

# Profinite Groups and Group Cohomology

Lectured by Dr Gareth Wilkes  
Typed by David Kurniadi Angdinata

Lent 2020

**Syllabus**

# Contents

<b>0</b>	<b>Introduction</b>	<b>3</b>
<b>1</b>	<b>Inverse limits</b>	<b>4</b>
1.1	Categories and limits . . . . .	4
1.2	Inverse limits and profinite groups . . . . .	7
1.3	Change of inverse system . . . . .	10
<b>2</b>	<b>Profinite groups</b>	<b>12</b>
2.1	The $p$ -adic integers . . . . .	12
2.2	The profinite completion of the integers . . . . .	13
2.3	Profinite matrix groups . . . . .	14
2.4	Subgroups, quotients, and homomorphisms . . . . .	15
2.5	Generators of profinite groups . . . . .	17
<b>3</b>	<b>Profinite completions</b>	<b>19</b>
3.1	Residual finiteness . . . . .	19
3.2	Finite quotients of free groups . . . . .	25
<b>4</b>	<b>Pro-<math>p</math> groups</b>	<b>30</b>
4.1	Generators of pro- $p$ groups . . . . .	30
4.2	Nilpotent groups . . . . .	32
4.3	Invariance of topology . . . . .	32
4.4	Hensel's lemma and $p$ -adic arithmetic . . . . .	34
<b>5</b>	<b>Cohomology of groups</b>	<b>36</b>
5.1	Group rings and chain complexes . . . . .	36
5.2	Different projective resolutions . . . . .	41
5.3	Cohomology and group extensions . . . . .	45
5.3.1	Worked example: extensions of $\mathbb{Z}^2$ by $\mathbb{Z}$ . . . . .	47
5.4	Cohomology of profinite groups . . . . .	49
5.4.1	Pro- $p$ groups of cohomological dimension one . . . . .	49
5.4.2	Presentations of pro- $p$ groups . . . . .	53

## 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  $\text{Gal}(K/\mathbb{Q})$ .
- For a topological space  $X$ , compactness, connectedness, simplicial homology groups  $H_\bullet(X)$ , 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

$$\text{Gal}(K/K_N) \rightarrow \text{Gal}(K/\mathbb{Q}) \twoheadrightarrow \text{Gal}(K_N/\mathbb{Q}).$$

$$\text{Then } \text{Gal}(K_N/\mathbb{Q}) = (\mathbb{Z}/p^N\mathbb{Z})^\times \text{ and } \text{Gal}(K/\mathbb{Q}) = \varprojlim_N (\mathbb{Z}/p^N\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

- 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  $j_A : A \rightarrow Z$  and  $j_B : B \rightarrow Z$  there is a unique function defined by

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

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

$$\begin{array}{ccccc} A & \xrightarrow{i_A} & A \sqcup B & \xleftarrow{i_B} & B \\ & \searrow j_A & \downarrow \exists! f & \swarrow j_B & \\ & & Z & & \end{array} .$$

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

$$\begin{array}{ccccc} A & \xleftarrow{p_A} & A \times B & \xrightarrow{p_B} & B \\ & \swarrow q_A & \uparrow \exists! f & \searrow q_B & \\ & & Z & & \end{array} ,$$

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

$$\begin{array}{ccccc} A & \longrightarrow & A * B & \longleftarrow & B \\ & \searrow & \downarrow & \swarrow & \\ & & Z & & \end{array} .$$

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

$$\begin{array}{ccccc} C & \xrightarrow{\phi_A} & A & & \\ \phi_B \downarrow & & \downarrow i_A & \searrow j_A & \\ B & \xrightarrow{i_B} & A \sqcup_C B & \xrightarrow{\exists! f} & Z \\ & \searrow j_B & & & \end{array} .$$

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

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

such that

- if  $f : X \rightarrow Y$ , then  $\text{id}_Y \circ f = f = f \circ \text{id}_X$ , and
- if  $f : W \rightarrow X$ ,  $g : X \rightarrow Y$ , and  $h : Y \rightarrow Z$ , 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 **Grp<sub>fin</sub>**, objects are finite groups.
- In **Grp<sub>inj</sub>**, 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  $\text{Obj } \mathcal{J} = J$  and morphisms  $\text{Mor } \mathcal{J} = \{i \rightarrow j \mid i \leq j\}$ .

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

$$\begin{array}{ccc} & Z & \\ q_A \swarrow & \downarrow \exists! f & \searrow q_B \\ A & \xleftarrow{p_A} P \xrightarrow{p_B} & B \end{array} \quad .$$

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

**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

$$\begin{array}{ccccc} & & P' & & \\ p'_A \swarrow & & \downarrow \exists! f & & \searrow p'_B \\ A & & & & B \\ p_A \swarrow & & \downarrow \exists! g & & \searrow p_B \\ & & P & & \end{array} \quad .$$

Consider  $f \circ g : P \rightarrow P$ . 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,  $f \circ g = \text{id}_P$ . Similarly,  $g \circ f = \text{id}_{P'}$ .  $\square$

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

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

$$\begin{array}{ccccc} A & \xrightarrow{i_A} & A \sqcup B & \xleftarrow{i_B} & B \\ & \searrow j_A & \downarrow \exists! f & \swarrow j_B & \\ & & Z & & \end{array} \quad .$$

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

Lecture 2  
Saturday  
23/01/21

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

- $F(\text{id}_X) = \text{id}_{F(X)}$ , 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  $X : \mathcal{J} \rightarrow \mathcal{C}$ . Often write  $X(j) = X_j$ , for  $j \in \text{Obj } \mathcal{J}$ .

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

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

$$\begin{array}{ccc} & Z & \\ p_i \swarrow & & \searrow p_j \\ X_i & \xrightarrow{X(f)} & X_j \end{array} .$$

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

$$\begin{array}{ccc} & Z & \\ q_i \swarrow & \downarrow \exists! g & \searrow q_j \\ & L & \\ p_i \swarrow & & \searrow p_j \\ X_i & \xrightarrow{X(f)} & X_j \end{array} ,$$

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

**Example 1.1.12.**

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

$$\bullet \quad \bullet,$$

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

$$\begin{array}{c} \bullet \longrightarrow \bullet \\ \downarrow \\ \bullet \end{array} ,$$

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

$$\begin{array}{ccc} C & \xrightarrow{\phi_{CA}} & A \\ \phi_{CB} \downarrow & & \\ B & & \end{array} .$$

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  $\{N \triangleleft_f G\}$ , where  $N \triangleleft_f G$  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**,

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

If  $N_1 \leq N_2$ , then  $X(N_1 \rightarrow N_2)$  is the quotient map  $\phi_{N_1 N_2} : G/N_1 \rightarrow G/N_2$ , 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**  $p_N : \widehat{G} \rightarrow G/N$  for all  $N \triangleleft_f G$  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  $q_N : Z \rightarrow G/N$  such that  $\phi_{N_1 N_2} \circ q_{N_1} = q_{N_2}$ , there exists a unique  $f : Z \rightarrow \widehat{G}$  such that  $p_N \circ f = q_N$  for all  $N$ .

Thus

$$\begin{array}{ccc} & Z & \\ & \downarrow \exists! f & \\ & \widehat{G} & \\ \swarrow & & \searrow \\ G/N_1 & \xrightarrow{\quad} & G/N_2 \end{array}$$

In particular,  $Z = G$  works, so there is a unique morphism  $\iota_G : G \rightarrow \widehat{G}$ , 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  $G : \mathcal{J} \rightarrow \mathbf{Grp}$ . Thus an inverse system is a group  $G_j$  for all  $j \in J$  and transition maps  $\phi_{ij} : G_i \rightarrow G_j$  if  $i \leq j$  such that  $\phi_{ii} = \text{id}$  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  $(G_j)_{j \in J}$  be an inverse system of groups. Then the inverse limit exists, and is given by the explicit description

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

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

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

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

$$\begin{array}{ccc} & Z & \\ & \downarrow \exists! f & \\ & \varprojlim_j G_j & \\ \swarrow & & \searrow \\ G_i & \xrightarrow{\quad} & G_j \end{array}$$

$\begin{array}{cc} q_i & q_j \\ p_i & p_j \end{array}$

□

**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  $\varprojlim_j G_j \subseteq \prod_j G_j$  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  $\prod_{j \in J} G_j \rightarrow G_i \times G_j$ , so  $\varprojlim_j G_j$  is closed in  $\prod_j G_j$ .  $\square$

**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

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

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  $Y_{I_1} \cap \dots \cap Y_{I_n} \supseteq Y_{I_1 \cup \dots \cup I_n} \neq \emptyset$ . 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.  $\square$

**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

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

Define

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

We need to show this gives the product topology. Let  $f : (X, \tau_{\text{product}}) \rightarrow (X, d)$  be the identity function. A basis for the metric topology are open balls  $B(x, 1/3^n)$  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

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

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

**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  $G \rightarrow \text{Sym } n$ , since by labelling cosets  $H, \dots, g_n H$  by symbols  $1, \dots, n$ ,  $G$  permutes these right cosets by  $g \cdot g_i H = (gg_i) H$  and  $H$  is recovered from this as  $\text{Stab } 1$ . So there are at most as many subgroups  $H$  as homomorphisms to  $\text{Sym } n$ , and there are only finitely many.  $\square$

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



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

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

*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  $f : G \rightarrow H$  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  $p_j : G \rightarrow G_j$  be the projection maps. A homomorphism  $f : H \rightarrow G$  is continuous if and only if each map  $f_j = p_j \circ f$  is continuous.*

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

**Proposition 1.2.15.** *Let  $f : H \rightarrow G_j$  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.  $\square$

**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  $U_j = \ker(p_j : G \rightarrow G_j)$  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  $V \supseteq U_k$ .  $\square$

**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.  $\square$

**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  $p_j(X) = p_j(G)$ .  $\square$

**Corollary 1.2.20.** *Let  $Y$  be a compact topological space and let  $f : Y \rightarrow G$  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.  $\square$

Lecture 4  
Thursday  
28/01/21

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

$$\overline{X} = \bigcap_{N \leq_o G} XN,$$

where  $N \leq_o G$  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  $N \leq_o G$ , so  $\overline{X} \subseteq \bigcap_{N \leq_o G} XN$ . 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  $\bigcap_N XN \subseteq \overline{X}$ .  $\square$

**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  $G \rightarrow G/U$  are a cone on the inverse system, so we get a well-defined homomorphism  $f : G \rightarrow \varprojlim_U G/U$ . Then

- $f$  is continuous, since compositions with projection maps are continuous,
- $f$  is surjective, since  $G \rightarrow G/U$  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  $g \notin \ker(G \rightarrow G/U)$ , so  $g \notin \ker f$ .

$\square$

### 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  $\prod_{j \in J} G_j \rightarrow \prod_{i \in I} G_i$  is a continuous homomorphism, and it restricts to  $f : G \rightarrow H$ . 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  $i \in I$ .

$\square$

**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  $p_j : \varprojlim_j X_j \rightarrow X_j$  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  $(G'_j)_{j \in J}$  such that  $G'_j \leq G_j$ , with surjective transition maps, such that  $\varprojlim_j G_j = \varprojlim_j G'_j$ .

*Proof.* Let  $p_j : G = \varprojlim_j G_j \rightarrow G_j$  be the projection. Define  $G'_j = p_j(G)$ . Since  $\phi_{ij} \circ p_i = p_j$ ,  $(G'_j)$  is an inverse system with  $\phi_{ij}|_{G'_i} : G'_i \rightarrow G'_j$ , 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  $\varprojlim_j G'_j = G$ .  $\square$

**Definition 1.3.7.** An inverse system  $(J, \leq)$  is **linearly ordered** if there exists a bijection  $f : J \rightarrow \mathbb{N}$  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

Let  $p$  be a prime. Consider

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

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  $a_n \equiv a_m \pmod{p^m}$  whenever  $n \geq m$ , since  $\mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^m\mathbb{Z}$ , and

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

Given  $a \in \mathbb{Z}$ , setting  $a_n = a \pmod{p^n}$  gives an element  $\iota(a) \in \mathbb{Z}_p$  for  $\iota : \mathbb{Z} \rightarrow \mathbb{Z}_p$ . Then  $\iota$  is injective, since if  $a \in \mathbb{Z}$ , and  $p^n > |a|$  then  $a \not\equiv 0 \pmod{p^n}$ , 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  $d(\alpha, \beta) = 0$ . If  $\alpha \neq \beta$ , take the smallest  $n$  such that  $a_n \neq b_n$ , and set  $d(\alpha, \beta) = p^{-n}$ , 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

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

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  $a \equiv a_n \pmod{p^n}$ . Then  $d(\alpha, \iota(a)) \leq p^{-n} < \epsilon$ .
- 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  $\alpha^{(k)} = (a_n^{(k)})_{n \in \mathbb{N}}$  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  $d(\alpha^{(k)}, \alpha^{(l)}) \leq p^{-n}$ , 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  $\alpha^{(k)} \rightarrow \beta$  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,  $N_1 \cap N_2 = \ker(G \rightarrow G/N_1 \times G/N_2)$  is a  $p$ -group. The **pro- $p$  completion** is

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

where  $G/N_1 \rightarrow G/N_2$  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  $0 \equiv ma_{n+r} \equiv p^r a_{n+r} s \pmod{p^{n+r}}$ , so  $p^n \mid a_{n+r} s$ . Thus  $p^n \mid a_{n+r}$ , so  $a_n \equiv a_{n+r} \equiv 0 \pmod{p^n}$ , a contradiction.  $\square$

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

*Proof.* Exercise. <sup>1</sup> □

## 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  $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  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*

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

*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

$$\begin{aligned} f_n : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \prod_{p \text{ prime}} \mathbb{Z}/p^{e_p(n)}\mathbb{Z} \\ 1 &\longmapsto (1, \dots, 1) \end{aligned},$$

and commutative diagrams

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

Passing to inverse limits,

$$\begin{aligned} \widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\sim} \varprojlim_n \prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z} \\ \cap & & \cap \\ \prod_n \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\sim} \prod_n \prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z} \end{aligned}.$$

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  $\widehat{\mathbb{Z}}$ .

---

<sup>1</sup>Exercise

### 2.3 Profinite matrix groups

For a commutative ring  $R$ , we have

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

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

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

By continuity of ring operations on  $\mathbb{Z}_p$ , addition and multiplication on matrices are continuous, and  $\det : \text{Mat}_{N \times N} \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  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

$$\text{GL}_N \mathbb{Z}_p = \{A \in \text{Mat}_{N \times N} \mathbb{Z}_p \mid \det A \in \mathbb{Z}_p^\times\}, \quad \text{SL}_N \mathbb{Z}_p = \{A \in \text{Mat}_{N \times N} \mathbb{Z}_p \mid \det A = 1\}.$$

Both are profinite groups.

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

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

*Proof.* The diagrams

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

commute.

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

□

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

$$\begin{aligned} \text{GL}_N \widehat{\mathbb{Z}} &= \left\{ A \in \text{Mat}_{N \times N} \widehat{\mathbb{Z}} \mid \det A \in \widehat{\mathbb{Z}}^\times \right\} = \varprojlim_n \text{GL}_N (\mathbb{Z}/n\mathbb{Z}) = \prod_p \text{GL}_N \mathbb{Z}_p, \\ \text{SL}_N \widehat{\mathbb{Z}} &= \left\{ A \in \text{Mat}_{N \times N} \widehat{\mathbb{Z}} \mid \det A = 1 \right\} = \varprojlim_n \text{SL}_N (\mathbb{Z}/n\mathbb{Z}) = \prod_p \text{SL}_N \mathbb{Z}_p, \end{aligned}$$

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

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

are dense. See problem sheet 2.

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

## 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  $H \leq_c G$  of  $G$ . Define  $H_j = p_j(H) \leq G_j$ . Then  $H_j$ , with transition maps  $\phi_{ij}|_{H_i} : H_i \rightarrow H_j$ , are an inverse system of finite groups. Define

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

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  $H = H'$ .  $\square$

**Remark 2.4.2.**

- The two topologies on  $H$  agree by  $\text{id} : (H, \tau_{\text{profinite}}) \rightarrow (H, \tau_{\text{subspace}})$ , 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  $f : G_1 \rightarrow G_2$  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  $H \leq_c G$  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.*  $p_j : G \rightarrow G_j$  are surjective, so  $[G : H] \geq [G_j : H_j]$ . Suppose  $[G : H] \geq N$ . There exist distinct cosets  $g_1H, \dots, g_NH$  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  $p_{j_{n,m}}(g_n^{-1}g_m) \notin H_{j_{n,m}}$ . Take  $k \leq j_{n,m}$  for all  $n$  and  $m$ . Then  $p_k(g_n^{-1}g_m) \notin H_k$  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.  $\square$

**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  $\psi_{ij} : Q_i \rightarrow Q_j$ , which are transition maps for the  $Q_j$ . Set  $Q = \varprojlim_j Q_j$ . The map  $\prod_h G_j \rightarrow \prod_j Q_j$  is continuous, so there is a continuous surjective group homomorphism  $f : G \rightarrow Q$ . 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,

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

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

This is the first isomorphism theorem for profinite groups.

**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  $f_j : G_j \rightarrow H_j$ , such that for all  $i \leq j$ ,

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

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

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

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

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

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

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

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  $f : G \rightarrow H = \varprojlim_j H_j$  such that  $p_j^H \circ f = f_j \circ p_j^G$ .  $\square$

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  $f : G \rightarrow H$  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  $(f_j) : (G_j)_{j \in J'} \rightarrow (H_i)_{i \in I'}$  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  $p_n^H \circ f : G \rightarrow H \rightarrow H_n$  is a continuous homomorphism, so its kernel is open in  $G$ . By Proposition 1.2.17 there exists  $k_n$  such that  $\ker(G \rightarrow G_{k_n}) \leq \ker(G \rightarrow H_n)$ , which means there is a quotient homomorphism

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

Then  $\ker(G \rightarrow G_{n+1}) \leq \ker(G \rightarrow G_n)$ , 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.  $\square$



## 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. <sup>2</sup> □

**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  $\text{Sym } n$  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  $\mathcal{U} = \{U \triangleleft_o G\}$  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

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

Then  $G_n \triangleleft G$ , 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  $\alpha \not\equiv 0 \pmod{p}$ . 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  $\alpha \equiv a_n \pmod{p^n}$ .

*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. □

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

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

---

<sup>2</sup>Exercise

$\Rightarrow$  Consider the group homomorphism

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

which is continuous as multiplication in a ring is continuous. So  $\text{im } f$  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  $1 \in \text{im } f$ , 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  $2^{-1} = (\dots, 5, 2) \in \mathbb{Z}_3 \leq \prod_{n \in \mathbb{N}} \mathbb{Z}/3^n\mathbb{Z}$ .

**Proposition 2.5.12.**  $\alpha \in \widehat{\mathbb{Z}}^\times$  if and only if  $\alpha \bmod n \in (\mathbb{Z}/n\mathbb{Z})^\times$  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  $\alpha \equiv k \bmod n$ .

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

**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  $\{z_1, \dots, z_d\} \subseteq H$ , there exists a generating set  $\{x_1, \dots, x_d\} \subseteq G$  such that  $f(x_i) = z_i$  for all  $i$ .*

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

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

$$N_G(\underline{y}) = |\{\text{generating vectors } \underline{x} \text{ of } G \mid f(\underline{x}) = \underline{y}\}|,$$

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

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

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.  $\square$

**Theorem 2.5.14** (Gaschutz's lemma for profinite groups). *Let  $f : G \rightarrow H$  be a continuous surjective homomorphism of profinite groups. Suppose  $G$  has a topological generating set of size  $d$ . Then for any topological generating set  $\{z_1, \dots, z_d\}$  of  $H$ , there is a topological generating set  $\{x_1, \dots, x_d\}$  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  $(f_j) : (G_j) \rightarrow (H_j)$  such that  $f = \varprojlim_j f_j$ . It is forced that  $f_j$  is surjective, since

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

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

$$X_j = \{\text{generating vectors } \underline{x}_j \in G_j^d \mid f_j(\underline{x}_j) = \underline{z}_j\} \neq \emptyset,$$

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  $f(\underline{x}) = \underline{z}$ .  $\square$

### 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  $\mathcal{N} = \{N \triangleleft_f \Gamma\}$ , there is an inverse system of finite groups  $\Gamma/N$ . Then  $\widehat{\Gamma} = \varprojlim_{N \in \mathcal{N}} \Gamma/N$ , where  $\Gamma/N_1 \rightarrow \Gamma/N_2$  if  $N_1 \leq N_2$ . Also had a canonical morphism  $\iota_\Gamma = \iota : \Gamma \rightarrow \widehat{\Gamma}$ . 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  $f : \Delta \rightarrow \Gamma$  be a group homomorphism. Then there exists a unique continuous group homomorphism  $\widehat{f} : \widehat{\Delta} \rightarrow \widehat{\Gamma}$  such that  $\widehat{f} \circ \iota_\Delta = \iota_\Gamma \circ f$ , so*

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

*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

$$S = \left\{ \delta \in \widehat{\Delta} \mid \widehat{f}_1(\delta) = \widehat{f}_2(\delta) \right\}.$$

Then  $S$  is closed, since it is the preimage of the diagonal in  $\widehat{\Gamma} \times \widehat{\Gamma}$  under  $(\widehat{f}_1, \widehat{f}_2) : \widehat{\Delta} \rightarrow \widehat{\Gamma} \times \widehat{\Gamma}$ , 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  $p_M : \widehat{\Delta} \rightarrow \Delta/M$ . So we get a composition

$$\begin{array}{ccc} \Delta & \xrightarrow{\iota_\Delta} & \widehat{\Delta} \\ & \searrow f & \swarrow p_M \\ & \Delta/M & \\ & \downarrow & \swarrow \widehat{f} \\ & \Gamma & \end{array}$$

Case 2. General case. Take some  $N \triangleleft_f \Gamma$ . There exists a unique  $q_N : \widehat{\Delta} \rightarrow \Gamma/N$  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

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

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

$$\begin{array}{ccc} \Delta & \xrightarrow{\iota_\Delta} & \widehat{\Delta} \\ f \downarrow & & \swarrow \widehat{f} \\ \Gamma & \xrightarrow{\iota_\Gamma} & \widehat{\Gamma} \\ & \searrow p_N & \swarrow q_N \\ & \Gamma/N & \end{array},$$

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.

**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  $N \triangleleft_f \Gamma$  such that  $\gamma \notin N$ , if and only if  $\gamma N \neq 1$  in  $\Gamma/N$ , if and only if there exists  $\phi : \Gamma \rightarrow G$  finite such that  $\phi(\gamma) \neq 1$ .

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

*Proof.*

$$\begin{aligned} \iota : \Gamma &\longrightarrow \hat{\Gamma} \leq \prod_N \Gamma/N \\ \gamma &\longmapsto (\gamma N) \end{aligned}.$$

□

**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

$$\gamma \notin N = \text{Core}_{\Gamma} \Delta = \bigcap_{g \in \Gamma} g \Delta g^{-1} \triangleleft_f \Gamma,$$

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  $N \triangleleft_f \Delta$  such that  $\gamma \notin N$ . Now  $\gamma \notin \text{Core}_{\Gamma} N \triangleleft_f \Gamma$ .

□

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

*Proof.* Exercise. <sup>3</sup>

□

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

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

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

□

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

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

*Proof.* 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  $\text{GL}_N R \rightarrow \text{GL}_N (R/\mathfrak{p})$  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  $\text{Isom } \mathbb{H}^2 \cong \text{PSL}_2 \mathbb{R}$ . □

---

<sup>3</sup>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  $\Delta \leq_f \Gamma$ .*

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

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

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

**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  $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \not\cong (\mathbb{Z}/2\mathbb{Z})^{\mathbb{R}}$ . 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  $V \triangleleft_o H$ , 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

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

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

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

commutes. The  $\phi_{n,n-1} : S_n \rightarrow S_{n-1}$  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  $G \cong H$ .  $\square$

**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  $\widehat{\Gamma} \cong \widehat{\Delta}$ .*

**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.  $\square$

Lecture 10  
Thursday  
11/02/21

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

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

$$\begin{array}{ccc} G & \longrightarrow & G/[G, G] \\ & \searrow & \swarrow \\ & A & \end{array}.$$

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  $A' = \mathbb{Z}^s \times T'$  for  $r, s \in \mathbb{N}$  and  $T$  and  $T'$  finite. We can see  $r$  and  $T$  from finite quotients, since

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

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

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

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

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

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

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

- Claim that  $G_1$  is not isomorphic to  $G_2$ . Suppose  $\Phi : G_2 \rightarrow G_1$  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  $\Phi(1, s) = (t^b, s^c)$ , and  $s^c$  generates  $\mathbb{Z}$ , so  $c = \pm 1$ . A contradiction comes from the computation of

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

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

- Consider finite quotients of  $G_1$ . Let  $f : G_1 \rightarrow Q$  be a finite quotient map. If  $\text{im}(\mathbb{Z} \rightarrow G_1 \rightarrow Q)$  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  $\kappa \equiv 2 \pmod{5}$ . We may now build an isomorphism defined by

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

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  $\mathbb{Z}^{\text{rk } F} = F_{\text{ab}} \cong F'_{\text{ab}} = \mathbb{Z}^{\text{rk } F'}$ . Thus  $\text{rk } F = \text{rk } F'$ , so  $F \cong F'$ .  $\square$

How about surface groups? If  $S_g$  is the fundamental group of an orientable surface of genus  $g$ , then

$$S_g = \langle a_1, b_1, \dots, a_g, b_g \mid [a_1, b_1] \dots [a_g, b_g] = 1 \rangle.$$

Then the abelianisation of  $S_g$  is  $\mathbb{Z}^{2g}$ . Hence  $\widehat{S}_g \not\cong \widehat{F}_r$ , 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*

$$\psi : \{\text{finite index subgroups of } G_1\} \rightarrow \{\text{finite index subgroups of } G_2\},$$

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

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

By the Nielsen-Schreier theorem,  $F_{2g}$  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  $\widehat{F}_{2g} \not\cong \widehat{S}_g$ .

**Remark 3.1.24.**

- Residually finite is not actually necessary, by replacing  $G_1$  by  $G_1/\ker \iota_{G_1}$  for  $\iota : G_1 \rightarrow \widehat{G}_1$ .
- $\phi$  and  $\psi$  do not depend on any homomorphism  $G_1 \rightarrow G_2$ .

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

$$\begin{array}{ccc} \psi & : & \{\text{finite index subgroups } H \leq G\} \longrightarrow \{\text{open subgroups of } \widehat{G}\} \\ & & H \longmapsto \overline{H} \end{array}.$$

*Then, if  $K \leq_f H \leq_f G$ ,*

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

*Proof.*

1. Let  $H \leq_f G$  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  $U \leq_o \widehat{G}$  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

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

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  $\overline{H} \cap G = H$ .

Lecture 11  
Saturday  
13/02/21

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  $[\widehat{G} : \overline{H}] = [G : H]$ . Also, there is a natural bijection of coset spaces  $G/H \rightarrow \widehat{G}/\overline{H}$ .
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  $\text{Sym}(\overline{H}/\overline{K}) = \text{Sym}(H/K) \leq \text{Sym}(G/K)$ . 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  $H/K \rightarrow \overline{H}/\overline{K}$ , 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  $\overline{H} \rightarrow \widehat{H}$ . This is surjective because  $H$  is dense in  $\widehat{H}$ . For injectivity, if  $h \in \overline{H} \setminus \{1\}$ , then there is  $U \triangleleft_o \widehat{G}$  such that  $h \notin U$ , and the map

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

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  $f : G \rightarrow G$  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  $G_n \triangleleft_o G$ , and  $G \cong \varprojlim_n G/G_n$ . Since  $f$  is a surjection,  $[G : f^{-1}(U)] = [G : U]$  for all  $U \leq_o G$ . If  $U$  has index at most  $n$ , then  $f^{-1}(U)$  has index at most  $n$ , so  $f^{-1}(U) \geq G_n$ , so  $f^{-1}(G_n) \geq G_n$ , so  $f(G_n) \leq G_n$ . So we have a quotient map  $f_n : G/G_n \rightarrow G/G_n$ , 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  $p_n(f(g)) = f_n(p_n(g)) \neq 1$  so  $g \notin \ker f$ . □

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

*Proof.* Let  $f : G \rightarrow G$  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  $f : G \rightarrow H$  and  $f' : H \rightarrow G$ . Then  $f$  and  $f'$  are isomorphisms of topological groups.

*Proof.*  $f' \circ f : G \rightarrow G$  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  $f^{-1} = (f' \circ f)^{-1} \circ f'$  and  $f'^{-1} = f \circ (f' \circ f)^{-1}$  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  $d(Q) = d(G)$ . 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  $d(F) \geq d(Q) = d(G)$ . So there is a surjection  $f : F \rightarrow G$ . This induces  $\widehat{f} : \widehat{F} \rightarrow \widehat{G}$ . 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.**  $\widehat{S_g} \not\cong \widehat{F_{2g}}$ .

*Proof.*  $S_g$  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

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

a HNN extension. Define

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

This is well-defined, since

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

- $f$  is surjective. Since  $\text{im } f \ni a^n, t$ ,  $\text{im } f \ni ta^nt^{-1} = a^m$ , and so  $\text{im } f \ni a$ , 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,  $ta^nt^{-1}$  does not commute with  $a$ , so  $[ta^nt^{-1}, a] \neq 1$ . But  $f([ta^nt^{-1}, a]) = [ta^{n^2}t^{-1}, a^n] = [a^{mn}, a^n] = 1$ .

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

## 3.2 Finite quotients of free groups

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

Previously,  $F_2 \hookrightarrow \text{SL}_2 \mathbb{Z} \rightarrow \text{SL}_2(\mathbb{Z}/n\mathbb{Z})$ .

**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  $\phi : G \rightarrow Q$  where  $|Q| = p^m$  such that  $\phi(g) \neq 1$ .

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

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

Then  $F_n$  are characteristic subgroups, so normal, and  $[F : F_n]$  is a power of  $p$ , by induction. Let  $X_n \rightarrow X$  be the cover corresponding to  $F_n \triangleleft F$ . Claim that  $\text{girth } X_{n+1} > \text{girth } X_n$ , so  $\text{girth } X_n \geq n$ . Let  $l$  be any loop in  $X_n$  of minimal length,  $\text{girth } X_n$ . 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  $e$ ,

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

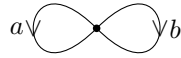
So we have a homomorphism

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

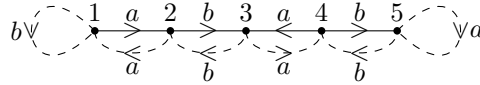
so  $[l] \notin F_{n+1}$ , hence  $l$  does not lift to  $X_{n+1}$ . Let  $g \in F \setminus \{1\}$ . Write  $g$  as a loop in  $X$ . Let  $n$  be the number of edges of  $l$ . Then  $l$  cannot lift to  $X_{n+1}$ , with  $\text{girth}$  at least  $n+1$ . So  $g \notin F_{n+1}$ .  $\square$

*Proof 2.* Let  $F = \langle a_1, \dots, a_k \rangle$  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  $g = s_1 \dots s_m$  where  $s_i$  is  $a_j^{\pm 1}$ . Let  $Y$  be a line segment labelled  $s_1 \dots s_m$ . We add edges to  $Y$  to make it a covering space of  $X$ . This covering space  $\tilde{X}$  does not lift  $g$ , so  $g \notin \pi_1(\tilde{X})$ .  $\square$

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



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



We get a homomorphism

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

acting on the right. Then

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

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  $\{abcb^2cb^{-1}c^{-1}b^{-1}a^{-1}, bc^{-1}b^{-1}abc, bcb^{-1}\}$  or  $\{abcb^2cb^{-1}c^{-1}b^{-1}a^{-1}, bc^{-1}b^{-1}a^{-1}bc, bcb^{-1}\}$  generate  $\langle a, b, c \rangle$ ?

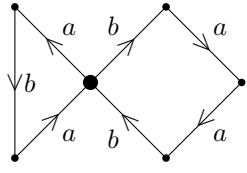
**Theorem 3.2.4** (Marshall Hall's theorem). *Let  $S$  be a finite subset of a finitely generated free group  $F$ . Let  $y \notin \langle S \rangle$ . Then there exists a finite group  $Q$  and  $f : F \rightarrow Q$  such that  $f(y) \notin f(\langle S \rangle)$ .*

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

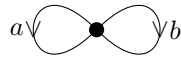
*Proof.* If  $S$  generates  $F$ , it generates  $\hat{F}$  topologically since  $\langle S \rangle = F$  is dense in  $\hat{F}$ . If  $\langle S \rangle \neq F$ , there exists  $y \notin \langle S \rangle$ . Take a finite group  $Q$  and  $f : F \rightarrow Q$  as in Theorem 3.2.4. Then  $f(y) \notin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

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

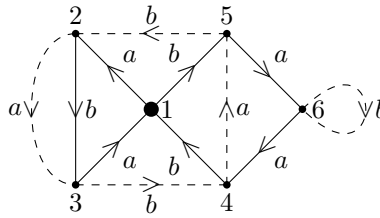
**Example 3.2.6.** Let  $F = \langle a, b \rangle$ , and let  $S = \{aba, ba^2b\}$ . We will show  $\langle S \rangle \neq F$ . Start by writing the elements of  $S$  as loops



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



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

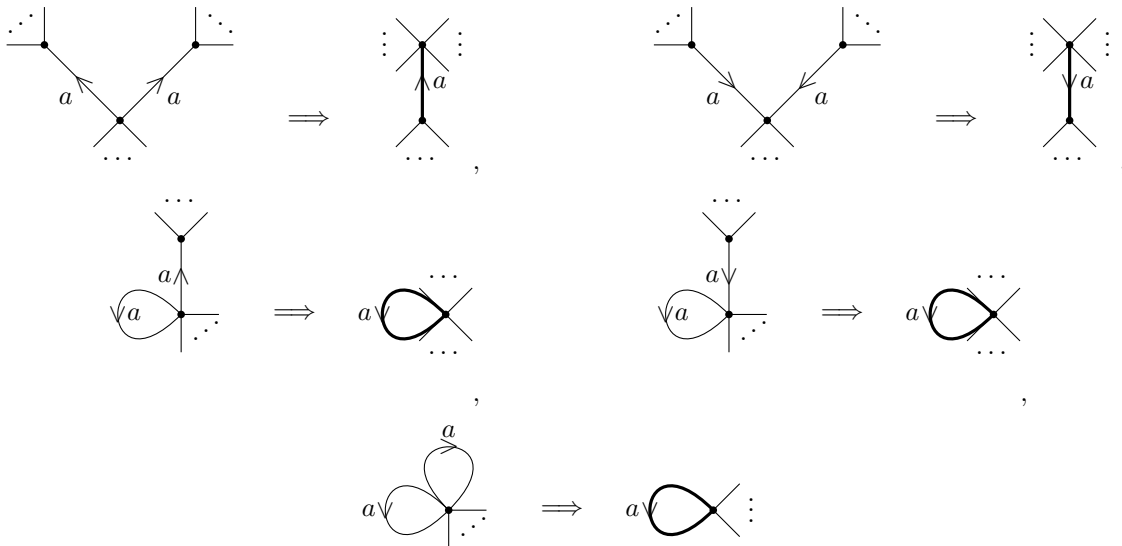


The explicit homomorphism to a finite group is

$$\begin{aligned} \phi : F &\longrightarrow \text{Sym } 6 \\ a &\longmapsto (123)(456) \\ b &\longmapsto (15234)(6) \end{aligned}$$

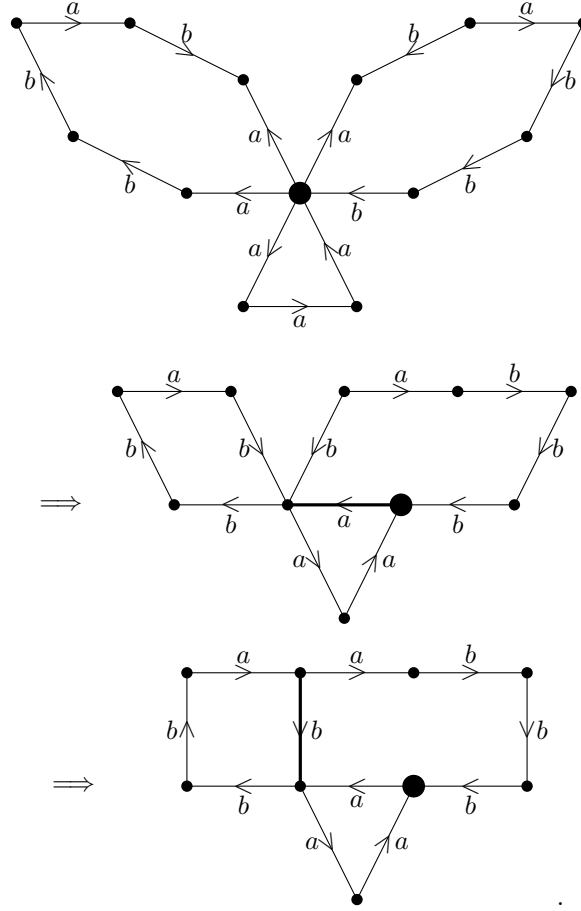
Note that  $\phi(\langle S \rangle) \leq \text{Stab } 1$  and  $\phi(a) \notin \text{Stab } 1$ .

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

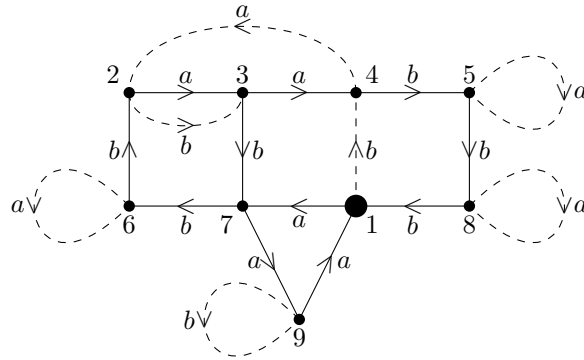


**Fact 3.2.7.** Folding  $Y$  gives a new graph  $Y'$  such that the image of  $\pi_1(Y) \rightarrow \pi_1(Y') \rightarrow \pi_1(X)$  is still  $\langle S \rangle$ .

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



Now can add edges to make a covering



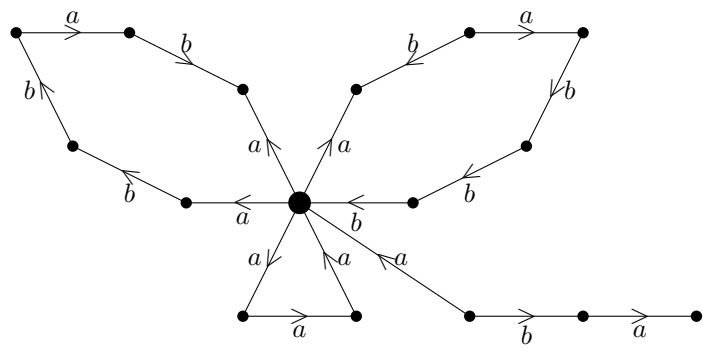
The homomorphism is

$$\begin{aligned} \phi : F &\longrightarrow \text{Sym } 9 \\ a &\longmapsto (179)(234)(5)(6)(8) \\ b &\longmapsto (1458)(2376)(9) \end{aligned}$$

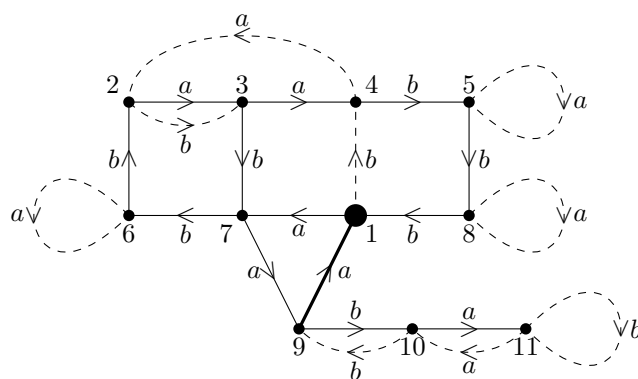
Then  $\phi(\langle S \rangle) \leq \text{Stab } 1$  and  $\phi(a) \notin \text{Stab } 1$ , so  $\phi(\langle S \rangle) \neq \phi(F)$ . Thus  $\langle S \rangle \neq F$ . The other case is that folding gives a one-vertex graph, then  $\langle S \rangle$  is generated by some standard generators of 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

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  $\phi(\langle S \rangle) \leq \text{Stab } 1$  and  $\phi(y) = (1 \mapsto 11) \notin \text{Stab } 1$ . 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 **Fratini 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  $G/\Phi$ .

□

**Proposition 4.1.3.** Let  $f : G \rightarrow H$  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  $\mathbb{Z}/4\mathbb{Z} = \mathcal{C}_4 \hookrightarrow \text{Sym } 5$ . Then  $\Phi(\mathbb{Z}/4\mathbb{Z}) = 2\mathbb{Z}/4\mathbb{Z} = \langle 2 \rangle$  and  $\Phi(\text{Sym } 5) = 1$ , since  $\mathcal{A}_5$  is ruled out by  $\text{Stab } 1$ , 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

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

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

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

where  $H_1(G, \mathbb{F}_p) = G_{\text{ab}}/pG_{\text{ab}}$  is a vector space  $\mathbb{F}_p^{d(G)}$  over  $\mathbb{F}_p$ .

*Proof.* On example sheet 3. □

Lecture 14  
Saturday  
20/02/21

**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  $M \leq_c H \leq_c G$  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  $H \leq_c G$  such that  $H \neq G$ . Then by Corollary 1.2.19, there exists  $p : G \rightarrow Q$  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.  $\square$

**Proposition 4.1.9.** Let  $f : G \rightarrow H$  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  $\varprojlim_{j \in J} \Phi(G_j) \leq \Phi(G)$ .  $\square$

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

$$\Phi(G) = \overline{[G, G]G^p} = H_1(G, \mathbb{F}_p), \quad G/\Phi(G) \cong \mathbb{F}_p^d,$$

where  $d = d(G)$  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  $\Phi(G) \leq \overline{[G, G]G^p}$ .  $\square$

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

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

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  $f(\overline{[G, G]G^p}) \leq \Phi(H)$ , so  $f(\Phi(G)) = f(\overline{[G, G]G^p}) \leq \Phi(H)$ . 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  $f(G) = H$ .  $\square$

## 4.2 Nilpotent groups

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

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

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  $f : G \rightarrow H$  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  $|G|$ .

- $\gamma_2(\mathbb{F}_p) = 1$ .
- There exists  $z \in Z(G) \setminus \{1\}$ . 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

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

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  $\{\gamma_n^{(p)}(G)\}$  are a basis of open normal subgroups of  $G$ .

*Proof.* If  $N \triangleleft_o G$ , 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  $\text{id} : G \rightarrow G$ .

**Proposition 4.3.2.** Let  $G$  be a pro- $p$  group and let  $K \leq_f G$ . 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  $X = \overline{X} = \bigcap_{N \triangleleft_o G} XN$ , 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  $N \triangleleft_o G$ . 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*

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

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

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

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

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

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

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

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

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  $G^d \rightarrow G$ . So  $X = \overline{X} = \bigcap_{N \triangleleft_o G} XN$ . We show  $X = [G, G]$ . Let  $g \in [G, G]$ . For any  $N \triangleleft_o G$ ,  $gN \in [G/N, G/N]$ . Since  $G/N$  is nilpotent,

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

Then  $g \in XN$  for all  $N \triangleleft_o G$ , 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

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

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

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

**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  $3^2 = 9 \equiv 2 \pmod{7}$ , 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

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

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

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

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  $r_1^2 \pmod{p}$ , where  $r_1 \in \mathbb{Z}$ . Then there is a unique  $\rho \in \mathbb{Z}_p$  such that  $\rho^2 = \lambda$  and  $\rho \equiv r_1 \pmod{p}$ .*

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

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

Now  $2r_k \equiv 2r_1 \not\equiv 0 \pmod{p}$ , so we can solve  $b_k + 2r_k a \equiv 0 \pmod{p}$  and find  $a_k$  such that  $(r_k + p^k a_k)^2 \equiv \lambda \pmod{p^{k+1}}$ . 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  $f(r) \equiv 0 \pmod{p^k}$  for some  $k$  and  $f'(r) \not\equiv 0 \pmod{p}$ , 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  $r \pmod{p}$ . Then there exists a unique  $\rho \in \mathbb{Z}_p$  such that  $f(\rho) = 0$  and  $\rho \equiv r \pmod{p^k}$ .*

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

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

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

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

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  $f(r_k) \equiv 0 \pmod{p^k}$  and  $r_{k+1} \equiv r_k \pmod{p^k}$ , and  $r_{k+1}$  will be unique modulo  $p^{k+1}$  with these properties. Then  $(r_k)$  is Cauchy and  $r_k \rightarrow \rho$ , 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

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

Can solve  $b_k + a f'(r_k) \equiv 0 \pmod{p}$  since  $f'(r_k) \equiv f'(r) \not\equiv 0 \pmod{p}$  is invertible modulo  $p$ . So set  $a_k$  such that  $b_k + a f'(r_k) \equiv 0 \pmod{p}$  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

$$\mathrm{GL}_N^{(k)} \mathbb{Z}_p = \ker (\mathrm{GL}_N \mathbb{Z}_p \rightarrow \mathrm{GL}_N (\mathbb{Z}/p^k \mathbb{Z})) = \{I + p^k A \mid A \in \mathrm{Mat}_{N \times N} \mathbb{Z}_p\},$$

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

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

*Proof.*  $|\mathrm{GL}_N^{(1)} (\mathbb{Z}/p^m \mathbb{Z})| = p^{(m-1)N^2}$ , and

$$\mathrm{SL}_N^{(1)} \mathbb{Z}_p \leq \mathrm{GL}_N^{(1)} \mathbb{Z}_p = \varprojlim_m \mathrm{GL}_N^{(1)} (\mathbb{Z}/p^m \mathbb{Z}).$$

□

**Remark 4.4.8.**  $\mathrm{GL}_N \mathbb{Z}_p$  and  $\mathrm{SL}_N \mathbb{Z}_p$  are not pro- $p$  groups, since  $\mathrm{SL}_N (\mathbb{Z}/p\mathbb{Z})$  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  $\mathrm{SL}_N^{(k)} \mathbb{Z}_p \rightarrow \mathrm{SL}_N^{(k+1)} \mathbb{Z}_p$ .

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

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

for some  $B$  which commutes with  $A$ , unless  $p = 2$ ,  $l = 2$ , and  $r = 1$ . Let  $I + p^{k+1} A \in \mathrm{GL}_N^{(k+1)} \mathbb{Z}_p$ . 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

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

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

- Start with  $B_1 = A$ . Then

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

- Assume  $B_n$  and  $E_n$  are given. Set  $B_{n+1} = B_n - p^n E_n$ . Then

$$\begin{aligned} (I + p^k B_{n+1})^p &= (I + p^k B_n - p^{k+n} E_n)^p = (I + p^k B_n)^p - p (I + p^k B_n)^{p-1} p^{k+n} E_n + \dots \\ &= I + p^{k+1} A + p^{k+n+1} E_n - p^{k+n+1} E_n + \dots = I + p^{k+1} A + p^{k+n+2} E_{n+1}. \end{aligned}$$

□

**Proposition 4.4.10.**

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

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  $d(H) \leq N^2$ .

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  $d(H) \leq R$  for all  $H \leq_c G$ , then

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

where  $F$  is finite.

## 5 Cohomology of groups

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

Lecture 17  
Saturday  
27/02/21

### 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

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

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

$$r_1 \cdot (m_1 + m_2) = r_1 \cdot m_1 + r_1 \cdot m_2, \quad (r_1 + r_2) \cdot m_1 = r_1 \cdot m_1 + r_2 \cdot m_1, \quad (r_1 r_2) \cdot m_1 = r_1 \cdot (r_2 \cdot m_1).$$

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  $\alpha : M_1 \rightarrow M_2$  such that  $\alpha(r \cdot m) = r \cdot \alpha(m)$  for all  $r \in \mathbb{Z}G$  and  $m \in M_1$ .

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**

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

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

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

$$\begin{aligned} f^* : \text{Hom}_G(M_2, N) &\longrightarrow \text{Hom}_G(M_1, N) \\ \alpha &\longmapsto \alpha \circ f \end{aligned}$$

Also, we have an **induced map**

$$\begin{aligned} f_* : \text{Hom}_G(N, M_1) &\longrightarrow \text{Hom}_G(N, M_2) \\ \beta &\longmapsto f \circ \beta \end{aligned}$$

Thus

$$\begin{array}{ccc} & N & \\ \beta \swarrow & & \searrow f_* \beta \\ M_1 & \xrightarrow{f} & M_2 \\ f^* \alpha \swarrow & & \searrow \alpha \\ & N & \end{array}$$

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

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

where  $s = \infty$  or  $t = -\infty$  are possible, such that  $d_n \circ d_{n+1} = 0$ , so  $\text{im } d_{n+1} \leq \ker d_n$ . The complex is **exact at**  $M_n$  if  $\text{im } d_{n+1} = \ker d_n$ . 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

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

**Example 5.1.9.**

- The complex

$$0 \rightarrow M_1 \xrightarrow{\alpha} M_2$$

is exact if and only if  $\alpha$  is injective.

- The complex

$$M_1 \xrightarrow{\alpha} M_2 \rightarrow 0$$

is exact if and only if  $\alpha$  is surjective.

- A **short exact sequence** is an exact sequence

$$0 \rightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \rightarrow 0,$$

that is  $\alpha$  is injective,  $\beta$  is surjective, and  $\ker \beta = \text{im } \alpha$ , such as

$$0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0.$$

**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  $g \cdot (\sum_x r_x x) = \sum_x (gr_x) x$ .

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  $\beta : P \rightarrow M_2$  there exists a  $G$ -linear  $\bar{\beta} : P \rightarrow M_1$  such that  $\alpha \circ \bar{\beta} = \beta$ , so

$$\begin{array}{ccc} & P & \\ \swarrow \bar{\beta} & \downarrow \beta & \\ M_1 & \xrightarrow{\alpha} M_2 & \longrightarrow 0 \end{array}.$$

**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  $\beta : \mathbb{Z}G\{X\} \rightarrow M_2$ . For each  $x \in X$  choose  $m_x \in M_1$  such that  $\alpha(m_x) = \beta(x)$ , since  $\alpha$  is surjective. Define

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

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

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

$$\cdots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} \mathbb{Z} \rightarrow 0,$$

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  $\text{Hom}_G(-, M)$  to get a sequence

$$\dots \xleftarrow{d_2^*} \text{Hom}_G(F_1, M) \xleftarrow{d_1^*} \text{Hom}_G(F_0, M),$$

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

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

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

Where do these come from? From topology. Consider a connected simplicial complex  $X$  whose universal cover  $\tilde{X}$  is contractible, with  $\pi_1(X) = G$ . Let  $X_n$  be the set of  $n$ -simplices of  $X$ . Then  $G$  acts on  $\tilde{X}$  with quotient  $X$ , and without fixing any points. Therefore the  $n$ -simplices of  $\tilde{X}$  are in bijection with  $G \times X_n$ . The simplicial chain complex of  $\tilde{X}$  is of the form

$$\dots \xrightarrow{d_2} \mathbb{Z}G\{X_1\} \xrightarrow{d_1} \mathbb{Z}G\{X_0\} \rightarrow \mathbb{Z} \rightarrow 0.$$

Since  $\tilde{X}$  is contractible,  $H_n(\tilde{X}) = 0$  for  $n > 0$ , so exact at  $\mathbb{Z}G\{X_n\}$  for  $n > 0$ , and  $H_0(\tilde{X}) \cong \mathbb{Z}$ . So we get a free resolution of  $\mathbb{Z}$ . Applying  $\text{Hom}_G(-, M)$  gives  $\text{Hom}_G(\mathbb{Z}G\{X_n\}, M)$ . Take the case  $M = \mathbb{Z}$ . Then  $\text{Hom}_G(\mathbb{Z}G\{X_n\}, \mathbb{Z}) \cong \text{Hom}(\mathbb{Z}\{X_n\}, \mathbb{Z})$ , so

$$\dots \leftarrow \text{Hom}(\mathbb{Z}\{X_1\}, \mathbb{Z}) \leftarrow \text{Hom}(\mathbb{Z}\{X_0\}, \mathbb{Z}),$$

which gives  $H^n(G, \mathbb{Z})$ . The dual is

$$\dots \rightarrow \mathbb{Z}\{X_1\} \rightarrow \mathbb{Z}\{X_0\},$$

which gives  $H_n(X)$ .

**Example 5.1.15.** Let  $G = \mathbb{Z} = \langle t \rangle$ . Consider the sequence

$$0 \rightarrow \mathbb{Z}G \xrightarrow{d_1} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0,$$

where  $d_1(x) = x(t-1)$  and

$$\epsilon\left(\sum_{g \in G} n_g g\right) = \sum_{g \in G} n_g$$

is the **augmentation map**. Claim that this is a free resolution of  $\mathbb{Z}$ .

- $\epsilon$  is obviously surjective.
- $\ker \epsilon \geq \text{im } d_1$ . If  $x = \sum_g n_g g$ , then

$$\epsilon(d_1(x)) = \epsilon(x(t-1)) = \epsilon(xt) - \epsilon(x) = \epsilon\left(\sum_g n_g (gt)\right) - \epsilon\left(\sum_g n_g g\right) = \sum_g n_g - \sum_g n_g = 0.$$

- $\ker \epsilon \leq \text{im } d_1$ . Let  $x = \sum_g n_g g$  such that  $\sum_g n_g = 0$ . Relabel each  $g = t^k$  for some  $k$ , so rewriting,

$$\begin{aligned} x &= \sum_k n_k t^k = n_L t^L + \dots + n_K t^K \\ &= n_L t^{L-1}(t-1) + \dots + (n_L + \dots + n_{K-2}) t^{K-1}(t-1) + (n_L + \dots + n_K) t^K \\ &= (n_L t^{L-1} + \dots + (n_L + \dots + n_{K-2}) t^{K-1})(t-1) \in \text{im } d_1. \end{aligned}$$

- $d_1$  is injective. Let  $x = \sum_k n_k t^k = n_L t^L + \dots$  for  $n_L \neq 0$ . Then  $x(t-1)$  has highest coefficient  $n_L t^{L+1} \neq 0$ .

Lecture 18  
Tuesday  
02/03/21

Let  $M$  be a  $G$ -module. Then

$$\begin{array}{ccc} 0 & \longleftarrow & \text{Hom}_G(\mathbb{Z}G, M) \xleftarrow{d^1} \text{Hom}_G(\mathbb{Z}G, M) \\ & \downarrow \iota \sim & \sim \downarrow \iota \\ 0 & \longleftarrow & M \longleftarrow M \end{array},$$

where  $\iota(\phi) = \phi(1)$ . Let  $m \in M$ , and let  $\phi \in \text{Hom}_G(\mathbb{Z}G, M)$  such that  $\iota(\phi) = \phi(1) = m$ . Then

$$\iota(d^1(\phi)) = d^1(\phi)(1) = \phi(d_1(1)) = \phi(t-1) = (t-1)\phi(1) = (t-1)m.$$

Thus

- $H^0(G, M) = \{m \in M \mid tm = m\} = M^G$  are the **invariants**, the elements on which  $G$  acts trivially,
- $H^1(G, M) = M/(t-1)M = M_G$  are the **coinvariants**, and
- $H^n(G, M) = 0$  for  $n \geq 2$ .

Let  $\alpha : \mathbb{Z}G\{X\} \rightarrow \mathbb{Z}G\{Y\}$  be  $G$ -linear for  $X = \{x_1, \dots, x_n\}$  and  $Y = \{y_1, \dots, y_m\}$  finite, so  $\mathbb{Z}G\{X\} \cong (\mathbb{Z}G)^n$  and  $\mathbb{Z}G\{Y\} \cong (\mathbb{Z}G)^m$ . Then  $\alpha$  can be written as a matrix multiplication

$$\alpha(x_i) = \sum_j a_{ij}y_j, \quad a_{ij} \in \mathbb{Z}G.$$

If  $(r_1 \ \dots \ r_n)$  is a row vector corresponding to  $\sum_i r_i x_i$ , then

$$\alpha((r_1 \ \dots \ r_n)) = \left( \sum_i r_i a_{i1} \ \dots \ \sum_i r_i a_{im} \right) = (r_1 \ \dots \ r_n) \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}.$$

Now if  $M$  is a  $G$ -module, we have

$$\begin{array}{ccc} \iota_X : \text{Hom}_G(\mathbb{Z}G\{X\}, M) & \longrightarrow & M^n \\ \psi & \longmapsto & \begin{pmatrix} \psi(x_1) \\ \vdots \\ \psi(x_n) \end{pmatrix}, \end{array} \quad \begin{array}{ccc} \iota_Y : \text{Hom}_G(\mathbb{Z}G\{Y\}, M) & \longrightarrow & M^m \\ \phi & \longmapsto & \begin{pmatrix} \phi(y_1) \\ \vdots \\ \phi(y_m) \end{pmatrix}. \end{array}$$

Then

$$\begin{array}{ccc} \text{Hom}_G(\mathbb{Z}G\{X\}, M) & \xleftarrow{\alpha^*} & \text{Hom}_G(\mathbb{Z}G\{Y\}, M) \\ \iota_X \downarrow \sim & & \sim \downarrow \iota_Y \\ M^n & \xleftarrow{\tilde{\alpha}} & M^m \end{array}.$$

Let  $(b_1 \ \dots \ b_m)^\top \in M^m$ , and let  $\phi \in \text{Hom}_G(\mathbb{Z}G\{Y\}, M)$  such that  $\iota_Y(\phi) = (b_1 \ \dots \ b_m)^\top$ , so  $\phi(y_i) = b_i$ . Then

$$\begin{aligned} \tilde{\alpha} \left( \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \right) &= \iota_X(\alpha^*(\phi)) = \begin{pmatrix} \alpha^*(\phi)(x_1) \\ \vdots \\ \alpha^*(\phi)(x_n) \end{pmatrix} = \begin{pmatrix} \phi(\alpha(x_1)) \\ \vdots \\ \phi(\alpha(x_n)) \end{pmatrix} = \begin{pmatrix} \phi \left( \sum_j a_{1j}y_j \right) \\ \vdots \\ \phi \left( \sum_j a_{nj}y_j \right) \end{pmatrix} \\ &= \begin{pmatrix} \sum_j a_{1j}\phi(y_j) \\ \vdots \\ \sum_j a_{nj}\phi(y_j) \end{pmatrix} = \begin{pmatrix} \sum_j a_{1j}b_j \\ \vdots \\ \sum_j a_{nj}b_j \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}. \end{aligned}$$

**Proposition 5.1.16.** *Let  $G$  be a finitely generated free group. If  $n \geq 2$  then  $H^n(G, M) = 0$  for all  $G$ -modules  $M$ .*

*Proof.* Let  $X$  be a wedge of circles with  $\pi_1(X) = G$ . Then  $\tilde{X}$  is a tree, so contractible, which gives a free resolution of  $G$

$$0 \rightarrow \mathbb{Z}G\{X_1\} \rightarrow \mathbb{Z}G\{X_0\} \rightarrow \mathbb{Z} \rightarrow 0,$$

where  $|X_0| = 1$  and  $|X_1| = \text{rk } G$ . Thus  $H^n(G, M) = 0$  for all  $n \geq 2$ .  $\square$

**Definition 5.1.17.** A group  $G$  has **cohomological dimension**  $\text{cd } G = n$  if  $H^m(G, M) = 0$  for all  $m > n$  and all  $G$ -modules  $M$  but there exists  $M$  such that  $H^n(G, M) \neq 0$ . If no  $n$  exists then  $\text{cd } G = \infty$ .

Free groups have cohomological dimension one. By Stallings, groups with cohomological dimension one are free.

**Definition 5.1.18.** Let  $(A_n, \alpha_n)$  and  $(B_n, \beta_n)$  be chain complexes. A **chain map**  $(f_n)$  is a sequence of  $G$ -linear maps  $f_n : A_n \rightarrow B_n$  such that  $f_{n-1} \circ \alpha_n = \beta_n \circ f_n$ , so

$$\begin{array}{ccc} A_n & \xrightarrow{\alpha_n} & A_{n-1} \\ f_n \downarrow & & \downarrow f_{n-1} \\ B_n & \xrightarrow{\beta_n} & B_{n-1} \end{array}$$

commutes.

**Proposition 5.1.19.** *If  $(f_n)$  is a chain map, then  $(f_n)$  gives induced maps*

$$(f_*)_n : H_n(A_\bullet) \rightarrow H_n(B_\bullet).$$

*These maps are functorial, so if  $(g_n) : (B_n) \rightarrow (C_n)$  then  $(g_*)_n \circ (f_*)_n = ((g \circ f)_*)_n : H_n(A_\bullet) \rightarrow H_n(C_\bullet)$ .*

*Proof.* Take  $x \in \ker \alpha_n$ . Define

$$(f_*)_n([x]) = [f_n(x)], \quad [x] = x + \text{im } \alpha_{n+1} \in H_n(A_\bullet).$$

Then  $\beta_n(f_n(x)) = f_{n-1}(\alpha_n(x)) = 0$ , so  $f_n(x) \in \ker \beta_n$ . The choice of  $x$  does not matter, since if  $x' = x + \alpha_{n+1}(y)$ , then

$$f_n(x') + \text{im } \beta_{n+1} = f_n(x) + f_n(\alpha_{n+1}(y)) + \text{im } \beta_{n+1} = f_n(x) + \beta_{n+1}(f_{n+1}(y)) + \text{im } \beta_{n+1} = f_n(x) + \text{im } \beta_{n+1}.$$

$\square$

**Corollary 5.1.20.** *Let  $f : M \rightarrow N$  be a map of  $G$ -modules. Then we get maps*

$$\begin{array}{ccc} (f_*)_n : \text{Hom}_G(F_n, M) & \longrightarrow & \text{Hom}_G(F_n, N) \\ \phi & \longmapsto & f \circ \phi \end{array}.$$

*These are chain maps, so we have*

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

**Lemma 5.1.21** (Snake lemma). *If*

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

*is a short exact sequence of chain complexes, where  $f_\bullet$  and  $g_\bullet$  are chain maps and each*

$$0 \rightarrow A_n \rightarrow B_n \rightarrow C_n \rightarrow 0$$

*is exact. Then there exists  $\delta_n : H_{n+1}(C_\bullet) \rightarrow H_n(A_\bullet)$  such that*

$$\cdots \rightarrow H_{n+1}(C_\bullet) \xrightarrow{\delta_n} H_n(A_\bullet) \xrightarrow{(f_*)_n} H_n(B_\bullet) \xrightarrow{(g_*)_n} H_n(C_\bullet) \rightarrow \cdots$$

*Proof.* See algebraic topology.  $\square$



**Proposition 5.1.22.** *Let*

$$0 \rightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \rightarrow 0$$

*be a short exact sequence of  $G$ -modules. There is a **long exact sequence***

$$\cdots \rightarrow H^n(G, M_1) \xrightarrow{(\alpha_*)_n} H^n(G, M_2) \xrightarrow{(\beta_*)_n} H^n(G, M_3) \xrightarrow{\delta} H^{n+1}(G, M_1) \rightarrow \cdots,$$

*where  $\delta$  are **connecting homomorphisms**.*

*Proof.* Apply the snake lemma to

$$0 \rightarrow \text{Hom}_G(F_\bullet, M_1) \xrightarrow{(\alpha_*)_\bullet} \text{Hom}_G(F_\bullet, M_2) \xrightarrow{(\beta_*)_\bullet} \text{Hom}_G(F_\bullet, M_3) \rightarrow 0,$$

where  $F_\bullet$  is a projective resolution of  $\mathbb{Z}$  by  $G$ -modules. It remains to prove

$$0 \rightarrow \text{Hom}_G(F_n, M_1) \xrightarrow{(\alpha_*)_n} \text{Hom}_G(F_n, M_2) \xrightarrow{(\beta_*)_n} \text{Hom}_G(F_n, M_3) \rightarrow 0$$

is exact for each  $n$ .

- $\ker(\alpha_*)_n = 0$ . Let  $\phi : F_n \rightarrow M_1$ . If  $(\alpha_*)_n(\phi) = 0$  then  $0 = \alpha \circ \phi$ , so for all  $x \in F_n$ ,  $0 = \alpha(\phi(x))$ , so  $0 = \phi(x)$  for all  $x$ , so  $\phi = 0$ .
- $\ker(\beta_*)_n = \text{im}(\alpha_*)_n$ . Let  $\phi : F_n \rightarrow M_2$  be in the kernel of  $(\beta_*)_n$ . Then  $\beta(\phi(x)) = 0$  for all  $x \in F_n$ , so  $\phi(x) \in \ker \beta = \text{im} \alpha$ , so there exists a unique  $y_x \in M_1$  such that  $\alpha(y_x) = \phi(x)$ . Declare

$$\begin{array}{ccc} \psi & : & F_n \longrightarrow M_1 \\ & & x \longmapsto y_x \end{array}.$$

Then  $(\alpha_*)_n(\psi) = \phi$ , and  $\psi$  is  $G$ -linear follows from uniqueness of  $y_x$ , since  $\alpha(gy_x) = g\alpha(y_x) = g\phi(x) = \phi(gx)$  implies that  $gy_x = y_{gx}$ .

- $(\beta_*)_n$  is surjective. Exactly the definition of  $F_n$  projective.

□

## 5.2 Different projective resolutions

**Theorem 5.2.1.** *The definition of  $H^n(G, M)$  is independent of the choice of projective resolution.*

*Proof.* Take two projective resolutions  $(F_n, d_n)$  and  $(F'_n, d'_n)$  of  $\mathbb{Z}$  by  $G$ -modules. Suppose we construct chain maps

- $f_n : F_n \rightarrow F'_n$  such that  $f_{n-1} \circ d_n = d'_n \circ f_n$ ,
- $g_n : F'_n \rightarrow F_n$  such that  $g_{n-1} \circ d'_n = d_n \circ g_n$ ,
- $s_n : F_n \rightarrow F_{n+1}$  such that  $d_{n+1} \circ s_n + s_{n-1} \circ d_n = g_n \circ f_n - \text{id}$ , and
- $s'_n : F'_n \rightarrow F'_{n+1}$  such that  $d'_{n+1} \circ s'_n + s'_{n-1} \circ d'_n = f_n \circ g_n - \text{id}$ .

These maps prove Theorem 5.2.1. Take a  $G$ -module  $M$ . Chain maps  $(f_n)$  and  $(g_n)$  give homomorphisms  $f_n^* : \text{Hom}_G(F'_n, M) \rightarrow \text{Hom}_G(F_n, M)$ , which give homomorphisms  $f_n^* : H_{F'_n}^n(G, M) \rightarrow H_{F_n}^n(G, M)$ . Take  $\phi : F_n \rightarrow M$  such that  $\phi \in \ker d^{n+1}$ . Then

$$\begin{aligned} f_n^*(g_n^*(\phi)) &= \phi \circ g_n \circ f_n = \phi \circ (\text{id} + d_{n+1} \circ s_n + s_{n-1} \circ d_n) = \phi + \phi \circ d_{n+1} \circ s_n + \phi \circ s_{n-1} \circ d_n \\ &= \phi + s_n^*(d^{n+1}(\phi)) + d^n(s_{n-1}^*(\phi)) = \phi + d^n(s_{n-1}^*(\phi)) \in \phi + \text{im } d^n. \end{aligned}$$

So  $f_n^*(g_n^*(\phi + \text{im } d^n)) = \phi + \text{im } d^n$ , that is  $f_n^* \circ g_n^* = \text{id}$ , on cohomology.

Construct  $f_n$ , inductively.

- Start with the identity  $f_{-1} : \mathbb{Z} \rightarrow \mathbb{Z}$  and  $f_{-2} : 0 \rightarrow 0$ .
- Suppose we have  $f_n$  and  $f_{n-1}$ . Build  $f_{n+1}$ . Since  $d'_n \circ f_n \circ d_{n+1} = f_{n-1} \circ d_n \circ d_{n+1} = 0$ , there exists  $f_{n+1} : F_{n+1} \rightarrow F'_{n+1}$  such that  $d'_{n+1} \circ f_{n+1} = f_n \circ d_{n+1}$ , so

$$\begin{array}{ccccccc}
 & & F_{n+1} & \xrightarrow{d_{n+1}} & F_n & \xrightarrow{d_n} & F_{n-1} \\
 & \swarrow f_{n+1} & \downarrow f_n \circ d_{n+1} & & \downarrow f_n & & \downarrow f_{n-1} \\
 F'_{n+1} & \xrightarrow[d'_{n+1}]{} & \ker d'_n = \operatorname{im} d'_{n+1} & \subset & F'_n & \xrightarrow{d'_n} & F'_{n-1}
 \end{array}$$

Construct  $s_n$  such that  $d_{n+1} \circ s_n + s_{n-1} \circ d_n = g_n \circ f_n - \operatorname{id} = h_n$ .

- Start with the zero map  $s_{-1} : \mathbb{Z} \rightarrow F_0$ .
- Assume  $s_{n-1}$  and  $s_{n-2}$  are constructed. Define  $t_n = h_n - s_{n-1} \circ d_n$ . Since  $d_n \circ t_n = d_n \circ h_n - d_n \circ s_{n-1} \circ d_n = h_{n-1} \circ d_n - (-s_{n-2} \circ d_{n-1} + h_{n-1}) \circ d_n = s_{n-2} \circ d_{n-1} \circ d_n = 0$ , there exists  $s_n$  such that  $d_{n+1} \circ s_n = t_n = h_n - s_{n-1} \circ d_n$ , so

$$\begin{array}{ccccccc}
 & & F_n & \xrightarrow{d_n} & F_{n-1} & \xrightarrow{d_{n-1}} & F_{n-2} \\
 & \swarrow s_n & \downarrow t_n & \searrow h_n & \swarrow s_{n-1} & \downarrow h_{n-1} & \swarrow s_{n-2} \\
 F_{n+1} & \xrightarrow[d_{n+1}]{} & \ker d_n = \operatorname{im} d_{n+1} & \subset & F_n & \xrightarrow{d_n} & F_{n-1} \xrightarrow{d_{n-1}} F_{n-2}
 \end{array}$$

□

**Definition 5.2.2.** Let

$$G^{(n)} = \{[g_1 \mid \cdots \mid g_n] : g_1, \dots, g_n \in G\}, \quad G^{(0)} = \{[\ ]\}.$$

The **bar resolution** is  $F_n = \mathbb{Z}G\{G^{(n)}\}$ , the free module with basis  $G^{(n)}$ , with

$$\begin{aligned}
 d_n : F_n &\longrightarrow F_{n-1} \\
 [g_1 \mid \cdots \mid g_n] &\longmapsto \begin{aligned} &g_1 [g_2 \mid \cdots \mid g_n] \\ &- [g_1 g_2 \mid \cdots \mid g_n] \\ &+ \cdots \\ &+ (-1)^{n-1} [g_1 \mid \cdots \mid g_{n-1} g_n] \\ &+ (-1)^n [g_1 \mid \cdots \mid g_{n-1}] \end{aligned},
 \end{aligned}$$

and the augmentation map

$$\begin{aligned}
 \epsilon : F_0 = \mathbb{Z}G\{[\ ]\} &\longrightarrow \mathbb{Z} \\
 g[\ ] &\longmapsto 1.
 \end{aligned}$$

**Fact 5.2.3.** This is a chain complex, so  $d_{n-1} \circ d_n = 0$ .

**Proposition 5.2.4.** *The bar resolution is exact.*

*Proof.* Forget the  $G$ -action. Then  $F_n$  is free abelian on the set  $G \times G^{(n)} = \{g[g_1 \mid \cdots \mid g_n]\}$ . Define abelian group homomorphisms

$$\begin{aligned}
 s_n : F_n &\longrightarrow F_{n+1} \\
 g[g_1 \mid \cdots \mid g_n] &\longmapsto [g \mid g_1 \mid \cdots \mid g_{n+1}].
 \end{aligned}$$

By a calculation,  $d_{n+1} \circ s_n + s_{n-1} \circ d_n = \operatorname{id}_{F_n}$ . If  $x \in \ker d_n$ , then

$$x = \operatorname{id}(x) = d_{n+1}(s_n(x)) + s_{n-1}(d_n(x)) = d_{n+1}(s_n(x)) \in \operatorname{im} d_{n+1},$$

so  $\ker d_n = \operatorname{im} d_{n+1}$ . □

Let  $M$  be a  $G$ -module. The **cochain group** is

$$C^n(G, M) = \{\text{functions } \phi : G^n \rightarrow M\} \cong \text{Hom}_G(F_n, M).$$

The dual of the  $d_n$  in the bar resolution is

$$d^n : C^{n-1}(G, M) \longrightarrow C^n(G, M)$$

$$\phi \longmapsto \left( (g_1, \dots, g_n) \mapsto \begin{array}{rcl} & g_1\phi(g_2, \dots, g_n) & \\ - & \phi(g_1g_2, \dots, g_n) & \\ + & \dots & \\ + & (-1)^{n-1}\phi(g_1, \dots, g_{n-1}g_n) & \\ + & (-1)^n\phi(g_1, \dots, g_{n-1}) & \end{array} \right).$$

The **group of  $n$ -cocycles** is

$$Z^n(G, M) = \ker d^{n+1} \leq C^n(G, M).$$

The **group of  $n$ -coboundaries** is

$$B^n(G, M) = \text{im } d^n \leq C^n(G, M).$$

Then

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

**Corollary 5.2.5.** *Let  $G$  be a group and  $M$  a  $G$ -module. Then*

$$H^0(G, M) = Z^0(G, M) = \ker d^1 = \{m \in M \mid \forall g, gm = m\} = M^G,$$

*the invariants. A function  $\phi : G \rightarrow M$  is a **crossed homomorphism** if  $\phi(gh) = g\phi(h) + \phi(g)$ , and a **principal crossed homomorphism** if  $\phi(g) = gm - m$  for some  $m \in M$ . Then*

$$H^1(G, M) = \{\text{crossed homomorphisms}\} / \{\text{principal crossed homomorphisms}\},$$

*which is  $\text{Hom}(G, M)$  if  $M$  is trivial.*

*Proof.* Take  $\phi \in C^0(G, M)$  such that  $\phi(1) = m$ . Then

$$d^1(\phi)(g) = g\phi(1) - \phi(1) = gm - m.$$

Let  $\phi \in C^1(G, M)$ . Then

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

so  $\phi \in \ker d^2$  if and only if  $\phi(gh) = g\phi(h) + \phi(g)$ . If  $M$  has trivial  $G$ -action,  $\phi$  is a homomorphism  $G \rightarrow M$ .  $\square$

**Proposition 5.2.6.** *Let  $\alpha : G_1 \rightarrow G_2$  be a group homomorphism. Let  $M$  be a  $G_2$ -module and make  $M$  into a  $G_1$ -module via*

$$g_1 \cdot m = \alpha(g_1)m, \quad g_1 \in G_1, \quad m \in M.$$

*Then there is a natural homomorphism*

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

*If  $\beta : G_0 \rightarrow G_1$  then  $(\alpha \circ \beta)^* = \beta^* \circ \alpha^*$ .*

*Proof.* Define maps by

$$\alpha^* : C^n(G_2, M) \longrightarrow C^n(G_1, M)$$

$$\phi \longmapsto ((g_1, \dots, g_n) \mapsto \phi(\alpha(g_1), \dots, \alpha(g_n)))$$

Then  $d^n \circ \alpha^* = \alpha^* \circ d^n$ , so

$$\begin{array}{ccc} C^n(G_2, M) & \xrightarrow{\alpha^*} & C^n(G_1, M) \\ d^n \downarrow & & \downarrow d^n \\ C^{n+1}(G_2, M) & \xrightarrow{\alpha^*} & C^{n+1}(G_1, M) \end{array}.$$

Thus  $\alpha^*$  induce maps on cohomology.  $\square$

We might like a sequence of groups

$$1 \rightarrow H \rightarrow G \rightarrow Q \rightarrow 1, \quad H \triangleleft G, \quad G/H = Q$$

to give a long exact sequence in cohomology. This is false.

**Example 5.2.7.** Let

$$1 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}^2 \rightarrow \mathbb{Z} \rightarrow 1.$$

Then

$$\begin{array}{ccccccc} \dots & \longrightarrow & H^2(\mathbb{Z}, M) & \longrightarrow & H^2(\mathbb{Z}^2, M) & \longrightarrow & H^2(\mathbb{Z}, M) \longrightarrow \dots \\ & & \parallel & & \parallel & & \\ & & 0 & & 0 & & \end{array},$$

and there exists  $M$  such that  $H^2(\mathbb{Z}^2, M) \neq 0$ .

**Lemma 5.2.8.** Let  $H \triangleleft G$ . Let  $M$  be a  $G$ -module. Let  $G$  act on  $C^n(H, M)$  by

$$g \cdot \phi = ((h_1, \dots, h_n) \mapsto g\phi(g^{-1}h_1g, \dots, g^{-1}h_ng)).$$

Then this descends to an action of  $G$  on  $H^n(H, M)$ , and  $H$  acts trivially, so this is an action of  $G/H$ .

*Proof.* We want  $g \cdot d^n(\phi) = d^n(g \cdot \phi)$ , which holds by direct computation. So the action of  $G$  is by chain maps, so gives an action on cohomology. For  $H$  acts trivially, we will just do  $n = 1$ . Take  $\phi \in Z^1(H, M)$  and let  $\eta, h \in H$ . Then

$$\begin{aligned} (\eta \cdot \phi)(h) - \phi(h) &= \eta\phi(\eta^{-1}h\eta) - \phi(h) = \eta(\eta^{-1}\phi(h\eta) + \phi(\eta^{-1})) - \phi(h) = \phi(h\eta) + \eta\phi(\eta^{-1}) - \phi(h) \\ &= h\phi(\eta) + \phi(h) + \eta\phi(\eta^{-1}) - \phi(h) = h\phi(\eta) + \eta\phi(\eta^{-1}) = h\phi(\eta) - \phi(\eta) = d^1(\phi(\eta))(h), \end{aligned}$$

since  $\phi(1 \cdot 1) = 1\phi(1) + \phi(1)$  so  $\phi(1) = 0$  and  $0 = \phi(1) = \phi(\eta\eta^{-1}) = \eta\phi(\eta^{-1}) + \phi(\eta)$ .  $\square$

The useful case is  $n = 1$ . If  $\phi : H \rightarrow M$  is a crossed homomorphism  $(g \cdot \phi)(h) = g\phi(g^{-1}hg)$ . If  $M$  is trivial, this reads  $(g \cdot \phi)(h) = \phi(g^{-1}hg)$  so the homomorphism  $\phi$  is  $G$ -invariant.

**Theorem 5.2.9** (Five-term inflation-restriction exact sequence). Let  $H \triangleleft G$  and  $Q = G/H$  and let  $M$  be a  $G$ -module. There is exact sequence

$$0 \rightarrow H^1(Q, M^H) \rightarrow H^1(G, M) \rightarrow H^1(H, M)^Q \rightarrow H^2(Q, M^H) \rightarrow H^2(G, M).$$

*Proof.* Just define the maps.

- **Restriction maps**

$$\begin{aligned} \text{Res} : \quad H^k(G, M) &\longrightarrow H^k(H, M)^Q \\ (f : G^k \rightarrow M) &\longmapsto (\text{Res } f : H^k \leq G^k \xrightarrow{f} M) \end{aligned}.$$

- **Inflation maps**

$$\begin{aligned} \text{Inf} : \quad H^k(Q, M^H) &\longrightarrow H^k(G, M) \\ (f : Q^k \rightarrow M^H) &\longmapsto (\text{Inf } f : G^k \twoheadrightarrow Q^k \xrightarrow{f} M^H \leq M) \end{aligned}.$$

- **Transgression maps.** Let  $s : Q \rightarrow G$  be a set-theoretic section, so  $(Q \rightarrow G \rightarrow Q) = \text{id}_Q$ , with  $s(1) = 1$ . Define

$$\begin{aligned} \rho : G &\longrightarrow H \\ g &\longmapsto gs(gH)^{-1}. \end{aligned}$$

If  $f : H \rightarrow M$  represents a  $Q$ -invariant cohomology class define

$$\begin{aligned} \text{Tg} : H^1(H, M)^Q &\longrightarrow H^2(Q, M^H) \\ f &\longmapsto ((g_1, g_2) \mapsto f(\rho(g_1)\rho(g_2)) - f(\rho(g_1g_2))) \end{aligned}.$$

$\square$

If  $G$  is a free group,  $H^2(G, M) = 0$  for all  $M$ .

**Corollary 5.2.10** (Hopf's formula). *Let  $F$  be a free group and  $R \triangleleft F$  and  $Q = F/R$ . Let  $A$  be an abelian group, viewed as a trivial module. Then*

$$H^2(Q, A) \cong \{F\text{-invariant homomorphisms } R \rightarrow A\} / \{\text{homomorphisms } F \rightarrow A\}.$$

*Proof.* There is an exact sequence

$$\text{Hom}(F, A) \rightarrow \text{Hom}(R, A)^F \rightarrow H^2(Q, A) \rightarrow 0.$$

□

If  $Q = \langle x_1, \dots, x_d \mid r_1, \dots, r_m \rangle$  is a presentation, then  $F = \langle x_1, \dots, x_d \rangle$  is free and  $R = \langle\langle r_1, \dots, r_m \rangle\rangle$  is a normal subgroup generated by  $r_i$ . Then  $d(H^1(Q, \mathbb{Z})) = d(\text{Hom}(Q, \mathbb{Z})) \leq d$ . An  $F$ -invariant homomorphism  $R \rightarrow \mathbb{Z}$  is determined by images of  $r_i$ , so  $d(H^2(Q, \mathbb{Z})) \leq m$ .

**Example 5.2.11.** Let  $Q = \mathbb{Z}/3\mathbb{Z}$  and let  $Q$  act on  $M = \mathbb{Z}^2$  via the order three matrix  $A = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ . Consider the short exact sequence of groups

$$\begin{array}{ccccccc} 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & Q \longrightarrow 1 \\ & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\ & & \mathbb{Z} & & \mathbb{Z} & & \mathbb{Z}/3\mathbb{Z} \end{array}.$$

Since  $H$  acts trivially on  $M$ ,  $H^1(H, M) = \text{Hom}(H, M) \cong \mathbb{Z}^2$  by  $f \mapsto f(1)$ . Then  $f \in H^1(H, M)^Q$  if and only if  $f(1)$  is  $Q$ -invariant, if and only if  $Af(1) = f(1)$ . If  $Ax = x$ , then  $x = 0$ , so  $H^1(H, M)^Q = 0$  and  $H^2(G, M) = 0$ . By the five-term exact sequence,  $H^2(Q, M) = 0$ .

### 5.3 Cohomology and group extensions

Take a group  $E$ , with an abelian normal subgroup  $M$ . Let  $E/M = G$ . Then  $E$  is an **extension of  $G$  by  $M$** , and  $E$  and  $E'$  are **equivalent** extensions if there is a commuting diagram

Lecture 21  
Tuesday  
09/03/21

$$\begin{array}{ccccccc} & & & E & & & \\ & \nearrow & & \downarrow \sim & \searrow & \pi & \\ 1 & \longrightarrow & M & & & G & \longrightarrow 1 \\ & \searrow & & E' & \nearrow & & \end{array}$$

The action of  $G$  on  $M$  is by conjugation in  $E$ . If  $m \in M$  and  $e \in E$ , then  $eme^{-1} \in M$ , which gives an action of  $E$  on  $M$ , and  $M$  is abelian, so  $M$  acts trivially on itself, which gives an action of  $G$  on  $M$ . If  $g \in G$ , take  $e$  such that  $\pi(e) = g$  and set

$$g \bullet m = eme^{-1}.$$

If this action is trivial, then  $E$  is a **central extension**. Given  $G$  and a  $G$ -module  $M$ , can construct the semidirect product  $M \rtimes G$ , where the set of elements is  $M \times G$  with multiplication

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

Then  $M \triangleleft M \rtimes G$ , with the correct action, and quotient  $G$ . So  $M \rtimes G$  is an extension, called the **split extension**

$$1 \rightarrow M \rightarrow M \rtimes G \rightarrow G \rightarrow 1,$$

where the **splitting** is the group homomorphism

$$\begin{array}{ccc} G & \longrightarrow & M \rtimes G \\ g & \longmapsto & (0, g) \end{array}.$$

**Notation 5.3.1.**  $M$  is a  $G$ -module, written additively, and  $M \leq E$ , which is non-abelian.

**Proposition 5.3.2.** *Let  $E$  be an extension of  $G$  by  $M$ . Assume there exists a splitting  $s : G \rightarrow E$ , a group homomorphism such that  $\pi \circ s = \text{id}_G$ . Then  $E$  is equivalent to  $M \rtimes G$ .*

*Proof.* Write down the equivalence  $(m, g) \mapsto ms(g)$ , which is a group homomorphism. □

**Theorem 5.3.3.** *We have a bijection*

$$\left\{ \begin{array}{l} \text{equivalence classes of} \\ \text{extensions of } G \text{ by } M \end{array} \right\} \quad \rightsquigarrow \quad \{ [\phi] \in H^2(G, M) \}.$$

*Proof.* Let  $E$  be an extension of  $G$  by  $M$ . Let  $\pi : E \rightarrow G$  be the quotient. Choose a set-theoretic section  $s : G \rightarrow E$ , a function such that  $\pi \circ s = \text{id}_G$ , so  $\pi(s(g)) = g$ . Choose  $s(1) = 1$ . Consider the function

$$\begin{aligned} \phi : G^2 &\longrightarrow M \\ (g_1, g_2) &\longmapsto s(g_1) s(g_2) s(g_1 g_2)^{-1}, \end{aligned}$$

since  $\pi(s(g_1) s(g_2) s(g_1 g_2)^{-1}) = g_1 g_2 (g_1 g_2)^{-1} = 1$ , and  $\phi \equiv 1$  if and only if  $s$  is a homomorphism.

- The 2-cochain  $\phi \in C^2(G, M)$  is a cocycle, that is  $d^3(\phi) = 0$ . Since  $s(g_1) s(g_2) = \phi(g_1, g_2) s(g_1 g_2)$ ,

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

Rewriting in  $M$ ,

$$\phi(g_1, g_2) + \phi(g_1 g_2, g_3) = g_1 \bullet \phi(g_2, g_3) + \phi(g_1, g_2 g_3),$$

so

$$0 = g_1 \bullet \phi(g_2, g_3) - \phi(g_1 g_2, g_3) + \phi(g_1, g_2 g_3) - \phi(g_1, g_2) = d^3(\phi)(g_1, g_2, g_3).$$

Thus  $\phi$  is a cocycle, and it is a **normalised cocycle**, since  $\phi(1, g) = \phi(g, 1) = 0$  for all  $g \in G$ .

- Let  $s' : G \rightarrow E$  be another section, with  $s'(1) = 1$ . Then  $\pi(s'(g) s(g)^{-1}) = 1$  so define

$$\begin{aligned} \psi : G &\longrightarrow M \\ g &\longmapsto s'(g) s(g)^{-1}. \end{aligned}$$

Now let us compute the cocycle  $\phi'$  coming from  $s'$ . Since  $s'(g) = \psi(g) s(g)$ ,

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

Back to  $M$ ,

$$\phi'(g_1, g_2) = \psi(g_1) + g_1 \bullet \psi(g_2) + \phi(g_1, g_2) - \psi(g_1 g_2) = \phi(g_1, g_2) + d^2(\psi)(g_1, g_2),$$

so  $[\phi] = \phi + \text{im } d^2 = \phi' + \text{im } d^2 = [\phi'] \in H^2(G, M)$ .

It remains to show that equivalent extensions give the same cohomology class, to construct an inverse, and show it is the inverse. Let  $\zeta \in H^2(G, M)$  and choose a normalised cocycle  $\phi$  such that  $\zeta = [\phi]$ . Can always choose normalised.<sup>4</sup> Define  $E_\phi$ , where the set is  $M \times G$  with group operation

$$(m_1, g_1) *_\phi (m_2, g_2) = (m_1 + g_1 \bullet m_2 + \phi(g_1, g_2), g_1 g_2).$$

- If  $s(g) = (0, g)$ , then  $s(g_1) *_\phi s(g_2) = (\phi(g_1, g_2), 1) *_\phi s(g_1 g_2)$ .
  - Associativity since  $\phi$  is a cocycle.
  - $(0, 1)$  is an identity since  $\phi$  is normalised.
  - Existence of inverses since  $\phi$  is a normalised cocycle.

Then  $E_\phi$  is an extension, since  $M \triangleleft E_\phi$ , with the right action, and  $E_\phi/M = G$ .

<sup>4</sup>Exercise: if  $\phi \in Z^2(G, M)$ , set  $\psi(g) = -\phi(1, g)$  and then  $\phi + d^2(\psi)$  turns out to be normalised

- If  $[\phi] = [\phi']$ , where  $\phi'$  is also normalised, then  $\phi - \phi' = d^2(\psi)$  for some  $\psi$ . Define

$$\begin{array}{ccc} E_\phi & \longrightarrow & E_{\phi'} \\ (m, g) & \longmapsto & (m + \psi(g), g) \end{array},$$

which is an equivalence of extensions. □

Back to Hopf's formula. Suppose  $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_m \rangle$ . Take an abelian group  $A$ , a trivial  $G$ -module. Let  $E$  be a central extension of  $G$  by  $A$ . Then  $E$  is generated by  $A$ , and some choices  $\bar{x}_1, \dots, \bar{x}_n$  of preimages of the  $x_i$ . Define  $\bar{r}_i$  as  $r_i$  with bars on top. Then in  $E$ ,  $\bar{r}_i = a_i \in A$ . Writing a presentation of  $E$ ,

$$\bar{E} = \langle \bar{x}_1, \dots, \bar{x}_n, A \mid \bar{r}_1 a_1^{-1}, \dots, \bar{r}_m a_m^{-1}, A \text{ central, relations of } A \rangle.$$

Then

$$\begin{array}{ccccccc} A & \longrightarrow & \bar{E} & \twoheadrightarrow & G & & \\ \parallel & & \downarrow & & \parallel & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G \longrightarrow 1 \end{array},$$

so  $A \hookrightarrow \bar{E}$ , and  $\bar{E} \cong E$ . Set  $F = \langle \bar{x}_1, \dots, \bar{x}_n \rangle$  and  $R = \ker(F \rightarrow G) = \langle \bar{r}_1, \dots, \bar{r}_m \rangle$ . Define an  $F$ -invariant homomorphism

$$\begin{array}{ccc} R & \longrightarrow & A \\ \bar{r}_i & \longmapsto & a_i \end{array},$$

since  $E$  is an extension. If we choose  $\bar{x}_i'$  instead of  $\bar{x}_i$ , then  $\bar{x}_i' = \bar{x}_i b_i$  for some  $b_i \in A$ . Then

$$\begin{array}{ccc} F & \longrightarrow & A \\ \bar{x}_i & \longmapsto & b_i \end{array}$$

is a homomorphism, and the homomorphism  $R \rightarrow A$  is changed by subtracting the restriction of  $F \rightarrow A$ . Thus

$$H^2(G, A) = \{F\text{-invariant homomorphisms } R \rightarrow A\} / \{\text{restrictions of homomorphisms } F \rightarrow A\}.$$

**Example 5.3.4.** Let  $G = \langle x_1, x_2 \mid x_1 x_2 x_1^{-1} x_2^{-1} x_1 \rangle$ . Any extension of  $G$  by  $\mathbb{Z}$  has a presentation

$$E = \langle \bar{x}_1, \bar{x}_2, a \mid \bar{x}_1 \bar{x}_2 \bar{x}_1^{-1} \bar{x}_2^{-1} \bar{x}_1 = a^k, a \text{ central} \rangle.$$

Then  $E$  is equivalent to the direct product, since by  $\bar{x}_1 \mapsto \bar{x}_1' = \bar{x}_1 a^k$ ,

$$E \cong \langle \bar{x}_1', \bar{x}_2, a \mid \bar{x}_1' \bar{x}_2 \bar{x}_1'^{-1} \bar{x}_2^{-1} \bar{x}_1' = 1, a \text{ central} \rangle \cong \mathbb{Z} \times G.$$

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

### 5.3.1 Worked example: extensions of $\mathbb{Z}^2$ by $\mathbb{Z}$

Let  $T = \mathbb{Z}^2 = \langle a, b \rangle$ . Take the free resolution of  $\mathbb{Z}$  by  $\mathbb{Z}T$ -modules

$$0 \rightarrow \mathbb{Z}T \xrightarrow{\beta} \mathbb{Z}T^2 \xrightarrow{\alpha} \mathbb{Z}T \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0,$$

where  $\epsilon$  is the augmentation  $\epsilon(g) = 1$  for all  $g \in T$ , and

$$\alpha \begin{pmatrix} x & y \end{pmatrix} = x(a-1) + y(b-1) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a-1 \\ b-1 \end{pmatrix}, \quad \beta \begin{pmatrix} z \\ z \end{pmatrix} = \begin{pmatrix} z(1-b) & z(a-1) \end{pmatrix} = z \begin{pmatrix} 1-b & a-1 \end{pmatrix}.$$

Exactness comes from topology, since it is the chain complex for the square tiling of the plane. Applying  $\text{Hom}_T(-, \mathbb{Z})$ ,

$$\begin{array}{ccccccc} 0 & \longleftarrow & \text{Hom}_T(\mathbb{Z}T, \mathbb{Z}) & \xleftarrow{\beta^*} & \text{Hom}_T(\mathbb{Z}T^2, \mathbb{Z}) & \xleftarrow{\alpha^*} & \text{Hom}_T(\mathbb{Z}T, \mathbb{Z}) \\ & & \downarrow \sim \phi \mapsto \phi(1) & & \downarrow \sim \phi \mapsto (\phi(1,0), \phi(0,1)) & & \downarrow \sim \phi \mapsto \phi(1) \\ 0 & \longleftarrow & \mathbb{Z} & \xleftarrow{\beta^*} & \mathbb{Z}^2 & \xleftarrow{\alpha^*} & \mathbb{Z} \end{array}.$$

Lecture 22  
Thursday  
11/03/21

Then

$$\alpha^*(z) = \begin{pmatrix} a-1 \\ b-1 \end{pmatrix} z = 0, \quad \beta^* \left( \begin{pmatrix} x \\ y \end{pmatrix} \right) = (1-b \quad a-1) \begin{pmatrix} x \\ y \end{pmatrix} = 0,$$

so

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

Comparing the bar resolution and the topological resolution,

$$\begin{array}{ccccccccc} \dots & \longrightarrow & \mathbb{Z}T\{T^{(2)}\} & \xrightarrow{d_2} & \mathbb{Z}T\{T^{(1)}\} & \xrightarrow{d_1} & \mathbb{Z}T\{T^{(0)}\} & \xrightarrow{\epsilon} & \mathbb{Z} \longrightarrow 0 \\ & & \downarrow f_2 & & \downarrow f_1 & & \downarrow f_0 & & \downarrow \text{id} \\ 0 & \longrightarrow & \mathbb{Z}T & \xrightarrow{\beta} & \mathbb{Z}T^2 & \xrightarrow{\alpha} & \mathbb{Z}T & \xrightarrow{\epsilon} & \mathbb{Z} \longrightarrow 0 \end{array}.$$

- $f_0([\ ])=1$ .
- Let  $[a^r b^s] \in T^{(1)}$  for  $r, s \in \mathbb{Z}$ . We want to set  $f_1([a^r b^s]) = (x_{r,s}, y_{r,s}) \in \mathbb{Z}T^2$  such that  $\alpha(x_{r,s}, y_{r,s}) = f_0(d_1([a^r b^s]))$ , and

$$x_{r,s}(a-1) + y_{r,s}(b-1) = f_0(a^r b^s [\ ] - [\ ]) = a^r b^s - 1 = (a^r - 1)b^s + b^s - 1.$$

Set

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

so  $S(a, r)(a-1) = a^r - 1$ . Then  $x_{r,s} = S(a, r)b^s$  and  $y_{r,s} = S(b, s)$ , so

$$f_1([a^r b^s]) = (S(a, r)b^s, S(b, s)).$$

- We want  $f_2([a^r b^s \mid a^t b^u]) = z_{r,s,t,u}$  such that  $\beta(z_{r,s,t,u}) = f_1(d_2([a^r b^s \mid a^t b^u]))$ , and

$$\begin{aligned} & ((1-b)z_{r,s,t,u}, (a-1)z_{r,s,t,u}) \\ &= f_1(a^r b^s [a^t b^u] - [a^{r+t} b^{s+u}] + [a^r b^s]) \\ &= (a^r b^s S(a, t)b^u - S(a, r+t)b^{s+u} + S(a, r)b^s, a^r b^s S(b, u) - S(b, s+u) + S(b, s)). \end{aligned}$$

By computation,  $z_{r,s,t,u} = S(a, r)b^s S(b, u)$ , so

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

A useful fact is that  $\epsilon$  is a ring homomorphism, and  $\epsilon(S(a, r)) = r$ , so the cochain representing  $p \in \mathbb{Z} \cong H^2(T, \mathbb{Z})$  is

$$\begin{array}{ccc} T^{(2)} \subseteq \mathbb{Z}T\{T^{(2)}\} & \xrightarrow{f_2} & \mathbb{Z}T \\ [a^r b^s \mid a^t b^u] & \longmapsto & S(a, r)b^s S(b, u) \xrightarrow{p\epsilon} \mathbb{Z} \end{array}.$$

The corresponding central extension of  $T$  by  $\mathbb{Z}$  is the set  $\mathbb{Z} \times T$  with group operation

$$(m, a^r b^s) * (n, a^t b^u) = (m + n + pr u, a^{r+t} b^{s+u}),$$

which is

$$\begin{pmatrix} 1 & pr & m \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & pt & n \\ 0 & 1 & u \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & p(r+t) & m+n+pru \\ 0 & 1 & s+u \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus the extension is isomorphic to

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



## 5.4 Cohomology of profinite groups

**Definition 5.4.1.** Let  $G$  be a profinite group. A **finite  $G$ -module** is a finite abelian group with an action

$$\begin{aligned} G \times M &\longrightarrow M \\ (g, m) &\longmapsto g \cdot m \end{aligned}$$

which is continuous.

**Definition 5.4.2.** Let

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

with  $d^n : C^{n-1}(G, M) \rightarrow C^n(G, M)$  by the same formula, and let

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

**Theorem 5.4.3** (Course convention). *All general results from section 5.1 to section 5.3 and from example sheet 4, can be applied to profinite groups, with substitutions groups to profinite groups, functions to continuous functions, and modules to finite modules.*

If  $E$  and  $E'$  are profinite groups, then extensions

$$\begin{array}{ccccccc} & & & E & & & \\ & & & \downarrow & & & \\ 1 & \longrightarrow & M & \begin{array}{c} \nearrow \\ \searrow \end{array} & \begin{array}{c} E \\ E' \end{array} & \begin{array}{c} \searrow \\ \nearrow \end{array} & G \longrightarrow 1 \end{array}$$

correspond to  $H^2(G, M)$ .

**Remark 5.4.4.** Let  $G = \widehat{\mathbb{Z}}$ . Consider the short exact sequence of modules

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0.$$

By the course convention,  $H^1(G, M) = \operatorname{Hom}(G, M)$  and there is a long exact sequence in cohomology. By common sense,  $H^2(\widehat{\mathbb{Z}}, M) = 0$ . Then  $H^1(\widehat{\mathbb{Z}}, \mathbb{Z}) = H^1(\widehat{\mathbb{Z}}, \mathbb{Q}) = 0$ , since any continuous homomorphism  $\widehat{\mathbb{Z}} \rightarrow \mathbb{Q}$  has compact image, so must be trivial. There is an isomorphism

$$\begin{aligned} H^1(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ a + n\mathbb{Z} &\longmapsto \frac{am}{n} + \mathbb{Z}. \end{aligned}$$

Thus

$$\begin{array}{ccccc} H^1(\widehat{\mathbb{Z}}, \mathbb{Q}) & \longrightarrow & H^1(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & H^2(\widehat{\mathbb{Z}}, \mathbb{Z}) \\ \parallel & & \parallel & & \\ 0 & & \mathbb{Q}/\mathbb{Z} & & \end{array},$$

so  $H^2(\widehat{\mathbb{Z}}, \mathbb{Z})$  would be infinite, which is silly.

### 5.4.1 Pro- $p$ groups of cohomological dimension one

**Definition 5.4.5.** A profinite group  $G$  has **cohomological dimension**  $\operatorname{cd} G = n$  if  $H^m(G, M) = 0$  for all  $m > n$  and for all finite modules  $M$  but there exists  $M$  such that  $H^n(G, M) \neq 0$ .

**Theorem 5.4.6.** *Let  $G$  be a pro- $p$  group. Then*

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

**Corollary 5.4.7.** *If  $G \neq 1$ , then  $\operatorname{cd} G = 1$  if and only if  $H^2(G, \mathbb{F}_p) = 0$ .*

*Proof.*  $H^1(G, \mathbb{F}_p) = \operatorname{Hom}(G, \mathbb{F}_p) \neq 0$ . □

Lecture 23  
Saturday  
13/03/21

**Definition 5.4.8.** A  $G$ -module  $M$  is **simple** if the only  $G$ -submodules of  $M$  are zero and  $M$ .

**Proposition 5.4.9.** Let  $G$  be a profinite group. Suppose  $H^n(G, S) = 0$  for all finite simple modules  $S$ . Then  $H^n(G, M) = 0$  for all finite  $M$ .

*Proof.* Suppose not, and let  $M$  be the smallest  $G$ -module such that  $H^n(G, M) \neq 0$ . Since  $M$  is not simple, there exists a non-trivial submodule  $N \subsetneq M$ . Then we have a short exact sequence of  $G$ -modules

$$0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0.$$

By Proposition 5.1.22, there is a long exact sequence, of which part is

$$\begin{array}{ccccccc} \dots & \longrightarrow & H^n(G, N) & \longrightarrow & H^n(G, M) & \longrightarrow & H^n(G, M/N) \longrightarrow \dots \\ & & \downarrow \cong & & & & \downarrow \cong \\ & & 0 & & & & 0 \end{array},$$

so  $H^n(G, M) = 0$ , a contradiction.  $\square$

**Definition 5.4.10.** Let  $M$  be a finite  $G$ -module. For a prime  $p$ ,  $M$  is called  **$p$ -primary** if  $|M|$  is a power of  $p$ .

If  $M$  is finite, then

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

where  $M_p$  are  $p$ -Sylow subgroups or  $p$ -primary components, in a unique way, so this decomposition is invariant under  $G$ , so all  $M_p$  are  $G$ -submodules of  $M$ .

**Proposition 5.4.11.** Let  $G$  be a pro- $p$  group and let  $M$  be a finite  $G$ -module. Then

$$H^n(G, M) = H^n(G, M_p), \quad n \geq 1.$$

*Proof.* Write  $M = M_p \oplus M'$ . Then

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

So we need  $H^n(G, M') = 0$ .

Part 1. If  $G$  is finite, this is on exercise sheet 4, since  $|G|$  and  $|M'|$  are coprime.

Part 2. Let  $G$  be a pro- $p$  group. Let  $\phi : G^n \rightarrow M'$  be a continuous function. We will find  $K \triangleleft_o G$  such that  $K$  acts trivially on  $M'$ , and such that  $\phi$  factors through  $(G/K)^n$ , so  $\phi(g_1, \dots, g_n) = \phi(g_1 k_1, \dots, g_n k_n)$ . Then

$$\begin{array}{ccc} 0 = H^n(G/K, M') & \longrightarrow & H^n(G, M') \\ \bar{\phi} & \longmapsto & \phi \end{array}.$$

The preimages of  $m \in M'$  are closed and open subsets of  $G^n$ , so they are unions of basic open subsets, cosets of open subgroups  $K_{i,m}^n$  where  $K_{i,m} \triangleleft_o G$ . By compactness, for each  $m$  only finitely many  $K_{i,m}$  are needed. Take the intersection of all of these to get the required  $K$ . All preimages of  $m \in M'$  are now unions of cosets of  $K^n$ , so  $\phi$  factors through  $(G/K)^n$ . Making  $K$  smaller, by intersecting with the kernel of  $G \rightarrow \text{Aut } M'$ , makes  $K$  act trivially. Now

$$\phi : G^n \xrightarrow{\pi} (G/K)^n \xrightarrow{\bar{\phi}} M'.$$

If  $d^{n+1}(\phi) = 0$ , then  $\bar{\phi} = d^n(\psi)$  for some  $\psi : (G/K)^{n-1} \rightarrow M'$ , by part 1. It follows that  $\phi = d^n(\psi \circ \pi)$ .  $\square$

**Remark 5.4.12.** In proving that all cocycles factor through some  $(G/K)^n$ , we really show that

$$H^n(G, M) = H^n\left(\varprojlim_{K \triangleleft_o G, K \text{ acts trivially}} G/K, M\right) = \varinjlim_K H^n(G/K, M).$$

**Proposition 5.4.13.** *Let  $G$  be a pro- $p$  group. The only finite simple  $p$ -primary  $G$ -module is  $\mathbb{F}_p$ .*

**Proposition 5.4.14.** *Let  $G$  be a pro- $p$  group. If  $H^n(G, \mathbb{F}_p) = 0$  for some  $n$ , then  $H^n(G, M) = 0$  for all finite  $G$ -modules  $M$ .*

**Proposition 5.4.15.** *Suppose there exists  $N \geq 1$  such that  $H^N(G, M) = 0$  for all finite  $G$ -modules  $M$ . Then  $\text{cd } G \leq N - 1$ .*

Proof for abstract groups, then apply course convention.

*Proof.* We show  $H^{N+1}(G, M) = 0$  for all  $M$ , then induct. Consider the **coinduced module**

$$\text{Coind}_G^K M = \text{Hom}_K(\mathbb{Z}G, M), \quad K \leq G.$$

By Shapiro's lemma,

$$H^n(G, \text{Coind}_G^K M) = H^n(K, M),$$

since  $\text{Hom}_G(F, \text{Coind}_G^K M) \cong \text{Hom}_K(F, M)$  for  $F$  a  $G$ -module. Consider  $K = 1$ . Consider

$$\begin{array}{ccc} \alpha : M & \longrightarrow & \text{Coind}_G^1 M \\ m & \longmapsto & (x \mapsto xm) \end{array}, \quad x \in \mathbb{Z}G,$$

which is injective and  $G$ -linear. So there exists a short exact sequence of modules

$$0 \rightarrow M \xrightarrow{\alpha} \text{Coind}_G^1 M \rightarrow M' \rightarrow 0,$$

which gives a long exact sequence

$$\begin{array}{ccccccc} H^n(G, \text{Coind}_G^1 M) & \longrightarrow & H^n(G, M') & \xrightarrow{\sim} & H^{n+1}(G, M) & \longrightarrow & H^{n+1}(G, \text{Coind}_G^1 M) \\ \uparrow \cong & & & & & & \uparrow \cong \\ H^n(1, M) = 0 & & & & & & H^{n+1}(1, M) = 0, \end{array}, \quad n \geq 1.$$

Since  $H^N(G, M') = 0$  for all  $M'$  by hypothesis,  $H^{N+1}(G, M) = 0$ . □

We have now proved the following.

**Theorem 5.4.16.** *Let  $G$  be a pro- $p$  group. If  $H^n(G, \mathbb{F}_p) = 0$  then  $\text{cd } G \leq n - 1$ .*

**Corollary 5.4.17.** *Topologically finitely generated free pro- $p$  groups have cohomological dimension one.*

*Proof.* To show  $H^2(G, \mathbb{F}_p) = 0$ , if and only if every extension is a split extension. Let

$$1 \rightarrow \mathbb{F}_p \rightarrow E \rightarrow G \rightarrow 1.$$

If  $\{x_1, \dots, x_d\}$  is a generating set of  $G$ , choose preimages  $e_i$  of  $x_i$  in  $E$ . Then the function  $x_i \mapsto e_i$  extends to a continuous homomorphism  $G \rightarrow E$  by freeness. So  $E$  is a split extension, and  $H^2(G, \mathbb{F}_p) = 0$ . □

**Theorem 5.4.18.** *Let  $f : G \rightarrow G'$  be a continuous homomorphism of topologically finitely generated pro- $p$  groups. Assume that*

$$f_1^* : H^1(G', \mathbb{F}_p) \rightarrow H^1(G, \mathbb{F}_p)$$

*is an isomorphism and*

$$f_2^* : H^2(G', \mathbb{F}_p) \rightarrow H^2(G, \mathbb{F}_p)$$

*is injective. Then  $f$  is an isomorphism.*

If  $G = \Gamma$  and  $G' = \Gamma'$  are finitely generated abstract groups, then  $f$  yields an isomorphism of pro- $p$  completions  $\widehat{\Gamma}_{(p)} \rightarrow \widehat{\Gamma'}_{(p)}$ .

**Corollary 5.4.19.** *Let  $G$  be a topologically finitely generated pro- $p$  group of cohomological dimension one. Then  $G$  is free.*

*Proof.* If  $d(G) = d$ , there is a surjection  $f : F \twoheadrightarrow G$  where  $F$  is free of rank  $d$ . Then  $F$  gives an isomorphism  $f_* : F/\Phi(F) \xrightarrow{\sim} G/\Phi(G) \cong \mathbb{F}_p^d$ . Since  $H^1(G, \mathbb{F}_p) = \text{Hom}(G, \mathbb{F}_p) = \text{Hom}(G/\Phi(G), \mathbb{F}_p)$ , the dual spaces are

$$f_1^* : \text{Hom}(G/\Phi(G), \mathbb{F}_p) = H^1(G, \mathbb{F}_p) \xrightarrow{\sim} \text{Hom}(F/\Phi(F), \mathbb{F}_p) = H^1(F, \mathbb{F}_p),$$

and  $f_2^* : H^2(G, \mathbb{F}_p) = 0 \rightarrow H^2(F, \mathbb{F}_p)$  is an injection. Thus  $f$  is an isomorphism.  $\square$

*Proof of Theorem 5.4.18.* Let  $G_n = \gamma_n^{(p)}(G)$  be the lower central  $p$ -series, where  $G_1 = G$  and  $G_{n+1} = [G, G_n]G_n^p$ , which are open in  $G$ . Since  $f(G_n) \leq G'_n$ ,  $f_n : G/G_n \rightarrow G'/G'_n$ . We show all  $f_n$  are isomorphisms, so  $f = \varprojlim_n f_n$  is an isomorphism, by induction.

- $n = 1$  is trivial.
- Consider  $G_n/G_{n+1}$ , which is a finite-dimensional vector space over  $\mathbb{F}_p$ . Then  $f$  induces an isomorphism  $G_n/G_{n+1} \rightarrow G'_n/G'_{n+1}$  if and only if  $f^* : \text{Hom}(G'_n/G'_{n+1}, \mathbb{F}_p) \rightarrow \text{Hom}(G_n/G_{n+1}, \mathbb{F}_p)$  is an isomorphism. A continuous homomorphism  $\phi : G_n \rightarrow \mathbb{F}_p$  factors through  $G_{n+1}$  if and only if  $\phi([g, g_n]) = 0$  for all  $g \in G$  and  $g_n \in G_n$ , if and only if  $\phi(g_n) = \phi(g^{-1}g_ng)$ , that is  $\phi$  is  $G$ -invariant. Then  $\text{Hom}(G_n/G_{n+1}, \mathbb{F}_p) \cong \text{Hom}(G_n, \mathbb{F}_p)^G = H^1(G_n, \mathbb{F}_p)^G$ . For the short exact sequence

$$1 \rightarrow G_n \rightarrow G \rightarrow G/G_n \rightarrow 1,$$

we have a five-term exact sequence

$$\begin{array}{ccccccccc} 0 & \rightarrow & H^1(G/G_n, \mathbb{F}_p) & \rightarrow & H^1(G, \mathbb{F}_p) & \rightarrow & H^1(G_n, \mathbb{F}_p)^G & \rightarrow & H^2(G/G_n, \mathbb{F}_p) & \rightarrow & H^2(G, \mathbb{F}_p) \\ & & \sim \uparrow & & \sim \uparrow & & \uparrow & & \sim \uparrow & & \hookrightarrow \uparrow \\ 0 & \rightarrow & H^1(G'/G'_n, \mathbb{F}_p) & \rightarrow & H^1(G', \mathbb{F}_p) & \rightarrow & H^1(G'_n, \mathbb{F}_p)^{G'} & \rightarrow & H^2(G'/G'_n, \mathbb{F}_p) & \rightarrow & H^2(G', \mathbb{F}_p) \end{array}.$$

By the five lemma, the middle map is an isomorphism, so  $G_n/G_{n+1} \xrightarrow{\sim} G'_n/G'_{n+1}$ . Then

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_n/G_{n+1} & \longrightarrow & G/G_{n+1} & \longrightarrow & G/G_n & \longrightarrow & 1 \\ & & \downarrow \sim & & \downarrow & & \downarrow \sim & & \\ 1 & \longrightarrow & G'_n/G'_{n+1} & \longrightarrow & G'/G'_{n+1} & \longrightarrow & G'/G'_n & \longrightarrow & 1 \end{array}.$$

By the five lemma,  $G/G_{n+1} \xrightarrow{\sim} G'/G'_{n+1}$ .

$\square$

**Example 5.4.20.** Let  $\Gamma = \langle x_1, x_2 \mid x_1x_2x_1^{-1}x_2^{-1}x_1 \rangle$ . By Example 5.3.4,  $H^2(\Gamma, \mathbb{F}_p) = 0$ . Then  $\Gamma_{\text{ab}} \cong \mathbb{Z}$ , generated by  $x_2$ , and  $H^1(\Gamma, \mathbb{F}_p) \cong \mathbb{F}_p$ , generated by  $(x_1, x_2) \mapsto (0, 1)$ . Let

$$f : \mathbb{Z} \rightarrow \Gamma \\ 1 \mapsto x_2.$$

Since  $f_1^* : H^1(\Gamma, \mathbb{F}_p) \rightarrow H^1(\mathbb{Z}, \mathbb{F}_p)$  is an isomorphism and  $f_2^* : H^2(\Gamma, \mathbb{F}_p) \rightarrow H^2(\mathbb{Z}, \mathbb{F}_p)$  is an injection,  $\widehat{\Gamma_{(p)}} \cong \mathbb{Z}_p$ .

Lecture 24  
Tuesday  
16/03/21

### 5.4.2 Presentations of pro- $p$ groups

**Definition 5.4.21.** Let  $X$  be a finite set and  $F$  the free pro- $p$  group on the set  $X$ . Let  $R \subseteq F$ . The pro- $p$  group with presentation  $G = [X \mid R]_p$  is defined to be  $G = F / \langle\langle R \rangle\rangle$ .

**Lemma 5.4.22.** Let  $F' \subseteq \widehat{F_{(p)}} = F$  be the free abstract group on  $X$ , and  $R \subseteq F'$ . Let  $\Gamma = \langle X \mid R \rangle$  be an abstract group, and let  $G = [X \mid R]_p$ . Then  $G = \widehat{F_{(p)}}$ .

*Proof.* Since  $F' \xrightarrow{\subseteq} F$  such that  $\langle\langle R \rangle\rangle \rightarrow \overline{\langle\langle R \rangle\rangle}$ ,

$$F' / \langle\langle R \rangle\rangle \rightarrow \langle \widehat{X \mid R} \rangle_{(p)} \twoheadrightarrow [X \mid R]_{(p)}.$$

There exists  $F \rightarrow \langle \widehat{X \mid R} \rangle_{(p)}$  sending  $X \rightarrow X$  such that  $R \rightarrow 1$ , so  $[X \mid R]_{(p)} \rightarrow \langle \widehat{X \mid R} \rangle_{(p)}$  is a surjection. By the Hopf property, surjections are isomorphisms.  $\square$

How many generators does a pro- $p$  group need? Since

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

the minimal number of generators is  $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$ .

**Theorem 5.4.23.** Let  $G$  be a topologically finitely generated pro- $p$  group, and let  $X$  be a finite topological generating set for  $G$ , so  $F(X) \twoheadrightarrow G$ . Let  $r_X$  be the minimal size of a set  $R \subseteq F(X)$  such that  $G = [X \mid R]_p$ . Then

$$|X| - r_X = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) - \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p).$$

**Remark 5.4.24.**

- Not true for abstract groups, since  $|X| - \rho_X$  is not a constant for abstract groups, where  $\rho_X$  is the minimal size of  $R$  such that  $\Gamma = \langle X \mid R \rangle$ , and different  $X$ 's need different numbers of relators.
- If  $G$  is a finite  $p$ -group, then  $r_X \leq \rho_X$ . Not known if equality holds.

**Lemma 5.4.25.** Let  $F$  be a pro- $p$  group and  $N \triangleleft_c F$ . Then there exists  $R \subseteq F$  of size  $r$  such that  $N = \overline{\langle\langle R \rangle\rangle}$  if and only if  $\dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^{F/N} \leq r$ .

*Proof.* If  $N = \overline{\langle\langle R \rangle\rangle}$ , then any  $\phi$  is determined by  $\phi(r)$  for  $r \in R$ , so there is an injection  $H^1(N, \mathbb{F}_p)^{F/N} \hookrightarrow \mathbb{F}_p^{|R|}$ , so  $\dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^{F/N} \leq |R|$ . Suppose  $\dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^{F/N} = r$ , so there exists  $R \subseteq N$  such that an  $F$ -invariant  $\phi : N \rightarrow \mathbb{F}_p$  vanishes if and only if  $\phi$  vanishes on  $R$ . Let  $N' = \overline{\langle\langle R \rangle\rangle} \subseteq N$ . Suppose  $N' \neq N$ . Then  $N'\Phi(N) \neq N$ , so  $M = N/N'\Phi(N)$  is a non-trivial abelian pro- $p$  group, and  $F$  acts by conjugation. So <sup>5</sup> there exists an  $F$ -invariant  $M \rightarrow \mathbb{F}_p$ , since the only simple  $F$ -module is  $\mathbb{F}_p$ , a contradiction.  $\square$

*Proof of Theorem 5.4.23.* By Lemma 5.4.25,  $r_X = \dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^{F/N}$ . By the five-term exact sequence,

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(G, \mathbb{F}_p) & \longrightarrow & H^1(F, \mathbb{F}_p) & \xrightarrow{\alpha} & H^1(N, \mathbb{F}_p)^{F/N} \xrightarrow{\beta} H^2(G, \mathbb{F}_p) \longrightarrow H^2(F, \mathbb{F}_p) \\ & & & & \uparrow \mathbb{R} & & \uparrow \mathbb{R} \\ & & & & \mathbb{F}_p^{|X|} & & 0 \end{array},$$

where  $\dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^{F/N} = r_X$ . Then

$$\dim_{\mathbb{F}_p} \text{im } \alpha = \dim_{\mathbb{F}_p} H^1(F, \mathbb{F}_p) - \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = |X| - \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p),$$

and

$$\dim_{\mathbb{F}_p} \ker \beta = \dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^{F/N} - \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = r_X - \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p).$$

Thus

$$|X| - r_X = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) - \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p).$$

$\square$

<sup>5</sup>Exercise: pure topology