Profinite Groups and Group Cohomology

April 5, 2016

Contents

Motivation

Profinite groups and group cohomology arise in many areas of mathematics. I will provide some broad motivation for each topic. The reason for this motivation is that in treating these topics rigorously and in some generality, we will see that there is a fair amount of language, notation, .etc needed for these topics. I cannot do both topics the time they separately deserve and have chosen profinite groups as the main topic.

There are many views one can take in exploring the topic of profinite groups. In Galois theory, one sees that profinite groups arise naturally in taking closures or limits in extension theory. Profinite groups arise in covering space theory of manifolds and varieties as limits of all of the finite deck/Galois groups of the covers. The profinite completion of a finitely generated group is a universal object for the finite representation theory of the group. All of these examples illustrate why profinite groups of centrally important in mathematics. They serve as completions/limits and as universal objects.

Group cohomology from my personal perspective is a tool/view that every mathematician should be casual familiar with. Cohomology theory, in the broadest sense, is amazingly diverse. It could measure the failure of satisfying a certain condition/equation. As such, it can be viewed as an obstruction. It could also parameterizes objects or encoding some infinitesimal deformation theory. For me, cohomology theory comes to life when it is used in a specific setting. For instance, if Γ is a group, there is an associated topological space $K(\Gamma,1)$ that has the same cohomology theory as Γ. The best example of such an association is the circle $S^1 = \mathbf{R}/\mathbf{Z}$ with the integers $\mathbf{Z}$. This gives a concrete picture to the abstract treatment I will give here. Time permitting, I may give a lecture at the end of the course on Galois cohomology in a concrete setting like Brauer groups. It would serve solely as a highlight for cohomology theory and lack in details.

The class notes will follow Wilson's book [14]. Another suggested reference for the class is Ribes–Zalesskii [13]. Additional references will be added as the lecture notes develop.

Chapter 1

Preliminaries

In this preliminary module, we will review some requisite material on topological spaces and topological groups. Important terms will be listed in **bold**. Blue text indicates that there is a link to a webpage with additional information.

1.1 Lecture 1. *Topological Spaces*

By a **topological space** we mean a pair $(X, \mathscr{T})$, where X is a set and $\mathscr{T}$ is a set of subsets of X satisfying:

(i) $\emptyset, X \in \mathscr{T}$.

(ii) If $U_1, U_2 \in \mathscr{T}$, then $U_1 \cap U_2 \in \mathscr{T}$.

(iii) For any subset $\mathscr{S} \subset \mathscr{T}$, $\bigcup_{U \in S} U \in \mathscr{T}$.

The sets $U \in \mathscr{T}$ are referred to as **$\mathscr{T}$–open sets** or simply **open** when the topology $\mathscr{T}$ is understood. A subset $C \subset X$ is **$\mathscr{T}$–closed** if $X - C \in \mathscr{T}$. Given a subset $Y \subset X$, we define the **closure** of Y in X to be the intersection of all the closed sets $C \subset X$ such that $Y \subset C$. We denote the closure of Y by $\overline{Y}$. We say $Y \subset X$ is **dense** if $\overline{Y} = X$. For each $x \in X$, we say $U \in \mathscr{T}$ is an **open neighborhood of x** or simply a **neighborhood of** x if $x \in U$. A **base** for a topology $\mathscr{T}$ is any subset $\mathscr{B}$ of $\mathscr{T}$ such that every $U \in \mathscr{T}$ can be expressed as a union of open sets in $\mathscr{B}$. A **neighborhood base** at x is any collection $\mathscr{B}_x$ of neighborhoods of x such that every neighborhood of x can be expressed as a union of sets in $\mathscr{B}_x$.

Example 1 (**Discrete Topology.**)**.** If $\mathscr{T}$ is the power set $\mathscr{P}(X)$ of X, then $\mathscr{T}$ is a topology. This topology is called the **discrete topology**. Every subset of X is both open and closed.

Given a topological space $(X,\mathscr{T})$ and a subset $Y \subset X$, we define the **subspace topology** $\mathscr{T}_{X,Y}$ on Y by

$$\mathscr{T}_{X,Y} = \{U \cap Y \ : \ U \in \mathscr{T}\}.$$

We will refer to $(Y,\mathscr{T}_{X,Y})$ as a subspace of $(X,\mathscr{T})$. We say that $(X,\mathscr{T})$ is **compact** if given any subset $\mathscr{C} \subset \mathscr{T}$ such that $X = \bigcup_{U \in \mathscr{C}} U$, there exists a finite subset $\mathscr{C}_0 \subset S$ such that $X = \bigcup_{U \in \mathscr{S}_0} U$. We will say that a subset $Y \subset (X,\mathscr{T})$ is compact if $(Y,\mathscr{T}_{X,Y})$ is a compact space. The following lemma is immediate from the definitions of closed and compact.

Lemma 1.1. *Let $(X,\mathscr{T})$ be a compact space. If $\mathscr{S}$ is a collection of closed sets of X such that for any finite subset $\mathscr{S}_0 \subset \mathscr{S}$, we have $\bigcap_{C \in \mathscr{S}_0} C \neq \emptyset$, then $\bigcap_{C \in \mathscr{S}} C \neq \emptyset$.*

We say a space $(X,\mathscr{T})$ is **Hausdorff** if given distinct $x_1, x_2 \in X$, there exists disjoint open sets $U_1, U_2 \in \mathscr{T}$ such that $x_i \in U_i$ for $i = 1,2$. If X is a Hausdorff space, then $\{x\}$ is closed for all $x \in X$. We say a space $(X,\mathscr{T})$ is **connected** if X cannot be expressed as the union of two disjoint closed sets. We say a space $(X,\mathscr{T})$ is **totally disconnected** if every connected subspace has at most one element.

Lemma 1.2. *Let X be a compact Hausdorff space.*

(a) If C_1, C_2 are disjoint closed subsets of X, then there exist disjoint open subsets U_1, U_2 of X such that $C_i \subset U_i$ for $i = 1,2$.

(b) If $x \in X$ and A_x is the intersection of all sets U containing x that are both open and closed, then A_x is connected.

(c) If X is also totally disconnected, then every open set is a union of sets that are both open and closed.

Proof. We start with (a). First, we assert that for each $x \in C_1$, there exist disjoint open sets U_x, V_x such that $x \in U_x$ and $C_2 \subset V_x$. For each $y \in C_2$, there exist disjoint open sets $U_{x,y}, V_{x,y}$ such that $x \in U_{x,y}$ and $y \in V_{x,y}$. The set of open sets $\mathscr{C}_x = \{X - C_2\} \cup \left\{V_{x,y}\right\}_{y \in C_2}$ is an open cover of X. Since X is compact, there exists a finite subset $\{y_1, \dots, y_n\}$ of C_2 such that X is a union of $X - C_2$ and the sets V_{x,y_i}. Taking

$$U_x = \bigcap_{i=1}^{n} U_{x,y_i}, \quad V_x = \bigcup_{i=1}^{n} V_{x,y_i}$$

verifies our first assertion. Varying U_x over $x \in C_1$, we obtain disjoint open sets U_x, V_x such that $x \in U_x$ and $C_2 \subset V_x$. As before, the sets $X - C_1$ and U_x are an open cover of X. Since X is compact, there exists a finite set $\{x_1, \ldots, x_m\}$ of C_1 such that X is a union of $X - C_1$ and the sets U_{x_i}. Finally, we define

$$U_1 = \bigcup_{i=1}^{m} U_{x_i}, \quad U_2 = \bigcap_{i=1}^{m} V_{x_i}.$$

Next we prove (b). Given $x \in X$, recall that A_x is the intersection of all subsets of X that contain x and are both open and closed. Assume that $A_x = C_1 \cup C_2$, where C_1, C_2 are open in A_x and disjoint. Since A_x is the intersection of closed sets, A_x is closed in X. Since $C_{i+1} = A - C_i$, both C_1, C_2 are closed in A_x. In tandem, we see that C_1, C_2 are also closed in X. By (a), there exists disjoint open sets U_1, U_2 in X such that $C_i \subset U_i$. Set $C = X - (U_1 \cup U_2)$ and let $\mathscr{S}$ be the collection of closed sets comprised of C and every set in X that contains x and is both open and closed. By construction, $\mathscr{S}$ is a collection of closed sets such that $\bigcap_{C' \in \mathscr{S}} C' = \emptyset$; for the latter, simply note that C is disjoint from A_x. Since X is compact, there exists a finite collection of subsets $V_1, \ldots, V_n$ of X that contain x, are both open and closed, and satisfy

$$C \cap \left(\bigcap_{i=1}^{n} V_i \right) = \emptyset.$$

Set $V = \bigcap_{i=1}^{n} V_i$ and note that $V \subset U_1 \cup U_2$. In particular, V is a disjoint union of $W_1 = V \cap U_1$ and $W_2 = V \cap U_2$, and so W_1, W_2 are both open and closed in V. Since V is also both open and closed in X, the subsets W_1, W_2 are both open and closed in X. Since $x \in V$, it follows that $x \in W_1$ or $x \in W_2$. If $x \in W_1$, then $A_x \subset W_1 \subset U_1$ and so $C_2 \subset A_x \cap U_2 \subset U_1 \cap U_2 = \emptyset$. Similarly, if $x \in W_2$, then $A_x \subset W_2 \subset U_2$ and so $C_1 \subset A_x \cap U_1 \subset U_1 \cap U_2 = \emptyset$. Hence, we see that A_x is connected.

Finally, we prove (c). Let U be an open set in X and let $x \in U$. For each $y \in X$ distinct from x, there exists a set F_y in X that is both open and closed and satisfies $x \in F_y, y \notin F_y$. Setting $U_y = X - F_y$, we see that X is the union of U with the sets U_y. Since X is compact, there exists a finite subset $\{y_1, \ldots, y_n\}$ of $X - \{x\}$ such that

$$X = U \cup \left(\bigcup_{i=1}^{n} (X - F_{y_i}) \right) = U \cup \left(X - \left(\bigcap_{i=1}^{n} F_{y_i} \right) \right).$$

Therefore, $\bigcap_{i=1}^{n} F_{y_i} \subset U$. Since this open and closed set contains x and x is arbitrary, the result follows. ♠

Given a pair of topological spaces X, Y, we say a function $f \colon X \to Y$ is **continuous** if for each open subset $V \subset Y$, the subset $f^{-1}(V) \subset X$ is open. Alternatively, $f^{-1}(C)$ is closed in X for every closed subset $C \subset Y$. We say a function $f\colon X \to Y$ is a **homeomorphism** if f is bijective and f, f^{-1} are both continuous.

Lemma 1.3.

(a) Every closed subset of a compact space is compact.

(b) Every compact subset of a Hausdorff space is closed.

(c) If $f\colon X \to Y$ is continuous and X is compact, then $f(X)$ is compact.

(d) If $f\colon X \to Y$ is continuous and bijective, X is compact, and Y is Hausdorff, then f is a homeomorphism.

(e) If $f, g\colon X \to Y$ are continuous and Y is Hausdorff, then the set

$$E(f,g) = \{x \in X \ : \ f(x) = g(x)\}$$

is a closed subset of X.

Proof. To prove (a), let X be a compact space and C is a closed subset of X. If $\mathscr{C}$ is an open covering of C, then for each $V \in \mathscr{C}$, there is an open subset U_V of X such that $V = C \cap U_V$. The open sets $X - C$ and the open sets $\{U_V\}_{V \in \mathscr{C}}$ form an open covering of X. Since X is compact, there is a finite subset $\mathscr{C}_0$ of $\mathscr{C}$ such that $X - C$ and $\{U_V\}_{V \in \mathscr{C}_0}$ cover X. It is clear that $\mathscr{C}_0$ is a cover of C.

To prove (b), let X be a Hausdorff space and $C \subset X$ a compact subspace. To prove that C is closed, we will prove that $X - C$ is open. For each $x \in X - C$ and $y \in C$, there exist disjoint open subsets $U_{x,y}, V_{x,y}$ in X such that $x \in U_{x,y}$ and $y \in V_{x,y}$. The collection $\mathscr{C} = \left\{V_{x,y}\right\}_{y \in C}$ is an open cover of C and since C is compact, there exists $\{y_1, \dots, y_n\} \subset C$ such that $\left\{V_{x,y_i}\right\}_{i=1}^{n}$ is a cover of C. The open set $U = \bigcap_{i=1}^{n} U_{x,y_i}$ is an open subset of X that contains x and is contained in $X - C$. Since $x \in X$ was arbitrary, we see $X - C$ is open.

To prove (c), giving any open cover $\mathscr{C}$ of $f(X)$, we have an associated open cover $f^{-1}(\mathscr{C}) = \left\{f^{1}(U)\right\}_{U \in \mathscr{C}}$. Since X is compact, there is a finite subset $\mathscr{C}_0$ of $\mathscr{C}$ such that $\left\{f^{-1}(U)\right\}_{U \in \mathscr{C}_0}$ is a cover. It is straightforward to see that $\mathscr{C}_0$ is the desired finite subcover needed to prove $f(X)$ is compact.

To prove (d), it is enough to prove that f is a closed mapping which follows from (a)-(c).

To prove (e), we show that $U_{f,g} = X - E_{f,g}$ is open. Given $x \in U_{f,g}$, by definition $f(x) \neq g(x)$. Since Y is Hausdorff, there exist disjoint open sets V_f, V_g of Y such that $\alpha(x) \in V_\alpha$ for $\alpha = f, g$.

Since f,g are continuous, $f^{-1}(V_f)\cap f^{-1}(V_g)$ is an open subset of $U_{f,g}$ containing x, and so $U_{f,g}$ is open since x was arbitrary. ♠

Lemma 1.4. *If X is totally disconnected, then $\{x\}$ is closed in X for every $x \in X$.*

Proof. Let C_x denote the closure of $\{x\}$ in X and assume that $C_x = U_1 \cup U_2$ where U_1, U_2 are disjoint union of open sets U_j in X. The sets $C_j = X - U_j$ are closed subsets and so one of them must contain x. Without loss of generality, we assume $x \in C_1$. Since C_x is the closure of $\{x\}$, we see that $C_x \subset U_1$ and so $U_2 = \emptyset$. ♠

Given an equivalence relationship $\sim$ on a space X, the quotient space of equivalence classes will be denoted by $X/\sim$. The set $X/\sim$ can be given a topological structure by taking the weakest topology on $X/\sim$ such that $\pi_\sim\colon X \to X/\sim$ is continuous. Specifically, $V \subset X/\sim$ is open if and only if $\pi_\sim^{-1}(V)$ is open in X. This topology is called the **quotient topology** and we refer to $X/\sim$ with this topology as the **quotient space**. This topology satisfies the following universal mapping property: If $f\colon X \to Y$ is a continuous function such that $f(x) = f(y)$ whenever $x \sim y$, then there exists a unique function $\widetilde{f}\colon (X/\sim) \to Y$ such that $f = \widetilde{f} \circ \pi_\sim$. We will refer to $\pi_\sim$ as the **quotient map** and will often simply denote it by π.

1.2 Lecture 2. *Filters and Product Spaces*

Given a family $\{X_\lambda\}_{\lambda\in\Lambda}$ of topological spaces, the product $\prod_{\lambda\in\Lambda} X_\lambda$ is the set of functions $x\colon \Lambda \to \cup_\lambda X_\lambda$ such that $x(\lambda) \in X_\lambda$. It is sometime convenient to view these functions as lists or vectors $x = (x_\lambda)$ where $x_\lambda = x(\lambda)$. For each $\lambda_0 \in \Lambda$, we have a projection map $\pi_{\lambda_0}\colon \prod_{\lambda\in\Lambda} X_\lambda \to X_{\lambda_0}$ given by $\pi_{\lambda_0}(x) = x_{\lambda_0}$. We endow $\prod_{\lambda\in\Lambda} X_\lambda$ with a topology generated by basic open sets of the form $\bigcap_{i=1}^n \pi_{\lambda_i}^{-1}(U_i)$ as we vary $n \in \mathbf{N}$, the indices $\lambda_1,\dots,\lambda_n \in \Lambda$, and open subsets $U_i \subset X_{\lambda_i}$. This topology is called the **product topology**. We refer to $\prod_{\lambda\in\Lambda} X_\lambda$ with the product topology as the **product space**. The following is left as an exercise.

Lemma 1.5. *Let $\{X_\lambda\}$ be a family of topological spaces with product space $\prod_{\lambda\in\Lambda} X_\lambda$. Given a topological space Z, there exists continuous functions $f_\lambda\colon Z \to X_\lambda$ for each $\lambda \in \Lambda$ if and only if there exists a continuous function $f\colon Z \to \prod_{\lambda\in\Lambda} X_\lambda$ such that $f_\lambda = \pi_\lambda \circ f$ for all $\lambda \in \Lambda$.*

For $a = (a_\lambda) \in \prod_{\lambda\in\Lambda} X_\lambda$ and an open neighborhood N_a of a in $\prod_{\lambda\in\Lambda} X_\lambda$, by definition of the product topology, there exists $n \in \mathbf{N}$, $\lambda_1,\dots,\lambda_n \in \Lambda$, and open sets $U_i \subset X_{\lambda_i}$ such that

$\bigcap_{i=1}^{n} \pi_{\lambda_i}^{-1}(U_i) \subset N_a$. In particular, the $a_{\lambda_i} \in U_i$ for $i = 1, \ldots, n$ and

$$\left\{ x \in \prod_{\lambda \in \Lambda} X_\lambda \ : \ \pi_{\lambda_i}(x) = a_{\lambda_i} \text{ for } i = 1, \ldots, n \right\} \subset N_a.$$

Theorem 1.6. *Let $\{X_\lambda\}_{\lambda \in \Lambda}$ be a family of topological spaces with product space $\prod_{\lambda \in \Lambda} X_\lambda$.*

(a) If each X_λ is Hausdorff, then $\prod_{\lambda \in \Lambda} X_\lambda$ is Hausdorff.

(b) If each X_λ is totally disconnected, then $\prod_{\lambda \in \Lambda} X_\lambda$ is totally disconnected.

(c) If each X_λ is compact, then $\prod_{\lambda \in \Lambda} X_\lambda$ is compact.

Proof of Theorem 1.6 (a) and (b). To prove (a), given distinct points $x, y \in \prod_{\lambda \in \Lambda} X_\lambda$, there exists $\lambda_0 \in \Lambda$ such that $x_{\lambda_0} \neq y_{\lambda_0}$. Since X_{λ_0} is Hausdorff, there exists disjoint opens sets $U_{\lambda_0}, V_{\lambda_0} \subset X_{\lambda_0}$ such that $x \in U_{\lambda_0}$, $y \in V_{\lambda_0}$. It follows that $U_x = \pi_{\lambda_0}^{-1}(U_{\lambda_0})$ and $V_x = \pi_{\lambda_0}^{-1}(V_{\lambda_0})$ separate x, y in $\prod_\lambda X_\lambda$.

To prove (b), if $C \subset \prod_{\lambda \in \Lambda} X_\lambda$ is a non-empty connected subset, then $\pi_\lambda(C) = C_\lambda$ is connected for each λ since π_λ is continuous. As X_λ is totally disconnected and C is not empty, C_λ is a singleton set $\{c_\lambda\}$ for each λ and hence $C = \{c\}$ where $c = (c_\lambda)$. ♠

To prove Theorem 1.6 (c), which is known as **Tychonoff's Theorem**, we will use ultrafilters and Zorn's lemma.

Recall in a non-empty partially ordered set S with relation $\leq$, a subset $C \subset S$ is a **chain** if for any pair of elements $c_1, c_2 \in C$, we have either $c_1 \leq c_2$ or $c_2 \leq c_1$. An element $m \in S$ is **maximal** if $m \leq s$ implies $s = m$.

Lemma 1.7 (Zorn's Lemma)**.** *If S is a non-empty partially ordered set such that for each chain $C \subset S$, there exists an element $s_C \in S$ such that $c \leq s_C$ for each $c \in C$, then S contains a maximal element.*

Given a set X and a family of subsets $\mathscr{L}$ of X that is closed under finite intersections and finite unions, we say a family of sets $\mathscr{F} \subset \mathscr{L}$ is a **filter** if

(i) If $F_1, F_2 \in \mathscr{F}$, then $F_1 \cap F_2 \in \mathscr{F}$.

(ii) If $F \in \mathscr{F}$ and $F \subset F'$ for some $F' \in \mathscr{F}$, then $F' \in \mathscr{F}$.

(iii) $\emptyset \notin \mathscr{F}$.

In discussing filters, we will often omit which family of sets $\mathscr{L}$ our filters reside in. The two primary examples for $\mathscr{L}$ will be the set of all closed sets and the power set on X. Unless specified otherwise, the reader can take $\mathscr{L} = \mathscr{P}(X)$.

The simplest examples of filters are principal filters given as follows. For any set $S \subset X$, we define $\mathscr{F}_S$ to be the set of subsets of X that contain S. It is a simple matter to see that (i)–(iii) is satisfied by $\mathscr{F}_S$. The filter $\mathscr{F}_S$ is called a **principal filter** associated to S. If X is a topological space and S is a closed subset, we take our filter $\mathscr{F}_S$ to be comprised of all supersets of S that are closed in X.

Another important example of a filter on X is the **cofinite filter** or **Fréchet** filter. This filter $\mathscr{F}_{cf}(X)$ is defined as

$$\mathscr{F}_{cf}(X) = \{Y \subset X \ : \ X - Y \text{ is finite}\}.$$

This is a filter provided X is infinite since $\emptyset \in \mathscr{F}_{cf}(X)$ when X is finite.

The set of all filters in X that are contained in $\mathscr{L}$ is a partially ordered set via set inclusion. A filter in $\mathscr{L}$ that is maximal with respect to this partial ordering is called a **ultrafilter** in $\mathscr{L}$. Note that since the union of a chain of filters in $\mathscr{L}$ is easily seen to be a filter, every filter $\mathscr{F}$ in $\mathscr{L}$ is contained in an ultrafilter in $\mathscr{L}$ by Zorn's Lemma. The following lemma contains some useful results on filters and ultrafilters.

Lemma 1.8.

(a) Every filter $\mathscr{F}$ is contained in an ultrafilter.

(b) A filter $\mathscr{F}$ in X is an ultrafilter if and only if for each $Y \subset X$, either $Y \in \mathscr{F}$ or $X - Y \in \mathscr{F}$.

(c) For any $x \in X$, the principal filter $\mathscr{F}_{\{x\}}$ is an ultrafilter.

(d) If X is finite, every ultrafilter $\mathscr{F}$ in X is principal.

(e) If X is infinite and $\mathscr{F}$ is a non-principal ultrafilter, then $\mathscr{F}$ contains $\mathscr{F}_{cf}$.

The proofs of the assertions are fairly easy and left to the reader.

Exercise 1. Prove Lemma 1.8.

We say that a set $\mathscr{S} \subset \mathscr{P}(X)$ satisfies the **finite intersection property** if for each finite subset $\mathscr{S}_0 \subset \mathscr{S}$, we have $\bigcap_{S \in \mathscr{S}_0} S \neq \emptyset$. By definition, a filter $\mathscr{F}$ satisfies the finite intersection property. Moreover, any collection of sets with the finite intersection property is contained in a filter.

Lemma 1.9. *If $\mathscr{S}$ is a family of subsets in X with the finite intersection property, then there exists a filter $\mathscr{F}$ that contains $\mathscr{S}$. If X is a topological space and $\mathscr{S}$ consists of closed subsets of X, the filter $\mathscr{F}$ can be taken to contain only closed subsets of X.*

Proof. The filter $\mathscr{F}$ can be built in two stages. First, we add all the finite intersections of the members of $\mathscr{S}$. Second, we take all of the supersets of the members of this new family to get the filter. If X is a topological space and $\mathscr{S}$ consists of closed subsets of X, then in the first stage, the new members will be closed. In the second stage, we simply add only the supersets of S that are closed in X. ♠

We saw in Lemma 1.1 that a topological space X is compact if any only if for each family of closed sets $\mathscr{S}$ of X with the finite intersection property must satisfy $\bigcap_{S\in\mathscr{S}} S \neq \emptyset$.

Lemma 1.10. *A topological space X is compact if and only if for each ultrafilter $\mathscr{F}$ in X of closed sets, we have $\bigcap_{F\in\mathscr{F}} F \neq \emptyset$.*

Proof. For the direct implication, simply note that since X is compact, by Lemma 1.1, we must have $\bigcap_{F\in\mathscr{F}} F \neq \emptyset$ for any filter $\mathscr{F}$ in X consisting of closed sets. For the converse direction, by Lemma 1.1, we must show that for any collection of closed sets $\mathscr{S}$ with the finite intersection property, that we have $\bigcap_{S\in\mathscr{S}} S \neq \emptyset$. By Lemma 1.9, $\mathscr{S}$ is contained in a filter $\mathscr{F}$ of closed sets and hence by hypothesis $\emptyset \neq \bigcap_{F\in\mathscr{F}} F \subset \bigcap_{S\in\mathscr{S}} S$. ♠

We are now ready to prove Theorem 1.6 (c).

Proof of Theorem 1.6 (c). By Lemma 1.10, it suffices to prove that for any ultrafilter $\mathscr{F}$ of closed subsets of $\prod_{\lambda\in\Lambda} X_\lambda$ must satisfy $\bigcap_{F\in\mathscr{F}} F \neq \emptyset$. For each $\lambda \in \Lambda$, we have the filter $\mathscr{F}_\lambda$ in X_λ given by taking all of the closed sets $C \subset X_\lambda$ such that $\pi_\lambda(F) \subset C$ for some $F \in \mathscr{F}$. Since X_λ is compact, we know that $\bigcap_{C\in\mathscr{F}_\lambda} C \neq \emptyset$ and we select $y_\lambda \in X_\lambda$ such that $y_\lambda \in C$ for all $C \in \mathscr{F}_\lambda$. We assert that $y = (y_\lambda)$ is contained in each $F \in \mathscr{F}$. If not, since $\prod_{\lambda\in\Lambda} X_\lambda - F$ is open, there exist open sets $U_1, \ldots, U_n$ in $X_{\lambda_1}, \ldots, X_{\lambda_n}$ such that $y \in \pi_{\lambda_i}^{-1}(U_i)$ for each i and F is disjoint from $\bigcap_{i=1}^n \pi_{\lambda_i}^{-1}(U_i)$. In particular,

$$F \subset \bigcup_{i=1}^n \left(\prod_{\lambda\in\Lambda} X_\lambda - \pi_{\lambda_i}^{-1}(U_i) \right).$$

Since $\mathscr{F}$ is an ultrafilter, by Lemma 1.8 (b), $\prod_{\lambda\in\Lambda} X_\lambda - \pi_{\lambda_{i_0}}^{-1}(U_{i_0}) \in \mathscr{F}$ for some i_0. However, we see that

$$\pi_{\lambda_{i_0}}\Big(\prod_{\lambda\in\Lambda} X_\lambda - \pi_{\lambda_{i_0}}^{-1}(U_{i_0})\Big) \subset X_{\lambda_{i_0}} - U_{i_0},$$

and so $X_{\lambda_{i_0}} - U_{i_0} \in \mathscr{F}_{\lambda_{i_0}}$. Since $y \in \pi_{\lambda_{i_0}}^{-1}(U_{i_0})$, we see that $y_{\lambda_{i_0}} \notin X_{\lambda_{i_0}} - U_{i_0}$, contradicting the fact that $y_\lambda \in C$ for all $\lambda \in \Lambda$ and $C \in \mathscr{F}_\lambda$. Therefore, we conclude that $y \in F$ for all $F \in \mathscr{F}$ and so $\bigcap_{F \in \mathscr{F}} F \neq \emptyset$ as needed to verify that $\prod_{\lambda \in \Lambda} X_\lambda$ is compact. ♠

We now record some results on topological groups that we will need in our discussion on profinite groups. By a **topological group**, we mean a set G that is both a topological space and a group (the binary operation will be denoted multiplicatively) such that the function $G \times G \to G$ given by $(g_1, g_2) \mapsto g_1 g_2^{-1}$ is continuous where the domain is equipped with the product topology. We will denote the identity element in G by 1_G and simply by 1 when G is understood. Given a topological group G, an element $g \in G$, and subsets $U, V \subset G$, we define

$$gU = \{gu \ : \ u \in U\}, \quad Ug = \{ug \ : \ u \in U\}$$
$$U^{-1} = \left\{u^{-1} \ : \ u \in U\right\}, \quad UV = \{uv \ : \ u \in U, \ v \in V\}.$$

We now state several lemmas.

Lemma 1.11. *Let G be a topological group.*

(a) The function $G \to G$ given by $g \mapsto g^{-1}$ is a homeomorphism. In particular, the function $G \times G \to G$ given by $(g_1, g_2) \mapsto g_1 g_2$ is continuous.

(b) For each $g \in G$, the functions $L_g, R_g \colon G \to G$ given by $L_g(h) = gh$, $R_g(h) = hg$ are homeomorphisms.

Lemma 1.12. *Let G be a topological group.*

(a) If H is an open or closed subgroup of G, then gH, Hg are open or closed for all $g \in G$.

(b) Every open subgroup of G is closed and every closed subgroup of finite index is open. If G is compact, every open subgroup of G has finite index.

(c) If H is a subgroup of G, then H is a topological group with respect to the subspace topology.

(d) If K is a normal subgroup of G, then G/K is a topological group with respect to the quotient topology and the quotient map $G \to G/K$ is an open mapping.

Lemma 1.13. *Let G be a topological group.*

(a) G is Hausdorff if and only if $\{1\}$ is closed.

(b) *If K is a normal subgroup, then G/K is Hausdorff if and only of K is closed.*

(c) *If G is totally disconnected, then G is Hausdorff.*

(d) *If G is compact and Hausdorff and C_1, C_2 are closed subsets of G, then C_1C_2 is closed.*

We leave the proofs of Lemmas 1.11, 1.12, and 1.13 to the reader.

Lemma 1.14. *Let G be a compact topological group and $\{X_\lambda\}_{\lambda\in\Lambda}$ a family of closed subsets with the property that for all $\lambda_1,\lambda_2 \in \Lambda$, there exists $\mu \in \Lambda$ such that $X_\mu \subset X_{\lambda_1} \cap X_{\lambda_2}$. If $Y \subset G$ is a closed subset, then*

$$\left(\bigcap_{\lambda\in\Lambda} X_\lambda\right) Y = \bigcap_{\lambda\in\Lambda} (X_\lambda Y).$$

Proof. Visibly, $(\bigcap_\lambda X_\lambda) Y \subset \bigcap_\lambda (X_\lambda Y)$. For the reverse inclusion, we argue by contradiction and assume that there exists $x \in \bigcap_\lambda (X_\lambda Y)$ and $x \notin (\bigcap_\lambda X_\lambda) Y$. It follows that $xY^{-1} \cap (\bigcap_\lambda X_\lambda) = \emptyset$. Since G is compact and the subsets xY^{-1}, X_λ are closed, there exists $n \in \mathbf{N}$ and $i_1,\dots,i_n \in \mathscr{I}$ such that $xY^{-1} \cap \bigcap_{i=1}^n X_{\lambda_i} = \emptyset$. By hypothesis, there exists $\mu \in \mathscr{I}$ such that $X_\mu \subset \bigcap_{i=1}^n X_{\lambda_i}$ and so $xY^{-1} \cap X_\mu = \emptyset$. However, that implies $x \notin X_\mu Y$, which is impossible since $x \in \bigcap_\lambda (X_\lambda Y)$. ♠

Lemma 1.15. *If G is a compact topological group and C is a subset of G that is both open and closed and contains 1, then C contains an open normal subgroup.*

Proof. To prove this lemma, we claim the following:

Claim: *There exists an open subset $U \subset C$ such that $1 \in U$, $U = U^{-1}$, and $U^n \subset C$ for all $n \in \mathbf{N}$ where U^n is defined inductively by $U^1 = U$ and $U^n = U^{n-1}U$.*

Assuming the claim, we prove the lemma. Let $H = \bigcup_{n\in\mathbf{N}} U^n$ be the subgroup generated by U. Since H is open, by Lemma 1.12, H is also closed and finite index in G. As $U^n \subset C$ for all n and C is closed, we see that H is contained in C. Since H is finite index, it has only finitely many conjugates in G and taking the intersection of all of the distinct G–conjugates of H, we obtain an open and closed normal subgroup of G inside of C. We leave the proof of the claim as an exercise. ♠

Exercise 2. Prove the above claim.

Proposition 1.16. *Let G be a compact, totally disconnected, topological group.*

(a) *Every open set in G is a union of cosets of open normal subgroups.*

(b) A subset of G is both open and closed if and only if it is a union of finitely many cosets of open normal subgroups.

(c) If $S \subset G$, then $\overline{S} = \bigcap_{\substack{N \lhd G \\ N \text{ open}}} NS$. In particular, if $C \subset G$ is closed, then $C = \bigcap_{\substack{N \lhd G \\ N \text{ open}}} NC$. Consequently, $\bigcap_{\substack{N \lhd G \\ N \text{ open}}} N = \{1\}$.

Proof. (a): Let $U \subset G$ be an open subset and $x \in U$. Since G is totally disconnected, by Lemma 1.2 (c), U can be expressed as a union of sets that are both open and closed. Hence, we can reduce to the case when U is both open and closed. Under that reduction, we see that the subset $x^{-1}U$ is open, closed, and contains 1. Hence by Lemma 1.15 contains an open normal subgroup. As x was arbitrary, the result follows.

(b): If U is both open and closed, by Part (a) we know that U is a union of cosets of open normal subgroups. Since U is closed and G is compact, U is also compact. Hence, U is a finite union of cosets of open normal subgroups. The converse is straightforward.

(c): This follows from Part (a) after taking complements. ♠

Finally, we note that if $\{G_\lambda\}_{\lambda \in \Lambda}$ is a family of topological groups, then $\prod_\lambda G_\lambda$ is a topological group with the product topology and binary operation given coordinate-wise. Note that if G_λ is compact, Hausdorff, and/or totally disconnected for each $\lambda \in \Lambda$, then $\prod_\lambda G_\lambda$ is compact, Hausdorff, and/or totally disconnected by Theorem 1.6.

1.3 Lecture 3. *Inverse Limits*

A **directed set** is a partially ordered set $(\mathscr{I}, \leq)$ such that for any $i_1, i_2 \in \mathscr{I}$ there exists $\ell \in \mathscr{I}$ with $i_1, i_2 \leq \ell$. An **inverse system of sets indexed by a directed set $\mathscr{I}$** is a pair (X_i, φ_{ij}) where $\{X_i\}_{i \in \mathscr{I}}$ is a family of sets and $\left\{\varphi_{ij} \colon X_j \to X_i\right\}_{\substack{i,j \in \mathscr{I} \\ i \leq j}}$ is a family of functions satisfying $\varphi_{ii} = \mathrm{Id}_{X_i}$ and $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$ for all $i, j, k \in \mathscr{I}$ with $i \leq j \leq k$. When each set X_i is equipped with a group structure, we require the functions φ_{ij} be homomorphisms. Similarly, if the sets X_i are equipped with topological or topological group structures, we require that the functions φ_{ij} be continuous functions or continuous homomorphisms. With those restrictions on the functions φ_{ij}, we will call such inverse systems, **inverse systems of groups**, **inverse systems of topological spaces**, or **inverse systems of topological groups**. For any inverse system of sets (X_i, φ_{ij}), there is an associated inverse system of topological spaces given by endowing the sets X_i with the discrete topology.

Example 2. Let $\mathscr{I} = \mathbf{N}$ and $p \in N$ be prime. For each $i \in \mathbf{N}$, set $Q_i = \mathbf{Z}/p^i\mathbf{Z}$ with $\varphi_{ij}\colon \mathbf{Z}/p^j\mathbf{Z} \to \mathbf{Z}/p^i\mathbf{Z}$ given by $\varphi_{ij}(n + p^j\mathbf{Z}) = n + p^i\mathbf{Z}$. The pair $(Z/p^i\mathbf{Z}, q_{ij})$ is an inverse system of finite groups/rings. We will discuss this example in detail later.

Example 3. Let G be a group and $\mathscr{I}$ a collection of normal subgroups H of G such that if $H_1, H_2 \in \mathscr{I}$ then there is $H \in \mathscr{I}$ with $H \subset H_1 \cap H_2$. The set $\mathscr{I}$ is a directed set under reverse-inclusion; $H \leq H'$ if and only if $H' \subset H$. We can form an inverse system of groups $(Q_H, \varphi_{H,H'})$ where $Q_H = G/H$ and $\varphi_{H,H'}\colon G/H' \to G/H$ when $H \leq H'$; the map $\varphi_{H,H'}$ comes from the isomorphism theorems. .

Given an inverse system of sets (X_i, φ_{ij}) and a set Y, we say that a family of functions $\psi_i\colon Y \to X_i$ is **compatible with** (X_i, φ_{ij}) provided the diagram

$$\begin{tikzcd} & Y \arrow[dl, "\psi_j"'] \arrow[dr, "\psi_i"] & \\ X_j \arrow[rr, "\varphi_{ij}"'] & & X_i \end{tikzcd}$$

commutes for all $i, j \in \mathscr{I}$ with $i \leq j$; that is, $\varphi_{ij} \circ \psi_j = \psi_i$. We will sometimes denote a compatible family of functions by (Y, ψ_i). If the inverse system is a system of groups, topological spaces, or topological groups, we insist that Y have the same structure and the functions ψ_i be homomorphisms, continuous, or continuous homomorphisms.

Definition 1.17 (Inverse Limit)**.** Let (X_i, φ_{ij}) be an inverse system of set (groups, rings, topological spaces, topological groups, .etc) with indexing set $\mathscr{I}$. We say that (X, φ_i) is an **inverse limit** of (X_i, φ_{ij}) if X is a set (group, ring, topological space, topological group, .etc) with a compatible family of functions φ_i that satisfies the following universal mapping property: If Y is another set (group, ring, topological space, topological group, .etc) with a compatible family of functions ψ_i, there exists a unique function $\psi\colon Y \to X$ such that the diagram

$$\begin{tikzcd} & Y \arrow[dl, "\psi"'] \arrow[dr, "\psi_i"] & \\ X \arrow[rr, "\varphi_i"'] & & X_i \end{tikzcd}$$

commutes for all $i \in \mathscr{I}$.

We now prove that inverse limits exists and are unique.

Theorem 1.18. *Let (X_i, φ_{ij}) be an inverse system of sets with indexing set $\mathscr{I}$.*

(a) If (X, φ_i) and (Y, ψ_i) are inverse limits of the inverse system (X_i, φ_{ij}), then there is a bijection (homeomorphism, isomorphism, .etc) $\overline{\varphi}\colon X \to Y$ such that $\psi_i \circ \overline{\varphi} = \varphi_i$ for all $i \in \mathscr{I}$.

(b) Define
$$X = \left\{ x \in \prod_i X_i \;:\; \varphi_{ij}(\pi_j(x)) = \pi_i(x) \textit{ for all } i, j \in \mathscr{I} \textit{ with } i \leq j \right\}$$
with functions $\varphi_i\colon X \to X_i$ given by $\varphi_i(x) = \pi_i(x)$. Then (X, φ_i) is an inverse limit of the inverse system (X_i, φ_{ij}).

(c) If (X_i, φ_{ij}) is an inverse system of topological groups and (X, φ_i) is an inverse limit, then X is a topological group and the functions φ_i are continuous homomorphisms.

Proof. (a): By the universal mapping property for inverse limits, we have functions $\varphi_X : X \to Y$ and $\varphi_Y : Y \to X$ such that $\varphi_i = \psi_i \circ \varphi_X$ and $\varphi_i \circ \varphi_Y = \psi_i$. Consequently, $\varphi_i \circ \varphi_Y \circ \varphi_X = \varphi_i$, and so $\varphi_Y \circ \varphi_X = \mathrm{Id}_X$ by the uniqueness of mapping in Definition 1.17. Similarly, $\psi_i \circ \varphi_X \circ \varphi_Y = \psi_i$, and so $\varphi_X \circ \varphi_Y = \mathrm{Id}_Y$. Hence φ_X is a bijection. Here is a nice commutative diagram for this proof:

$$\begin{tikzcd}
X \arrow[rr, leftrightarrow, "\mathrm{Id}_X"] \arrow[dr, "\varphi_i"] \arrow[dd, leftrightarrow, "\varphi_X"', "\varphi_Y"] & & X \arrow[dl, "\varphi_i"'] \arrow[dd, leftrightarrow, "\varphi_Y"', "\varphi_X"] \\
 & X_i & \\
Y \arrow[rr, leftrightarrow, "\mathrm{Id}_Y"'] \arrow[ur, "\psi_i"'] & & Y \arrow[ul, "\psi_i"]
\end{tikzcd}$$

(b): We must prove that (X, φ_i) is an inverse limit on (X_i, φ_{ij}) where
$$X = \left\{ x \in \prod_i X_i \;:\; \varphi_{ij}(\pi_j(x)) = \pi_i(x), \text{ for all } i, j \in \mathscr{I} \text{ with } i \leq j \right\}$$

and the functions φ_i are the restriction of the projection maps $\pi_i\colon \prod_j X_j \to X_i$ to X. Given a set Y with a compatible family of functions $\psi_i\colon Y \to X_i$, we need a unique function $\psi\colon Y \to X$ such that $\varphi_i \circ \psi = \psi_i$ for all $i \in \mathscr{I}$. We define $\psi\colon Y \to \prod_i X_i$ by $\psi(y) = (\psi_i(y))$ and note that the compatibility of the family ψ_i implies the image of ψ is in X. We leave the uniqueness of the map ψ to the reader.

(c): If X_i are topological spaces, X is a topological space via the subspace topology coming from the product space $\prod_i X_i$. If the X_i are also groups, X is a topological group and the functions φ_i are continuous homomorphisms. ♠

Given an inverse system of topological groups (X_i, φ_{ij}), Theorem 1.18 shows that there is a unique inverse limit (X, φ_i) and it is a topological group. We denote the limit by $\varprojlim X_i$.

Proposition 1.19. *Let (X_i, φ_{ij}) be an inverse system of topological spaces with indexing set $\mathscr{I}$ and $X = \varprojlim X_i$.*

(a) If each X_i is Hausdorff, then X is Hausdorff and $X \subset \prod_i X_i$ is closed.

(b) If each X_i is totally disconnected, then X is totally disconnected.

(c) If each X_i is compact and Hausdorff, then X is compact and Hausdorff. Moreover, if each X_i is non-empty, then X is non-empty.

Proof. (a): By Theorem 1.18 (a)-(b), we can view $X \subset \prod_i X_i$. Since X_i is Hausdorff for each $i \in \mathscr{I}$, by Theorem 1.6 (a), the product $\prod_i X_i$ is Hausdorff. Hence, X is Hausdorff as any subspace of a Hausdorff space is Hausdorff. By Lemma 1.3 (e), we know that

$$E_{i,j} = \left\{ x \in \prod_i X_i \ : \ \varphi_{ij}(\pi_j(x)) = \pi_i(x) \right\}$$

is a closed subset and so $X = \bigcap_{i \le j} E_{i,j}$ is closed.

(b): Any subspace of a totally disconnected space is totally disconnected.

(c): By Theorem 1.6 (c), $\prod_i X_i$ is compact and by Part (a), $X \subset \prod_i X_i$ is Hausdorff and closed. Hence, X is compact and Hausdorff by Lemma 1.3 (a). To prove that X is non-empty with each X_i is a non-empty, compact, Hausdorff space, one can check that $\bigcap_{i \le j} E_{i,j} \neq \emptyset$. We leave that as an exercise. ♠

Exercise 3. Prove that $\bigcap_{i \le j} E_{i,j} \neq \emptyset$.

The following suite of results will be useful in the sequel.

Proposition 1.20. *Let (X_i, φ_{ij}) be an inverse system of non-empty, compact Hausdorff spaces with indexing set $\mathscr{I}$ and $(X, \varphi_i) = \varprojlim (X_i, \varphi_{ij})$.*

(a) $\varphi_i(X) = \bigcap_{j \geq i} \varphi_{ij}(X_j)$ for each $i \in \mathscr{I}$.

(b) The set of subsets $\varphi_i^{-1}(U)$, varying over $i \in \mathscr{I}$ and open subsets $U \subset X_i$, form a base for X.

(c) If $Y \subset X$ satsfies $\varphi_i(Y) = X_i$ for each $i \in \mathscr{I}$, then Y is dense in X.

(d) If $\psi \colon Y \to X$ is a function and Y is a topological space, then ψ is continuous if and only if $\varphi_i \circ \psi$ is continuous for each $i \in \mathscr{I}$.

(e) If $f \colon X \to A$ is a continuous function and A is a discrete space, then there exists $r \in \mathscr{I}$ and a continuous function $f_r \colon X_r \to A$ such that $f = f_r \circ \varphi_r$.

Proof. As before, we will take $X \subset \prod_i X_i$ as in Theorem 1.18 (b).

(a): By compatibility of mappings, we know that $\varphi_i(X) = \varphi_{ij}(\varphi_j(X)) \subset \varphi_{ij}(X_j)$ for all $j \geq i$. Consequently, $\varphi_i(X) \subset \bigcap_{j \geq i} \varphi_{ij}(X_j)$. For the reverse inclusion, given $x \in \bigcap_{j \geq i} \varphi_{ij}(X_j)$ and $j \geq i$, we define

$$Y_j = \left\{ y \in X_j \ : \ \varphi_{ij}(y) = x \right\} = \varphi_{ij}^{-1}(\{x\}).$$

As $\{x\}$ is closed, φ_{ij} is continuous, and X_j is compact, Y_j is compact by Lemma 1.3 (a). If $i \leq j \leq k$ and $y \in Y_k$, we see that $\varphi_{jk}(y) \in Y_j$ since $\varphi_{ij}(\varphi_{jk}(y)) = \varphi_{ik}(y) = x$. In particular, the family (Y_j, φ_{jk}) is an inverse limit system of non-empty compact, Hausdorff spaces and so $Y = \varprojlim Y_j$ is a non-empty closed subset of $\prod_j Y_j$. For any $y \in Y$ with $y = (y_j)$, we have $\varphi_{jk}(y_k) = y_j$ and $y_i = x$. If $\ell \in \mathscr{I}$ and $i \not\leq \ell$, there exists $j \in \mathscr{I}$ such that $i, \ell \leq j$. We define $y_\ell \in Y_\ell$ by $\varphi_{\ell j}(y_j)$ and note that this is independent of j by compatibility of mappings. This yields $y \in X$ such that $\varphi_i(y) = x$.

(b): Every open subset in X is of the form

$$U = X \cap \left(\bigcap_{j=1}^{n} \pi_{i_j}^{-1}(U_j) \right)$$

where $n \in \mathbf{N}$, $i_1, \dots, i_n \in \mathscr{I}$, and $U_j \subset X_{i_j}$ is an open subset. For $u \in U$ with $u = (u_i)$, we select $k \geq i_1, \dots, i_n$. The set $\varphi_{i_j k}^{-1}(U_j)$ is open for all $j \in \{1, \dots, n\}$ and contains u_k. For $V_k =$

$\bigcap_{j=1}^{n} \varphi_{i_j k}^{-1}(U_j)$, we see that $\varphi_k^{-1}(V_k) \subset U$ and contains u. Hence, U is expressible as a union of open subsets of the form $\varphi_k^{-1}(U)$, and so this collection of open subsets of X is a base for X.

(c): For each $i \in \mathscr{I}$ and non-empty open subset $U \subset X_i$, we have $\varphi_i(Y) \cap U \neq \emptyset$ and so $Y \cap \varphi_i^{-1}(U) \neq \emptyset$. Hence, Y is dense since the open subsets $\varphi_i^{-1}(U)$ form a base for X by Part (b); recall that Y is dense if and only if $Y \cap U \neq \emptyset$ for any non-empty open set U.

(d): The direct implication follows from the continuity of the composition of continuous functions. For the reverse implication, we know that $\psi^{-1}(\varphi_i^{-1}(U))$ is an open subset of Y for all $i \in \mathscr{I}$ and open subsets $U \subset X_i$. Since $\varphi_i^{-1}(U)$ form a base by Part (b), it follows that ψ is continuous.

(e): Setting $A_0 = f(X)$, we see that A_0 is finite since it is compact and discrete. For each $a \in A_0$, the set $f^{-1}(a)$ is compact and open. Therefore, $f^{-1}(a)$ is a finite union of open sets of the form $\varphi_i^{-1}(U)$. Since A_0 is finite, there exists $n \in \mathbf{N}$, $i_1, \ldots, i_n \in \mathscr{I}$, and open sets $U_j \subset X_{i_j}$ such that for each $a \in A_0$, the set $f^{-1}(a)$ is a finite union of subsets from $\left\{\varphi_{i_1}^{-1}(U_1), \ldots, \varphi_{i_n}^{-1}(U_n)\right\}$. Now, select $\ell \in \mathscr{I}$ such that $\ell \geq i_j$ for all $j = 1, \ldots, n$. By compatibility of mappings, we have $\varphi_{i_j}^{-1}(U_j) = \varphi_\ell^{-1}(\varphi_{i_j \ell}(U_j))$ for each j. Therefore, for each $a \in A_0$, we have $f^{-1}(a) = \varphi_\ell^{-1}(U_a)$ for some open subset $U_a \subset X_\ell$. Next, set $C = X_\ell - \bigcup_{a \in A_0} U_a$. Since for every $x \in X$, we know that $\varphi_\ell(x) \in U_a$ for $a = f(x)$, we see that $C \cap \varphi_\ell(X) = \emptyset$. By Part (a), we have $C \cap \left(\bigcap_{k \geq \ell} \varphi_{\ell k}(X_k)\right) = \emptyset$. Since X_k is compact, there exists $m \in \mathbf{N}$ and $r_1, \ldots, r_m \in \mathscr{I}$ such that $C \cap (\bigcap_{s=1}^{m} \varphi_{\ell r_s}(X_{r_s})) = \emptyset$. Now take $r \geq r_1, \ldots, r_m$ and observe, by compatibility of mappings, that $C \cap \varphi_{\ell r}(X_r) = \emptyset$ and $\varphi_{\ell r}(X_r) \subset \bigcup_{a \in A_0} U_a$. For each $a \in A_0$, set $W_a = \varphi_{\ell r}^{-1}(U_a) \subset X_r$ and note that if $a \neq a'$, then $W_a \cap W_{a'} = \emptyset$. Moreover, for each $x \in X_r$, we know that $\varphi_{\ell r}(x) \in U_a$ for $f(x) = a$, and so $x \in W_a$. Hence, X_r is the disjoint union of the open and closed subsets W_a. The function $f_r \colon X_r \to A$ given by $f_r(x) = a$ for $x \in W_a$ is continuous and satisfies $f = f_r \circ \varphi_r$ ♠

Proposition 1.21. *Let X be a totally disconnected, compact, Hausdorff space. Then X is an inverse limit of its discrete quotient spaces.*

Proof. Let $\mathscr{I}$ be the set of all partitions of X into finitely many subsets that are both open and closed. For each $i \in \mathscr{I}$, we have the associated quotient space X_i given by the equivalence relation associated to the partition i and associated quotient map $q_i \colon X \to X_i$. Since the partition sets are both open and closed, X_i is a discrete space. As X is compact, these are precisely the discrete quotient spaces of X.

For $i, j \in \mathscr{I}$, we write $i \leq j$ if and only if there exists $q_{ij} \colon X_j \to X_i$ satisfying $q_{ij} \circ q_j = q_i$. As the maps q_j are surjective, if q_{ij} exists, it must be unique. Given $i, j \in \mathscr{I}$, we have associated partitions $i = \{U_1, \ldots, U_m\}$ and $j = \{V_1, \ldots, V_n\}$. For these partitions, we obtain a refinement

$k = \{U_r \cap V_s\}_{r,s=1}^{m,n}$ with $i, j \leq k$, and so $\mathscr{I}$ is a directed set. Hence, we have an inverse system (X_i, q_{ij}) and a compatible family of maps (X, q_i). Take $Y = \varprojlim(X_i, q_{ij})$ with projection maps $\widehat{q}_i \colon Y \to X_i$. By the universal mapping property for Y, there exists a unique continuous function $q \colon X \to Y$ such that $\widehat{q}_i \circ q = q_i$. We assert that q is a homeomorphism. Since q is continuous and X, Y are compact and Hausdorff, it suffices to show that q is bijective by Lemma 1.3 (d). Given $x_1, x_2 \in X$ with $q(x_1) = q(x_2)$, then $q_i(x_1) = q_i(x_2)$ for every $i \in \mathscr{I}$. In particular, no open and closed set of X can contain just one of x_1, x_2. Since X is totally disconnected, we must have $x_1 = x_2$. To see that q is onto, note that since $\widehat{q}_i(q(X)) = q_i(X) = X_i$, $q(X)$ is dense in Y. However, $q(X)$ is closed by Lemma 1.3 and so q is onto. ♠

Lecture 3: After hours thoughts Inverse limits are central to the theory of profinite groups and a great deal of time in this section was spent on developing the basic theory of profinite groups. A profinite group is an inverse limit of an inverse system of finite groups equipped with the discrete topology. In particular, profinite groups are totally disconnected, compact, Hausdorff topological groups. The points of the inverse limit are described concretely via the embedding of the completion $\varprojlim X_i \subset \prod_i X_i$. Specifically, it is the maximal subset of $\prod_i X_i$ such that the restriction of the projection maps π_i to the subset yields a compatible family of functions. The points of the inverse limit can be thought of as functions $f \colon \mathscr{I} \to \bigcup_i X_i$ such that $f(i) \in X_i$ and f is compatible with the maps φ_{ij}. These functions are called nets on the disjoint union of the sets $\bigcup_i X_i$ indexed by $\mathscr{I}$, and X can be viewed as the set of such nets that are compatible with the maps φ_{ij}.

Example 4. X_i is finite, $\mathscr{I} = \mathbf{N}$ and each φ_{ij} is surjective. The inverse limit of (X_i, φ_{ij}) is the set of sequences given as follows. For $i = 0$, we pick $x_0 \in X_0$. Next, we pick $x_1 \in X_1$ with $\varphi_{01}(x_1) = x_0$, and so forth to obtain a sequence $x_j \in X_j$. At each stage x_j, at the $(j+1)$–stage we can select any $x_{j+1} \in \varphi_{jj+1}^{-1}(x_j)$. In particular, the set of all such sequences can be thought of as sequences/paths in a $|X_0|$–rooted forest with vertices X_j and roots vertices in X_0.

Chapter 2

Profinite Groups and Completions

In this chapter, we introduce profinite groups and establish some basic results with regard to profinite groups.

2.1 Lecture 4. *Profinite Groups*

In this lecture, we introduce the concept of a profinite group. These groups are inverse limits of finite groups. Before define profinite groups, we prove a pair of requisite results on inverse limits of topological groups.

Proposition 2.1. *If (G, φ_i) is an inverse limit of an inverse system (G_i, φ_{ij}) of compact Hausdorff topological groups and $K \lhd G$ is an open normal subgroup, then there exists $i_K \in \mathscr{I}$ such that* $\ker \varphi_{i_K} \subset K$.

Proof. Since G is compact, K is finite index by Lemma 1.12 (b). Since G/K is discrete and $G \to G/K$ is continuous, the existence of i_K follows from Proposition 1.20 (e). ♠

Given a set X, a family $\mathscr{I}$ of non-empty subsets of X is called a **filter base** if for each $S_1, S_2 \in \mathscr{I}$, there exists $S_3 \in \mathscr{I}$ such that $S_3 \subset S_1 \cap S_2$. By adding all the supersets of the members of $\mathscr{I}$, we obtain a filter $\mathscr{F}(\mathscr{I})$ called the **filter spanned by** $\mathscr{I}$.

Given a filter base $\mathscr{I}$ of subgroups of a group G, we equip $\mathscr{I}$ with a partial relation $\leq_{rev}$ defined by $K \leq_{rev} L$ if and only if $L \subset K$. Since $\mathscr{I}$ is a filter base, it follows that $\mathscr{I}$ is a directed set. When $K \leq_{rev} L$, we obtain a surjective homomorphism $\varphi_{KL}\colon G/L \to G/K$ and see that $(G/K, \varphi_{KL})$ is an inverse limit system of groups indexed by $\mathscr{I}$.

Proposition 2.2. *Let G be a topological group with a filter base of closed, normal subgroups $\mathscr{I}$ and associated inverse system $(G/K, \varphi_{KL})$. Then there exists a continuous homomorphism $\theta\colon G \to \varprojlim G/K$ such that the following holds:*

(i) $\ker\theta = \bigcap_{K\in\mathscr{I}} K$.

(ii) *$\theta(G)$ is dense in $\varprojlim G/K$.*

(iii) *For each $K \in \mathscr{I}$, $\varphi_K \circ \theta\colon G \to G/K$ is the canonical quotient.*

Moreover, if G is compact, then θ is surjective, and if additionally $\bigcap_{K\in\mathscr{I}} = K = \{1\}$, then θ is isomorphism (of topological groups).

Proof. For each $K \in \mathscr{I}$, we have the canonical quotient $\psi_K\colon G \to G/K$. We define the continuous homomorphism $\theta\colon G \to \prod_K G/K$ by $\theta(g) = (\psi_K(g))_K$. By the isomorphism theorems, we see that the maps ψ_K are compatible with the inverse system $(G/K, \varphi_{KL})$ and so $\theta(G) \subset \varprojlim G/K \subset \prod_K G/K$. (i), (iii) follow from the definition of θ. (ii) follows from Proposition 1.20 (c).

If G is compact, since $\theta(G)$ is closed and dense, the map θ is onto. The validity of the additional assert follows from this with Part (i) and Lemma 1.3 (d). ♠

Throughout the remainder of this note, all finite groups will be equipped with the discrete topology unless stated otherwise. For a class of finite group $\mathscr{C}$, we say an inverse system of finite groups (G_i, φ_{ij}) is an **inverse system of $\mathscr{C}$–groups** if for each $i \in \mathscr{I}$, we have $G_i \in \mathscr{C}$. We call the inverse limit of an inverse system of $\mathscr{C}$–groups a **pro–$\mathscr{C}$ group**.

Example 5 (Class of Finite Groups)**.** Some important examples of classes of groups are the following:

- $\mathscr{C}_{fin}$ is the class of all finite groups. Inverse limits of finite groups (or $\mathscr{C}_{fin}$–groups) are called **profinite groups**.
- $\mathscr{C}_{cyc}$ is the class of all finite cyclic groups. Inverse limits of finite cyclic groups are called **procyclic groups**.
- For each prime $p \in \mathbf{N}$, $\mathscr{C}_p$ is the class of all finite p–groups. Inverse limits of finite p–groups are called **pro–p groups**.

- $\mathscr{C}_{ab}$, $\mathscr{C}_{nil}$, and $\mathscr{C}_{sol}$ are the classes of all finite abelian, nilpotent, and solvable groups. Inverse limits are called pro-abelian groups, pro-nilpotent groups, and pro-solvable groups, respectively.

We will say that a class of finite groups $\mathscr{C}$ is **closed under subgroups** if for each $G \in \mathscr{C}$ and each subgroup $H \subset G$, we have $H \in \mathscr{C}$. We say that $\mathscr{C}$ is **closed under products** if for any $G_1, G_2 \in \mathscr{C}$, we have $G_1 \times G_2 \in \mathscr{C}$. We say that $\mathscr{C}$ is **closed under quotients** if for each $G \in \mathscr{C}$ and each homomorphism $\varphi \colon G \to G'$, we have that $\varphi(G) \in \mathscr{C}$.

Theorem 2.3. *Let $\mathscr{C}$ be a class of finite groups that is closed under products and subgroups. Then the following are equivalent:*

(i) *G is a pro–$\mathscr{C}$ group.*

(ii) *G is isomorphic to a closed subgroup group of a product of $\mathscr{C}$–groups.*

(iii) *G is compact and $\bigcap_{\substack{N \lhd G, \\ G/N \in \mathscr{C}, \\ N \text{ open}}} N = \{1\}$.*

(iv) *G is compact, totally disconnected, and for every open normal subgroup $L \lhd G$, there is an open normal subgroup $N \lhd G$ with $N \subset L$ and $G/N \in \mathscr{C}$.*

If $\mathscr{C}$ is closed under quotients, then (iv) can be replaced with

(iv)' *G is compact, totally disconnected, and $G/L \in \mathscr{C}$ for every open normal subgroup $L \lhd G$.*

Proof. (i) $\to$ (ii). Since G is a pro–$\mathscr{C}$ group, then by Theorem 1.18 (b), $G \subset \prod_i G_i$ where $G_i \in \mathscr{C}$. Since each G_i is Hausdorff, by Proposition 1.19 (a), we know that G is a closed subgroup of $\prod_i G_i$.

(ii) $\to$ (iii). By assumption, G is a closed subgroup of a totally disconnected, compact, Hausdorff topological group $\prod_i G_i$ for some directed set $\mathscr{I}$ and groups $G_i \in \mathscr{C}$. Hence, G is compact by Lemma 1.3 (a). The assertion

$$\bigcap_{\substack{N \lhd G, \\ G/N \in \mathscr{C}, \\ N \text{ open}}} N = \{1\}$$

follows from Proposition 1.16 (c).

(iii) $\to$ (i). Set $\mathscr{I}$ be the filter base of open normal subgroups N of G such that $G/N \in \mathscr{C}$. Since G is compact, by Proposition 2.2, G is isomorphic with $\varprojlim G/N$.

(i) $\to$ (iv). Since G is a pro–$\mathscr{C}$ group, it follows that G is compact and totally disconnected. The additional assertion follows from Proposition 2.1.

(iv) $\to$ (iii). This follows from Proposition 1.16 (c).

We leave the proof of the remainder of the theorem involving (iv)' to the reader. ♠

We now restate Theorem 2.3 in the setting of profinite groups.

Corollary 2.4. *Let G be a topological group. Then the following are equivalent:*

(i) G is profinite.

(ii) G is isomorphic to a closed subgroup of a product of finite groups.

(iii) G is compact and $\bigcap_{\substack{N \lhd G,\\ N \text{ open}}} N = \{1\}$.

(iv) G is compact and totally disconnected.

The following result will be useful in our study of profinite groups.

Theorem 2.5.

(a) If G is a profinite group and $\mathscr{I}$ is a filter base of closed normal subgroups such that $\bigcap_{N\in\mathscr{I}} N = \{1\}$*, then* $G \cong \varprojlim_{N\in\mathscr{I}} G/N$*. If H is a closed subgroup, then* $H \cong \varprojlim_{N\in\mathscr{I}} H/(H\cap N)$*. If K is a closed normal subgroup, then* $G/K \cong \varprojlim_{N\in\mathscr{I}} G/KN$.

(b) If $\mathscr{C}$ is a class of finite group that is closed under subgroups and products, then closed subgroups, products, and inverse limits of pro–$\mathscr{C}$ groups are also pro–$\mathscr{C}$ groups. If $\mathscr{C}$ is also closed under quotients, then quotients of pro–$\mathscr{C}$ groups by closed normal subgroups are also pro–$\mathscr{C}$ groups.

Proof. (a): Since G is compact, the first assertion follows from Proposition 2.2. Since H is closed, H is compact and so the second assertion follows from Proposition 2.2 with the filter base $\mathscr{I}_H = \{H\cap N\}$. Finally, for the last assertion, since G is compact, G/K is compact. Since K is closed, for the filter base $\mathscr{I}_K = \{KN\}$ of open normal subgroups, we have $\bigcap_N N = K$ by Proposition 1.16 (c). Hence, the assertion follows by Proposition 2.2.

(b): This is clear for (a). ♠

Finally, we have the following factorization result.

Lemma 2.6. *Let G be a profinite group, A a discrete space, and $f\colon G \to A$ a function. Then f is continuous if and only if there exists an open normal subgroup K of G and a function $f_K\colon G/K \to A$ such that $f = f_K \circ \psi_K$ where $\psi_K\colon G \to G/K$ is the canonical quotient.*

Proof. This is an immediate consequence of Proposition 1.20 (e). ♠

We say the f **factors through** G/K when in the setting of Lemma 2.6.

2.2 Lecture 5. *Completions of Groups*

In this lecture, we turn out attention to profinite completions of groups with respect to filter bases of finite index, normal subgroups. We will also consider homomorphisms of a given group to the group of invertible matrices over a commutative ring with identity. We attach to each such representation an associated profinite completion.

Given a group Γ, we set $\mathscr{I}_\Gamma$ to be the filter base of finite index, normal subgroups of Γ. Given a filter base $\mathscr{I} \subset \mathscr{I}_\Gamma$, we have an associated inverse system of finite groups $(\Gamma/\Delta, \varphi_{ij})$ and with associated inverse limit $\Gamma_{\mathscr{I}} = \varprojlim \Gamma/\Delta$. We call $\Gamma_{\mathscr{I}}$ the **profinite completion of Γ with respect to $\mathscr{I}$**. We also have an associate topology on Γ coming from $\mathscr{I}$. Specifically, we define a neighborhood (filter) base for $\gamma \in \Gamma$ to be the $\gamma\mathscr{I} = \{\gamma\Delta\}_{\Delta\in\mathscr{I}}$. We call this topology the **profinite topology associated to $\mathscr{I}$** and denote it by $\mathscr{T}_{\mathscr{I}}$. Finally, for each $\Delta \in \mathscr{I}$, we let $\psi_\Delta\colon \Gamma \to \Gamma/\Delta = Q_\Delta$

Proposition 2.7. *Let Γ be a group, $\mathscr{I} \subset \mathscr{I}_\Gamma$ a filter base, and $\Gamma_{\mathscr{I}}$ the completion of Γ with respect to $\mathscr{I}$.*

(a) *There exists a unique continuous homomorphism $\varphi_{\mathscr{I}}\colon (\Gamma, \mathscr{T}_{\mathscr{I}}) \to \Gamma_{\mathscr{I}}$ such that the $\varphi_\Delta \circ \varphi_{\mathscr{I}} = \psi_\Delta$ for all $\Delta \in \mathscr{I}$.*

(b) *$\varphi_{\mathscr{I}}(\Gamma)$ is dense in $\Gamma_{\mathscr{I}}$.*

(c) $\ker \varphi_{\mathscr{I}} = \bigcap_{\Delta\in\mathscr{I}} \Delta$.

Proof. This follows from Proposition 2.2. ♠

Lemma 2.8. *Let Γ be a group, $\mathscr{I} \subset \mathscr{I}_\Gamma$ a filter base, and $\Gamma_{\mathscr{I}}$ the completion of Γ with respect to $\mathscr{I}$. If H is a finite group and $\theta\colon (\Gamma, \mathscr{T}_{\mathscr{I}}) \to H$ is a continuous homomorphism, then there exists a unique continuous homomorphism $\theta_{\mathscr{I}}\colon \Gamma_{\mathscr{I}} \to H$ with $\theta = \theta_{\mathscr{I}} \circ \varphi_{\mathscr{I}}$.*

Proof. Since θ is continuous, we know there exists $\Delta \in \mathscr{I}$ such that $\Delta \subset \ker\theta$. By the isomorphism theorems, we have a continuous homomorphism $\eta\colon \Gamma/\Delta \to H$ such that $\theta = \eta \circ \psi_\Delta$. Set $\theta_{\mathscr{I}} = \eta \circ \varphi_\Delta$. ♠

Proposition 2.9. *Let Γ be a group, $\mathscr{I} \subset \mathscr{I}_\Gamma$ a filter base, and $\Gamma_{\mathscr{I}}$ the completion of Γ with respect to $\mathscr{I}$. If H is a profinite group and $\theta\colon (\Gamma, \mathscr{T}_{\mathscr{I}}) \to H$ is a continuous homomorphism, then there exists a unique continuous homomorphism $\theta_{\mathscr{I}}\colon \Gamma_{\mathscr{I}} \to H$ such that $\theta = \theta_{\mathscr{I}} \circ \varphi_{\mathscr{I}}$.*

Proof. Let $H = \varprojlim (H_i, \psi_{ij})_{\mathscr{J}}$. For each $i \in \mathscr{J}$, we have continuous homomorphisms $\varphi_{H,i}\colon H \to H_i$. Since θ is continuous, by Lemma 2.8, there exists a unique continuous $\theta_{i,\mathscr{I}}\colon \Gamma_{\mathscr{I}} \to H_i$ such that $\varphi_{H,i} \circ \theta = \theta_{i,\mathscr{I}} \circ \varphi_{\mathscr{I}}$. The family of continuous homomorphisms $\theta_{i,\mathscr{I}}$ is compatible with (H_i, ψ_{ij}) and so by definition of inverse limits, there exists a unique continuous homomorphism $\theta_{\mathscr{I}}\colon \Gamma_{\mathscr{I}} \to H$. It is straightforward to see that this is the desired map. ♠

The **profinite completion of Γ** is the completion of Γ with respect to $\mathscr{I}_\Gamma$. We denote the profinite completion of Γ by $\widehat{\Gamma}$ and the associated continuous homomorphism $\widehat{\varphi}\colon \Gamma \to \widehat{\Gamma}$. Since $\mathscr{I}_\Gamma$ contains all of the filter bases $\mathscr{I}$ considered above, the profinite completion has continuous, surjective homomorphism to every completion $\Gamma_{\mathscr{I}}$.

Given a filter base $\mathscr{I} \subset \mathscr{I}_\Gamma$, we can take the filter $\mathscr{F} \subset \mathscr{I}_\Gamma$ spanned by $\mathscr{I}$. Note that we can take the completion of Γ with respect to $\mathscr{I}$ or $\mathscr{F}$. However, it follows from Theorem 2.5 that $\Gamma_{\mathscr{I}} \cong \Gamma_{\mathscr{F}}$. Given a pair of filter bases $\mathscr{I}_1, \mathscr{I}_2 \subset \mathscr{I}_\Gamma$, we say that $\mathscr{I}_1 \leq \mathscr{I}_2$ if $\mathscr{F}_1 \subset \mathscr{F}_2$ where $\mathscr{F}_1, \mathscr{F}_2 \subset \mathscr{I}_\Gamma$ are the filters (in $\mathscr{I}_\Gamma$) spanned by $\mathscr{I}_1, \mathscr{I}_2$

Lemma 2.10. *Given a pair of filter bases $\mathscr{I}_1, \mathscr{I}_2 \subset \mathscr{I}_\Gamma$, then $\mathscr{I}_1 \leq \mathscr{I}_2$ if and only if for each $\Delta_1 \in \mathscr{I}_1$, there exists $\Delta_2 \in \mathscr{I}_2$ such that $\Delta_2 \subset \Delta_1$.*

Proof. This is clear. ♠

Proposition 2.11. *If Γ is a group and $\mathscr{I}_1, \mathscr{I}_2 \subset \mathscr{I}_\Gamma$ are filter bases such that $\mathscr{I}_1 \leq \mathscr{I}_2$, then there exists a unique continuous homomorphism $\pi_{\mathscr{I}_1 \mathscr{I}_2}\colon \Gamma_{\mathscr{I}_2} \to \Gamma_{\mathscr{I}_1}$ such that $\varphi_{\mathscr{I}_1} = \pi_{\mathscr{I}_1 \mathscr{I}_2} \circ \varphi_{\mathscr{I}_2}$.*

Proof. Let $\mathscr{F}_1, \mathscr{F}_2$ be the filters spanned by $\mathscr{I}_1, \mathscr{I}_2$. Since $\mathscr{I}_1 \leq \mathscr{I}_2$, we know that $\mathscr{F}_1 \subset \mathscr{F}_2$. As noted above, $\Gamma_{\mathscr{F}_i} \cong \Gamma_{\mathscr{I}_i}$ and so we will work with the completions with respect to the filters $\mathscr{F}_1, \mathscr{F}_2$. As $\Gamma_{\mathscr{F}_1} \subset \prod_{Q \in \mathscr{F}_1} Q$ and $\mathscr{F}_1 \subset \mathscr{F}_2$, we have a continuous projection $\prod_{Q \in \mathscr{F}_2} \to \prod_{Q \in \mathscr{F}_1}$.

By construction, the image of $\Gamma_{\mathscr{F}_1}$ under this projection is onto $\Gamma_{\mathscr{F}_1}$ and satisfies the mapping equation. ♠

Corollary 2.12. *Let Γ be a group, $\mathscr{I} \subset \mathscr{I}_\Gamma$ a filter base, and $\Gamma_{\mathscr{I}}$ the completion of Γ with respect to $\mathscr{I}$. Then there exists a unique continuous surjective homomorphism $\pi_{\mathscr{I}}\colon \widehat{\Gamma} \to \Gamma_{\mathscr{I}}$ such that $\varphi_{\mathscr{I}} = \pi_{\mathscr{I}} \circ \widehat{\varphi}$.*

Setting $\mathscr{J}$ to be the directed set of filter bases $\mathscr{I} \subset \mathscr{I}_\Gamma$, we obtain an inverse system of profinite groups $(\Gamma_{\mathscr{I}}, \pi_{\mathscr{I}_1\mathscr{I}_2})$. It follows that $(\widehat{\Gamma}, \pi_{\mathscr{I}}) \cong \varprojlim(\Gamma_{\mathscr{I}}, \pi_{\mathscr{I}_1\mathscr{I}_2})$.

Given a class of finite groups $\mathscr{C}$ and a group Γ, we say that Γ is **residually** $\mathscr{C}$ if for each non-trivial $\gamma \in \Gamma$, there exists a homomorphism $\psi\colon \Gamma \to Q$ such that $\psi(\gamma) \neq 1$ and $Q \in \mathscr{C}$. Assuming that $\mathscr{C}$ is closed under subgroups and products, we have a filter base $\mathscr{I}_{\mathscr{C}} \subset \mathscr{I}_\Gamma$ comprised of $\Delta \in \mathscr{I}_\Gamma$ such that $\Gamma/\Delta \in \mathscr{C}$. When $\mathscr{C} = \mathscr{C}_{fin}$, if Γ is residually $\mathscr{C}_{fin}$, we simple say that Γ is **residually finite**.

Lemma 2.13. *Let Γ be a group and $\mathscr{C}$ a class of groups that is closed under products and subgroups.*

(a) Γ is residually $\mathscr{C}$ if and only if $\varphi_{\mathscr{I}_{\mathscr{C}}}$ is injective where $\varphi_{\mathscr{I}_{\mathscr{C}}}\colon \Gamma \to \Gamma_{\mathscr{I}_{\mathscr{C}}}$ is the unique continuous homomorphism to the completion associated to $\mathscr{I}_{\mathscr{C}}$.

(b) Γ is residually $\mathscr{C}$ if and only if Γ is Hausdorff in the topology $\mathscr{T}_{\mathscr{I}_{\mathscr{C}}}$.

Proof. Both (a) and (b) are straightforward applications of Proposition 2.7 (c). ♠

Given a commutative ring R with identity, the collection of ideals $\mathscr{I}_R$ of I is partially ordered under reverse inclusion. Given a filter base $\mathscr{I} \subset \mathscr{I}_R$, we have an inverse system of rings $(R/\mathfrak{a}, \varphi_{\mathfrak{a}_1\mathfrak{a}_2})$. We call the inverse limit $(R_{\mathscr{I}}, \varphi_{\mathfrak{a}})$ the **completion of R with respect to $\mathscr{I}$**. Let $\mathscr{I}_R^{cf} \subset \mathscr{I}_R$ be the filter of ideals $\mathfrak{a} \subset R$ such that $R/\mathfrak{a}$ is finite. The completion of R with respect to $\mathscr{I}_R^{cf}$ is called the **profinite ring completion of** R and will be denoted by $\widehat{R}$. This completion of R satisfies an analogous universal property among the completions associated to filter bases $\mathscr{I} \subset \mathscr{I}_R^{cf}$ as we saw above for $\widehat{\Gamma}$. Specifically, if $R_{\mathscr{I}}$ is the profinite ring completion of R with respect to $\mathscr{I}$, there is a continuous surjective ring homomorphism $\pi_{\mathscr{I}}\colon \widehat{R} \to R_{\mathscr{I}}$.

Given a commutative ring R with identity, we have the group $\mathrm{GL}(n,R)$ of invertible n by n matrices with coefficients in R. For each $\mathfrak{a} \in \mathscr{I}_R$, we have a homomorphism $r_{\mathfrak{a}}\colon \mathrm{GL}(n,R) \to \mathrm{GL}(n,R/\mathfrak{a})$ given by applying the ring homomorphism $R \to R/\mathfrak{a}$ to each coefficient. We call this homomorphism the **reduction homomorphism associated to** $\mathfrak{a}$. When $\mathfrak{a} \in \mathscr{I}_R^{cf}$, the group

$\mathrm{GL}(n,R)$ is finite since $R/\mathfrak{a}$ is finite. If $\mathfrak{a}_1 \le \mathfrak{a}_2$, then we have a surjective ring homomorphism $R/\mathfrak{a}_2 \to R/\mathfrak{a}_1$. This ring homomorphism applied to the coefficients yields a surjective group homomorphism $\varphi_{\mathfrak{a}_1\mathfrak{a}_2}\colon \mathrm{GL}(n,R/\mathfrak{a}_2) \to \mathrm{GL}(n,R/\mathfrak{a}_1)$. In total, we get an inverse system of finite groups $(\mathrm{GL}(n,R/\mathfrak{a}),\varphi_{\mathfrak{a}_1\mathfrak{a}_2})$ and an associated inverse limit $\varprojlim(\mathrm{GL}(n,R/\mathfrak{a}),\varphi_{\mathfrak{a}_1\mathfrak{a}_2})$.

Exercise 4. Prove that $\varprojlim(\mathrm{GL}(n,R/\mathfrak{a}),\varphi_{\mathfrak{a}_1\mathfrak{a}_2}) \cong \mathrm{GL}(n,\widehat{R})$. More generally, if $\mathscr{I} \subset \mathscr{I}_R^{cf}$ is a filter base, we can associate to $\mathscr{I}$ an inverse system of finite groups given as above by $\mathrm{GL}(n,R/\mathfrak{a})$ for $\mathfrak{a} \in \mathscr{I}$. Prove that $\varprojlim_{\mathfrak{a}\in\mathscr{I}} \mathrm{GL}(n,R/\mathfrak{a}) \cong \mathrm{GL}(n,R_{\mathscr{I}})$.

Given a group Γ, a commutative ring R with identity, a homomorphism $\rho\colon \Gamma \to \mathrm{GL}(n,R)$, and a filter base $\mathscr{I} \subset \mathscr{I}_R$, for each $\mathfrak{a} \in \mathscr{I}$, we have $\rho_{\mathfrak{a}}\colon \Gamma \to \mathrm{GL}(n,R/\mathfrak{a})$ via $\rho_{\mathfrak{a}} = r_{\mathfrak{a}} \circ \rho$. As these maps are compatible with the inverse system, we obtain $\rho_{\mathscr{I}}\colon \Gamma \to \mathrm{GL}(n,R_{\mathscr{I}})$. If $\mathscr{I} \subset \mathscr{I}_R^{cf}$, then $\mathscr{I}_\rho = \{\ker \rho_{\mathfrak{a}}\}$ is a filter subbase of $\mathscr{I}_\Gamma$.

Proposition 2.14. *Let Γ be a group, R a commutative ring with identity, a homomorphism $\rho\colon \Gamma \to \mathrm{GL}(n,R)$, and a filter base $\mathscr{I} \subset \mathscr{I}_R$. Then $\overline{\rho_{\mathscr{I}}(\Gamma)} \cong \Gamma_{\mathscr{I}_\rho}$.*

Proof. This follows by definition of $\mathscr{I}_\rho$. ♠

Given a homomorphism $\rho\colon \Gamma \to \mathrm{GL}(n,R)$ and a filter base $\mathscr{I} \subset \mathscr{I}_R$, we call $\Gamma_{\mathscr{I}_\rho}$ the completion associated to $(\rho,\mathscr{I})$. When $\mathscr{I} = \mathscr{I}_R^{cf}$, we call $\Gamma_{\mathscr{I}_\rho}$ the **profinite completion associated to** ρ.

We say that R is **residually finite** if for each non-zero $r \in R$, there exists $\mathfrak{a} \in \mathscr{I}_R^{cf}$ such that $r \neq 0$ mod $\mathfrak{a}$. As in the setting of groups, R is residually finite if and only if the ring homomorphism $\widehat{\varphi}\colon R \to \widehat{R}$ is injective.

Lemma 2.15 (Mal'cev)**.** *Let G be a group and R be a residually finite, commutative ring with identity. If there exist an injective representation $\rho\colon \Gamma \to \mathrm{GL}(n,R)$, then Γ is residually finite.*

The proof is left to the reader and can be done with the first two exercises below.

Exercise 5. If R is a residually finite commutative ring with identity, prove that $\mathrm{GL}(n,R)$ is residually finite. [Hint: consider $A - \mathrm{I}_n$]

Exercise 6. If $H \subset G$ is a subgroup of a residually finite group G, then H is residually finite.

Exercise 7. If Γ is a finitely generated group that is residually finite, then $\mathrm{Aut}(\Gamma)$, the group of automorphisms of Γ, is residually finite. [Hint: A filter base of characteristic subgroups of Γ gives rise to a filter base of normal subgroups of $\mathrm{Aut}(\Gamma)$]

Exercise 8. Let $\mathscr{I} \subset \mathscr{I}_\Gamma$ be a filter base. Prove that a normal subgroup $\Lambda \lhd \Gamma$ is closed in $\mathscr{T}_{\mathscr{I}}$ if and only if Γ/Λ is Hausdorff in the quotient topology induced by $\mathscr{T}_{\mathscr{I}}$.

Exercise 9. Prove that $\mathbf{Z}$ is residually finite (viewed as an additive abelian group or a commutative ring).

2.3 Lecture 6. *The Profinite Completion of* $\mathbf{Z}$

Today, we will determine the profinite completion of $\mathbf{Z}$ as an additive group or ring. There are many ways to compute $\widehat{\mathbf{Z}}$. To start, $\mathbf{Z}$ is a cyclic group generated by 1 and any homomorphism $\varphi\colon \mathbf{Z} \to G$ is determined completely by $\varphi(1)$. Moreover, for any non-injective homomorphism $\mathbf{Z} \to G$, the image is a cyclic group of order $m \in \mathbf{N}$. Conversely, for each integer m, there exists a surjective homomorphism $\pi_{m,r}\colon \mathbf{Z} \to C_m$ given by $\pi_{m,r}(1) = r$ where C_m denotes the cyclic group of order m and $r \in C_m$ is a generator. Note that for any two $r_1, r_2 \in C_m$, $\ker \pi_{m,r_1} = \ker \pi_{m,r_2}$. In particular, for each $m \in \mathbf{N}$, there is precisely one normal subgroup of $\mathbf{Z}$ of index m. This subgroup is given by $m\mathbf{Z}$ and is the subgroup of integers that are divisible by m. We often refer to this homomorphism as **reduction modulo** m and write $\mathbf{Z}/m\mathbf{Z}$ for C_m.

We have the partial order of $\mathbf{N}$ given by $m \leq_d n$ if and only if m divides n. When $m \leq_d n$, we have a homomorphism $r_{mn}\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ given by $r_{mn}(a + n\mathbf{Z}) = a + m\mathbf{Z}$. It is clear that $\mathbf{N}$ is a directed set with this partial ordering and so $(\mathbf{Z}/m\mathbf{Z}, r_{mn})$ is the inverse system of all finite quotient groups of $\mathbf{Z}$. That is, $\widehat{\mathbf{Z}} \cong \varprojlim(\mathbf{Z}/m\mathbf{Z}, r_{mn})$.

For each prime $p \in \mathbf{N}$, we have the inverse system $(\mathbf{Z}/p^i\mathbf{Z}, \varphi_{ij})$ and associated inverse limit $G_p = \varprojlim \mathbf{Z}/p^i\mathbf{Z}$. By the Fundamental Theorem of Arithmetic, $m = \prod_{i=1}^r p_i^{t_i}$ for a unique set of primes $p_1, \dots, p_r$ and powers $t_1, \dots, t_r \in \mathbf{N}$. Hence, by the Chinese Remainder Theorem, we know that $C_m = \prod_{i=1}^r C_{p_i^{t_i}}$. It follows then that $\widehat{\mathbf{Z}} = \prod_p G_p$. Moreover, for each prime p, the group G_p is the pro–p completion of $\mathbf{Z}$.

We now analyze the groups G_p. For each prime p, we let $\mathscr{I}_p = \left\{p^i\mathbf{Z}\right\}_{i\in\mathbf{N}}$. Since $p^{i+1}\mathbf{Z} \subset p^i\mathbf{Z}$, the set $\mathscr{I}_p \subset \mathscr{I}_{\mathbf{Z}}$ is a filter and we have $\widehat{\varphi_{\mathscr{I}_p}}\colon \mathbf{Z} \to G_p$. Since $\bigcap_i p^i\mathbf{Z} = \{0\}$, we also see that $\widehat{\varphi_{\mathscr{I}_p}}$ is injective.

There are a few different ways to view what G_p is. One standard approach is to prove that G_p is the group/ring of p–adic integers $\mathbf{Z}_p$. Technically speaking, we will take two versions of this. The first will be to equip $\mathbf{Z}$ with a metric and then take the completion. This view in the context of $\mathbf{Z}$ is to use the p–adic valuation and define a metric on $\mathbf{Z}$ via this valuation. However, there is a broader context in which one can take this approach and so we will do this for a general finitely generated group. The second approach is to introduce a concrete model for G_p and so a concrete object to study $G_p = \mathbf{Z}_p$. This method is briefly discussed after the discussion below on valuations and pseudometrics associated to filters.

Valuations and Pseudometrics Associated to Filters. Given a finitely generated group Γ, the set of finite index, normal subgroups $\mathscr{I}_\Gamma$ is countable. In fact, for each $m \in \mathbf{N}$, the subset of finite index, normal subgroups of index at most m, which we denote by $\mathscr{I}_\Gamma^m$, is finite. In what is written below, we can drop the assumption that Γ is finitely generated but must assume that the initial filter $\mathscr{I} \subset \mathscr{I}_\Gamma$ further satisfy that the set $\{\Delta \in \mathscr{I} \ : \ [\Gamma : \Delta] \leq m\}$ be finite for all $m \in \mathbf{N}$. We instead restrict ourselves to the setting when Γ is finitely generated.

Given a filter $\mathscr{I} \subset \mathscr{I}_\Gamma$, we define $\mathscr{I}^m = \mathscr{I} \cap \mathscr{I}_\Gamma^m$ and let m_j be the sequence of integers given by $\mathscr{I}^{m_j - 1} \neq \mathscr{I}^{m_j}$. We define $\Delta_{\mathscr{I},j} = \bigcap_{\Delta \in \mathscr{I}^{m_j}} \Delta$ for $j > 0$ and $\Delta_{\mathscr{I},0} = \Gamma$. Note that $\Delta_{\mathscr{I},j} \in \mathscr{I}$ and $\Delta_{\mathscr{I},j+1} \subset \Delta_{\mathscr{I},j}$ hold for all $j \in \mathbf{N}$. We set $K_{\mathscr{I}} = \bigcap_{j=0}^{\infty} \Delta_{\mathscr{I},j}$. Given $\gamma \in \Gamma$, we define $\nu_{\mathscr{I}}(\gamma) = \max\left\{ j \in \mathbf{N} \cup \{0, \infty\} \ : \ \gamma \in \Delta_{\mathscr{I},j} \right\}$ and note that $\nu_{\mathscr{I}}(\gamma) = \infty$ precisely when $\gamma \in K_{\mathscr{I}}$. Fixing a real number $\alpha > 1$, we define $|\gamma|_{\mathscr{I}} = \alpha^{-\nu_{\mathscr{I}}(\gamma)}$ and $d_{\mathscr{I}}(\gamma, \eta) = \left|\gamma\eta^{-1}\right|_{\mathscr{I}}$.

Exercise 10. Prove that $|\cdot|_{\mathscr{I}} : (\Gamma, \mathscr{T}_{\mathscr{I}}) \to \mathbf{R}$ is continuous.

The function $d_{\mathscr{I}}$ is a pseudometric, and we denote the pseudometric completion of $(\Gamma, d_{\mathscr{I}})$ by $\mathrm{C}_{\mathscr{I}}(\Gamma)$. Recall that this completion is done via Cauchy sequences. In our present setting, a sequence $\{\gamma_i\} \subset \Gamma$ is **Cauchy** if and only if for each $j \in \mathbf{N}$, there exists $n \in \mathbf{N}$ such that $\nu_{\mathscr{I}}(\gamma_{m_1}\gamma_{m_2}^{-1}) \geq j$ for all $m_1, m_2 \geq n$. Alternatively, for each $\varepsilon > 0$, there exists $n_\varepsilon \in \mathbf{N}$ such that if $n, m \geq n_\varepsilon$, then $d_{\mathscr{I}}(\gamma_m, \gamma_n) < \varepsilon$. Returning to the task at hand, by construction of the completion $\mathrm{C}_{\mathscr{I}}(\Gamma)$, we have a continuous function $\overline{\psi_{\mathscr{I}}} \colon (\Gamma, \mathscr{T}_{\mathscr{I}}) \to \mathrm{C}_{\mathscr{I}}(\Gamma)$. For this map, we identify an element $\gamma \in \Gamma$ with the equivalence class of Cauchy sequences in Γ that contains the constant sequence γ. Since $d_{\mathscr{I}}(\gamma, \eta) = 0$ if and only if $\gamma\eta^{-1} \in K_{\mathscr{I}}$, $\ker \overline{\psi_{\mathscr{I}}} = K_{\mathscr{I}}$; we say that $\mathscr{I}$ is **cofinal** if $K_\Gamma = \{1\}$.

Corollary 2.16. *Let Γ be a finitely generated group, $\mathscr{I} \subset \mathscr{I}_\Gamma$ a filter, $\mathrm{C}_{\mathscr{I}}(\Gamma)$ the associated pseudometric completion of Γ with respect to the pseudometric $d_{\mathscr{I}}$. If $\mathscr{I}$ is cofinal, then $d_{\mathscr{I}}$ is a metric and $\overline{\psi_{\mathscr{I}}}$ is injective.*

We also have a pseudometric on the profinite completion $\Gamma_{\mathscr{I}}$ of Γ with respect to $\mathscr{I}$. For each $\Delta \in \mathscr{I}$, we have a continuous homomorphism $\varphi_\Delta \colon \Gamma_{\mathscr{I}} \to \Gamma/\Delta$. We see that $\ker \varphi_\Delta = \overline{\varphi_{\mathscr{I}}(\Delta)}$ where the bar denotes the closure in $\Gamma_{\mathscr{I}}$. We hence take $\Lambda_{\mathscr{I},j} = \overline{\varphi_{\mathscr{I}}(\Delta_{\mathscr{I},j})}$ and define $\widehat{\nu_{\mathscr{I}}} \colon \Gamma_{\mathscr{I}} \to \mathbf{N} \cup \{0, \infty\}$ by $\widehat{\nu_{\mathscr{I}}}(\gamma) = \max\left\{ j \in \mathbf{N} \cup \{0, \infty\} \ : \ \gamma \in \Lambda_{\mathscr{I},j} \right\}$. Taking $\alpha > 0$ as above, we set $|\gamma|_{\mathscr{I}} = \alpha^{-\widehat{\nu_{\mathscr{I}}(\gamma)}}$ and $\widehat{d_{\mathscr{I}}}(\gamma, \eta) = \left|\gamma\eta^{-1}\right|_{\mathscr{I}}$.

Lemma 2.17. *Let Γ be a finitely generated group, $\mathscr{I} \subset \mathscr{I}_\Gamma$ a filter, $\Gamma_{\mathscr{I}}$ the profinite completion associated to $\mathscr{I}$, and $d_{\mathscr{I}}, \widehat{d_{\mathscr{I}}}$ the pseudometrics on $\Gamma, \Gamma_{\mathscr{I}}$ associated to $\mathscr{I}$. Then $d_{\mathscr{I}}(\gamma, \eta) = \widehat{d_{\mathscr{I}}}(\varphi_{\mathscr{I}}(\gamma), \varphi_{\mathscr{I}}(\eta))$.*

Proof. This follows immediate from the definitions of $d_{\mathscr{I}}$, $\widehat{d_{\mathscr{I}}}$, and the commutativity of the diagram

$$\begin{tikzcd}
\Gamma \arrow[rr, "\varphi_{\mathscr{I}}"] \arrow[dr, "\psi_\Delta"'] & & \Gamma_{\mathscr{I}} \arrow[dl, "\varphi_\Delta"] \\
& \Gamma/\Delta &
\end{tikzcd}$$

♠

Since $\widehat{d_{\mathscr{I}}}$ is continuous on $\Gamma_{\mathscr{I}} \times \Gamma_{\mathscr{I}}$ and $\Gamma_{\mathscr{I}}$ is compact, it follows that $(\Gamma_{\mathscr{I}}, \widehat{d_{\mathscr{I}}})$ is complete. For that discussion, we obtain the following result.

Corollary 2.18. *Let Γ be a finitely generated group, $\mathscr{I} \subset \mathscr{I}_\Gamma$ a filter, $\Gamma_{\mathscr{I}}$ the profinite completion associated to $\mathscr{I}$, and $\mathrm{C}_{\mathscr{I}}(\Gamma)$ the pseudometric completion of Γ with respect to the pseudometric $d_{\mathscr{I}}$. Then $\Gamma_{\mathscr{I}} \cong \mathrm{C}_{\mathscr{I}}(\Gamma)$ as topological groups.*

Returning to the profinite groups G_p with the above discussion in mind. For each prime $p \in \mathbf{N}$, we have the filter $\mathscr{I}_p = \left\{\mathbf{Z}/p^j\mathbf{Z}\right\}_{j=0}^{\infty}$ on $\mathbf{Z}$. We define

$$\nu_p(m) = \max\left\{ j \in \mathbf{N} \cup \{0,\infty\} \ : \ m \in p^j\mathbf{Z} \right\},$$

$|m|_p = p^{-\nu_p(m)}$, and $d_p(m,n) = |m-n|_p$. Since $\mathscr{I}_p$ is cofinal, we see that d_p is a metric and G_p is isomorphic to the metric completion of $(\mathbf{Z}, d_p)$.

Corollary 2.19. *For each prime $p \in \mathbf{N}$, we have $\varprojlim \mathbf{Z}/p^j\mathbf{Z} \cong \mathrm{C}_{\mathscr{I}_p}(\mathbf{Z})$.*

Concretely, we define the ***p*–adic integers** $\mathbf{Z}_p$ to be the ring of formal series $\sum_{j \geq 0} \alpha_j p^j$ where $\alpha_j \in \mathbf{Z}$ and $0 \leq \alpha_j \leq p$. For each $i_0 \in \mathbf{N}$, we have $\varphi_{i_0} \colon \mathbf{Z}_p \to \mathbf{Z}/p^{i_0}\mathbf{Z}$ given by

$$\psi_0\left(\sum_{j\geq 0} \alpha_j p^j\right) = \sum_{j=0}^{i_0-1} \alpha_j p^j + p^{i_0}\mathbf{Z}.$$

Since the homomorphisms ψ_i are compatible with the inverse system $(\mathbf{Z}/p^i\mathbf{Z}, r_{p^i p^j})$, we have a homomorphism $\theta \colon \mathbf{Z}_p \to G_p$. It is straightforward to check that θ is a bijection.

We finish with a few basic exercises.

Exercise 11. Prove that $\mathrm{C}_{\mathscr{I}}(\Gamma)$ is a compact, Hausdorff topological group.

Exercise 12. Let $(X_i,\varphi_i)_{\mathscr{I}},(Y_j,\psi_j)_{\mathscr{J}}$ be inverse systems of finite sets with inverse limits X,Y. Prove that $X\times Y\cong \varprojlim(X_i\times Y_j,\varphi_i\times\psi_j)_{\mathscr{I}\times\mathscr{J}}$.

Exercise 13. Let G be a profinite group and H a closed subgroup of G. Prove that H is the inverse limit of the open subgroup K of G such that $H\subset K$.

Exercise 14. Let Γ be a residually finite group viewed as a subgroup of the profinite completion $\widehat{\Gamma}$ of Γ. Prove the following are equivalent for $\gamma,\eta\in\Gamma$:

(a) γ,η are conjugate in $\widehat{\Gamma}$.

(b) For each $\Delta\in\mathscr{I}_\Gamma$, the images of γ,η in Γ/Δ are conjugate in Γ/Δ.

A group Γ is called **conjugacy separable** if for each pair $\gamma,\eta\in\Gamma$, we have that γ,η are conjugate in Γ if and only if γ,η are conjugate in $\widehat{\Gamma}$.

Exercise 15. Let Γ be a group and let X_Γ denote the set of conjugacy classes equipped with the quotient topology coming from the profinite topology on Γ. Prove that if Γ is conjugacy separable, then Γ is residually finite. Prove that Γ is conjugacy separable if and only if X_Γ is Hausdorff.

Exercise 16. Given a filter $\mathscr{I}\subset\mathscr{I}_{\mathbf{Z}}$, we denote the maps above in this setting by $\nu_{\mathscr{I}}$, $|\cdot|_{\mathscr{I}}$, $d_{\mathscr{I}}$, and $\mathrm{C}_{\mathscr{I}}(\mathbf{Z})$. From above, we know that $\mathrm{C}_{\mathscr{I}}(\mathbf{Z})\cong\mathbf{Z}_{\mathscr{I}}$ where $\mathbf{Z}_{\mathscr{I}}$ is the profinite completion of $\mathbf{Z}$ associated to $\mathscr{I}$. Determine $\mathbf{Z}_{\mathscr{I}}$ for the filters below:

(a) Let $\mathscr{I}=\{m_j\mathbf{Z}\}_{j=0}^{\infty}$ where $m_j=\mathrm{lcm}(1,\dots,j+1)$.

(b) Let $\mathscr{I}=\{m_j\mathbf{Z}\}_{j=0}^{\infty}$ where $m_j=\prod_{i=0}^{j}p_j$ where $p_0=1$ and p_i is the ith prime.

(c) Let $\mathscr{I}=\{p^jq^j\mathbf{Z}\}_{j=0}^{\infty}$.

(d) Let $\mathscr{I}=\{\mathbf{Z}\}\cup\left\{q_1^jq_2^{j^2}\dots q_r^{j^r}\mathbf{Z}\right\}_{j=1}^{\infty}$ where $q_1,\dots,q_r$ are fixed and relatively prime.

Exercise 17. Let $\mathscr{I}_1=\{\Delta_{1,j}\},\mathscr{I}_2=\{\Delta_{2,j}\}\subset\mathscr{I}_\Gamma$ be filters such that

(i) $\Delta_{i,j+1}\subset\Delta_{i,j}$ for all $i=1,2$ and $j\in\mathbf{N}$.

(ii) For all $i,j\in\mathbf{N}$, $\Gamma/(\Delta_{1,i}\cap\Delta_{2,j})\cong(\Gamma/\Delta_{1,i})\times\left(\Gamma/\Delta_{2,j}\right)$.

Let $\mathscr{F}\subset\mathscr{I}_\Gamma$ be the span of $\mathscr{I}_1\cup\mathscr{I}_2$. Prove that

$$\varprojlim_{\mathscr{F}}(\Gamma/\Delta)\cong\left(\varprojlim_{\mathscr{I}_1}(\Gamma/\Delta_{1,j})\right)\times\left(\varprojlim_{\mathscr{I}_2}(\Gamma/\Delta_{2,j})\right).$$

2.4 Lecture 7. *Free Groups and Presentations*

Given a set X, the **free group on the set X** is the unique group (up to isomorphism) $F(X)$ with $X \subset F(X)$ and satisfying the following universal mapping property: if $f\colon X \to G$ is any function where G is a group, then there exists a unique homomorphism $\varphi_f\colon F(X) \to G$ such that the restriction of φ_f to X is f. The existence of such a group can be done constructively in the same spirit as the construction of a vector space or free abelian group associated to a set. We briefly outline the approach.

We start by forming a set $\mathscr{A} = \{x\}_{x\in X} \cup \{x^{-1}\}_{x\in X}$ that we will call an **alphabet**. A **word** in the alphabet $\mathscr{A}$ is a finite ordered subset $w \subset \mathscr{A}$. By definition, $w = \left\{x_1^{\varepsilon_1}, \dots, x_m^{\varepsilon_m}\right\}$ where $x_i \in X$ and $\varepsilon_i = \pm 1$. We can combine words $w_1 = \left\{x_1^{\varepsilon_1}, \dots, x_m^{\varepsilon_m}\right\}$ and $w_2 = \left\{y_1^{\varepsilon_1'}, \dots, y_n^{\varepsilon_n'}\right\}$ to form a new word $w_1 w_2 \subset \mathscr{A}$ given by

$$w_1 w_2 = \left\{x_1^{\varepsilon_1}, \dots, x_m^{\varepsilon_m}, y_1^{\varepsilon_1'}, \dots, y_n^{\varepsilon_n'}\right\}.$$

We say that a word $w = \left\{x_i^{\varepsilon_i}\right\}_{i=1}^m$ is **reducible** if there exists an index $i \in \{1, \dots, n-1\}$ such that $x_i = x_{i+1}$ and $\varepsilon_i = -\varepsilon_{i+1}$, and we say w is **irreducible** otherwise. Given a reducible word $w \subset \mathscr{A}$ with $i \in \{1, \dots, n-1\}$ such that $x_i = x_{i+1}$ and $\varepsilon_i = -\varepsilon_{i+1}$, we can perform a reduction operation on w. Formally, we define a new word

$$\mathrm{R}_i(w) = \left\{x_1^{\varepsilon_1}, \dots, x_{i-1}^{\varepsilon_{i-1}}, x_{i+2}^{\varepsilon_{i+2}}, \dots, x_n^{\varepsilon_n}\right\}.$$

After applying finitely many reduction operations $R_{i_1}, \dots, R_{i_m}$ on the reducible word w, we obtain a unique irreducible word w_{irr}. We define $\mathscr{W}_X$ to be the set of irreducible words in the alphabet $\mathscr{A}$. We have a binary operation $*\colon \mathscr{W}_X \times \mathscr{W}_X \to \mathscr{W}_X$ given by $w_1 * w_2 = (w_1 w_2)_{irr}$. We also have an involution $\iota\colon \mathscr{W}_X \to \mathscr{W}_X$ given by

$$\iota(w) = \iota\left(\left\{x_i^{\varepsilon_i}\right\}_{i=1}^n\right) = \left\{x_{n-i+1}^{-\varepsilon_{n-i+1}}\right\}_{i=1}^n.$$

Setting $1_{\mathscr{W}_X} = \emptyset$, we see that $(\mathscr{W}_X, *, \iota, 1_{\mathscr{W}_X})$ is a group with multiplication operation $*$, inverse operation ι, and identity $1_{\mathscr{W}_X}$. Given any group G and any function $f\colon X \to G$, we define $\varphi_f\colon \mathscr{W}_X \to G$ by

$$\varphi_f(w) = \prod_{i=1}^n f(x_i)^{\varepsilon_i}, \quad w = \left\{x_i^{\varepsilon_i}\right\}_{i=1}^n.$$

It is straightforward to check that φ_f is a homomorphism with $f(x) = \varphi_f(x)$ for all $x \in X$.

Exercise 18. Prove that φ_f is unique.

Exercise 19. Prove $F(X) \cong F(Y)$ if and only if there exists a bijective function $X \to Y$.

Lemma 2.20. *If Γ is a group, then there exists a free group F and a surjective homomorphism $F \to \Gamma$.*

Proof. Take $X = \Gamma$, $F = F(X)$, $f\colon X \to \Gamma$ to be the identity, and apply the universal mapping property. ♠

Exercise 20. Prove that $F(\Gamma)/[F(\Gamma), F(\Gamma)] \cong \mathbf{Z}[\Gamma]$.

Given a group Γ, we know that there exists a set X and a surjective homomorphism $\Psi_X\colon F(X) \to \Gamma$. Since $\ker \Psi_X$ is a subgroup of the free group $F(X)$, by the Nielsen–Schreier Theorem it is a free group as well. In particular, there exists a set Y such that $\ker \Psi_X \cong F(Y)$. If we pick an isomorphism $F(Y) \to \ker \Psi_X$, we can identify $Y \subset F(Y)$ with a subset R_X of $\ker \Psi_X$. It follows that R_X generates $\ker \Psi_X$. We call any subset R of $\ker \Psi_X$ a **complete set of relations** if the set $\left\{ w^{-1} r w \;:\; r \in R,\ w \in F(X) \right\}$ generates $\ker \Psi_X$.

If Γ is a group with a surjective homomorphism $\Psi_X\colon F(X) \to \Gamma$ where R is a complete set of relations, then we call (X, R) a **presentation of Γ**. If X is finite, we say that the presentation (X, R) is **finitely generated**. If both X and R are finite, we say that the presentation (X, R) is **finite**. We say that a group Γ is **finitely generated**.if Γ admits a finitely generated presentations. We say that Γ is **finitely presentable** if Γ admits a finite presentation.

If X is a finite set with $|X| = r$, we denote $F(X)$ simply by F_r and call F_r the **rank r free group**. For a finitely generated group Γ, we define the **rank of Γ** to be minimum of $|X|$ over all finitely generated presentations (X, R) of Γ. We denote the rank of Γ by $\mathrm{Rank}(\Gamma)$.

Exercise 21. Prove that $\mathrm{Rank}(F_r) = r$. [Hint: Prove that if $|Y| < |X|$, then there cannot be a surjective homomorphism of $F(Y) \to F(X)$]

Lemma 2.21. *Let $F(X)$ be a free group on a set X. Then $F(X)$ is residually finite.*

Proof. We first reduce to the case when X is finite. Given a non-trivial irreducible word $w \in \mathscr{W}_X$, we know that $w = \left\{ x_1^{\varepsilon_1}, \dots, x_n^{\varepsilon_n} \right\}$ with $n \geq 1$. Set X_w be the subset of X of distinct letters x_i that appear in w. We have the function $f_w\colon X \to \mathscr{W}_{X_w}$ given by

$$f_w(x) = \begin{cases} \emptyset, & x \notin X_w, \\ x, & x \in X_w. \end{cases} .$$

By the universal mapping property, there exists a homomorphism $\varphi_{f_w}\colon F(X) \to F(X_w)$ with $\varphi_f(w) \neq 1_{\mathscr{W}_{X_w}}$. We now have a non-trivial, irreducible word $\varphi_{f_w}(w)$ in a finite rank free group $F(X_w)$.

We now complete the proof in the case when X is finite; the proof follows this one. As above, we have a non-empty irreducible word $w \in F(X)$ where $X = \{x_1, \dots, x_r\}$ and $w = \left\{x_{i_1}^{\varepsilon_1}, \dots, x_{i_n}^{\varepsilon_n}\right\}$ where $x_{i_j} \in X$ and $\varepsilon_i \in \{\pm 1\}$. We require a homomorphism $\psi\colon F(X) \to G$ with $|G| < \infty$ and $\psi(w) \neq 1$. To do this, we will define a function $X \to \mathrm{Sym}(n+1)$ where $\mathrm{Sym}(n+1)$ is the **symmetric group on $n+1$ points**. We seek permutations $\sigma_1, \dots, \sigma_r \in \mathrm{Sym}(n+1)$ such that $\sigma_{i_1}^{\varepsilon_1} \dots \sigma_{i_n}^{\varepsilon_n} \neq 1$. We first define the functions σ_j on subsets on $\{1, \dots, n+1\}$ by $\sigma_{i_j}^{\varepsilon_j}(j) = j+1$. From this, we have subsets $S_j \subset \{1, \dots, n+1\}$ where σ_j is defined and injective. We can extend each σ_j from S_j to $\{1, \dots, n+1\}$ to obtain bijective functions $\sigma_j \in \mathrm{Sym}(n+1)$; one could use Hall's Marriage/Matching Theorem, for instance, to prove that such extensions exists. By definition $(\sigma_{i_1}^{\varepsilon_1} \dots \sigma_{i_n}^{\varepsilon_n})(1) = n+1$, and so $\sigma_{i_1}^{\varepsilon_1} \dots \sigma_{i_n}^{\varepsilon_n} \neq 1$. Formally, we define $f\colon X \to \mathrm{Sym}(n+1)$ by $f(x_i) = \sigma_i$ and so by the universal mapping property for free groups, we have a homomorphism $\psi\colon F(X) \to \mathrm{Sym}(n+1)$ which extends f. By construction, $\psi(w) = \prod_{j=1}^n \sigma_{i_j}^{\varepsilon_j} \neq 1$ and so $F(X)$ is residually finite. ♠

Recall that if F_r is a rank r free group and $\Delta < F_r$ is a finite index subgroup of index k, then Δ is a free group of rank $1 + k(r-1)$ by Nielsen–Schreier formula. In particular, if $r = 2$, we see that if $\Delta < F_2$ has index k, then $\Delta \cong F_{k+1}$. Picking free generators x, y for F_2, by the universal mapping property, we have a surjective homomorphism $F_2 \to \mathbf{Z}$ induced by $x, y \mapsto 1$. For each positive integer k, we have the finite index subgroup $k\mathbf{Z}$ of $\mathbf{Z}$. The preimage of $k\mathbf{Z}$ under the surjective homomorphism $F_2 \to \mathbf{Z}$ gives an index k subgroup of F_2. In total, this discussion yields the following well-known fact.

Lemma 2.22. *For every $k \in \mathbf{N}$, there exists a free subgroup $F_k < F_2$.*

For a finite group Q, $\mathrm{Rank}(Q) \leq |Q| - 1$, and so there exists a finite index, normal subgroup Δ of F_2 and a surjective homomorphism $\psi\colon \Delta \to Q$; the index can be taken to be $\mathrm{Rank}(Q) - 1$. The subgroup $\ker \psi$ is a normal subgroup of Δ but need not be a normal subgroup of F_2. Since Δ is a normal subgroup, we have a homomorphism $\tau\colon \Gamma \to \mathrm{Aut}(\Delta)$ given by $\tau(\gamma)(\delta) = \gamma^{-1}\delta\gamma$. Fixing a complete set of Δ–coset representatives $\gamma_1, \dots, \gamma_t$, where $t = [F_2 : \Delta]$, we define $\Delta_Q = \bigcap_{j=1}^t \ker(\psi \circ \tau(\gamma_j))$. The subgroup Δ_Q is normal in F_2 and so we have the quotient $G = F_2/\Delta_Q$. Note that $\Delta_Q < \Delta$ by definition and so $\Delta/\Delta_Q < F_2/\Delta_Q$. By construction $\psi_{\Delta_Q}\colon \Delta \to \Delta/\Delta_Q$ is given by (γ_1 represents the trivial coset)

$$\psi \times (\psi \circ \tau(\gamma_2)) \times \cdots \times (\psi \circ \tau(\gamma_t))\colon \Delta \longrightarrow \underbrace{Q \times Q \times \cdots \times Q}_{t \text{ times}}.$$

In particular, F_2/Δ_Q contains the subgroup Δ/Δ_Q that projects onto Q. By definition, $\widehat{F_2} = \varprojlim_{\mathscr{I}_{F_2}} (F_2/\Lambda)$ where $\mathscr{I}_{F_2}$ is the filter of finite index, normal subgroups of F_2. By Proposition

1.19 (a), $\widehat{F_2}$ is a closed subgroup in the product group $\prod_{\mathscr{I}_{F_2}} F_2/\Lambda$. Inside this product, we have the factor F_2/Δ_Q and the restriction of the projection map π_{Δ_Q} to $\widehat{F_2}$ is onto. The factor group contains a subgroup of Q^t that projections onto Q. In particular, for any finite group Q, there exists a surjective homomorphism $\widehat{F_2} \to H$ is finite and $Q < H$.

From the above discussion, we see that $\widehat{F_2}$ is a fairly big group in a certain sense. By definition of rank, any finite group Q with $\mathrm{Rank}(Q) \leq 2$ admits a surjective homomorphism $F_2 \to Q$. Each such group will appear as a factor in $\prod_{\mathscr{I}_{F_2}} F_2/\Lambda$. It turns out every finite simple group has rank at most two. So groups like $\mathrm{PSL}(n, \mathbf{F}_q)$, $\mathrm{Alt}(n)$ and the Monster group all occur as factors for $\widehat{F_2}$. In fact, we know that most pairs in a finite simple group generate (see here the references therein); the alternating group $\mathrm{Alt}(n)$ has $(n!)^2/4$ pairs.

Here is a cool result of Hall:

Proposition 2.23. *Let G be a finite simple group and $\psi_i \colon F_r \to G$ be homomorphisms for $i = 1, 2$. Then $\psi_1 \times \psi_2$ is onto provided $\psi_2 \neq \varphi \circ \psi_1$ for some automorphism $\varphi \in \mathrm{Aut}(G)$.*

Exercise 22. Prove Proposition 2.23.

Consequently, these different homomorphisms largely give product-type structures in the sense that $F_r/(\ker\psi_1 \cap \ker\psi_2) \cong F_r/\ker\psi_1 \times F_r/\ker\psi_2$ when the above proposition is applicable. The finite quotients of F_r that are isomorphic to G that interact are the ones related by automorphisms. For finite groups of Lie type, these automorphisms are usually inner or induced by Galois automorphisms of finite fields. It should be noted that in terms of understanding the structure of $\widehat{F_2}$ or $\widehat{F_r}$, these complicated regions are of central importance.

Deficiency of a Presentation. Given a finite presentation (X, R) of a group Γ, we define the **deficiency of** (X, R) to be $\delta(X, R) = |X| - |R|$. We say that a presentation (X, R) is **balanced** if $\delta(X, R) = 0$ and **positive** if $\delta(X, R) > 0$. We prove a lemma of Lubotzky–Shalom [10]; see here.

Lemma 2.24. *If Γ is a group that admits a finite presentation (X, R) with $\delta(X, R) \geq 2$, then $Z(\widehat{\Gamma}) = 1$ where $Z(\cdot)$ denotes the center.*

Proof. We sketch the proof given in [10] which proceeds via contradiction. Assume $\gamma \in \widehat{\Gamma}$ is a non-trivial central element. Since $\widehat{\Gamma}$ is Hausdorff, there exists a open, normal subgroup Λ_0 such that $\gamma \notin \Lambda_0$. As Λ_0 is normal and $[\Lambda_0, \Lambda_0] < \Lambda_0$ is characteristic, $[\Lambda_0, \Lambda_0]$ is normal in $\widehat{\Gamma}$. The group $\widehat{\Gamma}$ acts on $\widehat{\Gamma}/[\Lambda_0, \Lambda_0]$ be conjugation. The action of Λ_0 is trivial and so we have an action of Γ/Λ_0. The subgroup $\Lambda_0/[\Lambda_0, \Lambda_0]$ is fixed by the action of $\widehat{\Gamma}/\Lambda_0$ and so we have an action of $\widehat{\Gamma}/\Lambda_0$ on $\Lambda_0/[\Lambda_0,\Lambda_0]$. This action is not faithful since $\gamma \in \Gamma - \Lambda_0$ is central. Now set $\Gamma_0 = \Gamma \cap \Lambda_0$. The profinite completion of the residually finite group $\Gamma/[\Gamma_0,\Gamma_0]$ is $\widehat{\Gamma}/[\Lambda_0,\Lambda_0]$. In particular, Γ/Γ_0 acts non-faithfully on $\Lambda_0/[\Lambda_0,\Lambda_0]$. However, this contradicts the following:

Theorem 2.25 (Jarden–Ritter)**.** *Let Γ_0,Γ be as above and let $Q = \Gamma/\Gamma_0$. Then there exists a normal subgroup $\Gamma_1 < \Gamma$ with $\Gamma_1 < \Gamma_0$, $\Gamma_0/\Gamma_1 \cong \mathbf{Z}^m$ for some m, and $(\mathbf{Q}Q)^{|X|-|R|-1}$ appears as a direct summand of the $\mathbf{Q}Q$–module $\Gamma_0/\Gamma_1 \otimes_{\mathbf{Z}} \mathbf{Q}$.*

♠

We also sketch an elementary proof of this result when Γ is a free group of rank at least two. It suffices to prove that for any (non-cyclic) finite group Q with a homomorphism $\psi_0\colon F_r \to Q$, there exists a finite group P with homomorphisms $\psi\colon F_r \to P$ and $\pi_{QP}\colon P \to Q$ such that (i) $Z(P) = 1$, and (ii) $\pi_{QP} \circ \psi = \psi_0$. The production of the group P is done in two stages. First, we fix a prime $p \in N$ and consider the $\mathbf{F}_p$–vector space $\mathbf{F}_p[Q] = V_p$. We lift the homomorphism $\psi_0\colon F_r \to Q$ to the finite group $\psi_1\colon V_p \rtimes Q$. Specifically, if $q_i = \psi_0(x_i)$, then $\psi_1(x_i) = p_i = (v_i,q_i)$ for some choice of $v_1,\dots,v_r \in V_p$. We set $P_1 = \psi_1(F_r)$ and then perform a similar extension but with P_1. We obtain $\psi_2\colon F_r \to W_p \rtimes P_1$ where $W_p = \mathbf{F}_p[P_1]$ and $\psi_2(x_i) = (w_i,p_i)$ for some choices $w_1,\dots,w_r \in W_p$. For an appropriate choices of $v_1,\dots,v_r \in \mathbf{F}_p[Q]$ and $w_1,\dots,w_r \in \mathbf{F}_p[P_1]$, the image $P_2 = \psi_2(F_r)$ has a quotient $P_2 \to P_2/Z(P_2) = P$ which is center free. The quotient is easy to describe. In $\mathbf{F}_p[P_1]$, there is a vector $v_0 = \sum_{\gamma \in P_1} \gamma$ and $Z(P_2) = \langle (v_0,1) \rangle$. In particular, if W is the quotient $\mathbf{F}_p$–vector space $\mathbf{F}_p[P_1]/\mathbf{F}_p[v_0]$, then $P = W \rtimes P_1$; see here for more details on this argument. The diagram below shows where all these groups reside:

$$\begin{tikzcd}
 & P_2 = \mathbf{F}_p\left[\mathbf{F}_p[Q] \rtimes Q\right] \rtimes P_1 \arrow[d] \arrow[dr] & \\
 & & P = W \rtimes P_1 \arrow[dl] \\
 & P_1 = \mathbf{F}_p[Q] \rtimes Q \arrow[d] & \\
F_r \arrow[uuur, "\psi_2"] \arrow[ur, "\psi_1"] \arrow[r, "\psi_0"'] & Q &
\end{tikzcd}$$

What Jarden–Ritter ensures for a general group Γ with $\delta(X,R) \geq 2$ are solutions to finding the vectors v_i, w_i in the above construction. The deficiency condition on (X,R) ensures that the homogenous linear systems associated to the above construction for Γ are underdetermined.

An important class of groups that admit presentations with positive deficiency are fundamental groups of closed (i.e. compact and without boundary), orientable surfaces of genus $g \geq 2$. Recall that the fundamental group of a closed, orientable surface Σ_g of genus g has a presentation of the form

$$\pi_1(\Sigma_g) = \left\{ \alpha_1, \beta_1, \dots, \alpha_g, \beta_g \ : \ \prod_{i=1}^{g} [\alpha_i, \beta_i] \right\}$$

where $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$ is the commutator. Note that when $g = 0$, the above group is trivial and when $g = 1$, the above group is $\mathbf{Z}^2 = \mathbf{Z} \times \mathbf{Z}$. For higher genus $g \geq 2$, these groups are closely related to non-abelian free groups. Similar to free groups and the role F_2 plays among the other finite rank free groups, the genus two surface group $\pi_1(\Sigma_2)$ contains all higher genus surface groups $\pi_1(\Sigma_g)$ as finite index subgroups; these containments are consequence of covering space theory.

We have a surjective homomorphism $\pi_1(\Sigma_g) \to F_g$ given by $\alpha_i \mapsto x_i$ and $\beta_i \mapsto 1$. Since we can pullback any filter $\mathscr{I}_{F_g}$ to $\mathscr{I}_{\pi_1(\Sigma_g)}$, the profinite completion $\widehat{\pi_1(\Sigma_g)}$ is also a rather big profinite group. (b) of the exercise below shows that groups with a presentation of deficiency at least two have surjective homomorphisms onto non-abelian free groups and so have big profinite completions. For clarification, though I've used the word "big" twice in reference to a profinite group, that is not an official adjective with regard to these notes. If I had to define "big", among (topologically) finitely generated profinite groups G, it would be used to address the class of profinite groups that admit a continuous surjective homomorphism to $\widehat{F}_r$ for some $r > 1$.

Exercise 23. Let Γ be a group with a finite presentation (X, R).

(a) Prove that if $\delta(X, R) \geq 1$, then there exists a finite index subgroup $\Gamma_0 < \Gamma$ and a surjective homomorphism $\Gamma_0 \to \mathbf{Z}$; the subgroup Γ_0 is called indicable and we say Γ is virtually indicable. [Hint: abelianize]

(b) Prove that if $\delta(X, R) \geq 2$, then there exists a surjective homomorphism $\Gamma \to F_2$. [Hint: cleverly "abelianize"]

(c) Prove that if there exists a surjective homomorphism $\Gamma \to \mathbf{Z}$, then there is a continuous surjective homomorphism $\widehat{\Gamma} \to \widehat{\mathbf{Z}}$. Is the converse true?

On the other end of the spectrum, the groups $\mathrm{SL}(n, \mathbf{Z})$ for $n \geq 3$ have much more restricted profinite completions. **Mennicke** and **Bass–Lazard–Serre/Bass–Milnor–Serre** that $\widehat{\mathrm{SL}(n, \mathbf{Z})} \cong \mathrm{SL}(n, \widehat{\mathbf{Z}})$. This is false for $n = 2$ as the finite index subgroup

$$\left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle$$

is a free group of rank two; this can be shown via the **ping-pong lemma** and **Möbius transformations**.

Exercise 24. Let

$$H_3(\mathbf{Z}) = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \;:\; x,y,z \in \mathbf{Z} \right\}.$$

Prove that $\widehat{H_3(\mathbf{Z})} = H_3(\widehat{\mathbf{Z}})$. The group $H_3(\mathbf{Z})$ is a **lattice** in the real 3–dimensional **Heisenberg group** $H_3(\mathbf{R})$.

2.5 Lecture 8. *Finitely Generated Groups and Subgroups*

The profinite theory of finitely generated groups works down from the profinite theory of finitely generated free groups by the universal mapping property of free groups. Before exploring further some topics in the profinite theory of finitely generated groups, we establish some basic language and results.

Given a group Γ, let $\mathrm{Filter}(\Gamma)$ denote the set of subfilters $\mathscr{I} \subset \mathscr{I}_\Gamma$. We have an equivalence relation on $\mathrm{Filter}(\Gamma)$ given by the partial ordering $\leq$ that we used ealier. Specifically, we say that $\mathscr{I}_2 \leq \mathscr{I}_1$ if for each $\Delta_1 \in \mathscr{I}_1$, there exists $\Delta_2 \in \mathscr{I}_2$ such that $\Delta_2 \subset \Delta_1$; we will say $\mathscr{I}_2$ is **finer** than $\mathscr{I}_1$ since that is the case for the associated topologies $\mathscr{T}_{\mathscr{I}_1}, \mathscr{T}_{\mathscr{I}_2}$. We say $\mathscr{I}_1 \sim \mathscr{I}_2$ if $\mathscr{I}_1 \leq \mathscr{I}_2$ and $\mathscr{I}_2 \leq \mathscr{I}_1$.

Lemma 2.26. *Let Γ be a group. Then the following are equivalent for $\mathscr{I}_1, \mathscr{I}_2 \in \mathrm{Filter}(\Gamma)$:*

(a) $\mathscr{I}_1 \sim \mathscr{I}_2$.

(b) $\mathrm{Id}\colon (\Gamma, \mathscr{T}_{\mathscr{I}_1}) \to (\Gamma, \mathscr{T}_{\mathscr{I}_2})$ *is a homeomorphism.*

(c) $\Gamma_{\mathscr{I}_1} \cong \Gamma_{\mathscr{I}_2}$.

Proof.

(a) if and only if (b):

To prove that Id is a homeomorphism, it suffices to prove that Id is continuous and open. Given $\Delta_2 \in \mathscr{I}_2$, since $\mathscr{I}_1$ is finer than $\mathscr{I}_2$, there exists $\Delta_1 \in \mathscr{I}_1$ such that $\Delta_1 \subset \Delta_2$. As these subgroups are finite index in Γ, we see that Δ_1 is finite index and open in Δ_2. Hence, Δ_2 is open in $\mathscr{T}_{\mathscr{I}_1}$

and so Id is continuous. Given $\Delta_1 \in \mathscr{I}_1$, since $\mathscr{I}_2$ is finer than $\mathscr{I}_1$, there exists $\Delta_2 \in \mathscr{I}_2$ such that $\Delta_2 \subset \Delta_1$, As before, this implies that Δ_1 is open in $\mathscr{T}_{\mathscr{I}_2}$.

For the converse, if $\mathrm{Id}\colon (\Gamma, \mathscr{T}_{\mathscr{I}_1}) \to (\Gamma, \mathscr{T}_{\mathscr{I}_2})$ is a homeomorphism, then each $\Delta_1 \in \mathscr{I}_1$ is open in $\mathscr{T}_{\mathscr{I}_2}$ and each $\Delta_2 \in \mathscr{I}_2$ is open in $\mathscr{T}_{\mathscr{I}_1}$. It is straightforward to see that this implies $\mathscr{I}_1 \sim \mathscr{I}_2$.

(b) if and only if (c):

If $\mathrm{Id}\colon (\Gamma, \mathscr{T}_{\mathscr{I}_1}) \to (\Gamma, \mathscr{T}_{\mathscr{I}_2})$ is a homeomorphism, then there is a bijection between Cauchy sequences under the associated pseudometrics for each topology. In particular, the pseudometric completions $\Gamma_{\mathscr{I}_1}, \Gamma_{\mathscr{I}_2}$ must be isomorphic. Converse, if the pseudometric completions are isomorphic, the induced subspace topologies coming from the pseudometrics must be homeomorphic. ♠

We define $\mathrm{Top}_{pro}(G) = \mathrm{Filter}(G)/\sim$. Given a pair of groups G,H, a homomorphism $\psi\colon G \to H$, and a filter $\mathscr{I} \subset \mathscr{I}_H$, we obtain a filter $\psi^\star(\mathscr{I}) = \left\{\psi^{-1}(\psi(G) \cap \Delta)\right\}_{\Delta \in \mathscr{I}}$. We call the filter $\psi^\star(\mathscr{I}) \subset \mathscr{I}_G$ the pullback of $\mathscr{I}$ by ψ. Formally, if $\mathrm{Filter}(G)$ is the subset of subfilters of $\mathscr{I}_G$, we obtain a function $\psi^\star\colon \mathrm{Filter}(H) \to \mathrm{Filter}(G)$. It is clear that $\psi^\star(\mathscr{I}_1) \sim \psi^\star(\mathscr{I}_2)$ when $\mathscr{I}_1 \sim \mathscr{I}_2$, and so $\psi^\star\colon \mathrm{Top}_{pro}(H) \to \mathrm{Top}_{pro}(G)$.

Exercise 25. What topologies can one endow $\mathrm{Top}_{pro}(\cdot)$ so that $\psi^\star$ is continuous?

Lemma 2.27. *Let G,H be groups and $\psi\colon G \to H$ a homomorphism. If ψ is surjective, then $\psi^\star$ is injective (on* Top_{pro}*).*

Proof. This is straightforward. ♠

If G is residually finite and $\psi\colon G \to H$ is not injective, then $\psi^\star$ cannot be onto. To see this, note first that since G is residually finite, there exists a cofinal filter $\mathscr{I} \in \mathrm{Filter}(G)$; take $\mathscr{I}_G$ for instance. As ψ is not injective, no filter $\mathscr{I} \in \mathrm{Filter}(H)$ can pullback to a cofinal filter in G. In particular, $\mathscr{I}$ is not in the image of $\psi^\star$. The following gives a necessary and sufficient conditions for the injectivity of $\psi^\star$.

Lemma 2.28. *If G,H are groups, $\psi\colon G \to H$ is a homomorphism, then $\psi^\star$ is surjective if and only if $\psi^\star(\mathscr{I}_H) = \mathscr{I}_G$ (on the level of* Top_{pro}*).*

Proof. Let us first deconstruct some notation. We have $\psi^\star\colon \mathrm{Top}_{pro}(H) \to \mathrm{Top}_{pro}(G)$ given by $[\left\{\psi^{-1}(\psi(G) \cap \Delta)\right\}_{\Delta \in \mathscr{I}}]$ where $[\cdot]$ denotes the equivalence class associated to $\sim$. If $\mathscr{I}_G = \psi^\star(\mathscr{I}_H)$, then for each $\Delta \in \mathscr{I}_G$, there exists $\Delta_H \in \mathscr{I}_H$ such that $\psi^{-1}(\psi(G) \cap \Delta_H) < \Delta$. Given any filter $\mathscr{I} \in \mathrm{Filter}(G)$ and any $\Delta \in \mathscr{I}$, from the above, we can find a $\Delta_H \in \mathscr{I}_H$ such that

$\psi^{-1}(\psi(G)\cap\Delta) \subset \Delta$. Passing to the filter spanned by the Δ_H if necessary, we obtain a filter $\mathscr{I}_H \in \mathrm{Filter}(H)$ such that $\psi^\star(\mathscr{I}_H) = \mathscr{I}$. For the converse, since $\mathscr{I}_G$ and $\mathscr{I}_H$ are the finest possible filters in $\mathrm{Filter}(G), \mathrm{Filter}(H)$, respectively, it follows that if $\psi^\star$ is surjective then $\psi^\star(\mathscr{I}_H) = \mathscr{I}_G$. ♠

Given a pair of residually groups G, H and an injective homomorphism $\psi\colon H \to G$, we see that $\psi^\star$ is surjective if and only if $\psi^\star(\mathscr{I}_G) = \mathscr{I}_H$. Since ψ is injective, we can identify H with its image under ψ. In this view, we have $H < G$ and ψ is an inclusion map. The pullback of the filter $\mathscr{I}_G$ is $\{H\cap\Delta\}_{\Delta\in\mathscr{I}_G}$. In particular, by Lemma 2.26, $\psi^\star$ is injective if and only if the subspace topology induced by $\mathscr{T}_{\mathscr{I}_G}$ is $\mathscr{T}_{\mathscr{I}_H}$.

Definition 2.29. Given a group G and a subgroup $H < G$, we say that H is **strongly separable** if H is closed in the profinite topology on G and the profinite topology of H is equivalent to the subspace topology on H induced by the profinite topology of G.

Proposition 2.30. *Let Γ be a group and Δ a strongly separable subgroup, $\overline{\Delta} \subset \widehat{\Gamma}$ be the closure of $\widehat{\varphi_\Gamma}(\Delta)$ where $\widehat{\varphi_\Gamma}\colon \Gamma \to \widehat{\Gamma}$. Then the induced continuous, homomorphism $\widehat{\Delta} \to \overline{\Delta}$ is an isomorphism.*

The validity of Proposition 2.30 is a consequence of Lemma 2.26 (b)-(c).

If Δ is a normal subgroup of Γ, $\overline{\Delta}$ is a closed, normal subgroup of $\widehat{\Gamma}$ and we get the diagram

$$\begin{tikzcd}
& \Delta \arrow[r, "\iota"] \arrow[dl, "\widehat{\varphi_\Delta}"'] \arrow[dd, "\widehat{\varphi_\Delta}"] & \Gamma \arrow[r, "\psi_\Delta"] \arrow[dd, "\widehat{\varphi_\Gamma}"] & \Gamma/\Delta \arrow[dd, "\overline{\varphi}"] \arrow[dr, "\widehat{\varphi_{\Gamma/\Delta}}"] & \\
\widehat{\Delta} \arrow[dr] & & & & \widehat{\Gamma/\Delta} \arrow[dl, "\pi_{\Gamma,\Delta}"] \\
& \overline{\Delta} \arrow[r, "\widehat{\iota}"'] & \widehat{\Gamma} \arrow[r, "\widehat{\psi_\Delta}"'] & \widehat{\Gamma}/\overline{\Delta} &
\end{tikzcd}$$

Since ψ_Δ is surjective, it follows that $\widehat{\Gamma}/\overline{\Delta} \cong \widehat{\Gamma/\Delta}$ without any assumptions on Δ. If Δ is strongly separable, we have $\overline{\Delta} \cong \widehat{\Delta}$, and so $\widehat{\Gamma/\Delta} \cong \widehat{\Gamma}/\widehat{\Delta}$. In particular, we have the following:

Corollary 2.31. *If Γ is a group and Δ is a normal, strongly separable subgroup, then we have the following commutative diagram:*

$$\begin{tikzcd}
1 \arrow[r] & \Delta \arrow[r] \arrow[d] & \Gamma \arrow[r] \arrow[d] & \Gamma/\Delta \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \widehat{\Delta} \arrow[r] & \widehat{\Gamma} \arrow[r] & \widehat{\Gamma/\Delta} \arrow[r] & 1
\end{tikzcd}$$

Given a short exact sequence of groups

$$1 \longrightarrow \Gamma_1 \longrightarrow \Gamma_2 \longrightarrow \Gamma_3 \longrightarrow 1,$$

if Γ_1 is finitely generated and $Z(\widehat{\Gamma_1}) = \{1\}$, then we can extend the short exact sequence to the associated profinite completions

$$1 \longrightarrow \widehat{\Gamma_1} \longrightarrow \widehat{\Gamma_2} \longrightarrow \widehat{\Gamma_3} \longrightarrow 1.$$

To see this, note that we have $\Gamma_2 \to \mathrm{Aut}(\Gamma_1)$ given by Γ_2–conjugation. Since Γ_1 is finitely generated, $\mathrm{Aut}(\widehat{\Gamma_1})$ is a profinite group (we will talk more about this in the next lecture) and so we have $\widehat{\Gamma_2} \to \mathrm{Aut}(\widehat{\Gamma_1})$. Restricting this homomorphism to Γ_1 and extending to the profinite completion, we obtain $\widehat{\Gamma_1} \to \widehat{\Gamma_2} \to \mathrm{Aut}(\widehat{\Gamma_1})$. Since $Z(\widehat{\Gamma_1})$ is trivial, we see that $\widehat{\Gamma_1} \to \widehat{\Gamma_2}$ is injective; this result and argument were borrowed from **BER** and the references therein.

Corollary 2.32. *If $1 \to \Gamma_1 \to \Gamma_2 \to \Gamma_3 \to 1$ is a short exact sequence of groups such that Γ_1 is finitely generated and $Z(\widehat{\Gamma_1}) = \{1\}$, then there is a short exact sequence of profinite completions $1 \to \widehat{\Gamma_1} \to \widehat{\Gamma_2} \to \widehat{\Gamma_3} \to 1$.*

Finite index subgroups are always strongly separable. However, it need not be the case that a general subgroup of G should be strongly separable. Indeed, by Exercise 8, if H is a normal subgroup of G, then H is closed in the profinite topology on G if and only if G/H is residually finite.

We say that a group G is **Hopfian** if any surjective homomorphism $\psi\colon G \to G$ is injective.

Lemma 2.33. *If G is not Hopfian, then G is not residually finite.*

Proof. For any $\psi\colon G \to G$ surjective, non-injective homomorphism and any non-trivial $\gamma \in \ker\psi$, one can show that $\gamma \in \bigcap_{\mathscr{I}_G} \Delta$. ♠

Example 6. Given $n, m \in \mathbf{N}$, we define the **Baumslag–Solitar group** $\mathrm{BS}(m,n)$ by the presentation

$$\left\{a, b \,:\, b^{-1}a^m b = a^n\right\}.$$

Exercise 26. Prove that $\mathrm{BS}(2,3)$ is not residually finite [Hint: Prove $\mathrm{BS}(2,3)$ is not Hopfian].

Exercise 27. Prove that every subgroup of $\mathbf{Z}^n$ is strongly separable [Hint: Linear algebra].

Exercise 28. Prove that every subgroup of $H_3(\mathbf{Z})$ is strongly separable [Hint: Linear algebra].

2.6 Lecture 9. *Automorphism Groups*

Let Γ be a finitely generated group and $\mathscr{I} \subset \mathscr{I}_\Gamma$ a filter. Recall that a subgroup $\Delta \subset \Gamma$ is said to be **characteristic** if for each $\lambda \in \mathrm{Aut}(\Gamma)$, we have $\lambda(\Delta) \subset \Delta$. We say $\mathscr{I}$ is **characteristic** if each $\Delta \in \mathscr{I}$ is characteristic.

Lemma 2.34. *If Γ is finitely generated and $\mathscr{I} \subset \mathscr{I}_\Gamma$ is a filter, then there exists a filter $\mathscr{I}_{char} \subset \mathscr{I}$ such that $\mathscr{I}_{char}$ is characteristic, indexed by* $\mathbf{N}$*, and $\varprojlim_{\mathscr{I}} \Gamma/\Delta \cong \varprojlim_{\mathscr{I}_{char}} \Gamma/\Delta$.*

Proof. Since Γ is finitely generated, there are only finite many subgroups of index at most m. For each $\Delta \in \mathscr{I}$, we define $\Delta_{char} = \bigcap_{\psi \in \mathrm{Aut}(\Gamma)} \psi(\Delta) < \Delta$. The subgroup Δ_{char} is finite index and characteristic. It follows that $\bigcap_{\Delta \in \mathscr{I}} \Delta = \bigcap_{\Delta \in \mathscr{I}_{char}} \Delta$ and so by Lemma 2.26, the associated completions are isomorphic. ♠

Remark 1. By Lemma 2.34, every filter $\mathscr{I} \in \mathrm{Filter}(\Gamma)$ contains a characteristic subfilter $\mathscr{I}_{char}$ with an isomorphic associated completion. We will occasionally use this result implicitly. We set $\mathscr{I}_\Gamma^{char}$ to be the filter of characteristic, finite index subgroups of Γ.

If $\mathscr{I}$ is characteristic, for each homomorphism $\psi_\Delta \colon \Gamma \to \Gamma/\Delta$, we have induced homomorphisms $\Phi_\Delta \colon \mathrm{Aut}(\Gamma) \to \mathrm{Aut}(\Gamma/\Delta)$ defined by $\Phi_\Delta(\lambda)(\gamma\Delta) = \lambda(\gamma)\Delta$. Any subgroup Λ of $\mathrm{Aut}(\Gamma)$ that contains $\ker \Phi_\Delta$ for some $\Delta \in \mathscr{I}_\Gamma^{char}$ will be called a **congruence subgroup**. We denote the induced directed subset of the subsets of finite index subgroups of $\mathrm{Aut}(\Gamma)$ by $\mathscr{I}_{cong}$. Note that $\mathscr{I}_{cong} \subset \mathscr{I}_{\mathrm{Aut}(\Gamma)}$, the latter being the filter of all finite index, normal subgroups of $\mathrm{Aut}(\Gamma)$, and we denote $\Lambda_{\mathscr{I}} = \varprojlim_{\mathscr{I}_{\mathrm{Aut}}} \mathrm{Aut}(\Gamma)/\Delta$. By construction, we have the homomorphism $\varphi_{\mathscr{I}_{cong}} \colon \mathrm{Aut}(\Gamma) \to \Lambda_{\mathscr{I}}$. This homomorphism is continuous in the topology induced by $\mathscr{I}_{cong}$. In particular, it is continuous with respect to the profinite topology induced by $\mathscr{I}_{\mathrm{Aut}(\Gamma)}$. We denote the completion of $\mathrm{Aut}(\Gamma)$ with respect to $\mathscr{I}_{cong}$ by $\mathrm{Aut}(\Gamma_{\mathscr{I}})$ and the fully profinite completion (i.e. the completion with respect to $\mathscr{I}_{\mathrm{Aut}(\Gamma)}$) by $\widehat{\mathrm{Aut}(\Gamma)}$. By Corollary 2.12, there exists a continuous, surjective homomorphism $\pi_{\mathscr{I}_{cong}} \colon \widehat{\mathrm{Aut}(\Gamma)} \to \mathrm{Aut}(\Gamma_{\mathscr{I}})$.

Exercise 29. Prove that if $\pi_{\mathscr{I}} \colon \widehat{\Gamma} \to \Gamma_{\mathscr{I}}$ is not injective, then $\pi_{\mathscr{I}_{cong}} \colon \widehat{\mathrm{Aut}(\Gamma)} \to \mathrm{Aut}(\Gamma_{\mathscr{I}})$ is not injective.

Exercise 30. Prove if Γ is a finitely generated group, then $\mathrm{Aut}(\widehat{\Gamma})$ is a profinite group.

Lemma 2.35. *If Γ is finitely generated and $\mathscr{I} \in \mathit{Filter}(\Gamma)$ is characteristic and cofinal, then $\mathscr{I}_{cong} \in \mathrm{Filter}(\mathrm{Aut}(\Gamma))$ is cofinal.*

Proof. Given a non-trivial $\lambda \in \mathrm{Aut}(\Gamma)$, we know that there exists $\gamma \in \Gamma$ such that $\lambda(\gamma) \neq \gamma$. Since $\mathscr{I}$ is cofinal, there exists $\Delta_\lambda \in \mathscr{I}$ such that $\gamma\lambda(\gamma)^{-1} \notin \Delta_\lambda$. In particular, $\gamma\Delta_\lambda \neq \lambda(\gamma)\Delta_\lambda$ and so $\Phi_{\Delta_\lambda}(\lambda) \neq 1$. ♠

When $\mathscr{I} = \mathscr{I}_\Gamma^{char}$, we denote the associated subfilter of $\mathscr{I}_{\mathrm{Aut}(\Gamma)}$ simply by $\widehat{\mathscr{I}}$. In this case, we have $(\mathrm{Aut}(\Gamma))_{\widehat{\mathscr{I}}} \cong \mathrm{Aut}(\widehat{\Gamma})$. We say the $\mathrm{Aut}(\Gamma)$ has the **congruence subgroup property** if $\ker \pi_{\widehat{\mathscr{I}}}$ is finite. Loosely, having the congruence subgroup property says that the abstract finite representation theory of the group $\mathrm{Aut}(\Gamma)$ is the same, up to finiteness, as the representation theory of $\mathrm{Aut}(\Gamma)$ viewed as the automorphism group of Γ. Recall that we have an exact sequence

$$1 \longrightarrow Z(\Gamma) \longrightarrow \Gamma \xrightarrow{\mathrm{Ad}} \mathrm{Aut}(\Gamma) \xrightarrow{\pi_{\mathrm{Aut}}} \mathrm{Out}(\Gamma) \longrightarrow 1$$

where $\mathrm{Ad}(\gamma)(\theta) = \gamma^{-1}\theta\gamma$. If $\gamma \in \Gamma$ and $\lambda \in \mathrm{Aut}(\Gamma)$, we have

$$\lambda \circ \mathrm{Ad}(\gamma) \circ \lambda^{-1}(\theta) = \lambda^{-1}(\gamma)\theta\lambda(\gamma) = \mathrm{Ad}(\lambda(\gamma))(\theta).$$

More compactly, if $\mathrm{Ad}(\gamma) = \mathrm{Ad}_\gamma$, we see that $\lambda\,\mathrm{Ad}_\gamma \lambda^{-1} = \mathrm{Ad}_{\lambda(\gamma)}$. Even better, we could write $\mathrm{Ad}_\lambda(\mathrm{Ad}_\gamma) = \mathrm{Ad}_{\lambda(\gamma)}$, where $\mathrm{Ad}_\lambda \in \mathrm{Aut}(\mathrm{Aut}(\Gamma))$; do enjoy the "visual" yin-yang relationships $\lambda\gamma$ have. The next lemma is an immediate consequence of this discussion.

Lemma 2.36. *If Γ is group, then $C_{\mathrm{Aut}(\Gamma)}(\mathrm{Ad}_\gamma) = \mathrm{Fix}(\gamma)$ where*

$$\mathrm{Fix}(\gamma) = \{\lambda \in \mathrm{Aut}(\Gamma) \ : \ \lambda(\gamma) = \gamma\}.$$

As a result of Lemme 2.36, we obtain the following corollary:

Corollary 2.37. *If Γ is a group, then $C_{\mathrm{Aut}(\Gamma)}(\mathrm{Ad}(\Gamma)) = \{\mathrm{Id}_\Gamma\}$.*

Lemma 2.38. *If Γ is a residually finite, finitely generated group with trivial center, then Γ is strongly separable in* $\mathrm{Aut}(\Gamma)$ *viewed as a subgroup via* Ad.

Proof. By Lemma 2.35, we know that $\mathscr{I}_\Gamma \sim \mathscr{I}_\Gamma^{char}$. In particular, it suffices to show for each $\Delta \in \mathscr{I}_\Gamma^{char}$, there exists $\psi\colon \mathrm{Aut}(\Gamma) \to \mathrm{Aut}(Q)$, where Q is a finite group, such that $\ker(\psi \circ \mathrm{Ad}) < \Delta$. Since Δ is characteristic, the quotient homomorphism $\psi_\Delta\colon \Gamma \to Q_0 = \Gamma/\Delta$ induces $\psi_0\colon \mathrm{Aut}(\Gamma) \to \mathrm{Aut}(Q_0)$. By definition of ψ_0, we see that $\psi_0(\mathrm{Ad}(\gamma)) = \mathrm{Ad}(\psi_\Delta(\gamma))$ for all $\gamma \in \Gamma$. In particular, $\ker(\psi_0 \circ \mathrm{Ad}) = \psi_\Delta^{-1}(Z(Q_0))$. Pick a complete set of coset representatives $\gamma_1, \dots, \gamma_r$ for $\psi_\Delta^{-1}(Z(Q_0))$ with respect to Δ. For each $i = 1, \dots, r$, since $Z(\Gamma) = \{1\}$, there exists $\eta_i \in \Gamma$ such that $[\gamma_i, \eta_i] \neq 1$. Since Γ is residually finite, there exists a surjective homomorphism $\psi_i\colon \Gamma \to Q_i$, where Q_i is finite, such that $\psi_i([\gamma_i, \eta_i]) \neq 1$. In particular, $\psi_i(\gamma_i) \notin Z(Q_i)$. Passing to the characteristic core of $\ker \psi_i$ if necessary, we may assume that $\ker \psi_i$ is characteristic. In total, we have $\Psi\colon \Gamma \to Q = \prod_{i=0}^r Q_i$ with $\ker \Psi$ characteristic and associated $\psi\colon \mathrm{Aut}(\Gamma) \to \mathrm{Aut}(Q)$. It follows that $\ker(\psi \circ \mathrm{Ad}) < \Delta$. ♠

Remark 2. If Γ is not center-free or residually finite, then $\mathrm{Ad}(\Gamma)$ is strongly separable though Γ does not inject into either $\widehat{\Gamma}$ nor $\mathrm{Aut}(\Gamma)$.

As a result of Corollary 2.31 and Lemma 2.38, we have the commutative diagram when Γ is center-free:

$$\begin{tikzcd}
1 \arrow[r] & \Gamma \arrow[r, "\mathrm{Ad}"] \arrow[dd, "\widehat{\varphi}_\Gamma"] & \mathrm{Aut}(\Gamma) \arrow[rr] \arrow[dd] \arrow[dr] & & \mathrm{Out}(\Gamma) \arrow[rr] \arrow[dd] \arrow[dr] & & 1 \\
& & & \widehat{\mathrm{Aut}(\Gamma)} \arrow[dl] & & \widehat{\mathrm{Out}(\Gamma)} \arrow[dl] & \\
& \widehat{\Gamma} \arrow[r, "\mathrm{Ad}"'] & \mathrm{Aut}(\widehat{\Gamma}) \arrow[rr] & & \mathrm{Out}(\widehat{\Gamma}) \arrow[rr] & & 1
\end{tikzcd}$$

Automorphisms of Free Groups. Given a homomorphism $\eta\colon \mathrm{Aut}(F_r) \to Q$, where Q is finite, we have $\mathrm{Ad}\colon F_r \to \mathrm{Aut}(F_r)$ and so $\psi_0\colon F_r \to Q$ given by $\eta \circ \mathrm{Ad}$. We denote $H = \psi_0(F_r)$ and note that H is a normal subgroup of Q since $\mathrm{Ad}(F_r) < \mathrm{Aut}(F_r)$ is normal and H is the image of a normal subgroup of a group under a surjective homomorphism. In particular, we have $\eta_1\colon \mathrm{Aut}(F_r) \to \mathrm{Aut}(H)$ given by $\eta_1(\lambda)(h) = \mathrm{Ad}_{\eta(\lambda)}(h)$; that is, $\eta_1 = (\mathrm{Ad})_{|H} \circ \eta$. Note that $\ker \eta_1 = \eta^{-1}(C_Q(H))$ is the centralizer of H in Q and so $\ker \eta < \ker \eta_1$. Unfortunately, to have the congruence subgroup property, we require that a congruence kernel $\ker \eta' < \ker \eta$ be contained in $\ker \eta$. The failure of this approach to work to prove that $\mathrm{Aut}(F_r)$ that has the congruence subgroup property is measured by $C_Q(H)$. However, by Corollary 2.37, we know that $C_{\mathrm{Aut}(F_r)}(F_r) = \{1\}$ and that should be viewed as evidence that one can pass to a finite index characteristic subgroup of $\ker \psi_0$ where we can ensure $C_Q(H) = \{1\}$.

Question: *Does* $\mathrm{Aut}(F_r)$ *have the congruence subgroup property for* $r > 2$*?*

Asada [2] (see also BER) proved that $\mathrm{Aut}(F_2)$ has the congruence subgroup property.

2.7 Lecture 10. *Rigidity*

Given a pair of finitely (presentable) generated groups Γ_1, Γ_2 and a homomorphism $\psi\colon \Gamma_1 \to \Gamma_2$, we have an induced continuous homomorphism $\widehat{\psi}\colon \widehat{\Gamma_1} \to \widehat{\Gamma_2}$. Recall that for $\mathscr{I} \in \mathrm{Filter}(\Gamma_2)$, we have $\psi^\star(\mathscr{I}) \in \mathrm{Filter}(\Gamma_1)$ defined by $\psi^\star(\mathscr{I}) = \psi^{-1}(\psi(\Gamma_1) \cap \Delta_2)$ where $\Delta_2 \in \mathscr{I}$. If ψ is an isomorphism, then $\widehat{\psi}$ is an isomorphism of profinite groups. In 1970, Grothendieck [7] asked whether the converse holds.

Question 2.39 (Grothendieck, 1970)**.** *If* Γ_1, Γ_2 *are finitely presentable, residually finite group and* $\psi\colon \Gamma_1 \to \Gamma_2$ *induced an isomorphism (of profinite groups)* $\widehat{\psi}\colon \widehat{\Gamma_1} \to \widehat{\Gamma_2}$*, does that imply* *that ψ is an isomorphism.*

Grothendieck provided some evidence for an affirmative answer to the above question by construction a group $\mathrm{Cl}_R(\Gamma)$ for a group Γ and commutative ring R with identity called the Tannakian dual group of Γ over R. By construction of $\mathrm{Cl}_R(\Gamma)$, there is a homomorphism $\Gamma \to \mathrm{Cl}_R(\Gamma)$ which is injective provided R is residually finite.

Question 2.40 (Grothendieck, 1970)**.** *Does there exist a commutative ring R such that for every finite presentable, residually finite group Γ, we have $\Gamma \cong \mathrm{Cl}_R(\Gamma)$? Given a fixed finitely presentable, residually finite group Γ, does there exists a commutative ring R such that $\mathrm{Cl}_R(\Gamma) \cong \Gamma$?*

These questions address to what extent the group invariants $\widehat{\Gamma}$ and $\mathrm{Cl}_R(\Gamma)$ determine the group. We have different levels of recovering that we can ask for:

Definition 2.41. Let Γ be a finitely presentable (finitely generated), residually finite group.

(i) We say that Γ is **profinite rigid** if whenever Λ is a finitely presentable (finitely generated) group with that $\widehat{\Gamma} \cong \widehat{\Lambda}$, then $\Gamma \cong \Lambda$.

(ii) We say that Γ is **strongly Grothendieck rigid** if whenever Λ is a finitely presentable (finitely generated) group and a homomorphism $\psi\colon \Gamma \to \Lambda$ such that $\widehat{\psi}\colon \widehat{\Gamma} \to \widehat{\Lambda}$ is an isomorphism of profinite groups, then ψ is an isomorphism.

(iii) We say that Γ is **Grothendieck rigid** if whenever $\Lambda < \Gamma$ is a finitely presentable (finitely generated) subgroup such that the inclusion $\iota\colon \Lambda \to \Gamma$ induces an isomorphism $\widehat{\iota}\colon \widehat{\Lambda} \to \widehat{\Gamma}$, then ι is an isomorphism.

We briefly mention a few results on the above questions of Grothendieck. Platonov–Tavgen [12] constructed finitely generated counterexamples to Question 2.39. Finitely presented examples where constructed by Bridson–Grunewald [5]. The examples that they constructed were of the form $\Gamma \times \Gamma$ and a subgroup $P < \Gamma \times \Gamma$. The inclusion map $\iota\colon P \to \Gamma \times \Gamma$ induces an isomorphism between their respective profinite completions. The further can arrange for the group Γ to be hyperbolic, in the sense of Gromov. For Question 2.40, Lubotzky [9] investigated the problem in 1980. He established several positive results and some negative results. Bridson–Grunewald also construct counterexamples to each part of Question 2.40.

2.8 Lecture 11. *Rigidity, continued*

In this lecture, I will outline some constructions of groups with isomorphic profinite completions due to Aka [1]. For a better account on the above questions of Grothendieck, see the recent paper of Bridson–Grunewald.

Finding finitely generated/finitely presented, residually finite groups Γ_1, Γ_2 with isomorphic profinite completions is not trivial. Let us make a few very modest observations to further substantiate that. For a finitely generated group Γ, we define $\mathscr{Q}(\Gamma) = \{(Q, m_Q)\}$ to be the set of all finite quotient groups of Γ where m_Q denotes the multiplicity for a given finite group Q. Specifically, we define m_Q to be the number of $\Delta \in \mathscr{I}_\Gamma$ such that $\Gamma/\Delta \cong Q$. Since Γ is finitely generated, $m_Q < \infty$ for any finite group Q.

Lemma 2.42. *If Γ_1, Γ_2 are finitely generated groups with $\widehat{\Gamma_1} = \widehat{\Gamma_2}$, then $\mathscr{Q}(\Gamma_1) = \mathscr{Q}(\Gamma_2)$.*

We leave the proof to the reader. As a consequence of this simple lemma, we see the following:

Proposition 2.43.

(a) $\widehat{F}_r \cong \widehat{F}_s$ *if and only if* $r = s$.

(b) $\widehat{\mathbf{Z}^m} \cong \widehat{\mathbf{Z}^n}$ *if and only if* $m = n$.

(c) $\widehat{\pi_1(\Sigma_g)} \cong \pi_1(\Sigma_{g'})$ *if and only if* $g = g'$.

Proof. (a) and (c) follow from (b) (and Exercise 33 below) since

$$F_r/[F_r, F_r] \cong \mathbf{Z}^r, \quad \pi_1(\Sigma_g)/[\pi_1(\Sigma_g), \pi_1(\Sigma_g)] \cong \mathbf{Z}^{2g}.$$

(b) follows immediately from Lemma 2.42. ♠

Question 2.44. *Does there exist a finitely presentable, non-free, residually finite group Γ such that $\widehat{\Gamma} \cong \widehat{F}_r$ for some $r \geq 2$? Similarly, $\widehat{\Gamma} \cong \widehat{\pi_1(\Sigma_g)}$ for $g \geq 2$ with $\Gamma \neq \pi_1(\Sigma_g)$?*

Note that there exists a finite generated, infinite index subgroup $P < F_2 \times F_2$ such that the inclusion homomorphism $\iota \colon P \to F_2 \times F_2$ induces an isomorphism $\widehat{\iota} \colon \widehat{P} \to \widehat{F_2 \times F_2} \cong \widehat{F}_2 \times \widehat{F}_2$; see [5].

Given a group Γ, we define the **lower central series** $\{\Gamma_j\}$ inductively via $\Gamma_0 = \Gamma$ and $\Gamma_{i+1} = [\Gamma, \Gamma_i]$. The subgroups Γ_j are **fully invariant** and the quotient groups $N(\Gamma, i) = \Gamma/\Gamma_i$ are the associated universal nilpotent quotient groups. Recall that we say that a group Γ is **nilpotent of step size i or class i** if $\Gamma_i = 1$. A group of class 0 is trivial and a group of class 1 is abelian. The groups $N(\Gamma, i)$ satisfy the following universal mapping property: For any homomorphism $\psi\colon \Gamma \to N$ where N is a nilpotent group of class i, there exists a unique homomorphism $\overline{\psi}\colon N(\Gamma, i) \to N$ such that the diagram

$$\begin{tikzcd} \Gamma \arrow[rr, "\psi"] \arrow[dr, "\psi_{i,nil}"'] & & N \\ & N(\Gamma, i) \arrow[ur, "\psi_i"'] & \end{tikzcd}$$

commutes where $\psi_{i,nil}\colon \Gamma \to N(\Gamma, i)$ is the quotient homomorphism. We say a group Γ is **residually nilpotent** if for each non-trivial $\gamma \in \Gamma$, there exists a nilpotent group N and a homomorphism $\psi\colon \Gamma \to N$ such that $\psi(\gamma) \neq 1$.

Exercise 31. Prove that Γ is residually nilpotent if and only if $\bigcap_{i \geq 0} \Gamma_i = \{1\}$.

Exercise 32. Prove that F_r and $\pi_1(\Sigma_g)$ are residually nilpotent for $r \geq 1$ and $g \geq 1$.

Give a fixed finitely generated, residually nilpotent group Γ, we say that a residually nilpotent group Δ is **para–Γ** if $N(\Gamma, i) \cong N(\Delta, i)$ for all $i \geq 1$. Baumslag [3] constructed examples of finitely generated, non-free, para-free groups; see also [4]. Prior to Baumslag's work, Magnus proved a rigidity result for para-free groups that have the same rank as their associated free group.

Theorem 2.45 (Magnus, 1939 [11])**.** *If Γ is a rank r, residually nilpotent group such that $N(\Gamma, i) \cong N(F_r, i)$ for $i \geq 1$, then $\Gamma \cong F_r$.*

Having the same representation theory to nilpotent groups is obviously a weaker relationship than having the same finite representation theory. Note that if Γ is residually finite and $\widehat{\Gamma} \cong \widehat{F_r}$ for some $r \geq 2$, it is not clear that Γ is residually nilpotent.

Question 2.46. *If Γ_1, Γ_2 are finitely presentable, residually finite groups such that $\widehat{\Gamma_1} \cong \widehat{\Gamma_2}$ and Γ_1 is residually nilpotent, is Γ_2 necessarily residually nilpotent?*

One can ask similarly if having a faithful representation to $\mathrm{GL}(n, \mathbf{C})$ for some n is a profinite invariant.

Question 2.47. *If Γ_1, Γ_2 are finitely presentable groups such that $\widehat{\Gamma_1} \cong \widehat{\Gamma_2}$ and there exists an injective representation $\rho_1\colon \Gamma_1 \to \mathrm{GL}(n_1, \mathbf{C})$ for some n_1, does there exist an injective $\rho_2\colon \Gamma_2 \to \mathrm{GL}(n_2, \mathbf{C})$ for some n_2?*

Exercise 33. Prove that if Γ_1, Γ_2 are finitely generated groups with $\widehat{\Gamma_1} \cong \widehat{\Gamma_2}$, then $\widehat{N(\Gamma_1, i)} \cong \widehat{N(\Gamma_2, i)}$ for all i. Additionally $N(\Gamma_1, 1) \cong N(\Gamma_2, 1)$.

In the above exercise, it need not be the case that $N(\Gamma_1, i) \cong N(\Gamma_2, i)$ when $\widehat{\Gamma_1} \cong \widehat{\Gamma_2}$. Indeed, there exist finitely generated, torsion free nilpotent groups Γ_1, Γ_2 such that $\widehat{\Gamma_1} \cong \widehat{\Gamma_2}$ but Γ_1, Γ_2 are not isomorphic.

Exercise 34. Prove that if Γ_1, Γ_2 are finitely generated nilpotent groups with $\widehat{\Gamma_1} \cong \widehat{\Gamma_2}$, then Γ_1, Γ_2 have the same step size.

We now describe a construction of Aka [1] that produces examples of non-isomorphic groups with the same profinite completions. We produce examples that are nilpotent, (virtually) polycyclic, and also examples that are lattices in semisimple Lie groups.

Recall that for each prime p, we defined a valuation $v_p \colon \mathbf{Z} \to \mathbf{N}$ given by

$$v_p(m) = \max\left\{\ell \in \mathbf{N} \ : \ p^\ell \mid m\right\}$$

when $m \neq 0$ and $v_p(0) = \infty$. We can extend this valuations to a valuation $v_p \colon \mathbf{Q} \to \mathbf{Z}$ by $v_p(a/b) = v_p(a) - v_p(b)$ and also have an associated absolute value $|\alpha|_p = p^{-v_p(\alpha)}$ for $\alpha \in \mathbf{Q}$. Finally, we have an associated metric $d_p(\alpha, \beta) = |\alpha - \beta|_p$ and denote the (Cauchy) completion of $\mathbf{Q}$ by this metric by $\mathbf{Q}_p$. The metric space $\mathbf{Q}_p$ is a locally compact field and is called the **field of p–adic numbers**. Ostrowski's Theorem states that any absolute value on $\mathbf{Q}$ is equivalent to a p–adic absolute value $|\cdot|_p$ for some prime p or the usual archimedean absolute value. The **ring of adeles or adele ring** is defined to be the locally compact topological ring $\mathbf{A}_{\mathbf{Q}} = \prod_p \mathbf{Q}_p$ where for $p = \infty$, we set $\mathbf{Q}_\infty = \mathbf{R}$.

If $K/\mathbf{Q}$ is a finite extension (i.e. a number field) and $|\cdot|_p$ is a valuation on $\mathbf{Q}$, we have finitely many extensions $v_{1,p}, \dots, v_{r_p,p}$ of $|\cdot|_p$ to K. Each extension v_i gives an associated completion $K_{v_{i,p}}$ which is a finite extension of $\mathbf{Q}_p$. The ring of K–adeles is defined similarly to be $\mathbf{A}_K = \prod_p \prod_{i=1}^{r_p} K_{v_{i,p}}$. We say that two number fields K_1, K_2 are **locally equivalent** if $\mathbf{A}_{K_1} \cong \mathbf{A}_{K_2}$.

Remark 3. The field K embeds diagonally into $\mathbf{A}_K$. The image is discrete and with respect to any Haar measure μ on $\mathbf{A}_K$, we have $\mu(\mathbf{A}_K/K) < \infty$; in fact $\mathbf{A}_K/K$ is compact.

There exist infinitely many pairs of locally equivalent, non-isomorphic number fields. The smallest example is a pair of degree 8 number fields. By definition, the number of real and complex embeddings of a pair of locally equivalent fields is the same and so the fields must have the same degree; they have the same discriminant, zeta function, and class number.

Example 7. Let K_1, K_2 be a pair of locally equivalent number fields. For each K_i, we denote the associated ring of integers by $\mathscr{O}_{K_i}$. The closure of $\mathscr{O}_{K_i}$ in $K_{v^i_{j,p}}$ is denoted by $\mathscr{O}_{v^i_{j,p}}$. The closure in $\mathbf{A}_{K_i}$, denoted by $\widehat{\mathscr{O}_{K_i}}$ is the product of these local completions. Set $\mathbf{U}(n,K)$ to be the subgroup of $\mathrm{GL}(n,K)$ of upper triangular, unipotent matrices with coefficients in K. The group $\mathbf{U}(n,\mathscr{O}_K)$ is the subgroup of $\mathbf{U}(n,K)$ of matrices with coefficients in $\mathscr{O}_K$. The group $\mathbf{U}(n,\mathscr{O}_K)$ is a finitely presented nilpotent group of step size $n-1$. The group $\mathbf{U}(n,\mathscr{O}_K)$ satisfies the congruence subgroup property and so $\mathbf{U}\widehat{(n,\mathscr{O}_K)} \cong \mathbf{U}(n,\widehat{\mathscr{O}_K})$. Since K_1,K_2 are locally equivalent, $\widehat{\mathscr{O}_{K_i}} \cong \widehat{\mathscr{O}_{K_2}}$ and so $\mathbf{U}(n,\mathscr{O}_{K_1})$ and $\mathbf{U}(n,\mathscr{O}_{K_2})$ have isomorphic profinite completions.

Example 8. Let K_1,K_2 be a pair of locally equivalent number fields and define $\mathbf{B}(n,\mathscr{O}_{K_i})$ to be the subgroup of n by n upper triangular matrices with coefficients in $\mathscr{O}_{K_i}$. For $n=2$, this group is

$$\mathbf{B}(2,\mathscr{O}_K) = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} \ : \ \alpha \in \mathscr{O}_K^1,\ \beta \in \mathscr{O}_K \right\}.$$

The group $\mathbf{B}(n,\mathscr{O}_K)$ is virtually polycyclic and by work of Chahal, we have $\mathbf{B}\widehat{(n,\mathscr{O}_K)} \cong \mathbf{B}(n,\widehat{\mathscr{O}_K})$. In particular, if K_1,K_2 are locally equivalent, then $\mathbf{B}\widehat{(n,\mathscr{O}_{K_1})} \cong \mathbf{B}\widehat{(n,\mathscr{O}_{K_2})}$.

Example 9. Take K_1,K_2 locally equivalent and $\mathrm{SL}(n,\mathscr{O}_{K_1}),\mathrm{SL}(n,\mathscr{O}_{K_2})$. These groups have isomorphic profinite completions, provided $n>2$ by the congruence subgroup property, but are not isomorphic. In fact, in both this pair and the previous pair, the groups cannot have finite index subgroups that are isomorphic.

2.9 Lecture 12. *Products of representations*

Given a collection of fields F_i indexed by a set I, we have the associated product ring $F_I = \prod_i F_i$. Given an ultrafilter ω on I, we define the equivalence relation $\sim_\omega$ on F_I as follows: $(a_i) = a \sim_\omega b = (b_i)$ if and only if $R_{a,b} = \{i \in I \ : \ a_i = b_i\} \in \omega$. We denote the equivalence classes in F_I by $[\cdot]_\omega$ and note that since ω is an ultrafilter, the ideal $\mathfrak{m}_\omega = [0]_\omega$ is a maximal ideal. The quotient field $F_I/\mathfrak{m}_\omega$ is called the **ultraproduct** of the F_i with respect to the ultrafilter ω and we denote $F_\omega = F_I/\mathfrak{m}_\omega$.

If I is finite, every ultrafilter on I is principal. In particular, if ω is an ultrafilter then there exists $i_0 \in I$ such that ω is the principal filter on the subset $\{i_0\}$. It is straightforward to see that in this case m_ω is $\ker \pi_{i_0}$ where $\pi_{i_0} \colon F_i \to F_{i_0}$ is projection onto i_0th factor. In particular, $F_\omega = F_{i_0}$. If I is infinite and ω is principal, we will have $F_\omega = F_{i_0}$ as in the finite case. In the event I is infinite and ω is a non-principal ultrafilter, we call the ultraproduct F_ω a **non-trivial ultraproduct**. We denote the projection ring homomorphism $\pi_\omega \colon F_I \to F_\omega$.

Remark 4. There is a bijection between filters on I and ideals in the product ring F_I. We see that when I is infinite, the maximal ideals of F_I split into two families. The ideals associated to principal ultrafilters are precisely the kernels of the projection onto single factors. The maximal ideals associated to non-principal ultrafilters are more mysterious. Each non-principal ultrafilter is a maximal filter that contains the cofinite or Fréchet filter.

Given an ultrafilter ω on I, for any subset I_1 of I, either $I_1 \in \omega$ or $I - I_1 \in \omega$. We define a finitely additive measure μ_ω on I by

$$\mu_\omega(A) = \begin{cases} 1, & A \in \omega \\ 0, & A \notin \omega. \end{cases}$$

We see that $\pi_\omega(a) = \pi_\omega(b)$ if and only if $\mu_\omega(R_{a,b}) = 1$. The ultraproduct F_ω only sees the algebraic structure that holds for almost every factor where almost every is measured with respect to the measure μ_ω.

Remark 5. One can define ultraproducts of various other sets with structure. Ultraproducts of sets, groups, rings, vector spaces, .etc.

Given ring homomorphisms $r_i\colon R \to F_i$, we have the associated product homomorphism $r\colon R \to \prod_i F_i$ and the associated ultraproduct homomorphism given by $\pi_\omega \circ r$. Given a group Γ, an indexing set I, and collection of fields F_i indexed by I, and a collection of homomorphisms $\psi_i\colon \Gamma \to \mathrm{GL}(n, F_i)$ for a fixed $n \in \mathbf{N}$, we have the product homomorphism $\Psi\colon \Gamma \to \prod_i \mathrm{GL}(n, F_i)$ and the associated ultraproduct representations $\Psi_\omega\colon \Gamma \to \mathrm{GL}(n, F_\omega)$.

Given $n \in \mathbf{N}$ and a group Γ, we say that Γ is **residually** GL_n if for each non-trivial $\gamma \in \Gamma$, there exists a field F_γ and a homomorphism $\psi_\gamma\colon \Gamma \to \mathrm{GL}(n, F_\gamma)$ such that $\psi_\gamma(\gamma) \neq 1$. We say that Γ is **fully residually** GL_n if for each finite subset $S \subset \Gamma$ of non-trivial elements, there exists a field F_S and a homomorphism $\psi_S\colon \Gamma \to \mathrm{GL}(n, F_S)$ such that $\psi_S(\gamma) \neq 1$ for all $\gamma \in S$.

Lemma 2.48. *Let Γ be a finitely generated group and $n \in \mathbf{N}$. Then Γ is fully residually GL_n if and only if there exists a field F and a injective homomorphism $\psi\colon \Gamma \to \mathrm{GL}(n, F)$.*

Proof. We first prove the converse direction and assume that $\psi\colon \Gamma \to \mathrm{GL}(n, F)$ is an injective homomorphism for some field F. For simplicity, we will assume that $\mathrm{char}(F) = 0$ and let K be the ring generated over $\mathbf{Q}$ by the matrix coefficients of $\psi(\gamma_i)$ where $\{\gamma_1, \dots, \gamma_t\}$ is a fixed finite generating set of Γ. Note that Q is independent of the generating set. Since $K/\mathbf{Q}$ is finitely generated, K is isomorphic to the field of rational functions in the variables $x_1, \dots, x_s$ and with coefficients in a number field $L/\mathbf{Q}$. The ring R generated over $\mathbf{Z}$ is isomorphic to the ring of polynomials in $x_1, \dots, x_s$ with coefficients in $S/\mathscr{O}_L$, where S is $\mathscr{O}_L$ with a finite number of inverted primes and with a finite number of inverted polynomials. In particular, the ring is residually finite. That Γ is fully residually GL_n is straightforward.

For the direct implications, we begin by ordering $\Gamma = \{\gamma_0 = 1, \gamma_1, \gamma_2, \dots\}$ and set $S_j = \{\gamma_1, \dots, \gamma_j\}$ for $j \in \mathbf{N}$. By hypothesis, for each $j \in \mathbf{N}$, there exists a field F_j and a homomorphism $\psi_j \colon \Gamma \to \mathrm{GL}(n, F_j)$ such that $\psi_j(\gamma_i) \neq 1$ for each $1 \leq i \leq j$. If Γ is finite, then we will eventually obtain an injective homomorphisms. Consequently, we can assume Γ is infinite. For any non-principal filter ω, we have the associated ultraproduct representation $\Psi_\omega \colon \Gamma \to \mathrm{GL}(n, F_\omega)$. For each $i_1, i_2 \in \mathbf{N}$, we have $i_{1,2} \in \mathbf{N}$ such that $\gamma_{i_{1,2}} = \gamma_{i_1}\gamma_{i_2}^{-1}$. For all $j \geq i_{1,2}$, we see that $\psi_j(\gamma_{i_1}) \neq \psi_j(\gamma_{i_2})$. As this is a cofinite set, we see that $\mu_\omega(R_{\gamma_{i_1},\gamma_{i_2}}) = 0$. Hence, $\psi_\omega(\gamma_1) \neq \psi_\omega(\gamma_2)$ and so ψ_ω is injective. ♠

Remark 6. The above proof actually shows that if Γ is fully residually GL_n, then there exists fields $\{F_i\}_{i \geq 1}$ and homomorphisms $\psi_i \colon \Gamma \to \mathrm{GL}(n, F_i)$ such that for *any* non-principal ultrafilter ω on $\mathbf{N}$, the ultraproduct representation $\Psi_\omega \colon \Gamma \to \mathrm{GL}(n, F_\omega)$ is injective.

One can prove Lemma 2.48 using the Baire Category Theorem and some complex geometry. The set $\mathrm{Hom}(\Gamma, \mathrm{GL}(n, \mathbf{C}))$ is an complex affine variety with finitely many irreducible components. Ordering Γ as before, for each $S_j = \{\gamma_i\}_{i=1}^{j}$, there exists $\rho_j \in \mathrm{Hom}(\Gamma, \mathrm{GL}(n, \mathbf{C}))$ such that $\rho_j(\gamma_i) \neq 1$ for $1 \leq i \leq j$. Since $\mathrm{Hom}(\Gamma, \mathrm{GL}(n, \mathbf{C}))$ has finitely many irreducible components, by the Pigeonhole Principal, one of the irreducible components must contain ρ_j for infinitely many $j \in \mathbf{N}$. Let $X \subset \mathrm{Hom}(\Gamma, \mathrm{GL}(n, \mathbf{C}))$ be such an irreducible component. For each non-trivial $\gamma \in \Gamma$, we have the analytic function $\mathrm{Eval}_\gamma \colon X \to \mathrm{GL}(n, \mathbf{C})$ given by $\mathrm{Eval}_\gamma(\rho) = \rho(\gamma)$. By selection of X, the function Eval_γ is non-constant and so $(\mathrm{Eval}_\gamma(1))^{-1}$ is nowhere dense. By the Baire Category Theorem, $B = \bigcup_{\gamma \neq 1} (\mathrm{Eval}_\gamma(1))^{-1}$ is nowhere dense and so $X - B$ is non-empty. By construction of $X - B$, for each $\rho \in X - B$, we see that ρ is injective.

In some sense, the difference between these proofs is that the Baire Category proof yields an existence result while the ultraproduct proof actually produces a faithful representation. However, this is somewhat misleading since one can actually produce an "explicit" faithful homomorphism via the Baire Category Theorem. If R_X is the ring of regular functions on the irreducible component X from the above proof, there is a representation $\rho_{taut} \colon \Gamma \to \mathrm{GL}(n, R_X)$ called the tautological representation. For each point $\rho \in X$, we can evaluate any element of R_X at ρ. For each $\gamma \in \Gamma$, we have $\rho_{taut}(\gamma) = (\alpha_{i,j})$ where $\alpha_{i,j} \in R_X$. For each $\rho \in X$, we have $\rho_{taut}(\gamma)(\rho) = (\alpha_{i,j}(\rho)) \in \mathrm{GL}(n, \mathbf{C})$, and we have $\rho_{taut}(\gamma)(\rho) = \rho(\gamma)$; in some sense, this is the definition of ρ_{taut}. That is, every representation $\rho \in X$ is a specialization/evaluation of the tautological representation. By selection of X, we know that there exists a faithful representation $\rho \in X$. Since ρ is a specialization of ρ_{taut}, it follows that ρ_{taut} is faithful.

Chapter 3

Group Cohomology

In this module, we develop the basic foundations of group cohomology. This topic can be developed through several different view points, and we will take the most concrete approach, working directly with cocycles. This choice was made mostly due to time constraints. Derived category theory and the concept of derived functors is a more contemporary view and has many advantages. If time allows, we will devote one or two lectures to the derived categorical approach through the derived functors Ext^i and Tor_i for $\mathrm{Hom}(\cdot,\cdot)$. This approach can be extended well beyond the category of G–modules.

3.1 Lecture 13. *Semidirect Products and Group Extensions*

Let H,K be groups and $\varphi\colon H \to \mathrm{Aut}(K)$ a homomorphism of H to the automorphism group of K. We can define a new group $K \rtimes_\varphi H$ by setting $K \rtimes_\varphi H = K \times H$, as a set, with group operation given by

$$(k_1,h_1) \cdot_{K\rtimes_\varphi H} (k_2,h_2) = (k_1 \cdot_K (\varphi(h_1)(k_2)), h_1 \cdot_H h_2)$$

where $\varphi(h_1)(k_2)$ is the image of k_2 under the automorphism $\varphi(h_1)$. As is standard, we use juxtaposition to denote the group operations of K, H, and $K \rtimes_\varphi H$, unless clarity mandates otherwise. The group $K \rtimes_\varphi H$ is the **semidirect product** of K,H. We have two inclusion maps $\iota_K, \iota_H\colon K,H \to K \rtimes_\varphi H$, which one can check are both injective homomorphisms. The the image of K under ι_K is a normal subgroup of $K \rtimes_\varphi H$, and so we have a quotient homomorphism $\psi_L\colon K \rtimes_\varphi H \to K \rtimes_\varphi H/\iota_K(K)$. One can check that the quotient group is isomorphic to H. In particular, we have the short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & K \arrow[r, "\iota_K"] & K \rtimes_{\varphi} H \arrow[r, "\psi_K"] & H \arrow[r] & 1. \end{tikzcd}$$

The inclusion homomorphism ι_H is a normalized section of ψ_K (i.e., a left inverse of ψ_K) and yields the commutative diagram

$$\begin{tikzcd} K \rtimes_{\varphi} H \arrow[r, bend left, "\psi_K"] & H \arrow[l, bend left, "\iota_H"] \arrow[loop right, "\mathrm{Id}_H"] \end{tikzcd}$$

The semidirect product $K \rtimes_{\varphi} H$ is also called the **external** or **outer semidirect product**.

Remark 7. If $\varphi \colon H \to \mathrm{Aut}(K)$ is the trivial homomorphism, then $K \rtimes_{\varphi} H \cong K \times H$.

If G is a group with a normal subgroup K, we have an induced homomorphism $\mathrm{Ad}_{K,G} \colon G \to \mathrm{Aut}(K)$ given by $\mathrm{Ad}_{K,G}(g)(k) = gkg^{-1}$ (the reader should be warned that convention for conjugation in these notes is not consistent but is (hopefully) locally consistent). If $H \subset G$ is a subgroup of G, the restriction of $\mathrm{Ad}_{k,G}$ to H yields a homomorphism $\varphi_{H,K} \colon H \to \mathrm{Aut}(K)$. If $H \cap K = \{1\}$ and $HK = G$, then one can show that $G \cong K \rtimes_{\varphi_{H,K}} H$. In particular, G is semidirect product and is sometimes called the **internal** or **inner semidirect product**. In total, these two different concepts of a semidirect product are related through the diagram below:

$$\begin{tikzcd} 1 \arrow[r] & K \arrow[r, "\iota_K"] \arrow[d, leftrightarrow] & G \arrow[r, "\psi_K"] \arrow[d, leftrightarrow] & H \arrow[r] \arrow[l, bend right, "\iota_H"'] \arrow[loop above, "\mathrm{Id}_H"] \arrow[d, leftrightarrow] & 1 \\ 1 \arrow[r] & K \arrow[r, "\iota_K"'] & K \rtimes_{\varphi_{H,K}} H \arrow[r, "\psi_K"'] & H \arrow[r] \arrow[l, bend left, "\iota_H"] \arrow[loop below, "\mathrm{Id}_H"] & 1 \end{tikzcd}$$

Example 10. Consider the following group. Set $G = \mathbf{Z} \times \mathbf{Z}^2$ which we view in coordinates as pairs $(t,(x,y)) = (t,z)$. We define the binary operation

$$(t_1,(x_1,y_1)) \cdot (t_2,(x_2,y_2)) = (t_1 + t_2 + 2\omega((x_1,y_1),(x_2,y_2)),(x_1+x_2,y_1+y_2))$$

where $\omega((x_1,y_1),(x_2,y_2)) = x_2y_1 - x_1y_2$. If we view $z = x+iy$, then

$$\omega(z_1,z_2) = \mathrm{Im}(z_1\overline{z_2})$$

where $\overline{\cdot}$ denotes complex conjugation and $\mathrm{Im}(z) = y$ is the imaginary part of z. One can check that G is a group with this binary operation. The subgroup $K = \{(t,(0,0)) \,:\, t \in \mathbf{Z}\}$ is a normal subgroup of G, K is isomorphic to $\mathbf{Z}$, and the quotient group $G/K = H$ is isomorphic to $\mathbf{Z}^2$. We have the short exact sequence

$$1 \longrightarrow K \xrightarrow{\iota_K} G \xrightarrow{\psi_K} H \longrightarrow 1.$$

We say a function $s\colon H \to G$ is a **section of** ψ_K if $\psi_K \circ s = \mathrm{Id}_H$, and we will assume that $s(1) = 1$; such a section is sometimes said to be normalized. One can check that there is no choice of section s of ψ_K that is a homomorphism. For instance, consider the section s_0 given by $s_0(z) = (0,z)$. We see that if $z_1 = (x_1,y_1)$ and $z_2 = (x_2,y_2)$, then

$$s_0(z_1z_2) = (0, z_1+z_2), \quad s_0(z_1)s_0(z_2) = (2\omega(z_1,z_2), z_1+z_2).$$

The function ω measures the failure of s_0 to be a homomorphism. The function ω is an example of a 2–cocycle. It is also a symplectic 2–form on $\mathbf{R}^2$, which we saw is also the imaginary part of the standard hermitian inner product on $\mathbf{C}$. This symplectic form is also the volume form $\mathbf{R}^2$ or the determinant function on $\mathrm{Mat}(2,\mathbf{R})$.

Before beginning a general treatment on group cohomology, we first consider a concrete problem in group theory. Given that we have not yet discussed what group cohomology is, one can consider this discussion as a special case of the theory we will develop shortly. The reader that is unfamiliar with cohomology theory should reread these special cases after reading over the general theory in the next section; see Lecture 14.

Let $1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\psi_A} G \longrightarrow 1$ be a short exact sequence of groups with A abelian. Since A is abelian, the homomorphism $\mathrm{Ad}_{A,E}\colon E \to \mathrm{Aut}(A)$ descends to the quotient $E/A = G$, and so we have a homomorphism $\varphi\colon G \to \mathrm{Aut}(A)$. We will refer to A with this action as a ***G*–module**. For a (normalized) section $s\colon G \to E$ of ψ_A, we obtain an explicit description of the action via

$$\varphi(g)a = \iota^{-1}(s(g)\iota(a)s(g)^{-1}).$$

We say that E, as above, is an **extension of G by A with action φ**. In the event A (or more accurately, $\iota(A)$) is central, we say that E is a **central extension of G of A**. In the case of a central extension, the homomorphism φ is trivial. Finally, we say that an extension E is **split** if there exists a section s of ψ_K that is also a group homomorphism; note it must be normalized. We call any section s that is a also homomorphism a **splitting of E**. The following lemma is a consequence of the discussion above on semidirect products.

Lemma 3.1. *Let E be an extension of G by A with action φ. Then the following are equivalent:*

(a) E is split.

(b) There exists a subgroup G' of E such that $G' \cap \iota(A) = \{1\}$ and $G'\iota(A) = E$.

(c) E is isomorphic to the semidirect product $A \rtimes_\varphi G$.

From the viewpoint of extensions, each action $\varphi\colon G \to \mathrm{Aut}(A)$ gives rise to a unique split extension. However, the splitting (i.e., the section s from the definition) need not be unique. In the case that G acts trivially on A, we know that $E = A \times G$; note that we are assuming E is split. Given a splitting $s\colon G \to A \times G$, we have an associated homomorphism $\eta_s\colon G \to A$ given by $\eta_s(g) = \mathrm{P}_A(s(g))$. We see that $s(g) = (\eta_s(g), g)$ and so the different splittings of the split extension E are in bijection with $\mathrm{Hom}(G,A)$ when A is a trivial G–module.

If the G–action is not trivial, the different splittings of the split extension $A \rtimes_\varphi G$ are parameterized in a more complicated way. Given a splitting $s\colon G \to A \rtimes_\varphi G$, we have the exact sequence

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota"] & A \rtimes_\varphi G \arrow[r, "\psi_A"] & G \arrow[r] \arrow[l, bend left, "s"] & 1. \end{tikzcd}$$

The homomorphism $s\colon G \to A \rtimes_\varphi G$ is of the form $s(g) = (d(g), g)$ where $d\colon G \to A$ is a function. Since s is a homomorphism, we see that

$$s(gh) = (d(gh), gh) = (d(g) + \varphi(g)d(h), gh) = s(g)s(h),$$

and so

$$d(gh) = dg + \varphi(g)d(h).$$

A function $d\colon G \to A$ is called a **derivation** or **crossed homomorphism** if $d(gh) = d(g) + \varphi(g)d(h)$ for all $g,h \in G$; if necessary for clarity, we will refer to d as a derivation relative to the action φ.

Exercise 35. Prove that $s\colon G \to A \rtimes_\varphi G$ is a splitting if and only if $s(g) = (d(g), g)$ for some derivation d.

Our present interest will be classifying the splittings s up to conjugation. We say two splittings s_1, s_2 of $A \rtimes_\varphi G$ are **conjugate** if there exists $a \in A$ such that

$$s_1(g) = \iota(a)s_2(g)\iota(a)^{-1}.$$

Note that if s_1, s_2 are conjugate and $s_i(g) = (d_i(g), g)$ for $i = 1, 2$, then

$$\iota(a)s_2(g)\iota(a)^{-1} = (a,1)(d_2(g),g)(-a,1) = (a + d_2(g) - \varphi(g)a, g).$$

In particular, if s_1, s_2 are conjugate, then

$$d_1(g) = a + d_2(g) - \varphi(g)a$$

or

$$d_2(g) - d_1(g) = \varphi(g)a - a.$$

We say that a derivation d is **principal** if there exists $a_0 \in A$ such that $d(g) = \varphi(g)a_0 - a_0$. Set $D(G,A)$ to be the group of derivations of G into A and $P(G,A)$, the group of principal derivations. From above, we see that if s_1, s_2 are conjugate splittings with associated derivations d_1, d_2, then $d_2 - d_1$ is a principal derivation. Conversely, if $d_2 - d_1$ is principal, then s_1, s_2 are coinjugate. In particular, $H^1_\varphi(G,A) = D(G,A)/P(G,A)$ parameterizes the splittings of E up to conjugation. The group $H^1_\varphi(G,A)$ is the **first cohomology of G with coefficients in the G–module** A, and typically, one views A as a G–module and we denote $H^1_\varphi(G,A)$ simply by $H^1(G,A)$.

Remark 8. Given a group G and any commutative ring R with identity, the **R–group ring** $R[G]$ is defined to be

$$\left\{ \sum_{i=1}^{n} r_i g_i \ : \ r_i \in R, \ g_i \in G \right\}$$

with additive and multiplicative operations given by ”coordinate” addition and ”polynomial” multiplication. For $R = \mathbf{Z}$, we have a ring homomorphism $\varepsilon \colon \mathbf{Z}[G] \to \mathbf{Z}$ given by

$$\varepsilon\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i.$$

In fact, one can construct an identical ring homomorphism for *any* commutative ring R with identity. The kernel of this ring homomorphism is called the **augmentation ideal** and will be denoted by I_G. The augmentation ideal is a G–module by restricting the G–module structure of $\mathbf{Z}[G]$ to I_G. We have a derivation $D_G \colon G \to I_G$ given by $D_G(g) = g - 1$, which is simply the principal derivation associated to 1. Given any G–module A and a derivation $d \colon G \to A$, there exists a unique G–module homomorphism $\lambda \colon I \to A$ such that $d = f \circ D_G$. In particular,

$D(G,A) = \mathrm{Hom}_{\mathbf{Z}[G]}(I_G, A)$ and we have the commutative diagram:

$$\begin{tikzcd}
G \arrow[rr, bend left, "D_G"] \arrow[dr, bend right, "d"'] & & \mathbf{Z}[G] \arrow[dl, bend left, "f"] \\
& A &
\end{tikzcd}$$

We now return to our investigation of extensions of G by a fixed G–module A. Given such an extension E, we have the short exact sequence

$$1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{P} G \longrightarrow 1.$$

Note that we are fixing the action of G on A and so $\mathrm{Ad}_{A,E} \colon E \to \mathrm{Aut}(A)$ descends to $\varphi \colon G \to \mathrm{Aut}(A)$. Fixing a normalized section $s \colon G \to E$ of P, for each $g,h \in G$, we have $s(g)s(h) = f(g,h)s(gh)$ for some $f(g,h) \in E$. Since s is a section of P, $f(g,h) \in \iota(A)$, which we can identify with A, and so $f(g,h) \in A$. In particular, we will view the function f as $f \colon G \times G \to A$. Since s is normalized, it follows that $f(g,1) = f(1,g) = 0$ for all $g \in G$. Note that we are viewing G as a multiplicative group and A as an additive group, and so denote the identities by $1,0$, respectively.

Remark 9. Though we have insisted that G–modules be abelian, the example of the $\mathbf{Z}$–group ring is an example of a possibly non-abelian G–module. When G is a finite group, the $\mathbf{Q}$–algebra $\mathbf{Q}[G]$ is semisimple $\mathbf{Q}$–algebra and so by the Wedderburn Structure Theorem, is isomorphic to a sum of algebras $\mathrm{Mat}(d_j, D_j)$ where $d_j \in \mathbf{N}$ and D_j is a $\mathbf{Q}$–division algebra. Over $\mathbf{C}$ (or $\overline{\mathbf{Q}}$), $\mathbf{C}[G]$ is isomorphic to a direct sum of matrix algebras. The individual factors in this algebra encode the irreducible representation theory of the group G. Taking this algebra over fields of positive characteristic, the associated algebra encodes information about the characteristic p representation theory, where p is the characteristic of the given field. These are very natural G–modules, whether G is finite or infinite. When G is infinite, the $\mathbf{C}$–group algebra (or the group algebra over other reasonable rings) encodes information about the representation theory. However, one can now have irreducible, infinite dimensional representations, and such representations are important in understanding the structure of G. Invariants like group C^*–algebras and group von Neumann algebras are important examples of completions of $\mathbf{C}[G]$ that encode information about the unitary representation theory of G. The group algebra, like the profinite completion, the quotients of G by its lower central or derived theory, and the cohomology of a group G, all are natural objects that encode information about the representation theory of G.

We have a set theoretic bijection between $A \times G$ and E given by $(a,g) \mapsto \iota(a)s(g)$. We define a group operation on $A \times G$ by

$$(a_1,g_1)(a_2,g_2) = (a_1 + \varphi(g_1)a_2 + f(g_1,g_2), g_1g_2).$$

It is straightforward to check that E is isomorphic with $A \times G$ but with this new group operation. The associativity of the group operation forces an additional condition on the function f. Specifically,

$$f(g,h) + f(gh,k) = \varphi(g)f(h,k) + f(g,hk)$$

for all $g,h,k \in G$.

Exercise 36. Let G be a group and A a G–module. If $f\colon G \times G \to A$ is a function that satisfies

$$f(g,1) = f(1,g) = 0, \quad f(g,h) + f(gh,k) = \varphi(g)f(h,k) + f(g,hk) \tag{3.1}$$

for all $g,h,k \in G$, prove that $E_f = A \times G$ with binary operation

$$(a_1,g_1)(a_2,g_2) = (a_1 + \varphi(g_1)a_2 + f(g_1,g_2), g_1g_2) \tag{3.2}$$

is a group.

Functions f that satisfy (3.1) are called normalized 2–cocycles. Of course, the function f depends on the choice of a normalized section. Every normalized section s' is given by $s'(g) = \iota(c(g))s(g)$ for some function $c\colon G \to A$ with $c(1) = 0$; this is a normalized 1–cocycle. The 2–cocycle associated to the section s' is given by

$$f'(g,h) = c(g) + \varphi(g)c(h) - c(gh) + f(g,h).$$

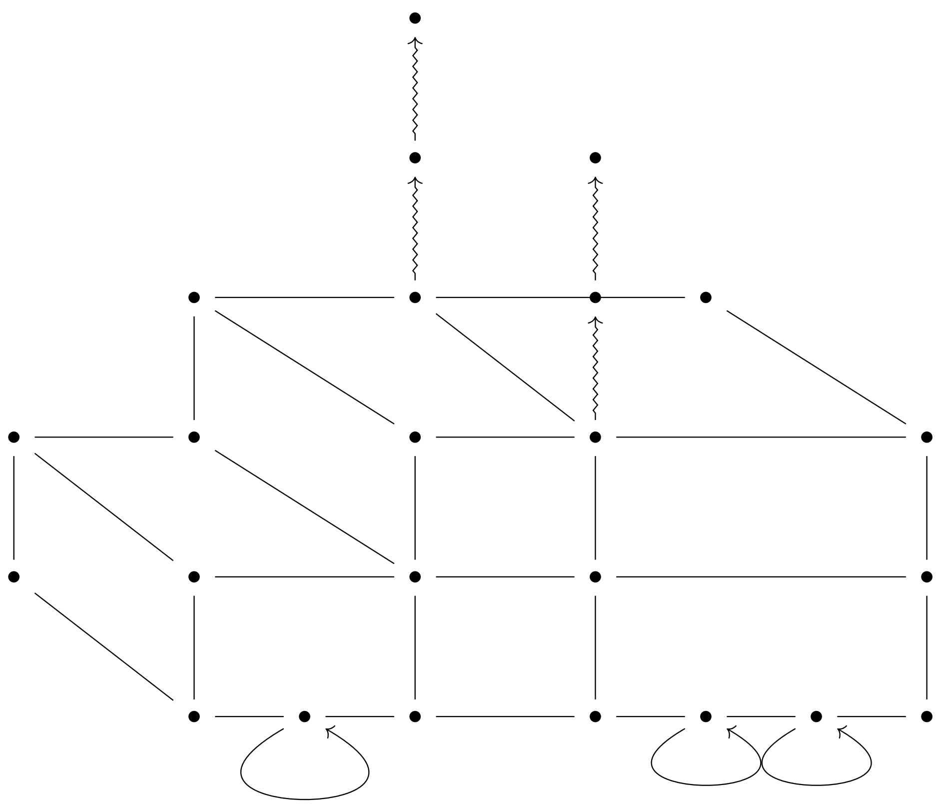
We say that a 2–cocycle f is a **coboundary** if there exists $c\colon G \to A$ with $c(1) = 0$ such that

$$f(g,h) = \varphi(g)c(h) - c(g,h) + c(g)$$

for all g,h. If $Z_2(G,A)$ is the group of normalized 2–cocycles satisfying (3.1) and $B_2(G,A)$ is the subgroup of coboundary 2–cocyles, we define $H^2(G,A) = Z_2(G,A)/B_2(G,A)$.

Exercise 37. Prove that if f, f' are normalized 2–cocycles such that $f - f'$ is a coboundary, then $E_f, E_{f'}$ are isomorphic.

We end this lecture with an exercise in using the package tikzcd. Below is a truck that was made with that package. See this document for more on this package. It is handy for making more ”exotic” diagrams:



3.2 Lecture 14. *Group Cohomology With Abelian Coefficients*

Today, we develop a cohomology theory for groups G with coefficients in a G–module A. We will proceed concretely using cocycles and coboundary maps in order to produce a complex of abelian groups $\mathscr{C} = \{C_k(G,A), \delta_k\}_{k\geq 0}$ from which we will define the cohomology groups $H^k(G,A)$.

Let G be a (discrete) group and A a G–module. Recall that have a function $G \times A \to A$ that satisfies

$$(g_1 g_2)a = g_1(g_2 a), \quad g \cdot 0 = 0, \quad g(a+b) = ga + gb$$

all $g, g_1, g_2 \in G$ and $a, b \in A$. For each $k \geq 0$, we define $C_k(G,A)$ to be the set of functions $f\colon G^k \to A$ and note that $C_k(G,A)$ is a group via point-wise addition. We call $C_k(G,A)$ the group of (inhomogenous) k–cochains. Note that our present convention with be to view G^0 as a single point and so $C_0(G,A) = A$.

For each $k \geq 0$, we have a coboundary map $d_k\colon C_k(G,A) \to C_{k+1}(G,A)$ defined by

$$d_k(f)(g_1,\ldots,g_{k+1}) \stackrel{\text{def}}{=} \varphi(g_1)f(g_2,\ldots,g_{k+1}) + (-1)^{k+1}f(g_1,\ldots,g_k) + \sum_{j=1}^{k}(-1)^j f(g_1,\ldots,g_{j-1},g_jg_{j+1},\ldots,g_{k+1}).$$

For $k = 0$, each $f \in C_0(G,A)$ is identified with a fixed $a_f \in A$ and $d_0(f)(g) = \varphi(g)a_f - a_f$. For $k = 1$ and $f \in C_1(G,A)$, we have

$$d_1(f)(g_1,g_2) = \varphi(g_1)f(g_2) - f(g_1g_2) + f(g_1).$$

Lemma 3.2. *If G is a (discrete) group and A a G–module, then $d_{k+1} \circ d_k(f) = 0$ for all $k \geq 0$ and $f \in C_k(G,A)$.*

Proof. One can check this using the definition of d_k. ♠

Since $d_{k+1} \circ d_k$ is the trivial map, it follows that $\mathrm{Image}(d_k) \subset \ker d_{k+1}$. We define $B_k(G,A) = \mathrm{Image}(d_{k-1})$, $Z_k(G,A) = \ker d_k$, and $H^k(G,A) \stackrel{\text{def}}{=} Z_k(G,A)/B_k(G,A)$. We call $B_k(G,A)$ the group of coboundaries and call $H^k(G,A)$ the **kth cohomology group of G with coefficients in A**.

Example 11 ($H^0(G,A)$)**.** For $k = 0$, as before, each element of $f \in C_0(G,A)$ is identified with a fixed $a_f \in A$. From the definition of d_0, we see that

$$d_0(f)(g) = \varphi(g)a_f - a_f,$$

and so $f \in \ker d_0$ if and only if $\varphi(g)a_f - a_f = 0$ for all $g \in G$. In particular, $f \in \ker d_0$ if and only if a_f is fixed by every $g \in G$. We denote the G–submodule of A of G–fixed points by A^G. Since $B_0(G,A) = 0$, we see that $H^0(G,A) = \ker d_0/B_0(G,A) = A^G$.

Lemma 3.3. *If A is a trivial G–module, then $H^1(G,A) = \mathrm{Hom}(G,A)$.*

Proof. To verify the lemma, we will determine $Z_1(G,A)$ and $B_1(G,A)$ when A is a trivial G–module. Above, we computed d_0 and so $d_0(f)(g) = \varphi(g)a_f - a_f$ where $a_f \in A$ is the element of A associated to f. Since G acts trivially on A, we have $\varphi(g)a_f = a_f$ and so $d_0(f) = 0$. Hence, $B_1(G,A) = 0$. We also computed d_1 and have

$$d_1(f)(g_1,g_2) = \varphi(g_1)f(g_2) - f(g_1g_2) + f(g_1).$$

As before, since the G–action is trivial, we have $\varphi(g_1)f(g_2) = f(g_2)$, and so the above simplifies in this case to $d_1(f)(g_1,g_2) = f(g_1) + f(g_2) - f(g_1g_2)$. If $f \in Z_1(G,A)$, then $d_1(f)$ is zero and so $f(g_1) + f(g_2) = f(g_1g_2)$. In particular, $f \in \mathrm{Hom}(G,A)$. As the reverse containment also holds, we have $Z_1(G,A) = \mathrm{Hom}(G,A)$. Combining this equality with the definition of $H^1(G,A)$ and our computation of $B_1(G,A)$ yields $H^1(G,A) = \mathrm{Hom}(G,A)$. ♠

Example 12. Consider $G = \mathbf{Z}$ and $A = \mathbf{Z}$, viewed as a trivial $\mathbf{Z}$–module. We see that $H^0(\mathbf{Z},\mathbf{Z}) = \mathbf{Z}$ since this is a trivial module. From above, $H^1(\mathbf{Z},\mathbf{Z}) = \mathrm{Hom}(\mathbf{Z},\mathbf{Z})$. Since every $f \in \mathrm{Hom}(\mathbf{Z},\mathbf{Z})$ is completely determined by $f(1)$ and this can take any $\mathbf{Z}$–value, we see that $H^1(\mathbf{Z},\mathbf{Z}) = \mathbf{Z}$. We assert that $H^2(\mathbf{Z},\mathbf{Z}) = 0$. To see this, note that given any short exact sequence

$$1 \longrightarrow \mathbf{Z} \longrightarrow E \xrightarrow{P} \mathbf{Z} \longrightarrow 1 ,$$

there is always a splitting.

Example 13. Consider $G = F_r$, a free group of rank r and $A = \mathbf{Z}$, viewed as a trivial module. As before, we have $H^0(F_r,\mathbf{Z}) = \mathbf{Z}$ and $H^1(F_r,\mathbf{Z}) = \mathrm{Hom}(F_r,\mathbf{Z}) = \mathrm{Hom}(\mathbf{Z}^r,\mathbf{Z}) = \mathbf{Z}^r$. By the universal mapping property for free groups, any short exact sequence

$$1 \longrightarrow \mathbf{Z} \longrightarrow E \xrightarrow{P} F_r \longrightarrow 1$$

has a splitting and so $H^2(F_r,\mathbf{Z}) = 0$. To see this, take any section s of P and let $G = \langle s(x_1),\dots,s(x_r)\rangle$ be the subgroup generated by lifts of a free basis $\{x_1,\dots,x_r\}$ of F_r. The group G is generated by r elements and so we have a surjective homomorphism $\lambda\colon F_r \to G$. In particular, we have surjective homomorphism $F_r \to F_r$ given by $P \circ \lambda$. Since free groups are residually finite and hence hopfian, this must be an isomorphism. In particular, G is a free group of rank r and E is split.

Cohomology groups are functorial in both variables. We start with the functoriality in the second variable. Given a pair of G–modules A,B and homomorphism $\psi\colon A \to B$ of G–modules, given any $f \in C_k(G,A)$, we obtain $\psi \circ f \in C_k(G,B)$. In particular, we have $\psi_\star\colon C_k(G,A) \to C_k(G,B)$. It follows that $\psi_\star(Z_k(G,A)) \subset Z_k(G,B)$ and $\psi_\star(B_k(G,A)) \subset Z_k(G,B)$ and so we get an induced homomorphism $\psi_\star\colon H^k(G,A) \to H^k(G,B)$. More generally, if we have a short exact sequence of G–modules

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1 ,$$

we obtain a long exact sequence in cohomology groups.

Proposition 3.4. *Let G be a group and $1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$ be a short exact sequence of G–modules. Then there is a long exact sequence in cohomology group*

$$0 \longrightarrow H^0(G,A) \longrightarrow H^0(G,B) \longrightarrow H^0(G,C) \xrightarrow{\delta_0} H^1(G,A) \longrightarrow \dots$$

The group homomorphisms are induced by the short exact sequence except for $\delta_j\colon H^j(G,C) \to H^{j+1}(G,A)$ which are called the connecting homomorphisms.

The proof of Proposition 3.4 is an application of the previous discussion on the group homomorphisms induced by G–module homomorphisms and the snake lemma. The snake lemma is used in constructing the connecting homomorphisms. We briefly discuss the construction of the connecting homomorphisms. Given a short exact sequence of G–modules

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1,$$

for each $k \geq 0$, we have the commutative diagram with exact rows:

$$\begin{tikzcd}
 & \vdots \arrow[d, "d_{k-1,A}"] & \vdots \arrow[d, "d_{k-1,B}"] & \vdots \arrow[d, "d_{k-1,C}"] & \\
0 \arrow[r] & C_k(G,A) \arrow[r] \arrow[d, "d_{k,A}"] & C_k(G,B) \arrow[r] \arrow[d, "d_{k,B}"] & C_k(G,C) \arrow[r] \arrow[d, "d_{k,C}"] & 0 \\
0 \arrow[r] & C_{k+1}(G,A) \arrow[r] \arrow[d, "d_{k+1,A}"] & C_{k+1}(G,B) \arrow[r] \arrow[d, "d_{k+1,B}"] & C_{k+1}(G,C) \arrow[r] \arrow[d, "d_{k+1,C}"] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

We say that the (co)chain complexes $\{C_k(G,A), d_{k,A}\}$, $\{C_k(G,B), d_{k,B}\}$, and $\{C_k(G,C), d_{k,C}\}$ form a short exact sequence of chain complexes in this case. The snake lemma is not obviously applicable to our current setting though it is a quite standard application in contemporary mathematics. In order to apply the snake lemma, we construct the following commutative diagram:

$$\begin{tikzcd}
 & C_k(G,A)/B_k(G,A) \arrow[r] \arrow[d, "\alpha_k"] & C_k(G,B)/B_k(G,A) \arrow[r] \arrow[d, "\beta_k"] & C_k(G,C)/B_k(G,C) \arrow[r] \arrow[d, "\gamma_k"] & 0 \\
0 \arrow[r] & Z_{k+1}(G,A) \arrow[r] & Z_{k+1}(G,B) \arrow[r] & Z_{k+1}(G,C) &
\end{tikzcd} \tag{3.3}$$

The horizontal maps are induced by the short exact sequence in chain complexes. The vertical arrows are given by $x + B_k(G,\star) \mapsto d_k(x) \in Z_{k+1}(G,\star)$.

Exercise 38. Prove that (3.3) is commutative and exact.

The kernel of the vertical maps are (note $\star$ represents the greek analog on the left side)

$$\ker(\star_k) = Z_k(G,\star)/B_k(G,\star) = H^k(G,\star)$$

and the cokernel is

$$\operatorname{coker}(\star_k) = Z_{k+1}(G,\star)/B_{k+1}(G,\star) = H^{k+1}(G,\star)$$

by definition of the vertical maps and the definitions of $Z_k(G,\star)$, $B_k(G,\star)$. Given a diagram (3.3), the snake lemma asserts the existence of a (natural) homomorphism $\delta_k \colon \ker(\gamma_k) \to \operatorname{coker}(\alpha_k)$. The construction of the homomorphism δ_k is somewhat involved but is done via a diagram chasing argument; ”diagram chasing” has its own wiki entry. Indeed, the depiction of the diagram chasing argument gave the snake lemma its name, with its progression through the diagram similar to that of the Mayan snake deity (see the picture here):

$$
\begin{tikzcd}
 & \ker(\alpha_k) \arrow[d] & \ker(\beta_k) \arrow[d] & \ker(\gamma_k) \arrow[d] & \\
 & C_k(G,A)/B_k(G,A) \arrow[r] \arrow[d, "\alpha_k"] & C_k(G,B)/B_k(G,A) \arrow[r] \arrow[d, "\beta_k"] & C_k(G,C)/B_k(G,C) \arrow[r] \arrow[d, "\gamma_k"] & 0 \\
0 \arrow[r] & Z_{k+1}(G,A) \arrow[r] \arrow[d] & Z_{k+1}(G,B) \arrow[r] \arrow[d] & Z_{k+1}(G,C) \arrow[d] & \\
 & \operatorname{coker}(\alpha_k) & \operatorname{coker}(\beta_k) & \operatorname{coker}(\gamma_k) &
\end{tikzcd}
$$

The connecting homomorphism goes through the path:

$$
\begin{tikzcd}
 & & \ker(\gamma_k) \arrow[d] \arrow[dddll, bend right, "\delta_k"'] \\
 & C_k(G,B)/B_k(G,A) \arrow[r] \arrow[d, "\beta_k"] & C_k(G,C)/B_k(G,C)] \\
Z_{k+1}(G,A) \arrow[r] \arrow[d] & Z_{k+1}(G,B) & \\
\operatorname{coker}(\alpha_k) & &
\end{tikzcd}
$$

In applications of the long exact sequence of cohomology groups associated to a short exact sequence of G–modules, it is important to understand the connecting homomorphisms.

If $\rho\colon G \to G'$ is a group homomorphism and A is an G'–module, we get can view A also as a G–module via ρ. Given a k–cochain $f'\colon (G')^k \to A$, we obtain $f\colon G^k \to A$ via $f(g_1,\dots,g_k) = f'(\rho(g_1),\dots,\rho(g_k))$, and so an induced homomorphism of abelian groups $\rho^\star\colon C_k(G',A) \to C_k(G,A)$. One can check that $\rho^\star(B_k(G',A)) \subset B_k(G,A)$ and $\rho^\star(Z_k(G',A)) \subset Z_k(G,A)$, and so we obtain an induced group homomorphism of cohomology groups $\rho^\star\colon H^k(G',A) \to H^k(G,A)$.

A special case of the above example is the case when ρ is an injective homomorphism, in which case we can view G as a subgroup of G' via ρ. In this case, we often disregard the homomorphism ρ. Specifically, if $G < G'$ is a subgroup and A is a G'–module, we can restrict the action of G' on A to the subgroup G. This yields a G–module structure on A. Given a k–cochain $f \in C_k(G',A)$, we can restrict the function f to the subset G^k, and so obtain a k–cocycle in $C_k(G,A)$. This yields an induced map $C_k(G',A) \to C_k(G,A)$. The claim that $B_k(G',A) \subset B_k(G,A)$ and $Z_k(G',A) \subset Z_k(G,A)$ are obvious in this case and we again obtain $\mathrm{Res}^k_{G',G} \colon H^k(G',A) \to H^k(G,A)$. This map is referred to as the restriction map.

There is a long exact sequence in cohomology groups associated to a short exact sequence of groups

$$1 \longrightarrow G \xrightarrow{\iota} G' \longrightarrow G/G' \longrightarrow 1$$

This long exact sequence gives rise to the so-called inflation-restriction sequence and is typically done via Lyndon/Serre–Hochschild/Grothendieck spectral sequences; see here, for instance. We will construct this sequence using projective resolutions first and, if time permits, also discuss how spectral sequences can be applied to obtain this sequence.

3.3 Lecture 15. *Projective Resolutions*

The next three sections follow Gille and Szamuely [6, Ch. 3] very closely. See here for more.

Let R be a ring with identity. We say that an R–module P is **projective** if given R–modules A, B and a surjective R–module homomorphism $\alpha \colon A \to B$, the induced R–module homomorphism $\alpha_\star \colon \mathrm{Hom}(P,A) \to \mathrm{Hom}(P,B)$ is surjective where $\alpha_\star(f) = \alpha \circ f$. Given an R–module A, a **projective resolution** of A is an exact sequence of projective R–modules

$$\cdots \xrightarrow{p_{i+2}} P_{i+1} \xrightarrow{p_{i+1}} P_i \xrightarrow{p_i} \cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} A$$

We denote the resolution by $P_\bullet = (P_i, p_i)$ and view $A = P_{-1}$. If $B_\bullet = (B_i, b_i)$

$$\cdots \xrightarrow{b_{i+2}} B_{i+1} \xrightarrow{b_{i+1}} B_i \xrightarrow{b_i} \cdots \xrightarrow{b_2} B_1 \xrightarrow{b_1} B_0 \xrightarrow{b_0} B$$

is an exact sequence of R–modules and $\alpha \colon A \to B$ is an R–module homomorphism, arguing inductively, one can define R–module homomorphisms $\alpha_i \colon P_i \to B_i$ that make the diagram

$$\begin{tikzcd}
\cdots \arrow[r, "p_{i+2}"] & P_{i+1} \arrow[r, "p_{i+1}"] \arrow[d, "\alpha_{i+1}"] & P_i \arrow[r, "p_i"] \arrow[d, "\alpha_i"] & \cdots \arrow[r, "p_2"] & P_1 \arrow[r, "p_1"] \arrow[d, "\alpha_1"] & P_0 \arrow[r, "p_0"] \arrow[d, "\alpha_0"] & A \arrow[d, "\alpha"] \\
\cdots \arrow[r, "b_{i+2}"'] & B_{i+1} \arrow[r, "b_{i+1}"'] & B_i \arrow[r, "b_i"'] & \cdots \arrow[r, "b_2"'] & B_1 \arrow[r, "b_1"'] & B_0 \arrow[r, "b_0"'] & B
\end{tikzcd}$$

commute. Moreover, if $\beta_i \colon P_i \to B_i$ are R–module homomorphisms for which the diagram

$$\begin{tikzcd}
\cdots \arrow[r, "p_{i+2}"] & P_{i+1} \arrow[r, "p_{i+1}"] \arrow[d, "\beta_{i+1}"] & P_i \arrow[r, "p_i"] \arrow[d, "\beta_i"] & \cdots \arrow[r, "p_2"] & P_1 \arrow[r, "p_1"] \arrow[d, "\beta_1"] & P_0 \arrow[r, "p_0"] \arrow[d, "\beta_0"] & A \arrow[d, "\alpha"] \\
\cdots \arrow[r, "b_{i+2}"'] & B_{i+1} \arrow[r, "b_{i+1}"'] & B_i \arrow[r, "b_i"'] & \cdots \arrow[r, "b_2"'] & B_1 \arrow[r, "b_1"'] & B_0 \arrow[r, "b_0"'] & B
\end{tikzcd}$$

commutes, then there exist R–module homomorphisms $\gamma_i \colon P_i \to B_{i+1}$ for $i \geq -1$ such that

$$\alpha_i - \beta_i = \gamma_{i-1} \circ p_i + b_{i+1} \circ \gamma_i.$$

This relationship requires this diagram

$$\begin{tikzcd}
 & P_i \arrow[r, "p_i"] \arrow[d, "\alpha_i"'] & P_{i-1} \arrow[dl, "\gamma_{i-1}"] \\
B_{i+1} \arrow[r, "b_{i+1}"] & B_i & \\
 & P_i \arrow[u, "\beta_i"'] \arrow[ul, "\gamma_i"] &
\end{tikzcd}$$

which is part of the full diagram:

$$\begin{tikzcd}
\cdots \arrow[r, "p_{i+2}"] & P_{i+1} \arrow[r, "p_{i+1}"] \arrow[d, "\alpha_{i+1}"] & P_i \arrow[r, "p_i"] \arrow[d, "\alpha_i"] \arrow[dl, "\gamma_i"] & \cdots \arrow[r, "p_2"] & P_1 \arrow[r, "p_1"] \arrow[d, "\alpha_1"] & P_0 \arrow[r, "p_0"] \arrow[d, "\alpha_0"] \arrow[dl, "\gamma_0"] & A \arrow[d, "\alpha"] \arrow[dl, "\gamma_{-1}"] \\
\cdots \arrow[r, "b_{i+2}"'] & B_{i+1} \arrow[r, "b_{i+1}"'] & B_i \arrow[r, "b_i"'] & \cdots \arrow[r, "b_2"'] & B_1 \arrow[r, "b_1"'] & B_0 \arrow[r, "b_0"'] & B \\
\cdots \arrow[r, "p_{i+2}"'] & P_{i+1} \arrow[r, "p_{i+1}"'] \arrow[u, "\beta_{i+1}"] & P_i \arrow[r, "p_i"'] \arrow[u, "\beta_i"] \arrow[ul, "\gamma_i"] & \cdots \arrow[r, "p_2"'] & P_1 \arrow[r, "p_1"'] \arrow[u, "\beta_1"] & P_0 \arrow[r, "p_0"'] \arrow[u, "\beta_0"] \arrow[ul, "\gamma_0"] & A \arrow[u, "\alpha"'] \arrow[ul, "\gamma_{-1}"]
\end{tikzcd}$$

Given a group G and a G–module A, we can define the cohomology groups $H^k(G,A)$ using projective resolutions. We start with a projective resolution (of G–modules) $P_\bullet = (P_k, p_k)$ of the trivial G–module $\mathbf{Z}$, say

$$\cdots \xrightarrow{p_{i+2}} P_{i+1} \xrightarrow{p_{i+1}} P_i \xrightarrow{p_i} \cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} \mathbf{Z}.$$

For each P_k, we have the abelian group $\mathrm{Hom}_G(P_k,A)$ of G–module homomorphisms and for each $k \geq 0$, we have homomorphisms $\delta^k \colon \mathrm{Hom}_G(P_k,A) \to \mathrm{Hom}_G(P_{k+1},A)$ given by

$$(\delta^k(f))(x) = (f \circ p_{k+1})(x).$$

One can check that $\mathscr{C} = (\mathrm{Hom}_G(P_k,A), \delta^k)$ is a complex of abelian groups and so we can define cohomology groups as before via $\ker \delta^k/\mathrm{Image}(\delta^{k-1})$. Specifically, we have

$$\cdots \xleftarrow{\delta^{k+1}} \mathrm{Hom}_G(P_{k+1},A) \xleftarrow{\delta^k} \mathrm{Hom}_G(P_k,A) \xleftarrow{\delta^{k-1}} \cdots \xleftarrow{\delta^1} \mathrm{Hom}_G(P_1,A) \xleftarrow{\delta^0} \mathrm{Hom}_G(P_0,A)$$

and define $H^k(G,A) = H^k(\mathrm{Hom}_G(P_\bullet,A))$. Projective resolutions give an alternative method for defining cohomology groups. We will not prove that these two different methods yield the same cohomology groups.

Remark 10. By taking an explicit projective resolution of $\mathbf{Z}$ as done below, one can recover the construction of the cohomology groups using cochains, cocycles, and coboundaries.

However, we will prove that $H^0(\mathrm{Hom}_G(P_\bullet,A)) = A^G$ and that these groups do not depend on the choice of the projective resolution $P_\bullet$ of $\mathbf{Z}$. First, we verify that $A^G = H^0(\mathrm{Hom}_G(P_\bullet,A))$. To that end, we have

$$P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} \mathbf{Z} \longrightarrow 0$$

and have $\mathrm{Image}(p_1) = \ker p_0$ by exactness. Since $\mathbf{Z}$ is a trivial G–module and any homomorphism of $Z \to A$ is determined by the image of 1, it follows that if $f\colon \mathbf{Z} \to A$ is a G–module homomorphism, then $f(1) \in A^G$. Moreover, for any element $a \in A^G$, we have a G–module homomorphism $f_a\colon \mathbf{Z} \to A$ given by $f_a(1) = a$. Hence, $\mathrm{Hom}_G(\mathbf{Z},A) = A^G$. Since p_0 is onto, every $f \in \mathrm{Hom}_G(\mathbf{Z},A)$ yields $f_0 \in \mathrm{Hom}_G(P_0,A)$ via $f_0 = f \circ p_0$. By exactness, $f_1 = f_0 \circ p_1$ is trivial, and so $f_0 \in \ker \delta^0$. It is straightforward to see that the converse also holds and so $\ker \delta^0 = A^G$.

We now prove that $H^k(\mathrm{Hom}_G(P_\bullet,A))$ does not depend on the choice of the projective resolution $P_\bullet$. To that end, let $Q_\bullet = (Q_j,q_j)$ be another projective resolution of $\mathbf{Z}$ as a trivial G–module. From above, we have G–module homomorphisms $\alpha_i\colon P_i \to Q_i$ and $\beta_i\colon Q_i \to P_i$ with the commutative diagram:

$$\begin{tikzcd}
\cdots \arrow[r, "p_{i+2}"] & P_{i+1} \arrow[r, "p_{i+1}"] \arrow[d, shift left, "\alpha_{i+1}"] & P_i \arrow[r, "p_i"] \arrow[d, shift left, "\alpha_i"] & \cdots \arrow[r, "p_2"] & P_1 \arrow[r, "p_1"] \arrow[d, shift left, "\alpha_1"] & P_0 \arrow[r, "p_0"] \arrow[d, shift left, "\alpha_0"] & \mathbf{Z} \arrow[d, leftrightarrow, "\mathrm{Id}"] \\
\cdots \arrow[r, "q_{i+2}"] & Q_{i+1} \arrow[r, "q_{i+1}"] \arrow[u, shift left, "\beta_{i+1}"] & Q_i \arrow[r, "q_i"] \arrow[u, shift left, "\beta_i"] & \cdots \arrow[r, "q_2"] & Q_1 \arrow[r, "q_1"] \arrow[u, shift left, "\beta_1"] & Q_0 \arrow[r, "q_0"] \arrow[u, shift left, "\beta_0"] & \mathbf{Z}
\end{tikzcd}$$

We get induced maps

$$\alpha_i^\star\colon H^i(\mathrm{Hom}_G(Q_i,A)) \to H^i(\mathrm{Hom}_G(P_i,A)), \quad \beta_i^\star\colon H^i(\mathrm{Hom}_G(P_i,A)) \to H^i(\mathrm{Hom}_G(Q_i,A)).$$

We assert that $\alpha_i^\star \circ \beta_i^\star = \mathrm{Id}$ and $\beta_i^\star \circ \alpha_i^\star = \mathrm{Id}$. As the two arguments are logically identical, we will only prove $(\beta_i \circ \alpha_i)^\star = \alpha_i^\star \circ \beta_i^\star = \mathrm{Id}$. To that end, we have the diagram

$$\begin{tikzcd}
\cdots \arrow[r, "p_{i+2}"] & P_{i+1} \arrow[r, "p_{i+1}"] \arrow[d, "\beta_{i+1}\circ\alpha_{i+1}"] & P_i \arrow[r, "p_i"] \arrow[d, "\beta_i\circ\alpha_i"] & \cdots \arrow[r, "p_2"] & P_1 \arrow[r, "p_1"] \arrow[d, "\beta_1\circ\alpha_1"] & P_0 \arrow[r, "p_0"] \arrow[d, "\beta_0\circ\alpha_0"] & \mathbf{Z} \arrow[d, "\mathrm{Id}"] \\
\cdots \arrow[r, "p_{i+2}"'] & P_{i+1} \arrow[r, "p_{i+1}"'] & P_i \arrow[r, "p_i"'] & \cdots \arrow[r, "p_2"'] & P_1 \arrow[r, "p_1"'] & P_0 \arrow[r, "p_0"'] & \mathbf{Z} \\
\cdots \arrow[r, "p_{i+2}"'] & P_{i+1} \arrow[r, "p_{i+1}"'] \arrow[u, "\mathrm{Id}"] & P_i \arrow[r, "p_i"'] \arrow[u, "\mathrm{Id}"] & \cdots \arrow[r, "p_2"'] & P_1 \arrow[r, "p_1"'] \arrow[u, "\mathrm{Id}"] & P_0 \arrow[r, "p_0"'] \arrow[u, "\mathrm{Id}"] & \mathbf{Z} \arrow[u, "\mathrm{Id}"]
\end{tikzcd}$$

From above, we obtain G–module homomorphisms $\gamma_i\colon P_i \to P_{i+1}$ such that

$$\beta_i \circ \alpha_i - \mathrm{Id} = \gamma_{i-1} \circ p_i + p_{i+1} \circ \gamma_i.$$

For $f \in \mathrm{Hom}(P_i, A)$ such that $f \circ p_{i+1} = 0$ (i.e, $f \in \ker \delta^k$), we see that

$$f \circ \beta_i \circ \alpha_i - f = f \circ \gamma_{i-1} \circ p_i.$$

In particular, $f \circ \beta_i \circ \alpha_i - f \in \mathrm{Image}(\delta^{i-1})$ and it follows then that $(\beta_i \circ \alpha_i)^\star$ is the identity.

Remark 11. Given two R–modules M, N, we can define

$$\mathrm{Ext}^i_R(M,N) = H^i(\mathrm{Hom}_R(P_\bullet, N))$$

where $P_\bullet$ is a projective resolution of M. In particular, $H^i(G,A) = \mathrm{Ext}^i_{\mathbf{Z}[G]}(\mathbf{Z}, A)$.

For each $i \geq 0$, we have the G–module $\mathbf{Z}[G^{i+1}]$ with action given by $g(g_0, \ldots, g_{i+1}) = (gg_0, \ldots, gg_{i+1})$. These are free $\mathbf{Z}[G]$–modules (and hence projective) since $\mathbf{Z}[G^{i+1}] \cong (\mathbf{Z}[G])^{i+1}$. For each $i > 0$, we define G–module homomorphisms $p_i \colon \mathbf{Z}[G^{i+1}] \to \mathbf{Z}[G^i]$ by

$$p_i = \sum_{j=0}^{i} (-1)^j \theta_{i,j}$$

where (the right hand side of the equality below is fairly common notation)

$$\theta_{i,j}(a_0, \ldots, a_i) = (a_0, \ldots, a_{j-1}, a_{j+1}, \ldots, a_i) = (a_0, \ldots, \widehat{a}_j, \ldots, a_i).$$

In the case $i = 0$, we take the augmentation map $p_0 = \varepsilon$ and so get a projective resolution of $\mathbf{Z}$ via

$$\longrightarrow \mathbf{Z}[G^{i+1}] \xrightarrow{p_i} \mathbf{Z}[G^i] \xrightarrow{p_{i-1}} \cdots \xrightarrow{p_2} \mathbf{Z}[G^2] \xrightarrow{p_1} \mathbf{Z}[G] \xrightarrow{p_0} \mathbf{Z} \longrightarrow 0$$

Example 14. Take G to be a finite cyclic group of order n and fix a generator g of G. We define $N \colon \mathbf{Z}[G] \to \mathbf{Z}[G]$ by

$$N(a) = \sum_{j=0}^{n-1} g^j a$$

and $\mu_{g-1} \colon \mathbf{Z}[G] \to \mathbf{Z}[G]$ given by

$$\mu_{g-1}(a) = (g-1)a = ga - a.$$

It is straightforward to verify that $\ker N = \mathrm{Image}(\mu_{g-1})$ and $\ker \mu_{g-1} = \mathrm{Image}(N)$. Hence, we have a free resolution of the trivial G–module $\mathbf{Z}$ via

$$\xrightarrow{N} \mathbf{Z}[G] \xrightarrow{\mu_{g-1}} \mathbf{Z}[G] \xrightarrow{N} \mathbf{Z}[G] \xrightarrow{\mu_{g-1}} \mathbf{Z}[G] \xrightarrow{\varepsilon} \mathbf{Z} \longrightarrow 0$$

For any G–module A, we can define maps $N \colon A \to A$ and $\mu_{g-1} \colon A \to A$ via the same formulas. One can check that

$$H^0(G,A) = A^G, \quad H^{2i+1}(G,A) = \ker N / \mu_{g-1}(A), \quad H^{2i+2}(G,A) = A^G / N(A).$$

Let G be a group with subgroup H. We can view $\mathbf{Z}[G]$ with the standard G–action as an H–module via restricting the action of G to an H–action. Given an H–module A, we define $M_H^G(A) = \mathrm{Hom}_H(\mathbf{Z}[G], A)$ and view $M_H^G(A)$ as a G–module via the action $(g\psi)(\eta) = \psi(g\eta)$ where $\psi \in M_H^G(A)$ and $\eta \in \mathbf{Z}[G]$.

Lemma 3.5. *Let G be a group, $H \subset G$ a subgroup, A an H–module, and M a G–module. Then there is a canonical isomorphism* $\mathrm{Hom}_G(M, M_H^G(A)) \to \mathrm{Hom}_H(M, A)$.

Proof. Given $\psi \in \mathrm{Hom}_G(M, \mathrm{Hom}_H(\mathbf{Z}[G], A))$, we have $\psi(m) = \psi_m \in \mathrm{Hom}_H(\mathbf{Z}[G], A)$. We define

$$\Psi \colon \mathrm{Hom}_G(M, \mathrm{Hom}_H(\mathbf{Z}[G], A)) \longrightarrow \mathrm{Hom}_H(M, A)$$

by $\Psi(\psi)(m) = \psi_m(1)$. To see this is an isomorphism, it suffices to construct an inverse; the reader can verify these functions are group homomorphisms. To that end, given $\phi \in \mathrm{Hom}_H(M, A)$, $m \in M$, and $g \in \mathbf{Z}[G]$, we define $\Psi^{-1}(\phi) \in \mathrm{Hom}_G(M, \mathrm{Hom}_H(\mathbf{Z}[G], A))$ by $(\Psi^{-1}(\phi)(m))(g) = \phi(gm)$. One can check that this is indeed the inverse of Ψ. ♠

We can apply Lemma 3.5 to a projective resolution of $\mathbf{Z}$, viewed as a trivial G–module. Specifically, we have

$$\cdots \xrightarrow{p_{i+2}} P_{i+1} \xrightarrow{p_{i+1}} P_i \xrightarrow{p_i} \cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} \mathbf{Z}$$

and

$$\cdots \xleftarrow{\delta^{k+1}} \mathrm{Hom}_H(P_{k+1}, A) \xleftarrow{\delta^k} \mathrm{Hom}_H(P_k, A) \xleftarrow{\delta^{k-1}} \cdots \xleftarrow{\delta^1} \mathrm{Hom}_H(P_1, A) \xleftarrow{\delta^0} \mathrm{Hom}_H(P_0, A)$$

By Lemma 3.5, this complex is isomorphic (as complexes) with

$$\cdots \xleftarrow{\delta^k} \mathrm{Hom}_H(P_k, M_H^G(A)) \xleftarrow{\delta^{k-1}} \cdots \xleftarrow{\delta^1} \mathrm{Hom}_H(P_1, M_H^G(A)) \xleftarrow{\delta^0} \mathrm{Hom}_H(P_0, M_H^G(A))$$

Hence, we have $H^k(G, M_H^G(A)) \cong H^k(H, A)$ for all k.

Corollary 3.6 (Shapiro's Lemma)**.** *If G is a group, $H \subset G$ is a subgroup, A is an H–module, and $M_H^G = \mathrm{Hom}_H(\mathbf{Z}[G], A))$ is the associated G–module, then $H^k(G, M_H^G(A)) \cong H^k(H, A)$ for all $k \geq 0$.*

The G–module $M_H^G(A)$ is called the **coinduced module** associated to the H–module A. If $H = \{1\}$, then A is simply an abelian group and the coinduced module is denoted simply by $M^G(A)$. Since $H^k(\{1\}, A) = 0$ for all $k > 0$, we see that $H^k(G, M^G(A)) = 0$ for all $k > 0$ and $H^0(G, M^G(A)) = A$.

Remark 12. Given a G–module A and $\psi \in \mathrm{Hom}_G(\mathbf{Z}[G], A)$, note that ψ is completely determined by its value at 1. In particular, $A \cong \mathrm{Hom}_G(\mathbf{Z}[G], A)$. Given $\psi \in \mathrm{Hom}_G(\mathbf{Z}[G], A)$, we can view this also as a homomorphism of H–modules via restriction and thus get $\mathrm{Hom}_G(\mathbf{Z}[G], A) \to \mathrm{Hom}_H(\mathbf{Z}[G], A) = M_H^G(A)$. Passing to cohomology and applying Shapiro's lemma, we get $\mathrm{Res} \colon H^k(G, A) \to H^k(H, A)$, which are the same restrictions homomorphisms we constructed before using cochains.

If H is finite index, we can construct a homomorphism $\mathrm{Cor}\colon H^k(H,A) \to H^k(G,A)$. This homomorphism is constructed as follows. First, we fix a complete set of coset representatives $g_1,\ldots,g_n$ for H in G. Given a G–module A and an H–module homomorphism $\phi\colon \mathbf{Z}[G] \to A$, we define the function $\phi_H^G\colon \mathbf{Z}[G] \to A$ by

$$\psi_H^G(x) = \sum_{j=1}^{n} g_j \phi(g_j^{-1}x).$$

The function $\psi_H^G \in \mathrm{Hom}_G(\mathbf{Z}[G],A)$ does not depend on the choice of the coset representatives. This yields a G–module homomorphism $M_H^G(A) = \mathrm{Hom}_H(\mathbf{Z}[G],A) \to \mathrm{Hom}_G(\mathbf{Z}[G],A) = A$. Passing to cohomology and using Shapiro's lemma, we get a group homomorphism $\mathrm{Cor}\colon H^k(H,A) \to H^k(G,A)$ called the **corestriction map**.

Lemma 3.7. *Let G be a group, H a finite index subgroup, and A a G–module. Then*

$$\mathrm{Cor}\circ\mathrm{Res}\colon H^k(G,A) \longrightarrow H^k(G,A)$$

are given by multiplication by $[G:H]$, the index of G in H.

Proof. To see this, it suffices to check that if $\phi\colon \mathbf{Z}[G] \to A$ is G–module homomorphism and not just an H–module homomorphism, then $\phi_H^G(x) = [G:H]\phi(x)$. This fact is easily seen from the definition of ϕ_H^G as since ϕ is a G–module map, we have $g_j\phi(g_j^{-1}(x)) = g_jg_j^{-1}\phi(x) = \phi(x)$. ♠

Applying Lemma 3.7 to the case when $H = \{1\}$ and G is finite, we obtain the following corollary.

Corollary 3.8. *If G is finite and of order n and A is any G–module, then for every $k > 0$, the elements of $H^k(G,A)$ have order divisible by n.*

3.4 Lecture 16. *Inflation and the Inflation-Restriction Sequence*

Given a group G, a normal subgroup $H \lhd G$, and a G–module A, the submodule A^H of H–fixed elements of A is invariant under the action of G. To see this assertion, given $a \in A^H$ and $g \in G$, we must show for each $h \in H$ that $h(ga) = ga$. For that, note that

$$h(ga) = (gg^{-1}h)(ga) = (g(g^{-1}hg)(a)) = ga$$

since $g^{-1}hg \in H$. As a result, A^H also can be viewed as a G/H–module with the action given by $gH(a) = ga$. Now, we take a projective resolution $P_\bullet = (P_i, p_i)$ of the trivial G–module $\mathbf{Z}$ and a projective resolution $Q_\bullet = (Q_i, q_i)$ of the trivial G/H–module $\mathbf{Z}$. Via the surjective homomorphism $G \to G/H$, we can view each of the G/H–modules Q_i as G–modules. In particular, we have the diagram of G–modules

$$\begin{tikzcd}
\cdots \arrow[r] & P_i \arrow[r, "p_i"] & P_{i-1} \arrow[r, "p_{i-1}"] & \cdots \arrow[r] & P_1 \arrow[r, "p_1"] & P_0 \arrow[r, "p_0"] & \mathbf{Z} \arrow[d, "\mathrm{Id}"] \\
\cdots \arrow[r] & Q_i \arrow[r, "q_i"] & Q_{i-1} \arrow[r, "q_{i-1}"] & \cdots \arrow[r] & Q_1 \arrow[r, "q_1"] & Q_0 \arrow[r, "q_0"] & \mathbf{Z}
\end{tikzcd}$$

Applying the result from the beginning of §3.3, we have G–module homomorphisms $\alpha_i \colon P_i \to Q_i$ such that the diagram

$$\begin{tikzcd}
\cdots \arrow[r] & P_i \arrow[r, "p_i"] \arrow[d, "\alpha_i"] & P_{i-1} \arrow[r, "p_{i-1}"] \arrow[d, "\alpha_{i-1}"] & \cdots \arrow[r] & P_1 \arrow[r, "p_1"] \arrow[d, "\alpha_1"] & P_0 \arrow[r, "p_0"] \arrow[d, "\alpha_0"] & \mathbf{Z} \arrow[d, "\mathrm{Id}"] \\
\cdots \arrow[r] & Q_i \arrow[r, "q_i"] & Q_{i-1} \arrow[r, "q_{i-1}"] & \cdots \arrow[r] & Q_1 \arrow[r, "q_1"] & Q_0 \arrow[r, "q_0"] & \mathbf{Z}
\end{tikzcd}$$

commutes. The G–module homomorphisms α_i induce G–module homomorphisms $\alpha_i^\star \colon \mathrm{Hom}_G(Q_i, A^H) \to \mathrm{Hom}_G(P_i, A^H)$ via $\alpha_i^\star(f) = f \circ \alpha_i$. Since the Q_i are G/H–modules, we know that H acts trivially on each Q_i and thus $\mathrm{Hom}_G(Q_i, A^H) = \mathrm{Hom}_{G/H}(Q_i, A^H)$. In particular, we have $\alpha_i^\star \colon \mathrm{Hom}_{G/H}(Q_i, A^H) \to \mathrm{Hom}_G(P_i, A^H)$. Therefore, we get induced homomorphisms on cohomology groups $H^k(G/H, A^H) \to H^k(G, A^H)$, which as before, do not depend on the choices of the projective resolutions $P_\bullet$ and $Q_\bullet$. Finally, the G–module inclusion homomorphism $A^H \to A$ induces $H^k(G, A^H) \to H^k(G, A)$ for all k. In total, we obtain

$$\begin{tikzcd}
H^k(G/H, A^H) \arrow[r] \arrow[rr, bend right, "\mathrm{Inf}"'] & H^k(G, A^H) \arrow[r] & H^k(G, A).
\end{tikzcd}$$

The homomorphism Inf is called the **inflation map** or **inflation homomorphism**. On the level of cochains, if $f \colon (G/H)^k \to A^H$ is a k–cochain, then by precomposing f with the projection homomorphism $G^k \to (G/H)^k$, we obtain $\tilde{f} \colon G^k \to A^H$. Via the G–module inclusion homomorphism $A^H \to A$, we obtain $\widetilde{f} \colon G^k \to A$. This yields $C_k(G/H, A^H) \to C_k(G, A)$ for each k and the induced group cohomology homomorphisms for these cochain complexes are the inflation homomorphisms.

Continuing with our group G and normal subgroup $H \lhd G$, we start with a pair of G–modules A, B. For each $g \in G$, we define

$$g_\star \colon \mathrm{Hom}_H(B, A) \longrightarrow \mathrm{Hom}_H(B, A)$$

by $g_\star(\phi)(b) = g^{-1}\phi(gb)$ where $\phi \in \mathrm{Hom}_H(B, A)$ and $b \in B$. To see that $g_\star(\phi) \colon B \to A$ is an H–module homomorphism, we must show that $g_\star(\phi)(hb) = hg_\star(\phi)(b)$ for all $h \in H$ and $b \in B$. For that, we have

$$\begin{aligned}
g_\star(\phi)(hb) &= g^{-1}\phi(g(hb)) = g^{-1}\phi((ghg^{-1})gb) \\
&= g^{-1}(ghg^{-1})\phi(gb) = h(g^{-1}\phi(gb)) = hg_\star(\phi)(b).
\end{aligned}$$

As $(g^{-1})_\star \circ g_\star = \mathrm{Id}$, we see that $g_\star \in \mathrm{Aut}(\mathrm{Hom}_H(B, A))$. Additionally, $h_\star(\phi) = \phi$ for any $\phi \in \mathrm{Hom}_H(B, A)$.

As before, we take a projective resolution $P_\bullet$ of the trivial G–module $\mathbf{Z}$. Note that since $\mathbf{Z}[G]$ is a free $\mathbf{Z}[H]$–module, $P_\bullet$ is also a projective resolution of $\mathbf{Z}$ viewed as a trivial H–module. For each $g \in G$, we have the commutative diagram

$$\begin{array}{ccccccccc}
\cdots \xleftarrow{\delta^k} & \mathrm{Hom}_H(P_k,A) & \xleftarrow{\delta^{k-1}} & \mathrm{Hom}_H(P_{k-1},A) & \longleftarrow \cdots \xleftarrow{\delta^1} & \mathrm{Hom}_H(P_1,A) & \xleftarrow{\delta^0} & \mathrm{Hom}_H(P_0,A) \\
& \downarrow{\scriptstyle g_\star} & & \downarrow{\scriptstyle g_\star} & & \downarrow{\scriptstyle g_\star} & & \downarrow{\scriptstyle g_\star} \\
\cdots \xleftarrow[\delta^k]{} & \mathrm{Hom}_H(P_k,A) & \xleftarrow[\delta^{k-1}]{} & \mathrm{Hom}_H(P_{k-1},A) & \longleftarrow \cdots \xleftarrow[\delta^1]{} & \mathrm{Hom}_H(P_1,A) & \xleftarrow[\delta^0]{} & \mathrm{Hom}_H(P_0,A)
\end{array}$$

and so obtain automorphisms of the cohomology groups $g_\star\colon H^k(H,A) \to H^k(H,A)$ for each k. Since $h_\star = \mathrm{Id}$ for any $h \in H$, this yields an action of G/H on the cohomology groups $H^k(H,A)$. In particular, we can view these cohomology groups as G/H–modules and call this action the **conjugate action** of G/H on $H^k(H,A)$.

Lemma 3.9. *Given a group G, a normal subgroup $H \lhd G$, and an exact sequence of G–modules*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

there is a long exact sequence of G/H–modules

$$0 \longrightarrow H^0(H,A) \longrightarrow H^0(H,B) \longrightarrow H^0(H,C) \longrightarrow H^1(H,A) \longrightarrow \cdots$$

where G/H acts by the conjugate action on the groups $H^*(H,\star)$.

The proof of Lemma 3.9 is straightforward and left as an exercise.

Exercise 39. Prove Lemma 3.9

Lemma 3.10. *Given a group G, a normal subgroup $H \lhd G$, and a G–module A, we have:*

(a) $M^G(A)^H = M^{G/H}(A)$.

(b) $H^k(H, M^G(A)) = 0$ *for all* $k > 0$.

Proof. By definition, $M^G(A) = \mathrm{Hom}(\mathbf{Z}[G],A)$ and so $M^G(A)^H \cong \mathrm{Hom}(\mathbf{Z}[G/H],A) = M^{G/H}(A)$. For (b), since $\mathbf{Z}[G]$ is a free $\mathbf{Z}[H]$–module, $M^G(A)$ is a direct sum of copies of $M^H(A)$ and so $H^k(H,M^G(A))$ is a direct sum of copies of $H^k(H,M^H(A))$. However, $H^k(H,M^H(A)) = 0$ for all $k > 0$ by Shapiro's lemma (see Corollary 3.6) and so $H^k(H,M^G(A)) = 0$ for all $k > 0$. ♠

Theorem 3.11 (Inflation-Restriction)**.** *Given a group G, a normal subgroup $H \lhd G$, and a G–module A, there is a natural homomorphism $\tau\colon H^1(H,A)^{G/H} \to H^2(G/H,A^H)$ and an exact sequence*

$$\begin{array}{ccccccc}
0 \longrightarrow & H^1(G/H,A^H) & \xrightarrow{\mathrm{Inf}} & H^1(G,A) & \xrightarrow{\mathrm{Res}} & H^1(H,A)^{G/H} \\
& & & & & \downarrow{\scriptstyle\tau} \\
& & & H^2(G,A) & \xleftarrow[\mathrm{Inf}]{} & H^2(G/H,A^H)
\end{array}$$

Proof. We have an exact sequence of G–modules

$$0 \longrightarrow A \longrightarrow M^G(A) \longrightarrow M^G(A)/A \longrightarrow 0, \tag{3.4}$$

which can also be viewed as an exact sequence of H–modules. From this short exact sequence, we obtain the long exact sequence

$$0 \longrightarrow A^H \longrightarrow M^G(A)^H \longrightarrow (M^G(A)/A)^H \longrightarrow H^1(H,A) \longrightarrow H^1(H,M^G(A)).$$

By Lemma 3.10, $H^1(H,M^G(A)) = 0$ and so $(M^G(A)/A)^H \to H^1(H,A)$ in onto. Setting

$$B = \ker((M^G(A)/A)^H \to H^1(H,A)),$$

we have two short exact sequences

$$0 \longrightarrow A^H \longrightarrow M^G(A)^H \longrightarrow B \longrightarrow 0 \tag{3.5}$$

and

$$0 \longrightarrow B \longrightarrow (M^G(A)/A)^H \longrightarrow H^1(H,A) \longrightarrow 0. \tag{3.6}$$

By Lemma 3.9, these sequences are exact sequences of G/H–modules and so we have a long exact sequence in G/H–cohomology groups from (3.5):

$$0 \longrightarrow A^G \longrightarrow M^G(A)^G \longrightarrow B^{G/H} \longrightarrow H^1(G/H,A^H) \longrightarrow H^1(G/H,M^G(A)^H).$$

By Lemma 3.10, $H^1(G/H,M^G(A)^H) = 0$. We also have the long exact sequence of G–cohomology groups coming from (3.4):

$$0 \longrightarrow A^G \longrightarrow M^G(A)^G \longrightarrow (M^G(A)/A)^G \longrightarrow H^1(G,A) \longrightarrow H^1(G,M^G(A)).$$

The cohomology group $H^1(G,M^G(A) = 0$ by Shapiro's lemma. Finally, we have the long exact sequence coming from the short exact sequence (3.6):

$$0 \longrightarrow B^{G/H} \longrightarrow (M^G(A)/A)^G \longrightarrow H^1(H,A)^{G/H} \longrightarrow H^1(G/H,B).$$

In total, we obtain the diagram:

$$\begin{tikzcd}
 & & & 0 \arrow[d] & & \\
0 \arrow[r] & A^G \arrow[r] \arrow[d, "\mathrm{Id}"] & M^G(A)^G \arrow[r] \arrow[d, "\mathrm{Id}"] & B^{G/H} \arrow[r] \arrow[d] & H^1(G/H,A^H) \arrow[r] & 0 \\
0 \arrow[r] & A^G \arrow[r] & M^G(A)^G \arrow[r] & (M^G(A)/A)^G \arrow[r] \arrow[d] & H^1(G,A) \arrow[r] & 0 \\
 & & & H^1(H,A)^{G/H} \arrow[d] & & \\
 & & & H^1(G/H,B) & &
\end{tikzcd}$$

From the above diagram, we assert that there is an exact sequence

$$0 \longrightarrow H^1(G/H,A^H) \xrightarrow{\alpha} H^1(G,A) \xrightarrow{\beta} H^1(H,A)^{G/H} \longrightarrow H^1(G/H,B).$$

We first describe the homomorphism $H^1(G/H,A^H) \to H^1(G,A)$. Note that we can view A^H and B as G–modules via the projection homomorphism $G \to G/H$. This yields a commutative diagram

$$\begin{tikzcd}
B^{G/H} \arrow[r, "\mathrm{Id}"] \arrow[d] & B^G \arrow[r] \arrow[d] & (M^G(A)/A)^G \arrow[d] \\
H^1(G/H,A^H) \arrow[r] \arrow[rr, bend right, "\mathrm{Inf}"'] & H^1(G,A^H) \arrow[r] & H^1(G,A).
\end{tikzcd}$$

The homomorphism $H^1(G/H,A^H) \to H^1(G,A^H)$ is induced by projection homomorphism $G \to G/H$ and $H^1(G,A^H) \to H^1(G,A)$ is induced by the G–module inclusion $A^H \to A$. In particular, $\alpha = \mathrm{Inf}$.

Next, we describe where the homomorphism β comes from. For that, we have the diagram

$$\begin{tikzcd}
(M^G(A)/A)^G \arrow[r] \arrow[d] & H^1(G,A) \arrow[d, "\mathrm{Res}"] \\
(M^G(A)/A)^H \arrow[r] & H^1(H,A)
\end{tikzcd}$$

and so $\beta = \mathrm{Res}$.

Finally, we have the commutative diagram

$$\begin{tikzcd}
H^1(H,A)^{G/H} \arrow[r] & H^1(G/H,B) \arrow[r] \arrow[d] & H^1(G/H,(M^G(A)/A)^H) \arrow[r, "\mathrm{Inf}"] & H^1(G,M^G(A)/A) \arrow[d] \\
 & H^2(G/H,A^H) \arrow[rr, "\mathrm{Inf}"'] & & H^2(G,A)
\end{tikzcd}$$

where the top row comes from (3.6) and is exact at $H^1(G/H,B)$. The vertical arrows are isomorphism and are induced from (3.4) and (3.5); note this make use of Shapiro's lemma and Lemma 3.10. In total, this yields the long exact sequence needed to complete the proof of the theorem. ♠

The map τ is called the **transgression map**. Explicitly, it given by the following piece of the last commutative diagram in the proof of Theorem 3.11:

$$\begin{tikzcd}
H^1(H,A)^{G/H} \arrow[r] \arrow[dr, bend right, "\tau"'] & H^1(G/H,B) \arrow[d, "\cong"] & \\
 & H^2(G/H,A^H) \arrow[r, "\mathrm{Inf}"'] & H^2(G,A)
\end{tikzcd}$$

The following result is a generalization of the inflation-restriction sequence from Theorem 3.11. We will not include a proof and refer the reader to [6].

Theorem 3.12. *Let G be a group, $H \lhd G$ a normal subgroup, and A a G–module. If $H^j(H,A) = 0$ for all $1 \leq j \leq k-1$, then there exists a natural homomorphism*

$$\tau_{k,A} \colon H^k(H,A)^{G/H} \to H^{k+1}(G/H,A^H)$$

such that the sequence

$$\begin{tikzcd}
0 \arrow[r] & H^k(G/H,A^H) \arrow[r, "\mathrm{Inf}"] & H^k(G,A) \arrow[r, "\mathrm{Res}"] & H^k(H,A)^{G/H} \arrow[d, "\tau_{k,A}"] \\
 & & H^{k+1}(G,A) & H^{k+1}(G/H,A^H) \arrow[l, "\mathrm{Inf}"]
\end{tikzcd}$$

3.5 Lecture 17. *Cup Product*

Let $A^\bullet = (A_i, \delta_A^i)$ and $B^\bullet = (B_j, \delta_B^j)$ be complexes of abelian groups. We can form a double complex by taking the tensor product of the terms $A_i \otimes B_j$. This yields the double complex:

$$\begin{tikzcd}
 & \vdots & \vdots & \vdots & \\
\cdots \arrow[r] & A_{i-1}\otimes B_{j+1} \arrow[u, "\delta_v^{i-1,j+1}"] \arrow[r, "\delta_h^{i-1,j+1}"] & A_i\otimes B_{j+1} \arrow[u, "\delta_v^{i,j+1}"] \arrow[r, "\delta_h^{i,j+1}"] & A_{i+1}\otimes B_{j+1} \arrow[u, "\delta_v^{i+1,j+1}"'] \arrow[r, "\delta_h^{i+1,j+1}"] & \cdots \\
\cdots \arrow[r] & A_{i-1}\otimes B_j \arrow[u, "\delta_v^{i-1,j}"] \arrow[r, "\delta_h^{i-1,j}"] & A_i\otimes B_j \arrow[u, "\delta_v^{i,j}"] \arrow[r, "\delta_h^{i,j}"] & A_{i+1}\otimes B_j \arrow[u, "\delta_v^{i+1,j}"'] \arrow[r, "\delta_h^{i+1,j}"] & \cdots \\
\cdots \arrow[r] & A_{i-1}\otimes \arrow[u, "\delta_v^{i-1,j-1}"] \arrow[r, "\delta_h^{i-1,j-1}"'] & A_i\otimes B_{j-1} \arrow[u, "\delta_v^{i,j-1}"] \arrow[r, "\delta_h^{i,j-1}"'] & A_{i+1}\otimes B_{j-1} \arrow[u, "\delta_v^{i+1,j-1}"'] \arrow[r, "\delta_h^{i+1,j-1}"'] & \cdots \\
 & \vdots \arrow[u] & \vdots \arrow[u] & \vdots \arrow[u] &
\end{tikzcd}$$

where

$$\delta_h^{i,j} : A_i \otimes B_j \longrightarrow A_{i+1} \otimes B_j, \quad \delta_v^{i,j} : A_i \otimes B_j \longrightarrow A_i \otimes B_{j+1}$$

are defined by

$$\delta_h^{i,j} = \delta_A^i \otimes \mathrm{Id}, \quad \delta_v^{i,j} = \mathrm{Id} \otimes (-1)^i \delta_B^j.$$

Note that this double complex is not commutative as the squares skew-commute

$$\delta_h^{i,j+1} \circ \delta_v^{i,j} = -\delta_v^{i+1,j} \circ \delta_h^{i,j}.$$

We can form a graded complex from this above double complex by setting

$$T_n = \bigoplus_{i+j=n} A_i \otimes B_j$$

and with differentials $\delta^n \colon T_n \to T_{n+1}$ given on each component $A_i \otimes B_j$ by $\delta_h^{i,j} + \delta_v^{i,j}$. The skew-commutativity of squares implies that $\delta^{n+1} \circ \delta^n = 0$ for all $n \geq 0$. We call the complex $T^\bullet = (T_n, \delta^n)$ the **tensor product** of $A^\bullet$ and $B^\bullet$ and will denote this complex simply by $A^\bullet \otimes B^\bullet$.

Given two complexes of abelian groups $A^\bullet = (A_i, \delta_A^i)$, $B^\bullet = (B_j, \delta_B^j)$ and two abelian groups A, B, we have the complexes $P_\bullet = (P_i, p_i) = \mathrm{Hom}(A^\bullet, A)$ and $Q_\bullet = (Q_j, q_j) = \mathrm{Hom}(B^\bullet, B)$. Given $f_1 : A_i \to A$ and $f_2 \colon B_j$, i.e. $f_1 \in P_i = \mathrm{Hom}(A_i, A)$ and $f_2 \in Q_j = \mathrm{Hom}(B_j, B)$, we have $f_1 \otimes f_2 \colon A_i \otimes B_j \to A \otimes B$. The homomorphism $f_1 \otimes f_2$ is an element of the complex $\mathrm{Hom}(A^\bullet \otimes B^\bullet, A \otimes B) = R_\bullet = (R_k, r_k)$ and has degree $i + j$; here $R_k = \mathrm{Hom}(T_k, A \otimes B)$. Note that if $f_1 \in B_i(P_\bullet) = \mathrm{Image}(p_{i-1})$ and $f_2 \in B_j(Q_\bullet) = \mathrm{Image}(q_{j-1})$, it is clear that $f_1 \times f_2 \in B_{i+j}(R_\bullet) = \mathrm{Image}(r_{i+j})$. Similarly, if $f_1 \in \ker(p_i) = Z_i(P_\bullet)$ and $f_2 \in \ker(q_j) = Z_j(Q_\bullet)$, then $f_1 \otimes f_2 \in Z_{i+j}(R_\bullet)$. In particular, we obtain a homomorphism

$$H^i(\mathrm{Hom}(A^\bullet, A)) \times H^j(B^\bullet, B) \longrightarrow H^{i+j}(\mathrm{Hom}(A^\bullet \otimes B^\bullet, A \otimes B).$$

If $A^\bullet$ and $B^\bullet$ are complexes of G–modules, we can define a G–module structure of the tensor product $A_i \otimes B_j$ by $g(a \otimes b) = ga \otimes gb$. Applying the above that the setting of G–module complexes yields

$$H^i(\mathrm{Hom}_G(A^\bullet, A)) \times H^j(\mathrm{Hom}_G(B^\bullet, B)) \longrightarrow H^{i_j}(A^\bullet \otimes B^\bullet, A \otimes B).$$

Lemma 3.13. *Given a group G and a projective resolution $P_\bullet$ of the trivial G–module $\mathbf{Z}$, then $P_\bullet \otimes P_\bullet$ is a projective resolution of the trivial $(G \times G)$–module $\mathbf{Z}$.*

We refer the reader to Proposition 3.4.3 in [6] for a proof of this fact. Now consider G–modules A, B with G and $P_\bullet$ as in Lemma 3.13. We obtain

$$H^i(G,A) \times H^j(G,B) = H^i(\mathrm{Hom}_G(P_\bullet, A)) \times H^j(\mathrm{Hom}(P_\bullet, B)) \longrightarrow H^{i+j}(\mathrm{Hom}_{G\times G}(P_\bullet \otimes P_\bullet, A \otimes B) = H^{i+j}(G \times G, A \otimes B).$$

We have the diagonal embedding $G \to G \times G$ and so can apply the restriction homomorphism to the image, obtaining

$$H^{i+j}(G \times G, A \otimes B) \xrightarrow{\quad \mathrm{Res} \quad} H^{i+j}(G, A \otimes B).$$

The composition of these two homomorphisms yields

$$H^i(G,A) \times H^j(G,B) \longrightarrow H^{i+j}(G, A \otimes B)$$

and is called the **cup product**. Given $a \in H^i(G,A)$ and $b \in H^j(G,B)$, we denote the cup product of a, b by $a \cup b \in H^{i+j}(G, A \otimes B)$.

Proposition 3.14. *Let G be a group and A, B a pair of G–modules.*

(a) If $a \in H^i(G,A)$ and $b \in H^j(G,B)$, then

$$a \cup b = (-1)^{ij}(b \cup a).$$

(b) The cup product is associative.

(c) If $A \to A'$, $B \to B'$ are homomorphisms of G–modules, then the following diagram commutes:

$$\begin{tikzcd}
H^i(G,A) \times H^j(G,B') \arrow[r, "\cup"] & H^{i+j}(G, A \otimes B') \\
H^i(G,A) \times H^i(G,B) \arrow[r, "\cup"] \arrow[u] \arrow[d] & H^{i+j}(G, A \otimes B) \arrow[u] \arrow[d] \\
H^i(G,A') \times H^j(G,B) \arrow[r, "\cup"] & H^{i+j}(G, A' \otimes B).
\end{tikzcd}$$

Proof. Add. ♠

Remark 13. If we take $A = B = \mathbf{Q}$ as a trivial G–module, we see that the cup product yields

$$H^i(G,\mathbf{Q}) \times H^j(G,\mathbf{Q}) \longrightarrow H^{i+j}(G,\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Q}) \cong H^{i+j}(G,\mathbf{Q})$$

where the isomorphism of the two right most groups is via the isomorphism $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Q} \to \mathbf{Q}$. The groups $H^{\bullet}(G,\mathbf{Q})$ then form a graded ring called the rational cohomology ring.

Given G–modules A, B, C and a G–module homomorphism $A \times B \to C$, we have group homomorphisms

$$H^i(G,A) \times H^j(G,B) \xrightarrow{\ \cup\ } H^{i+j}(G,A \otimes B) \longrightarrow H^{i+j}(G,A \times B) \longrightarrow H^{i+j}(G,C)$$

where the middle and right arrows are induced by $A \otimes B \to A \times B \to C$. One says that $A \times B \to C$ **induces pairings** between the cohomology groups $H^i(G,A)$ and $H^j(G,B)$.

We now state and prove some further properties about the cup product.

Proposition 3.15. *Given a group G and an exact sequence*

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0$$

of G modules such that

$$0 \longrightarrow A_1 \otimes_{\mathbf{Z}} B \longrightarrow A_2 \otimes_{\mathbf{Z}} B \longrightarrow A_3 \otimes_{\mathbf{Z}} B \longrightarrow 0$$

is exact for some G–module B, then for all $a \in H^i(G,A_3)$ and $b \in H^j(G,B)$, we have

$$\delta(a) \cup b = \delta(a \cup b) \in H^{i+j+1}(G,A_1 \otimes B)$$

where $\delta\colon H^i(G,A_3) \to H^{i+1}(G,A_1)$ is the connected homomorphism.

Proof. Add. ♠

Proposition 3.16. *Given a group G and an exact sequence*

$$0 \longrightarrow B_1 \longrightarrow B_2 \longrightarrow B_3 \longrightarrow 0$$

of G modules such that

$$0 \longrightarrow A \otimes_{\mathbf{Z}} B_1 \longrightarrow A \otimes_{\mathbf{Z}} B_2 \longrightarrow A \otimes_{\mathbf{Z}} B_3 \longrightarrow 0$$

is exact for some G–module A, then for all $a \in H^i(G,A)$ and $b \in H^j(G,B_3)$ we have

$$a \cup \delta(b) = (-1)^i \delta(a \cup b) \in H^{i+j+1}(G,A \otimes B_1)$$

where $\delta\colon H^i(G,B_3) \to H^{i+1}(G,B_1)$ is the connecting homomorphism.

Proof. Add. ♠

We leave the next result as an exercise.

Proposition 3.17. *Given a group G and a pair of exact sequences of G–modules*

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0, \quad 0 \longrightarrow B_1 \longrightarrow B_2 \longrightarrow B_3 \longrightarrow 0$$

and a $\mathbf{Z}$*–bilinear G–equivariant function $A_2 \times B_2 \to C$ for some G–module C such that the restriction of the bilinear function to the subgroup $A_1 \times B_1$ is trivial, then there are homomorphisms $A_1 \times B_3 \to C$ and $A_3 \times B_1 \to C$ such that the induced homomorphisms in cohomology satisfy*

$$\delta_A(a) \cup b = (-1)^{i+1} a \cup \delta_B \in H^{i+j+1}(G,C)$$

where δ_A, δ_B are the associated connecting homomorphisms.

Exercise 40. Prove Proposition 3.17.

Proposition 3.18. *Let G be a group, a subgroup $H \subset G$, and G–modules A,B, we have the following properties:*

(i) If $a \in H^i(H,A)$ and $b \in H^j(H,B)$, then

$$\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b).$$

(ii) If H is normal subgroup of G, $a \in H^i(G/H, A^H)$, and $b \in H^j(G/H, B^H)$, then

$$\mathrm{Inf}(a \cup b) = \mathrm{Inf}(a) \cup \mathrm{Inf}(b).$$

(iii) If H is finite index in G, $a \in H^i(H,A)$, and $b \in H^j(G,B)$, then

$$\mathrm{Cor}(a \cup \mathrm{Res}(b)) = \mathrm{Cor}(a) \cup b.$$

(iv) If H is normal in G, $\overline{g} \in G/H$, $a \in H^i(H,A)$, and $b \in H^j(H,B)$, then

$$\overline{g}_\star(a \cup b) = \overline{g}_\star(a) \cup \overline{g}_\star(b).$$

Proof. Add. ♠

Chapter 4

Assorted Topics

Chapter 5

Junk Yard

This chapter contains supplemental material and solutions to some of the exercises in the main body of the text.

5.1 Solutions to Some Exercises

Bibliography

[1] M. Aka, *Arithmetic groups with isomorphic finite quotients*, J. Algebra **352** (2012), 322–340.

[2] M. Asada, Mamoru, *The faithfulness of the monodromy representations associated with certain families of algebraic curves*, J. Pure Appl. Algebra **159** (2001), 123–147.

[3] G. Baumslag, *Groups with the same lower central sequence as a relatively free group. I. The groups*, Trans. Amer. Math. Soc. **129** (1967) 308–321.

[4] G. Baumslag and U. Stammbach, *A non-free parafree group all of whose countable subgroups are free*, Math. Z. **148** (1976), 63–65.

[5] M. R. Bridson and F. J. Grunewald, *Grothendieck's problems concerning profinite completions and representations of groups*, Ann. of Math. **160** (2004), 359–373.

[6] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge Stud. Adv. Math., 2006.

[7] A. Grothendieck, *Représentations linéaires et compactification profinie des groupes discrets*, Manuscripta Math. **2** (1970), 375–396.

[8] D. D. Long and A. W. Reid, *Grothendieck's problem for 3-manifold groups*, Groups Geom. Dyn. **5** (2011), 479–499.

[9] A. Lubotzky, *Tannaka duality for discrete groups*, Amer. J. Math. **102** (1980), 663–689.

[10] A. Lubotzky, Y. Shalom, *Finite representations in the unitary dual and Ramanujan groups*, Contemp. Math. **347** (2004), 173–190.

[11] W. Magnus, *Über freie Faktorgruppen und freie Untergruppen gegebener Gruppen*, Monatsh. Math. **47** (1939), 307–313.

[12] V. Platonov and O. I. Tavgen, *Grothendieck's problem on profinite completions of groups*, Soviet Math. Dokl. **33** (1986), 822825.

[13] L. Ribes, P. Zalesskii, *Profinite Groups*, Springer-Verlag, 2010.

[14] J. S. Wilson, *Profinite Groups*, Oxford University Press, 1996.

Index