

**Proposition 3.1.32.** *Let $G$ be a finitely generated residually finite group. Assume there is a finite quotient $Q$ of $G$ such that $\mathrm{d}(Q) = \mathrm{d}(G)$. If $\widehat{G}$ is isomorphic to $\widehat{F}$ for $F$ a free group, then $G \cong F$.*

*Proof.* Assume $\widehat{G} \cong \widehat{F}$. Then $Q$ is a quotient of $F$, so $\mathrm{d}(F) \geq \mathrm{d}(Q) = \mathrm{d}(G)$. So there is a surjection $f : F \to G$. This induces $\widehat{f} : \widehat{F} \to \widehat{G}$. Then $\widehat{f}$ is surjective, so by the Hopf property, since $\widehat{F} \cong \widehat{G}$, $\widehat{f}$ is an isomorphism. Thus $f$ is an isomorphism, since

$$\begin{array}{ccc} F & \xrightarrow{f} & G \\ \downarrow & & \downarrow \\ \widehat{F} & \xrightarrow[\sim]{} & \widehat{G} \end{array}.$$

□

**Corollary 3.1.33.** $\widehat{\mathrm{S}_g} \ncong \widehat{\mathrm{F}_{2g}}$.

*Proof.* $\mathrm{S}_g$ has rank $2g$, and maps onto $Q = (\mathbb{Z}/2\mathbb{Z})^{2g}$. □

**Example 3.1.34.** Let $n$ and $m$ be coprime integers such that $|n|, |m| > 1$. Define

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

a HNN extension. Define

$$\begin{array}{rccc} f & : & \mathrm{BS}(n,m) & \longrightarrow & \mathrm{BS}(n,m) \\ & & t & \longmapsto & t \\ & & a & \longmapsto & a^n \end{array}.$$

This is well-defined, since

$$f : ta^n t^{-1} a^{-m} \mapsto ta^{n^2} t^{-1} a^{mn} = \left(ta^n t^{-1}\right)^n a^{-mn} = a^{mn} a^{-mn} = 1.$$

- $f$ is surjective. Since $\operatorname{im} f \ni a^n, t$, $\operatorname{im} f \ni ta^n t^{-1} = a^m$, and so $\operatorname{im} f \ni a$, since there exist $r$ and $s$ such that $nr + ms = 1$ so $a = (a^n)^r (a^m)^s$.
- But $f$ is not injective. By Britton's lemma, $tat^{-1}$ does not commute with $a$, so $\left[tat^{-1}, a\right] \neq 1$. But $f\left(\left[tat^{-1}, a\right]\right) = \left[ta^n t^{-1}, a^n\right] = [a^m, a^n] = 1$.

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

## 3.2 Finite quotients of free groups

Lecture 12
Tuesday
16/02/21

**Theorem 3.2.1.** *Free groups are residually finite.*

Previously, $\mathrm{F}_2 \hookrightarrow \mathrm{SL}_2 \mathbb{Z} \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

**Remark 3.2.2.** This is true for infinitely generated free groups. If $F = \langle a_i \rangle_{i \in I}$, take some $g \in F \setminus \{1\}$. Then $g$ can be written as a finite product of $a_i^{\pm 1}$, so you need only finitely many $a_i$. Factoring out the others gives $F \twoheadrightarrow F' \twoheadrightarrow Q$, where $F'$ is a finitely generated free group in which $g$ is mapped to a non-trivial element.

Residual finiteness if and only if $\iota : G \hookrightarrow \widehat{G}$. Residual $p$-finiteness, stronger than residual finiteness, is $\iota : G \hookrightarrow \widehat{G_{(p)}}$, if and only if for all $g \in G \setminus \{1\}$, there exists $\phi : G \to Q$ where $|Q| = p^m$ such that $\phi(g) \neq 1$.

*Proof 1 (non-examinable).* Let $p$ be a prime. Let $X$ be a wedge of $k$ circles, and $F = \pi_1(X)$. Construct $F_n \lhd F$ inductively, by

$$F_1 = F, \qquad F_{n+1} = \bigcap \{\ker f \mid f : F_n \to \mathbb{Z}/p\mathbb{Z}\} = \ker\left(F_n \to \prod_f \mathbb{Z}/p\mathbb{Z}\right).$$

Then $F_n$ are characteristic subgroups, so normal, and $[F : F_n]$ is a power of $p$, by induction. Let $X_n \to X$ be the cover corresponding to $F_n \lhd F$. Claim that $\operatorname{girth} X_{n+1} > \operatorname{girth} X_n$, so $\operatorname{girth} X_n \geq n$. Let $l$ be any loop in $X_n$ of minimal length, $\operatorname{girth} X_n$. We show $l$ does not lift to $X_{n+1}$. Because $l$ is minimal length, there exists an edge $e$ which it crosses once exactly. Collapsing everything except $e$,

$$\begin{array}{rcl} F_n = \pi_1(X_n) & \longrightarrow & \pi_1\left(\mathrm{S}^1\right) = \mathbb{Z} \\ [l] & \longmapsto & 1 \end{array}.$$

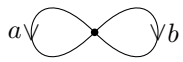
So we have a homomorphism

$$\begin{array}{rcl} F_n & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ [l] & \longmapsto & 1 \neq 0 \end{array},$$

so $[l] \notin F_{n+1}$, hence $l$ does not lift to $X_{n+1}$. Let $g \in F \setminus \{1\}$. Write $g$ as a loop in $X$. Let $n$ be the number of edges of $l$. Then $l$ cannot lift to $X_{n+1}$, with girth at least $n+1$. So $g \notin F_{n+1}$. □

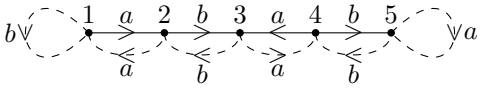
*Proof 2.* Let $F = \langle a_1, \ldots, a_k \rangle$ be a free group. Let $X$ be a bouquet of $k$ circles with $\pi_1(X) = F$. Let $g \in F \setminus \{1\}$. Write $g$ as a product $g = s_1 \ldots s_m$ where $s_i$ is $a_j^{\pm 1}$. Let $Y$ be a line segment labelled $s_1 \ldots s_m$. We add edges to $Y$ to make it a covering space of $X$. This covering space $\widetilde{X}$ does not lift $g$, so $g \notin \pi_1\left(\widetilde{X}\right)$. □

**Example 3.2.3.** Let $F = \langle a, b \rangle$, and let $X$ be




.

If $g = aba^{-1}b$, then $\widetilde{X}$ is




.

We get a homomorphism

$$\begin{array}{rcccl} \phi & : & F & \longrightarrow & \operatorname{Sym} 5 \\ & & a & \longmapsto & (12)(34)(5) \\ & & b & \longmapsto & (1)(23)(45) \end{array},$$

acting on the right. Then

$$\phi(g): \qquad 1 \mapsto 5, \qquad 2 \mapsto 3, \qquad 3 \mapsto 4, \qquad 4 \mapsto 1, \qquad 5 \mapsto 2,$$

so $\phi(g) = (15234)$.

We can also answer stronger questions.

- Given $S \subseteq F$, does $S$ generate $F$? Given $g \in F \setminus \{1\}$, does $g \in \langle S \rangle$?
- Does $\left\{abcb^2cb^{-1}c^{-1}b^{-1}a^{-1}, bc^{-1}b^{-1}abc, bcb^{-1}\right\}$ or $\left\{abcb^2cb^{-1}c^{-1}b^{-1}a^{-1}, bc^{-1}b^{-1}a^{-1}bc, bcb^{-1}\right\}$ generate $\langle a, b, c \rangle$?

**Theorem 3.2.4** (Marshall Hall's theorem)**.** *Let $S$ be a finite subset of a finitely generated free group $F$. Let $y \notin \langle S \rangle$. Then there exists a finite group $Q$ and $f : F \to Q$ such that $f(y) \notin f(\langle S \rangle)$.*

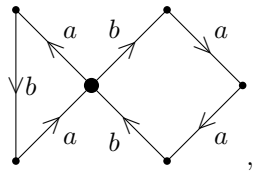
**Corollary 3.2.5.** *A finite subset $S \subset F$ generates $F$ if and only if $S$ topologically generates $\widehat{F}$.*

*Proof.* If $S$ generates $F$, it generates $\widehat{F}$ topologically since $\langle S \rangle = F$ is dense in $\widehat{F}$. If $\langle S \rangle \neq F$, there exists $y \notin \langle S \rangle$. Take a finite group $Q$ and $f : F \to Q$ as in Theorem 3.2.4. Then $f(y) \notin f(\langle S \rangle)$, so $f(\langle S \rangle) \neq f(F)$. Thus $\langle S \rangle$ is not dense in $\widehat{F}$. □

Marshall Hall's theorem says there exists $H \leq_{\mathrm{f}} F$ such that $H = \langle S \rangle * H'$.

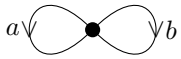
Lecture 13
Thursday
18/02/21

**Example 3.2.6.** Let $F = \langle a, b \rangle$, and let $S = \left\{aba, ba^2b\right\}$. We will show $\langle S \rangle \neq F$. Start by writing the elements of $S$ as loops



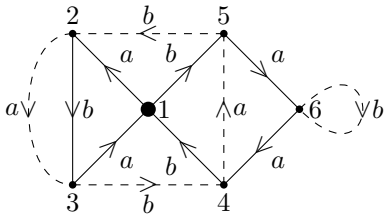

,

and call it $Y$. We have a natural continuous map $Y \to X$, where $X$ is




.

Then $\pi_1(Y) \to \langle S \rangle \leq \pi_1(X)$. Now add edges to make a covering space



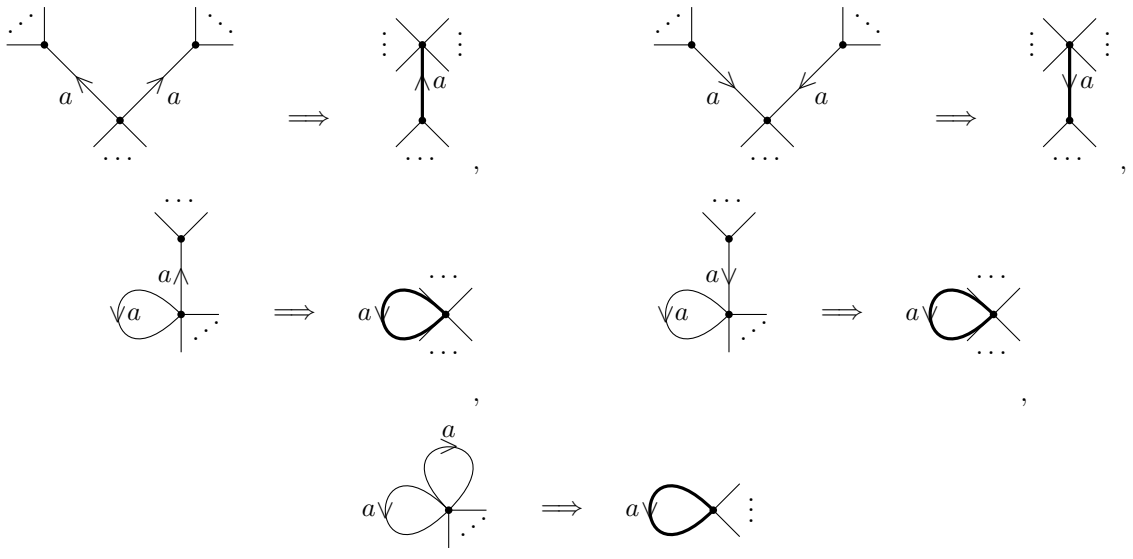

.

The explicit homomorphism to a finite group is

$$\begin{array}{rcccl} \phi & : & F & \longrightarrow & \operatorname{Sym} 6 \\ & & a & \longmapsto & (123)(456) \\ & & b & \longmapsto & (15234)(6) \end{array}.$$

Note that $\phi(\langle S \rangle) \leq \operatorname{Stab} 1$ and $\phi(a) \notin \operatorname{Stab} 1$.

A **Stallings fold** is an operation on oriented, labelled graphs such that




,

,

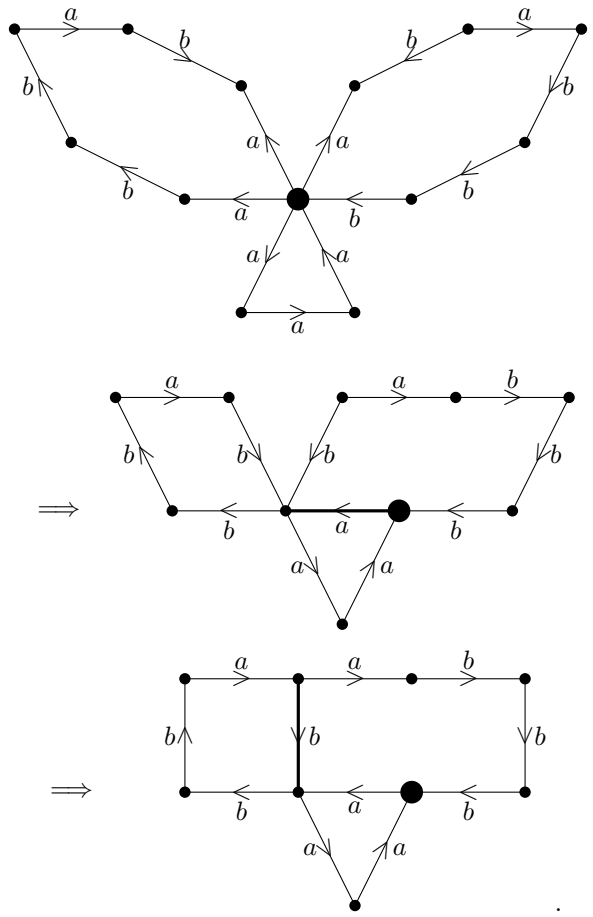
,

,

.

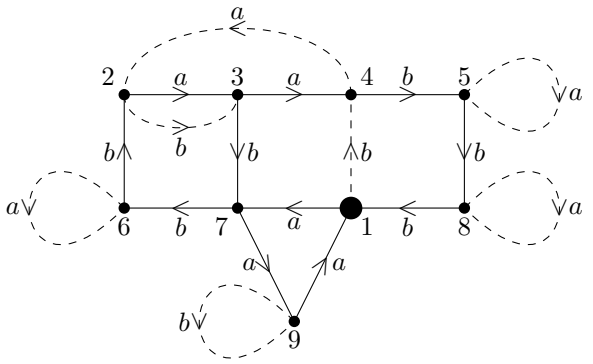
**Fact 3.2.7.** Folding $Y$ gives a new graph $Y'$ such that the image of $\pi_1(Y) \to \pi_1(Y') \to \pi_1(X)$ is still $\langle S \rangle$.

**Example 3.2.8.** Let $F = \langle a, b \rangle$, and let $S = \left\{a^3, ab^2aba^{-1}, ab^{-1}ab^3\right\}$. Folding,




.

Now can add edges to make a covering




.

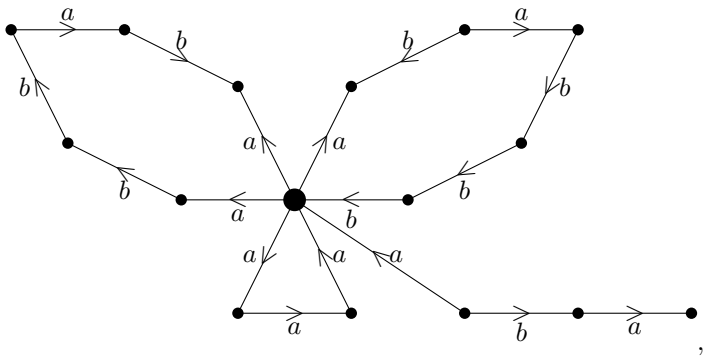
The homomorphism is

$$\begin{array}{rcccl} \phi & : & F & \longrightarrow & \operatorname{Sym} 9 \\ & & a & \longmapsto & (179)\,(234)\,(5)\,(6)\,(8) \\ & & b & \longmapsto & (1458)\,(2376)\,(9) \end{array} .$$

Then $\phi(\langle S \rangle) \leq \operatorname{Stab} 1$ and $\phi(a) \notin \operatorname{Stab} 1$, so $\phi(\langle S \rangle) \neq \phi(F)$. Thus $\langle S \rangle \neq F$. The other case is that folding gives a one-vertex graph, then $\langle S \rangle$ is generated by some standard generators of $F$.

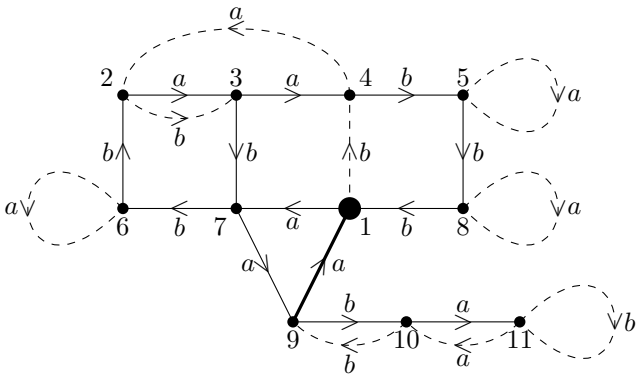
What if we want to know if a specific $y$ lies in $\langle S \rangle$? Add $y$ into the starting graph as a line.

**Example 3.2.9.** Let $y = a^{-1}ba$. Fold




,

and make a covering space




.

Thus $\phi(\langle S \rangle) \leq \operatorname{Stab} 1$ and $\phi(y) = (1 \mapsto 11) \notin \operatorname{Stab} 1$. The other option is that $y$ gets folded into being a loop, then $y \in \langle S \rangle$.

# 4 Pro-$p$ groups

Recall that a pro-$p$ group is an inverse limit of finite $p$-groups, groups of order $p^n$ for $p$ a fixed prime. For example, the pro-$p$ completion of a group such as $\mathbb{Z}_p = \widehat{\mathbb{Z}_{(p)}}$.

## 4.1 Generators of pro-$p$ groups

**Definition 4.1.1.** Let $G$ be a finite group. The **Frattini subgroup** of $G$, denoted $\Phi(G)$, is

$$\Phi(G) = \bigcap \{M \mid M \text{ is a maximal proper subgroup of } G\},$$

such that if $M \leq H \leq G$ then $M = H$ or $H = G$.

Importantly, if $G$ is finite, then every proper subgroup is contained in a maximal proper subgroup.

**Proposition 4.1.2.** *For $G$ a finite group and $S \subseteq G$, the following are equivalent.*

1. *$S$ generates $G$.*
2. *$S\Phi(G)$ generates $G$, so $\Phi(G)$ are non-generators.*
3. *The image of $S$ in $G/\Phi(G)$ generates $G/\Phi(G)$.*

*Proof.*

1 $\implies$ 2. Trivial.

2 $\implies$ 3. Trivial.

3 $\implies$ 1. Suppose $S$ does not generate $G$. Then $\langle S\rangle$ is a proper subgroup, so, since $G$ is finite, $\langle S\rangle$ is contained in a maximal proper subgroup $M$ of $G$. Since $\Phi = \Phi(G) \leq M$, $M/\Phi \neq G/\Phi$, so $S\Phi/\Phi \leq M/\Phi \neq G/\Phi$, so $S\Phi/\Phi$ does not generate $G/\Phi$.

□

Lecture 14
Saturday
20/02/21

**Proposition 4.1.3.** *Let $f : G \to H$ be a surjection of finite groups. Then $f(\Phi(G)) \leq \Phi(H)$. Hence, $\Phi(G)$ is a characteristic subgroup of $G$.*

**Remark 4.1.4.** Surjection is necessary. For example, let $\mathbb{Z}/4\mathbb{Z} = \mathcal{C}_4 \hookrightarrow \operatorname{Sym} 5$. Then $\Phi(\mathbb{Z}/4\mathbb{Z}) = 2\mathbb{Z}/4\mathbb{Z} = \langle 2\rangle$ and $\Phi(\operatorname{Sym} 5) = 1$, since $\mathcal{A}_5$ is ruled out by $\operatorname{Stab} 1$, a maximal proper subgroup not containing $\mathcal{A}_5$.

*Proof.* Let $M$ be a maximal proper subgroup of $H$. We claim $f^{-1}(M)$ is a maximal proper subgroup of $G$. Properness follows from surjectivity. If $\ker f \leq f^{-1}(M) < G' \leq G$, then $M < f(G') \leq H = f(G)$. Since $M$ is maximal, $f(G') = H$. Then $G' = G$, since if $g \in G$, then $f(g) = f(g') \in H$, for some $g' \in G'$, then $gg'^{-1} \in \ker f$, so $g \in g' \ker f \leq G'$. Thus $\Phi(G) \leq f^{-1}(M)$, so $f(\Phi(G)) \leq M$, so $f(\Phi(G)) \leq \Phi(H)$. □

**Definition 4.1.5.** Let $G$ be a group and $H, K \leq G$. Let $m$ be an integer. Define

$$[H,K] = \langle\{[h,k] \mid h \in H,\ k \in K\}\rangle, \qquad H^m = \langle\{h^m \mid h \in H\}\rangle, \qquad HK = \{hk \mid h \in H,\ k \in K\}.$$

If $H \triangleleft G$ then $HK$ is a subgroup and $H^m$ is normal. If $H \triangleleft G$ and $K \triangleleft G$ then $HK \triangleleft G$ and $H \cap K \geq [H,K] \triangleleft G$.

**Proposition 4.1.6.** *Let $G$ be a finite $p$-group. Then*

$$\Phi(G) = [G,G]\,G^p = \langle\{[g_1,g_2]\,g_3^p \mid g_1,g_2,g_3 \in G\}\rangle = \ker\left(G \to G_{\mathrm{ab}} \to G_{\mathrm{ab}}/pG_{\mathrm{ab}}\right),$$

*where $\mathrm{H}_1(G,\mathbb{F}_p) = G_{\mathrm{ab}}/pG_{\mathrm{ab}}$ is a vector space $\mathbb{F}_p^{\mathrm{d}(G)}$ over $\mathbb{F}_p$.*

*Proof.* On example sheet 3. □

**Definition 4.1.7.** Let $G$ be a profinite group. Define the **Frattini subgroup**

$$\Phi(G) = \bigcap \{M \mid M \text{ is a maximal proper closed subgroup of } G\},$$

which is closed, where if $M \leq_{\mathrm{c}} H \leq_{\mathrm{c}} G$ then $H = M$ or $H = G$.

**Proposition 4.1.8.** *Any proper closed subgroup of a profinite group $G$ is contained in a proper open subgroup. Hence a maximal proper closed subgroup is open, and any closed subgroup is contained in a maximal proper closed subgroup.*

*Proof.* Let $H \leq_{\mathrm{c}} G$ such that $H \neq G$. Then by Corollary 1.2.19, there exists $p : G \to Q$ for $Q$ finite such that $p(H) \neq p(G)$. Then $p^{-1}(p(H))$ is open and proper, and contains $H$. Open subgroups have finite index, so maximal if and only if smallest index. □

**Proposition 4.1.9.** *Let $f : G \to H$ be a surjective continuous homomorphism of profinite groups. Then $f(\Phi(G)) \leq \Phi(H)$.*

**Proposition 4.1.10.** *Let $G$ be profinite and $S \subseteq G$. Then the following are equivalent.*

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

**Proposition 4.1.11.** *Let $(G_j)_{j\in J}$ be a surjective inverse system of finite groups and $G = \varprojlim_j G_j$. Then*

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

*Proof.* $\Phi(G) = \varprojlim_j p_j(\Phi(G)) \leq \varprojlim_j \Phi(G_j)$. Let $M$ be a maximal proper closed subgroup of $G$. Since $M$ is open, there exists $i \in J$ such that $\ker p_i \leq M$. This implies $\ker p_j \leq M$ for $j \leq i$. Then $p_j(M)$ is a maximal proper subgroup of $G_j$ for all $j \leq i$, so $\Phi(G_j) \leq p_j(M)$ for all $j \leq i$. Pass to the cofinal subsystem $\{j \leq i\}$. Now $\varprojlim_j \Phi(G_j) \leq \varprojlim_j p_j(M) = M$. So $\varprojlim_{j\in J} \Phi(G_j) \leq M$ for all $M$, so $\varprojlim_{j\in J} \Phi(G_j) \leq \Phi(G)$. □

**Proposition 4.1.12.** *Let $G$ be a topologically finitely generated pro-$p$ group. Then*

$$\Phi(G) = \overline{[G,G]\,G^p} = \mathrm{H}_1(G, \mathbb{F}_p), \qquad G/\Phi(G) \cong \mathbb{F}_p^d,$$

*where $d = \mathrm{d}(G)$ is the minimal size of a topological generating set of $G$.*

*Proof.* Write $G = \varprojlim_j G_j$ as a surjective inverse system of finite $p$-groups. We know $\Phi(G) = \varprojlim_j [G_j, G_j] G_j^p$. For any $[g_1, g_2] g_3^p$ for $g_1, g_2, g_3 \in G$ we have $p_j([g_1, g_2] g_3^p) = [p_j(g_1), p_j(g_2)] p_j(g_3)^p \in [G_j, G_j] G_j^p$, so $\overline{[G,G]\,G^p} \leq \varprojlim_j [G_j, G_j] G_j^p = \Phi(G)$. Since $G/\overline{[G,G]\,G^p}$ is topologically finitely generated, abelian, and every element has order $p$, it is finite and equal to $\mathbb{F}_p^d$ for some $d$. But $\Phi(\mathbb{F}_p^d) = \{0\}$, so $\Phi(G) \leq \overline{[G,G]\,G^p}$. □

**Example 4.1.13.** Generation of $\widehat{F_{(p)}}$ is easy. Let $F = \langle a, b \rangle$. Then

$$\begin{array}{ccc} \widehat{F_{(p)}} & \longrightarrow & \widehat{F_{(p)}}/\Phi = \mathbb{F}_p^2 \\ a & \longmapsto & (1,0) \\ b & \longmapsto & (0,1) \end{array}.$$

**Corollary 4.1.14.** *Let $f : G \to H$ be a continuous homomorphism of topologically finitely generated pro-$p$ groups. Then $f(\Phi(G)) \leq \Phi(H)$. So $f$ induces a map*

$$f_* : G/\Phi(G) \to H/\Phi(H),$$

*and $f$ is surjective if and only if $f_*$ is surjective.*

*Proof.* $f([g_1, g_2] g_3^p) = [f(g_1), f(g_2)] f(g_3)^p \in \Phi(H)$ for all $g_1, g_2, g_3 \in G$. Then $f([G,G]\,G^p) \leq \Phi(H)$, so $f(\Phi(G)) = f\left(\overline{[G,G]\,G^p}\right) \leq \Phi(H)$. If $f_*$ is surjective, then the image of $f(G)$ in $H/\Phi(H)$ generates $H/\Phi(H)$, so $f(G)$ topologically generates $H$. So $f(G) = H$. □

## 4.2 Nilpotent groups

Lecture 15
Tuesday
23/02/21

**Definition 4.2.1.** The **lower central series** of a group $G$ to be the sequence $G_n = \gamma_n(G)$ defined by

$$G_1 = G, \qquad G_{n+1} = [G, G_n], \qquad G_{n+1} \leq G_n.$$

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

The following are properties.

**Proposition 4.2.2.** *$\gamma_n(G)$ is **fully characteristic**, so if $f : G \to H$ then $f(\gamma_n(G)) \leq \gamma_n(H)$. If $f$ is surjective, we have equality.*

**Proposition 4.2.3.** *Subgroups and quotients of nilpotent groups are nilpotent.*

**Proposition 4.2.4.** *Finite $p$-groups $G$ are nilpotent.*

*Proof.* Proof by induction on $|G|$.

Base case. $\gamma_2(\mathbb{F}_p) = 1$.

Inductive step. There exists $z \in \mathrm{Z}(G) \setminus \{1\}$. Then $G/\langle z \rangle$ is nilpotent, so $\gamma_{c+1}(G/\langle z \rangle) = 1$ for some $c$. Thus $\gamma_{c+1}(G) \leq \langle z \rangle$, so $\gamma_{c+2}(G) = [G, \gamma_{c+1}(G)] = 1$.

□

The following is a variant. For pro-$p$ groups, the **lower central $p$-series** is

$$\gamma_1^{(p)}(G) = G, \qquad \gamma_{n+1}^{(p)}(G) = \overline{\left[G, \gamma_n^{(p)}(G)\right] \left(\gamma_n^{(p)}(G)\right)^p},$$

so $\gamma_2^{(p)}(G) = \Phi(G)$. Then $\gamma_n^{(p)}(G)$ is open for topologically finitely generated pro-$p$ groups, since by induction, $\gamma_{n+1}^{(p)}(G) \geq \Phi\left(\gamma_n^{(p)}(G)\right)$.

**Proposition 4.2.5.** *Let $G$ be a $p$-group. Then $\gamma_n^{(p)}(G) = 1$ for some $n$.*

**Proposition 4.2.6.** *Let $G$ be a topologically finitely generated pro-$p$ group, then $\left\{\gamma_n^{(p)}(G)\right\}$ are a basis of open normal subgroups of $G$.*

*Proof.* If $N \lhd_{\mathrm{o}} G$, then $G/N$ is a $p$-group, so $\gamma_n^{(p)}(G/N) = 1$. Thus $N \geq \gamma_n^{(p)}(G)$. □

## 4.3 Invariance of topology

**Theorem 4.3.1** (Serre)**.** *Let $G$ be a topologically finitely generated pro-$p$ group. Then all finite index subgroups are open.*

Thus

- every homomorphism to a finite group is continuous,
- by Proposition 1.2.14 every homomorphism to a profinite group is continuous, and
- no other topology on $G$ makes it a profinite group, by applying Theorem 4.3.1 to $\mathrm{id} : G \to G$.

**Proposition 4.3.2.** *Let $G$ be a pro-$p$ group and let $K \leq_{\mathrm{f}} G$. Then $[G : K]$ is a power of $p$.*

*Proof.* Without loss of generality $K$ is normal. Let $[G : K] = m = p^r m'$ for $m'$ coprime to $p$. Let

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

Then $X$ is closed, since it is the image of $G$ under $g \mapsto g^m$. Thus $X = \overline{X} = \bigcap_{N \lhd_{\mathrm{o}} G} XN$, by Proposition 1.2.21. Let $g \in G$. We will show $g^{p^r} \in K$ for all $g \in G$. This implies the result by Cauchy's theorem. Let $N \lhd_{\mathrm{o}} G$. Let $[G : N] = p^s$. Let $t = \max(r, s)$. Then $g^{p^t} \in N$ and $\gcd(p^t, m) = p^r$. So there exist $a, b \in \mathbb{Z}$ such that $p^r = ma + p^t b$. Then $g^{p^r} = (g^a)^m \left(g^{p^t}\right)^b \in XN$. □

**Lemma 4.3.3.** *Let $G$ be a nilpotent group with a finite generating set $a_1, \dots, a_d$. Then every $g \in [G,G]$ may be written*

$$g = [a_1, x_1] \dots [a_d, x_d], \qquad x_1, \dots, x_d \in G.$$

*Proof.* We induct on the nilpotency class $c$ of $G$.

Base case. If $c = 1$, then $1 = \gamma_2(G) = [G,G]$, so $G$ is abelian, which is trivial.

Inductive step. The result is true for $G/\gamma_c(G)$. So there exist $x_1, \dots, x_d \in G$ and $u \in \gamma_c(G) = [G, \gamma_{c-1}(G)]$ such that

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

Seek a nice form of $u$. There are commutator relations

$$[xy, z] = [x,z]^y [y,z], \qquad [x, yz] = [x,z][x,y]^z.$$

For any $v \in \gamma_{c-1}(G)$, these imply that

$$[a_i a_j, v] = [a_i, v][a_j, v], \qquad [a_i, v]^2 = \left[a_i, v^2\right],$$

$$\left[a_i^{-1}, v\right] = [a_i, v]^{-1} = \left[a_i, v^{-1}\right], \qquad [a_i, v][a_i, w] = [a_i, vw],$$

since $[\cdot, v] \in \gamma_c(G)$ is central in $G$. We can write $u$ in the form

$$u = [a_1, v_1] \dots [a_d, v_d], \qquad v_i \in \gamma_{c-1}(G).$$

Finally,

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

□

**Proposition 4.3.4.** *If $G$ is a topologically finitely generated pro-p group, then $[G,G]\,G^p$ is open and closed, and equals $\Phi(G)$.*

*Proof.* Let

$$G^{\{p\}} = \{g^p \mid g \in G\} \subseteq G^p.$$

Then $G/[G,G]$ is abelian, and in abelian groups we have $g^p h^p = (gh)^p$, so $g^p h^p (gh)^{-p} \in [G,G]$, so $[G,G]\,G^p = [G,G]\,G^{\{p\}}$. Claim that $[G,G]$ is closed. Let $a_1, \dots, a_d$ be a topological generating set of $G$. Let

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

Then $X$ is closed, since it is the image of a continuous map $G^d \to G$. So $X = \overline{X} = \bigcap_{N \lhd_o G} XN$. We show $X = [G,G]$. Let $g \in [G,G]$. For any $N \lhd_o G$, $gN \in [G/N, G/N]$. Since $G/N$ is nilpotent,

$$gN = [a_1 N, x_1 N] \dots [a_d N, x_d N], \qquad x_i N \in G/N.$$

Then $g \in XN$ for all $N \lhd_o G$, so $g \in \bigcap_N XN = \overline{X} = X$. Thus $[G,G]\,G^{\{p\}}$ is the image of $[G,G] \times G$ under the continuous function

$$\begin{array}{ccc} [G,G] \times G & \longrightarrow & G \\ (x, g) & \longmapsto & xg^p \end{array},$$

so $[G,G]\,G^{\{p\}}$ is closed. □

*Proof of Theorem 4.3.1.* Proof by contradiction. Suppose $G$ is topologically finitely generated pro-$p$ and $K$ is finite index but not open, such that $[G:K]$ is as small as possible. Without loss of generality $K$ is normal. Consider

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

Then $G/K$ is a non-trivial $p$-group. So the image of $M$ is $\Phi(G/K) = [G/K, G/K]\,(G/K)^p < G/K$. So $M$ is proper in $G$, so $M = K$, otherwise $K <_o M <_o G$. Hence $\Phi(G) \leq K$ is open, so $K$ is open. □

## 4.4 Hensel's lemma and $p$-adic arithmetic

Lecture 16
Thursday
25/02/21

Previously, there exists $x$ such that $\alpha x = 1$ if and only if $\alpha \not\equiv 0 \mod p$.

**Lemma 4.4.1.** *Let $f(X)$ be a polynomial with coefficients in $\mathbb{Z}_p$. Then $f$ has a root in $\mathbb{Z}_p$ if and only if $f$ has a root modulo $p^k$ for all $k$.*

**Example 4.4.2.** Hensel lifting. Let $p = 7$. Then $3^2 = 9 \equiv 2 \mod 7$, so $X^2 - 2$ has a root modulo 7. To get a root modulo 49, consider $3 + 7a$ for $0 \leq a \leq p - 1 = 6$. Then

$$(3 + 7a)^2 = 3^2 + 7(6a) + 49a^2 \equiv 2 + 7(1 + 6a) \mod 49.$$

Choose the unique $a$ such that $1 + 6a \equiv 0 \mod 7$, so $a = 1$. Then $3 + 7(1) = 10$ is a root of $X^2 - 2 \mod 49$, and $10^2 = 49(2) + 2$. Now we can repeat. To solve modulo $7^3$,

$$(10 + 49a)^2 = 10^2 + 49(20a) + 49^2a^2 \equiv 2 + 49(2 + 20a) \mod 7^3,$$

and solve for $a = 2$.

**Proposition 4.4.3** (Hensel's lemma for square roots)**.** *Let $p \neq 2$ be prime. Suppose $\lambda \in \mathbb{Z}_p$ is congruent to a non-zero square $r_1^2 \mod p$, where $r_1 \in \mathbb{Z}$. Then there is a unique $\rho \in \mathbb{Z}_p$ such that $\rho^2 = \lambda$ and $\rho \equiv r_1 \mod p$.*

*Proof.* Construct elements $r_k \in \mathbb{Z}$, unique modulo $p^k$, such that $r_k^2 \equiv \lambda \mod p^k$ and $r_{k+1} \equiv r_k \mod p^k$. Then $(r_k)$ is Cauchy, so there exists $\rho \in \mathbb{Z}_p$ such that $r_k \to \rho$ and $\rho^2 = \lambda$.

- $r_1$ is given.
- Suppose we have $r_k$. Consider $r_k + p^k a$ for $0 \leq a \leq p - 1$. We have $r_k^2 = \lambda + p^k b_k$ for $b_k \in \mathbb{Z}_p$. Then

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

  Now $2r_k \equiv 2r_1 \not\equiv 0 \mod p$, so we can solve $b_k + 2r_k a \equiv 0 \mod p$ and find $a_k$ such that $\left(r_k + p^k a_k\right)^2 \equiv \lambda \mod p^{k+1}$. Set $r_{k+1} = r_k + p^k a_k$.

□

**Proposition 4.4.4** (Hensel's lemma)**.** *Let $f(x)$ be a polynomial with coefficients in $\mathbb{Z}_p$. Let $r \in \mathbb{Z}_p$ such that $f(r) \equiv 0 \mod p^k$ for some $k$ and $f'(r) \not\equiv 0 \mod p$, where $f' : \sum_n a_n x^n \mapsto \sum_n n a_n x^{n-1}$ is the formal derivative, and $f'(r)$ only depends on $r \mod p$. There there exists a unique $\rho \in \mathbb{Z}_p$ such that $f(\rho) = 0$ and $\rho \equiv r \mod p^k$.*

**Lemma 4.4.5.** *For $r, a \in \mathbb{Z}_p$ and $k \geq 1$ we have*

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

*Proof.* It suffices to do $f(x) = x^r$. Then

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

and $p^{k+1} \mid p^{2k} \mid p^{ki}$. □

*Proof of Proposition 4.4.4.* Construct $r_k$ for $k \geq K$, such that $f(r_k) \equiv 0 \mod p^k$ and $r_{k+1} \equiv r_k \mod p^k$, and $r_{k+1}$ will be unique modulo $p^{k+1}$ with these properties. Then $(r_k)$ is Cauchy and $r_k \to \rho$, so $f(\rho) = 0$.

- $r_K$ is given.
- If $r_k$ is constructed, consider $r_k + p^k a$ for $0 \leq a \leq p - 1$. We have $f(r_k) = b_k p^k$ for some $b_k \in \mathbb{Z}_p$. Now

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

  Can solve $b_k + a f'(r_k) \equiv 0 \mod p$ since $f'(r_k) \equiv f'(r) \not\equiv 0 \mod 0$ is invertible modulo $p$. So set $a_k$ such that $b_k + a f'(r_k) \equiv 0 \mod p$ and set $r_{k+1} = r_k + p^k a_k$.

□

We can also do Hensel-type things in $\mathrm{GL}_N \mathbb{Z}_p$.

**Definition 4.4.6.** Let

$$\mathrm{GL}_N^{(k)} \mathbb{Z}_p = \ker\left(\mathrm{GL}_N \mathbb{Z}_p \to \mathrm{GL}_N\left(\mathbb{Z}/p^k\mathbb{Z}\right)\right) = \left\{\mathrm{I} + p^k A \;\middle|\; A \in \mathrm{Mat}_{N\times N} \mathbb{Z}_p\right\},$$

$$\mathrm{SL}_N^{(k)} \mathbb{Z}_p = \ker\left(\mathrm{SL}_N \mathbb{Z}_p \to \mathrm{SL}_N\left(\mathbb{Z}/p^k\mathbb{Z}\right)\right).$$

**Proposition 4.4.7.** *$\mathrm{GL}_N^{(1)} \mathbb{Z}_p$ and $\mathrm{SL}_N^{(1)} \mathbb{Z}_p$ are pro-$p$ groups.*

*Proof.* $\mathrm{SL}_N^{(1)} \mathbb{Z}_p \leq \mathrm{GL}_N^{(1)} \mathbb{Z}_p = \varprojlim_m \mathrm{GL}_N^{(1)}\left(\mathbb{Z}/p^m\mathbb{Z}\right)$ and $\left|\mathrm{GL}_N^{(1)}\left(\mathbb{Z}/p^m\mathbb{Z}\right)\right| = p^{(m-1)N^2}$. □

**Remark 4.4.8.** $\mathrm{GL}_N \mathbb{Z}_p$ and $\mathrm{SL}_N \mathbb{Z}_p$ are not pro-$p$ groups, since $\mathrm{SL}_N\left(\mathbb{Z}/p\mathbb{Z}\right)$ is not a $p$-group.

**Proposition 4.4.9.** *Let $p \neq 2$. The continuous function*

$$\begin{array}{ccc} \mathrm{GL}_N^{(k)} \mathbb{Z}_p & \longrightarrow & \mathrm{GL}_N^{(k+1)} \mathbb{Z}_p \\ A & \longmapsto & A^p \end{array}$$

*maps surjectively for $k \geq 1$. Also for $\mathrm{SL}_N^{(k)} \mathbb{Z}_p \twoheadrightarrow \mathrm{SL}_N^{(k+1)} \mathbb{Z}_p$.*

*Proof.* For $r \geq 1$ and $A$ a matrix over $\mathbb{Z}_p$, we have

$$\left(\mathrm{I} + p^r A\right)^p = \mathrm{I} + p^{r+1}A + \sum_{l=2}^{p} p^{rl}\binom{p}{p-l} A^l = \mathrm{I} + p^{r+1}A + p^{r+2}B,$$

for some $B$ which commutes with $A$, unless $p = 2$, $l = 2$, and $r = 1$. Let $\mathrm{I} + p^{k+1}A \in \mathrm{GL}_N^{(k+1)} \mathbb{Z}_p$. We show the following inductive statement for $n \geq 1$. There exist $B_n$ and $E_n$, which are polynomials in $A$, hence commute with $A$ and each other, such that

$$B_{n+1} \equiv B_n \mod p^n, \qquad \left(\mathrm{I} + p^k B_n\right)^p = \mathrm{I} + p^{k+1}A + p^{k+n+1}E_n.$$

Then $(B_n)$ is Cauchy so $B_n \to B_\infty \in \mathrm{Mat}_{N\times N} \mathbb{Z}_p$, and $\left(\mathrm{I} + p^k B_\infty\right)^p = \mathrm{I} + p^{k+1}A$.

- Start with $B_1 = A$. Then
$$\left(\mathrm{I} + p^k A\right)^p = \mathrm{I} + p^{k+1}A + p^{k+2}E_1.$$
- Assume $B_n$ and $E_n$ are given. Set $B_{n+1} = B_n - p^n E_n$. Then
$$\begin{aligned}\left(\mathrm{I} + p^k B_{n+1}\right)^p &= \left(\mathrm{I} + p^k B_n - p^{k+n}E_n\right)^p = \left(\mathrm{I} + p^k B_n\right)^p - p\left(\mathrm{I} + p^k B_n\right)^{p-1} p^{k+n}E_n + \dots \\ &= \mathrm{I} + p^{k+1}A + p^{k+n+1}E_n - p^{k+n+1}E_n + \dots = \mathrm{I} + p^{k+1}A + p^{k+n+2}E_{n+1}.\end{aligned}$$

□

**Proposition 4.4.10.**

$$\Phi\left(\mathrm{GL}_N^{(k)} \mathbb{Z}_p\right) = \mathrm{GL}_N^{(k+1)} \mathbb{Z}_p, \qquad \mathrm{GL}_N^{(k)} \mathbb{Z}_p / \mathrm{GL}_N^{(k+1)} \mathbb{Z}_p \cong \mathbb{F}_p^{N^2},$$

*a **uniform pro-$p$ group**, with isomorphisms*

$$\begin{array}{ccc} \mathrm{GL}_N^{(k)} \mathbb{Z}_p / \mathrm{GL}_N^{(k+1)} \mathbb{Z}_p & \longrightarrow & \mathrm{GL}_N^{(k+1)} \mathbb{Z}_p / \mathrm{GL}_N^{(k+2)} \mathbb{Z}_p \\ x & \longmapsto & x^p \end{array}.$$

**Theorem 4.4.11.** *Let $H$ be any closed subgroup of $\mathrm{GL}_N^{(1)} \mathbb{Z}_p$. Then $\mathrm{d}(H) \leq N^2$.*

Compare to a free group as a subgroup of $\mathrm{SL}_2 \mathbb{Z}$.

**Theorem 4.4.12.** *If $G$ is a pro-$p$ group, such that $\mathrm{d}(H) \leq R$ for all $H \leq_{\mathrm{c}} G$. Then*

$$G/\mathbb{Z}_p^a \hookrightarrow \mathrm{GL}_R \mathbb{Z}_p \times F,$$

*where $F$ is finite.*

# 5 Cohomology of groups

Lecture 17
Saturday
27/02/21

In the homology of spaces, a simplicial complex $X$ gives a family of abelian groups $\mathrm{H}_n(X)$ with $\mathbb{Z}$ coefficients. In the cohomology of groups, a group $G$ gives a family of abelian groups $\mathrm{H}^n(G;M)$ with $M$ coefficients.

## 5.1 Group rings and chain complexes

Let $G$ be an abstract group.

**Definition 5.1.1.** The **group ring** of $G$ is a ring $\mathbb{Z}G$ defined as follows. The additive group of $\mathbb{Z}G$ is the free abelian group with basis $\{g \mid g \in G\}$, so an element is a finite formal sum $\sum_{g\in G} n_g g$ for $n_g \in \mathbb{Z}$. The ring multiplication is defined on the basis by $g \cdot h = gh$ and extended bilinearly.

Thus $\mathbb{Z}G$ is non-commutative unless $G$ is abelian, and has an identity $e$, the multiplicative identity in $\mathbb{Z}[G]$, usually called 1.

**Example 5.1.2.** If $e$ is the identity of $G$, then $(e+g)(e-2h) = e+g-2h-2gh$.

**Definition 5.1.3.** A **left $G$-module**, or **$\mathbb{Z}G$-module**, is an abelian group $M$ equipped with a $G$-action, a function

$$\begin{array}{ccc} \mathbb{Z}G \times M & \longrightarrow & M \\ (r,m) & \longmapsto & r\cdot m \end{array},$$

such that for all $r_1, r_2 \in \mathbb{Z}G$ and for all $m_1, m_2 \in M$,

$$r_1\cdot(m_1+m_2) = r_1\cdot m_1 + r_1\cdot m_2, \qquad (r_1+r_2)\cdot m_1 = r_1\cdot m_1 + r_2\cdot m_1, \qquad (r_1r_2)\cdot m_1 = r_1\cdot(r_2\cdot m).$$

A **trivial module**, or a **module with trivial $G$-action**, is a module such that $g\cdot m = m$ for all $g \in G$ and for all $m \in M$.

**Definition 5.1.4.** Let $M_1$ and $M_2$ be $G$-modules. A **morphism of $G$-modules**, or **$G$-linear map**, is an abelian group homomorphism $\alpha : M_1 \to M_2$ such that $\alpha(r\cdot m) = r\cdot\alpha(m)$ for all $r \in \mathbb{Z}G$ and $m \in M$.

Note that only need to check this for basis elements $r = g$.

**Definition 5.1.5.** Let $M$ and $N$ be $G$-modules. Define the **Hom-group**

$$\mathrm{Hom}_G(M,N) = \{G\text{-linear maps } \alpha : M \to N\},$$

with abelian group structure $(\alpha+\beta)(m) = \alpha(m)+\beta(m)$. If $\mathrm{Hom}(M,N)$, this means $\mathrm{Hom}_1(M,N)$, the abelian group homomorphisms.

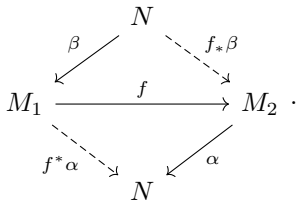
**Definition 5.1.6.** If $f : M_1 \to M_2$ is a morphism of $G$-modules then we have a **dual map**

$$\begin{array}{rcccc} f^* & : & \mathrm{Hom}_G(M_2,N) & \longrightarrow & \mathrm{Hom}_G(M_1,N) \\ & & \alpha & \longmapsto & \alpha\circ f \end{array}.$$

Also, we have an **induced map**

$$\begin{array}{rcccc} f_* & : & \mathrm{Hom}_G(N,M_1) & \longrightarrow & \mathrm{Hom}_G(N,M_2) \\ & & \beta & \longmapsto & f\circ\beta \end{array}.$$

Thus



Submodules and quotients are the obvious things.

**Definition 5.1.7.** Let $M$ be a $G$-module. Then a **$G$-submodule** is a subgroup $N \leq M$ such that $g \cdot n \in N$ for all $g \in G$ and $n \in N$. If $N$ is a submodule, we have a **quotient module** $M/N$, the abelian group $M/N$, with the $G$-action $g \cdot (m + N) = g \cdot m + N$.

**Definition 5.1.8.** A **chain complex of $G$-modules** $(M_n) = (M_n, d_n)_{t \leq n \leq s}$ is a sequence of $G$-modules

$$M_s \xrightarrow{d_s} M_{s-1} \to \cdots \to M_{t+1} \xrightarrow{d_{t+1}} M_t,$$

where $s = \infty$ or $t = -\infty$ are possible, such that $d_n \circ d_{n+1} = 0$, so $\operatorname{im} d_{n+1} \leq \ker d_n$. 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 chain complex is the family of $G$-modules

$$\mathrm{H}_n(M_\bullet) = \begin{cases} \ker d_s & n = s \\ \ker d_n / \operatorname{im} d_{n+1} & t < n < s \\ M_t / \operatorname{im} d_{t+1} & n = t \end{cases}.$$

**Example 5.1.9.**

- The complex
$$0 \to M_1 \xrightarrow{\alpha} M_2$$
is exact if and only if $\alpha$ is injective.
- The complex
$$M_1 \xrightarrow{\alpha} M_2 \to 0$$
is exact if and only if $\alpha$ is surjective.
- A **short exact sequence** is an exact sequence
$$0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0,$$
that is $\alpha$ is injective, $\beta$ is surjective, and $\ker \beta = \operatorname{im} \alpha$, such as
$$0 \to N \to M \to M/N \to 0.$$

**Definition 5.1.10.** Given a set $X$, the **free $\mathbb{Z}G$-module on** $X$, denoted $\mathbb{Z}G\{X\}$, is set of finite formal sums $\sum_{x \in X} r_x x$ for $r_x \in \mathbb{Z}G$. The $G$-action is the obvious one $g \cdot (\sum_x r_x x) = \sum_x (g r_x) x$.

If $X$ is finite, $\mathbb{Z}G\{X\} \cong (\mathbb{Z}G)^{|X|}$.

**Definition 5.1.11.** A $G$-module $P$ is **projective** if, for every surjective $G$-linear map $\alpha : M_1 \twoheadrightarrow M_2$ and every $G$-linear $\beta : P \to M_2$ there exists a $G$-linear $\overline{\beta} : P \to M_1$ such that $\alpha \circ \overline{\beta} = \beta$, so

$$\begin{array}{ccccc} & & & & P \\ & & \overset{\overline{\beta}}{\swarrow} & & \downarrow \beta \\ M_1 & \xrightarrow[\alpha]{} & \twoheadrightarrow & M_2 & \longrightarrow 0 \end{array}.$$

**Proposition 5.1.12.** *Free modules are projective.*

*Proof.* Let $\mathbb{Z}G\{X\}$ be a free module and take $\alpha : M_1 \twoheadrightarrow M_2$ and $\beta : \mathbb{Z}G\{X\} \to M_2$. For each $x \in X$ choose $m_x \in M_1$ such that $\alpha(m_x) = \beta(x)$, since $\alpha$ is surjective. Define

$$\begin{array}{rccc} \overline{\beta} & : & \mathbb{Z}G\{X\} & \longrightarrow & M_1 \\ & & x & \longmapsto & m_x \end{array},$$

and extend linearly, so $\overline{\beta}\left(\sum_{x \in X} r_x x\right) = \sum_{x \in X} r_x m_x$. □

**Definition 5.1.13.** A **projective resolution of $\mathbb{Z}$ by $\mathbb{Z}G$-modules** is an exact sequence

$$\ldots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} \mathbb{Z} \to 0,$$

where each $F_n$ is projective, and $\mathbb{Z}$ has trivial $G$-action.

**Definition 5.1.14.** Take a projective resolution as above. Let $M$ be a $G$-module. Apply the functor $\mathrm{Hom}_G(-, M)$ to get a sequence

$$\ldots \xleftarrow{d^2 = d_2^*} \mathrm{Hom}_G(F_1, M) \xleftarrow{d^1 = d_1^*} \mathrm{Hom}_G(F_0, M),$$

where $d^n = d_n^*$ is the dual map, so $C_n = \mathrm{Hom}_G(F_{-n}, M)$ for $n \leq 0$ is a chain complex. The **$n$-th cohomology group of $G$ with coefficients in $M$** is

$$\mathrm{H}^n(G, M) = \begin{cases} \ker d^1 & n = 0 \\ \ker d^{n+1} / \operatorname{im} d^n & n > 0 \end{cases}.$$

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

Where do these come from? From topology.