Profinite Groups and Group Cohomology

Gareth Wilkes

Part III Lent Term 2021

Introduction

Much of the story of pure mathematics can be expressed as a desire to answer the question 'When are two objects different?'. Showing that two objects are 'the same' in some sense may be considerably easier than proving the contrary. For example, the theory of infinite cardinal numbers may be seen as answering the question 'why is the set of real numbers different from the set of rational numbers?'. In this context it is considerably easier, for example, to exhibit a bijection between $\mathbb{Z}$ and $\mathbb{Q}$ than to show that no bijection between $\mathbb{Q}$ and $\mathbb{R}$ can possibly exist.

In many cases we show that objects are different by defining 'invariants': quantities which (ideally) may be computed, are preserved under isomorphism, and are easier to tell apart than the original object. Some examples of invariants you may have met are given below.

- For a (finite-dimensional) vector space V, the base field $\mathbb{F}$ and the dimension $\dim_{\mathbb{F}}(V)$ determine V up to linear isomrphism.
- For an algebraic field extension $K/\mathbb{Q}$, the degree $[K : \mathbb{Q}]$ and, under some conditions, the Galois group of K over $\mathbb{Q}$.
- For a topological space X, the properties of compactness, connectedness, and path-connectedness may be considered to be invariants.
- For a simplicial complex X, the homology groups $H_*(X)$.
- For a path-connected topological space X, the fundamental group $\pi_1 X$.

This last example is a somewhat odd invariant. It is extremely powerful and often gives fine control over the space X. However, groups are in general just as difficult to distinguish as spaces. In fact, to some extent, they are impossible to distinguish, even for groups that are given by finite presentations: it is even known (by the Adian-Rabin Theorem) that there can be no algorithm that takes as input a finite presentation and decides whether the presentation gives the trivial group. Never mind the harder question of an algorithm taking in two finite presentations and deciding if they give isomorphic groups.

This theorem does not stop us from attempting to design algorithms that distinguish between groups under certain additional conditions. For example, one class of groups for which it is definitely possible to decide isomorphism is the class of finite groups: between any two finite groups there are only finitely many possible bijections, so one can just check all possible bijections to see whether they're isomorphisms. This would be a pretty terrible algorithm, but it would eventually decide the question.

For infinite finitely presented groups, this suggests one conceivable way to tell two groups apart. One can begin to list finite quotients of the two groups and compare the two lists. If these lists differ at some point (that is, there is a finite group which is a quotient of one but not the other), then we will have proved that the two groups are not isomorphic. Of course, we know that this procedure cannot *always* work—but it is still worthwhile to investigate when it does.

For theoretical purposes, one does not really want to work with such an unwieldy object as 'the set of all finite quotients' of a group G. Instead one combines these finite groups into one limiting object, the *profinite completion* of the group. Such a 'limit of finite groups' is the central object of the course, a *profinite group*.

Most of the time we will be studying profinite groups as interesting objects in their own right, or as the profinite completion of a known group. It is worthwhile, however, to mention in the introductory section two other areas of mathematics where profinite groups arise naturally. Neither of these areas is a course pre-requisite, so we will not see these concepts further in this course and can be ignored for those without the precise necessary background.

One key area in which profinite groups arise naturally (and indeed, in which they were first defined) is Galois theory: specifically, the Galois group of an infinite Galois extension of fields is naturally a profinite group. Let us see one example. Consider the field extension K obtained from $\mathbb{Q}$ by adjoining all p^n-th roots of unity for some fixed prime p, as n varies over $\mathbb{N}$. Define also the extension K_N of $\mathbb{Q}$ by adjoining all p^n-th roots for $n \leq N$. Then the K_N form an increasing union of subfields of K such that $K = \bigcup K_N$. Each extension K/K_N is Galois, as are the extensions $K_N/\mathbb{Q}$ and $K/\mathbb{Q}$. It follows that there are natural quotient homomorphisms

$$\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(K_N/\mathbb{Q}) \cong (\mathbb{Z}/p^N\mathbb{Z})^\times.$$

The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ may be considered to be a 'limit' of these finite groups in a certain sense (to be defined soon). This behaviour is typical: every Galois group of an infinite Galois extension may be considered to be a limit of finite Galois groups.

I will also mention that profinite groups also appear in algebraic geometry in the guise of *étale fundamental groups*, though to be perfectly honest I'm not qualified to expand upon this remark further.

The second part of this course also concerns a certain 'invariant' intended to distinguish groups from one another, the theory of *group cohomology*. As the name may suggest, this theory is intimately connected with the homology theory of spaces as studied in Part II Algebraic Topology, but has its own indepedent strengths and weaknesses. Much like the homology group of a space, we will take a group G and define a collection of abelian groups depending on G, called the *cohomology groups* of G. These can be powerful theoretical tools in many contexts. As one key application we will show how cohomology groups provide a solution to the following natural question:

> Given a group G and an abelian group A, how many groups E can there be such that $A \lhd E$ and $E/A = G$?

It is readily seen that a good answer to this question would allow one in principle to classify all groups with order p^n, or more generally all solvable groups, so this particular application of cohomology theory may be seen as carrying on some of the story from IB Group Theory.

At the conclusion of the course we will combine our two main threads into the cohomology theory of profinite groups, and establish some remarkably strong theorems which show that in some ways our profinite groups are actually better behaved than normal groups!

First however, we must lower our sights back down to fundamentals. We begin with some category theory.

Chapter 1

Inverse limits

1.1 Categories and limits

As was mentioned in the introductory section, we will be seeking to combine the information contained in, for example, the set of finite quotients of a given group into one object which we can study. Let us see some basic constructions which combine several objects into one.

Let A and B be two sets, with no particular relationship between them. How might these be combined into one object? Two constructions should come to mind fairly quickly: the product $A \times B$ and the disjoint union $A \sqcup B$. What properties of $A \times B$ and $A \sqcup B$ describe their relationship to A and B?

The disjoint union comes equipped with inclusion maps $i_A \colon A \to A \sqcup B$ and $i_B \colon B \to A \sqcup B$. Furthermore, it is in some sense the 'minimal' object that sensibly contains both A and B: for any other set Z with maps $j_A \colon A \to Z$ and $j_B \colon B \to Z$, there is a unique function $f \colon A \sqcup B \to Z$ which restricts to j_A and j_B, defined simply by $f(a) = j_A(a)$ for $a \in A$ and $f(b) = j_B(b)$ for $b \in B$. This situation would be represented diagrammatically as follows:

$$\begin{tikzcd}
A \arrow[r, "i_A"] \arrow[dr, "j_A"'] & A \sqcup B \arrow[d, "\exists! f"] & B \arrow[l, "i_B"'] \arrow[dl, "j_B"] \\
& Z &
\end{tikzcd} \tag{1.1}$$

This diagram *commutes* in the sense that 'following the arrows' gives the same result whatever path is taken—for example, $f \circ i_A = j_A$. The sort of property described above—where some data (e.g. the set Z and the functions j_A and j_B) implies the unique existence of something else (here, the map f) is called a *universal property.*

We see that the disjoint union tells us about maps *leaving* A and B. What about maps *to* A and B? This is where the product comes in. The product $A \times B$ is equipped with the usual projection maps $p_A : A \times B \to A$ and $p_B : A \times B \to B$. Once again, there is a 'universality' condition too. Given a set Z and maps $q_A : Z \to A$ and $q_B : Z \to B$, there is a unique map $g \colon Z \to A \times B$ such that $p_A \circ g = q_A$ and $p_B \circ g = q_B$, defined by $g(c) = (q_A(c), q_B(c))$. In the form of a diagram:

$$\begin{tikzcd}
& Z \arrow[dl, "q_A"'] \arrow[d, "\exists!\, g"] \arrow[dr, "q_B"] & \\
A & A \times B \arrow[l, "p_A"] \arrow[r, "p_B"'] & B
\end{tikzcd} \tag{1.2}$$

Note the similarity between these two diagrams: one is obtained from the other by reversing the direction of the arrows. We say that the product and disjoint union of sets are *dual* to one another. Duality in this situation is often denoted by the prefix ‘co-’; the disjoint union may thus also be called a *coproduct*.

Let us now move back to group theory, and insist that all our functions are group homomorphisms. We can still ask what groups may play the roles of $A \sqcup B$ and $A \times B$ in the diagrams above. The product $A \times B$ is of course a perfectly sensible group, and satisfies the same universal property: the projection maps p_A and p_B are group homomorphisms, and provided we assume Z is a group and q_A and q_B are homomorphisms, then so is $g = (q_A, q_B)$. So in ‘the category of groups’, the product $A \times B$ is still a product in the sense of the universal property.

What about a coproduct? Given two groups A and B, there is no sensible way to put a group structure on the disjoint union $A \sqcup B$. Is there a group which could replace it?

It turns out that the answer is the *free product* $A * B$, which you met in Part II Algebraic Topology. Indeed, this was essentially the definition of free product that was given. In Algebraic Topology, this was viewed as a special case of another universal property: the *pushout*. For a pushout, the given data is not just two unrelated groups A and B, but also a third group C and maps $\phi_A \colon C \to A$ and $\phi_B \colon C \to B$. The pushout $A \amalg_C B$ was defined to be a group equipped with maps $i_A \colon A \to A \amalg_C B$ and $i_B \colon B \to A \amalg_C B$, such that $i_A \circ \phi_A = i_B \circ \phi_B$, and such that for any other group Z with maps $j_A \colon A \to Z$ and $j_B \colon B \to Z$ such that $j_A \circ \phi_A = j_B \circ \phi_B$, there is a unique homomorphism $f \colon A \amalg_C B \to Z$ such that $f \circ i_A = j_A$ and $f \circ i_B = j_B$.

This blizzard of notation is rather better described with the commutative diagram below.

$$\begin{tikzcd}
C \arrow[r, "\phi_A"] \arrow[d, "\phi_B"] & A \arrow[d, "i_A"'] \arrow[ddr, "j_A"] & \\
B \arrow[r, "i_B"] \arrow[drr, "j_B"'] & A \amalg_C B \arrow[dr, dashed, "\exists!\, f"] & \\
& & Z
\end{tikzcd} \tag{1.3}$$

The language which unifies these situations is the language of category theory. This is not primarily a course in category theory, so we will only introduce the minimum level of terminology required for our needs, and not worry too much about developing things in the abstract.

Definition 1.1.1. A category C consists of:

- a collection of ‘objects’ $\mathrm{Obj}(\mathsf{C})$;

- a collection of 'morphisms' (or 'arrows') $\mathrm{Mor}(\mathsf{C})$, where each morphism f has a domain X and a codomain Y in $\mathrm{Obj}(\mathsf{C})$—denoted by '$f\colon X \to Y$';
- for each $X \in \mathrm{Obj}(\mathsf{C})$, an 'identity morphism' $\mathrm{id}_X\colon X \to X$;
- for each pair of morphisms $f\colon X \to Y$, $g\colon Y \to Z$, a 'composition morphism' $g \circ f\colon X \to Z$

such that:

- for all $f\colon X \to Y$, $f = \mathrm{id}_Y \circ f = f \circ \mathrm{id}_X$; and
- composition is associative—that is, if $f\colon W \to X$, $g\colon X \to Y$, and $h\colon Y \to Z$ then $h \circ (g \circ f) = (h \circ g) \circ f$.

It will be seen that this is a pretty loose set of axioms, and there are a huge range of examples of categories.

The word 'morphism' is used here because in the case of most categories we will meet, each element of $\mathrm{Obj}(\mathsf{C})$ is some sort of set and the morphisms between them are functions saisfying some conditions. However nothing in the definition of 'category' requires us to have this extra structure. In more abstract category theory the word 'arrow' is more appropriate. We generally stick to 'morphism' in this course, except sometimes for a poset category (see Definition 1.1.4 below).

There a many natural categories which are familiar.

- Sets, the category whose objects are sets and whose morphisms are functions;
- Grps, the category of groups and group homomorphisms;
- $\mathsf{Grps}_{\mathsf{fin}}$, the category of finite groups and group homomorphisms;
- $\mathsf{TopGrps}$, the category of topological groups and continuous group homomorphisms (see Definition 1.2.21);
- $\mathsf{Vect}_{\mathsf{k}}$, the vector spaces and linear maps over a field k;
- R-Mod, the category of modules over a ring R, whose morphisms are R-linear maps.

Many more could be listed, along with variations of the above—for instance, one could ask for all homomorphisms to be injective, or insist that all groups are abelian. One important example slightly different to the above is a *poset category* (short for 'partially ordered set category').

Definition 1.1.2. A *partial ordering* $\preceq$ on a set J is a binary relation such that:

- $i \preceq i$ for all $i \in J$;
- if $i \preceq j$ and $j \preceq i$ then $i = j$;
- if $i \preceq j$ and $j \preceq k$ then $i \preceq k$.

A *poset* is a set J equipped with a partial ordering.

If, for every $i, j \in J$, one of $i \preceq j$ and $j \preceq i$ *must* hold, then $\preceq$ is a *total ordering.*

Remark 1.1.3. I suppose logically a set with a total ordering ought to be called a toset, but no one seems to use this word.

Definition 1.1.4. Let $(J, \preceq)$ be a poset. The corresponding *poset category* is a category J defined by setting $\mathrm{Obj}(\mathsf{J}) = J$, and with a unique morphism/arrow $i \to j$ if $i \preceq j$ (and no morphism $i \to j$ if $i \not\preceq j$).

The transitivity property of a partial ordering ensures that compostion in this category makes sense. The identity morphisms are of course the unique arrow $i \to i$ given by $i \preceq i$.

The advantage of category theory in our context is that it allows a definition via universal property to be made, and its basic principles established, once and for all rather than making it once for sets, once for groups, etc etc. For example, a product is defined as follows.

Definition 1.1.5. Let C be a category. A *product* of two objects $A, B \in \mathrm{Obj}(\mathsf{C})$ is an object P equipped with morphisms $p_A \colon P \to A$ and $p_B \colon P \to B$, such that for any object Z and morphisms $q_A \colon Z \to A$ and $q_B \colon Z \to B$, there is a unique morphism $g \colon Z \to P$ such that $p_A \circ g = q_A$ and $p_B \circ g = q_B$.

$$\begin{tikzcd} & Z \arrow[dl, "q_A"'] \arrow[d, "\exists!\, g"] \arrow[dr, "q_B"] & \\ A & P \arrow[l, "p_A"] \arrow[r, "p_B"'] & B \end{tikzcd} \tag{1.4}$$

Remark 1.1.6. It is standard to talk about 'the product P', but this is not totally accurate: the product consists *both* of P *and* the maps p_A and p_B.

Remark 1.1.7. This is just a definition; nothing here says that such a P exists. For instance, in the category of groups of order at most 4, there is no product of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. However, universal product definitions do usually force uniqueness, up to a point.

Definition 1.1.8. Objects A and B in a category C are *isomorphic* if there are morphisms $f \colon A \to B$ and $g \colon B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

Proposition 1.1.9. *Let C be a category and let A and B be objects of C. If a product of A and B exists, then it is unique up to unique isomorphism.*

Proof. Let P with maps p_A and p_B be a product of A and B, and let P', with maps p'_A and p'_B, be another product of A and B. Applying the universal property (1.4) to P, with $Z = P'$, yields a unique map $f \colon P' \to P$ such that $p_A \circ f = p'_A$ and $p_B \circ f = p'_B$. Applying it to P', with $Z = P$ gives $g \colon P \to P'$ such that $p'_A \circ g = p_A$ and $p'_B \circ g = p_B$. Now consider $f \circ g \colon P \to P$. This satisies $p_A \circ f \circ g = p_A$ and $p_B \circ f \circ g = p_B$. The identity id_P also satisfies these conditions, so by the uniqueness part of Definition 1.1.5, we have $\mathrm{id}_P = f \circ g$. Similarly $\mathrm{id}_{P'} = g \circ f$, so P and P' are isomorphic. □

Remark 1.1.10. Basically all proofs that a universal property gives uniqueness up to isomorphism follow this pattern, so we shall not trouble to write them out. Note that the uniqueness statement is about the whole product structure—i.e. both the object P *and* the maps p_A and p_B. For instance, there are many isomorphisms from $\mathbb{Z} \times \mathbb{Z}$ to itself, but only the identity preserves both the projection maps.

Remark 1.1.11. Having established uniqueness up to isomorphism, we are free to fix some notation and say that the product object P will be denoted $A \times B$.

The dual notion to the product, the coproduct, unifies disjoint unions of sets and free products of groups.

Definition 1.1.12. Let C be a category. A *coproduct* of two objects $A, B \in \mathrm{Obj}(\mathsf{C})$ is an object $A \amalg B$ equipped with morphisms $i_A \colon A \to A \amalg B$ and $i_B \colon B \to A \amalg B$, and such that for any other object Z with maps $j_A \colon A \to Z$ and $j_B \colon B \to Z$, there is a unique morphism $f \colon A \amalg B \to Z$ such that $f \circ i_A = j_A$ and $f \circ i_B = j_B$.

$$\begin{tikzcd}
A \arrow[r, "i_A"] \arrow[dr, "j_A"'] & A \amalg B \arrow[d, "\exists!\, f"] & B \arrow[l, "i_B"'] \arrow[dl, "j_B"] \\
& Z &
\end{tikzcd} \tag{1.5}$$

Products are the first example of what category theorists call a *limit*. Coproducts are therefore *colimits*. We will give a formal definition because, while slightly painful, it is easier in the long run than trying to avoid the proper terminology. However, as with the notion of 'category', we will deal more with concrete settings than the abstract theory.

We begin with the natural notion of morphism of categories.

Definition 1.1.13. Let C and D be categories. A *functor* $\mathbf{F} \colon \mathsf{C} \to \mathsf{D}$ associates an object $\mathbf{F}(X) \in \mathrm{Obj}(\mathsf{D})$ to each $X \in \mathrm{Obj}(\mathsf{C})$, and a morphism $\mathbf{F}(f) \colon \mathbf{F}(X) \to \mathbf{F}(Y)$ for each $(f \colon X \to Y) \in \mathrm{Mor}(\mathsf{C})$, such that $\mathbf{F}(\mathrm{id}_X) = \mathrm{id}_{\mathbf{F}(X)}$ for all X and $\mathbf{F}(g \circ f) = \mathbf{F}(g) \circ \mathbf{F}(f)$ for all $f \colon X \to Y$ and $g \colon Y \to Z$.

Definition 1.1.14. Let J and C be categories. A *diagram of shape* J *in* C is a functor $\mathbf{X} \colon \mathsf{J} \to \mathsf{C}$. We may denote $\mathbf{X}(j) = X_j$ for $j \in \mathrm{Obj}(\mathsf{J})$.

Example 1.1.15.

1. If J is the category with two objects 1 and 2 and no morphisms other than the required identity morphisms, a diagram of shape J in C is a choice of two objects X_1 and X_2 of C.

2. If J is the category with three objects 0, 1 and 2, a morphism $0 \to 1$ and a morphism $0 \to 2$ (and no other non-trivial morphisms), then a diagram of type J would be three objects X_0, X_1 and X_2 and choices of morphisms $X_0 \to X_1$ and $X_0 \to X_2$.

Definition 1.1.16. A *cone* on a diagram $\mathbf{X} \colon \mathsf{J} \to \mathsf{C}$ is an object C in C together with morphisms $p_j \colon C \to X_j$ for each $j \in \mathrm{Obj}(\mathsf{J})$, such that for any $\alpha \colon i \to j$ in J, we have $\mathbf{X}(\alpha) \circ p_i = p_j$.

$$\begin{tikzcd}
& C \arrow[dl, "p_i"'] \arrow[dr, "p_j"] & \\
X_i \arrow[rr, "\mathbf{X}(\alpha)"] & & X_j
\end{tikzcd}$$

A *limit* of a diagram $\mathbf{X}\colon \mathsf{J} \to \mathsf{C}$ is a cone L (with morphisms p_j), such that for any other cone Z (with morphisms q_j), there is a unique morphism $f\colon Z \to L$ such that $p_j \circ f = q_j$ for all $j \in \mathrm{Obj}(\mathsf{J})$.

$$\begin{tikzcd}
 & Z \arrow[d, red, "\exists!\, f"] \arrow[ddl, blue, bend right, "q_i"'] \arrow[ddr, blue, bend left, "q_j"] & \\
 & L \arrow[dl, "p_i"'] \arrow[dr, "p_j"] & \\
X_i \arrow[rr, "\mathbf{X}(\alpha)"] & & X_j
\end{tikzcd} \tag{1.6}$$

Once again, this is merely a definition: no claim is made that limits always exist.

Example 1.1.17. For the two-point category J from Example 1.1.15(1), a limit of a diagram of type J is a product $X_1 \times X_2$. Compare (1.6) with Diagram (1.4).

As with all universal properties, there is a dual notion.

Definition 1.1.18. A *cocone* on a diagram $\mathbf{X}\colon \mathsf{J} \to \mathsf{C}$ is an object C in C together with morphisms $p_j\colon X_j \to C$ for each $j \in \mathrm{Obj}(\mathsf{J})$, such that for any $\alpha\colon i \to j$ in J, we have $p_i = p_j \circ \mathbf{X}(\alpha)$.

$$\begin{tikzcd}
X_j \arrow[rr, "\mathbf{X}(\alpha)"] \arrow[dr, blue, "p_i"'] & & X_j \arrow[dl, blue, "p_j"] \\
 & C &
\end{tikzcd}$$

A *colimit* of a diagram $\mathbf{X}\colon \mathsf{J} \to \mathsf{C}$ is a cocone L (with morphisms p_j), such that for any other cocone Z (with morphisms q_j), there is a unique morphism $f\colon L \to Z$ such that $f \circ p_j = q_j$ for all $j \in \mathrm{Obj}(\mathsf{J})$.

$$\begin{tikzcd}
X_i \arrow[rr, "\mathbf{X}(\alpha)"] \arrow[dr, "p_i"'] \arrow[ddr, blue, bend right, "q_i"'] & & X_j \arrow[dl, "p_j"] \arrow[ddl, blue, bend left, "q_j"] \\
 & L \arrow[d, red, "\exists!\, f"] & \\
 & Z &
\end{tikzcd} \tag{1.7}$$

Proposition 1.1.19. *Limits and colimits, if they exist, are unique up to isomorphism.*

Proof. The proof is, mutatus mutandi, the same as Proposition 1.1.9. □

Example 1.1.20.

1. For the two-point category J from Example 1.1.15(1), a colimit of a diagram of type J is a coproduct $X_1 \amalg X_2$.
2. For the three-point category J from Example 1.1.15(2), a colimit of a diagram of type J is a pushout $X_1 \amalg_{X_0} X_2$ (defined as in Diagram (1.3)).

   Remark 1.1.21. Diagram (1.3) may not look quite like the diagram (1.7) defining a colimit—limits and colimits are defined in terms of commuting triangles, whereas the pushout diagram has a commuting square. The reason for this is simply that we omitted the map $i_C = i_B\phi_B = i_A\phi_A$ from the pushout diagram.

We are now in a position to begin to define the eponymous objects of the course. We began this course by asking how the various finite quotients of a group may be assembled into some coherent object which can be studied. Armed with the notion of a limit we may now proceed with this.

1.2 Inverse limits and profinite groups

Let G be a group. The set of finite index normal subgroups N of G form a partially ordered set, where the ordering is given by inclusion: $N_1 \preceq N_2$ if and only if $N_1 \subseteq N_2$. Let N be the corresponding poset category. Define a functor $\mathsf{N} \to \mathsf{Grps}$ by sending each normal subgroup $N \in \mathrm{Obj}(\mathsf{N})$ to the group G/N, and sending each arrow $(N_1 \to N_2) \in \mathrm{Mor}(\mathsf{N})$—which means $N_1 \subseteq N_2$—to the natural quotient map $\phi_{N_1N_2}\colon G/N_1 \to G/N_2$. This is a diagram of shape N in Grps, so we can ask what its limit is. This limit is the object we seek, that contains precisely the knowledge of the finite quotients of G (this statement will be made precise in Theorem 3.1.12 later in the course).

Since this is a key definition of the course, we spell out the definition more explicitly.

Definition 1.2.1. Let G be a group. The *profinite completion* of G, denoted $\widehat{G}$, is a group $\widehat{G}$ admitting homomorphisms $p_N\colon \widehat{G} \to G/N$ for every finite index normal subgroup N of G, such that:

- whenever $N_1 \subseteq N_2$, we have $\phi_{N_1N_2} \circ p_{N_1} = p_{N_2}$; and
- if Z is any group admitting homomorphisms $q_N\colon Z \to G/N$ such that $\phi_{N_1N_2} \circ q_{N_1} = q_{N_2}$ whenever $N_1 \subseteq N_2$, then there is a unique homomorphism $f\colon Z \to \widehat{G}$ such that $p_N \circ f = q_N$ for all N.

$$\begin{tikzcd}
 & Z \arrow[d, "\exists!\, f"] \arrow[ddl, bend right, "q_{N_1}"'] \arrow[ddr, bend left, "q_{N_2}"] & \\
 & \widehat{G} \arrow[dl, "p_{N_1}"'] \arrow[dr, "p_{N_2}"] & \\
G/N_1 \arrow[rr, "\phi_{N_1N_2}"] & & G/N_2
\end{tikzcd}$$

(1.8)

Remark 1.2.2. One group that obviously satisfies the properties of Z in the above diagram is G itself, so there is a natural homomorphism $\iota\colon G \to \widehat{G}$. This is called simply 'the canonical morphism', or sometimes 'the canonical inclusion'—although it is not always an inclusion.

Remark 1.2.3. The word 'profinite' refers to taking a limit of finite objects. The rationale for the word 'completion' will be seen in more detail later: it turns out that $\widehat{G}$ has a natural topology, and may be considered as a complete metric space, in which $\iota(G)$ is dense.

We have not yet shown that any such object $\widehat{G}$ actually has the courtesy to exist. We will prove this shortly, but in a slightly broader context which saves duplication of effort. It is overly restrictive for us to insist that the collection of finite groups in the limit actually arises as the set of finite quotients $\{G/N\}$ for some fixed group G. So instead we pick out some properties of this family of finite groups, and use them to make a more flexible definition.

Definition 1.2.4. A poset $(J, \preceq)$ is an *inverse system* if for any $i, j \in J$ there is some $k \in J$ such that $k \preceq i$ and $k \preceq j$.

An *inverse system of groups* consists of an inverse system $(J, \preceq)$ and a functor from the corresponding poset category J to Grps: that is, we have a group G_j for each $j \in J$ and, whenever $i \preceq j$, we have some homomorphism $\phi_{ij}\colon G_i \to G_j$ such that $\phi_{ii} = \mathrm{id}_{G_i}$ and $\phi_{jk} \circ \phi_{ij} = \phi_{ik}$ when $i \preceq j \preceq k$.

We will usually abbreviate this notation to 'the inverse system of groups $(G_j)_{j \in J}$'. The maps ϕ_{ij} are called 'transition maps'.

The *inverse limit* of an inverse system of groups (more informally, the *inverse limit of the groups* G_j) is the limit of this functor $\mathsf{J} \to \mathsf{Grps}$. It is denoted $\varprojlim_{j \in J} G_j$.

Again, let us explicitly write out the universal property of $\varprojlim_{j \in J} G_j$. It comes equipped with maps $p_i\colon \varprojlim G_j \to G_i$ such that $\phi_{ij} p_i = p_j$; and for any group Z with maps $q_i\colon Z \to G_i$ such that $\phi_{ij} q_i = q_j$, there is a unique map $f\colon Z \to \varprojlim G_j$ such that $p_i \circ f = q_i$.

$$\begin{tikzcd}
 & Z \arrow[d, "\exists!\, f"] \arrow[ddl, bend right, "q_i"'] \arrow[ddr, bend left, "q_j"] & \\
 & \varprojlim G_j \arrow[dl, "p_i"'] \arrow[dr, "p_j"] & \\
G_i \arrow[rr, "\phi_{ij}"] & & G_j
\end{tikzcd} \tag{1.9}$$

Remark 1.2.5. There is absolutely nothing special about groups in this definition. Groups are the focus of the course so the definition was made for groups. An inverse system of sets, or modules, or objects in any category, is a functor from J to Sets or whatever category is relevant. The inverse limit is then a limit in that category.

Remark 1.2.6. At this point a mathematician must grimace and apologise for the notation that has become too standard to change over the centuries. Quite apart from the order of composition in '$\phi_{jk} \circ \phi_{ij} = \phi_{ik}$', we must cope with the fact that an 'inverse limit' is a *limit*, not a *colimit.* The dual notion to an inverse limit is called a 'direct limit', which is a colimit.

There is no good way to scream in formal mathematical writing, but I would avail myself of it here if there were.

Definition 1.2.7. A *profinite group* is the inverse limit of an inverse system of finite groups.

Our first task is to show that these limits actually exist; we do this by giving an explicit description. Recall that limits are only really defined up to isomorphism, so what we give is, strictly speaking, some *choice* of limit—but this distinction is not worth worrying about.

Proposition 1.2.8. *Let $(G_j)_{j\in J}$ be an inverse system of groups. Then the inverse limit of (G_j) exists, and is given by*

$$\varprojlim G_j = \left\{ (g_j)_{j\in J} \in \prod_{j\in J} G_j \textit{ such that } \phi_{ij}(g_i) = g_j \textit{ for all } i \preceq j \right\}.$$

Proof. First note that, since ϕ_{ij} is a group homomorphism, the set L on the right hand side above is actually a group, being a subgroup of the direct product. Furthermore, the projection maps $\prod G_j \to G_i$ for each $i \in J$ restrict to give maps $p_i \colon L \to G_i$ which, by definition, satisfy $\phi_{ij} \circ p_i = p_j$ for $i \preceq j$.

Now let Z be any group with maps $q_i \colon Z \to G_i$ such that $\phi_{ij} \circ q_i = q_j$ whenever $i \preceq j$. Define $f \colon Z \to \prod G_j$ by $f(z) = (q_j(z))_{j\in J}$. By the given property of the q_i, the image of this map is contained in L, so we consider f to be a map $Z \to L$. Note that $p_i \circ f = q_i$ and the definition of the product $\prod G_j$ ensures that f is uniquely defined by this property. Hence L satisfies the definition of $\varprojlim G_j$. □

Remark 1.2.9. This proposition actually used barely any of the hypotheses in the statement. The fact that we have an inverse system is irrelevant. One key reason that we consider inverse systems rather than general limits will be seen in Proposition 1.2.14 below. We also used very few properties of the category of groups: only the existence of products and certain subgroups. Essentially the same proof thus applies to inverse limits of sets, which we record below as it may be useful.

Proposition 1.2.10. *Let $(X_j)_{j\in J}$ be an inverse system of sets. Then the inverse limit of (X_j) exists, and is given by*

$$\varprojlim X_j = \left\{ (x_j)_{j\in J} \in \prod_{j\in J} X_j \textit{ such that } \phi_{ij}(x_i) = x_j \textit{ for all } i \preceq j \right\}.$$

Remark 1.2.11. The explicit form of limit presented by the above proposition will be our primary means of study of profinite groups. The categorical notions are sometimes more elegant for stating properties, and are necessary for a full treatment of the subject.

This explicit description allows us to define a topology on a profinite group. The fact that this topology is well-behaved is what allows much of the theory to take place. As abstract groups, profinite groups are quite unpleasant—unless they are finite, they are actually uncountable (see Exercise Sheet 1). The existence of a useful topology is a key point of the theory, so that a profinite group is almost never considered as an abstract group divorced from its topology.

Definition 1.2.12 (Topology of a profinite group)**.** Let $(G_j)_{j\in J}$ be an inverse system of finite groups. Endow each G_j with the discrete topology, and give $\prod G_j$ the product topology. The topology on $\varprojlim G_j \subseteq \prod G_j$ is the subspace topology.

By Tychonoff's Theorem, $\prod G_j$ is compact and Hausdorff. Each condition $\phi_{ij}(g_i) = g_j$ describes a closed subset of $\prod G_j$, and the intersection of all these subsets is $\varprojlim G_j$. Thus the inverse limit, endowed with the subspace topology, is a closed subspace of $\prod G_j$. Note that $\varprojlim G_j$ is thus a compact Hausdorff space.

Proposition 1.2.13. *A profinite group is a compact Hausdorff space.*

Before delving any further into the structure of profinite groups, we had perhaps better have a way to check that they are non-trivial. Compactness provides such a way.

Proposition 1.2.14. *Let $(X_j)_{j\in J}$ be an inverse system of non-empty finite sets. Then $X = \varprojlim X_j$ is non-empty.*

Proof. Since $\prod X_j$ is compact, we may use the finite intersection property. Let $I_1 \subseteq J$ be any finite subset. Define

$$Y_{I_1} = \left\{ (x_j)_{j\in J} \in \prod_{j\in J} X_j \text{ s.t. } \phi_{ij}(x_i) = x_j \ \forall i,j \in I_1 \text{ with } i \preceq j \right\}$$

Note that each Y_{I_1} is closed in $\prod X_j$, and that

$$Y_{I_1} \cap \cdots \cap Y_{I_n} \supseteq Y_{I_1\cup\cdots\cup I_n}$$

We show that each Y_{I_1} is non-empty. Since J is an inverse system and I_1 is finite, there exists some $i_0 \in J$ such that $i_0 \preceq i$ for all $i \in I_1$. Choose some $x_{i_0} \in X_{i_0}$. Set $x_j = \phi_{i_0 j}(x_{i_0})$ for $j \succeq i_0$, and choose x_j arbitrarily elsewhere. This produces an element $(x_j) \in \prod X_j$, which by construction lies in Y_{I_1} since if $i,j \in I_1$ and $i \preceq j$ then

$$x_j = \phi_{i_0 j}(x_{i_0}) = \phi_{ij}\phi_{i_0 i}(x_{i_0}) = \phi_{ij}(x_i).$$

We now apply the finite intersection property to the Y_{I_1} to conclude that their intersection is non-empty; this intersection is exactly $\varprojlim X_j$ so we are done. □

The topology of a profinite group is even better behaved under a restriction on the inverse system J.

Proposition 1.2.15. *Let J be a countable set and let $(X_J)_{j\in J}$ be a family of finite sets. Then the product $X = \prod X_j$ is* metrizable*: there exists a metric d on X such that the metric topology agrees with the product topology.*

Proof. Without loss of generality assume $J = \mathbb{N}$. Give each space X_n the discrete metric d_n defined by

$$d_n(x,y) = \begin{cases} 0 & \text{if } x = y \\ 1 & \text{if } x \neq y \end{cases}$$

Define the function d on $X \times X$ by

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

It is an easy exercise to show that this defines a metric on X.

Consider the 'identity function'

$$f\colon (X, \mathcal{T}_{\text{prod}}) \to (X, d), \quad f(x) = x$$

from X equipped with the product topology to X equipped with the metric topology. We claim that this is a homeomorphism. It is a bijection from the compact space $(X, \mathcal{T}_{\text{prod}})$ to the Hausdorff space (X, d), so it is enough to show that f is continuous.

A basis for the metric topology consists of open balls $B(x, 1/3^n)$ for $x \in X$ and $n \in N$. Note that

$$d((x_n),(y_n)) < \frac{1}{3^n} \quad \text{if and only if} \quad x_k = y_k \quad \forall k \leq n$$

Hence, denoting by p_n the projection maps $p_n\colon X \to X_n$, we have

$$f^{-1}(B((x_n), 1/3^n)) = \{y = (y_n) \mid y_k = x_k \ \forall k \leq n\} = \bigcap_{k=1}^{n} p_k^{-1}(x_k)$$

which is an open set in the product topology. Hence f is a homeomorphism and we are done. □

Remark 1.2.16. This metric itself doesn't have a great deal to do with the group structure of a profinite group, so won't appear much. It is nevertheless comforting to know that the topology on a profinite group is as well-behaved as a compact metric space.

Remark 1.2.17. The condition that an inverse system is countable will appear in various places through the course as a convenient simplification. It is also a fairly natural one: in group theory the reasonable groups to consider are usually the finitely generated ones, and in the context of finitely generated groups we will always be able to use countable inverse systems. We will see other useful consequences of countability of the inverse system later.

Lemma 1.2.18. *Let G be a finitely generated group. For each $n \in \mathbb{N}$, there are only finitely many subgroups of G of index n.*

Proof. For each subgroup H of G of index n, we may find a homomorphism from G to the symmetric group S_n by labelling the right cosets $H, g_2H, \ldots, g_nH$ of H in G by the symbols $1, \ldots, n$ and letting G act on the right cosets by translation. The subgroup H may be recovered as the stabiliser of 1 (i.e. of the coset H) under this action. So there are at most as many subgroups of index n as there are homomorphisms $G \to S_n$. A homomorphism is determined by the image of some finite generating set of G, so there are only finitely many homomorphisms $G \to S_n$ for fixed n and thus only finitely many subgroups of G of index n. □

Proposition 1.2.19. *Let G be a finitely generated group. The family of finite-index normal subgroups $N \lhd G$ is countable.*

Proof. There are only finitely many subgroups of G of each given index, hence there are only countably many finite index normal subgroups of G. □

It is important to note that the group theory and the topology are not unrelated: profinite groups are *topological groups* in the following sense.

Proposition 1.2.20. *Let G be a profinite group with the above topology. The multiplication map $m\colon G \times G \to G$, $(g, h) \mapsto gh$ and the inversion map $i\colon G \to G$, $g \mapsto g^{-1}$ are continuous.*

Proof. To be completed on Exercise Sheet 1. □

Definition 1.2.21. A *topological group* is a group G endowed with a topology such that the multiplication and inversion maps are continuous.

Definition 1.2.22. Let G and H be topological groups. We say G and H are *topologically isomorphic* or *isomorphic as topological groups* if there is a bijective function $f\colon G \to H$ which is both a homeomorphism and an isomorphism of groups.

Remark 1.2.23. When discussing profinite groups, we shall usually only consider continuous homomorphisms. It is not impossible that a fallible lecturer will fail to mention the word ‘continuous’ or may simply refer to ‘maps of profinite groups’, but it should be assumed that maps are continuous homomorphisms. An exception to this will be in Section 4.3, where we shall prove a surprising theorem that all homomorphisms between certain types of profinite groups are in fact continuous.

Remark 1.2.24. One of the most pleasing results of elementary topology is that ‘a continuous bijection from a compact space to a Hausdorff space is a homeomorphism’. Profinite groups are compact and Hausdorff, so this result makes life much easier when verfiying that maps are homeomorphisms. It will often be used without specific reference to avoid repetition. In particular, for profinite groups, the notion of ‘topological isomorphism’ reduces to ‘there exists a continuous group isomorphism’.

We also note that there is an easy way to check whether a homomorphim of profinite groups is continuous.

Proposition 1.2.25. *Let H be a topological group and let $G = \varprojlim G_j$ be an inverse limit of finite groups. Let $p_j\colon G \to G_j$ be the projections. A homomorphism $f\colon H \to G$ is continuous if and only if every map $f_j = p_j \circ f\colon H \to G_j$ is continuous.*

Proof. Consider the map $f\colon H \to G \subseteq \prod G_j$. This function is continuous if and only if its composition with every p_j is continuous by definition of the product topology. □

Proposition 1.2.26. *Let $f\colon H \to G_j$ be a homomorphism from a topological group to a finite group (equipped with the discrete topology). Then f is continuous if and only if* $\ker(f_j)$ *is an open subgroup of H.*

Proof. Since $\{1\}$ is an open subset in the discrete topology on G_j, if f is continuous then $\ker(f) = f^{-1}(1)$ is open.

Assume $f^{-1}(1)$ is open. Since multiplication on topological groups is continuous, it follows that $f^{-1}(g)$ is open for any $g \in G_j$. Taking unions, we find that $f^{-1}(U)$ is open for any subset U of G_j, so f is continuous. □

Proposition 1.2.27. *Let G be a compact topological group. A subgroup of G is open if and only if it has finite index and is closed.*

Proof. Exercise. □

It is immediate from the definition of a profinite group $G = \varprojlim G_j$ that G has a good supply of open subgroups: the kernels U_j of the maps $p_j\colon G \to G_j$. In fact the topology of a profinite group is entirely governed by its open subgroups.

Proposition 1.2.28. *Let $(G_j)_{j\in J}$ be an inverse system of finite groups with inverse limit G. The open subgroups $U_j = \ker(G \to G_j)$ form a* basis of open neighbourhoods of the identity *in the sense that any open set $V \subseteq G$ which contains the identity contains some U_j.*

Proof. Let V be an open subset of G containing the identity. By definition of the product topology, V is a union of basic open sets of the form $p_{j_1}^{-1}(X_{j_1}) \cap \cdots p_{j_n}^{-1}(X_{j_n})$ for some $j_1, \ldots, j_n \in J$ and $X_{j_i} \subseteq G_{j_i}$. Fix one such basic open set which contains the idenity. Then certainly $1 \in X_{j_i}$ for each i. So we have

$$1 \in p_{j_1}^{-1}(1) \cap \cdots p_{j_n}^{-1}(1) = U_{j_1} \cap \cdots \cap U_{j_n} \subseteq V$$

To turn this intersection into a single U_j, we use the definition of inverse system to find $k \in J$ such that $k \preceq j_i$ for all i. Since $p_{j_i} = \phi_{kj_i} \circ p_k$ where ϕ_{kj_i} is a transition map, we have $\ker p_k \subseteq \ker p_{j_i}$: hence $U_k \subseteq U_{j_i}$ for all i, and $1 \in U_k \subseteq V$ as required. □

Because multiplication in a topological group is continuous, we immediately acquire neighbourhood bases of the other points of G as well.

Corollary 1.2.29. *Let $(G_j)_{j\in J}$ be an inverse system of finite groups with inverse limit G. Let $g = (g_j) \in G$. The open cosets $gU_j = p_j^{-1}(g_j)$ form a basis of open neighbourhoods of g in the sense that for any open set $V \subseteq G$ which contains g there exists some j such that $g \in gU_j \subseteq V$.*

Corollary 1.2.30. *Let $(G_j)_{j\in J}$ be an inverse system of finite groups with inverse limit G. A subset $X \subseteq G$ is dense in G if and only if $p_j(X) = p_j(G)$ for all $j \in J$.*

Proof. Suppose X is not dense in G. Then there exists a non-empty open set U which does not intersect X. By shrinking U we may assume that U is a basic open set of the form $U = p_j^{-1}(g_j)$ for some $j \in J$ and some $g_j \in G_j$. Since U is non-empty, $g_j \in p_j(G)$, and since $U \cap X = \emptyset$, we have $g_j \notin p_j(X)$ and thus $p_j(X) \neq p_j(G)$ as required.

On the other hand, if X is dense then for any $g_j \in p_j(G)$, the open set $p_j^{-1}(g_j)$ is non-empty and thus intersects X. So $g_j \in p_j(X)$ also and we have $p_j(G) \subseteq p_j(X)$. The other containment is obvious. □

Corollary 1.2.31. *Let $(G_j)_{j\in J}$ be an inverse system of finite groups with inverse limit G. Let X be a compact topological space and let $f\colon X \to G$ be a continuous map. Then f is surjective if and only if $p_j(f(X)) = p_j(G)$ for all $j \in J$.*

Proof. The 'only if' direction is obvious. For the 'if' direction, by the previous corollary we know that $f(X)$ is dense in G. Since X is compact, $f(X)$ is compact and hence closed. Hence $f(X)$ is a closed dense set, i.e. all of G. □

We also record a useful characterisation of the closure of a set.

Proposition 1.2.32. *Let G be a profinite group and let $X \subseteq G$ be a subset. Then the closure of G is equal to*

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

where the intersection is taken over the open subgroups of G.

Proof. Each set XN is a union of N-cosets, hence is open and closed in G and contains X—so $\overline{X} \subseteq XN$ for all N.

Now, if $g \notin \overline{X}$ then there is some open set $U \subseteq G$ such that $g \in U$ and $X \cap U = \emptyset$. Then by Corollary 1.2.29 there exists some open subgroup $N = G_j$ of G such that $g \in gN \subseteq U$. Then $g \notin XN$: for if $g = xn$ then $x = gn^{-1} \in gN \subseteq U$, a contradiction. This completes the proof. □

We also note that there is a converse to Proposition 1.2.28.

Proposition 1.2.33. *Let G be a profinite group and let $\mathcal{U}$ be a collection of open normal subgroups of G forming a neighbourhood basis at the identity. Then $G = \varprojlim_{U\in\mathcal{U}} G/U$.*

Proof. The surjective quotient maps $G \to G/U$ yield a surjective continuous homomorphism $f\colon G \to \varprojlim G/U$. Since $\mathcal{U}$ is a neighbourhood base, if $g \in G \smallsetminus \{1\}$ there is $U \in \mathcal{U}$ such that $g \notin U$. It follows that f is injective and we are done. □

1.3 Change of inverse system

It can often be convenient to place additional assumptions on, or otherwise modify, an inverse system. One very useful modification is an analogue of the notion of 'passing to a subsequence'.

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

Remark 1.3.2. A cofinal subsystem of an inverse system is itself an inverse system.

Example 1.3.3. Let J be an inverse system and let $k \in J$. The set

$$J_{\preceq k} = \{j \in J \mid j \preceq k\}$$

is a cofinal subsystem of J. We may refer to this as a *principal cofinal subsystem.*

A key property of passing to a subsequence of a convergent subsequence is that the limit does not change. Indeed the notion of subsequence would be pretty useless otherwise.

Proposition 1.3.4. *Let $(G_j)_{j\in J}$ be an inverse limit of finite groups, and let $I \subseteq J$ be cofinal. Then $H = \varprojlim_{i\in I} G_i$ is topologically isomorphic to $G = \varprojlim_{j\in J} G_j$.*

Proof. The projection map $\prod_{j\in J} G_j \to \prod_{i\in I} G_i$ is a continuous group homomorphism, and clearly restricts to a continuous homomorphism $f\colon G \to H$. We need only check that f is bijective.

Let $(g_j)_{j\in J} \in G$ and assume $f(g) = 1$—that is, $g_i = 1$ for all $i \in I$. Since I is cofinal, any $j \in J$ has some $i \in I$ such that $i \preceq j$. Then $g_j = \phi_{ij}(g_i) = 1$, so that g is the identity. Hence f is injective.

Finally we show that f is surjective. Let $h = (h_i)_{i\in I} \in H$, and define an element $g = (g_j)_{j\in J} \in \prod_{j\in J} G_j$ by setting g_j to be $\phi_{ij}(h_i)$ for some $i \in I$ such that $i \preceq j$. Since I is cofinal, this defines an element g_j for every $j \in J$.

Note that it is immaterial which i is chosen for a given j. If $i_1 \preceq j$ and $i_2 \preceq j$, take $k \in I$ such that $k \preceq i_1$ and $k \preceq i_2$. Since $(h_i) \in H$, we have

$$\phi_{i_1 j}(h_{i_1}) = \phi_{i_1 j}\phi_{k i_1}(h_k) = \phi_{kj}(h_k) = \phi_{i_2 j}(h_{i_2})$$

as claimed.

It follows also that (g_j) is a valid element of $G = \varprojlim_{j\in J} G_j$: if $j_1 \preceq j_2$, choose $i \preceq j_1$. Then we have

$$\phi_{j_1 j_2}(g_{j_1}) = \phi_{j_1 j_2}\phi_{i j_1}(h_i) = \phi_{i j_2}(h_i) = g_{j_2}$$

Finally note that $g_i = h_i$ for $i \in I$, so that $f(g) = h$ as required. □

Another useful modification to an inverse system is the assumption that the transition maps are surjective. In this case one can strengthen Proposition 1.2.14.

Definition 1.3.5. An inverse system of groups is *surjective* if all the transition maps are surjective.

Proposition 1.3.6. *Let $(X_j)_{j\in J}$ be an inverse system of finite sets, where all the transition maps $\phi_{ij}\colon X_i \to X_j$ are surjective. Then the projection maps $p_k\colon X \to X_k$ are surjective.*

Proof. Exercise. □

Given a profinite group we can always assume that the inverse system giving it is indeed a surjective inverse system.

Proposition 1.3.7. *Let $(G_j)_{j\in J}$ be an inverse system of finite groups. Then there is an inverse system $(G'_j)_{j\in J}$ with surjective transition maps with the same limit.*

Proof. Let $G = \varprojlim G_j$ be the inverse limit and let $p_j : G \to G_j$ be the projections. Let $G'_j = p_j(G)$. Since $\phi_{ij}p_i = p_j$, the transition maps restrict to maps $\phi'_{ij} : G'_i \to G'_j$ making the G'_j into an inverse system. Note that ϕ'_{ij} is surjective. If $g = (g_j) \in G$ then by definition all $g_j \in G'_j$. So the inverse limit of the G'_j is exactly G. □

We mention one particular species of inverse system that we will often seek to use. It possesses the advantage that elements can often be constructed by straightforward inductions in addition to the usual methods of inverse limits.

Definition 1.3.8. An inverse system $(J, \preceq)$ is *linearly ordered* if there is a bijection $f : J \to \mathbb{N}$ such that $i \preceq j$ if and only if $f(i) \geq f(j)$.

Remark 1.3.9. Note the reversal of sign in the last inequality above. This is rather awkward but could probably only be avoided by talking about contravariant functors or by reversing all the other conventions so far. The reason for the switch is that the natural numbers, written as a poset with the usual ordering, would give inverse systems that look like this:

$$G_0 \to G_1 \to G_2 \to \cdots$$

whose limit would just be G_0—not very interesting. But we will often encounter systems of groups that look like

$$\cdots \to G_2 \to G_1 \to G_0$$

for which the corresponding poset would look like

$$\cdots \preceq 2 \preceq 1 \preceq 0.$$

That is, $i \preceq j$ if and only if $i \geq j$. We refer to this as the *'wrong-way' ordering on* $\mathbb{N}$.

Remark 1.3.10. In the linearly ordered poset $\mathbb{N}$ with the wrong-way ordering, a cofinal subsystem is the same thing as an increasing sequence k_n of integers.

Proposition 1.3.11. *Let J be a countable inverse system, such that J has no global minimum—that is, for all $j \in J$ there exists $i \in J$ such that $i \preceq j$ but $i \neq j$. Then J has a linearly ordered cofinal subsystem.*

Proof. Exercise. □

Remark 1.3.12. Note that the restriction to J without a global minimum only eliminates some trivial cases: if J posesses a global minimum m then $\varprojlim X_j = X_m$ for any inverse system $(X_j)_{j\in J}$.

Remark 1.3.13. Given the last proposition, one may wonder why we bothered to set up the theory of inverse limits in the first place. But many inverse systems that naturally arise are not linearly ordered, and it would be awkward to have to first turn them into linearly ordered systems before working with them. Instead the existence of cofinal linearly ordered subsystems should be thought of as a useful theoretical tool, to ease certain proofs.

Remark 1.3.14. Passing to subsystems in this manner should make it clear, in case it needed to be stated, that a profinite group is not the limit of a *unique* inverse system. There may be many ways to achieve the same limit, so one must be careful when trying to compare two profinite groups through their inverse systems. We will return to this point later.

Chapter 2

Profinite groups

In this chapter we will establish some of the basics of group theory in the context of profinite groups, and begin to examine some examples. We will begin with the p-adic integers, which should be vaguely familiar from Metric and Topological Spaces.

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

Let p be a prime number. Consider the following inverse system of finite rings, indexed over $\mathbb{N}$ with its 'wrong-way' ordering.

$$\begin{tikzcd} \cdots \arrow[r] & \mathbb{Z}/p^{n+1}\mathbb{Z} \arrow[r] & \mathbb{Z}/p^n\mathbb{Z} \arrow[r] & \cdots \arrow[r] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r] & \mathbb{Z}/p\mathbb{Z} \end{tikzcd}$$

where the homomorphisms are the obvious 'reduce modulo p^n' maps. The *ring of p-adic integers* $\mathbb{Z}_p$ is defined to be the inverse limit of this system (in the category of rings). We also consider $\mathbb{Z}_p$ as an additive group—which is just the limit in the category of groups where we forget that multiplication is a thing we can do.

What is an element $\alpha \in \mathbb{Z}_p$? From the explicit description of inverse limit (Proposition 1.2.10), we can describe α as a sequence $(a_n)_{n\in\mathbb{N}}$ of integers modulo p^n such that $a_n \equiv a_m$ modulo p^m if $n \geq m$. Each a_n can be thought of as 'α modulo p^n', and is the image of α under the natural map $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ which we get from the definition of the limit. Addition and multiplication of elements is done 'component-wise'.

One way to get such sequences of elements is of course to choose some genuine integer $a \in \mathbb{Z}$ and let $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ be the reduction of a modulo p^n. This gives a map $\iota\colon \mathbb{Z} \to \mathbb{Z}_p$, $a \to \alpha = (a_n)_{n\in\mathbb{N}}$ (which is the same map as we get from the category-theoretic definition of inverse limit—the maps $\mathbb{Z} \to \mathbb{Z}/p^n$ constitute a cone on the inverse system).

This map ι is injective: if $a \in \mathbb{Z}$ and $p^n > |a|$ then a is not congruent to 0 modulo p^n, so $a_n \neq 0$ in $\mathbb{Z}/p^n$ and so $\iota(a) \neq 0$.

The p-adic integers have a natural metric described as follows. Let $\alpha = (a_n)$ and $\beta = (b_n)$ be elements of $\mathbb{Z}_p$. If $\alpha = \beta$ set $d(\alpha, \beta) = 0$ of course. Otherwise there is some smallest integer n such that $a_n \neq b_n$, and we set $d(\alpha, \beta) = p^{-n}$ for this smallest value of n. It is a quick exercise to check that this is actually a metric. The metric obtained by restricting d to $\iota(\mathbb{Z})$ gives the 'p-adic metric on the integers', which you have seen in Metric and Topological Spaces. In this topology, α and β are considered to be 'very close together' if you can only tell them apart modulo p^n for 'very large n'.

The open balls, say about 0 (the identity element of the additive group $\mathbb{Z}_p$), in this metric have a nice description.

$$\begin{aligned} B(0,r) &= \{\alpha = (a_n) \mid a_n = 0 \text{ for } n \leq -\log_p(r)\} \\ &= \ker\left(\mathbb{Z}_p \to \mathbb{Z}/p^{\lfloor -\log_p(r) \rfloor}\mathbb{Z}\right) \end{aligned}$$

So the open balls about 0 are the open subgroups $p^n\mathbb{Z}_p$ of $\mathbb{Z}_p$—the same ones we saw as a neighbourhood basis of the identity in Proposition 1.2.28.

Note that $\iota(\mathbb{Z})$ is *dense* in $\mathbb{Z}_p$: let $\alpha = (a_n) \in \mathbb{Z}_p$ and $\epsilon > 0$. Take $n > -\log_p(\epsilon)$ and choose some integer a such that $a \equiv a_n$ modulo p^n. Then $d(\alpha, \iota(a)) \leq p^{-n} < \epsilon$, proving the density of $\iota(\mathbb{Z})$.

The p-adic metric of the integers is not complete: a sequence of integers

$$a_n = 1 + p + p^2 + \cdots + p^n$$

is Cauchy, but doesn't converge to any element of $\mathbb{Z}$. It does however converge, almost tautologously, to an element of $\mathbb{Z}_p$: the element $\alpha = (a_n)$.

By contrast, the space of p-adic integers $\mathbb{Z}_p$ is complete. We already know it is a compact metric space, and therefore complete. We can also see this directly: let $\alpha^{(k)} = (a_n^{(k)})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ ($k \in \mathbb{N}$) be a Cauchy sequence of p-adics (with apologies for the breakdown in notation: the sequence of $\alpha^{(k)}$ is being indexed by k, and we want to show it converges to something as $k \to \infty$). What does being Cauchy mean in this context? Unpacking the definition, for each n we know there exists K_n such that for all $k, l \geq K_n$

$$d(\alpha^{(k)}, \alpha^{(l)}) \leq p^{-n}$$

That is, $a_n^{(k)} = a_n^{(l)}$ for all $k, l \geq K_n$. So for fixed n the sequence $a_n^{(k)}$ is eventually constant as $k \to \infty$. Let this constant value be $b_n \in \mathbb{Z}_p$, so that $a_n^{(k)} = b_n$ for all $k \geq K_n$.

It is easy to see that $\beta = (b_n)$ is a valid element of $\mathbb{Z}_p$, and the last statement of the paragraph above says $d(\alpha^{(k)}, \beta) \leq p^{-n}$ for $k \geq K_n$, hence $\alpha^{(k)} \to \beta$ as $k \to \infty$.

So $\mathbb{Z}_p$ is a complete metric space, containing a copy of $\mathbb{Z}$ as a dense subset. That is, $\mathbb{Z}_p$ is a *completion* of $\mathbb{Z}$. It is not the profinite completion of $\mathbb{Z}$, because we are missing some of the quotients $\mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}$ and are only looking at those quotients $\mathbb{Z}/p^n\mathbb{Z}$ which have order a power of the prime p. It is a different object, called the *pro-p completion* of $\mathbb{Z}$.

Course Convention 2.1.1. From now on we will drop the map ι from the notation and simply consider $\mathbb{Z}$ to be a subgroup of $\mathbb{Z}_p$.

Definition 2.1.2. Let p be a prime. A p-group is a finite group whose order is a power of p. A *pro-p group* is an inverse limit of an inverse system of p-groups.

Definition 2.1.3 (Pro-p completion)**.** Let G be a group and let p be a prime. The set of normal subgroups N of G such that G/N is a finite p-group form a poset N_p under inclusion. We have a functor $\mathsf{N}_p \to \mathsf{Grps}$ defined by sending N to G/N, and with arrows $G/N_1 \to G/N_2$ being the natural quotient maps if $N_1 \subseteq N_2$. The *pro-p completion of G* is the inverse limit of the system of groups $(G/N)_{N\in\mathsf{N}_p}$.

Pro-p completions are similar in many ways to profinite completions, and one may ask why we bother to study both. One answer is that they are useful for different things: profinite completions contain a lot more information in general (for instance, in the profinite completion of $\mathbb{Z}$ we have concepts of 'odd and even', because we have the quotient $\widehat{\mathbb{Z}} \to \mathbb{Z}/2\mathbb{Z}$, but in the 3-adic completion $\mathbb{Z}_3$ 'odd and even' are meaningless concepts), but are often more tricky to work with. As we shall see through this course, finite p-groups are much better behaved than general finite groups[1], and this niceness carries over to pro-p groups to some extent. We will see a first example of bad behaviour shortly, when we compare $\mathbb{Z}_p$ with the profinite completion $\widehat{\mathbb{Z}}$.

Before moving on we will study a few of the elementary properties of $\mathbb{Z}_p$ as a group or ring, which will illustrate neatly how a profinite group may share some properties with finie groups and some with infinite groups.

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

Proof. Being abelian derives immediately from the fact that all the groups $\mathbb{Z}/p^n\mathbb{Z}$ are abelian, hence so is the product $\prod \mathbb{Z}/p^n\mathbb{Z}$ of which $\mathbb{Z}_p$ is a subgroup.

Torsion-freeness may be more surprising for a limit of finite groups. Let $\alpha = (a_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p \smallsetminus \{0\}$ and suppose we have $m \in \mathbb{N}$ such that $m\alpha = 0$ (recall that we are using additive notation for this group). We wish to show $m = 0$; assume that it is not. Then let $m = p^r s$ where s is coprime to p. We have $ma_n = 0$ for all n by definition.

Choose some N such that $a_N \neq 0$ and consider a_{N+r}. We have $ma_{N+r} \equiv 0$ modulo p^{N+r}, i.e. $p^{N+r} \mid p^r s a_{N+r}$. Hence $p^N \mid a_{N+r}$ since s is coprime to p. This implies that $a_{N+r} \equiv 0$ modulo p^N, a contradiction since $a_{N+r} \equiv a_N$ modulo p^N. □

Another way that $\mathbb{Z}_p$ behaves more like $\mathbb{Z}$ than like the finite rings $\mathbb{Z}/p^n$ is that it has no zero-divisors. The following argument is a slight expansion of torsion-freeness in this case.

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

Proof. Exercise. □

However, $\mathbb{Z}_p$ differs from $\mathbb{Z}$ in a highly significant way: it has many different generators. Only $+1$ and -1 generate $\mathbb{Z}$ as an abelian group, which in some circumstances may thus be slightly inflexible. However the finite groups $\mathbb{Z}/p^n$ have many generators, and this property carries over to $\mathbb{Z}_p$. We will discuss this later once we have defined properly what 'generator' means in the context of a topological group.

[1] Except the prime 2. No one likes 2.

2.2 The profinite completion of the integers

Of course, if we want to study profinite completions of groups, we ought start with the integers. One can carry out various analyses of $\widehat{\mathbb{Z}}$ in the fashion of the previous section on the p-adics (and some of these make good exercises). The study of $\widehat{\mathbb{Z}}$ can however be reduced to the study of the p-adics by the following proposition.

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 may be written as a product of prime powers

$$n = \prod_{p \text{ prime}} p^{e_p(n)}$$

(where all but finitely many e_p will be zero). The classical Chinese Remainder Theorem gives a canonical isomorphism

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow[f_n]{\cong} \prod_{p \text{ prime}} \mathbb{Z}/p^{e_p(n)}\mathbb{Z}$$

These maps are compatible with the quotient maps $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, in the sense that all the natural diagrams

$$\begin{tikzcd}
\mathbb{Z}/mn\mathbb{Z} \arrow[r, "\cong", "f_{mn}"'] \arrow[d] & \prod_{p \text{ prime}} \mathbb{Z}/p^{e_p(mn)}\mathbb{Z} \arrow[d] \\
\mathbb{Z}/n\mathbb{Z} \arrow[r, "\cong", "f_n"'] & \prod_{p \text{ prime}} \mathbb{Z}/p^{e_p(n)}\mathbb{Z}
\end{tikzcd}$$

commute. Passing to inverse limits gives an isomorphism

$$\widehat{\mathbb{Z}} \cong \varprojlim_{n \in \mathbb{N}} \prod_{p \text{ prime}} \mathbb{Z}/p^{e_p(n)}\mathbb{Z}.$$

It remains to show that the inverse limit on the right really is $\prod_p \mathbb{Z}_p$. For this, note that the natural continuous surjections $\prod_p \mathbb{Z}_p \twoheadrightarrow \prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z}$ form a cone, hence we have a homomorphism

$$f\colon \prod_p \mathbb{Z}_p \to \varprojlim_{n \in \mathbb{N}} \prod_{p \text{ prime}} \mathbb{Z}/p^{e_p(n)}\mathbb{Z}.$$

This is continuous by Proposition 1.2.25 and surjective by Corollary 1.2.31. Further, f is injective because every non-trivial element of $\prod \mathbb{Z}_p$ is non-trivial in some quotient $\mathbb{Z}/p^e\mathbb{Z}$ for some p and e. Hence f is a topological isomorphism as required. □

Alternative proof. Firstly, we have a continuous homomorphism from $\widehat{\mathbb{Z}}$ to each $\mathbb{Z}_p$: the (continuous) projection maps $\widehat{\mathbb{Z}} \to \mathbb{Z}/p^n$ constitute a cone on the inverse system $(\mathbb{Z}/p^n\mathbb{Z})$, so the definition of the limit yields a natural homomorphism $\widehat{\mathbb{Z}} \to \mathbb{Z}_p$. This homomorphism is continuous by Proposition 1.2.25.

The universal property of the product then gives a continuous homomorphism $f\colon \widehat{\mathbb{Z}} \to \prod \mathbb{Z}_p$.

To show that f is surjective, it is enough to show that $\operatorname{im}(f)$ is dense in the product: for $\widehat{\mathbb{Z}}$ is compact, hence its image is compact and thus closed. By the definition of the product topology, and our known bases for the $\mathbb{Z}_p$, a basic open set in $\prod \mathbb{Z}_p$ takes the form

$$U = (x_1 + p_1^{n_1}\mathbb{Z}_{p_1}) \times \cdots \times (x_r + p_r^{n_r}\mathbb{Z}_{p_r}) \times \prod_{q \neq p_i} \mathbb{Z}_q$$

Hence to establish density of f, it is enough to show that the compositions

$$\widehat{\mathbb{Z}} \to \prod \mathbb{Z}_p \to \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}$$

are all surjective. But by the classical Chinese Remainder Theorem we have a commuting diagram

$$\begin{tikzcd}
\widehat{\mathbb{Z}} \arrow[r] \arrow[d] & \prod_{p \text{ prime}} \mathbb{Z}_p \arrow[d] \\
\mathbb{Z}/m\mathbb{Z} \arrow[r, "\cong"] & \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}
\end{tikzcd}$$

where $m = p_1^{n_1} \cdots p_r^{n_r}$. Since the natural map $\widehat{\mathbb{Z}} \to \mathbb{Z}/m\mathbb{Z}$ is surjective, we can conclude that f is indeed surjective.

To show that f is injective, let $g \in \widehat{\mathbb{Z}} \smallsetminus \{0\}$. Then there exists $m \in \mathbb{Z}$ such that g does not vanish under the natural map to $\mathbb{Z}/m\mathbb{Z}$. Taking a prime factorisation $m = p_1^{n_1} \cdots p_r^{n_r}$, the same commuting diagram as above shows that g maps to a non-trivial element of $\prod \mathbb{Z}_p$ as required. □

Corollary 2.2.2. *The group $\widehat{\mathbb{Z}}$ is torsion-free abelian.*

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

Proof. This is an example of the standard fact that any product of non-trivial rings $R_1 \times R_2$ has zero-divisors, viz. $(r_1, 0) \cdot (0, r_2) = 0$. In the case of $\widehat{\mathbb{Z}}$, a non-zero element α is a zero-divisor if and only if the projection of α to $\mathbb{Z}_p$ is zero for some prime p. □

2.3 Profinite matrix groups

A somewhat more intersting family of profinite groups (and the first nonabelian ones we will consider) are matrix groups over the rings $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}}$. For any commutative ring R we are entitled to consider a set of matrices

$$\mathrm{Mat}_{N\times M}(R) = \{N \times M \text{ matrices of elements of } R\}$$

with addition and multiplication defined by the same formulae as for real matrices. Since it is obtained by a formula consisting of multiplications and additions—that is, ring operations—we also have a determinant function

$$\det\colon \mathrm{Mat}_{N\times N}(R) \to R$$

Let us first discuss $\mathbb{Z}_p$. The set of matrices acquires an obvious topology—either by writing it as an inverse limit

$$\mathrm{Mat}_{N\times M}(\mathbb{Z}_p) = \varprojlim \mathrm{Mat}_{N\times M}(\mathbb{Z}/p^n\mathbb{Z})$$

or by using the obvious bijection with $\mathbb{Z}_p^{NM}$. Since the ring multiplication on $\mathbb{Z}_p$ is continuous, it follows that matrix multiplication is continuous too, as is the determinant function.

Linear algebra over $\mathbb{Z}_p$ is in many ways similar to linear algebra over $\mathbb{Z}$. (Indeed most of the point of linear algebra is that the base ring/field is rather irrelevant). Since $\mathbb{Z}_p$ is an integral domain, it has a field of fractions $\mathbb{Q}_p$ (of which you will see some properties on the example sheet) and any results about linear algebra not requiring any special properties of a field will apply to matrices over $\mathbb{Q}_p$. In particular, any square matrix over $\mathbb{Q}_p$ has an inverse over $\mathbb{Q}_p$ if and only if its determinant is non-zero. Since the formula for an inverse is the same as over $\mathbb{Q}$ and involves dividing by a determinant, if the matrix has coefficients in $\mathbb{Z}_p$ then the inverse has coefficients in $\mathbb{Z}_p$ as well if and only if the determinant is an invertible element of $\mathbb{Z}_p$. So we can define two families of topological groups

$$\begin{aligned}\mathrm{GL}_N(\mathbb{Z}_p) &= \left\{A \in \mathrm{Mat}_{N\times N}(\mathbb{Z}_p) \mid \det A \in \mathbb{Z}_p^\times\right\}\\ \mathrm{SL}_N(\mathbb{Z}_p) &= \{A \in \mathrm{Mat}_{N\times N}(\mathbb{Z}_p) \mid \det A = 1\}\end{aligned}$$

Both of these are profinite groups, and are of course given by appropriate inverse limits

Lemma 2.3.1. *For all $N \geq 1$ and each prime p we have*

$$\begin{aligned}\mathrm{GL}_N(\mathbb{Z}_p) &= \varprojlim \mathrm{GL}_N(\mathbb{Z}/p^n\mathbb{Z})\\ \mathrm{SL}_N(\mathbb{Z}_p) &= \varprojlim \mathrm{SL}_N(\mathbb{Z}/p^n\mathbb{Z})\end{aligned}$$

Proof. The determinant functions commute with quotients modulo p^n: there is a commutative diagram

$$\begin{tikzcd}\mathrm{Mat}_{N\times N}(\mathbb{Z}_p) \arrow[r] \arrow[d, "\det"] & \mathrm{Mat}_{N\times N}(\mathbb{Z}/p^n\mathbb{Z}) \arrow[d, "\det"] \\ \mathbb{Z}_p \arrow[r] & \mathbb{Z}/p^n\mathbb{Z}\end{tikzcd}$$

The desired statements now follow from the known fact, for a matrix A over $\mathbb{Z}_p$, that $\det A$ is invertible over $\mathbb{Z}_p$ (respectively, equals 1) if and only if it is invertible modulo each p^n (respectively, equals 1 modulo each p^n). □

We can also define matrices over $\widehat{\mathbb{Z}}$, although one should be a little circumspect since this is not an integral domain. We do however have $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, so the matrix groups split as well:

$$\mathrm{Mat}_{N\times M}(\widehat{\mathbb{Z}}) = \prod_p \mathrm{Mat}_{N\times M}(\mathbb{Z}_p)$$

This reduces most questions about these matrices to questions about matrices over $\mathbb{Z}_p$. We can of course also define general and special linear groups, and these too will be inverse limits and products

$$\begin{aligned} \mathrm{GL}_N(\widehat{\mathbb{Z}}) &= \varprojlim \mathrm{GL}_N(\mathbb{Z}/n\mathbb{Z}) = \prod_p \mathrm{GL}_N(\mathbb{Z}_p) \\ \mathrm{SL}_N(\widehat{\mathbb{Z}}) &= \varprojlim \mathrm{SL}_N(\mathbb{Z}/n\mathbb{Z}) = \prod_p \mathrm{SL}_N(\mathbb{Z}_p) \end{aligned}$$

We will mainly deal with the special linear groups $\mathrm{SL}_N(\mathbb{Z}_p)$ and $\mathrm{SL}_N(\widehat{\mathbb{Z}})$, since they are more closely related to the classical group $\mathrm{SL}_N(\mathbb{Z})$. Of course the natural inclusions $\mathbb{Z} \subseteq \mathbb{Z}_p$, $\mathbb{Z} \subseteq \widehat{\mathbb{Z}}$ give us inclusions

$$\mathrm{SL}_N(\mathbb{Z}) \subseteq \mathrm{SL}_N(\mathbb{Z}_p), \quad \mathrm{SL}_N(\mathbb{Z}) \subseteq \mathrm{SL}_N(\widehat{\mathbb{Z}})$$

These subgroups are in fact dense, a fact you will prove on the Exercise Sheets. It is less obvious than it may look: density in $\mathrm{SL}_N(\widehat{\mathbb{Z}})$ is equivalent to the surjectivity of the maps

$$\mathrm{SL}_N(\mathbb{Z}) \to \mathrm{SL}_N(\mathbb{Z}/n\mathbb{Z})$$

and it is far from clear why, for example,

$$\begin{pmatrix} 7 & 9 \\ 4 & 9 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/13\mathbb{Z})$$

is the modulo 13 reduction of any integer matrix of determinant 1.

2.4 Subgroups, quotients and homomorphisms

Just as with ordinary group theory, one wants to consider subgroups. For a topological group it makes most sense to study those subgroups which behave sensibly with regard to the topology: i.e. which are closed or open subsets.

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

Proof. Let $G = \varprojlim G_j$ be a profinite group and let H be a closed subgroup of G. Define an inverse system of finite groups $(H_j)_{j \in J}$ by $H_j = p_j(H) \leq G_j$, and with transition maps being the restrictions of the transition maps $\phi_{ij} \colon G_i \to G_j$. The inverse limit of the H_j is a profinite group H', which is clearly equal to

$$\left\{ (g_j)_{j \in J} \in \prod_{j \in J} G_j \text{ such that } g_j \in H_j \ \forall j \text{ and } \phi_{ij}(g_i) = g_j \text{ for all } i \preceq j \right\}.$$

It remains to show that $H' = H$. By definition of H_j, if $h \in H$ then $h \in H'$.

Suppose $g = (g_j) \notin H$. Since H is closed, $G \smallsetminus H$ is an open subset of G. By Corollary 1.2.29, there is some j such that $p_j^{-1}(g_j) \subseteq G \smallsetminus H$. It follows that $p_j(h) \neq g_j$ for all $h \in H$, i.e. $g_j \notin H_j$. So $g \notin H'$, and we conclude that $H = H'$. □

Remark 2.4.2. It is reassuring to note that the topology on H coming from its expression as $\varprojlim H_j$ is the same as the subspace topology induced on it by G: Proposition 1.2.25 shows that the natural map

$$\mathrm{id} \colon (H, \mathcal{T}_{\mathrm{profinite}}) \to (H, \mathcal{T}_{\mathrm{subspace}})$$

is continuous, whence it is a homeomorphism since the profinite topology is compact and the subspace topology is Hausdorff.

Although we did not use it above to avoid leading the witness, a better notation for H' would be $\overline{H}$. The second paragraph of the proof above actually shows that H' is contained in the closure of H in G: in our case we have the hypothesis that H is closed, so the closure is just H itself. In fact H' is equal to the closure of H in G regardless of whether H is closed: since $H \subseteq H' \subseteq \overline{H}$, we need only show that H' is closed; but it is the intersection of the closed subgroups $p_j^{-1}(H_j)$. We decant this into a separate statement for later reference.

Proposition 2.4.3. *Let $G = \varprojlim G_j$ be a profinite group and let H be a subgroup of G. Set $H_j = p_j(H) \leq G_j$. Then the closure of H in G is $\overline{H} = \varprojlim H_j$. In particular, if H is closed then $H = \varprojlim H_j$.*

We also note that the index of a closed subgroup of a profinite group may be readily determined from the inverse system.

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

Proof. Elementary exercise. □

Proposition 2.4.5. *Let $G = \varprojlim G_j$ be a profinite group, where (G_j) is a surjective inverse system of finite groups. Let H be a closed subgroup of G and let H_j be the image of H in G_j. Then H is finite index in G if and only if $[G_i : H_i]$ is constant on some cofinal subsystem $I \subseteq J$. In this case we have $[G : H] = [G_i : H_i]$ where $i \in I$.*

Proof. Since the projections $p_j\colon G \to G_j$ are surjective, it follows that $[G : H] \geq [G_j : H_j]$ for all $j \in J$.

Suppose $[G : H] \geq N$ for some $N \in \mathbb{N}$—so that there are representatives $g_1, \ldots, g_N$ of distinct right cosets g_nH of H in G. Then the elements $g_m^{-1}g_n$, for $n \neq m$, lie outside the closed subgroup H. For each $g_m^{-1}g_n$ there is then some $j_{m,n}$ such that $p_{j_{m,n}}(g_m^{-1}g_n) \notin H_{j_{m,n}}$. Taking some k such that $k \preceq j_{m,n}$ for all $m \neq n$ we find $p_k(g_m^{-1}g_n) \notin H_k$ for all $m \neq n$. Then the elements $p_k(g_n)$ represent different cosets of H_k, so that $[G_k : H_k] \geq N$. For any i in the principal cofinal subsequence $J_{\preceq k} = \{i \preceq k\}$ of J, it follows that $[G_i : H_i] \geq [G_k : H_k] \geq N$ also.

We may now conclude the result. If $[G : H] = N$ is finite, then we have some k such that

$$[G : H] \geq [G_i : H_i] \geq N = [G : H]$$

for all $i \preceq k$.

On the other hand, assume that $[G : H]$ is infinite and that $[G_i : H_i] = N$ is constant on some cofinal subsystem $I \subseteq J$. From above, since $[G : H] \geq N + 1$ we can find a k such that $[G_k : H_k] \geq N + 1$. But there is some $i \in I$ with $i \preceq k$, so we have a contradiction:

$$[G_i : H_i] \geq [G_k : H_k] \geq N + 1 > N = [G_i : H_i]$$

□

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

Proof. Let $G = \varprojlim G_j$ be a surjective inverse limit of finite groups. Let $p_j \colon G \to G_j$ be the projections and let $\phi_{ij} \colon G_i \to G_j$ be the transition maps. Let $N_j = p_j(N)$ and recall that we can identify N with $\varprojlim N_j$.

Noting that N_j is normal subgroup of G_j, set $Q_j = G_j/N_j$. Since $\phi_{ij}(N_i) = N_j$ the transition maps define give homomorphisms $\psi_{ij} \colon Q_i \to Q_j$ which make the Q_j into an inverse system. Let $Q = \varprojlim Q_j$ be the inverse limit. We claim that Q is topologically isomorphic to the group G/N (equipped with the quotient topology).

The natural map $\prod G_j \to \prod Q_j$ (which is continuous because each map of discrete sets $G_j \to Q_j$ is continuous) restricts to a continuous group homomorphism $f \colon G \to Q$. If $g = (g_j) \in G$ then $f(g) = 1$ if and only if $g_j \in N_j$ for all j—that is, the kernel of f is N. By the first isomorphism theorem for groups there is a group isomorphism $\bar{f} \colon G/N \to Q$. Because f is continuous, $\bar{f}$ is continuous by definition of the quotient topology on G/N. Being the image of the compact set G, the space G/N is compact. The profinite group Q is Hausdorff, so it follows that $\bar{f}$ is a homeomorphism as well as a group isomorphism. □

The final three sentences of this proof constitute a proof of the 'first isomorphism theorem for profinite groups'.

Proposition 2.4.7 (First Isomorphism Theorem)**.** *Let G and Q be profinite groups and let $f \colon G \to Q$ be a continuous surjective group homomorphism. Let $G/\ker(f)$ have the quotient topology and let $q \colon G \to G/\ker(f)$ be the quotient map. Then there exists a topological isomorphism $\bar{f} \colon G/\ker(f) \to Q$ such that $\bar{f}q = f$.*

In both Proposition 2.4.1 and Proposition 2.4.6 we saw continuous homomorphisms between profinite groups which arise as *morphisms of inverse systems*—that is, as families of maps between the finite groups in the inverse system.

Definition 2.4.8. Let $(G_j)_{j\in J}$ and $(H_j)_{j\in J}$ be inverse systems of finite groups indexed by the same poset J. Let the transition maps for G_j and H_j be ϕ^G_{ij} and ϕ^H_{ij} respectively.

A *morphism of inverse systems* $(f_j) \colon (G_j) \to (H_j)$ is a family of group homomorphisms $f_j \colon G_j \to H_j$, such that for all $i \preceq j$ we have $f_j \circ \phi^G_{ij} = f_i \circ \phi^H_{ij}$.

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

Proposition 2.4.9. *Let $(f_j) \colon (G_j) \to (H_j)$ be a morphism of inverse systems of finite groups. There is a unique continuous homomorphism $f \colon \varprojlim G_j \to \varprojlim H_j$ such that $p^H_j f = f_j p^G_j$, where $p^G_j \colon G \to G_j$ and $p^H_j \colon H \to H_j$ are the projection maps.*

Proof. The maps $f_j p^G_j \colon G \to H_j$ make G into a cone on the diagram (H_j), so by definition of inverse limit there is a unique homomorphism $G \to H$ with the desired properties. It is continuous by Proposition 1.2.26. □

Remark 2.4.10. We refer to such a map f as *induced by* the morphism of inverse systems. We may write $f = \varprojlim f_j$.

Of course, it is perfectly possible to have continuous homomorphisms between profinite groups which are given as inverse limits over completely different inverse systems. Even if the inverse systems are the same, it is not the case that every continuous homomorphism arises from a morphism of inverse systems. However, if we allow ourselves the flexibility of passing to cofinal subsystems, we will be able to treat homomorphisms as if they come from morphisms of inverse systems.

Proposition 2.4.11. *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 surjective inverse systems with no global minimum. Let $f\colon G \to H$ be a continuous homomorphism. Then there are cofinal subsystems J' and I' of J and I respectively, an order-preserving bijection $J' \cong I'$, and a morphism of inverse systems $(f_j)\colon (G_j)_{j\in J'} \to (H_i)_{i\in I'}$ inducing f.*

Proof. By Proposition 1.3.11 we may assume that both J and I are linearly ordered. Without loss of generality therefore assume I and J are $\mathbb{N}$ with the wrong-way ordering. Construct an increasing sequence (k_n) of natural numbers as follows; this will be the desired cofinal subsystem of J. Each map $G \to H \to H_n$ is a continuous homomorphism, whose kernel is thus an open neighbourhood of the identity of G. By Proposition 1.2.28 there exists k_n such that $\ker(G \to G_{k_n}) \subseteq \ker(G \to H_n)$—whence the homomorphism f descends to a homomorphism $f_n\colon G_{k_n} \to H_n$. Since the kernels $\ker(G \to G_m)$ are a nested sequence, we may assume that $k_n \geq k_{n-1}$. The sequence $J' = \{k_n\}_{n\in\mathbb{N}}$ gives a cofinal subsystem of J, and the f_n are the required morphism of inverse systems. □

Remark 2.4.12. The assumption that the inverse systems are countable is actually necessary to make this proposition work as stated, rather than just being a simplifying assumption. For example, if I were countable and the profinite group G were a profinite group which is not metrisable as a topological space—for example a product of uncountably many copies of $\mathbb{Z}/2\mathbb{Z}$—then there is no countable cofinal subsystem of J, since all profinite groups given as limits of countable systems of finite groups are metrisable by Proposition 1.2.15.

2.5 Generators of profinite groups

Definition 2.5.1. Let G be a topological group and let S be a subset of G. We say that S is a *(topological) generating set* for G if the subgroup $\langle S\rangle$ generated by S is a dense subgroup of G. The group G is *(topologically) finitely generated* if it has a finite topological generating set.

Remark 2.5.2. It is fairly common to be lazy and omit the word ‘topologically’, especially with regard to finite generation. This may be justified (at least for profinite groups) on the grounds that the only profinite groups which are genuinely finitely generated (so that $\langle S\rangle$ equals G, and is not merely dense in it) are the finite groups, so ‘a finitely generated profinite group’ can only really mean ‘a topologically finitely generated group’ within the bounds of sense. If it happens that, for some strange reason, we want to consider the usual notion of generation we may talk of, for example, ‘abstractly finitely generated’—meaning that we consider only the abstract group structure and forget that there is any topology to worry about.

Definition 2.5.3. Let G be a toplogical group and let $S \subseteq G$. The *closed subgroup of G (topologically) generated by S* is the smallest closed subgroup of G containing S. It is denoted by $\overline{\langle S\rangle}$.

The notation is justified by the following easy observation.

Proposition 2.5.4. *Let G be a topological group and let H be a subgroup. Then the closure of H in G is also a subgroup. Hence the closed subgroup of G topologically generated by a subset S is the closure of the subgroup $\langle S\rangle$ abstractly generated by S.*

Proof. Exercise. □

Lemma 2.5.5. *Let Γ be a finitely generated group and let H be a finite index subgroup of Γ. Then H is finitely generated.*

Proof (non-examinable). Let $x_1, \ldots, x_n$ be a generating set of Γ. For each left coset Hg of H in Γ choose some $s_{Hg} \in \Gamma$ such that $gs_{Hg} \in H$, and such that $s_{H1} = 1$. Note that the condition $gs_{Hg} \in H$ is independent of the coset representative g of Hg. We claim that the finite set S=

$$\{s_{Hg}^{-1}x_i^{\pm 1}s_{Hg'} : Hg \in H\backslash G, Hg' = Hs_{Hg}^{-1}x_i^{\pm 1}\}$$

generates H.

Let $h \in H$. Since h is an element of Γ, we may write it as a product $h = a_1 \cdots a_r$ where each a_r is of the form $x_i^{\pm 1}$. Define left cosets Hg_i inductively for $0 \leq i \leq r$, such that that $g_0 = 1$ and for all $i \geq 1$ we have

$$s_{Hg_{i-1}}^{-1}a_i s_{Hg_i} \in H.$$

We then have an expression

$$h = a_1 \cdots a_r = s_{Hg_0}\prod_{i=1}^{r}\big(s_{Hg_{i-1}}^{-1}a_i s_{Hg_i}\big)s_{Hg_r}^{-1}.$$

By construction $s_{Hg_0} = 1$. We must also have $s_{Hg_r} = 1$ because every other term in the above expression lies in H, so $s_{Hg_r} \in H$, hence $g_r \in H$ and $s_{Hg_r} = s_H = 1$. We have thus written h as a product of terms from S, and we are done. □

Proposition 2.5.6. *If G is a topologically finitely generated profinite group 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 a finite index subgroup of $\langle S\rangle$, hence is finitely generated. Since U is open and $\langle S\rangle$ is dense in G, it follows that Γ is dense in U. Hence U has a finitely generated dense subgroup, so is topologically finitely generated. □

As one should really be expecting by this point, generation in profinite groups is determined by the behaviour of finite quotients.

Proposition 2.5.7. *Let $(G_j)_{j\in J}$ be a surjective inverse system of finite groups, with inverse limit G and projection maps $p_j\colon G \to G_j$. Then a subset $S \subseteq G$ is a topological generating set for G if and only if $p_j(S)$ (abstractly) generates G_j for all j.*

Proof. By Corollary 1.2.30, $\langle S\rangle$ is dense in G if and only if $G_j = p_j(\langle S\rangle) = \langle p_j(S)\rangle$ for all $j \in J$—i.e. when $p_j(S)$ abstractly generates G_j for all $j \in J$. □

Lemma 2.5.8. *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; for the image of S determines the image of $\langle S\rangle$, whence of G by continuity. There are only countably many functions from S to a finite symmetric group $\mathrm{Sym}(n)$, so G has at most countably many open subgroups U. The open subgroups of G form a neighbourhood base of the identity, hence by Proposition 1.2.33 we have $G \cong \varprojlim G/U$. □

Example 2.5.9. One specific way of writing a topologically finitely generated profinite group G as the inverse limit of a countable inverse system—indeed, a linearly ordered system—will appear several times in this course. Let G_n be the intersection of all open subgroups of G with index at most n. For each n there are only finitely many open subgroups of G with index at most n: just as in Lemma 1.2.18 they are in correspondence with the continuous homomorphisms $G \to \mathrm{Sym}(n)$, and since G is topologically finitely generated there are only finitely many of these. Then G_n is an open subgroup of G, being the intersection of only finitely many open subgroups.

The system $\{G_n\}$ is clearly cofinal in the system of all open subgroups U of G. In the above lemma we saw that $G = \varprojlim G/U$, so passing to the cofinal subsystem we also have $G = \varprojlim G/G_n$.

Profinite groups have a tendency to have huge numbers of potential generating sets. Let us start by examining the p-adic integers $\mathbb{Z}_p$.

Proposition 2.5.10. *Let $\mathbb{Z}_p^\times$ be the set of elements of $\mathbb{Z}_p$ which topologically generate $\mathbb{Z}_p$. Then $\alpha \in \mathbb{Z}_p^\times$ if and only if $\alpha \not\equiv 0$ modulo p.*

In particular, $\mathbb{Z}_p^\times$ is a closed uncountable subset of $\mathbb{Z}_p$ and for every n and every generator $a_n \in \mathbb{Z}/p^n$ there is some $\alpha \in \mathbb{Z}_p^\times$ such that $\alpha \equiv a_n$ modulo p^n.

Proof. If $\alpha = (a_n)$ has $a_1 \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ then $p \nmid a_n$ for any n. Hence a_n is coprime to p and thus is a generator of $\mathbb{Z}/p^n\mathbb{Z}$ for all n. It follows that α topologically generates $\mathbb{Z}_p$. □

Remark 2.5.11. The notation $\mathbb{Z}_p^\times$ is of course derived from the ring theory: the generators here are the invertible elements of the ring $\mathbb{Z}_p$. To see this, let α be a generator of $\mathbb{Z}_p$ and consider the map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ given by ring multiplication $x \mapsto \alpha x$. This is continuous since $\mathbb{Z}_p$ is a topological ring in the obvious way. The image of f includes αn for all $n \in \mathbb{Z}$, (that is, the abstract subgroup generated by α) and is closed since it's the image of the compact set $\mathbb{Z}_p$ under the continuous map f. Since α generates $\mathbb{Z}_p$, the smallest closed subgroup containing it is $\mathbb{Z}_p$ itself. So f is surjective and in particular there is some $\beta \in \mathbb{Z}_p$ such that $\alpha\beta = 1$.

Remark 2.5.12. This proposition means, of course, that many elements of $\mathbb{Z}$ are invertible in $\mathbb{Z}_p$. For example if $p \neq 2$ then 2 generates $\mathbb{Z}_p$ and hence an element $2^{-1} \in \mathbb{Z}_p$ exists. It may be instructive to consider what this element looks like, for $p = 3$ for instance. $2^{-1} \in \mathbb{Z}_3$ consists of a sequence of integers $a_n \in \mathbb{Z}/3^n\mathbb{Z}$ such that $2a_n \equiv 1$ modulo 3^n. This sequence is uniquely determined (since multiplication by 2 is a bijection $\mathbb{Z}/3^n \to \mathbb{Z}/3^n$ for all n). So 2^{-1} looks like the sequence

$$2^{-1} = (\dots, 122, 41, 14, 5, 2) \in \mathbb{Z}_3 \subseteq \prod_{n=1}^{\infty} \mathbb{Z}/3^n\mathbb{Z}$$

Proposition 2.5.13. *For every n and every $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ there exists an generator $\kappa \in \widehat{\mathbb{Z}}^\times$ of $\widehat{\mathbb{Z}}$ such that $\kappa \equiv k$ modulo n.*

Proof. Follows from the previous proposition via the Chinese Remainder Theorem. □

The 'for every n' part of Proposition 2.5.10—that generators of finite quotients lift to generators of the profinite group—will now be extended more widely in the powerful shape of Gaschutz's Lemma. It is of course dramatically far from being true for abstract groups. The integers $\mathbb{Z}$ have a paltry two generators ±1, and cannot even lift all the generators of $\mathbb{Z}/5\mathbb{Z}$.

Theorem 2.5.14 (Gaschutz's Lemma (Finite groups))**.** *Let $f\colon G \to H$ be a surjective homomorphism where G is a finite group. Assume that G has some generating set of size d. Then for any generating set $\{z_1, \dots, z_d\}$ of H there exists some generating set $\{x_1, \dots, x_d\}$ of G such that $f(x_i) = z_i$ for all i.*

Proof. It is convenient for this proof to speak of 'generating vectors' $\underline{x} = (x_1, \dots, x_d) \in G^d$ for G—that is, ordered generating sets rather than unordered generating sets. We extend f to the obvious map $G^d \to H^d$ and continue to denote this by f.

We will prove, by induction on $|G|$ (and for H fixed), the following statement $(*)$.

> The number $N_G(\underline{y})$ defined by
>
> $$(*) \qquad N_G(\underline{y}) = \#\big(\text{Generating vectors } \underline{x} \text{ of } G \text{ such that } f(\underline{x}) = \underline{y}\big)$$
>
> is independent of $\underline{y}$, where $\underline{y} \in H^d$ is a generating vector for H.

The theorem follows from this at once: G has *some* generating vector $\underline{x}'$, so $N_G(f(\underline{x}')) \geq 1$; hence $N_G(\underline{z}) \geq 1$ for the given $\underline{z} = (z_1, \dots, z_d)$ as well.

Let $\underline{y} \in H^d$ be a generating vector for H and let $\mathcal{C}$ be the set of d-generator proper subgroups of G. Every $\underline{x} \in G^d$ with $f(\underline{x}) = \underline{y}$ either generates G or generates some proper subgroup $C \in \mathcal{C}$: hence

$$|\{\underline{x} \text{ such that } f(\underline{x}) = \underline{y}\}| = N_G(\underline{y}) + \sum_{C \in \mathcal{C}} N_C(\underline{y})$$

Furthermore we have

$$|\{\underline{x} \text{ such that } f(\underline{x}) = \underline{y}\}| = |\ker(f)|^d$$

so that

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

Every term on the right-hand side is independent of $\underline{y}$ by the inductive hypothesis. So $N_G(\underline{y})$ is independent of $\underline{y}$ too and the proof is complete. □

By 'the standard inverse limit argument', this will apply to profinite groups as well.

Theorem 2.5.15 (Gaschutz's Lemma (Profinite groups)). *Let $f\colon G \to H$ be a continuous surjective homomorphism where G and H are profinite groups. Assume that G has some topological generating set of size d. Then for any topological generating set $\{z_1, \dots, z_d\}$ of H there exists some topological generating set $\{x_1, \dots, x_d\}$ of G such that $f(x_i) = z_i$ for all i.*

Proof. By Propositions 1.3.7 and 2.4.11 we may assume that G and H are written as surjective inverse limits of finite groups

$$G = \varprojlim_{j \in J} G_j, \quad H = \varprojlim_{j \in J} H_j$$

with a morphism of inverse systems

$$(f_j)\colon (G_j) \to (H_j)$$

with inverse limit f and with each f_j a surjective group homomorphism.

Let $\underline{z}$ be some given generating vector of H, and let $\underline{z}_j$ be its image in H_j^d—which is a generating vector for H_j. Consider the finite sets

$$X_j = \{\text{Generating vectors } \underline{x}_j \in G_j^d \text{ such that } f_j(\underline{x}_j) = \underline{z}_j\}$$

which are non-empty by the first version of Gaschutz's Lemma. The transition maps $\phi_{ij}\colon G_i \to G_j$ map X_i to X_j, so the X_j are an inverse system of non-empty finite sets. The inverse limit of these is non-empty by Proposition 1.2.14; and an element of the inverse limit is a generating vector for G which maps to $\underline{z}$ as required. □

Chapter 3

Profinite Completions

3.1 Residual finiteness

Remark 3.1.1 (Remark on terminology and notation)*.* This chapter will involve both profinite groups and the more familiar 'normal' groups—the 'abstract' groups. Abstract groups are also sometimes called 'discrete' groups to signify that they are not usually considered to have any interesting topology on them. I will try to use 'abstract' consistently, but may slip into 'discrete' from force of habit. I consider 'discrete' to be potentially misleading since the 'discrete' groups do actually have a topology on them to consider: the topology induced from the map to the profinite completion.

Let us recall what we have already seen of profinite completions.

Given an abstract group Γ, we can form an inverse system from its finite quotients: the elements of this inverse system are the groups Γ/N where $N \lhd_f \Gamma$ is a finite index normal subgroup of Γ; and the maps of this inverse system are the natural quotient maps $\Gamma/N_1 \to \Gamma/N_2$ where $N_1 \subseteq N_2$.

The inverse limit $\widehat{\Gamma} = \varprojlim \Gamma/N$ is the *profinite completion* of Γ. It comes with a canonical group homomorphism $\iota\colon \Gamma \to \widehat{\Gamma}$, which has dense image by Corollary 1.2.30. Note that this means that for any abstract generating set X of Γ, the image $\iota(X)$ is a topological generating set of $\widehat{\Gamma}$.

An important property of the profinite completion which we have not yet spelled out is that $\widehat{\bullet}$ is a *functor*.

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

Proof. Uniqueness will follow from the density of $\iota_\Delta(\Delta)$ in $\widehat{\Delta}$: if $\hat{f}_1$ and $\hat{f}_2$ are two homomorphisms satisfying the conclusion of the proposition, consider the set

$$S = \{g \in \widehat{\Delta} : \hat{f}_1(g) = \hat{f}_2(g)\}.$$

Continuity of $\hat{f}_1$ and $\hat{f}_2$ shows that S is closed in $\widehat{\Delta}$, and S contains $\iota_\Delta(\Delta)$, and so is also dense. Hence S is all of $\widehat{\Delta}$ and so $\hat{f}_1$ and $\hat{f}_2$.

We prove existence first for the case when Γ is finite, so that $\Gamma = \widehat{\Gamma}$. Then $\ker f$ is a finite index normal subgroup M of Δ, and by the definition of the profinite completion there is a continuous projection map $\widehat{\Delta} \to \Delta/M$. The composition $\hat{f}\colon \widehat{\Delta} \to \Delta/M \to \Gamma$ is the required continuous homomorphism.

$$\begin{tikzcd}
\Delta \arrow[rr, "\iota_\Delta"] \arrow[dr] \arrow[ddr, "f"'] & & \widehat{\Delta} \arrow[dl] \arrow[ddl, "\hat{f}"] \\
& \Delta/M \arrow[d] & \\
& \Gamma &
\end{tikzcd}$$

Now we deal with the general case. For any finite index normal subgroup $N \lhd_f \Gamma$ we have a map $p_N \iota_\Gamma f\colon \Delta \to \Gamma/N$ to a finite group Γ/N (where $p_N\colon \widehat{\Gamma} \to \Gamma/N$ is the projection). By the finite case above, this extends to a unique continuous homomorphism $q_N\colon \widehat{\Delta} \to \Gamma/N$ such that $p_N \iota_\Gamma f = q_N \iota_\Delta$.

$$\begin{tikzcd}
\Delta \arrow[rr, "\iota_\Delta"] \arrow[d, "f"] & & \widehat{\Delta} \arrow[dl, dashed, "\hat{f}"'] \arrow[ddl, "q_N"] \\
\Gamma \arrow[r, "\iota_\Gamma"] \arrow[dr] & \widehat{\Gamma} \arrow[d, "p_N"'] & \\
& \Gamma/N &
\end{tikzcd}$$

By uniqueness these maps q_N are compatible with the transition maps $\Gamma/N_1 \to \Gamma/N_2$, so by definition of the limit there is a unique continuous homomorphism $\hat{f}\colon \widehat{\Delta} \to \widehat{\Gamma}$ such that $p_N \hat{f} = q_N$. Then $p_N \hat{f} \iota_\Delta = p_N \iota_\Gamma f$ for all N, whence $\hat{f} \iota_\Delta = \iota_\Gamma f$. □

It follows immediately from the uniqueness part of the propositions that the functor conditions $\widehat{f_1 f_2} = \hat{f}_1 \hat{f}_2$ and $\widehat{\mathrm{id}_\Gamma} = \mathrm{id}_{\widehat{\Gamma}}$ hold. One sometimes says that $\hat{f}$ is *induced* by f.

In the case $\Gamma = \mathbb{Z}$, we saw that ι was *injective*, which justified the word 'completion' and allowed us to identify $\mathbb{Z}$ as a subgroup of $\widehat{\mathbb{Z}}$ and forget the map ι. This injectivity may fail for general Γ; but we will generally not work with groups for which ι is not injective. The classical name for this property is 'residual finiteness'.

Definition 3.1.3. Let Γ be an abstract group. We say that Γ is *residually finite* if for every $\gamma \in \Gamma \smallsetminus \{1\}$ there exists a finite index normal subgroup $N \subseteq \Gamma$ such that $\gamma \notin N$ (or equivalently, that γN is a non-trivial element of Γ/N).

Proposition 3.1.4. *An abstract group Γ is residually finite if and only if the map $\iota\colon \Gamma \to \widehat{\Gamma}$ is injective.*

Proposition 3.1.5. *Any subgroup of a residually finite group is residually finite.*

Proof. Exercise. □

Proposition 3.1.6. *Let Γ be an abstract group and let $\Delta \leq \Gamma$ be a finite index subgroup. If Δ is residually finite, then Γ is residually finite.*

Proof. Let $\gamma \in \Gamma \smallsetminus \{1\}$. We must find a finite-index normal subgroup of Γ which does not contain γ.

If $\gamma \notin \Delta$, then the normal core of Δ—the finite index normal subgroup

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

of Γ—does not contain γ and we are done. (Note that this intersection has only finitely many different terms (at most one for each coset $g\Delta \in \Gamma/\Delta$), so is genuinely finite index.)

If $\gamma \in \Delta$, then residual finiteness of Δ implies that there exists a finite index subgroup N of Δ which does not contain γ. Then N also has finite index in Γ, and the core $\mathrm{Core}_\Gamma(N)$ is the finite index normal subgroup of Γ that we require. □

Many of the examples of finitely generated groups you are familiar with are residually finite.

Proposition 3.1.7. *Finitely generated abelian groups are residually finite.*

Proof. Exercise. □

Proposition 3.1.8. *The groups* $\mathrm{SL}_N(\mathbb{Z})$ *and* $\mathrm{GL}_N(\mathbb{Z})$ *are residually finite for any* N.

Proof. For a matrix $A \in \mathrm{GL}_N(\mathbb{Z})$, take a prime p larger than the absolute value of all the entries of A. Then A is not killed by the homomorphism $\mathrm{GL}_N(\mathbb{Z}) \to \mathrm{GL}_N(\mathbb{F}_p)$. □

These examples already imply many others. For example, free groups embed into $\mathrm{SL}_N(\mathbb{Z})$ and hence are residually finite—though we will give a direct proof later which does not rely on this embedding (which, after all, we haven't proved in this course).

It is fitting here to mention a generalisation of this result.

Theorem 3.1.9 (Malcev's theorem (Non-examinable))**.** *Let G be a finitely generated subgroup of* $\mathrm{GL}_N(K)$ *where K is a field. Then G is residually finite.*

The proof is similar in essence to the case of $\mathrm{GL}_N(\mathbb{Z})$. The group G may be taken to live inside a group $\mathrm{GL}_N(R)$ where R is the ring generated by the matrix entries of a generating set of G. This finitely generated ring can be shown to have enough maximal ideals P such that the maps $\mathrm{GL}_N(R) \to \mathrm{GL}_N(R/P)$ show that $\mathrm{GL}_N(R)$, and hence G, is residually finite. Showing that these maximal ideals exist, and that the fields R/P are finite, requires more commutative algebra than is pre-requisite for this course, so we will leave Malcev's theorem as an unproven statement.

The only consequence we will mention now is that the fundamental group of a surface is residually finite: as you may have seen in IB Geometry, a surface is the quotient of the hyperbolic plane by a group of isometries. This group of isometries is the fundamental group (the hyperbolic plane is the unversal covering space of the surface) and is a subgroup of the group of all isometries of hyperbolic space—which is $\mathrm{PSL}_2(\mathbb{R})$ and is thus residually finite by the same arguments as for Malcev's theorem.

Proposition 3.1.10. *The fundamental group of a surface is residually finite.*

You will see some additional results about residual finiteness on the example sheets, as well as a finitely presented group which is not only not residually finite, but has no non-trivial finite quotients whatsoever.

Now we will finally verify a claim made early on in the course, that profinite completions contain the same information as the set of isomorphism types of finite quotients of a group. We first quantify what are the open subgroups of $\widehat{\Gamma}$.

Lemma 3.1.11. *Let Γ be an abstract group. The open subgroups of $\widehat{\Gamma}$ are exactly the subgroups $\overline{\iota(\Delta)}$ for $\Delta \leq_f \Gamma$.*

Proof. If $\Delta \leq_f \Gamma$ is finite index then take a finite set of coset representatives $\{\gamma_i\}$ of Δ. Since

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

we see that $\overline{\iota(\Delta)}$ is closed and finite index, hence open. Note that in the computation above, the union has finitely many terms so we may exchange the closure and union processes, and the third equality uses the continuity of the translations by $\iota(\gamma_i)$.

Conversely if U is open in $\widehat{\Gamma}$ then, since $\iota(\Gamma)$ is dense, we have $U = \overline{\iota(\Gamma) \cap U}$. Setting $\Delta = \iota^{-1}(U)$, the subgroup Δ is finite index in Γ and has $\iota(\Delta) = \iota(\Gamma) \cap U$. □

Theorem 3.1.12. *Let G and H be topologically finitely generated profinite groups. Suppose that the sets of isomorphism types of continuous finite quotients of G and H are equal. Then G and H are isomorphic profinite groups.*

Proof. Let G_n be the intersection of all open subgroups of G of index at most n, and define H_n similarly. By Example 2.5.9 we have $G = \varprojlim G/G_n$.

Firstly, G/G_n is a finite quotient of G, hence by hypothesis there is an open normal subgroup V of H with $H/V \cong G/G_n$. The intersection of the index-at-most-n subgroups of G/G_n is trivial by definition, so by taking preimages we find that V may be written as an intersection of some open subgroups of H of index at most n—hence $H_n \subseteq V$ and

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

By symmetry, we also have $|H/H_n| \leq |G/G_n|$, whence we have equality and find that $V = H_n$, so $G/G_n \cong H/H_n$ for all n.

To show that the inverse limits $\varprojlim G/G_n$ and $\varprojlim H/H_n$ are isomorphic, it is not quite sufficient to say that G/G_n and H/H_n are isomorphic: we must also establish the existence of a family of isomorphisms which are *maps of inverse systems.*

Let S_n denote the set of isomorphisms $G/G_n \to H/H_n$. Let $f_n \in S_n$. Now, f_n takes a subgroup of G/G_n of index at most $n-1$ to such a subgroup of H/H_n; so f_n takes G_{n-1}/G_n to H_{n-1}/H_n and therefore defines a quotient map

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

with the property that the natural diagram

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

commutes. In this way, the sets S_n, with the maps $\phi_{n,n-1}$ between them, become an inverse system of non-empty finite sets. Hence there exists some element of the inverse limit—and such an element is precisely an isomorphism of inverse systems

$$(f_n)\colon G/G_n \to H/H_n$$

which shows $G \cong H$. □

As an immediate corollary, we find the same result for abstract groups.

Theorem 3.1.13. *Let Γ and Δ be finitely generated abstract groups. Suppose that the sets of isomorphism types of finite quotients of Γ and Δ are equal. Then $\widehat{\Gamma}$ and $\widehat{\Delta}$ are isomorphic profinite groups.*

We now turn our attention towards the question of how much we can learn about a group from its finite quotients (or, equivalently as we now know, from its profinite completion). It is natural to restrict our attention to residually finite groups—if a group doesn't have a good supply of finite quotients, we won't learn much! We also restrict to finitely generated groups.

Definition 3.1.14. A property $\mathcal{P}$ of groups is a *profinite invariant* if, whenever finitely generated residually finite groups G and H have isomorphic profinite completions, G has property $\mathcal{P}$ if and only if H has property $\mathcal{P}$.

This is a fairly loose definition, and merely establishes some phrasing.

We start with the most tractable class of groups: the abelian groups.

Proposition 3.1.15. *Being an abelian group is a profinite invariant.*

Proof. Let G and H be finitely generated residually finite groups with isomorphic profinite completions. Suppose H is abelian. Then every quotient group of H is abelian; hence every finite quotient of G is abelian. Suppose for a contradiction that G is not abelian. Then there are elements g_1 and g_2 of G such that the commutator $[g_1, g_2]$ does not vanish. Since G is residually finite, there is a finite quotient $\phi\colon G \to Q$ such that $\phi([g_1, g_2])$ is non-trivial. But Q is known to be abelian, so $\phi(g_1)$ and $\phi(g_2)$ commute, giving a contradiction. □

Proposition 3.1.16. *Let G and H be finitely generated groups with isomorphic profinite completions. Then the abelianizations $G_{\text{ab}} = G/[G, G]$ and $H_{\text{ab}} = H/[H, H]$ are isomorphic.*

Proof. Suppose $\widehat{G} \cong \widehat{H}$. We show first that $\widehat{G_{\text{ab}}} \cong \widehat{H_{\text{ab}}}$: since G and H have the same sets of finite quotients, they have the same sets of abelian finite quotients—which are exactly the sets of finite quotients of the abelianizations. By Theorem 3.1.12 therefore, $\widehat{G_{\text{ab}}} \cong \widehat{H_{\text{ab}}}$.

We are now left to show that if two finitely generated abelian groups A and A' have isomorphic profinite completions then they are isomorphic. By the classification of finitely generated abelian groups, we have

$$A \cong \mathbb{Z}^r \times T, \quad A' \cong \mathbb{Z}^s \times T'$$

for some integers r and s and some finite abelian groups T and T'.

We can derive r from the set of finite quotients of A:

$$r = \max\{k \text{ such that } A \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^r \ \forall n\}$$

from which formulation it follows that $r = s$. We can now also identify T from the set of finite quotients: it is the largest (by size) finite group such that A maps onto $(\mathbb{Z}/n\mathbb{Z})^r \times T$ for all n. Hence $T \cong T'$ and $A \cong A'$. □

Remark 3.1.17. Notice how we had to use such a strong result as the classification of finitely generated abelian groups here—there is no simple answer!

These two propositions put together show that a finitely generated abelian group A is *profinitely rigid* in the sense that any finitely generated residually finite group with the same finite quotients as A is isomorphic to A.

At this point I would like to give several lectures establishing profinite rigidity results for large interesting classes of groups. Unfortunately I can't because there is a huge amount of uncertainty and open questions in this area. Let us see a first example to show that even a group with a finite index abelian subgroup need not retain its profinite rigidity.

Example 3.1.18. Let $\phi\colon C_{25} \to C_{25}$ be the automorphism which sends $t \mapsto t^6$, where t is a generator of the cyclic group C_{25}. Note that ϕ is an order 5 automorphism: $6^5 \equiv 1 \mod 25$ but no smaller positive power of ϕ is the identity.

Form the semidirect products

$$G_1 = C_{25} \rtimes_\phi \mathbb{Z}, \quad G_2 = C_{25} \rtimes_{\phi^2} \mathbb{Z}.$$

We claim that these groups are not isomorphic, yet have isomorphic profinite completions. We write elements of both groups as elements of the set $C_{25} \times \mathbb{Z}$, and write the group operations as $\star_1$ and $\star_2$.

Let s be a generator of $\mathbb{Z}$ and write $\mathbb{Z} = \langle s \rangle$ multiplicatively. Suppose an isomorphism $\Psi\colon G_2 \to G_1$ exists. By using the quotient map $C_{25} \rtimes \mathbb{Z} \to \mathbb{Z}$ one sees that the given C_{25} is the only order 25 subgroup of each G_i, hence $\Psi(C_{25}) = C_{25}$ and $\Psi((t,1)) = (t^a, 1)$ for some $a \in \mathbb{Z}$ which is coprime to 25. Let $\Psi(1,s) = (t^b, s^c)$. Since $(t,1)$ and $(1,s)$ generate both the G_i, the element s^c must generate $\mathbb{Z}$ (again we can see this using the projection map). Hence $c = \pm 1$. But now we find a contradiction by computing the image of the element $(1,s) \star_2 (t,1) \star_2 (1,s^{-1})$ under Ψ in two different ways.

$$\Psi((1,s) \star_2 (t,1) \star_2 (1,s^{-1})) = \Psi((\phi^2(t),1)) = (\phi^2(t)^a, 1)$$
$$\Psi((1,s) \star_2 (t,1) \star_2 (1,s^{-1})) = (t^b, s^c) \star_1 (t^a,1) \star_1 (\phi^{-c}(t^b), s^{-c}) = (\phi^c(t^a), 1)$$

But $\phi^c(t^a) \neq \phi^2(t^a)$, since t^a generates $\mathbb{Z}/25\mathbb{Z}$ and $\phi^2 \neq \phi^c$, giving us the desired contradiction.

Now we consider the finite quotients of the G_i. Let $f\colon G_i \to Q$ be a finite quotient map. If the image of $\mathbb{Z} \to G_i \to Q$ has order m, then clearly $5m\mathbb{Z}$ is contained in the kernel of f, so the map to Q factors through the finite quotient $C_{25} \rtimes_{\phi^i} \mathbb{Z}/5m\mathbb{Z}$. (This group is well-defined since ϕ and ϕ^2 are order 5 automorphisms so there is a well-defined action of $\mathbb{Z}/5m\mathbb{Z}$ on C_{25}). Hence the quotients $C_{25} \rtimes_{\phi^i} \mathbb{Z}/5m\mathbb{Z}$ are a cofinal subsequence of the system of finite quotients of the G_i, and we find that

$$\widehat{G_i} = \varprojlim C_{25} \rtimes_{\phi^i} \mathbb{Z}/5m\mathbb{Z} = C_{25} \rtimes_{\phi^i} \widehat{\mathbb{Z}}$$

We may now build an isomorphism $\Omega\colon \widehat{G_2} \to \widehat{G_1}$, taking our cue from the earlier calculations. The problem with building the isomorphism Ψ before was that neither of generators ± 1 of $\mathbb{Z}$ was congruent to 2 modulo 5. But $\widehat{\mathbb{Z}}$ *does* have generators of that form by Proposition 2.5.13. Let $\kappa \in \widehat{\mathbb{Z}}^{\times}$ be congruent to 2 modulo 5. Define

$$\Omega(t^b, s^\lambda) = (t^b, s^{\lambda\kappa})$$

where $\lambda \in \widehat{\mathbb{Z}}$. It is easy to see that this is a continuous bijection. It is also a homomorphism:

$$\begin{aligned}\Omega((t^b, s^\lambda) \star_2 (t^c, s^\mu)) &= \Omega((t^b\phi^{2\lambda}(t^c), s^{\lambda+\mu})) = (t^b\phi^{2\lambda}(t^c), s^{\kappa(\lambda+\mu)})\\ \Omega((t^b, s^\lambda)) \star_1 \Omega((t^c, s^\mu)) &= (t^b, s^{\lambda\kappa}) \star_1 (t^c, s^{\mu\kappa}) = (t^b\phi^{\kappa\lambda}(t^c), s^{\kappa(\lambda+\mu)})\end{aligned}$$

and these two lines are equal since ϕ has order 5 and $\kappa \equiv 2 \mod 5$, so that $\phi^2 = \phi^\kappa$. Hence $\widehat{G_2} \cong \widehat{G_1}$.

Even for free groups the answer to the profinite rigidity question is unknown.

Open Question 3.1.19 ('Remeslennikov's Question')**.** *Let F be a finitely generated free group and let G be a finitely generated residually finite group. If $\widehat{F} \cong \widehat{G}$, must G be isomorphic to F?*

It is perhaps worth decanting this question into a more primitive form. Below, $d(G)$ denotes the minimal size of a generating set of a group G.

Open Question 3.1.20. *Does there exist a finitely generated residually finite group G (other than a free group) and an integer n such that a finite group Q is a quotient of* G if and only if $d(Q) \leq n$*?*

For now let us simply show that certain families of groups we have met do not give an answer to Remeslennikov's question.

Proposition 3.1.21. *Let F and F' be finitely generated free groups. If $\widehat{F} \cong \widehat{F'}$ then $F \cong F'$.*

Proof. If F is a free group of rank r then its abelianisation is $\mathbb{Z}^r$. Since abelianization is a profinite invariant, F' also has abelianization $\mathbb{Z}^r$—hence is a free group of rank r and is isomorphic to F. □

How about surface groups? Certainly we can't get away with just using the abelianization this time: if S_g is the fundamental group of a surface of genus g,

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

then the abelianization of S_g is $\mathbb{Z}^{2g}$. This shows that $\widehat{S}_g \not\cong \widehat{F}_r$ for a free group F_r of rank r, except if $r = 2g$. How can we distinguish $\widehat{S}_g$ from $\widehat{F}_{2g}$?

We will give two solutions to this question. Both illustrate techniques that can be used more generally. First we will codify what information an isomorphism of profinite completions gives about the whole lattice of finite index subgroups of the groups in question.

Theorem 3.1.22 ('Basic correspondence')**.** *Let G_1 and G_2 be finitely generated residually finite groups, and suppose $\phi\colon \widehat{G}_1 \to \widehat{G}_2$ is an isomorphism of their profinite completions. Then there is an induced bijection ψ between the set of finite index subgroups of G_1 and the set of finite index subgroups of G_2, such that if $K \leq_{\mathrm{f}} H \leq_{\mathrm{f}} G_1$, then:*

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

Let us see why this implies that S_g does not have the same profinite completion as F_{2g}. Any finite index subgroup of S_g is the fundamental group of a finite sheeted covering space of a surface of genus g. A finite covering of a surface is again a surface—hence its fundamental group has abelianisation $\mathbb{Z}^{2g'}$ for some g'.

On the other hand, F_{2g} has an index 2 subgroup. This subgroup is a free group of rank $2(2g-1)+1$ by the Nielsen-Schrier formula—so its abelianisation is $\mathbb{Z}^{4g-1}$, an abelian group of *odd* rank. If $\widehat{F}_{2g} \cong \widehat{S}_g$ then by the Basic Correspondence and Proposition 3.1.16, there is a finite index subgroup of S_g with this abelianisation—but all the finite index subgroups of S_g have even rank abelianisation, a contradiction.

The Basic Correspondence follows immediately from the following proposition, which relates the subgroup structure of a group to that of its profinite completion:

Proposition 3.1.23. *Let G be a finitely generated residually finite group, and let $\widehat{G}$ be its profinite completion. Identify G with its image under the canonical inclusion $G \hookrightarrow \widehat{G}$. Let ψ be the function sending a finite index subgroup $H \leq_{\mathrm{f}} G$ to its closure $\overline{H}$. If $K \leq_{\mathrm{f}} H \leq_{\mathrm{f}} G$ then:*

1. $\psi\colon \{H \leq_{\mathrm{f}} G\} \to \{U \leq_{\mathrm{o}} \widehat{G}\}$ *is a bijection;*
2. $[H : K] = [\overline{H} : \overline{K}]$;
3. $K \lhd H$ *if and only if* $\overline{K} \lhd \overline{H}$;
4. *if* $K \lhd H$, *then* $H/K \cong \overline{H}/\overline{K}$; *and*
5. $\widehat{H} \cong \overline{H}$.

Proof. Some of part 1 was already essentially proved as Lemma 3.1.11. I repeat the proof here for convenience.

If $H \leq_f G$ is finite index then take a finite set of coset representatives $\{g_i\}$ of H in G. Since

$$\widehat{G} = \overline{G} = \overline{\bigcup_i g_i H} = \bigcup_i g_i \overline{H}$$

we see that $\overline{H}$ is closed and finite index, hence open.

Conversely if U is open in $\widehat{G}$ then since G is dense, we have $U = \overline{G \cap U}$. Setting $H = G \cap U$, H is finite index in G with closure U.

Hence the given function ψ is a surjection. To see that it is a bijection, we must show that if H is a finite index subgroup of G then $G \cap \overline{H} = H$. Certainly $H \subseteq G \cap \overline{H}$. Now consider the action of G on the set of cosets G/H. Since G/H is finite, this extends to an action of $\widehat{G}$ on G/H (i.e. a continuous homomorphism $f\colon \widehat{G} \to \mathrm{Sym}(G/H)$). All elements of H, hence of $\overline{H}$, fix the coset H. But if $g \notin H$ then g does not fix the coset H. Then $\{x \in \widehat{G} | f(x)(H) = gH\}$ is an open subset of $\widehat{G}$ which contains g but intersects H trivially. Hence $g \notin \overline{H}$ and we are done.

To show (2), let $\{g_i\}$ be a complete set of coset representatives of H in G. We already know that the cosets $g_i\overline{H}$ cover $\widehat{G}$; we must also show that they are distinct cosets. But if $g_i\overline{H} = g_j\overline{H}$ then $g_i^{-1}g_j \in \overline{H} \cap G = H$ so $i = j$. Hence $[G : H] = [\widehat{G} : \overline{H}]$, from which the more general statement follows at once. Note also that this gives a natural bijection of coset spaces $G/H = \widehat{G}/\overline{H}$.

For (3), first note that if $\overline{K} \lhd \overline{H}$ then immediately $K = \overline{K} \cap G \lhd \overline{H} \cap G = H$. Conversely, if K is normal in H, consider the continuous action of $\overline{H}$ on $\overline{H}/\overline{K} = H/K$. The dense subgroup K of $\overline{K}$ fixes every element of H/K by normality, so by continuity $\overline{K}$ acts trivially on $\overline{H}/\overline{K}$ whence $\overline{K}$ is normal in $\overline{H}$.

Part (4): since $K = \overline{K} \cap H$ we have a natural homomorphism $H/K \to \overline{H}/\overline{K}$. This is surjective by density of H and is thus an isomorphism by (2).

Finally, to show (5), note that $\overline{H}$ maps to all the finite quotients H/K in a natural way, hence has a continuous homomorphism $\overline{H} \to \widehat{H}$. This is surjective because H is dense; it is injective because if $h \in \overline{H} \smallsetminus \{1\}$ then there is an open subgroup $U \leq_o \widehat{G}$ such that $h \notin U$, and the map $\overline{H} \to H/U \cap H$ shows that h does not map to the trivial element of $\widehat{H}$. □

A second way to show that the surface group is not isomorphic to the free group is to rely on the rank of the surface group, and a useful property called the Hopf property.

Proposition 3.1.24 (Hopf property for profinite groups). *Let G be a topologically finitely generated profinite group and let $f\colon G \to G$ be a surjective continuous map. Then f is an isomorphism.*

Proof. Let G_n be the intersection of all open subgroups of G with index at most n. As in Example 2.5.9, since G is topologically finitely generated the G_n are open normal subgroups of G and $G = \varprojlim G/G_n$.

Since f is surjective, $[G : f^{-1}(U)] = [G : U]$ for all open subgroups U of G. If U is an open subgroup of index at most n then $f^{-1}(U)$ is also open of index at most n and thus contains G_n. It follows that $G_n \subseteq f^{-1}(G_n)$ and $f(G_n) \subseteq G_n$. Thus f induces a map

$$f_n\colon G/G_n \to G/G_n$$

for all n. This map is surjective, and hence is an isomorphism since G/G_n is finite (by the Pigeonhole Principle). It follows that $f = \varprojlim f_n$ is an isomorphism. □

Corollary 3.1.25 (Hopf property for residually finite groups)**.** *Let G be a finitely generated residually finite group. Then any surjective homomorphism from G to itself is an isomorphism.*

Proof. An epimorphism $f \colon G \to G$ induces, by Proposition 3.1.2, a continuous homomorphism

$$\hat{f} \colon \widehat{G} \to \widehat{G}.$$

The image of this map is compact and includes the dense subset G of $\widehat{G}$, hence $\hat{f}$ is surjective, and hence is an isomorphism by the previous proposition. Since G is residually finite, it injects into $\widehat{G}$. It follows that f is injective. □

Definition 3.1.26. A (topological) group G is *Hopfian*, or *has the Hopf property*, if every (continuous) surjection from G to itself is an isomorphism (resp., an isomorphism of topological groups).

Remark 3.1.27. In many circumstances it can be easier to check that a homomorphism, which you suspect is an isomorphism, is surjective than it is to check injectivity: for surjectivity you need to show that some generating set is contained in the image, while injectivity requires taking any element of the source group and showing that its image is non-trivial. In the presence of the Hopf property, you can often dispense with checking an injectivity condition, by the following result.

Proposition 3.1.28. *Let G be a Hopfian group and let H be a group. Suppose there are surjections $f \colon G \to H$ and $f' \colon H \to G$. Then f and f' are isomorphisms.*

Proof. The composition $f'f \colon G \to G$ is surjective, hence is an isomorphism by the Hopf property. If follows immediately that f is injective, and that f' is injective on the image of f. Since this is all of H, it follows that f' is injective too. □

Much the same applies for continuous maps of Hopfian topological groups.

Proposition 3.1.29. *Let G be a Hopfian topological group and let H be a topological group. Suppose there are continuous surjections $f \colon G \to H$ and $f' \colon H \to G$. Then f and f' are isomorphisms of topological groups.*

Proof. The only outstanding question is whether f and f' are homeomorphisms (i.e. have continuous inverses). This is a consequence of the fact that if f and f' are continuous bijections, such that $f'f$ is a homeomorphism, then $f^{-1} = (f'f)^{-1}f'$ and $f'^{-1} = f(f'f)^{-1}$ are also continuous. □

Proposition 3.1.30. *Let G be a residually finite group. Assume that there exists a finite quotient group Q of G such that $d(G) = d(Q)$. If $\widehat{G}$ is isomorphic to the profinite completion of a free group, then G is free.*

Proof. Let F be a free group such that $\widehat{F} \cong \widehat{G}$. Then Q is also a quotient of F, so $d(F) \geq d(Q) = d(G)$. So G has a generating set of size $d(F)$, and there is a surjective map $f\colon F \to G$. This induces a continuous map $\hat{f}\colon \widehat{F} \to \widehat{G}$, which is a surjection since its image contains the dense subgroup G. Since $\widehat{G} \cong \widehat{F}$, by the Hopf property for profinite groups we know that $\hat{f}$ is an isomorphism. Hence $\hat{f}$ is injective so f is injective and thus an isomorphism. □

Corollary 3.1.31. *A surface group does not have the same profinite completion as a free group.*

Proof. The surface group S_g has rank at most $2g$, and maps onto $Q = \mathbb{F}_2^{2g}$ which has rank $d(Q) = 2g$. □

The Hopf property can also be a useful tool for proving that a certain group is *not* residually finite.

Example 3.1.32. Let n and m be coprime integers. Let $BS(n,m)$ be the group[1] with presentation

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

Define a homomorphism $f\colon BS(n,m) \to BS(n,m)$ by $f(t) = t$, $f(a) = a^n$. This gives a well-defined homomorphism, since the relation is killed by f:

$$ta^n t^{-1} a^{-m} \mapsto ta^{n^2} t^{-1} a^{-mn} = (ta^n t^{-1})^n a^{-nm} = a^{nm} a^{-nm} = 1$$

Furthermore, f is surjective: its image contains t, a^n and therefore a^m; since m and n are coprime, the image of f must contain a also.

However, f is not injective: tat^{-1} and a do not commute[2] in $BS(n,m)$, so their commutator is non-trivial; however

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

Hence $BS(n,m)$ is non-Hopfian, and hence is not residually finite.

3.2 Finite quotients of free groups

One extremely important family of groups that have not yet appeared in this course in a very prominent way are the free groups. These too are residually finite. One can in fact deduce this from the results already seen: those of you taking Geometric Group Theory will have seen that free groups are actually subgroups of $\mathrm{SL}_2(\mathbb{Z})$, and are therefore residually finite. Due to the importance of this fact, we will give a self-contained proof. In fact we'll give two, and then use the method from one of these proofs to construct many useful finite quotients of free groups.

Theorem 3.2.1. *Let F be a finitely generated free group. Then F is residually finite.*

[1] Here 'BS' stands for 'Baumslag–Solitar', after two mathematicians who popularised the use of these groups.

[2] Actually, this is less than obvious. The easiest way to prove it is to make $BS(n,m)$ act on a tree, but that sort of theory is beyond the scope of this course. We will simply assume that $[tat^{-1}, a] \neq 1$.

Remark 3.2.2. This theorem statement concerns finitely generated free groups, but the conclusion holds for infinitely generated free groups too: if g is a non-trivial element of a free group F with generating set S, then g may be written as a product of elements of X and their inverses. Only finitely many elements of X are used in this product; by factoring out all the other elements gives a map to a finitely generated free group in which g survives as a non-trivial element. This finitely generated free group has a finite quotient that does not kill g, which witnesses residual finiteness of F.

Theorem 3.2.1, Proof 1 (Non-examinable). Let X be a wedge of k circles, whose fundamental group F is the free group on k generators. Construct a sequence of finite-index normal subgroups of F inductively, by setting

$$F_1 = F, \quad F_{n+1} = \bigcap \{\ker(f) \mid f\colon F_n \to \mathbb{Z}/2\mathbb{Z}\}$$

These are characteristic (and hence normal) subgroups of F and one may show by induction that each F_n has finite-index. Let $X_n \to X$ be the covering space corresponding to the subgroup $F_n \lhd F$.

Each X_n is a finite graph; we claim that the *girth* of X_{n+1} (that is, the length of the shortest cycle in X_n) is greater than the girth of X_n. To see this, let l be any cycle of minimal length in X_n; we must show that it does not lift to a loop in X_{n+1}. Since l is minimal length it crosses every edge at most once; choose some edge e which l crosses. Collapsing the complement of e to a point gives a continuous map from X_n to a circle, sending l to a generator of $\pi_1 S^1 \cong \mathbb{Z}$; this gives a homomorphism $F_n \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ which does not contain $[l]$ in the kernel, so $[l] \notin F_{n+1}$ and l does not lift to X_{n+1}. So the shortest loop in X_{n+1} is longer than the shortest loop in X_n; that is

$$\text{girth}(X_{n+1}) > \text{girth}(X_n)$$

By induction it follows that $\text{girth}(X_n) \geq n$, so X_n has no loops shorter than length n.

Let $g \in F \smallsetminus \{1\}$. We can represent g by an edge loop l in X. Let n be the number of edges in l; then from above l cannot be lifted to a loop in X_{n+1}. It follows that $g \notin F_{n+1}$. This shows that F is residually finite. □

Remark 3.2.3. In fact this proof does more: the finite quotients F/F_n all have order a power of 2, so the free group is *residually* 2*-finite*—so that injects into its pro-2 completion. We can replace 2 with any other prime number p in the above and show that free groups are residually p-finite for all p. One might ask whether this stronger property always holds for a residually finite group; but already finite such as A_n (which are of course residually finite) rule that out.

Corollary 3.2.4. *A finitely generated free group is residually p-finite for all p, and hence injects into its pro-p completion.*

Theorem 3.2.1, Proof 2. This is one of those proofs which makes much more sense in pictures than in words; it is best to refer to Example 3.2.6 while reading this proof.

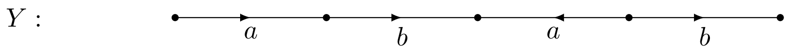
Let F be the free group generated by $a_1, \ldots, a_k$. Let X be a bouquet of k circles, with oriented edges labelled with the a_i to give an isomorphism $F \cong \pi_1 X$. Let $g \in F \smallsetminus \{1\}$. We wish to show that there is some finite index subgroup of F not containing g. Equivalently, by covering space theory, we want to show that there is some finite-sheeted covering space $\widetilde{X} \to X$ not containing g in its fundamental group.

Write g as a product $s_1 \cdots s_m$ of generators a_i and their inverses—and assume that this word is reduced in the sense that we never see $a_i a_i^{-1}$ or $a_i^{-1} a_i$ as a subword. Let Y be a line segment with m edges labelled with the a_i so that reading from one end of Y to the other spells out the word $s_1 \cdots s_m$. If we can find a finite sheeted covering $\widetilde{X} \to X$ such that Y embeds into $\widetilde{X}$ (as a labelled graph) then we are done: the fundamental group of $\widetilde{X}$ (with basepoint at the start y_0 of the segment Y) is a finite index subgroup of $\pi_1 X$ which does not contain g, since the loop labelled by $s_1 \cdots s_m$ in X lifts to the non-closed path Y in $\widetilde{X}$, not to a loop based at y_0.

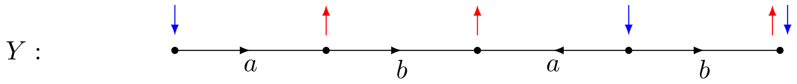
To construct $\widetilde{X}$, note that a covering space of X is the same thing as a graph with edges labelled by the a_i such that each vertex has exactly one incoming edge labelled a_i for each i and exactly one outgoing edge labelled a_i. In Y the number of vertices missing an incoming a_i equals the number of vertices missing an outgoing a_i, since each of these quantities is just $m+1$ minus the number of a_i-labelled edges in Y. Therefore we can add in extra edges labelled a_i between the vertices so that no vertex is missing an incoming or outgoing a_i-edge. Doing this for each i gives us the required $\widetilde{X}$. □

Remark 3.2.5. The technique of Proof 2 gives an algorithm for constructing finite quotients of the free group which show that a given element is non-trivial. The covering space does not in general give a *normal* subgroup—but we can easily produce a map to a permutation group witnessing that our element is non-trivial. See the example below.

Example 3.2.6. To construct a finite-index subgroup of the free group on two generators a and b not containing the element $g = aba^{-1}b$. First take a line segment Y with labels spelling out the word g.

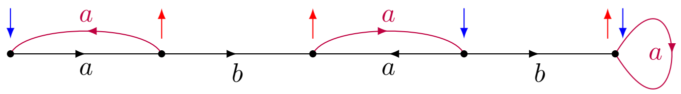


To make this into a covering space of the bouquet of two circles X we must add in more edges. Mark the vertices missing an outgoing a-edge with red arrows and those missing incoming a-edges with blue arrows:

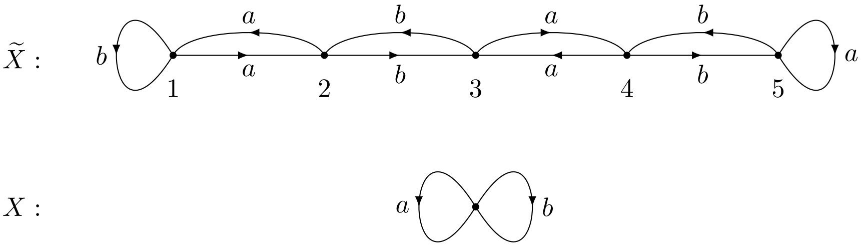


Being equal in number, we can pair these vertices up and join them with new a-edges to create a new graph in which every edge has one incoming a-edge and one outgoing a-edge.

Do the same for the b-edges and we obtain a graph $\widetilde{X}$ which is a covering space of the wedge of two circles X and whose fundamental group (with base-



point the leftmost vertex) does not contain g because reading the word $aba^{-1}b$ does not give a closed loop.



To produce an explicit homomorphism to a finite group showing g is non-trivial, note that the free group F acts on the set of vertices of $\widetilde{X}$: for each vertex x of $\widetilde{X}$, the vertex $a \cdot x$ is found by following the arrow labelled a coming out of x. Labelling the vertices of $\widetilde{X}$ by $1, \ldots, 5$ we find the following map to S_5:

$$a \mapsto (12)(34)(5), \quad b \mapsto (1)(23)(45)$$

note that the image of g under this homomorphism is (15234), which is indeed non-trivial.

Free groups thus have enough finite quotients to separate individual elements from the identity. In fact we can use similar techniques of contructing covering graphs to do much more—to separate out entire subgroups and compute whether a given subset generates the free group.

Generation of free groups is a surprisingly difficult question to decide. For example, take the free group F on three generators a, b and c. One of the triples of elements

- $abcb^2cb^{-1}c^{-1}b^{-1}a^{-1}$, $bc^{-1}b^{-1}abc$, bcb^{-1}
- $abcb^2cb^{-1}c^{-1}b^{-1}a^{-1}$, $bc^{-1}b^{-1}a^{-1}bc$, bcb^{-1}

generates F; the other does not. How can we tell the difference?

More generally, given a finite subset $S \subset F$ and an element $y \in F$, can we tell whether $y \in \langle S \rangle$? We can answer these questions by working with graphs, and in doing so will establish that we can use finite quotients of F to tell whether elements lie in $\langle S \rangle$ or not.

Theorem 3.2.7 (Marshall Hall's Theorem). *Let S be a finite subset of a finitely generated free group F, and let $y \notin \langle S\rangle$. Then there exists a finite group Q and a group homomorphism $f\colon F \to Q$ such that $f(y) \notin f(\langle S\rangle)$.*

We will not give a *formal* proof of this, for the simple reason that such a proof is essentially a more notationally-intense version of a worked example. We will give several examples to illustrate the method for constructing Q, from which it will be obvious that we can construct such a Q for every S and y.

Remark 3.2.8. Actually the traditional statement of Marshall Hall's Theorem is that $\langle S\rangle$ is a free factor of some finite index subgroup H of F—there is $H' \leq H$ such that $H = \langle S\rangle * H'$. We will essentially prove both statements, but the statement about free factors requires slightly more knowledge of fundamental groups of graphs than was discussed in Algebraic Topology, and which it would be out-of-place to discuss now.

Corollary 3.2.9. *A finite subset $S \subseteq F$ generates F if and only if it topologically generates the profinite completion $\widehat{F}$.*

Proof. If S generates F then it topologically generates $\widehat{F}$, since F is dense in $\widehat{F}$. If X does not generate S then there is some $y \notin \langle S\rangle$, and the Theorem guarantees a finite quotient $f\colon F \to Q$ such that $f(\langle S\rangle) \neq f(F)$. By definition this extends to a continuous homomorphism $\hat{f}\colon \widehat{F} \to Q$ such that $\hat{f}(\langle S\rangle) \neq \hat{f}(\widehat{F})$; it follows that $\langle S\rangle$ is not dense in $\widehat{F}$. □

Remark 3.2.10. We will compare this with the situation for the pro-p completion of F at the start of the next chapter.

First recall how we can build and identify covering spaces of certain graphs. For a free group F on generators $a_1, \ldots, a_n$, let X be the wedge on n circles—a graph with one vertex and with n edges. Labelling one edge with an arrow 'a_i' for each i identifies F with $\pi_1 X$. A graph morphism $Y \to X$ is described as follows. Every vertex of Y must be mapped to the single vertex of X. The map on the edges may then be specified by labelling each edge with an arrow a_i, to send it to the edge of X with the same label and direction.

When is this a covering map? The conditions to be a covering map are that the graph Y 'looks locally like' X—which amounts to saying that every vertex of Y 'looks like' the vertex of X, having exactly one edge labelled a_i coming into it and exactly one leaving it, for each i.

If Y is not a covering space of X, but every vertex has *at most* one edge of any label entering/leaving it, then we can turn Y into a covering space by simply adding more edges to take care of missing labels.

If on the other hand some vertices have, for example, two a_1 edges leaving it, then we can modify Y by gluing (or 'folding') these two edges together. So long as Y is a finite graph, if we keep doing this we will eventually have no more folds to do—at which point we can add more edges to get a covering space of X. This technique is sometimes called *Stallings folding.* Let us see some examples, in the context of Marshall Hall's Theorem.

Example 3.2.11. Take F to be the free group on two generators a and b. Let $S = \{aba, ba^2b\}$. We will construct a finite quotient of F witnessing the fact that S does not generate F. First draw a labelled graph Y which represents S: start from a basepoint v_0 and draw a labelled cycle spelling out each element

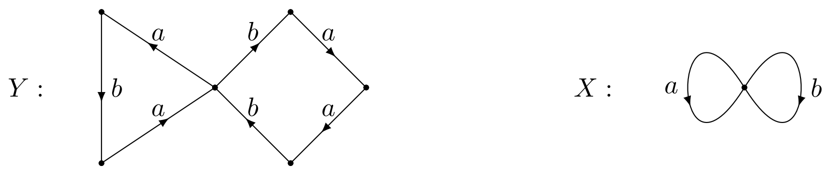


Figure 3.1: The length 3 cycle on the left spells the word aba and the cycle on the right spells ba^2b, in each case starting from the central vertex.

of S. See Figure 3.1. Note that in this case there are no folds which can be performed: every vertex has at most one edge of a given label entering or leaving it. This implies that we can complete Y to a covering space of X by adding more edges—and therefore implies that S does not generate X, since this covering has degree greater than 1 (the degree being the number of vertices). We show in Figure 3.2 one *possible* way of adding new edges to Y to make a covering space $\overline{Y}$ of X; there are many others.

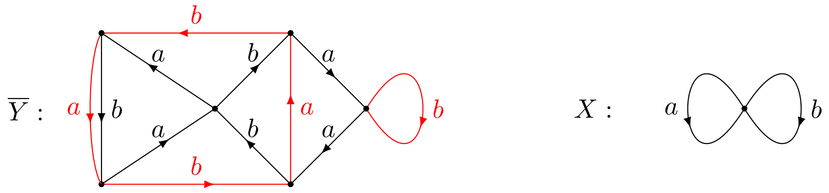


Figure 3.2: A folded graph may have edges added to it to form a covering space of X. The new edges are shown in red.

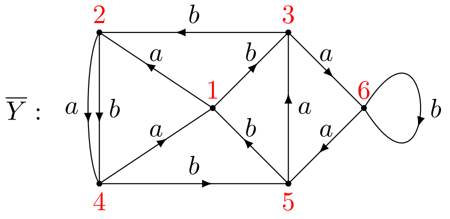
Finally, to construct an explicit map from F to a finite group, label the vertices of the graph $\overline{Y}$ by $1, \ldots, 6$. Then a and b act as permutations on this set, by 'following the arrows round'—a vertex i is sent by a to the unique vertex j such that there is an arrow $i \xrightarrow{a} j$.

This gives a homomorphism from F to the symmetric group S_6. By construction, the elements of S can be read along loops in Y based at the starting vertex v_0; so the images of these elements in S_6 fix the label of the vertex v_0. Since a and b do not both fix this vertex, we find that the image of F properly contains the image of $\langle S \rangle$.

In this last example we could immediately add edges to Y to build a covering space. Let us see an example where folding is needed.

Example 3.2.12. Again take a free group on two generators a and b. Now let $S = \{a^3, ab^2aba^{-1}, ab^{-1}ab^3\}$. We draw a labelled graph Y as before, with cycles representing the elements of S (read starting from one central vertex).

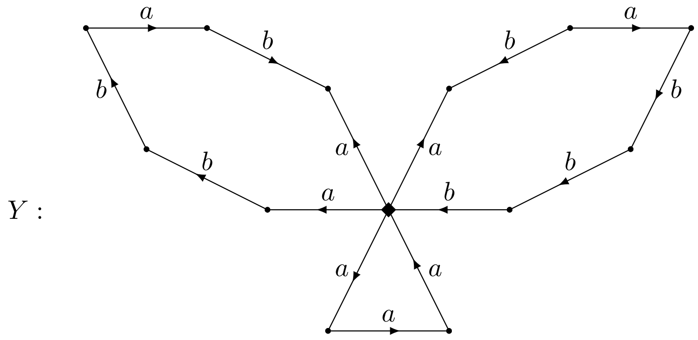
We cannot add edges to Y to make it into a covering space of X: we have *four* edges labelled a coming out of the central vertex, and a covering space would have just one. Therefore we fold these edges together to get a new graph



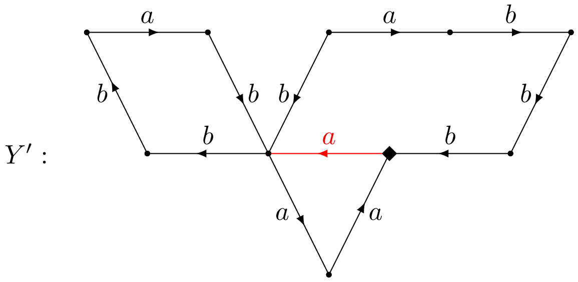
$$a \mapsto (1\,2\,4)(3\,6\,5)$$
$$b \mapsto (1\,3\,2\,4\,5)(6)$$

$$aba \mapsto (1)(2\,3\,5\,4\,6)$$
$$ba^2b \mapsto (1)(2\,4\,6\,2)(3)(5)$$

Figure 3.3: The covering space $\overline{Y}$ of X may be used to construct a homomorphism $F \to S_6$ as shown. Note that the elements of S must fix the vertex 1 by construction—so the image of $\langle S \rangle$ in S_6 is contained in the stabiliser of 1.



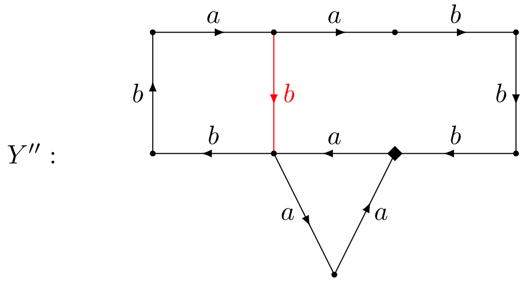
Y'. The image of $\pi_1 Y'$ in $\pi_1 X$ is still equal to $\langle S \rangle$: I will include a proof later for completeness, but for now just assume it to preserve the flow of the argument. The folded graph Y' is shown below, with the folded edge in red.

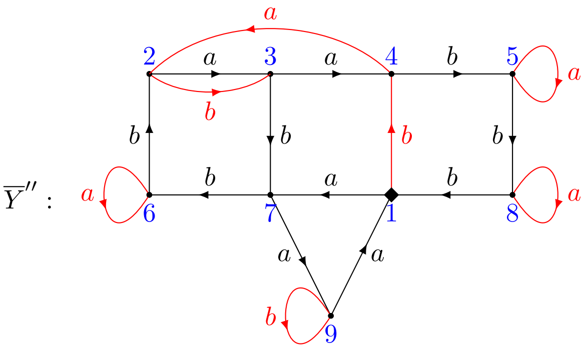


This new graph Y' is still not ‘fully folded’—there are two b edges entering the same vertex (the endpoint of the red arrow). So fold these edges together also, to get a graph Y''. Note that each fold decreases the number of edges, so this procedure cannot go on forever.

At last the graph Y'' is fully folded: each vertex has at most one edge of a given label entering or leaving it. Thus we can add more edges to get a covering space $\overline{Y}''$ of X:

We have also numbered the vertices of this graph, to yield a group homo-





morphism $F \to S_9$ which shows that $\langle S\rangle \neq F$.

$$a \mapsto (1\,7\,9)(2\,3\,4)(5)(6)(8), \quad b \mapsto (1\,4\,5\,8)(2\,3\,7\,6)(9)$$

$$a^3 \mapsto \mathrm{id}, \quad ab^2aba^{-1} \mapsto (1)(2\,4\,7\,3\,9\,8)(5\,6), \quad ab^{-1}ab^3 = (1)(2)(3)(4\,7\,8)(5\,6\,9)$$

Again the image of S is contained in the stabiliser of 1, so the image of F is not equal to the image of $\langle S\rangle$.

And what would happen if our set S actually did generate F? The only way the construction above fails to give a finite quotient distinguishing $\langle S\rangle$ from F is if the graph we obtain after folding as much as possible only has one vertex: then the fact that the image of S stabilises the starting vertex tells us nothing. A fully folded graph with one vertex must be a subgraph of X: so we find that $\langle S\rangle$ is actually the subgroup generated by some subset of the given generating set of F. So either $\langle S\rangle = F$ or we find that $F/\langle\langle S\rangle\rangle$ is a free group on the remaining generators: and picking any non-trivial finite quotient of the latter group will give a finite quotient of F witnessing that S does not generate F.

Finally, what if we have, as in the statement of Marshall Hall's Theorem a specific element $g \notin \langle S\rangle$ which we wish to see in a finite quotient? We essentially combine Examples 3.2.6 and 3.2.12.

Example 3.2.13. Take the set S from Example 3.2.12 and let $g = a^{-1}ba$. In our original covering space we have $a^{-1}ba \in \mathrm{stab}(1)$, so we do not immediately see that $a^{-1}ba \notin \langle S\rangle$. Instead we can add this element as a line segment in the original diagram, and then follow the same procedure of folding and adding edges to find a finite quotient which does the correct job.

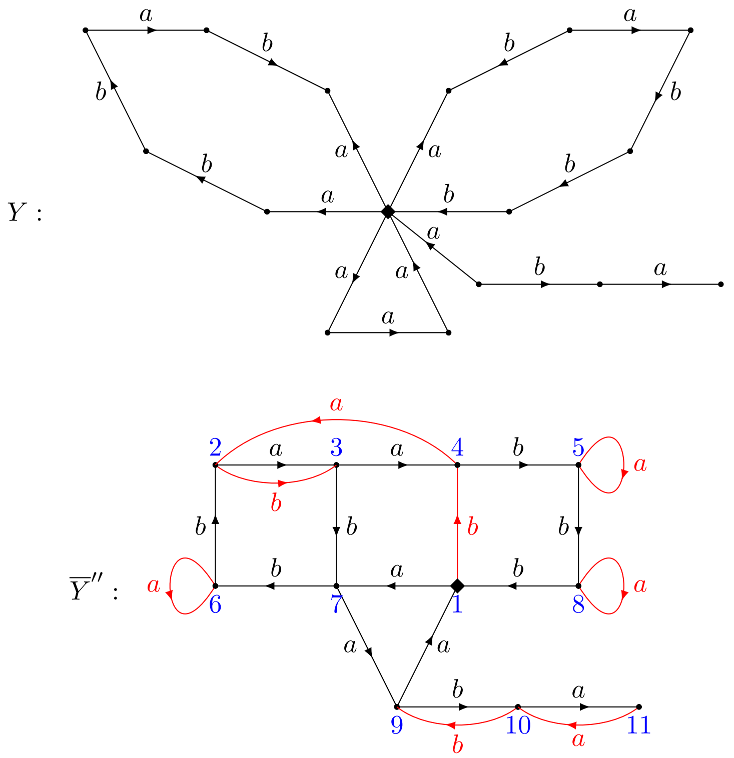


Figure 3.4: Modification of Example 3.2.12 to show additionally that $a^{-1}ba \notin \langle S \rangle$; we now have $a^{-1}ba\colon 1 \mapsto 11$, so this element lies outside the stabiliser of 1.

The missing ingredient to make all this rigorous is the statement that a Stallings fold does not change the image of the fundamental group in $\pi_1 X$. This sort of proposition is really a technical lemma about the fundamental group and thus not really part of this course, but a proof is included in these notes for completeness.

Proposition 3.2.14 (Non-examinable)**.** *Let Y and X be connected graphs and let $f\colon Y \to X$ be a graph morphism. Let v_0 be a vertex in Y and let $f(v_0) = x_0$. Suppose we have a vertex $u \in Y$ and two (oriented) edges ϵ, ϵ' starting at u such that $f(\epsilon) = f(\epsilon')$. Form a new quotient graph Y' by identifying ϵ with ϵ', and let $p\colon Y \to Y'$ and $f'\colon Y' \to X$ be the quotient maps. Then $p_*\colon \pi_1(Y, v_0) \to \pi_1(Y', p(v_0))$ is a surjection and the images of $\pi_1(Y, v_0)$ and $\pi_1(Y', p(v_0))$ in $\pi_1(X, x_0)$ are equal.*

Proof. The second part follows from the first, by considering the commuting diagram

$$\begin{tikzcd}
\pi_1(Y, y_0) \arrow[rr, "f_*"] \arrow[dr, two heads, "p_*"'] & & \pi_1(X, x_0) \\
& \pi_1(Y', p(y_0)) \arrow[ur, "f'_*"'] &
\end{tikzcd}$$

As for the first part, the surjectivity of p_*, let l be a cycle in Y' given by edges

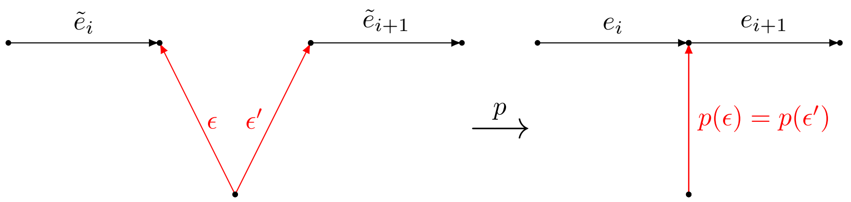


Figure 3.5: Diagram for Proposition 3.2.14

$e_1 \cdots e_n$. We will lift l to a loop in Y. For each i choose a preimage $\tilde{e}_i$ of e_i in Y. Let $o(e)$ and $t(e)$ denote the start and end points of an oriented edge e in a graph. Then we have $p(o(\tilde{e}_i)) = p(t(\tilde{e}_{i+1}))$ for all i. There is at most one vertex of Y' with two preimages in Y: the image of $t(\epsilon)$ and $t(\epsilon')$. So we have $o(\tilde{e}_i) = t(\tilde{e}_{i+1})$ except possibly if $o(\tilde{e}_i) = t(\epsilon)$ and $t(\epsilon') = t(\tilde{e}_{i+1})$ (or vice versa). In this case we add two edges to our proposed path to join up the endpoints of e_i and e_{i+1}:

$$\tilde{e}_i\tilde{e}_{i+1} \quad \rightsquigarrow \quad \tilde{e}_i\epsilon^{-1}\epsilon'\tilde{e}_{i+1}$$

Performing this operation for each i where it is necessary we get a valid cycle in Y. The image of this loop in Y' is equal to $e_1 \cdots e_n$, with possibly the interpolation of some segments $\epsilon^{-1}\epsilon'$. But since by definition $p(\epsilon) = p(\epsilon')$ this path is clearly homotopic to l. Hence p_* is a surjection on fundamental groups. □

Chapter 4

Pro-p groups

In this chapter we will consider a certain class of profinite groups in more detail: the pro-p groups. Recall that these are inverse limits of finite groups all of whose orders are powers of a fixed prime p. These groups are substantially better behaved than a general profinite group. In fact we shall see that they can even be better behaved than abstract groups. We start this discussion by considering their generation properties—we will find that after all the hard work to study whether a set generates an abstract free group in the last chapter, deciding the same question for a pro-p group amounts to nothing more than linear algebra!

4.1 Generators of pro-p groups

Definition 4.1.1. Let G be a finite group. The *Frattini subgroup* of G, denoted $\Phi(G)$, is the intersection of all maximal proper subgroups of G.

Remark 4.1.2. There is nothing particularly preventing us from defining this for all groups rather than just finite ones; but the theory for finite groups is more sensible because any proper subgroup is then contained in a maximal proper subgroup. This is not necessarily true for infinite groups.

Proposition 4.1.3. *If $f\colon G \to H$ is a surjective map of finite groups then $f(\Phi(G)) \subseteq \Phi(H)$. Hence $\Phi(G)$ is a characteristic normal subgroup of G.*

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 of f. If $f^{-1}(M) \subsetneq G' \subseteq G$ then $M \subsetneq f(G') = H$. Then $G = G' \cdot \ker(f) = G'$ since $\ker(f) \subseteq G'$. For any $g \in \Phi(G)$ we thus have $f(g) \in M$ for all M, so that $g \in \Phi(H)$. □

Proposition 4.1.4. *For G a finite group and a subset $S \subseteq G$, the following are equivalent:*

(i) S generates G;

(ii) $S\Phi(G)$ generates G;

(iii) the image $S\Phi(G)/\Phi(G)$ of S in $G/\Phi(G)$ generates $G/\Phi(G)$.

Proof. It is immediate that (i)⇒(ii)⇒(iii). Let us abbreviate $\Phi = \Phi(G)$. It remains to show that if $S\Phi/\Phi$ generates G/Φ then S generates G. But if S does not generate G, then $\langle S\rangle$ is contained in some maximal proper subgroup $M \subseteq G$. Since $\Phi \subseteq M$, we have $S\Phi/\Phi \subseteq M/\Phi \subsetneq G/\Phi$, so that the image of S does not generate $G/\Phi(G)$. □

Note that the implication '$\langle S\rangle$ is proper, hence is contained in some maximal proper subgroup M' uses the hypothesis that G is finite.

Such a proposition is of course of little value when the Frattini subgroup is trivial (as it often is, e.g. for any finite simple group). However, for finite p-groups the Frattini subgroup does give valuable information.

Definition 4.1.5. Let G be a group and let H and K be subgroups of G. Let m be an integer. Define

$$[H,K] = \langle\{[h,k] : h \in H, k \in K\}\rangle, \quad H^m = \langle\{h^m : h \in H\}\rangle$$

and define HK to be the set

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

Note that $[H,K]$ and H^m are forced to be subgroups by definition (they are the *subgroups generated by* the given sets); while HK is a *set*, which need not always be a subgroup. If either H or K is normal in G then HK is indeed a subgroup of G. Note also that $HH = H$; the multiplication notation does not imply statements such as $HH = H^2$.

Proposition 4.1.6. *If H is a normal subgroup of G then H^m is a normal subgroup of G for each $m \in \mathbb{Z}$. If H and K are normal subgroups of G then HK and $[H,K]$ are normal in G.*

Proposition 4.1.7. *Let G be a finite p-group. Then*

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

Hence $G/\Phi(G)$ is isomorphic to $\mathbb{F}_p^d$ where d is the minimal size of a generating set of G.

The usual notation for the group $G_{\mathrm{ab}}/pG_{\mathrm{ab}}$, the *mod-p abelianisation of* G, is $H_1(G,\mathbb{F}_p)$. This notation will not be put on a very concrete basis in this course, but should be reminiscent of Algebraic Topology, where for a connected simplicial complex X one has $H_1(X) \cong (\pi_1 X)_{\mathrm{ab}}$. We will be meeting the dual vector space $H^1(G,\mathbb{F}_p)$ later in the course.

Proof. To be completed on the Exercise Sheet. □

Thus Proposition 4.1.4 reduces the question of generation for a finite p-group essentially to linear algebra: does a given set of vectors generate the $\mathbb{F}_p$-vector space $G_{\mathrm{ab}}/pG_{\mathrm{ab}}$?

We may also define the Frattini subgroup of a profinite group.

Definition 4.1.8. Let G be a profinite group. Define

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

The first thing we do is replace 'closed subgroups' in this definition with 'open subgroups'. This doesn't imply that $\Phi(G)$ is necessarily open, as the intersection above may involve infinitely many M. However, being an intersection of closed subgroups, $\Phi(G)$ is always closed.

Proposition 4.1.9. *Any proper closed subgroup of a profinite group G is contained in a proper open subgroup. Hence maximal closed subgroups of G are open, and any proper closed subgroup is contained in a maximal proper closed subgroup.*

Proof. Let $H \leq G$ be a proper closed subgroup. Then (by Corollary 1.2.30) there exists a finite quotient $p \colon G \to Q$ such that $p(H) \neq Q$. Then $p^{-1}(p(H))$ is a proper open subgroup of G containing H.

It follows immediately that maximal proper closed subgroups are open. Any proper open subgroup is contained in a maximal proper open subgroup since open subgroups have finite index, hence any proper closed subgroup is contained in a maximal proper closed subgroup. □

The following propositions are now identical to Propositions 4.1.3 and 4.1.4.

Proposition 4.1.10. *Let $f \colon G \to H$ be a surjective continuous homomorphism of profinite groups. Then $f(\Phi(G)) \subseteq \Phi(H)$.*

Proof. □

Proposition 4.1.11. *For G a profinite group and a subset $S \subseteq G$, the following are equivalent*

(i) S topologically generates G;

(ii) $S\Phi(G)$ topologically generates G;

(iii) the image $S\Phi(G)/\Phi(G)$ of S in $G/\Phi(G)$ topologically generates $G/\Phi(G)$.

It wouldn't be a profinite groups lecture without having an inverse limit proposition. The theory of Frattini subgroups is no exception.

Proposition 4.1.12. *Let $(G_j)_{j \in J}$ be a surjective inverse system of finite groups, and let $G = \varprojlim G_j$. Then $\Phi(G) = \varprojlim \Phi(G_j)$.*

Proof. Let $p_j \colon G \to G_j$ be the quotient maps. By Proposition 4.1.10 we have

$$p_j(\Phi(G)) \subseteq \Phi(G_j)$$

for all j, hence $\Phi(G) \subseteq \varprojlim \Phi(G_j)$.

Next let M be a maximal proper closed subgroup of G. Since M is open, by Proposition 1.2.28 there is some i such that $\ker p_i \subseteq M$. We also then have $\ker p_j \subseteq M$ for all $j \preceq i$. Then $p_j(M)$ is a maximal proper subgroup of G_j for all $j \preceq i$, so that $\Phi(G_j) \subseteq p_j(M)$ for all $j \preceq i$. Hence $\varprojlim \Phi(G_j) \subseteq \varprojlim p_j(M) = M$. Since this holds for all M, we have $\varprojlim \Phi(G_j) \subseteq \bigcap M = \Phi(G)$. □

For finitely generated pro-p groups, the question of generation thus comes down to linear algebra: deciding whether a certain family of vectors spans a vector space (over the field $\mathbb{F}_p$).

Proposition 4.1.13. *Let G be a topologically finitely generated pro-p group. Then $H_1(G, \mathbb{F}_p) := G/\Phi(G) \cong \mathbb{F}_p^d$ where d is the minimal size of a topological generating set of G; and*

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

Proof. Write G as a surjective inverse limit of finite p-groups $G = \varprojlim G_j$. We already know $\Phi(G) = \varprojlim [G_j, G_j]G_j^p$ by Propositions 4.1.7 and 4.1.12. For any element of G of the form $[g_1, g_2]g_3^p$ 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 $[G,G]G^p \subseteq \Phi(G)$ and hence $\overline{[G,G]G^p} \subseteq \Phi(G)$ since $\Phi(G)$ is closed.

Now $G/\overline{[G,G]G^p}$ is abelian, topologically finitely generated and every element has order p, hence[1] $G/\overline{[G,G]G^p} \cong \mathbb{F}_p^d$ for some d. Since $\Phi(\mathbb{F}_p^d) = \{0\}$ we have $\Phi(G) \subseteq \overline{[G,G]G^p}$ by Lemma 4.1.10. Hence $\Phi(G) = \overline{[G,G]G^p}$ as required.

Since a subset of G topologically generates G if and only if it generates $G/\Phi(G)$, we find that the minimal size of a topological generating set for G is d. □

Corollary 4.1.14. *Let $f\colon G \to H$ be a continuous homomorphism of topologically finitely generated pro-p groups. Then $f(\Phi(G)) \subseteq \Phi(H)$, hence f induces a group homomorphism (i.e. linear map of $\mathbb{F}_p$-vector spaces) $f_*\colon G/\Phi(G) \to H/\Phi(H)$ and f is surjective if and only if f_* is surjective.*

Proof. For any element of G of the form $[g_1, g_2]g_3^p$ we have $f([g_1, g_2]g_3^p) \subseteq \overline{[H,H]H^p} = \Phi(H)$. These elements topologically generate $\Phi(G)$, hence $f(\Phi(G))$ is contained in $\Phi(H)$. Then $\Phi(G)$ is contained in the kernel of the map $G \to H \to H/\Phi(H)$, and there is an induced map $f_*\colon G/\Phi(G) \to H/\Phi(H)$.

If f is surjective then f_* is clearly surjective. If f_* is surjective then $f(G)$ topologically generates $H/\Phi(H)$, hence it topologically generates H. But $f(G)$ is closed in H so $f(G) = H$. □

Remark 4.1.15. It is actually necessary to use the characterisation $\Phi(G) = \overline{[G,G]G^p}$ here rather than just the defining property of Frattini subgroups. For example, the Frattini subgroup of the symmetric group S_5 is trivial (the only proper normal subgroups are A_5 and 1; but stab(1) $\leq S_5$ is a maximal subgroup not containing A_5, so A_5 cannot be $\Phi(S_5)$). Let $G = \mathbb{Z}/4\mathbb{Z}$ and map $f\colon G \to S_5$ by sending a generator of G to the 4-cycle $(1\,2\,3\,4)$. Then $\Phi(G) = \langle 2 \rangle \leq \mathbb{Z}/4\mathbb{Z}$, and $f(\Phi(G)) \nsubseteq \Phi(S_5) = \{1\}$, so there is no induced map $G/\Phi(G) \to S_5/\Phi(S_5)$.

4.2 Nilpotent groups

One important character of p-groups is that they are *nilpotent*—meaning that eventually, iterated commutators vanish. We have used this implictly in the past, but it is valuable to quantify it properly as we will exploit nilpotence in the main theorem of the chapter.

[1] If S generates a dense subgroup of such a group, then $\langle S \rangle$ is abelian, finitely generated and every element has order p—so $\langle S \rangle$ is abelian, and a profinite group with a dense finite subgroup is finite.

Definition 4.2.1. Define the *lower central series* of a group G to be the following sequence of subgroups. Let $G_1 = G$. For $n \geq 1$ define $G_{n+1} = [G, G_n]$ to be the subgroup of G *generated by* the elements

$$\{[g, h] : g \in G, h \in G_n\}$$

The lower central series is often denoted $G_n = \gamma_n(G)$.

A group Γ is *nilpotent of class* c if $G_{c+1} = \{1\}$ and $G_n \neq \{1\}$ for $n \leq c$.

A key part of the power of the lower central series is that it is *fully characteristic*: for any group homomorphism $f \colon G \to H$, we have $f(\gamma_n(G)) \subseteq \gamma_n(H)$. You will prove this, and the next two propositions, on the exercise sheet.

Lemma 4.2.2. *The lower central subgroup $\gamma_n(G)$ is a* fully characteristic *subgroup of G. If $f \colon G \to H$ is surjective then $f(\gamma_n(G)) = \gamma_n(H)$.*

Proof. Exercise. □

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

Proof. Exercise. □

Proposition 4.2.4. *A finite p-group is nilpotent.*

Proof. Proceed by induction. An abelian p-group is certainly nilpotent. Let G be a p-group and assume that all smaller p-groups are nilpotent. Take $z \in Z(G)$. Then $G/\langle z\rangle$ is nilpotent by hypothesis, hence $\gamma_{c+1}(G/\langle z\rangle) = 1$ for some c. Hence $\gamma_{c+1}(G) \subseteq \langle z\rangle$. But now

$$\gamma_{c+2}(G) = [G, \gamma_{c+1}(G)] \subseteq [G, \langle z\rangle] = 1$$

since z is central. Hence G is nilpotent also. □

Another important class of nilpotent groups are given by certain matrix groups.

Example 4.2.5. Let R be a commutative ring with identity. Let $UT(m, R)$ be the group of upper triangular matrices over R whose diagonal entries all equal 1. That is,

$$UT(m, R) = \left\{ \begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\} \subseteq \mathrm{GL}_m(R).$$

Then $UT(n, R)$ is nilpotent.

Proof (non-examinable). Let Z_n be the set of $m \times m$ matrices $A = (a_{ij})$ over R such that $a_{ij} = 0$ for $j - i < n$, and let $H_n = \{I + A \mid A \in Z_n\}$. Then $H_1 = UT(n, R)$ and $H_n \supseteq H_{n+1}$ for all n. Also note $H_m = \{I\}$.

An elementary calculation shows that if $A \in Z_k$ and $B \in Z_l$ then $AB \in Z_{k+l}$: for every $1 \leq r \leq m$, either $j - r < l$ or $r - i < k$ or $j - i \geq k + l$, so

$$(AB)_{ij} = \sum_r a_{ir} b_{rj} = 0 \quad \text{if } j - i < k + l$$

We prove by a 'top-down' induction that H_n is a subgroup. The only tricky part is to show that inverses of elements of H_n lie in H_n. This is certainly true for $H_m = \{I\}$. If $A = (a_{ij}) \in Z_n$ for $n \geq 1$ then

$$((I + A)(I - A))_{ij} = I + A - A - A^2 = I - A^2$$

and $A^2 \in Z_{2n}$. Since $2n > n$, by induction we have $(I - A^2)^{-1} \in H_{2n}$ and $(I+A)^{-1} = (I-A)A'$ for some $A' \in H_{2n}$. Equivalently we may write $(I+A)^{-1} = I - A + A''$ for some $A'' \in Z_{2n}$.

Let $I+A \in H_1$ and let $I+B \in H_n$. We will show that $[I+A, I+B] \in H_{n+1}$. For, taking $A'' \in Z_2$ and $B'' \in Z_{2n}$ as above, we have

$$\begin{aligned}
&(I + A)(I + B)(I + A)^{-1}(I + B)^{-1} \\
&\quad = (I + A)(I + A)^{-1}(I - B + B'') + (I + A)B(I - A + A'')(I - B + B'') \\
&\quad = I - B + B'' + B + B(-A + A'')(I + B)^{-1} + AB(I + A)^{-1}(I + B)^{-1} \\
&\quad = I + \underbrace{B'' + B(-A + A'')(I + B)^{-1} + AB(I + A)^{-1}(I + B)^{-1}}_{\in Z_{n+1}}
\end{aligned}$$

It now follows by induction that $\gamma_n(UT(m)) \subseteq H_n$, and since $H_m = 1$, we find that $UT(m)$ is indeed nilpotent. □

Analogously to the lower central series of a general nilpotent group, one may also define the *lower central p-series* $\gamma_n^{(p)}(G) = G_n$ of a pro-p group G by

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

For topologically finitely generated pro-p groups this is a neighbourhood basis of the identity in G, which is very well behaved: the quotients G_n/G_{n+1} are all vector spaces over $\mathbb{F}_p$. The lower central p-series is also defined uniformly over all pro-p groups, which can make it highly useful for applications. It will play a key role in the penultimate theorem of the course.

Proposition 4.2.6. *Let G be a finite p-group. Then $\gamma_n^{(p)}(G) = 1$ for some n.*

Proof. Proceeds exactly as the proof that G is nilpotent. □

Proposition 4.2.7. *Let G be a topologically finitely generated pro-p group. Then $\gamma_n^{(p)}(G)$ is finitely generated and open in G.*

Proof. Proceed by induction. For each n, we clearly have

$$\Phi(\gamma_n^{(p)}(G)) \subseteq \gamma_{n+1}^{(p)}(G).$$

By Proposition 4.1.13, the Frattini subgroup of a finitely generated pro-p group is open, hence the same is true of $\gamma_{n+1}^{(p)}(G)$; and open subgroups are topologically finitely generated. □

Proposition 4.2.8. *Let G be a topologically finitely generated pro-p group. Then $\{\gamma_n^{(p)}(G)\}$ is a neighbourhood basis of the identity of G.*

Proof. Let N be any open subgroup of G. Then G/N is a finite p-group, hence $\gamma_n^{(p)}(G/N) = 1$ for some n; it follows that $\gamma_n^{(p)}(G) \subseteq N$. □

4.3 Invariance of topology

In this section we will prove the following theorem, originally due to Serre, which shows that our insistence on considering continuous homomorphisms was not in fact a restriction at all!

Theorem 4.3.1. *Let G be a topologically finitely generated pro-p group and let H be a profinite group. Any group homomorphism $G \to H$ is continuous.*

Corollary 4.3.2. *Let G be a topologically finitely generated pro-p group. Then there is no other topology on G making it into a profinite group.*

Remark 4.3.3. We will prove this theorem for pro-p groups. It is in fact true for *all* finitely generated profinite groups, by a remarkable and difficult theorem of Nikolay Nikolov and Dan Segal.

First we must establish several lemmas and preliminary results about pro-p groups, which showcase much of the interplay between topology and algebra which makes the theory of profinite groups so rich.

Proposition 4.3.4. *Let G be a pro-p group and let K be a subgroup of finite index of G. Then $[G : K]$ is a power of p.*

Proof. We may as well assume, by passing to a core, that K is a normal subgroup of G.

Let $[G : K] = m = p^r m'$ where m' is coprime to p. Let $X = \{g^m : g \in G\} \subseteq K$. Being the image of G under the continuous function $g \mapsto g^m$, the set X is compact and closed. Thus (by Proposition 1.2.32)

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

We will show that $g^{p^r} \in K$ for every $g \in G$, from which it follows by Cauchy's Theorem applied to G/K that K has index a power of p as required. So let $g \in G$.

Let $N \lhd_o G$ be any normal open subgroup of G. Let $[G : N] = p^s$ and let $t = \max(r, s)$. Then we have $g^{p^t} \in N$ and $\mathrm{hcf}(p^t, m) = p^r$. Hence there exist $a, b \in \mathbb{Z}$ such that $am + bp^t = p^r$. Then

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

This is true for every N, hence we find

$$g^{p^r} \in \bigcap XN = \overline{X} = X \subseteq K$$

as required. □

Lemma 4.3.5. *Let G be a nilpotent group with a finite generating set $a_1, \ldots, a_d$. Then every element g of the commutator subgroup $[G, G]$ may be written in the form*

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

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

Proof. We induct on the nilpotency class c of G. The base case $c = 1$ (that is, when G is abelian) is trivial.

By induction, then, the result is true in $G/\gamma_c(G)$, so that there exist x_1,..., x_d in G and $u \in \gamma_c(G)$ such that

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

We now seek a nice form for $u \in \gamma_c(G) = [G, \gamma_{c-1}(G)]$. Using the usual commutator relations

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

(for the convention $[x, y] = x^{-1}y^{-1}xy$), we find that for any $v \in \gamma_{c-1}(G)$ and $w \in G$, the following hold:

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

Note here that any commutator $[-, v]$ lies in $\gamma_c(G)$ and is therefore central in G.

Using these relations, the element $u \in [G, \gamma_{c-1}(G)]$, which is by definition of the form $[g_1, v_1] \cdots [g_r, v_r]$ where $v_i \in \gamma_{c-1}(G)$ and $g_i \in G$ (so that the g_i may be written as products of the a_i and their inverses), can be re-written into the form $[a_1, v_1'] \cdots [a_d, v_d']$ for $v_i' \in \gamma_{c-1}(G)$.

Then we have

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

and, using the above relations again, we find

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

as required. □

Proposition 4.3.6. *If G is a topologically finitely generated pro-p group, then $[G, G]$ is closed in G.*

Proof. Let $a_1, \dots, a_d$ be a topological generating set for G and let

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

Note that X is a compact and closed, being the image of G^d under the continuous function

$$(x_1, \dots, x_d) \mapsto [a_1, x_1] \cdots [a_d, x_d]$$

We will show that $X = [G, G]$, so that $[G, G]$ is indeed closed. Certainly it is true that $X \subseteq [G, G]$.

Let $g \in [G, G]$. For any $N \lhd_o G$, the image gN of g in G/N is in the commutator subgroup $[G/N, G/N]$. Since G/N is finite nilpotent, and is generated by the images of the a_i, the previous lemma shows that gN lies in the image of X—that is, $g \in XN$. This is true for all N, whence

$$g \in \bigcap_{N \lhd_o G} XN = \overline{X} = X$$

as required. □

Proposition 4.3.7. *If G is a topologically finitely generated pro-p group, then $[G,G]G^p$ is open and closed in G and equals $\Phi(G)$.*

Proof. Let $G^{\{p\}} = \{g^p : g \in G\}$, which is a (perhaps proper) subset of G^p. Now, $G/[G,G]$ is an abelian group, and in an abelian group products of p^{th} powers are again p^{th} powers (i.e. $a^p b^p = (ab)^p$ in an abelian group). It follows that $[G,G]G^{\{p\}} = [G,G]G^p$. The set $[G,G]$ is closed by the previous proposition, and is hence compact since G is compact. Then $[G,G]G^{\{p\}}$ is also compact: it is the image of the continuous map

$$[G,G] \times G \to G, \quad (x,g) \mapsto xg^p$$

Hence $[G,G]G^p$ is indeed closed. It follows that it equals the Frattini subgroup $\Phi(G) = \overline{[G,G]G^p}$, which is already known to be open. □

Theorem 4.3.8. *Let G be a topologically finitely generated pro-p group. Then any finite index subgroup K of G is open.*

Proof. Suppose the theorem is not true, and let G and K be a pair providing a counterexample of minimal index. It suffices to consider K normal: any finite-index subgroup contains a finite-index normal subgroup, and if a subgroup of G contains an open subgroup then it is itself open.

Consider $M = [G,G]G^pK$. Now, G/K is a non-trivial p-group, and the image of M in G/K is the Frattini subgroup $\Phi(G/K)$, which is a proper subgroup of G/K. Hence M is a proper subgroup of G. If $K \neq M$, then by the minimality hypothesis we must have K open in M and M open in G, so that K is open in G. Otherwise, we have $K = M$, so that K contains the subgroup $[G,G]G^p$—which is open by the previous proposition. Hence K itself is open too. □

Proof of Theorem 4.3.1. Let $f\colon G \to H$ be a group homomorphism from a topologically finitely generated pro-p group to a profinite group. Let $U \lhd_o H$ be a basic open subgroup of H. Then U is finite index in H, so $f^{-1}(U)$ is finite index in G. By the previous theorem, any finite index subgroup of G is open, so $f^{-1}(U)$ is open and f is continuous. □

Proof of Corollary 4.3.2. If G is a topologically finitely generated pro-p group, then by the above all finite index subgroups of G are open. If $\mathcal{T}$ is any topology making the abstract group G into a profinite group $\widetilde{G}$, then all the open subgroups have finite index—so the identity map $G \to \widetilde{G}$ is continuous. Since G is compact and $\widetilde{G}$ is Hausdorff, this map is also a homeomorphism and we are done. □

4.4 Hensel's Lemma and p-adic arithmetic.

Consider the old argument that 2 has no square root in the rational numbers.

> Assume m/n is a square root of 2 given as a fraction in lowest terms. Then $m^2 = 2n^2$. Since 2 is prime, we find 2 divides m so that $m = 2m'$. Then $n^2 = 2m'^2$ and 2 divides n as well, giving a contradiction.

What may this mean for arithmetic over the p-adic integers, for p a prime not equal to 2? In $\mathbb{Z}_p$ we no longer have any statement that '2 is prime', or anything like it: indeed 2 is invertible in $\mathbb{Z}_p$ for $p \neq 2$. So no argument similar to the one above could be used to show that 2 is not a square in $\mathbb{Z}_p$. In fact, as we will discover, whether 2 is a square depends on the prime chosen: for instance, 2 has no square root in $\mathbb{Z}_3$ or $\mathbb{Z}_5$, but does have a square root in $\mathbb{Z}_7$.

Remark 4.4.1. In the last paragraph we switched from discussing 'rational roots' to 'integer roots'. The reason is the simple fact (which you should convince yourself of) that for $x \in \mathbb{Q}_p$, $x^2 \in \mathbb{Z}_p$ if and only if $x \in \mathbb{Z}_p$.

What should by now be a routine exercise in inverse limits gives a starting point for the solution of polynomials in $\mathbb{Z}_p$.

Lemma 4.4.2. *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 the reduction of f modulo p^k has a root in $\mathbb{Z}/p^k\mathbb{Z}$ for all k.*

Proof. Exercise. □

A remarkable fact about the p-adic integers is that quite often we need not check any of the $\mathbb{Z}/p^k\mathbb{Z}$ except the first, through a process sometimes called *'Hensel lifting'*. Let us see an example.

Example 4.4.3. Modulo 7 we have $3^2 = 9 \equiv 2$, so the polynomial $x^2 = 2$ has a root in $\mathbb{Z}/7\mathbb{Z}$. Let us try to 'lift' this root to a root in $\mathbb{Z}/7^2\mathbb{Z}$. Consider the elements $3 + 7a \in \mathbb{Z}/49\mathbb{Z}$—those which map to 3 modulo 7. We have

$$(3 + 7a)^2 = 9 + 7 \cdot 2 \cdot 3 \cdot a + 49a^2 \equiv 2 + 7(1 + 6a) \equiv 2 + 7(1 - a) \mod 49$$

Therefore setting $a = 1$ gives a root modulo 49 (and indeed $(3 + 7)^2 = 100 \equiv 2$ modulo 49).

The key point here is that the $(7a)^2$ term vanished modulo 49, leaving us with a *linear* equation $1+6a = 0$ to be solved in $\mathbb{Z}/7\mathbb{Z}$. It is also important that the cofficient of a here is invertible in $\mathbb{Z}/7\mathbb{Z}$ (that is, non-zero) so that there is a (unique) solution for a. There is nothing to stop us performing this operation again to find a root of 2 modulo $7^3 = 343$, or indeed modulo any 7^k.

Example 4.4.4. To find a square root of 2 in $\mathbb{Z}/343\mathbb{Z}$: take the square root 10 of 2 in $\mathbb{Z}/49\mathbb{Z}$ and consider the elements $10 + 7^2a$. We have

$$(10 + 7^2a)^2 = 100 + 7^2 \cdot 20 \cdot a + 7^4a^2 \equiv 2 + 7^2(2 + 6a)$$

So setting $a = 2$ gives a root modulo 343; specifically we find that $108^2 \equiv 2$ modulo 343.

Let us turn this method into a theorem.

Proposition 4.4.5 (Hensel's Lemma for square roots)**.** *Let $p \neq 2$ be a prime. Suppose that $\lambda \in \mathbb{Z}_p$ is congruent to a non-zero square r_1^2 modulo p, for $r_1 \in \mathbb{Z}$. Then there is a unique $\rho \in \mathbb{Z}_p$ such that $\rho^2 = \lambda$ and $\rho \equiv r_1$ modulo p.*

Proof. We construct a sequence of elements $r_k \in \mathbb{Z}$, unique modulo p^k, such that $r_k^2 \equiv \lambda$ modulo p^k and $r_{k+1} \equiv r_k$ modulo p^k. The second condition shows that (r_k) is a Cauchy sequence in $\mathbb{Z}_p$, and thus converge to some unique $\rho \in \mathbb{Z}_p$; the first then says $\rho^2 = \lambda$.

Suppose we have constructed r_k. Consider the elements $r_k + p^k a$ for $0 \leq a \leq p-1$; these represent all the elements of $\mathbb{Z}/p^{k+1}\mathbb{Z}$ which are congruent to r_k modulo p_k. Since $r_k^2 \equiv \lambda$ modulo p_k we can write $r_k^2 = \lambda + b_k p^k$ for some $b_k \in \mathbb{Z}_p$. We have

$$(r_k + p^k a)^2 = r_k^2 + p^k \cdot 2r_k a + p^{2k} a^2 \equiv \lambda + p^k (b_k + 2r_k a) \quad \text{modulo } p^{k+1}.$$

Since $2r_k \neq 0$ in $\mathbb{F}_p$ there is a unique a such that $b_k + 2r_k a \equiv 0$ modulo p; for this value a_k of a we set $r_{k+1} = r_k + p^k a_k$ and have $r_{k+1}^2 \equiv \lambda$ modulo p^{k+1} as required. □

Remark 4.4.6. When actually implementing this in practice, it is worth noting that the value of r_k only matters modulo p^k; it may help to change it modulo p^k to ease computation.

With this preliminary lemma out of the way, we can establish the true Hensel's Lemma.

Proposition 4.4.7 (Hensel's Lemma)**.** *Let $f(x)$ be a polynomial with coefficients in $\mathbb{Z}_p$, for p a prime. Let $r \in \mathbb{Z}_p$ such that $f(r) \equiv 0$ modulo p^K for some K and $f'(r) \not\equiv 0$ modulo p. Then there exists a unique $\rho \in \mathbb{Z}_p$ such that $f(\rho) = 0$ and $\rho \equiv r$ modulo p^K.*

Remark 4.4.8. Here $f'(x)$ is the formal derivative of $f(x)$. There is no analysis happening here: we simply define the derivative of a polynomial $\sum_{n=0}^N a_n x^n$ to be $\sum n a_n x^{n-1}$.

Lemma 4.4.9. *Let $f(x)$ be a polynomial with $\mathbb{Z}_p$-coefficients. Then for $r, a \in \mathbb{Z}_p$ and $k \geq 1$ we have*

$$f(r + p^k a) \equiv f(r) + p^k a f'(r) \quad \textit{modulo } p^{k+1}$$

Proof. Since the statement is linear in f, it suffices to prove it for $f(x) = x^n$. Using the binomial formula we have

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

Now simply note that each term in the sum on the right hand side has a factor p^{2k}, hence also a factor p^{k+1}. □

Proof of Hensel's Lemma. We construct a sequence $r_k \in \mathbb{Z}_p$ for $k \geq K$, starting with $r_K = r$, and such that $r_{k+1} \equiv r_k$ modulo p^k and $f(r_k) \equiv 0$ modulo p^k. The first condition ensures that (r_k) is a Cauchy sequence in $\mathbb{Z}_p$, converging to some $\rho \in \mathbb{Z}_p$; and the second condition ensures that $f(\rho) = 0$. Each r_k will be unique modulo p^k, so that ρ is unique with these properties.

Suppose that we have constructed r_k. Consider the elements $r_k + p^k a_k$ for $a_k = 0, \ldots, p-1$, which give representatives for all elements of $\mathbb{Z}/p^{k+1}$ which are congruent to r_k modulo p^k. By construction $f(r_k) \equiv 0$ modulo p_k, so that $f(r_k) = p^k b_k$ for some $b_k \in \mathbb{Z}_p$. We have

$$f(r_k + p^k a_k) \equiv f(r_k) + p^k a_k f'(r_k) \equiv p^k (b_k + a_k f'(r)) \quad \text{modulo } p^{k+1}$$

where we note that $f'(r_k) \equiv f'(r)$ modulo p. Since $f'(r)$ is non-zero in $\mathbb{F}_p$, it is invertible, so there exists a unique a_k such that $b_k + a_k f'(r) \equiv 0$ modulo p. For this value of a_k set $r_{k+1} = r_k + p^k a_k$. Then $f(r_{k+1}) \equiv 0$ modulo p^{k+1} and we are done. □

Example 4.4.10. Find a primitive cube root of unity modulo $7^3 = 343$.

Solution. Modulo 7 we have $2^3 \equiv 1$. Let us find r_3 such that $r_3^3 \equiv 1$ modulo 343 and $r_3 \equiv 2$ modulo 7. Take $f(x) = x^3 - 1$. We have $r_1 = 2$ and $r_1^3 - 1 = 8 = 1 + 7$ so that $b_1 = 1$. Note that $f'(r_1) = 12 \equiv 5 \not\equiv 0$ modulo 7, so we may apply Hensel lifting. We solve $b_1 + f'(r_1)a_1 = 1 + 5a_1 = 0$ in $\mathbb{F}_7$ to find $a_1 = 4$.

Set $r_2 = 2 + 4 \cdot 7 = 30$. Then $f(r_2) = 30^3 - 1 = 26999 = 551 \cdot 49$, so $b_2 = 551 \equiv 5$ modulo 7. We solve $b_2 + f'(r_1)a_2 \equiv 0$ modulo 7 to find $a_2 = -1$. Then $r_3 = r_2 + 49 \cdot a_2 = -19$ is a cube root of 1 modulo 343. You may check if you like that $(-19)^3 = -6859 = 1 + (-20) \cdot 343$. □

One can interpret Hensel's Lemma, for polynomials $x^n - a$, as using the ring structure of $\mathbb{Z}_p$ to solve equations $x^n = a$ in the group $\mathbb{Z}_p^\times$. Another key family of pro-p groups sitting inside a similar ring structure are the pro-p matrix groups.

Definition 4.4.11. Define the following closed subgroups of $\mathrm{GL}_N(\mathbb{Z}_p)$.

$$\begin{aligned} \mathrm{GL}_N^{(k)}(\mathbb{Z}_p) &= \ker(\mathrm{GL}_N(\mathbb{Z}_p) \to \mathrm{GL}_N(\mathbb{Z}/p^k\mathbb{Z})) \\ \mathrm{SL}_N^{(k)}(\mathbb{Z}_p) &= \ker(\mathrm{SL}_N(\mathbb{Z}_p) \to \mathrm{SL}_N(\mathbb{Z}/p^k\mathbb{Z})) \end{aligned}$$

Proposition 4.4.12. *The groups $\mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$ and $\mathrm{SL}_N^{(1)}(\mathbb{Z}_p)$ are pro-p groups.*

Remark 4.4.13. The group $\mathrm{GL}_N(\mathbb{Z}_p)$ is not itself a pro-p group, since the quotient group $\mathrm{GL}_N(\mathbb{F}_p)$ has order

$$|\mathrm{GL}_N(\mathbb{F}_p)| = \prod_{k=0}^{N-1} (p^{N-k} - 1) \cdot p^{N(N-1)/2}$$

and is not a p-group.

Proof. It is clear that $\mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$ will be the inverse limit of the similarly defined groups $\mathrm{GL}_N^{(1)}(\mathbb{Z}/p^m\mathbb{Z})$. Each of these groups has the form

$$\mathrm{GL}_N^{(1)}(\mathbb{Z}/p^m\mathbb{Z}) = \{I + pA \mid A \in \mathrm{Mat}_{N\times N}(\mathbb{Z}/p^m\mathbb{Z})\}$$

and thus clearly have order $p^{N^2(m-1)}$. Hence $\mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$ is pro-p.

Since $\mathrm{SL}_N^{(1)}(\mathbb{Z}_p)$ is a closed subgroup of $\mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$, it too is a pro-$p$ group. □

We can manipulate this group to prove Hensel-type results. *For the rest of this section we assume that p is an odd prime.* The prime $p = 2$ is simply more annoying, though it does not really cause any fatal complications.

Proposition 4.4.14. *The continuous function $A \mapsto A^p$ maps $\mathrm{GL}_N^{(k)}(\mathbb{Z}_p)$ surjectively onto $\mathrm{GL}_N^{(k+1)}(\mathbb{Z}_p)$ for all $k \geq 1$. Furthermore the same is true in $\mathrm{SL}_N(\mathbb{Z}_p)$.*

Remark 4.4.15. This map is of course not a group homomorphism.

Proof. Firstly note that for any $r \geq 1$ and any matrix A with coefficients in $\mathbb{Z}_p$, we have

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

for some B; besides $I + p^{r+1}A$, all other terms in the binomial expansion have a coefficient

$$p^{rl}\binom{p}{p-l}$$

for $l \geq 2$ which always[2] has a factor p^{r+2}.

Now let $I + p^{k+1}A \in \mathrm{GL}_N^{(k+1)}(\mathbb{Z}_p)$. We will show inductively the following statement for all $n \geq k$.

> There exist matrices B_n and E_n for $n \geq 1$, which may be expressed as polynomials in A, such that
>
> $$B_{n+1} \equiv B_n \mod p^n, \quad (I + p^k B_n)^p = I + p^{k+1}A + p^{k+n+1}E_n$$
>
> for all n.

The significance of the condition that the various matrices be polynomials in A is that they all commute with each other. The first of the displayed conditions guarantees that the matrices B_n converge in the p-adic toplogy to some B_∞; the second condition then guarantees, upon taking $n \to \infty$, that $1 + p^k B_\infty$ is a p-th root of $1 + p^{k+1}A$.

To start the construction, take $B_1 = A$. By the above calculation, we find that

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

for some E_1. Note that E_1 is some polynomial in A, hence commutes with A.

Now assume the inductive hypthesis holds for a given n; we will construct the required matrices B_{n+1} and E_{n+1} for the next step of the induction. Define $B_{n+1} = B_n - p^n E_n$. Then, noting that all relevant matrices commute so that we may apply the binomial formula, we have

$$\begin{aligned}
&(I + p^k B_{n+1})^p \\
&\quad= (I + p^k B_n - p^{k+n}E_n)^p \\
&\quad= (I + p^k B_n)^p - p(I + p^k B_n)^{p-1}p^{k+n}E_n + (\text{terms divisible by } p^{k+n+2}) \\
&\quad= I + p^{k+1}A + p^{k+n+1}E_n - p^{k+n+1}E_n + (\text{terms divisible by } p^{k+n+2}) \\
&\quad= I + p^{k+1}A + p^{k+n+2}E_{n+1}
\end{aligned}$$

where E_{n+1} is some polynomial in E_n and B_n, and therefore expressible as a polynomial in A. This completes the proof of the inductive statement.

We now have our matrix $C = 1 + p^k B_\infty$ such that $C^p = A$.

For the ‘Furthermore’ part it remains to show that if A has determinant 1 then C has determinant 1, so that it lies in $\mathrm{SL}_N(\mathbb{Z}_p)$ rather than $\mathrm{GL}_N(\mathbb{Z}_p)$. Let $\kappa = \det C \in \mathbb{Z}_p^\times$. We have $\kappa^p = 1$—but by Question 10 on Exercise Sheet 3 there are no order p elements of $\mathbb{Z}_p^\times \cong \mathbb{Z}_p \times C_{p-1}$. Hence $\det C = 1$ as required. □

The following is an elementary calculation.

[2] Except if $p = 2$, $r = 1$ and $l = 2$—hence our exclusion of the case $p = 2$.

Lemma 4.4.16. *Let A and B be $N \times N$ matrices over $\mathbb{Z}_p$. Then*

$$(I + p^k A)(I + p^k B) \equiv (I + p^k B)(I + p^k A) \equiv I + p^k(A + B) \mod p^{k+1}$$

Proposition 4.4.17. *For all k, we have*

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

and

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

Proof. By the previous proposition, we know that each element of $\mathrm{GL}_N^{(k+1)}(\mathbb{Z}_p)$ is a p^{th} power of an element of $\mathrm{GL}_N^{(k)}(\mathbb{Z}_p)$, hence is contained in the Frattini subgroup. The Lemma now shows that $\mathrm{GL}_N^{(k)}(\mathbb{Z}_p)/\mathrm{GL}_N^{(k+1)}(\mathbb{Z}_p)$ is an abelian group, which we know to have exponent p, and is thus a vector space $\mathbb{F}_p^d$ for some d. It is generated by the set of matrices

$$I + p^k E_{i,j}$$

where $E_{i,j}$ has zero entries except for a 1 in the (i, j)-position. These matrices are easily seen to be linearly independent in $\mathrm{GL}_N^{(k)}(\mathbb{Z}_p)/\mathrm{GL}_N^{(k+1)}(\mathbb{Z}_p)$, whence $d = N^2$. Since the Frattini subgroup of $\mathbb{F}_p^{N^2}$ is trivial, we also have the inclusion

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

which completes the result. □

Corollary 4.4.18. *For any k, the function $x \mapsto x^p$ induces an isomorphism*

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

Proof. By Proposition 4.4.14, this map is surjective. By the lemma it is a group homomorphism, and by the previous proposition the two groups have the same size. Hence we have an isomorphism as claimed. □

Theorem 4.4.19. *Let H be any closed subgroup of $\mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$. Then $d(H) \leq N^2$, where $d(H)$ is the minimal size of a generating set of H.*

Proof. It is sufficient to show that for all K, every subgroup of

$$G = \mathrm{GL}_N^{(1)}(\mathbb{Z}_p)/\mathrm{GL}_N^{(K+1)}(\mathbb{Z}_p)$$

may be generated by at most N^2 elements. Let $H \leq G$, and let

$$G_m = \mathrm{GL}_N^{(m)}(\mathbb{Z}_p)/\mathrm{GL}_N^{(K+1)}(\mathbb{Z}_p) \leq G,$$

and let $H_m = G_m \cap H$. We prove by a top-down induction that $d(H_m) \leq N^2$. The base case is

$$H_K \leq G_K = \mathrm{GL}_N^{(K)}(\mathbb{Z}_p)/\mathrm{GL}_N^{(K+1)}(\mathbb{Z}_p) \cong \mathbb{F}_p^{N^2}$$

which immediately implies $d(H_K) \leq N^2$.

Now assume that $d(H_{m+1}) \leq N^2$. Let e be the dimension of

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

and take $h_1, \ldots, h_e \in H_m$ whose images generate H_m/H_{m+1}. By the above corollary, we have an isomorphism

$$G_m/G_{m+1} \cong G_{m+1}/G_{m+2}$$

given by raising elements to p^{th}-powers. It follows that $h_1^p, \ldots, h_e^p$ are linearly independent in G_{m+1}/G_{m+2}, and therefore also independent in $H_{m+1}/\Phi(H_{m+1})$. Therefore there exist $y_1, \ldots, y_{d-e} \in H_{m+1}$ (where $d = d(H_{m+1})$) such that H_{m+1} is generated by $\{h_1^p, \ldots, h_e^p, y_1, \ldots, y_{d-e}\}$. By definition of the h_i we then have

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

So $d(H_m) \leq d(H_{m+1}) \leq N^2$ as required. □

Corollary 4.4.20 (Non-examinable)**.** *There is no continuous injection from a non-abelian free pro-p group to* $\mathrm{GL}_N(\mathbb{Z}_p)$ *for any* N*.*

Proof. Since open subgroups of free pro-p groups are free, and $\mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$ is open in $\mathrm{GL}_N(\mathbb{Z}_p)$, it suffices to check for maps into $\mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$.

If F is a free pro-p group of rank $r \geq 2$, then F has open subgroups of index p^n for all n. By a suitably formulated pro-p version of the Basic Correspondence, such subgroups are free pro-p groups of rank $p^n(r-1)+1$. So a free pro-p group has subgroups H of arbitrarily high $d(H)$, which cannot all embed into $\mathrm{GL}_N(\mathbb{Z}_p)$ for a fixed N, by the previous theorem. □

This should be contrasted with the case for discrete groups, where as already seen the group $\mathrm{SL}_2(\mathbb{Z})$ contains a free group.

Remarkably Theorem 4.4.19 almost has a converse. We don't have time to prove this in this course, but I will state the theorem for interest's sake.

Theorem 4.4.21 (Non-examinable)**.** *Let* G *be a pro-p group and suppose there is an integer* R *such that* $d(H) \leq R$ *for all closed subgroups* H *of* G*. Then* G *has an abelian normal subgroup* $A \cong \mathbb{Z}_p^a$ *for some* $a \leq R$*, such that there is a continuous injection*

$$G/A \hookrightarrow \mathrm{GL}_R(\mathbb{Z}_p) \times F$$

for some finite p-group F*.*

Chapter 5

Cohomology of Groups

In Algebraic Topology you studied the homology theory of topological spaces, an exceedingly useful theory which essentially translates questions of topology into questions about abelian groups. In this chapter we will develop the closely related theory of *cohomology of groups*. We will not be seeing the word 'profinite' for a little while, but will instead develop cohomology theory for discrete groups. The profinite theory will return at the conclusion of the course with some more remarkable facts concerning pro-p groups.

Remark 5.0.1. You may be curious why we have 'homology' of spaces and 'cohomology' of groups. In truth there is also a cohomology theory of spaces and a homology theory of groups. However for topological spaces the homology theory is more natural to define; for groups it is cohomology which is both easier and more useful.

5.1 Group rings and chain complexes

Throughout let G be an abstract group.

Definition 5.1.1 (Group ring)**.** Let G be a group. The *group ring* (or sometimes *group algebra*) of G is the ring $\mathbb{Z}G$ defined as follows. The additive group of $\mathbb{Z}G$ is the free abelian group with basis $\{g : g \in G\}$—so that a generic element is a finite formal sum $\sum n_g g$ for $n_g \in \mathbb{Z}$. The ring multiplication is defined on basis elements by $g \cdot h = (gh)$ and extended bilinearly to all of $\mathbb{Z}G$.

Example 5.1.2. For $g, h \in G$ and e the identity element of G, we have

$$(e + g)(e - 2h) = e + g - 2h - 2gh$$

in the group ring $\mathbb{Z}G$.

Remark 5.1.3. The multiplicative identity of $\mathbb{Z}G$ is the basis element e; this is usually renamed to 1 by convention.

Remark 5.1.4. Warning: this is not a *commutative* ring, unless G is an abelian group. In the 'Groups, Rings and Modules' course all rings were assumed commutative, but many useful rings are not.

Commutativity notwithstanding, the definition of a module over $\mathbb{Z}G$ is identical to that which you have learned before.

Definition 5.1.5. A (left) G-module (or $\mathbb{Z}G$-module) is an abelian group M equipped with a G-action—a function $\mathbb{Z}G \times M \to M$, $(r, m) \mapsto r \cdot m$ such that

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

A module has *trivial G-action* if $g \cdot m = m$ for all $g \in G, m \in M$.

Definition 5.1.6. Let M_1 and M_2 be G-modules. A *morphism of G-modules* (or *G-linear map*) is a group homomorphism $\alpha\colon M_1 \to M_2$ such that $\alpha(r \cdot m) = r \cdot \alpha(m)$ for all $m \in M_1$, $r \in \mathbb{Z}G$. Note that it suffices to check this condition for basis elements $r = g \in G$.

Definition 5.1.7. Let M and N be G-modules. Let $\operatorname{Hom}_G(M, N)$ be the *Hom-group*: the set of G-linear maps $\alpha\colon M \to N$, with group operation given by addition:

$$(\alpha + \beta)(m) = \alpha(m) + \beta(m)$$

Taking Hom-groups is in a certain sense a functor, and maps of G-modules induce maps of Hom-groups in the following way.

Definition 5.1.8. If $f\colon M_1 \to M_2$ is a morphism of G-modules then we have a 'dual map'

$$f^*\colon \operatorname{Hom}_G(M_2, N) \to \operatorname{Hom}_G(M_1, N), \quad \phi \mapsto \phi \circ f$$

for each G-module N.

Similarly, we use subscript stars to denote 'induced maps': if $f\colon N_1 \to N_2$ is a G-linear map, then we have a map

$$f_*\colon \operatorname{Hom}_G(M, N_1) \to \operatorname{Hom}_G(M, N_2), \quad \phi \mapsto f \circ \phi$$

for each G-module M.

Submodules, quotient modules, etc. are defined in the natural way.

Definition 5.1.9. Let M be a G-module. A (G-)*submodule* of M is a subgroup $N \leq M$ such that $g \cdot n \in N$ for all $n \in N$. If N is a submodule of M, we may define the *quotient module* M/N to be the abelian group M/N with the G-action $g \cdot (m + N) = (g \cdot m) + N$.

Definition 5.1.10. A *chain complex* of G-modules is a sequence of G-modules

$$M_s \xrightarrow{d_s} M_{s-1} \xrightarrow{d_{s-1}} \cdots \xrightarrow{d_{t+2}} M_{t+1} \xrightarrow{d_{t+1}} M_t$$

such that for every $t < n < s$ we have $d_n d_{n+1} = 0$—that is, $\operatorname{im} d_{n+1} \subseteq \ker d_n$. We may also abbreviate this notationally to 'a chain complex $(M_n, d_n)_{t \leq n \leq s}$'.

The chain complex is *exact at M_n* if $\operatorname{im} d_{n+1} = \ker d_n$. The chain complex is *exact*, or *an exact sequence* if it is exact at M_n for all $s < n < t$. Note that there is no condition at M_s or M_t.

The *homology* of the chain complex is the family of abelian groups

$$H_s(M_\bullet) = \ker d_s, \quad H_n(M_\bullet) = \ker d_{n-1} / \operatorname{im} d_n, \quad H_t(M_\bullet) = M_t / \operatorname{im} d_{t+1}$$

for $t < n < s$. Note that an exact sequence is one for which $H_n(M_\bullet) = 0$ for $t < n < s$.

Remark 5.1.11. There is no need for the sequence to have finite length; we could have infinite chains of M_i in one direction (or both).

Example 5.1.12.

- Exactness of a sequence

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

means that $\ker \alpha = \operatorname{im}(0)$—i.e. that α is injective.

- Exactness of a sequence

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

means that α is surjective.

- An exact sequence of the form

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

is called a *short exact sequence.* Here α is injective, β is surjective and $\operatorname{im} \alpha = \ker \beta$.

Definition 5.1.13. Given a set X, the *free* $\mathbb{Z}G$*-module on* X is the set of finite formal sums $\sum_{x \in X} r_x x$ where $r_x \in \mathbb{Z}G$ is non-zero for only finitely many x. The G-action is the obvious one $g \cdot \sum_{x \in X} r_x x = \sum_{x \in X} (g r_x) x$.

We will use the (slightly non-standard) notation $\mathbb{Z}G\{X\}$.

Definition 5.1.14. A G-module P is *projective* if, for every surjective morphism of G-modules $\alpha \colon M_1 \twoheadrightarrow M_2$ and every morphism $\beta \colon P \to M_2$ there exists a morphism of G-modules $\bar{\beta} \colon P \to M_1$ such that $\bar{\beta}\alpha = \beta$.

$$\begin{tikzcd}
 & P \arrow[dl, dotted, "\bar{\beta}"'] \arrow[d, "\beta"] & \\
M_1 \arrow[r, "\alpha"] & M_2 \arrow[r] & 0
\end{tikzcd}$$

Proposition 5.1.15. *Free modules are projective.*

Proof. Let $\mathbb{Z}G\{X\}$ be a free module, let $\alpha \colon M_1 \to M_2$ be a surjective morphism of G-modules and let $\beta \colon \mathbb{Z}G\{X\}$. For each $x \in X$ choose, using surjectivity of α, some $m_x \in M_1$ such that $\alpha(m_x) = \beta(x)$. Then define a map $\bar{\beta} \colon \mathbb{Z}G\{X\} \to M_1$ by

$$\bar{\beta}(\sum r_x x) = \sum r_x m_x.$$

□

Definition 5.1.16 (Projective resolution)**.** A *projective resolution of* $\mathbb{Z}$ *by* $\mathbb{Z}G$*-modules* is an exact sequence

$$\cdots \xrightarrow{d_{n+2}} F_{n+1} \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} F_{n-1} \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_1} F_0 \xrightarrow{d_0} \mathbb{Z} \longrightarrow 0$$

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

At this point we can begin to connect these notions to what you've already seen in topology. Consider a connected simplicial complex X whose universal cover $\widetilde{X}$ is contractible. Let X_n be the set of n-simplices of X. As you know, the fundamental group $G = \pi_1 X$ acts on $\widetilde{X}$ and does not fix any points. It follows that the set of n-simplices of $\widetilde{X}$ are in bijection with $G \times X_n$. Thus the n^{th} simplicial chain group of $\widetilde{X}$ is the free $\mathbb{Z}G$-module $\mathbb{Z}G\{X_n\}$. Then the simplicial chain complex of $\widetilde{X}$ is a chain complex

$$\cdots \xrightarrow{d_{n+2}} \mathbb{Z}G\{X_{n+1}\} \xrightarrow{d_{n+1}} \mathbb{Z}G\{X_n\} \xrightarrow{d_n} \cdots \xrightarrow{d_1} \mathbb{Z}G\{X_0\}$$

Since $\widetilde{X}$ is a connected, contractible space, its homology groups vanish except for $H_0(\widetilde{X}) \cong \mathbb{Z}$. So the above sequence, augmented with a map to $\mathbb{Z}$ at the end, is an exact sequence: and is a projective resolution of $\mathbb{Z}$ by $\mathbb{Z}G$-modules.

This is a useful source of projective resolutions, for those groups which are the fundamental group of a suitably nice complex X.

Definition 5.1.17 (Group cohomology)**.** Take a projective resolution

$$\cdots \to F_{n+1} \to F_n \to \cdots \to F_0 \to \mathbb{Z} \to 0$$

of $\mathbb{Z}$ by $\mathbb{Z}G$-modules. Let M be a G-module. Take Hom-groups $\operatorname{Hom}_G(-, M)$ to obtain a sequence

$$\cdots \leftarrow \operatorname{Hom}_G(F_{n+1}, M) \xleftarrow{d^{n+1}} \operatorname{Hom}_G(F_n, M) \longleftarrow \cdots \xleftarrow{d^1} \operatorname{Hom}_G(F_0, M)$$

where d^n is the dual map of d_n.

Then the n^{th} *cohomology groups* $H^n(G, M)$ are the abelian groups

$$H^n(G, M) = \ker(d^{n+1}) / \operatorname{im}(d^n), \quad H^0(G, M) = \ker(d^1).$$

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

Remark 5.1.18. Note that after passing to Hom-groups, we dropped the '$\mathbb{Z}$ term' at the extreme right of the diagram.

Remark 5.1.19. Here d^n is the dual map

$$d^n \colon \operatorname{Hom}_G(F_{n-1}, M) \to \operatorname{Hom}_G(F_n, M), \quad \phi \mapsto \phi \circ d_n$$

For total consistency we should use the notation $d^n = d_n^*$, but for the cochain maps d^n seems more common.

Remark 5.1.20. Comparing this with Definition 5.1.10, we see that these 'cohomology groups' are just the *homology* groups of a chain complex

$$C_n = \operatorname{Hom}_G(F_{-n}, M)$$

defined in dimensions $-\infty < n \leq 0$. The switches to upper indices and the prefix 'co-' are in some sense mathematically irrelevant: they are there mainly to prevent our brains from having to think about chain complexes indexed over the negative integers.

To compare this again to the topological situation above, the chain complex

$$\cdots \xrightarrow{d_{n+2}} \mathbb{Z}\{X_{n+1}\} \xrightarrow{d_{n+1}} \mathbb{Z}\{X_n\} \xrightarrow{d_n} \mathbb{Z}\{X_{n-1}\} \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_1} \mathbb{Z}\{X_0\}$$

for X is obtained from the free resolution of $G = \pi_1 X$ by 'killing the G-action'. On the other hand, if we take the chain complex for $\widetilde{X}$ and take Hom-groups $\mathrm{Hom}_G(-, \mathbb{Z})$, where $\mathbb{Z}$ has the trivial G-action, we obtain a chain complex

$$\longleftarrow \mathrm{Hom}(\mathbb{Z}\{X_{n+1}\}, \mathbb{Z}) \xleftarrow[d^{n+1}]{} \mathrm{Hom}_G(\mathbb{Z}\{X_n\}, \mathbb{Z}) \xleftarrow[d^n]{} \cdots$$

(one should note that a G-linear map $\mathbb{Z}G\{X_n\} \to \mathbb{Z}$ is determined by the image of X_n—so are in bijection with the abelian group homomorphisms $\mathbb{Z}\{X_n\} \to \mathbb{Z}$).

In this way it is seen that $H^n(\pi_1 X, \mathbb{Z})$ is closely related to $H_n(X)$. We will not explore this relationship in depth in this course, largely because defining group homology would be more time-consuming than is really worthwhile.

Example 5.1.21. Let $G \cong \mathbb{Z}$ be generated by an element t. Consider the sequence of G-modules

$$0 \longrightarrow \mathbb{Z}G \xrightarrow[\cdot(t-1)]{d_1} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

where ϵ is the *augmentation map* which sends $g \mapsto 1$ for all $g \in G$ (with the appropriate $\mathbb{Z}$-linear extension to all of $\mathbb{Z}G$), and the map d_1 is right-multiplication[1] by $t - 1$.

This is a resolution of $\mathbb{Z}$ by projective (even free) G-modules. This may be seen via topology: it is actually the simplicial chain complex of a line. Let us also show it directly.

Obviously ϵ is surjective. It is also very easy to check that the sequence of maps above is actually a chain complex, i.e. $\epsilon(x(t-1)) = 0$ for all $x \in \mathbb{Z}G$.

Let $x = \sum n_g g$ be an element of $\mathbb{Z}G$ such that $\epsilon(x) = 0$. Since G is infinite cyclic, let us relabel this sum: each g is of the form t^k for some k, so we may write $x = \sum_{k=K}^{L} n_k t^k$ (recall that elements of $\mathbb{Z}G$ have only finitely many terms). If $\epsilon(x) = 0$ then by definition $\sum n_k = 0$. Now we have

$$\begin{aligned}
x &= n_L t^L + n_{L-1} t^{L-1} + n_{L_2} t^{L-2} + \cdots + n_K t^K \\
&= n_L t^{L-1} \cdot (t-1) + (n_L + n_{L-1}) t^{L-1} + n_{L_2} t^{L-2} + \cdots + n_K t^K \\
&= (n_L t^{L-1} + (n_L + n_{L-1}) t^{L-2}) \cdot (t-1) + (n_L + n_{L-1} + n_{L-2}) t^{L-2} + \cdots \\
&\ \ \vdots \\
&= y \cdot (t-1) + (\textstyle\sum n_k) t^K = y \cdot (t-1)
\end{aligned}$$

for some y as required.

Finally, the multiplication by $(t-1)$ map is injective: let $x = \sum n_k t^k$ be a non-zero element of $\mathbb{Z}G$. Let L be the greatest integer such that $n_L \neq 0$. Then the t^{L+1} coefficient of $x(t-1)$ is $n_L \neq 0$, so $x(t-1) \neq 0$.

Now let M be any G-module. We will compute $H^n(G, M)$. First note that we have a natural isomorphism

$$\iota\colon \mathrm{Hom}_G(\mathbb{Z}G, M) \xrightarrow{\cong} M, \quad \phi \mapsto \phi(1)$$

[1] In the present case, G is abelian so left and right multiplication agree. More generally, if G is a group and $g \in G$, then only a *right*-multiplication map $\mathbb{Z}G \to \mathbb{Z}G$, $x \mapsto xg$ would be a morphism of (left) G-modules.

since $\mathbb{Z}G$ is a free G-module with basis $\{1\}$. The dual d^1 of d_1 is given by the action of $t-1$ on M: if $\phi \in \mathrm{Hom}_G(\mathbb{Z}G, M)$ and $x \in \mathbb{Z}G$ then

$$d^1(\phi)(x) \coloneqq \phi(d_1(x)) = \phi(x(t-1))$$

hence

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

Hence the dual chain complex $\mathrm{Hom}_G(F_\bullet, M)$ is

$$0 \longleftarrow M \xleftarrow{(t-1)\cdot} M.$$

Hence

$$\begin{aligned} H^0(G,M) &= \ker((t-1)\cdot) = \{m \in M \mid tm = m\} = M^G, \\ H^1(G,M) &= M/\{(t-1)m \mid m \in M\} = M_G, \\ H^n(G,M) &= 0 \quad (n \geq 2). \end{aligned}$$

Here M^G is the group of *invariants* of M—the largest subgroup on which G acts trivially—and M_G is the group of *co-invariants* of M, which is 'dual' to the invariants M^G in the sense that it is the largest quotient of M on which G acts trivially.

The isomorphism ι used in this proof, and the corresponding computations of the dual maps d^n, are an important part of computing cohomology groups. Let us expand on this in more generality.

Let $\mathbb{Z}G\{X\}$ and $\mathbb{Z}G\{Y\}$ be free modules over finite sets X and Y. By labelling $X = \{x_1 \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_m\}$ we may consider $\mathbb{Z}G\{X\} \cong \mathbb{Z}G^n$ and $\mathbb{Z}G\{Y\} \cong \mathbb{Z}G^m$.

If $\alpha\colon \mathbb{Z}G\{X\} \to \mathbb{Z}G\{Y\}$ is a G-linear map, we may think of α as multiplication of a row vector $(r_1, \ldots, r_n) \in \mathbb{Z}G^n$ by an $n \times m$ matrix A with entries in $\mathbb{Z}G$: define elements $a_{ij} \in \mathbb{Z}G$ by

$$\alpha(x_i) = \sum_j a_{ij} y_j$$

so that

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

Now let M be a G-module. There is an isomorphism

$$\iota_X\colon \mathrm{Hom}_G(\mathbb{Z}G\{X\}, M) \to M^m$$

given by $\iota_X(\phi) = (\phi(x_1), \ldots, \phi(x_n))$. There is a similar isomorphism ι_Y. We now wish to 'compute the dual map α^* in terms of the isomorphisms ι'—i.e. to compute the map $\tilde{\alpha}$ which makes the diagram

$$\begin{tikzcd} \mathrm{Hom}_G(\mathbb{Z}G\{X\}, M) \arrow[d, "\iota_X"] & \mathrm{Hom}_G(\mathbb{Z}G\{Y\}, M) \arrow[l, "\alpha^*"'] \arrow[d, "\iota_Y"] \\ M^n & M^m \arrow[l, "\tilde{\alpha}"'] \end{tikzcd}$$

commute. Let $(b_1, \dots, b_m) \in M^m$ and let $\phi\colon \iota_Y^{-1}(b_1, \dots, b_m)$, so that $\phi(y_i) = b_i$ for each i. We can compute.

$$\begin{aligned}
\tilde{\alpha}(b_1, \dots, b_m) &= \iota_X \alpha^*(\phi) \\
&= \big(\alpha^*(\phi)(x_1), \dots, \alpha^*(\phi)(x_n)\big) \\
&= \big(\phi(\alpha(x_1)), \dots, \phi(\alpha(x_n))\big) \\
&= \big(\phi(\sum_j a_{1j} y_j), \dots, \phi(\sum_j a_{nj} y_j)\big) \\
&= ((\sum_j a_{1j} b_j), \dots, (\sum_j a_{nj} b_j)).
\end{aligned}$$

Hence $\tilde{\alpha}$ may be seen to be the multiplication of the matrix A on the left of a column vector $(b_1, \dots, b_m)^T \in M^m$.

$$\tilde{\alpha}((b_1, \dots, b_m)^T) = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} \sum_j a_{1j} b_j \\ \vdots \\ \sum_j a_{nj} b_j \end{pmatrix}$$

The fact that all cohomology groups of $\mathbb{Z}$ vanish in dimensions higher than one extends to other free groups as well.

Proposition 5.1.22. *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 fundamental group G. Then universal cover of X is a simply connected graph, i.e. a tree. It is therefore contractible. It has no simplices of dimension 2 or greater, so we have a free resolution of G of the form

$$0 \longrightarrow \mathbb{Z}G\{X_1\} \xrightarrow{d_1} \mathbb{Z}G\{X_0\} \longrightarrow \mathbb{Z} \longrightarrow 0$$

It follows that $H^n(G, M) = 0$ for all $n \geq 2$, for all G-modules M. □

Definition 5.1.23. A group G has *cohomological dimension n* if $H^m(G, M) = 0$ for all G-modules M and all $m > n$, but there exists some G-module M such that $H^n(G, M) \neq 0$. If no such n exists then G has infinite cohomological dimension.

Remark 5.1.24. The above proposition therefore says that free groups have cohomological dimension (at most) 1. Since the only fundamental groups of 1-dimensional spaces (i.e. graphs) are free, it seems natural to wonder if the converse to this proposition is true. In fact it is, by a theorem of Stallings. The proof is too involved for this course; we will however see a proof of the corresponding theorem for free pro-p groups.

Later in the course we will be needing ways to compare different chain complexes, as well as cohomology groups with different coefficients. The following propositions provide the basic language.

Definition 5.1.25. Let (A_n, α_n) and (B_n, β_n) be chain complexes. A *chain map* (f_n) is a sequence of G-linear maps $f_n \colon A_n \to B_n$ such that for all n we have $\beta_n f_n = f_{n-1}\alpha_n$.

$$\begin{tikzcd}
A_n \arrow[r, "\alpha_n"] \arrow[d, "f_n"] & A_{n-1} \arrow[d, "f_{n-1}"] \\
B_n \arrow[r, "\beta_n"] & B_{n-1}
\end{tikzcd}$$

Proposition 5.1.26. *If (f_n) is a chain map from (A_n, α_n) to (B_n, β_n) then (f_n) induces a well-defined map on the homology groups of the complexes*

$$f_* \colon H_n(A_\bullet) \to H_n(B_\bullet).$$

Moreover, these maps are functorial: if $(g_n) \colon (B_n) \to (C_n)$ is another chain map then

$$(gf)_* = g_* f_* \colon H_n(A_\bullet) \to H_n(C_\bullet).$$

Proof. If $x \in \ker \alpha_n$ then define $f_*([x]) = [f_n(x)]$, where $[x]$ denotes the class $x + \operatorname{im} \alpha_{n+1} \in H_n(A_\bullet)$. First note that $f_n(x) \in \ker \beta_n$ defines a valid class in $H_n(B_\bullet)$, since

$$\beta_n f_n(x) = f_{n-1}\alpha_n(x) = f_{n-1}(0) = 0.$$

Morevover the choice of representative for the class $[x]$ does not matter: if $x' + \operatorname{im} \alpha_{n+1} = x + \operatorname{im} \alpha_{n+1}$, then $x' = x + \alpha_{n+1}(y)$ for some y and

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

hence $[f_n(x)] = [f_n(x')]$. The other properties follow immediately. □

Corollary 5.1.27. *Let $f \colon M \to N$ be a map of G-modules. Then there is an induced functorial map*

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

for each n.

Proof. For a projective resolution (F_n) of $\mathbb{Z}$ by G-modules, apply the previous propostion to the chain map given by

$$\operatorname{Hom}_G(F_n, M) \to \operatorname{Hom}_G(F_n, N), \quad \phi \mapsto f \circ \phi$$

□

These functorial maps on cohomology are not the only relations between cohomology for different coefficient groups—there is also the following *long exact sequence*, derived via the snake lemma.

Proposition 5.1.28. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a short exact sequence of G-modules. Then there is an exact sequence*

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

The proof of this result comprises two ingredients, one of which you have already seen last year.

Lemma 5.1.29 (Snake Lemma). *Let*

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

be a short exact sequence of chain complexes—that is, $f_\bullet$ and $g_\bullet$ are chain maps and the corresponding sequences of abelian groups are exact for each n.

Then there exist maps $\delta_n \colon H_{n+1}(C_\bullet) \to H_n(A_\bullet)$ such that the sequence

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

is exact.

Proof. Proof not examinable on this course—see Part II Algebraic Topology. □

Lemma 5.1.30. *Let*

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

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

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

is exact.

Proof. There are three statements to prove.

- $\ker f_* = 0$. Let $\phi \in \mathrm{Hom}_G(F, M_1)$. If $f_*\phi = 0$ then for all $x \in F$, $f(\phi(x)) = 0$, whence $\phi(x) = 0$ since f is injective.
- $\ker g_* = \operatorname{im} f_*$. Since $gf = 0$, $g_*f_* = 0$ so the inclusion $\supseteq$ is immediate. Now let $\psi \in \ker g_* \subseteq \mathrm{Hom}_G(F, M_2)$. Then for all $x \in F$ we have $g(\psi(x)) = 0$, so by exactness of the original sequence there exists a unique $y \in M_1$ such that $f(y) = \psi(x)$. Define $\phi(x) = y$. It is easy to check (using the uniqueness of y) that this map ϕ is G-linear and has $f_*\phi = \psi$—so $\phi \in \operatorname{im} f_*$ as required.
- $\operatorname{im} g_* = \mathrm{Hom}_G(F, M_3)$. This follows immediately from the hypothesis that F is projective.

□

Proof of Proposition 5.1.28. Consider a resolution $F_\bullet$ of $\mathbb{Z}$ by projective G-modules. Then by the second lemma above, we have a short exact sequence of chain complexes

$$0 \longrightarrow \mathrm{Hom}_G(F_\bullet, M_1) \xrightarrow{f_*} \mathrm{Hom}_G(F_\bullet, M_2) \xrightarrow{g_*} \mathrm{Hom}_G(F_\bullet, M_3) \longrightarrow 0$$

Now apply the Snake Lemma. □

Remark 5.1.31. The indices in Proposition 5.1.28 may appear to be going the 'wrong way' relative to the Snake Lemma—from H^n to H^{n+1}. This is a consequence of the relabelling in Remark 5.1.20: recall that $\mathrm{Hom}_G(F_\bullet, M)$ should really be thought of as having negative dimensions, so our snake map is, in accordance with the Snake Lemma, going from H_{-n} to H_{-n-1}.

5.2 Different projective resolutions

We have not yet addressed an important question about the definition of cohomology: does the particular projective resolution we choose matter? It does not[2], as we will now show. This could be regarded as analogous to homotopy equivalence of homology of spaces; you may recognise the use of chain homotopies below from Part II Algebraic Topology.

Theorem 5.2.1. *The definition of $H^n(G, M)$ does not depend on the choice of projective resolution.*

Proof (Non-examinable, except for the construction of the maps f_n). Take projective resolutions (F_n, d_n) and (F'_n, d'_n) of $\mathbb{Z}$ by $\mathbb{Z}G$-modules. Suppose we can build the following:

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

The chain maps f_n give chain maps $f_n^* \colon \mathrm{Hom}_G(F'_n, M) \to \mathrm{Hom}_G(F_n, M)$, which induce homomorphisms from the cohomology of G with respect to F'_n to that with respect to F_n. Similarly for g_n.

These maps on cohomology are isomorphisms: let $\phi \in \ker d^{n+1}$ be an n-cocycle. We show that $f_n^* g_n^*(\phi)$ differs from ϕ by a coboundary—so that on the level of cohomology, $f_n^* g_n^* = \mathrm{id}$. For $x \in F_n$ we have:

$$\begin{aligned}
f_n^* g_n^*(\phi)(x) &= \phi(g_n f_n(x)) \\
&= \phi(x) + \phi(d_{n+1}s_n(x)) + \phi(s_{n-1}d_n(x)) \\
&= \phi(x) + s_n^* d^{n+1}\phi(x) + d^n(s_{n-1}^*(\phi))(x) \\
&= \phi(x) + 0 + d^n(s_{n-1}^*(\phi))(x)
\end{aligned}$$

so $f_n^* g_n^*(\phi) = \phi + d^n(s_{n-1}^*(\phi))$ as required. Similarly $g_n^* f_n^* = \mathrm{id}$ on cohomology.

It only remains to actually construct all the maps f_n, g_n, s_n and s'_n. The symmetry of the situation means we only actually construct the f_n and s_n. This is where the assumption that the resolution is projective becomes useful at last.

The first step is the easiest: considering the '$\mathbb{Z}$' at the end of the projective resolution (F_n) to be the 'dimension -1 term', set $f_{-1} = \mathrm{id} \colon \mathbb{Z} \to \mathbb{Z}$. Next, inductively assume that we have constructed f_{n-1} and f_n with the required property. Consider the map $f_n d_{n+1} \colon F_{n+1} \to F'_n$. We have

$$d'_n \circ (f_n d_{n+1}) = f_{n-1} d_n d_{n+1} = 0$$

so $f_n d_{n+1}$ maps F_{n+1} into $\ker d'_n$.

$$\begin{tikzcd}
 & F_{n+1} \arrow[r, "d_{n+1}"] \arrow[dl, red, "f_{n+1}"'] \arrow[d, red, "f_n d_{n+1}"] & F_n \arrow[r, "d_n"] \arrow[d, "f_n"] & F_{n-1} \arrow[d, "f_{n-1}"] \\
F'_{n+1} \arrow[r, two heads, "d'_{n+1}"] & \ker d'_n \arrow[r, "\subseteq"] & F'_n \arrow[r, "d'_n"] & F'_{n-1}
\end{tikzcd}$$

[2] At this stage of the course it would be rather surprising if it did...

By exactness of the sequence (F'_n), the kernel $\ker d'_n$ is the image of F'_{n+1} under the map d'_{n+1}. Therefore, *because* F_{n+1} *is projective*, there exists some $f_{n+1} \colon F_{n+1} \to F'_{n+1}$ such that $d'_{n+1} f_{n+1} = f_n d_{n+1}$ as required.

To build the s_n, first set $h_n = g_n f_n - \mathrm{id} \colon F_n \to F_n$ and note that this is a chain map with $h_{-1} = 0$. Set s_{-1} to be the zero map $\mathbb{Z} \to F_0$. To get started, note that $d_0 h_0 = h_{-1} d_0 = 0$, so h_0 maps F_0 into $\ker d_0$. As before, since (F_n) is exact, the map $d_1 \colon F_1 \to \ker d_0$ is surjective, so by projectivity of F_0 there exists some $s_0 \colon F_0 \to F_1$ such that $h_0 = d_1 s_0 = d_1 s_0 + s_{-1} d_0$ as required.

$$\begin{tikzcd}
& F_0 \arrow[dl, "s_0"'] \arrow[d, "h_0"] \arrow[dr, "h_0"] \arrow[rr, "d_0"] & & \mathbb{Z} \arrow[d, "0"] \\
F_1 \arrow[r, two heads, "d_1"] & \ker d_0 \arrow[r, "\subseteq"] & F_0 \arrow[r, "d_0"] & \mathbb{Z}
\end{tikzcd}$$

Now suppose for an induction that s_{n-1} and s_{n-2} have been constructed with the desired properties. Consider the map

$$t_n = h_n - s_{n-1} d_n \colon F_n \to F_n$$

We have

$$\begin{aligned}
d_n t_n &= d_n h_n - d_n s_{n-1} d_n \\
&= h_{n-1} d_n - (h_{n-1} - s_{n-2} d_{n-1}) d_n \\
&= s_{n-2} d_{n-1} d_n = 0
\end{aligned}$$

so t_n maps F_n to $\ker d_n$. As before, exactness and projectivity give the existence of $s_n \colon F_n \to F_{n+1}$ such that $d_{n+1} s_n = t_n = h_n - s_{n-1} d_n$, as required.

$$\begin{tikzcd}
& F_n \arrow[dl, "s_n"'] \arrow[d, "t_n"] \arrow[dr, "h_n"] \arrow[rr, "d_n"] & & F_{n-1} \arrow[d, "h_{n-1}"] \arrow[dl, "s_{n-1}"'] \\
F_{n+1} \arrow[r, two heads, "d_{n+1}"] & \ker d_n \arrow[r, "\subseteq"] & F_n \arrow[r, "d_n"] & F_{n-1}
\end{tikzcd}$$

□

It is important to note that this proposition (more specifically, the construction of the f_n) gives an explicit constructive means of switching between different projective resolutions. We will see an example later, where we switch between an easy-to-compute resolution arising from topology and a rather bulky but technically useful resolution called the *bar resolution*[3]. Let us meet this resolution. You should note the similarity the differential maps here have with simplicial boundary maps from Part II Algebraic Topology.

Let $G^{(n)}$ denote the set of symbols

$$G^{(n)} = \{[g_1|g_2|\cdots|g_n] \text{ such that } g_1, \ldots, g_n \in G\}$$

By convention, $G^{(0)}$ consists of one ‘empty’ symbol [].

[3] For the very intuitive reason that the notation has bars in it.

Let $F_n = \mathbb{Z}G\{G^{(n)}\}$ be the free $\mathbb{Z}G$ module with basis $G^{(n)}$. Define a map $d_n\colon F_n \to F_{n-1}$ by the formula

$$\begin{aligned} d_n([g_1|g_2|\cdots|g_n]) &= g_1 \cdot [g_2|g_3|\cdots|g_n] - [g_1g_2|g_3|\cdots|g_n] \\ &\quad + [g_1|g_2g_3|\cdots|g_n] - \cdots + (-1)^{n-1}[g_1|g_2|\cdots|g_{n-1}g_n] \\ &\quad +(-1)^n[g_1|g_2|\cdots|g_{n-1}] \end{aligned}$$

on basis elements—with the natural G-linear extension to all of F_n. It is an elementary (if somewhat tedious to write) calculation exercise to show that $d_{n-1}d_n = 0$. So (F_n, d_n) is indeed a chain complex. It remains a chain complex if we append the natural map $F_0 \to \mathbb{Z}$, $[] \mapsto 1$. To show that it is a *resolution* of $\mathbb{Z}$, we must show exactness.

Proposition 5.2.2. *The bar resolution is exact.*

Proof (non-examinable). To show exactness, we take the perhaps surprising step of forgetting the G-action—we will regard $F_\bullet$ as a chain complex of abelian groups. This doesn't affect exactness of course, which is simply a statement about the kernels and images of some maps. So for this proof we regard F_n as a free abelian group with basis

$$G \times G^{(n)} = \{g_0[g_1|g_2|\cdots|g_n] \text{ such that } g_0, \ldots, g_n \in G\}$$

We define a sequence of group homomorphisms $s_n\colon F_n \to F_{n+1}$ such that

$$\mathrm{id}_{F_n} = d_{n+1}s_n + s_{n-1}d_n$$

This is sufficient to prove the result: if $x \in \ker d_n$, then

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

so the sequence is exact.

The maps s_n are defined on the basis $G \times G^{(n)}$ of the free abelian group F_n by

$$s(g_0[g_1|g_2|\cdots|g_n]) = [g_0|g_1|g_2|\cdots|g_n]$$

Note that this map is *not* G-linear. It is only left to check that the required relation

$$\mathrm{id}_{F_n} = d_{n+1}s_n + s_{n-1}d_n$$

holds on the basis $G \times G^{(n)}$. This computation is left to the reader. □

The bar resolution has advantages and disadvantages. The key disadvantage is that the chain groups F_n are enormous: even if G is finite, then F_n is a free abelian group of rank $|G|^{n+1}$. However, the bar resolution is very useful theoretically: it is defined in the same way for all groups G and is totally explicit, making it good for constructions. It is also worth noting that the existence of the bar resolution is the first proof we have seen of the existence of *any* projective resolution for an arbitrary group G—and it is a *free* resolution, meaning that we may always allow ourselves to take a free resolution to prove a technical result if it simplifies matters. We will see in the next section one crucial appearance of the bar resolution in low dimensions.

First we make some additional definitions.

Definition 5.2.3. The group of *n-cochains* of G with coefficients in a G-module M is the abelian group

$$C^n(G, M) = \{\text{functions } \phi\colon G^n \to M\}.$$

Note that this is canonically isomorphic to the group $\mathrm{Hom}_G(F_n, M)$, where F_n is as in the bar resolution, since a G-linear map $F_n \to M$ is uniquely determined by its restriction to basis elements.

The n^{th} coboundary map is the map

$$d^n\colon C^{n-1}(G, M) \to C^n(G, M)$$

dual to the map d_n in the bar resolution. That is, for $\phi \in C^{n-1}(G, M)$,

$$\begin{aligned}(d^n\phi)(g_1, \ldots, g_n) &= g_1 \cdot \phi(g_2, g_3, \ldots, g_n) - \phi(g_1g_2, g_3, \ldots, g_n)\\ &+ \phi(g_1, g_2g_3, \ldots, g_n) - \cdots + (-1)^{n-1}\phi(g_1, g_2, \ldots, g_{n-1}g_n)\\ &+ (-1)^n\phi(g_1, g_2, \ldots, g_{n-1}).\end{aligned}$$

The group of *n-cocycles* is

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

and the group of *n-coboundaries* is

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

Note that

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

Remark 5.2.4. The terms 'coboundary' and 'cocycle' were actually defined earlier for arbitrary projective resolutions. Unless there is a particular resolution being used in a particular context, these words generally refer to the coboundaries and cocycles of the bar resolution.

The bar resolution allows us to give general interpretations of H^0 and H^1.

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

$$H^0(G, M) = M^G.$$

A crossed homomorphism *is a function $\phi\colon G \to M$ such that*

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

for all $g, h \in G$. A principal *crossed homomomorphism is a map ϕ of the form*

$$\phi(g) = gm - m$$

for some $m \in M$. Then principal crossed homomorphisms are crossed homomorphisms, and

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

In particular, if M is a trivial G-module then

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

is the set of group homomorphisms $G \to M$.

What about $H^2(G, M)$? That will be the topic of the next section.

The bar resolution also allows us to build natural maps between the cohomologies of different groups.

Proposition 5.2.6. *Let $\alpha\colon G_1 \to G_2$ be a group homomorphism. Let M be a G_2-module and let G_1 act on M via*

$$g_1 \cdot m := \alpha(g_1) \cdot m$$

for $g_1 \in G_1$, $m \in M$. Then there is a natural homomorphism

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

If $\beta\colon G_0 \to G_1$ then $\beta^*\alpha^* = (\alpha\beta)^*$.

Remark 5.2.7. Here 'natural' carries the meaning that no choices are made in the definition. In particular this means that these natural maps repect whatever constructions are made using homology: for example, given a short exact sequence of G_2-modules, the maps f^* will fit into a commuting diagram relating the corresponding long exact sequences of cohomology groups for G_1 and G_2. We won't be exploiting this connection much in this course, so we won't trouble to make this remark more precise.

Proof. Define maps $\alpha^*\colon C^n(G_2, M) \to C^n(G_1, M)$ by

$$(\alpha^*\phi)(g_1, g_2, \ldots, g_n) = \phi(\alpha(g_1), \ldots, \alpha(g_n))$$

These maps clearly commute with the differential maps, hence are chain maps and induce maps of the cohomology groups as required by Proposition 5.1.26. □

The presence of these maps can lead one to ask more detailed questions about the relationship between the cohomologies of different groups. In particular, given a short exact sequence of groups

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

(i.e., H is a normal subgroup of G and $G/H = Q$), is there a long exact sequence of cohomology groups analogous to Proposition 5.1.28? The disappointing answer is that there is not, and the relationship between the cohomologies of H, G and Q is considerably more complicated than the course time allows us to discuss[4]. An obvious counterexample to the hoped-for long exact sequence would be given by the short exact sequence of groups

$$0 \to \mathbb{Z} \to \mathbb{Z}^2 \to \mathbb{Z} \to 0$$

since $H^2(\mathbb{Z}, \mathbb{Z}) = 0$ but $H^2(\mathbb{Z}^2, \mathbb{Z}) \neq 0$.

For this course we content ourselves with seeing relationships in low dimensions (which are often the most useful parts anyway).

[4] Search online for 'spectral sequences', if you really must know.

Lemma 5.2.8. *Let H be a normal subgroup of G and let M be a G-module. Let G act on the set of cochains $C^n(H,M)$ by*

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

Then this descends to an action of G on $H^n(H,M)$. Moreover the action of H on this cohomology group is trivial (so we may regard this as an action of G/H on $H^n(H,M)$ if we wish).

Proof. To show that we have an action on cohomology it suffices to show that the action of an element $g\in G$ is a chain map—i.e. $g\cdot(d^n\phi)=d^n(g\cdot\phi)$ for all $\phi\in C^{n-1}(H,M)$. We have

$$\begin{aligned}
g\cdot(d^n\phi)(h_1,\dots,h_n) &= g(g^{-1}h_1g)\phi(g^{-1}h_2g,\dots,g^{-1}h_ng)\\
&\quad -g\phi(g^{-1}h_1gg^{-1}h_2g,\dots,g^{-1}h_ng)+\cdots\\
&= h_1g\phi(g^{-1}h_2g,\dots,g^{-1}h_ng)\\
&\quad -g\phi(g^{-1}h_1h_2g,\dots,g^{-1}h_ng)+\cdots\\
&= h_1(g\cdot\phi)(h_2,\dots,h_n)-(g\cdot\phi)(h_1h_2,\dots,h_n)+\cdots\\
&= d^n(g\cdot\phi)(h_1,\dots,h_n)
\end{aligned}$$

as required. To show that H acts trivially, we must take a cocycle and show that applying the action of $h\in H$ only adds a coboundary. We will only write out this proof for 1-cocycles; the other cases are fundamentally the same, but are simply more painful to write out.

Let $\phi\in Z^1(H,M)$ and let $h,h_1\in H$. Then, using several times the relation $\phi(h_1h_2)=h_1\phi(h_2)+\phi(h_1)$ for all $h_1,h_2\in H$, we find

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

which is indeed a coboundary $\psi(h_1)=(h_1-1)\phi(h)$. □

A simple but often useful case of this proposition is the case $n=1$. Here $\phi\in H^1(H,M)$ is represented by a crossed-homomorphism $\phi\colon H\to M$, with G-action given by

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

In particular, ϕ lies in the space of invariants $H^1(H,M)^G$ if and only if

$$[\phi(ghg^{-1})]=[g\phi(h)]$$

for all $h\in H$ and $g\in G$. If the action of G on M is trivial, this may be termed a 'G-invariant homomorphism $H\to M$'.

Theorem 5.2.9 ('Five term exact sequence')**.** *Let H be a normal subgroup of G, let $Q=G/H$ and let M be a G-module. Then there is an exact sequence*

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

Remark 5.2.10. Note that there is no '$\to 0$' at the end; there is no statement that the final map is surjective.

Proof (Non-examinable sketch; definition of maps only). We will omit most of the proof of this result from the course, and only trouble to define the maps involved. The rest of the proof—checking that the maps are well-defined, and checking exactness at all positions—consists of tedious but elementary checks which it would not be beneficial to spend time on.

The maps in the sequence are as follows. The definitions are given on the level of cochains, and to check that they really induce the desired maps on cohomology is part of the omitted tedium.

- *Restriction maps*

$$H^k(G,M) \to H^k(H,M)^Q$$
$$(f\colon G^k \to M) \mapsto (\mathrm{Res}(f)\colon H^k \hookrightarrow G^k \xrightarrow{f} M)$$

- *Inflation maps*

$$H^k(Q,M^H) \to H^k(G,M)$$
$$(f\colon Q^k \to M^H) \mapsto (\mathrm{Inf}(f)\colon G^k \to Q^k \xrightarrow{f} M^H \subseteq M)$$

- The *transgression map* $\mathrm{Tg}\colon H^1(H,M)^Q \to H^2(Q,M^H)$, defined in the following manner. Let $s\colon Q \to G$ be a set-theoretic section with $s(1) = 1$—that is, a function $s\colon Q \to G$ such that $s(gH)H = gH$ for all $gH \in G/H = Q$. Define $\rho\colon G \to H$ by $\rho(g) = gs(gH)^{-1}$ (where $gH \in G/H = Q$ is a right coset).

  Take a 1-cohomology class which is invariant under the action of Q and let $f\colon H \to M$ be some cocycle represnting this class. Define the cochain $\mathrm{Tg}(f)\colon G^2 \to M$ by

$$\mathrm{Tg}(f)(g_1,g_2) = f(\rho(g_1)\rho(g_2)) - f(\rho(g_1g_2)).$$

  Changing g_1 and g_2 by multiplying by elements of H does not in fact change the value of this cochain, so this defines a cochain $Q^2 \to M$.

□

As may be guessed from the fact that $H^2(G)$ is left dangling at the end of the sequence in this theorem, this sequence is generally more useful in cases where we know a good deal about G already and hope to learn more about the quotient group Q. One classical example is the following corollary, which deals with relating cohomology to a presentation of a group.

Corollary 5.2.11 (Hopf's Formula). *Let F be a free group, let R be a normal subgroup of F and let $Q = F/R$. Let A be an abelian group, considered as a trivial module over F. Then*

$$H^2(Q,A) \cong \frac{\{F\text{-invariant homomorphisms } f\colon R \to A\}}{\{\text{Homomorphisms } F \to A\}}$$

Proof. Apply the Five Term Exact Sequence, noting that free groups have vanishing second cohomology and using the characterisation of H^1 given in Corollary 5.2.5. □

It is important to note that R is in general an infinitely generated group, so this formula is rather difficult to compute with in practice.

One immediate application is to get bounds on the size of cohomology groups. We already know that, for example.

$$d(H^1(Q,\mathbb{Z})) = d(\mathrm{Hom}(Q,\mathbb{Z})) \leq d(Q)$$

since any homomorphism is determined by its image on a generating set of Q. If we have a presentation of Q,

$$Q = \langle x_1, \ldots, x_d \,|\, r_1, \ldots, r_m \rangle$$

then $R = \langle\!\langle r_1, \ldots, r_m \rangle\!\rangle^F$ and an F-invariant homomorphism $R \to \mathbb{Z}$ is determined by its image on the r_i. It follows that

$$d(H^1(Q,\mathbb{Z})) \leq d, \quad d(H^2(Q,\mathbb{Z})) \leq m.$$

One might be tempted to hope that these are always equalities, at least if the presentation Q is 'minimal' in some sense. In fact this is not true—but at the end of the course we will find that a suitable version of this statement does hold for pro-p groups.

We will use both Hopf's formula and the Five Term Exact Sequence to great effect later when dealing with pro-p groups; for now let us just consider the following simple example.

Example 5.2.12. Let $Q = \mathbb{Z}/3\mathbb{Z}$, and let Q act on $M = \mathbb{Z}^2$ via the order 3 matrix $A = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$. Consider the short exact sequence of groups

$$0 \to H = \mathbb{Z} \xrightarrow{3} G = \mathbb{Z} \to Q \to 0.$$

Since H acts trivially on M, we have

$$H^1(H,M) = \mathrm{Hom}(\mathbb{Z},M) \cong \mathbb{Z}^2$$

An element of this group is Q-invariant if and only if the corresponding element of $\mathbb{Z}^2$ is fixed by A. The only solution of $Ax = x$ is zero, so $H^1(H,M)^Q = 0$. Since $H^2(G,M) = 0$ also, it follows from the five term exact sequence that $H^2(\mathbb{Z}/3\mathbb{Z},M) = 0$.

5.3 Cohomology and group extensions

Let us now turn to a problem which at first sight has nothing to do with cohomology, but is in fact intimately connected. Suppose we have a group E, which contains an abelian normal subgroup M. Let $E/M = G$. Such an E is called an *extension of G by M*[5]. There is a natural notion of equivalence between extensions: group isomorphisms which 'remember G and M'. That is, extensions

[5] Or sometimes 'an extension of M by G', because mathematicians cannot necessarily remember which way round it goes.

E and E' of G by M are *equivalent* if there is a commuting diagram of group homomorphisms

$$\begin{tikzcd}
 & & E \arrow[dd] \arrow[dr] & & & \\
1 \arrow[r] & M \arrow[ur] \arrow[dr] & & G \arrow[r] & 1 \\
 & & E' \arrow[ur] & & &
\end{tikzcd}$$

It is an exercise to show that equivalent extensions are isomorphic as groups. The converse is not necessarily true: you will see an example of this on the example sheet.

How might one go about classifying extensions up to equivalence? The first thing to note is that M is not just an abelian group, but comes with the structure of a G-module. The group E acts on its normal subgroup M by conjugation. The action of M on itself is trivial since M is abelian, so this descends to an acton of G on M by homomorphisms. If the G-action is trivial, then M is central in E and E is called a *central extension.*

Given a group G and a G-module M, there is always one extension that can be constructed: the *semi-direct product*[6] $E = M \rtimes G$, which you met in Part IB. The underlying set of this group is $M \times G$, with multiplication given by

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

Remark 5.3.1 (Notational health warning). In the formula above, G is written as a group with multiplication operation, and the abelian group M is written with additive notation. This makes total sense in the context; however earlier on this page we have M being a subgroup of the (perhaps non-abelian) group E, where really the group operation is multiplicative. The answer to this quandry is to simply that we never really calculate much in E, but I felt I should give the warning.

It is easy to check that the semi-direct product is an extension of G by M. Could it be the only one?

The semidirect product has a very special property among extensions: G, as well as being a quotient of $E = M \rtimes G$, is also a *subgroup* of E (the subgroup $\{0\} \times G$ in the notation above). Expressed abstractly, this means that there is a group homomorphism $s\colon G \to M \rtimes G$ such that the composite $G \to M \rtimes G \to G$ is the identity map. Such a map is called a *splitting*, so another name for 'semi-direct product' is *split extension.*

Proposition 5.3.2. *Let E be an extension of G by M. Assume there is a spitting $s\colon G \to E$. Then E is equivalent to the semidirect product $M \rtimes G$.*

Proof. Exercise. □

Now let E be an extension of G by M. Let $\pi\colon E \to G$ be the quotient map. We will try to measure how far it is from being a semidirect product—in

[6] Observe the order of the notation: G acts on the *left* of M, and is written to the *right* in the semidirect product $M \rtimes G$. The formula for multiplication in the semidirect product makes it obvious why we do this.

other words, what is the obstruction to the existence of a splitting $G \to E$? We can always find a *set-theoretic section* $s\colon G \to E$—that is, a *function* such that $G \xrightarrow{s} E \xrightarrow{\pi} G$ is the identity, but which is not necessarily a group homomorphism. Such an s is simply a choice of preimage $s(g) \in E$ for each $g \in G$. Without loss of generality assume $s(1) = 1$. To measure how far s is from being a group homomorphism, consider the function

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

which vanishes if and only if s is a group homomorphism. Note that applying the quotient map $\pi\colon E \to G$ sends $\phi(g_1, g_2)$ to the identity, so in fact $\phi(g_1, g_2)$ is an element of M. That is, $\phi\colon G^2 \to M$ is a 2-cochain.

More than this, ϕ is a 2-*cocycle*. To see this, calculate $s(g_1)s(g_2)s(g_3)$ in two different ways:

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

If we equate these two values, cancel the $s(g_1g_2g_3)$ term, convert the remainder into the additive notation we use in M, and remember that the action of G is defined by conjugation, this becomes

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

which, rearranged, gives the familiar form

$$0 = g_1 \cdot \phi(g_2, g_3) - \phi(g_1g_2, g_3) + \phi(g_1, g_2g_3) - \phi(g_1, g_2) = (d^3\phi)(g_1, g_2, g_3)$$

so ϕ is indeed a cocycle.

Note that ϕ is also a *normalized* cocycle, in the sense that

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

To summarise, an extension of G by M, together with a choice of the set-theoretic section s, gives a normalized 2-cocycle $\phi \in Z^2(G, M)$. What difference does a different choice of s make? Let $s'\colon G \to E$ be another set-theoretic section with $s'(1) = 1$. Then $\pi(s(g)s'(g)^{-1}) = 1$ for all g, so $s'(g)s(g)^{-1} = \psi(g)$ is a function $G \to M$. Let us compute the new cocycle ϕ' corresponding to s'.

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

Thus we find (again swapping to the additive notation) that

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

so that ϕ and ϕ' differ by a coboundary.

We have now proved part of the following theorem.

Theorem 5.3.3. *Let G be a group and let M be a G-module. There is a* bijection

$$\begin{Bmatrix}\text{Equivalence classes of}\\ \text{extensions of } G \text{ by } M\end{Bmatrix} \longleftrightarrow H^2(G,M)$$

We have so far proved the existence of a map from the set of extensions to $H^2(G,M)$. The details of the remainder of the proof are largely left as an exercise, and consists of the following parts:

- proving that equivalent extensions yield the same element of $H^2(G,M)$;
- constructing the inverse map, which takes a cohomology class and builds an extension class from it; and
- proving that these two maps are inverse to each other.

The most important part to note for future use is the inverse map. Let $[\phi] \in H^2(G,M)$ be a cohomology class represented by a normalized cocycle $\phi \in Z^2(G,M)$. All cohomology classes may be represented by a normalized cocycle; we prove this in Lemma 5.3.4, but delay that lemma until later to maintain the flow of the argument. Define a group structure E_ϕ on the set $M \times G$ by the formula

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

The fact that this really is a group multiplication—that is, it is associative and elements have inverses—follows from the property that ϕ is a normalized cocycle, by calculations very similar to those above which take a group and derive a cocycle from it.

That E_ϕ really is an extension of G by M is readily established; M embeds as the subgroup $M \times \{0\} \subseteq E_\phi$, and the set projection $M \times G \to G$ is a group homomorphism.

Finally, if ϕ' is another normalized cocycle representing the class $[\phi]$, so that $\phi - \phi'$ is a coboundary $d^2\psi$, then we may define a map $E_\phi \to E_{\phi'}$ by

$$(m, g) \mapsto (m + \psi(g), g)$$

This is a group homomorphism, and in fact an equivalence of extensions (this uses the fact that $\psi(1) = 0$, which derives from the normalization of the cocycles ϕ and ϕ').

The proof concludes with the delayed lemma on normalization of 2-cocycles.

Lemma 5.3.4. *Let $\phi \in Z^2(G,M)$. Then there is a cochain $\psi \in C^1(G,M)$ such that $\phi + d^2\psi$ is normalized. Hence every cohomology class in $H^2(G,M)$ is represented by a normalized cocycle.*

Proof. Let $\psi(g) = -\phi(1,g)$. Then

$$(\phi + d^2\psi)(1,g) = \phi(1,g) - (\phi(1,g) - \phi(1,g) + \phi(1,1)) = \phi(1,g) - \phi(1,1)$$

and

$$(\phi + d^2\psi)(g,1) = \phi(g,1) - (g \cdot \phi(1,1) - \phi(1,g) + \phi(1,g)) = \phi(g,1) - g \cdot \phi(1,1).$$

By computing $d^3\phi(1,1,g) = 0$ and $d^3\phi(g,1,1) = 0$ respectively one finds that both these expressions vanish as required. □

Having established that extensions correspond with elements of $H^2(G,M)$, let us remark upon a neat connection with Hopf's formula from earlier.

Suppose that G has a presentation

$$G = \langle x_1, \dots, x_n \mid r_1, \dots, r_m \rangle$$

and suppose that A is an abelian group (considered as a trivial module). Let E be a central extension of G by A. Then E is generated by A together with the images $\bar{x}_1, \dots, \bar{x}_n$ of the generators of G under some section $G \to E$. If we define $\bar{r}_i$ to be the word r_i, written as a word in the $\bar{x}_i$ by replacing each x_i with $\bar{x}_i$, then since r_i vanishes in G, the element $\bar{r}_i$ of E must equal some $a_i \in A$. Define therefore group by a presentation

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

It is not difficult to show that this is actually a presentation of E, by considering the obvious diagram

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

Now let F be the free group generated by $x_1, \dots, x_n$ and let R be the kernel of the natural map $F \to G$. One may attempt to define an F-invariant homomorphism $R \to A$ by sending $r_i \mapsto a_i$. In fact it follows from the fact that E is genuinely an extension of G by A that this map is really a well-defined F-invariant homomorphism.

This homomorphism depends on the initial choice of section $x_i \mapsto \bar{x}_i$ of $E \to G$. Choosing a different section corresponds to an operation $\bar{x}_i \mapsto \bar{x}_i b_i$ where $b_i \in A$. This choice of b_i specifies a homomorphism $b \colon F \to A$, and our map $R \to A$ is changed by subtracting the restriction of b. In this way we recover the correspondence

$$H^2(G,A) \cong \frac{\{F\text{-invariant homomorphisms } f \colon R \to A\}}{\{\text{Homomorphisms } F \to A\}}$$

from Hopf's formula.

This is not necessarily a terribly good way to go about computing the cohomology of a group: given an assignment $r_i \mapsto a_i$ it is rather difficult to check whether it genuinely gives a well-defined F-invariant map. However in some circumstances it can be a useful methodology to prove that certain extensions are equivalent.

Example 5.3.5. Let G be the group with presentation

$$G = \langle x_1, x_2 \mid x_1 x_2 x_1^{-1} x_2^{-1} x_1 \rangle.$$

We claim that $H^2(G,\mathbb{Z}) = 0$. Let a generator of $\mathbb{Z}$ be labelled a. Then any central extension of G by $\mathbb{Z}$ has a presentation of the form

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

for some $k \in \mathbb{Z}$. Now the substitution $\bar{x}_1 \mapsto \bar{x}_1 a^k$ has the effect

$$\bar{x}_1 \bar{x}_2 \bar{x}_1^{-1} \bar{x}_2^{-1} \bar{x}_1 a^{-k} \mapsto \bar{x}_1 a^k \bar{x}_2 \bar{x}_1^{-1} a^{-k} \bar{x}_2^{-1} \bar{x}_1 a^k a^{-k} = \bar{x}_1 \bar{x}_2 \bar{x}_1^{-1} \bar{x}_2^{-1} \bar{x}_1$$

since a is central; so our presentation becomes

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

the presentation of the split extension $\mathbb{Z} \times G$. Hence all extensions of G by $\mathbb{Z}$ are split, and $H^2(G, \mathbb{Z}) = 0$.

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

In this section we will classify the central extensions of $\mathbb{Z}^2$ by $\mathbb{Z}$. Firstly we compute the cohomology groups of $T = \mathbb{Z}^2$. Let a and b denote generators of T. Begin with the free resolution

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

of $\mathbb{Z}$, where

$$\beta(z) = (z \cdot (1-b), z \cdot (a-1)), \quad \alpha(x, y) = x \cdot (a-1) + y \cdot (b-1)$$

and ϵ is the augmentation map. This may be proved to be exact either directly–in a similar way to Example 5.1.21—or by noting that it is a cellular chain complex for the square tiling of the plane.

Applying $\mathrm{Hom}_T(-, \mathbb{Z})$ gives a chain complex

$$0 \longleftarrow \mathrm{Hom}_G(\mathbb{Z}T, \mathbb{Z}) \xleftarrow{\beta^*=0} \mathrm{Hom}_G(\mathbb{Z}T^2, \mathbb{Z}) \xleftarrow{\alpha^*=0} \mathrm{Hom}_G(\mathbb{Z}T, \mathbb{Z})$$

whence $H^2(T, \mathbb{Z}) = \mathrm{Hom}_T(\mathbb{Z}T, \mathbb{Z}) \cong \mathbb{Z}$, with generator represented by the augmentation map $\mathbb{Z}T \to \mathbb{Z}$ which sends $1 \mapsto 1$.

To show that $\beta^* = 0$, take a T-linear map $f\colon (\mathbb{Z}T)^2 \to \mathbb{Z}$ and $z \in \mathbb{Z}T$ and compute:

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

which vanishes since the action of T on $\mathbb{Z}$ is trivial. The vanishing of α^* is similar.

Next, we need to turn this cohomology group into a form we can use to build extensions—specifically into the form provided by the bar resolution. We therefore use the method of Proposition 5.2.1 to build a chain map from the bar resolution to the given resolution above, in dimensions 0, 1 and 2:

$$\begin{tikzcd}
\mathbb{Z}T\{T^{(2)}\} \arrow[r, "d_2"] \arrow[d, "f_2"] & \mathbb{Z}T\{T^{(1)}\} \arrow[r, "d_1"] \arrow[d, "f_1"] & \mathbb{Z}T\{T^{(0)}\} \arrow[r, "\epsilon"] \arrow[d, "\mathrm{id}"] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
\mathbb{Z}T \arrow[r, "\beta"] & \mathbb{Z}T^2 \arrow[r, "\alpha"] & \mathbb{Z}T \arrow[r, "\epsilon"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

In dimensions -1 and 0 we may use the identity map. Next we must construct

$$f_1\colon \mathbb{Z}T\{T^{(1)}\} \to \mathbb{Z}T^2$$

such that $\alpha f_1 = d_1$. Since the domain of this map is a free G-module with basis $\{[a^r b^s] \mid r, s \in \mathbb{Z}\}$, we just need to find appropriate elements $(x_{r,s}, y_{r,s}) \in \mathbb{Z}T^2$ to send these basis elements to: that is, we must solve the equation

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

Define a symbol

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

so that $S(a, r)(a - 1) = a^r - 1$ in all cases. Then we have

$$\alpha(S(a, r)b^s, S(b, s)) = S(a, r)b^s(a - 1) + S(b, s)(b - 1) = d_1([a^r b^s])$$

as required. Note that we use the fact that T is abelian, so its group ring is commutative.

So we may define f_1 by the formula

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

To define f_2, we must do essentially the same process: for each pair of elements $(a^r b^s, a^t b^u) \in T^2$, find $z_{r,s,t,u} \in \mathbb{Z}T$ such that

$$f_1 d_2([a^r b^s | a^t b^u]) = \beta(z_{r,s,t,u}).$$

We have

$$\begin{aligned} f_1 d_2([a^r b^s | a^t b^u]) &= f_1(a^r b^s [a^t b^u] - [a^{r+t} b^{s+u}] + [a^r b^s]) \\ &= (a^r b^s S(a, t)b^u - S(a, r + t)b^{s+u} + S(a, r)b^s, \\ &\qquad a^r b^s S(b, u) - S(b, s + u) + S(b, s)) \end{aligned}$$

Such elements $z_{r,s,t,u}$ are perhaps best found by solving the case when all the $r, \ldots, u$ are positive, and then checking that the result extends to the other cases. Here it will be sufficient for me to note that

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

works, and that this may be checked for yourselves using the relation

$$S(a, r + t) = a^r S(a, t) + S(a, r).$$

So we define

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

Now let us find a cochain $\phi\colon T^2 \to \mathbb{Z}$ representing the cohomology class

$$p \in \mathbb{Z} \cong \operatorname{Hom}_T(\mathbb{Z}T, \mathbb{Z}) = H^2(T, \mathbb{Z})$$

From the previous work, such a cochain is given by the composition

$$\phi\colon T^2 \xrightarrow{f_2} \mathbb{Z}T \xrightarrow{p \cdot \epsilon} \mathbb{Z}$$

Since ϵ is a ring homomorphism, and since $\epsilon(S(a,r)) = r$, we find

$$\phi(a^r b^s, a^t b^u) = p\epsilon(z_{r,s,t,u}) = pru.$$

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

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

This constitutes a classification of the central extensions of T by $\mathbb{Z}$. If you wish for a more concrete interpretation, note that the group multiplication above is the same as provided by the matrix multiplication

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

so that all extensions of T by $\mathbb{Z}$ are equivalent to a group

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

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

5.4 Cohomology of profinite groups

We will conclude the course by applying our cohomological tools to profinite groups, and will prove some powerful theorems showing how pro-p groups in particular are governed by their cohomology in strong ways—theorems which are much more difficult, or are simply not true, for abstract groups.

If this course were to be totally complete and rigorous, we would now embark upon the redevelopment of cohomology theory for profinite groups—defining what a free profinite module is, defining chain complexes and homology groups and showing that cohomology is well-defined and so on. This would be incredibly tedious however, and consist of largely repeating the proofs while stating that all maps are continuous, or that certain topologies are well-defined. Instead we will make the following definitions—essentially converting the fact that the bar resolution gives the cohomology from a theorem into a definition.

Definition 5.4.1. Let G be a profinite group. A *finite G-module* is a finite abelian group M equipped with an action function $G \times M \to M, (g, m) \mapsto g \cdot m$ which is continuous.

Definition 5.4.2. Let G be a profinite group and let M be a finite G-module. Define the set of *n-cochains*, for $n \geq 0$, to be the abelian group

$$C^n(G, M) = \{\text{Continuous functions } \phi\colon G^n \to M\}$$

Define maps $d^n\colon C^{n-1}(G, M) \to C^n(G, M)$ by the formula

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

Define the group of *n-cocycles* to be

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

and the group of *n-coboundaries* to be

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

Define the n^{th} *cohomology group* of G with coefficients in M to be

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

Remark 5.4.3. It is perfectly possible to extend the definition of G-module, and of cohomology, to relax the restriction that M is finite. One such extension will be seen on Exercise Sheet 4.

As mentioned above, the theory of cohomology of a profinite group is almost identical to the theory of cohomology of discrete groups. Not necessarily all the proofs will work in the way we've defined them—for instance, a coinduced module is not necessarily finite—but slight modifications of the arguments ensure that in fact all the general results carry over. We codify this as follows.

Course Convention 5.4.4. All general results from Sections 5.1 to 5.3, and Exercise Sheet 4, may be applied to profinite groups, by substituting all groups with profinite groups, maps with continuous maps, and modules with finite modules.

As an example, we can translate Theorem 5.3.3 into the following statement.

Definition 5.4.5. An *extension of a profinite group G by a finite G-module M* is a short exact sequence of the form

$$0 \to M \to E \to G \to 1$$

where E is a profinite group and $M \lhd_o E$ is an open normal subgroup, and the conjugation action of E induces the given action of G on M. Two extensions are equivalent if there is a commuting diagram

$$\begin{tikzcd}
 & & E \arrow[dd] \arrow[dr] & & \\
1 \arrow[r] & M \arrow[ur] \arrow[dr] & & G \arrow[r] & 1 \\
 & & E' \arrow[ur] & &
\end{tikzcd}$$

of continuous group homomorphisms.

Theorem 5.4.6. *Let G be a profinite group and let M be a finite G-module. There is a* bijection

$$\left\{\begin{matrix}\text{Equivalence classes of}\\ \text{extensions of } G \text{ by } M\end{matrix}\right\} \longleftrightarrow H^2(G,M)$$

Remark 5.4.7 (Why only finite modules?). It is perfectly legitimate to wonder why we demanded that G-modules be finite for G a profinite group. In fact one can expand the class a little—see Question 10 on Example Sheet 4 for some work with one notion of the 'correct' class of modules—but allowing arbitrary G-modules leads pretty rapidly to pathologies.

Assume for the sake of argument that a cohomology theory of profinite groups exists with all our desired properties.

Let $G = \widehat{\mathbb{Z}}$. Consider the short exact sequence of abelian groups

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

all considered to be G-modules with a trivial action. If the Course Convention is to hold, we should have $H^1(G, M) = \mathrm{Hom}(G, M)$ (the set of continuous homomorphisms). Note that the only continuous homomorphism from $\widehat{\mathbb{Z}}$ to $\mathbb{Q}$ is the zero homomorphism, since a continuous map from the compact space $\widehat{\mathbb{Z}}$ to a discrete space has finite image and $\mathbb{Q}$ has no non-trivial finite subgroups. That is, $H^1(\widehat{\mathbb{Z}}, \mathbb{Q}) = 0$.

On the other hand, there are many non-trivial continuous homomorphisms from $\widehat{\mathbb{Z}}$ to $\mathbb{Q}/\mathbb{Z}$: any $x \in \mathbb{Q}/\mathbb{Z}$ has finite order, so the function $1 \mapsto x$ extends to a continuous homomorphism $\widehat{\mathbb{Z}} \to \langle x \rangle \subseteq \mathbb{Q}/\mathbb{Z}$. Hence in fact we have $H^1(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}$.

But now apply Proposition 5.1.28 to the above short exact sequence to find a long exact sequence, part of which reads

$$0 = H^1(\widehat{\mathbb{Z}}, \mathbb{Q}) \to H^1(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \hookrightarrow H^2(\widehat{\mathbb{Z}}, \mathbb{Z})$$

so $H^2(\widehat{\mathbb{Z}}, \mathbb{Z}) \neq 0$, and our free group no longer has cohomological dimension 1!

5.4.1 Pro-p groups of cohomological dimension one

Recall the definition of cohomological dimension, which we restate here in the appropriate form for profinite groups.

Definition 5.4.8. A group G has *cohomological dimension* n if $H^m(G, M) = 0$ for all $m > n$ and all finite G-modules M, but there exists some finite G-module M such that $H^n(G, M) \neq 0$.

Theorem 5.4.9. *Let G be a pro-p group. Then*

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

Corollary 5.4.10. *A non-trivial pro-p group G has cohomological dimension 1 if and only if $H^2(G, \mathbb{F}_p) = 0$.*

Proof of Corollary. The theorem implies that $H^2(G, \mathbb{F}_p) = 0$ if and only if G has cohomological dimension at most 1; and by Proposition 4.1.7, if G is a non-trivial pro-p group then it admits a homomorphism onto $\mathbb{F}_p$, whence $H^1(G, \mathbb{F}_p) \neq 0$. □

The proof of this theorem proceeds in several stages. First we show that we need only worry about 'simple' modules.

Definition 5.4.11. A G-module M is *simple* if the only G-submodules of M are M itself and $\{0\}$.

Proposition 5.4.12. *Let G be a profinite group and suppose $H^n(G,S) = 0$ for all finite simple G-modules S. Then $H^n(G,M) = 0$ for all finite G-modules M.*

Proof. Suppose the result is not true, and let M be the smallest finite G-module such that $H^n(G,M) \neq 0$. By hypothesis M is not simple, so has a proper non-trivial G-submodule N. The G-modules N and M/N are both strictly smaller than N, so $H^n(G,N) = 0 = H^n(G,M/N)$. However the short exact sequence of modules

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

yields, by Prop 5.1.28, a long exact sequence of cohomology groups including a section

$$0 = H^n(G,N) \to H^n(G,M) \to H^n(G,M/N) = 0$$

which forces the contradiction $H^n(G,M) = 0$. □

Definition 5.4.13. Let M be a finite G-module. For a prime p, we call M a *p-primary* module if $|M|$ is a power of p.

If M is any finite G-module, then the finite abelian group M decomposes in a unique way as the direct sum of its p-Sylow subgroups

$$M = \oplus_{p\ \mathrm{prime}} M_p.$$

These Sylow subgroups M_p are G-submodules of M, called its *p-primary components.*

Proposition 5.4.14. *Let G be a pro-p group, let M be a finite G module, and let the p-primary component of M be M_p. Then $H^n(G,M) = H^n(G,M_p)$.*

Proof. Write $M = M_p \oplus M'$, where M' has order coprime to p. Then

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

so we need only prove that $H^n(G,M') = 0$.

This is true if G is a finite p-group, by a result you will prove on Example Sheet 4. From this we derive the result for an arbitrary pro-p group G.

Let $\phi\colon G^n \to M$ be a continuous cocycle. Then the preimages of the points $m \in M$ are open subsets of G^n, hence are unions of basic open sets—i.e. cosets of open subgroups $K_{i,m}^n$ where $K_{i,m}$ is an open normal subgroup in G. By compactness we need only finitely many such cosets, and so only finitely many $K_{i,m}$. Taking the intersection of all of these gives an open normal subgroup K such that all preimages $\phi^{-1}(m)$ are unions of cosets of K^n in G^m. Without loss of generality (by passing to a smaller subgroup) we may assume that K acts trivially on M.

It follows that ϕ descends to a cocycle $(G/K)^n \to M$. By the result just quoted, $H^n(G/K,M) = 0$, so this cocycle is equals $d^n\psi$ for some cochain $\psi \in C^{n-1}(G/K,M)$. Composing ψ with the natural map $G^{n-1} \to (G/K)^{n-1}$ shows that ϕ is also a coboundary. Hence $H^n(G,M) = 0$. □

Remark 5.4.15. Had we formally defined direct limits in this course, the middle section of this proof—that all cocycles factor through some $(G/K)^n$—is essentially a proof that inverse limits commute with cohomology in the sense that

$$H^n(G, M) = \varinjlim H^n(G/K, M)$$

where the limit is taken over those open normal subgroups K which act trivially on M.

Proposition 5.4.16. *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.*

Proof. In light of the previous two propositions, it is enough to show that the only simple p-primary G-module is $\mathbb{F}_p$. This you will do on Example Sheet 4. □

Proposition 5.4.17. *Let G be a pro-p group. The only finite simple p-primary G-module is $\mathbb{F}_p$.*

Proof. On Exercise Sheet 4. □

To prove Theorem 5.4.9, it only remains to transfer the information that cohomology vanishes to higher dimensions.

Proposition 5.4.18. *Suppose that there exists $N \geq 1$ such that $H^N(G, M) = 0$ for all G-modules M. Then* $\mathrm{cd}(G) \leq N - 1$.

Proof (non-examinable). In accordance with course convention, we prove this proposition for discrete groups G. Let M be a G-module. On Example Sheet 4 you will study the *coinduced module*

$$\mathrm{coind}_G^K(M) = \mathrm{Hom}_K(\mathbb{Z}G, M),$$

where K is a subgroup of G, and show it has the property that

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

for all n. Consider the case $K = 1$, when the coinduced module consists of the abelian group homomorphisms from $\mathbb{Z}G$ to M. Consider the map

$$\alpha \colon M \to \mathrm{Hom}_1(\mathbb{Z}G, M), \quad m \mapsto (x \mapsto xm)$$

This is a G-linear map, which is clearly injective. Let the quotient module $\mathrm{coind}_G^1(M)/\alpha(M)$ be denoted M'. Since the trivial subgroup 1 has vanishing cohomology in dimensions at least 1, the long exact sequence in cohomology associated to the short exact sequence of modules

$$0 \to M \to \mathrm{coind}_G^1(M) \to M' \to 0$$

reads, for all $n \geq 1$,

$$0 = H^n(G, \mathrm{coind}_G^1(M)) \to H^n(G, M') \to H^{n+1}(G, M) \to 0$$

The middle map is therefore an isomorphism. If $n = N$ then $H^N(G, M')$ vanishes by hypothesis, hence so does $H^{N+1}(G, M)$ for all G. Inductively this shows $H^n(G, M) = 0$ for all $n \geq N$ as required. □

Corollary 5.4.19. *(Topologically finitely generated) free profinite groups and free pro-p groups have cohomological dimension 1.*

Proof. Let F be a free profinite group. Let M be any finite G-module. Let E be an extension of F by M. Then this extension splits: let X be a free generating set for F, and choose for each $x \in X$ a preimage e_x of x in E. The function $x \mapsto e_x$ now extends, by the universal property of a free profinite group, to a continuous group homomorphism $F \to E$ splitting the extension. Hence every extension is split, and $H^2(F, M) = 0$ for all G-modules M.

For pro-p groups we use the same argument, for the specific case $M = \mathbb{F}_p$—then E is automatically a pro-p group, and we can apply the universal property of a free pro-p group. □

To prove the converse statement, we will prove instead the following stronger theorem, which illustrates the powerful control that cohomology exerts on the behaviour of pro-p groups.

Theorem 5.4.20. *Let G and G' be topologically finitely generated pro-p groups. Let $f\colon G \to G'$ be a continuous homomorphism. Assume that*

$$f^*\colon H^1(G', \mathbb{F}_p) \to H^1(G, \mathbb{F}_p)$$

is an isomorphism and

$$f^*\colon H^2(G', \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$$

is an injection. Then f is an isomorphism.

Proof (non-examinable). Let $G_n^{(\prime)} = \gamma_n^{(p)}(G^{(\prime)})$ be the n^{th} term of the lower central p-series of G or G'. These are fully characteristic subgroups, so $f(G_n) \subseteq G'_n$ and f induces maps

$$f_n\colon G/G_n \to G'/G'_n.$$

We show by induction that these are all isomorphisms; the result then follows since

$$G^{(\prime)} = \varprojlim G^{(\prime)}/G_n^{(\prime)}.$$

The base case $n = 1$ is trivial. Assume therefore that f_n is an isomorphism.

Consider the group G_n/G_{n+1}. By definition, $G_{n+1} = \overline{[G, G_n]G_n^p}$, and is open in G by Corollary 4.2.7. It follows that G_n/G_{n+1} is a finite dimensional vector space over $\mathbb{F}_p$, so f induces an isomorphism

$$G_n/G_{n+1} \to G'_n/G'_{n+1}$$

if and only if its dual map

$$f^*\colon \operatorname{Hom}(G'_n/G'_{n+1}, \mathbb{F}_p) \to \operatorname{Hom}(G_n/G_{n+1}, \mathbb{F}_p)$$

is an isomorphism.

Now, a continuous homomorphism $\phi\colon G_n \to \mathbb{F}_p$ factors through G_n/G_{n+1} if and only if it kills $[G, G_n]G_n^p$. A p^{th} power obviously vanishes when mapped to $\mathbb{F}_p$. For $g \in G, g_n \in G_n$, we have

$$\phi([g, g_n]) = \phi(g^{-1}g_n^{-1}gg_n) = -\phi(g^{-1}g_ng) + \phi(g_n)$$

So ϕ factors through G_n/G_{n+1} if and only if it is G-invariant. It follows that

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

This can be recognised as one of the terms in the Five Term Exact Sequence for the short exact sequence of groups

$$1 \to G_n \to G \to G/G_n \to 1$$

The Five Term Exact Sequence, along with the functorial behaviour of the map f on cohomology, gives us a commuting diagram (where all coefficient modules are $\mathbb{F}_p$):

$$\begin{tikzcd}
H^1(G/G_n) \arrow[r] & H^1(G) \arrow[r] & H^1(G_n)^G \arrow[r] & H^2(G/G_n) \arrow[r] & H^2(G) \\
H^1(G'/G'_n) \arrow[r] \arrow[u] & H^1(G') \arrow[r] \arrow[u] & H^1(G'_n)^{G'} \arrow[r] \arrow[u] & H^2(G'/G'_n) \arrow[r] \arrow[u] & H^2(G') \arrow[u]
\end{tikzcd}$$

By hypothesis, the second vertical map is an isomorphism and the fifth map is an injection; by induction the first and fourth maps are isomorphisms; thus by the Five Lemma[7], the central map is an isomorphism also. Hence $G_n/G_{n+1} \cong G'_n/G'_{n+1}$.

Finally, we conclude the induction by noting that f now gives a commuting diagram

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

which shows that f_{n+1} is an isomorphism as required. □

Corollary 5.4.21. *Let G be a finitely generated pro-p group of cohomological dimension 1. Then G is a free pro-p group.*

Proof. Let F be a topologically finitely generated free pro-p group of rank equal to the minimal size of a generating set for G. Then there is a surjection $f\colon F \to G$ such that the corresponding map

$$f_*\colon F/\Phi(F) \to G/\Phi(G)$$

is an isomorphism, where Φ denotes the Frattini subgroup. Since all maps from G to $\mathbb{F}_p$ factor through the Frattini quotient, we find that $\mathrm{Hom}(G/\Phi(G), \mathbb{F}_p) = H^1(G, \mathbb{F}_p)$ and that

$$f^*\colon H^1(G, \mathbb{F}_p) \to H^1(F, \mathbb{F}_p)$$

is an isomorphism. Since $H^2(G, \mathbb{F}_p) = 0$, the map f^* on H^2 is injective, so by the theorem f is an isomorphism. □

In fact we have a bonus theorem with exactly the same proof as Theorem 5.4.20!

[7] You met this in Algebraic Topology: the proof is simply a matter of a diagram chase.

Theorem 5.4.22. *Let G and G' be finitely generated abstract groups. Let $f\colon G \to G'$ be a homomorphism. Assume that*

$$f^*\colon H^1(G', \mathbb{F}_p) \to H^1(G, \mathbb{F}_p)$$

is an isomorphism and

$$f^*\colon H^2(G', \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$$

is an injection. Then G and G' have isomorphic pro-p completions.

Proof. Once again let G_n be the n^{th} term of the lower central p-series. Then the pro-p completion of G is the inverse limit $\varprojlim G/G_n$. The rest of the proof proceeds as in the previous theorem. □

Example 5.4.23. Let G be the group with presentation

$$G = \langle x_1, x_2 \mid x_1x_2x_1^{-1}x_2^{-1}x_1\rangle$$

from Example 5.3.5. By the argument in that example (with $\mathbb{Z}$ replaced by $\mathbb{F}_p$), we have $H^2(G, \mathbb{F}_p) = 0$. The abelianisation of G is easily seen to be isomorphic to $\mathbb{Z}$, and generated by the image of x_2. Then the map $\mathbb{Z} \to G, 1 \mapsto x_2$ satisfies the conditions of the theorem and shows that the pro-p completion of G is isomorphic to $\mathbb{Z}_p$.

5.4.2 Presentations of pro-p groups

We will now consider for a short time a little of the theory of group presentations for pro-p groups, in order to contrast with the theory of discrete groups. Many of the definitions may be made for general profinite groups just as well, but we will be able to prove more about the pro-p world and introducing both would lead to more confusion than it's worth.

Definition 5.4.24. Let X be a finite set and let F be the free pro-p group generated by X. Let R be a set of elements of F. The pro-p group with presentation

$$\lfloor X \mid R \rfloor_p$$

is defined to be

$$G = F/\overline{\langle\!\langle R \rangle\!\rangle},$$

the quotient of F by the closed normal subgroup generated by R.

Remark 5.4.25. Note that the elements of R need not be elements of the discrete free group generated by the x_i—i.e. you may not be able to write them down. For example the free group $\mathbb{Z}_3$ has an element κ such that $2\kappa = 1$, but you can't write κ down in a finite way.

Remark 5.4.26. The use of symbols $\lfloor X \mid R \rfloor_p$ is not the standard convention; so far as I'm aware the standard notation uses $\langle X \mid R \rangle$, just as for discrete group presentations. I decided to introduce new notation to reduce the chance of confusion.

First we note an easy relation of normal presentations to pro-p presentations.

Lemma 5.4.27. *Let F_{disc} be the free discrete group generated by X. Let $R \subseteq F_{\mathrm{disc}}$. Let Γ be the discrete group*

$$\Gamma = \langle X \mid R \rangle$$

and let G be the pro-p group

$$G = \lfloor X \mid R \rfloor_p.$$

Then G is the pro-p completion of Γ.

Proof. The natural inclusion $F_{\mathrm{disc}} \to F$ induces a group homomorphism $\Gamma \to G$ since obviously $\langle\!\langle R \rangle\!\rangle^{F_{\mathrm{disc}}} \subseteq \overline{\langle\!\langle R \rangle\!\rangle}^{F}$. This in turn gives a natural surjection $\iota \colon \widehat{\Gamma}_{(p)} \to G$.

To show ι is an injection, let $x \in \widehat{\Gamma}_{(p)} \smallsetminus \{1\}$. Then there is a map $f : \widehat{\Gamma}_{(p)} \to P$ a finite p-group P such that $f(x) \neq 1$. This yields a homomorphism

$$\bar{f} \colon F^{\mathrm{disc}} \to \Gamma \to \widehat{\Gamma}_{(p)} \to P$$

such that the image of R is trivial. Then the extension of $\bar{f}$ to a continuous map $F \to P$ also kills R, and hence kills $\overline{\langle\!\langle R \rangle\!\rangle}$. Hence we get a natural map $G \to P$ such that

$$\begin{tikzcd}
\widehat{\Gamma}_{(p)} \arrow[rr] \arrow[dr] & & G \arrow[dl] \\
& P &
\end{tikzcd}$$

commutes. It follows that $\iota(x) \neq 1$ as required. □

We have already seen that the first cohomology controls the number of elements needed to generate a pro-p group, since

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

where $\Phi(G)$ is the Frattini subgroup. We can also ask how many relations we need to impose to write down a presentation for G with a given generating set.

Theorem 5.4.28. *Let G be a topologically finitely generated pro-p group and let X be a finite topological generating set for G. Let r_X be the minimal size of a set $R \subseteq F(X)$, where $F(X)$ is the free pro-p group generated by X, such that*

$$G = \lfloor X \mid R \rfloor_p.$$

Then

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

Remark 5.4.29. There is a slight ambiguity in the notation here, since a particular presentation does not really specify how the generating set X maps to the group (even if we use the same letters). A more precise way to state the theorem would be to note that the generating set X specifies a surjective map $F(X) \to G$ whose kernel is a closed normal subgroup N of $F(X)$. Then r_X is the smallest size of a set R such that $N = \overline{\langle\!\langle R \rangle\!\rangle}$.

Remark 5.4.30. Before proving this theorem, I will remark how different the situation is for presentations of discrete groups. Again, for a group Γ and a finite generating set X of Γ, let ρ_X be the smallest cardinality of a set R in the free group on X such that

$$\Gamma = \langle X \mid R \rangle$$

The theorem above says that in pro-p groups, $|X| - r_X$ is a constant value, and tells us what this value is. For infinite discrete groups it is known that $|X| - \rho_X$ *does* depend on the generating set X, even to the extent that different generating sets of the same size can have different ρ_X. Both these questions seem to be open for finite groups.

Another interesting question concerns finite p-groups. If G is a finite p-group with generating set X, need it be true that $\rho_X = r_X$? There is an obvious inequality: $r_X \leq \rho_X$ since every discrete presentation $G = \langle X \mid R \rangle$ for a finite p-group G is also a pro-p presentation $G = \lfloor X \mid R \rfloor_p$. Does equality hold? Astonishingly this seems to be an open question! Much is deep and unknown about presentations of groups. Seen in this light Theorem 5.4.28 becomes rather more surprising!

Let us embark on the proof. First some topology.

Lemma 5.4.31 (Non-examinable)**.** *Let G and L be non-trivial profinite groups and assume that L acts continuously on G—so that there is a continuous function $L \times G \to G$ giving the action $(g, l) \mapsto l \cdot g$. Then G has a proper open normal subgroup which is invariant under the action of L.*

Proof. Let U be an open normal subgroup of G. We claim that

$$\widetilde{L} = \{l \in L \mid l \cdot U = U\}$$

is open in L. If we assume the claim, then $\widetilde{L}$ has finite index in L, so there are only finitely many subgroups of G of the form $l \cdot U$. The intersection $\bigcap l \cdot U$ is now an intersection of finitely many open normal subgroups of G—so is an open normal subgroup of G, and it is certainly L-invariant as required.

It remains to prove the claim. Let $\rho \colon L \times G \to G$ denote the action. Fix $l \in \widetilde{L}$. We must find an open neighbourhood of l inside $\widetilde{L}$. For each $u \in U$ we have $(l, u) \in \rho^{-1}U$. Since ρ is continuous, there are open sets $A_u \subseteq L$ and $B_u \subseteq U$ such that $(l, u) \in A_u \times B_u \subseteq \rho^{-1}(U)$. Now, U is compact, and the open sets B_u cover U—hence there is a finite subcover. Take $u_1, \ldots, u_k$ such that $U = \bigcup B_{u_i}$. Let $A = \bigcap A_{u_i}$. This is a finite intersection, so is an open subset of L containing l. But if $a \in A$ and $v \in U$, then $v \in B_{u_i}$ for some i, so that $a \cdot v \in \rho(A_{u_i} \times B_{u_i}) \subseteq U$. Hence $A \subseteq \widetilde{L}$, and $\widetilde{L}$ is open as claimed. □

Lemma 5.4.32 (Non-examinable)**.** *Let F be a pro-p group and let N be a closed normal subgroup of F. There exists a set R of size r which generates N as a closed normal subgroup of F if and only if*

$$\dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^{F/N} \leq r.$$

Proof. First we will put the quantity on the left into a more manageable form.

$$\begin{aligned} H^1(N, \mathbb{F}_p)^{F/N} &= \mathrm{Hom}(N, \mathbb{F}_p)^{F/N} \\ &= \{\phi \colon N \to \mathbb{F}_p \mid \phi(fnf^{-1}) = \phi(n)\ \forall n \in N, f \in F\} \end{aligned}$$

Now, if $N = \overline{\langle\langle R \rangle\rangle}$, where R is a finite set, then a map $\phi \in H^1(N, \mathbb{F}_p)^{F/N}$ is determined by its image on R, so certainly there is an injection

$$H^1(N, \mathbb{F}_p)^{F/N} \hookrightarrow \mathbb{F}_p^{|R|}$$

from which the inequality

$$\dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^{F/N} \leq r$$

follows.

Now suppose that

$$\dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^{F/N} = r;$$

we will find a set R which normally generates N and such that $|R| = r$. Any map from N to $\mathbb{F}_p$ factors through $N/\Phi(N)$. If it is F-invariant then it also factors through $N/\Phi(N)[N, F]$. This latter is an $\mathbb{F}_p$-vector space to which $H^1(N, \mathbb{F}_p)^{F/N}$ is dual. Therefore there exists a set R of r elements of N which yield a basis of $N/\Phi(N)[N, F]$, to which a given basis of $H^1(N, \mathbb{F}_p)^{F/N}$ is dual. Then any map $\phi \in H^1(N, \mathbb{F}_p)^{F/N}$ which vanishes when restricted to R is zero. We will show that this implies that $N = \overline{\langle\langle R \rangle\rangle}$.

Let $N' = \overline{\langle\langle R \rangle\rangle}$ and suppose $N' \neq N$. Then $N'\Phi(N) \neq N$, and so $M = N/\Phi(N)N' \neq 0$. This latter group is a non-trivial abelian pro-p group with a continuous F-action, so by Lemma 5.4.31 there is an F-invariant open normal subgroup U of M. Then M/U is a finite pro-p F-module, and so by Proposition 5.4.17 there is an F-invariant map $M/U \to \mathbb{F}_p$. This gives in turn a non-trivial F-invariant map $N \to \mathbb{F}_p$, which vanishes on N', and hence on R. This contradiction concludes the proof. □

Proof of Theorem 5.4.28. Let X be a generating set for G and let N be the kernel of the natural map $F(X) \to G$. Then r_X is the size of a minimal generating set for N as a closed normal subgroup of $F = F(X)$. By the previous lemma, we have

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

Now apply the Five Term Exact Sequence. Since $F(X)$ is free pro-p, and thus of cohomological dimension 1, the five term exact sequence takes the form

$$0 \to H^1(G, \mathbb{F}_p) \to H^1(F, \mathbb{F}_p) \xrightarrow{\alpha} H^1(N, \mathbb{F}_p)^{F/N} \xrightarrow{\beta} H^2(G, \mathbb{F}_p) \to H^2(F, \mathbb{F}_p) = 0$$

Consider the image of the map marked α. By the rank-nullity theorem this is equal to

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

On the other hand, by exactness the image of α equals the kernel of β; again the rank-nullity theorem implies

$$\dim_{\mathbb{F}_p} \operatorname{im}(\alpha) = \dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p)^{F/N} - \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = r_X - \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$$

Equating these two formulae and re-arranging completes the proof of the theorem. □