Topics in Homological algebra

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Pavith R

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

December, 2022

Supervisor: Dr. Supriya Pisolkar

Certificate

This is to certify that this dissertation entitled Topics in Homological algebra towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Pavith R at Indian Institute of Science Education and Research under the supervision of Dr. Supriya Pisolkar, Associate Professor, Department of Mathematics , during the academic year 2022-2023.

Supriya

Dr. Supriya Pisolkar

Committee:

Dr. Supriya Pisolkar

Dr. Vivek Mohan Mallick

This thesis is dedicated to my parents for giving me constant support and always encouraging me in my endeavours.

Declaration

I hereby declare that the matter embodied in the report entitled Topics in Homological algebra are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Dr. Supriya Pisolkar and the same has not been submitted elsewhere for any other degree.

R. Pavith

Pavith R

Acknowledgments

I would like to express my deepest gratitude to my supervisor, Dr. Supriya Pisolkar who guided me throughout this project. I am especially grateful for her patience and support at each stage of the project. I am also grateful to my TAC's expert member Dr. Vivek Mohan Mallick and the discipline-wise project coordinator Dr. Steven Spallone for their valuable feedback. Many thanks to my fellow students Biswanath Samanta and A P Aravintakshan for their feedback and help during discussions. Lastly, I'd like to mention my family for their constant motivation and emotional support.

Abstract

Homological algebra is the study of homology in an algebraic setting. In this project we explore various standard tools of homological algebra such as Ext groups, Tor groups, Long exact sequence of cohomology etc, and the concepts required to realize those tools such as projective modules and resolutions, cochain complexes, etc. We also present a few topics from category theory initially to better understand these tools. We then focus on the specific case of group cohomology and related results which we apply to profinite groups. Finally we apply a few results from cohomology of profinite group to arrive at the Golod-Shafarevich inequality for finite p-groups.

Contents

Introduction

Homology is a general way of associating a sequence of algebraic objects such as modules or abelian groups to mathematical objects. Historically they were defined in the context of Algebraic topology to differentiate and categorize manifolds based on their holes. Homological Algebra studies homology in algebraic settings. The concept has evolved to be defined on other mathematical objects such as modules, groups, etc. It's development was closely intertwined with that of category theory. Homological algebra affords means and tools to extract information contained in the sequence attached to objects which are presented in the form of homological invariants which provides insights and elucidates on the structure of the object itself.

In this project we will explore various tools of Homological algebra, and proceed to apply it in the case of group cohomology. We then explore about profinite groups and it's cohomology which is helpful in interpreting invariants related to the presentation of pro-p groups such as generator rank and relation rank. We then explore Golod-Shafarevich inequality, which is an inequality between the generator rank and relation rank of a finite p-group. Many proofs of Golod-Shafarevich inequality exists in literature of which Helmut Koch's [8] proof is the one that the proof in this thesis is primarily based on.

This thesis is primarily a literature review of concepts and results from Homological algebra and in particular group cohomology, and few results from it being used in exploring Golod-Shafarevich inequality. However a few examples have been discussed and few details have been added to the proofs to make it easier for the reader to understand.

Chapter 1

Category theory

In this chapter we will explore the basic terminologies of category theory such as what is a category, subcategory, Functor, natural transformations, product etc, and look at a few examples to understand them. This chapter is primarily based on [1]

Definition 1.0.1. *A category $\mathcal{C}$ consists of a class obj$(\mathcal{C})$ of objects, a set of morphisms Hom(A, B) for every ordered pair (A, B) of objects, and compositions*

$$Hom(A, B) \times Hom(B, C) \to Hom(A, C),$$

denoted by

$$(f, g) \mapsto gf,$$

for every ordered triple A, B, C of objects. They must follow the bellow axioms,

1. *the Hom sets are pairwise disjoint,*

2. *for each object A, there is an identity morphism $1_A \in$ Hom(A, A) such that $f \circ 1_A = f$ and $1_B \circ f = f, \forall f \in$ Hom(A, B)*

3. *composition is associative, given $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, then*

$$(hg)f = h(gf)$$

Example 1. *The class of all groups with group homomorphisms as the morphisms forms* *the category **Groups**. Given a ring R, the class of all left R-Modules with module homomorphisms as the morphisms is the category* ${}_R$***Mod***.

Definition 1.0.2. *A category $\mathcal{S}$ is a subcategory of $\mathcal{C}$ if,*

- $obj(\mathcal{S}) \subseteq obj(\mathcal{C})$,
- $Hom_{\mathcal{S}}(A,B) \subseteq Hom_{\mathcal{C}}(A,B) \quad \forall A, B \in obj(\mathcal{S})$,
- *if* $f \in Hom_{\mathcal{S}}(A,B)$ *and* $g \in Hom_{\mathcal{S}}(B,C)$, *then* $gf \in Hom_{\mathcal{S}}(A,C) = gf \in Hom_{\mathcal{C}}(A,C)$.
- *if* $A \in obj(\mathcal{S})$, *then* $1_A \in Hom_{\mathcal{S}}(A,A) = 1_A \in Hom_{\mathcal{C}}(A,A)$.

A category $\mathcal{S}$ is called a full subcategory if $\forall A, B \in obj(\mathcal{S})$, $\mathrm{Hom}_{\mathcal{S}}(A,B) = \mathrm{Hom}_{\mathcal{C}}(A,B)$.

Example 2. *The category **Ab.** of abelian groups is a full subcategory of **Groups**.*

Definition 1.0.3. *If $\mathcal{C}$ and $\mathcal{D}$ are categories, then a functor $T : \mathcal{C} \to \mathcal{D}$ is a function such that,*

1. *if* $A \in obj(\mathcal{C})$ *then* $T(A) \in obj(\mathcal{D})$.
2. *if* $f \in Hom_{\mathcal{C}}(A,B)$ *then* $T(f) \in Hom_{\mathcal{D}}(T(A), T(B))$.
3. *if* $A \xrightarrow{f} B \xrightarrow{g} C$ *in* $\mathcal{C}$, *then* $T(A) \xrightarrow{T(f)} T(B) \xrightarrow{T(g)} T(C)$ *in* $\mathcal{D}$, *and* $T(gf) = T(g)T(f)$.
4. $T(1_A) = 1_{T(A)}, \quad \forall A \in obj(\mathcal{C})$.

If $\mathcal{C}$ and $\mathcal{D}$ are the same as above, then a contravariant functor $T : \mathcal{C} \to \mathcal{D}$ is defined in the same way, except (ii) and (iii), which becomes

- if $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ then $T(f) \in \mathrm{Hom}_{\mathcal{D}}(T(B), T(A))$.
- if $A \xrightarrow{f} B \xrightarrow{g} C$ in $\mathcal{C}$, then $T(C) \xrightarrow{T(g)} T(B) \xrightarrow{T(f)} T(A)$ in $\mathcal{D}$, and $T(gf) = T(f)T(g)$.

Example 3. *If $\mathcal{C}$ is a category and $A \in obj(\mathcal{C})$, then the* Hom functor $T_A : \mathcal{C} \to$ ***Sets***, *denoted by $Hom(A, \square)$, is defined as,*

$$T_A(B) = Hom(A,B) \quad \forall B \in obj(\mathcal{C}),$$

and if $f \in Hom(B, B')$*, then* $T_A(f) : Hom(A, B) \to Hom(A, B')$ *given by*

$$g \mapsto fg, \quad \forall g \in Hom(A, B)$$

.

Example 4. *If* $\mathcal{C}$ *is a category and* $B \in obj(\mathcal{C})$*, then the contravariant* Hom functor $T_B : \mathcal{C} \to \boldsymbol{Sets}$*, denoted by* $Hom(\Box, B)$*, is defined as,*

$$T_B(A) = Hom(A, B) \quad \forall A \in obj(\mathcal{C}),$$

and if $f \in Hom(A, A')$*, then* $T_B(f) : Hom(A', B) \to Hom(A, B)$ *given by*

$$h \mapsto hf, \quad \forall h \in Hom(A', B)$$

.

Definition 1.0.4. *Let* $S, T : \mathcal{A} \to \mathcal{B}$ *be functors. A* natural transformation $\tau : S \to T$ *is a one parameter family of morphisms in* $\mathcal{B}$*,*

$$\tau = \{\tau_A : SA \to TA\}_{A \in obj(\mathcal{C})},$$

making the following diagram commute $\forall f \in Hom(A, A')$ *in* $\mathcal{A}$ *:*

$$\begin{tikzcd}
SA \arrow[r, "\tau_A"] \arrow[d, "Sf"'] & TA \arrow[d, "Tf"] \\
SA' \arrow[r, "\tau_{A'}"] & TA'
\end{tikzcd}$$

If each τ_A in the natural transformation τ is an isomorphism, then τ is called a *natural isomorphism.* Given two categories $\mathcal{A}$ and $\mathcal{B}$, equivalence of categories is when there exists functors $S : \mathcal{A} \to \mathcal{B}$ and $T : \mathcal{B} \to \mathcal{A}$, and natural isomorphisms $\tau : ST \to 1_{\mathcal{B}}$ and $\eta : TS \to 1_{\mathcal{A}}$.

Theorem 1.0.5 (Adjoint isomorphism)**.** *Given a right R-module* A_R*, a right S module* C_S *and a* R, S*-bi module* ${}_RB_S$*, there exists a natural isomorphism,*

$$\tau_{A,B,C} : Hom_S(A \otimes_R B, C) \to Hom_R(A, Hom_S(B, C))$$

with $\tau_{A,B,C}(f)(a)(b) = f(a \otimes b)$ *where* $a \in A$, $b \in B$ *and* $f \in Hom_S(A \otimes_R B, C)$

Definition 1.0.6. *Let* $\mathcal{C}$ *be a category and let* $\{X_i\}_{i \in I}$ *be a family of objects in* $\mathcal{C}$ *indexed by the set* I*. The product of* $\{X_i\}_{i \in I}$ *is an object* X *together with morphisms* $\pi_i : X \to X_i$ *such that for every object* Y *and every family of morphisms* $f_i : Y \to X_i$ *indexed by* I*, there exists a unique morphism* $f : Y \to X$ *such that* $f_i = \pi_i f$*, that is the following diagram commutes* $\forall i \in I$*.*

$$\begin{tikzcd}
Y \arrow[d, dashed, "f"] \arrow[dr, "f_i"] & \\
X \arrow[r, "\pi_i"] & X_i
\end{tikzcd}$$

Example 5. *In the category of* ***Sets*** *the product of a family of sets is the Cartesian product of the family. In the category of* ***Groups*** *the product of a family of groups is the direct product of the family.*

Definition 1.0.7. *Let* $\mathcal{C}$ *be a category and let* $\{X_i\}_{i \in I}$ *be a family of objects in* $\mathcal{C}$ *indexed by the set* I*. The coproduct of* $\{X_i\}_{i \in I}$ *is an object* X *together with morphisms* $j_i : X_i \to X$ *such that for every object* Y *and every family of morphisms* $f_i : X_i \to Y$ *indexed by* I*, there exists a unique morphism* $f : X \to Y$ *such that* $f_i = f j_i$*, that is the following diagram commutes* $\forall i \in I$*.*

$$\begin{tikzcd}
Y & \\
X \arrow[u, dashed, "f"] & X_i \arrow[l, "j_i"'] \arrow[ul, "f_i"']
\end{tikzcd}$$

Example 6. *In the category of* ***Sets****, the coproduct of a family of objects is the disjoint union of the family, where as in the category* ***Ab*** *of abelian groups it is the direct sum.*

In a category $\mathcal{C}$, a collection of objects and morphisms $\{X_i, \phi_{ij}\}_{i \in I}$, indexed by a directed poset I, where the morphisms $\phi_{ij} : X_i \to X_j$ for all $i \geq j$ are such that,

- the map $\phi_{ii} : X_i \to X_i$ is the identity in X_i for all $i \in I$ and
- $\phi_{ik} = \phi_{jk} \circ \phi_{ij}$ for all $i, j, k \in I$ such that $i \geq j \geq k$.

is called an inverse system in $\mathcal{C}$.

Definition 1.0.8. *Let $\{X_i, \phi_{ij}\}_{i\in I}$ be an inverse system in $\mathcal{C}$. The inverse limit of this system is an object $X \in \mathcal{C}$ along with a set of morphisms $\pi_i : X \to X_i$ for all $i \in I$, such that $\pi_j = \phi_{ij} \circ \pi_i$ for all $i \geq j$ and $i, j \in I$.*

X is often denoted by $X = \varprojlim\limits_{i\in I} X_i$ and it is universal in the sense that if there exists an object Y and morphisms $h_i : Y \to X_i$ in $\mathcal{C}$ such that $h_j = \phi_{ij} \circ h_i$ for all $i \geq j$, then there exists a unique morphism $g : Y \to X$ such that $h_i = \pi_i \circ g$, that is, the following diagram commutes.

$$\begin{tikzcd}
& Y \arrow[d, "g"'] \arrow[ddl, "h_i"'] \arrow[ddr, "h_j"] & \\
& X \arrow[dl, "\pi_i"] \arrow[dr, "\pi_j"'] & \\
X_i \arrow[rr, "\phi_{ij}"] & & X_j
\end{tikzcd}$$

Since we'll mostly be using inverse limits in the context of groups in this thesis, it will be presented here. If $\{G_i, \phi_{ij}\}_{i\in I}$ is an inverse system of groups, that is, G_i are groups and ϕ_{ij} are group homomorphism then the inverse limit is given by

$$\varprojlim G_i = \{(g_i)_{i\in I} \in \prod_{i\in I} G_i \big| g_j = \phi_{ij}(g_j), \text{for all} \quad i \geq j \in I\}$$

is a sub group of the product $\prod_{i\in I} G_i$, with the group homomorphisms $\pi_i : \varprojlim G_i \to G_i$ of the inverse limits induced from the projections $p_i : \prod_{i\in I} G_i \to G_i$.

Chapter 2

Projective, Injective and Flat modules

In this chapter we'll explore about a few special kinds of modules, namely projective, injective and flat modules. We'll see the definitions of these modules, a few examples and a few propositions which help us to characterise these modules. Finally we'll see a few theorems which tell us about the existence of enough projective and injective modules in the category of ${}_R\mathbf{Mod}$, that helps us in constructing projective or injective resolutions for any given R-module, which we'll use in the next chapter. This chapter is primarily based on results from [1]

2.1 Projective modules

Definition 2.1.1. *A left R-module P is* projective *if, whenever $p : A \to B$ is surjective and $h : P \to B$ is any map, there exists a lifting $g : P \to A$, making the following diagram commute.*

$$\begin{tikzcd} & P \arrow[dl, dashed, "g"'] \arrow[d, "h"] & \\ A \arrow[r, "p"] & B \arrow[r] & 0 \end{tikzcd}$$

Proposition 2.1.2. *Every free left R-module is projective.*

Proof. Let P be a free left R-module with basis $\mathbb{B}$. Let A and B be left R-modules with $j : A \to B$ a surjection and $k : P \to B$ be a homomorphism. Now for every $b \in \mathbb{B}$ there exists a $a_b \in A$ such that $k(b) = j(a_b)$, since j is a surjection. Now the required lifting $g : P \to A$ is the map such that $b \mapsto a_b$. To verify the commutativity of the diagram, we have $j \circ g(b) = j(a_b) = k(b)$. As $j \circ g$ and k agree on the basis $\mathbb{B}$, they agree on P. □

$$\begin{tikzcd}
& P \arrow[d, "k"] \arrow[dl, dashed, "g"'] & \\
A \arrow[r, "j"] & B \arrow[r] & 0
\end{tikzcd}$$

Proposition 2.1.3. *A left R-module P is projective if and only if $Hom_R(P, \Box)$ is an exact functor.*

Proof. We know that $\mathrm{Hom}_R(P, \Box)$ is a left exact functor. This reduces the proof to showing that P is projective $\Leftrightarrow 0 \to A \xrightarrow{i} B \xrightarrow{j} c \to 0$ is exact $\implies j^* : Hom_R(P, B) \to Hom_R(P, C)$ from $0 \to Hom_R(P, A) \xrightarrow{i^*} Hom_R(P, B) \xrightarrow{j^*} Hom_R(P, C)$ is surjctive. Now if P is projective then given a $h \in Hom_R(P, C)$ there exists a lifting $g : P \to B$ such that $h = j \circ g = j^*(g)$, since j is a surjection. This shows that j^* is surjective. Conversely, if $j*$ is surjective then for any map $h : P \to C$ there exists a map $g \in Hom_R(P, B)$ such that $h = j^*(g) = j \circ g$, thus P is projective. □

Proposition 2.1.4. *A left R-module P is projective if and only if every short exact sequence of modules of the form $0 \to A \xrightarrow{i} B \xrightarrow{j} P \to 0$ splits.*

Proof.

$$\begin{tikzcd}
& & & P \arrow[d, "id"] \arrow[dl, dashed, "g"'] & \\
0 \arrow[r] & A \arrow[r, "i"] & B \arrow[r, "j"] & P \arrow[r] & 0
\end{tikzcd}$$

Suppose P is projective, from the above diagram we can see that there exists a map $g : P \to B$ such that $j \circ g = id$, which implies that g is a section and thus the exact sequence splits. Conversely, if all exact sequence ending with P splits, then consider the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{ker}p \arrow[r, "i"] & F \arrow[r, shift left, "p"] \arrow[d, dotted, "g_0"] & P \arrow[l, shift left, "k"] \arrow[r] \arrow[d, "h"] & 0 \\
& & B \arrow[r, "j"] & C \arrow[r] & 0
\end{tikzcd}$$

We have that $j : B \to C$ is surjective and $h : P \to C$ is any map, and have to show that there exists a lifting $g : P \to B$ such that $jg = h$. Since every module is a quotient of free module , we have a free module F with $p : F \to P$ a surjection, thus the top row of the above diagram is exact, thus splits by hypothesis. Thus there exists a section $k : P \to F$. Now F is projective and $hp : F \to C$ is a map, thus there exists a lifting $g_0 : F \to B$ such that $jg_0 = hp$. Now $g = g_0k : P \to B$ is the required lift, as $jg = jg_0k = hpk = hid = h$. □

Using the results from the above propositions we can now give a solid characterisation of projective modules.

Theorem 2.1.5. *A left R-module P is projective, if and only if it is a direct summand of a free left R-module*

Proof. Suppose that P is projective, then since every module can be identified with a quotient of free module we get the following exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{ker}p \arrow[r, "i"] & F \arrow[r, "p"] & P \arrow[r] & 0
\end{tikzcd}$$

which splits, from the previous proposition thus P is a direct summand of F which is a free R-module. Now if suppose P is a direct summand of F, then we get the maps $j : F \to P$ and $p : P \to F$ such that $jp = id$. Thus if $k : B \to C$ is a surjection and $h : P \to C$ is any map, similar to the proof of the previous proposition we have the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{ker}p \arrow[r, "i"] & F \arrow[r, shift left, "j"] \arrow[d, dashed, "g_0"] & P \arrow[l, shift left, "p"] \arrow[r] \arrow[d, "h"] & 0 \\
 & & B \arrow[r, "k"] & C \arrow[r] & 0
\end{tikzcd}$$

and with arguments identical to the previous proposition we get a lfiting $g = g_0p : P \to B$ such that $kg = h$, and thus P is projective. □

Corollary 2.1.6. *A finitely generated left R-module P is projective, if and only if it is a direct summand of R^n for some $n \in \mathbb{N}$.*

We get this result from taking the free module F to be explicitly R^n as P is finitely generated.

Corollary 2.1.7. *1. Every direct summand of a projective module is projective*

2. Every direct sum of projective modules is projctive.

This comes from the facts that(1) a direct summand of a projective module which itself is a direct summand of a free module is in turn itself a direct summand of a free module, and that (2) direct sum of a collection of free modules is itself free.

Theorem 2.1.8. *If R is a PID, then every finitely generated projective R-module is free.*

Proof. Let R be a PID, and P be a finitely generated projective R-module, then from the previous corollary, it is the direct summand of a finitely generated free R-module (like R^n), thus is a submodule of a free module. But in a PID, a submodule of a finitely generated free module is itself free, thus P is free. □

Example 7. $\mathbb{Z}/6\mathbb{Z} = \{[0],[1],[2],[3],[4],[5]\}$ is a ring of residue classes of six elements, with $\mathbb{Z}/6\mathbb{Z} = I \oplus J$, where $I = \{[0],[3]\}$ and $J = \{[0],[2],[4]\}$ are ideals in $\mathbb{Z}/6\mathbb{Z}$, since I and J are direct summands of the free $\mathbb{Z}/6\mathbb{Z}$-module $\mathbb{Z}/6\mathbb{Z}$, they are non free projective modules.

Theorem 2.1.9. *The category of ${}_R\boldsymbol{Mod}$ has enough projectives: given any R-module A, there exists an projective R-module P with a surjection $p : P \to A$.*

Proof. We know that every R-module is a quotient of a free module. Thus take P to be that free module so that we can get a surjective map $p : P \to A$, and as P is free it is projective. □

2.2 Injective modudles

Definition 2.2.1. *A left R-module E is* injective *if, whenever $i : A \to B$ is injective and $h : A \to E$ is any map, there exists $g : B \to E$, making the following diagram commute.*

$$\begin{tikzcd}
 & E & \\
0 \arrow[r] & A \arrow[u, "h"] \arrow[r, "i"] & B \arrow[ul, dashed, "g"']
\end{tikzcd}$$

Proposition 2.2.2. *A left R-module E is injective if and only if $Hom_R(\Box, E)$ is an exact functor.*

Proposition 2.2.3. *If a left R-module E is injective, then every short exact sequence of modules of the form $0 \to E \xrightarrow{i} B \xrightarrow{p} C \to 0$ splits.*

Proof. Suppose E is a injective module, consider the following diagram.

$$\begin{tikzcd}
 & E & & & \\
0 \arrow[r] & E \arrow[u, dotted, "id"] \arrow[r, "i"] & B \arrow[ul, "q"'] \arrow[r, "j"] & C \arrow[r] & {}
\end{tikzcd}$$

Due to injectivity of E the map $id : E \to E$ can be extended to a map $q : B \to E$ such that $qi = id$. Thus the exact sequnce splits. □

Proposition 2.2.4. *If $(E_k)_{k \in K}$ is a family of injective left R-modules, then $\Pi_{k \in K} E_k$ is also an injective left R-module.*

$$\begin{tikzcd}
 & E & \\
0 \arrow[r] & A \arrow[u, "f"] \arrow[r, "i"] & B \arrow[ul, dashed, "g"']
\end{tikzcd}
\qquad
\begin{tikzcd}
 & E_k & \\
0 \arrow[r] & A \arrow[u, "p_k f"] \arrow[r, "i"] & B \arrow[ul, dotted, "g_k"']
\end{tikzcd}$$

Proof. Consider the above diagrams. The map $i : A \to B$ is injective, let $E = \Pi E_k$ and let $p_k : E \to E_k$ be the natural projections. Suppose $f : A \to E$ be any map, then $p_k f : A \to E_k$ can be extended to $g_k : B \to E_k$ such that $g_k 1 = p_k f$, due to the injectivity of each E_k. Now define $g : B \to E$ to be the map $g : b \mapsto (g_k(b))_{k \in K}$.Now g is the required extension of f as $gi(b) = (g_k(i(b)))_{k \in K} = (p_k f(b))_{k \in K} = f(b)$. □

For a finite collection of left R-modules, their direct product and product co-insides, thus we have the following corollary.

Corollary 2.2.5. *A finite direct sum of injective left R-modules is injective.*

Proposition 2.2.6. *Every direct summand of injective left R-modules is injective.*

Proof. Without loss of generality, let $I = I_1 \oplus I_2$ be an injective module, with $i : I_1 \to I$ the natural injection and $p : I \to I_1$ the natural projection so that $pi = id_{I_1}$. Consider the following diagram.

$$\begin{tikzcd}
 & I_1 \arrow[r, shift left, "i"] & I_1 \oplus I_2 \arrow[l, shift left, "p"] \\
0 \arrow[r] & B \arrow[u, "h"] \arrow[r, "j"] & C \arrow[u, dotted, "g_0"']
\end{tikzcd}$$

Let $j : B \to C$ be an injective map and $h : B \to I_1$ any map, we have to show that there exists a map $g : C \to I_1$ such that $gj = h$. Now $ih : B \to I$ is a map, therefore due to injectivity of I there exists a map $g_0 : C \to I$ such that $g_0 j = ih$. Now $g = pg_0$ is the required map, as $gj = pg_0 j = pih = id_{I_1} h = h$. Therefore I_1 which is a direct summand of I is injective. □

Theorem 2.2.7 (Baer Criterion)**.** *A left R-module is injective if and only if every R-map $f : I \to E$, where I is an ideal of R, can be extended to $g : R \to E$*

Proof. Let E be an injective R-module. Consider the following diagram.

$$\begin{tikzcd}
 & E & \\
0 \arrow[r] & I \arrow[u, "h"] \arrow[r, "i"] & R \arrow[ul, dashed, "g"']
\end{tikzcd}$$

Where I is an ideal in R. Since I and R are R-modules themselves, the existence of g is just a specific case of the definition of injective module.

Conversely, suppose that every map $h : I \to E$ can be extended to a map $g : R \to E$. Then consider the following diagram.

$$\begin{tikzcd}
 & E & \\
0 \arrow[r] & A \arrow[u, "f"] \arrow[r, "i"] & B
\end{tikzcd}$$

where A and B are R-modules, $i : A \to B$ an injective map and $f : A \to E$ any map. We have to show that there exists $g : B \to E$ such that $gi = f$. For convenience of notation, assume i to be inclusion. Let $\mathcal{A}$ be the set of all ordered pair (A', g') such that $A \subseteq A' \subseteq B$ and $g' : A' \to E$ is an extension of g. $\mathcal{A}$ is non-empty as (A, g) is in $\mathcal{A}$. We define a partial order on $\mathcal{A}$, where $(A', g') \leq (A'', g'')$ if $A' \subseteq A''$ and restriction of g'' to A' is g'. This set has an upper bound and thus by Zorn's lemma there is a maximal element (A_0, g_0). It can be shown that $A_0 = B$ using the hypothesis and thus E is injective. □

Definition 2.2.8. *Let M be a R-module over a domain R, we say $m \in M$ is divisible by $r \in R$, if $\exists m' \in M$ such that $m = rm'$. M is called a divisible module if each $m \in M$ is divisible by every $r \in R$.*

Divisible R-modules have the following properties.

1. Frac(R) is a divisible R-module.
2. Direct sums and direct products of divisible R-modules are divisible.
3. Every quotient of a divisible R-module is divisible. It follows that direct summands of divisible R-modules are divisible.

Theorem 2.2.9. *Let R be a domain, then every injective module is a divisible module. The converse is also true when R is a PID.*

Proof. Suppose that E is an injective R-module, then we have to show that E is divisible, that is , given any $m \in E$ and $r_0 \in R$ we have to find a $x \in E$ such that $m = r_0 x$. We define a map $f : (r_0) \to E$ where $f(rr_0) = er_0$. Since E is injective there exists an extension $g : R \to E$. Now $1e = f(1r_0) = h(r_0 1) = r_o h(1)$, thus the required $x = h(1)$. Conversely, let E be a divisible R-module, where R is a PID. Suppose there is a map $f : I \to E$ where I is an ideal of R. Since R is a PID $I = (a)$ for some $a \in R$, and since E is a divisible module, there exists a $e \in E$ such that $f(a) = ae$ as $f(a) \in E$ and $a \in I \subseteq R$. Define $h : R \to E$ such that $h(s) = se$. Also h extends f as for any $s = ra \in I$, $h(s) = h(ra) = rae = rf(a) = f(ra) = f(s)$. Thus by Baer's criterion E is an injective module. □

Lemma 2.2.10. *Every abelian group M can be embedded as a subgroup of some injective ableian group.*

Proof. Every abelian group M is the quotient of some free abelian group $F = \bigoplus_i \mathbb{Z}_i$. Thus $M = F/T = \bigoplus_i \mathbb{Z}_i/T$ for some $T \subseteq F$. Thus we can embed $M = \bigoplus_i \mathbb{Z}_i/T \subseteq \bigoplus_i \mathbb{Q}_i/T$ which is induced from the inclusion of $\mathbb{Z}$ in $\mathbb{Q}$. As $\mathbb{Q} = Frac(\mathbb{Z})$, $\mathbb{Q}$ is divisible so is $\bigoplus_i \mathbb{Q}_i$, thus the quotient $\bigoplus_i \mathbb{Q}_i/T$ is also divisible. Since $\mathbb{Z}$ is a PID, divisible $\mathbb{Z}$-modules are injective, thus we have embedded M inside the injective $\mathbb{Z}$ module $\bigoplus_i \mathbb{Q}_i/T$. □

Lemma 2.2.11. *If D is a divisible abelian group, then $Hom_{\mathbb{Z}}(R, D)$ is an injective left R-module.*

Proof. $\text{Hom}_{\mathbb{Z}}(R, D)$ is a left R-module. If $f \in \text{Hom}_{\mathbb{Z}}(R, D)$, then for $a \in R$, $(af)(r) = f(ra)$ $\forall r \in R$. Now to show that $\text{Hom}_{\mathbb{Z}}(R, D)$ is injective, we have to show that $\text{Hom}_R(\square, Hom_{\mathbb{Z}}(R, D))$ is an exact functor. By adjoint isomorphism theorem, this is isomorphic to the functor $Hom_{\mathbb{Z}}(R \otimes_R \square, D)$. This is the composition of the two functors $R \otimes_R \square$ and $Hom_{\mathbb{Z}}(\square, D)$. Since D is an injective $\mathbb{Z}$-module, $Hom_{\mathbb{Z}}(\square, D)$ is an exact functor and $R \otimes_R \square$ is naturally isomorphic to the identity functor, and thus is also exact, which gives us that their composition is also exact. □

Theorem 2.2.12. *The category of $_R$**Mod** has enough injectives. If M is an R-module, then there exists an injective R-module E with an injective homomorphism $i : M \to E$.*

Proof. Since every module is an abelian group, we can regard M as an abelian group and we have an injective map $\psi : M \to Hom_{\mathbb{Z}}(R, M)$, where $m \in M$, $m \mapsto \psi_m$ and $\psi_m(r) = (rm)$ $\forall r \in R$. ψ is an injective map because if $\psi_m = \psi'_m$ then $rm = rm'$ $\forall r \in R$, thus is true for $r = 1_R$ which gives us $m = m'$. By lemma 3.2.8 there exists a injective abelian group D with an injective map $i : M \to D$. Now since $Hom_{\mathbb{Z}}(R, \square)$ is a left exact functor, the induced map $i' : Hom_{\mathbb{Z}}(R, M) \to Hom_{\mathbb{Z}}(R, D)$ is also injective. Thus we have $i'\psi : M \to Hom_{\mathbb{Z}}(R, D)$ is also injective. From lemma 3.2.9 $Hom_{\mathbb{Z}}(R, D)$ is injective R-module, thus we only have to show that $i'\psi$ is a R-module homomorphism. Now let $b, r \in R$ and $m \in M$, $b\big((i'\psi)(m)(r)\big) = b\big((i'\psi_m)(r)\big) = i\psi_m(rb) = i(rbm)$, and $i'\psi(bm)(r) = i\psi_{bm}(r) = i(rbm)$. This shows that $i'\psi$ is an R homomorphism. □

2.3 Flat modules

Definition 2.3.1. *Let R be a ring, a right R-module A is flat if $A \otimes_R \square$ is an exact functor.*

That is to say, if $0 \to B \xrightarrow{f} C \xrightarrow{g} D \to 0$ is an short exact sequence of left R-modules, then the sequence $0 \to A \otimes_R B \xrightarrow{A \otimes_R f} A \otimes_R C \xrightarrow{A \otimes_R g} A \otimes_R D \to 0$ is exact. Since the functor $A \otimes_R \square$ is right exact it is equivalent to showing $A \otimes_R B \xrightarrow{A \otimes_R f} A \otimes_R C$ is injective whenever f is injective.

Since the functor $R \otimes_R \square$ is naturally isomorphic to the identity functor of ${}_R\mathbf{Mod}$, $R \otimes_R \square$ is exact, and thus the R-module R is a flat module.

Proposition 2.3.2. *A direct sum $\oplus_j M_j$ of right R-modules is flat* if and only if *each M_j is flat.*

Proposition 2.3.3. *Every projective right R-module is flat.*

Proof. Any free right R-module, which is a direct sum of copies of R is flat by proposition 2.3.2. Now any projective right R-module is direct summand of a free R-module and hence is flat, again from proposition 2.3.2. □

Proposition 2.3.4. *If every finitely generated submodule M of an R-module B is flat, then B is flat.*

Theorem 2.3.5. *If R is a domain and A is a flat R-module, then A is torsion free. The converse is true if R is a PID.*

Proof. If R is a domain and A a flat R-module, then from the exactness of $0 \to R \to Q$, where $Q = Frac(R)$, we get $0 \to R \otimes_R A \to Q \otimes_R A$ to be exact. Since $R \otimes_R A \cong A$ we get an embedding of A in $Q \otimes_R A$ which is torsion free as it is a vector space over Q. Thus A is torsion free. Conversely, if R is a PID and if A is a torsion free R-module, then every finitely generated submodule of A is free hence flat. Thus A is flat by proposition 2.3.4. □

Chapter 3

Complexes, Ext groups and Tor groups

In this chapter we will explore about cochain complexes, projective resolution of any given R-module, and how they are used in defining certain invariant associated with the R-module, such as the Ext and Tor groups. This chapter is primarily based on results from [2]

3.1 Complexes

Definition 3.1.1. *Let $\mathcal{C}$ be a sequence of abelian group homomorphisms, $0 \to C^0 \xrightarrow{d_1} C^1 \xrightarrow{d_2} \dots \xrightarrow{d_{n-1}} C^{n-1} \xrightarrow{d_n} C^n \xrightarrow{d_{n+1}} \dots$. The sequence $\mathcal{C}$ is called a cochain complex, if the composition of any two successive maps is zero: $d_n \circ d_{n+1} = 0 \quad \forall n$.*

Definition 3.1.2. *The n^{th} cohomology group of a cochain complex $\mathcal{C}$ is the quotient group $ker(d_{n+1})/im(d_n)$ denoted by $H^n(\mathcal{C})$.*

There is an analogous concept called chain complex where the maps are descending, that is, of the form $\cdots \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} \cdots \xrightarrow{d_1} C_0 \to 0$. Here the groups $H_n(\mathcal{C}) = ker(d_n)/im(d_{n+1})$ are called the homology groups. Whatever statements and results we see in the following sections on cochain complexes and cohomology group has an analogous counterpart in chain complexes and homology groups. Note that if a cochain or chain complex is exact the cohomology groups and the homology groups respectively will be trivial, and vice versa. Thus the cohomology groups and homology groups can be considered as the measure of deviation from exactness of their respective complexes.

Definition 3.1.3. *Let $\mathcal{A} = \{A^n\}$ and $\mathcal{B} = \{B^n\}$ be cochain complexes. A homomorphism between these two complexes $\alpha : \mathcal{A} \to \mathcal{B}$ is a set of homomorphisms $\alpha_n : A^n \to B^n$ for all n, such that the following diagram commutes.*

$$\begin{tikzcd}
\cdots\cdots\cdots \arrow[r] & A^n \arrow[r, "d_n"] \arrow[d, "\alpha_n"] & A^{n+1} \arrow[r] \arrow[d, "\alpha_{n+1}"] & \cdots\cdots\cdots \\
\cdots\cdots\cdots \arrow[r] & B^n \arrow[r, "d'_n"] & B^{n+1} \arrow[r] & \cdots\cdots\cdots
\end{tikzcd}$$

Proposition 3.1.4. *A homomorphism of cochain complexes $\alpha : \mathcal{A} \to \mathcal{B}$, induces a group homomorphism between the cohomology groups $H^n(\mathcal{A})$ and $H^n(\mathcal{B})$ for all $n \geq 0$.*

If $\alpha : \mathcal{A} \to \mathcal{B}$ is a homomorphism, then $\alpha_n : A^n \to B^n$ takes elements of ker(d) into ker(d') and elements of im(d) into im(d'), due to the commutativity of the above diagram mentioned in definition 3.1.3. Thus it induces a homomorphism between the cohomology groups.

Definition 3.1.5. *Let $\mathcal{A} = \{A^n\}$, $\mathcal{B} = \{B^n\}$ and $\mathcal{C} = \{C^n\}$ be cochain complexes. A short exact sequence of cochain complexes $0 \to \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} \mathcal{C} \to 0$ is a sequence of homomorphisms of complexes such that $0 \to A^n \xrightarrow{\alpha_n} B^n \xrightarrow{\beta_n} C^n \to 0$ is exact for every n.*

Theorem 3.1.6 (Long exact sequence in cohomology)**.** *Let $0 \to \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} \mathcal{C} \to 0$ be a short exact sequence of cochain complexes. Then there is a long exact sequence of cohomology groups: $0 \to H^0(\mathcal{A}) \to H^0(\mathcal{B}) \to H^0(\mathcal{C}) \xrightarrow{\delta_0} H^1(\mathcal{A}) \to H^1(\mathcal{B}) \to H^1(\mathcal{C}) \xrightarrow{\delta_1} H^2(\mathcal{A}) \to \ldots$*

The maps between the cohomology group at each level are the induced maps from proposition 3.1.3. The δ_n maps are defined in the following. Let $d_n : A^n \to A^{n+1}$, $d'_n : B^n \to B^{n+1}$, $d''_n : C^n \to C^{n+1}$ be the cochain maps, and α_n and β_n as in definition 3.1.5. Then $\delta_n(\bar{c})$ where $\bar{c} \in H^n(\mathcal{C})$ is given by $\delta_n(\bar{c}) = \bar{a}$, where $c = \beta_n(b)$ and $d'_n(b) = \alpha_{n+1}(a)$ where $a \in A^{n+1}$, $b \in B^n$, $c \in C^n$ and c is a representative of the class $\bar{c}$ and $\bar{a}$ is the class of a in $H^{n+1}(\mathcal{A})$. The exactness of the long exact sequence can be proved by diagram chasing using the following commutative diagram.

$$\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\cdots & A^{n-1} \arrow[r, "d_n"] \arrow[d, "\alpha_{n-1}"] & A^n \arrow[r, "d_{n+1}"] \arrow[d, "\alpha_n"] & A^{n+1} \arrow[d, "\alpha_{n+1}"] & \cdots \\
\cdots & B^{n-1} \arrow[r, "d'_n"] \arrow[d, "\beta_{n-1}"] & B^n \arrow[r, "d'_{n+1}"] \arrow[d, "\beta_n"] & B^{n+1} \arrow[d, "\beta_{n+1}"] & \cdots \\
\cdots & C^{n-1} \arrow[r, "d''_n"] \arrow[d] & C^n \arrow[r, "d''_{n+1}"] \arrow[d] & C^{n+1} \arrow[d] & \cdots \\
& 0 & 0 & 0 &
\end{tikzcd}$$

3.2 Projective resolution and $\mathbf{Ext}_R^n(A, D)$ groups

Definition 3.2.1. *Let A be an R-module. A projective resolution of A is an exact sequence*

$$\ldots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \to \ldots \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \to 0$$

such that each P_i is a projective R-module.

Every R-module A has a projective resolution. This comes from theorem 2.1.9, that the category of ${}_R\mathbf{Mod}$ has enough projectives. We first apply the theorem to A to get $P_0 \xrightarrow{\epsilon} A \to 0$, then apply the theorem to $\ker(\epsilon)$ to get $P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \to 0$, and successively apply the theorem to the kernel of the previous map to get projective resolution of a given module, which by construction is exact and each P_n projective.

By taking homomorphisms into D for each term above, we get a cochain complex

$$0 \to \mathrm{Hom}_R(A, D) \xrightarrow{\epsilon} Hom_R(P_0, D) \xrightarrow{d_1} Hom_R(P_2, D) \xrightarrow{d_2} \ldots$$

Here the maps are the induced maps obatined from using $\mathrm{Hom}_R(\Box, D)$ on the projective resolution of A.

Definition 3.2.2. *The n^{th} cohomology groups of the above cochain complex is called Ext* *groups, given by*

$$Ext^n_R(A, D) = kerd_{n+1}/imd_n$$

where $Ext^0_R(A, D) = kerd_1$.

It can similarly be defined using an injective resolution of a R-module D

$$0 \to D \to E_0 \to E_1 \to E_2 \to \cdots$$

and the functor $\mathrm{Hom}_R(A, \Box)$.

Proposition 3.2.3. *For any R module* $Ext^0_R(A, D) = Hom_R(A, D)$

Proof. By definition $\mathrm{Ext}^0_R(A, D) = \mathrm{ker}d_1$, and since the functor $\mathrm{Hom}_R(A, \Box)$ is left exact $\ker(d_1) = \mathrm{im}(\epsilon) \cong \mathrm{Hom}_R(A, D)$, since ϵ is injective. $\Box$

Proposition 3.2.4. *Let* $f : A \to A'$ *be a homomorphism of R-modules, then for each n there exists a lift* f_n *between projective resolutions of A and* A' *such that the following diagram commutes.*

$$\begin{tikzcd}
\dots \arrow[r, "d_2"] & P_1 \arrow[r, "d_1"] \arrow[d, "f_2"] & P_0 \arrow[r, "\epsilon"] \arrow[d, "f_1"] & A \arrow[r] \arrow[d, "f"] & 0 \\
\dots \arrow[r, "d_2'"] & P_1' \arrow[r, "d_1'"] & P_o' \arrow[r, "\epsilon'"] & A' \arrow[r] & 0
\end{tikzcd}$$

This in turn gives us the following induced homomorphism between the two related cochain complexes

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_R(A, D) \arrow[r, "\epsilon"] & \mathrm{Hom}_R(P_0, D) \arrow[r, "d_1"] & \mathrm{Hom}_R(P_1, D) \arrow[r, "d_2"] & \dots \\
0 \arrow[r] & \mathrm{Hom}_R(A', D) \arrow[r, "\epsilon'"] \arrow[u, "f"'] & \mathrm{Hom}_R(P_0', D) \arrow[r, "d_1'"] \arrow[u, "f_1"'] & \mathrm{Hom}_R(P_1', D) \arrow[r, "d_2'"] \arrow[u, "f_2"'] & \dots
\end{tikzcd}$$

Proposition 3.2.5. $\forall\ n \geq 0$ *the induced group homomorphisms between the cohomology groups of the above cochain complexes* $\phi_n : Ext^n_R(A', D) \to Ext^n_R(A, D)$, *are independent of the choice of lifts* f_n.

Theorem 3.2.6. *The cohomology groups* $Ext^n_R(A, D)$ *are independent of the choice of projective resolution of the R-module A, and are only dependant on the R-modules A and D.*

Proof. Suppose there are two projective resolutions of A by P_is and P_i's. Consider the following diagram.

$$\begin{tikzcd}
{} \arrow[r, dotted] & P_1 \arrow[r] \arrow[d, "f_1"] & P_0 \arrow[r] \arrow[d, "f_0"] & A \arrow[r] \arrow[d, "f"] & 0 \\
{} \arrow[r, dotted] & P_1' \arrow[r] \arrow[d, "g_1"] & P_0' \arrow[r] \arrow[d, "g_0"] & A' \arrow[r] \arrow[d, "g"] & 0 \\
{} \arrow[r, dotted] & P_1 \arrow[r] & p_0 \arrow[r] & A \arrow[r] & 0
\end{tikzcd}$$

where $A = A'$ and $f = g = id_A$. Let ϕ_ns and ψ_ns be the maps induced on the cohomology groups by f_ns and g_ns respectively. If one considers the top and bottom rows of the diagram, g_nf_ns are lifts of gf, and $\psi_n\phi_n$ is the respective induced map between the cohomology groups. But $gf = id_Aid_A = id_A$ thus id_{P_i}s are also lifts of gf, and the maps on cohomology groups induced by id_{P_i}s are id. By proposition 3.2.5, $\psi_n\phi_n = id$ on the cohomology groups. Similarly $\phi_n\psi_n = id$ which gives us that ϕ_n and ψ_n are isomorphism on the cohomology groups. Thus the cohomology groups $\text{Ext}_R^n(A, D)$ are independent of the choice of projective resolution of the R-module A. □

Theorem 3.2.7. *Let $0 \to L \to M \to N \to 0$ be an exact sequence of R-modules. Then there exists long exact sequences of abelian groups*
$0 \to Hom_R(N, D) \to Hom_R(M, D) \to Hom_R(L, D) \xrightarrow{\delta_0} Ext_R^1(N, D) \to Ext_R^1(M, D) \to Ext_R^1(L, D) \xrightarrow{\delta_1} Ext_R^2(N, D) \to \dots$ *and*
$0 \to Hom_R(D, L) \to Hom_R(D, M) \to Hom_R(D, N) \xrightarrow{\delta_0} Ext_R^1(D, L) \to Ext_R^1(D, M) \to Ext_R^1(D, N) \xrightarrow{\delta_1} Ext_R^2(D, L) \to \dots$

We get the results by applying the appropriate Hom functors, $Hom_R(\Box, D)$ and $Hom_R(D, \Box)$ respectively to the diagram in lemma 3.2.8, and applying theorem 3.1.6 to the resulting exact sequence of cochain complex.

Lemma 3.2.8 (Horseshoe lemma)**.** *Let $0 \to L \to M \to N \to 0$ be an exact sequence of R-modules. If we have a projective resolution of L by P_is and projective resolution of N by P_i's, then we have the following commutative diagram where the rows and columns are exact.*

$$\begin{tikzcd}
 & {} \arrow[d, dotted] & {} \arrow[d, dotted] & {} \arrow[d, dotted] & \\
0 \arrow[r] & P_1 \arrow[r] \arrow[d] & P_1 \oplus P'_1 \arrow[r] \arrow[d] & P'_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_0 \arrow[r] \arrow[d] & P_0 \oplus P'_0 \arrow[r] \arrow[d] & P'0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Proposition 3.2.9. *A R-module Q is injective $\Leftrightarrow$ $Ext^n_R(A,Q) = 0 \quad \forall$ R-modules A and $\forall n \geq 1$.*

Proposition 3.2.10. *A R-module P is projective $\Leftrightarrow$ then $Ext^n_R(P,B) = 0 \quad \forall$ R-modules B abd $\forall n \geq 1$.*

Both the above propositions follows from theorem 3.2.7.

3.3 Tor$^R_n(A, B)$ groups

If D is a right R-module, then for every left R-module B, the tensor product $D \otimes_R B$ is an abelian group, and the functor $D \otimes_R \square$ is a right exact functor. If a projective resolution of B is

$$\ldots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \to \ldots \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} B \to 0$$

then on using $D \otimes_R \square$ functor we get the chain complex
$\ldots \xrightarrow{1 \otimes_R d_{n+1}} D \otimes_R P_n \xrightarrow{1 \otimes_R d_n} D \otimes_R P_{n-1} \to \ldots \xrightarrow{1 \otimes_R d_1} D \otimes_R P_0 \xrightarrow{1 \otimes_R \epsilon} D \otimes_R B \to 0.$

Definition 3.3.1. *The homology groups of the above chain complex are called tor groups denoted by*

$$Tor^R_n(D,B) = ker(1 \otimes_R d_n)/im(1 \otimes_R d_{n+1})$$

and $Tor^R_0(D,B) = D \otimes_R P_0/im(1 \otimes_R d_1)$.

Proposition 3.3.2. *For any right R-modudle B an left R-module D $Tor^R_0(D,B) \cong D \otimes_R B$*

Analogous to the results from the previous section on $\mathrm{Ext}_R^n(A, D)$ groups we have the following

If $f : B \to B'$ is a R-module homomorphism, then there is an induced group homomorphism $\psi_n : \mathrm{Tor}_n^R(D, B) \to \mathrm{Tor}_n^R(D, B')$ on the homology groups, depending only on f.

Theorem 3.3.3. *The homology groups $Tor_n^R(D, B)$ are independent of the choice of projective resolution of B.*

Theorem 3.3.4. *Let $0 \to L \to M \to N \to 0$ be an exact sequence of R-modules. Then there exists long exact sequences of abelian groups $\cdots \to Tor_2^R(D, N) \xrightarrow{\delta_1} Tor_1^R(D, L) \to Tor_1^R(D, M) \to Tor_1^R(D, N) \xrightarrow{\delta_0} D \otimes_R L \to D \otimes_R M \to D \otimes_R N \to 0$*

Proposition 3.3.5. *A right R-module D is flat $\Leftrightarrow$ $Tor_n^R(D, B) = 0 \quad \forall$ left R-modules B and $\forall n \geq 1$.*

The proofs for the propositions and theorems presented above in this section are almost identical and analogous to the ones in the previous section on Ext groups, and hence are omitted.

Proposition 3.3.6. *Let A and B be $\mathbb{Z}$-modules and let $t(A)$ and $t(B)$ denote respective their torsion submodules, then $Tor_1^{\mathbb{Z}}(A, B) \cong Tor_1^{\mathbb{Z}}(t(A), t(B))$.*

Proof. We know that over a PID R, an R-module B is flat if and only if B is torsion free. Here $B/t(B)$ is a torsion free $\mathbb{Z}$-module. Consider the exact sequence $0 \to t(B) \xrightarrow{i} B \xrightarrow{p} B/t(B) \to 0$, where i is the natural inclusion and p the natural projection. By theorem 3.3.4 we get the following exact sequence $\cdots \to \mathrm{Tor}_2^R(A, B/t(B)) \xrightarrow{\delta_1} \mathrm{Tor}_1^R(A, t(B)) \to \mathrm{Tor}_1^R(A, B) \to \mathrm{Tor}_1^R(A, B/t(B)) \xrightarrow{\delta_0} A \otimes_R t(B) \to A \otimes_R B \to A \otimes_R B/t(B) \to 0$. And by proposition 3.3.5, it reduces to $0 \to \mathrm{Tor}_1^R(A, t(B)) \to \mathrm{Tor}_1^R(A, B) \to 0$ since $B/t(B)$ is flat, which gives us $\mathrm{Tor}_1^{\mathbb{Z}}(A, B) \cong \mathrm{Tor}_1^{\mathbb{Z}}(A, t(B))$. Similarly $\mathrm{Tor}_1^{\mathbb{Z}}(A, B) \cong \mathrm{Tor}_1^{\mathbb{Z}}(t(A), B)$, which combined with the previous result gives us $\mathrm{Tor}_1^{\mathbb{Z}}(A, B) \cong \mathrm{Tor}_1^{\mathbb{Z}}(t(A), t(B))$. □

Chapter 4

Group cohomology

In this chapter we will explore about cohomology of groups and related results such as shapiro's lemma. This chapter is primarily based on results from [2]

Definitions 4.0.1. *Let G be a group. An abelian group A on which G acts on the left as automorphisms is called a G-module. We define A^G to be the set of elements in A, fixed by all elements of G. A G-module homomorphism $\phi : A \to B$ is a map such that*

$$\phi(g.a) = g.\phi(a) \qquad \forall g \in G, a \in A.$$

Example 8. *If we take A to be the vector space $\mathbb{R}^n$ and $G = GL_n(\mathbb{R})$ then A is a G-module with the element of G acting as linear transformations on A.*

Theorem 4.0.2. *The category of ${}_G$**Mod** is equivalent to the category of ${}_{\mathbb{Z}G}$**Mod**.*

Where ${}_G$**Mod** is the category of G-modules and ${}_{\mathbb{Z}G}$**Mod** is the category of the modules of the group ring $\mathbb{Z}G$.

Proposition 4.0.3. *Suppose A is a G-module and $Hom_{\mathbb{Z}G}(\mathbb{Z}, A)$ is the group of all $\mathbb{Z}G$ module homomorphisms from $\mathbb{Z}$ (trivial G action on $\mathbb{Z}$) to A, then $Hom_{\mathbb{Z}G}(\mathbb{Z}, A) \cong A^G$.*

Proof. A $\mathbb{Z}G$-module homomorphism $f : \mathbb{Z} \to A$ is completely determined by its value on generator of $\mathbb{Z}$ which is $1_{\mathbb{Z}}$. Let us denote by f_a the map $1 \mapsto a$. We have $a = f_a(1) = f_a(g.1) = g.f_(1) = g.a$ as G acts trivially on $\mathbb{Z}$. Thus $a \in A^G$. For the other way, let $b \in A^G$.

Let f_b be the $\mathbb{Z}$-map with $f_b(1) = b$, since $b \in A^G$, f_b is also a $\mathbb{Z}G$-map, that is a G-module homomorphism since $f_b(g.m) = f_b(m) = mf_b(1) = mb = g.mb = gf_b(m)$. Thus we have the required bijection between $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$ and A^G □

Thus a short exact sequence of G-modules $0 \to A \to B \to C \to 0$, gives an exact sequence $0 \to A^G \to B^G \to C^G$. If we have a projective $\mathbb{Z}G$-module resolution of $\mathbb{Z}$, we can extend the above sequence on the right. One such common resolution is the standard or bar resolution of $\mathbb{Z}$, given by

$$\ldots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} F_{n-1} \to \ldots \xrightarrow{d_1} F_0 \xrightarrow{aug} \mathbb{Z} \to 0$$

where $F_n = \mathbb{Z}G \otimes_{\mathbb{Z}} \mathbb{Z}G \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}G$ ($n+1$ terms). F_n is a free $\mathbb{Z}G$-module with basis of the form $(1 \otimes_{\mathbb{Z}} \ g_1 \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} g_n)$, and G action on the simple tensors given by $g.(g_0 \otimes_{\mathbb{Z}} \ g_1 \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} g_n) = (g.g_0 \otimes_{\mathbb{Z}} \ g_1 \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} g_n)$ and the map aug given by $\Sigma_{g \in G} \alpha_g g \mapsto \Sigma_{g \in G} \alpha_g$.

Using $\mathrm{Hom}_{\mathbb{Z}G}(\square, A)$ functor on the bar resolution of $\mathbb{Z}$ we get the following cochain complex,

$$0 \to \mathrm{Hom}_{\mathbb{Z}G}(F_0, A) \xrightarrow{d_1} \mathrm{Hom}_{\mathbb{Z}G}(F_1, A) \xrightarrow{d_2} \cdots \xrightarrow{d_n} \mathrm{Hom}_{\mathbb{Z}G}(F_n, A) \to \cdots$$

We can simplify the cochain complex in the following way to make working with them more explicit.The elements of $\mathrm{Hom}_{\mathbb{Z}G}(F_n, A)$ are completely determined by their value on the basis elements of F_n as a $\mathbb{Z}G$-module, which are of the form $(1 \otimes_{\mathbb{Z}} \ g_1 \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} g_n)$, which can be identified with the n-tuple $(g_1, g_2, \ldots, g_n) \in G \times \cdots \times G$. Thus the group $\mathrm{Hom}_{\mathbb{Z}G}(F_n, A)$ can be identified with the set of functions from $G^n = G \times \cdots \times G$ to A.

Definition 4.0.4. *We define $C^n(G, A)$ to be the set of all functions from G^n to A, with $C^0(G, A)$ defined to be A.*

Each $C^n(G, A)$ is an additive abelian group with operation given by $(f_1 + f_2)(g_1, g_2, \ldots, g_n) = f_1(g_1, g_2, \ldots, g_n) + f_2(g_1, g_2, \ldots, g_n) \quad \forall f_1, f_2 \in C^n(G, A)$

Definition 4.0.5. *We define $d_0 : C^0(G, A) \to C^1(G, A)$ by $d_1(f)(g) = g.f - f$ and for $n \geq 1$*

we define the n^{th} co-boundary homomorphism $d_n : C^n(G,A) \to C^{n+1}(G,A)$ by ,

$$\begin{aligned} d_n(f)(g_1,\ldots,g_{n+1}) =& g_1 \cdot f\left(g_2,\ldots,g_{n+1}\right) \\ &+ \sum_{i=1}^{n} (-1)^i f\left(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_{n+1}\right) \\ &+ (-1)^{n+1} f\left(g_1,\ldots,g_n\right) \end{aligned}$$

We will see why the co-boundary homomorphisms are of this form in a later chapter. Thus with the above definitions the above cochain complex becomes

$$0 \to C^0(G,A) \xrightarrow{d_1} C^1(G,A) \xrightarrow{d_2} \cdots \xrightarrow{d_n} C^n(G,A) \to \cdots$$

Definition 4.0.6. *1. For $n \geq 0$ let $Z^n(G,A) = ker(d_n)$, which are called the group of n-cocyles.*

2. For $n \geq 1$ $B^n(G,A) = im(d_{n-1})$,which are called the group of n-coboundaries.

Thus the cohomology group becomes $H^n(G,A) = \mathrm{ker}d_n/\mathrm{im}d_{n-1} = Z^n(G,A)/B^n(G,A)$.

For $n = 0$, $C^0(G,A) \cong A$.Thus any $f \in C^0(G,A)$ can be identified with some $a \in A$, thus $d_0(f)(g) = g.f - f = g.a - a$. Thus $\ker(d_0)$ is the set $\{a \in A \mid g.a - a = 0\}$ which is nothing but A^G. Thus $H^0(G,A) = \ker(d_0) = A^G$.

For $n = 1$, $C^1(G,A)$ is the set of all functions $f : G \to A$. Now if $f \in Z^1(G,A)$ then by the definition of the co boundary map d_1, $d_1 f(g_1,g_2) = g_1.f(g_2) - f(g_1g_2) + f(g_1) = 0$. Thus we get $f(g_1g_2) = f(g_1) + g_1.f(g_2)$. Such functions are called crossed homomorphisms. If $f \in B^1(G,A)$ then f is of the form $f(g) = g.a - a$ for some $a \in A$. Now if the action of G on A is trivial, then $g_1.f(g_2) = f(g_2)$, thus f is a 1-cocyle if $f(g_1g_2) = f(g_1) + f(g_2)$, that is, f is a group homomorphism between G and A. And the 1-coboundary becomes $f(g) = g.a - a = a - a = 0$. Thus for a group G with trivial action on A, the group $H^1(G,A) = Hom(G,A)$ is the set of group homomorphisms between G and A.

Example 9.

Let G be cyclic of order m with generator σ. Let $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{m-1} \in \mathbb{Z}G$.

Then $N(\sigma-1)=(\sigma-1)N=\sigma^n-1=0$. This gives a simple projective $\mathbb{Z}G$ resolution of $\mathbb{Z}$

$$\ldots \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \ldots \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{\text{aug}} \mathbb{Z} \longrightarrow 0$$

Using the functor $\mathrm{Hom}_{\mathbb{Z}G}(\square, A)$, the above exact sequence becomes the complex

$$0 \longrightarrow A \xrightarrow{\sigma-1} A \xrightarrow{N} A \xrightarrow{\sigma-1} A \xrightarrow{N} \ldots$$

From the above chain complex kernel of the map N are the $a \in A$ annihilated by N thus $\ker(N) =_N A$ and kernel of $\sigma - 1$ are the elemenets of A fixed by G which is A^G.

Thus

$$H^n(G,A) = \begin{cases} ker(\sigma-1)/im(N) = A^G/NA & \text{if } n \text{ is even, } n \geq 2 \\ ker(N)/im(\sigma-1) = NA/(\sigma-1)A & \text{if } n \text{ is odd, } n \geq 1 \end{cases}$$

Proposition 4.0.7. *Suppose $mA = 0$ for some integer $m \geq 1$. Then $mZ^n(G,A) = mB^n(G,A) = mH^n(G,A) = 0$ for all $n \geq 0$*

Theorem 4.0.8. *(Long exact sequence in group cohomology) Suppose there is a short exact sequence of G-module $0 \to A \to B \to C \to 0$. Then there is a exact sequence of abelain group $0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta_0} H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,C) \xrightarrow{\delta_1} \cdots \xrightarrow{\delta_{n-1}} H^n(G,A) \longrightarrow H^n(G,B) \longrightarrow H^n(G,C) \xrightarrow{\delta_n} H^{n+1}(G,A) \longrightarrow \cdots$*

This comes form applying theorem 3.2.7 to the exact sequence $0 \to A \to B \to C \to 0$ of $\mathbb{Z}G$-modules.

Definition 4.0.9. *A G-module M is called cohomologically trivial for G if $H^n(G,M) = 0 \quad \forall n \geq 1$.*

Corollary 4.0.10. *If $0 \to A \to M \to C \to 0$ is a short exact sequence of G-modules where M is cohomologically trivial, then*

$$H^{n+1}(G,A) \cong H^n(G,C) \quad \textit{for all } n \geq 1$$

Proof. Applying theorem 4.0.8 to the given short exact sequence and noting that $H^n(G,M) = 0 \quad \forall n \geq 1$, we get the exact sequences $0 \to H^n(G,C) \xrightarrow{\delta_n} H^{n+1}(G,A) \to 0$, which gives us the required isomorphism. □

Definition 4.0.11. *If H is a subgroup of G and A is a H-module, we define the induced G-module $M_H^G(A)$ as $Hom_{\mathbb{Z}H}(\mathbb{Z}G, A)$.*

Proposition 4.0.12. *If H is a subgroup of G with finite index, then $M_H^G(A) \cong \mathbb{Z}G \otimes_{\mathbb{Z}H} A$.*

Proposition 4.0.13 (Shapiro's lemma)**.** *For any subgroup H of G and any H-module A, we have $H^n\left(G, M_H^G(A)\right) \cong H^n(H, A), \quad \forall n \geq 0$.*

Proof. Let $\cdots \to P_n \to \cdots \to P_0 \to \mathbb{Z} \to 0$ b a projective $\mathbb{Z}G$ resolution of $\mathbb{Z}$. We get the cohomology groups by taking $\mathbb{Z}G$ homomorphisms into $M_H^G(A)$ which makes the terms in the cochain complex to be $Hom_{\mathbb{Z}G}(P_n, M_H^G(A)) = Hom_{\mathbb{Z}G}(P_n, Hom_{\mathbb{Z}H}(\mathbb{Z}G, A))$. Now since $\mathbb{Z}G$ is a free $\mathbb{Z}H$-module, the same projective resolution of $\mathbb{Z}$ can be taken as a projective $\mathbb{Z}H$ resolution, and the terms in the cochain comlex will be $Hom_{\mathbb{Z}H}(P_n, A)$. But by adjoint isomorphism theorem, $Hom_{\mathbb{Z}G}(P_n, Hom_{\mathbb{Z}H}(\mathbb{Z}G, A)) \cong Hom_{\mathbb{Z}H}(P_n, A)$. Thus we have $H^n\left(G, M_H^G(A)\right) \cong H^n(H, A), \quad \forall n \geq 0$ □

Chapter 5

Topological Groups

Topological groups are topological spaces which also admits a group structure on the underlying set in a compatible way. Various new properties arises due to having both a topology on the set and an algebraic structure in a compatible way. In this chapter a few such properties will be explored which will be helpful later when exploring profinite groups. First is to see how the two structures are combined in a compatible way. This chapter is primarily based on results from [4]

Definition 5.0.1. *A topological group is a set G which is a group as well as a topological space with the group structure and topology related by the axiom that the maps $m : G{\times}G \to G$, $(x, y) \mapsto xy$ and $i : G \to G, \quad x \mapsto x^{-1}$ are continuous where $x, y \in G$ and x^{-1} is the inverse of x in G.*

Example 10. *The additive group of real numbers $\mathbb{R}$ with the usual topology(euclidean). Any abstract group with the discrete topology.*

Some general properties of topological spaces are listed

1. if $z = xy$ and W a neighbourhood of z, then there exists neighbourhoods U and V of x and y respectively such that $UV \subseteq W$.
   Similarly for every neighbourhood P of a there exists a neighbourhood Q of a^{-1} such that $Q^{-1} \subseteq P$.

2. For each $x \in G$ the maps $y \mapsto xy$ and $y \mapsto yx$ are homeomorphisms.

3. Similarly the map $z \mapsto z^{-1}$ is a homeomorphism.

4. If U is any open subset of G, then zU, Uz, U^{-1}, PU and UP are all open in G for any $z \in G$ and any subset $P \subseteq G$ of G.

5. If U is any neighbourhood of $e \in G$, then there exsits a neighbourhood V of e such that, $VV^{-1} \subseteq U$.

6. Every neighbourhood P of e contains a symmetric neighbourhood, that is, a neighbourhood Q of e such that $Q = Q^{-1}$.

7. Every neighbour hood of a $z \in G$ is of the form zU and Vz such that U and V are neighbourhoods of e.

8. The map $(x, y) \mapsto xy^{-1}$ is continuous if and only if the maps $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are both continuous.

Proposition 5.0.2. *If $P \subseteq G$, then the closure $\bar{P}$ of P is given by $\bar{P} = \bigcap PU = \bigcap UP$, where U runs over all the neighbourhoods of the identity e.*

Proof. Let $x \in \bigcap PU$. Let O be a neighbourhood of x. Then O is of the form $O = xU$ for some U neighbourhood of e. Since $x \in PU$ for all U neighbourhood of e, $x \in PU^{-1}$, thus $x = py^{-1}$ where $p \in P$ and $y \in U$. Therefore $xy = p \in xU$. Thus $O = xU$ intersects P. We have thus shown that any neighbourhood O of x intersects P, thus $x \in \bar{P}$, therefore $\bigcap PU \subseteq \bar{P}$.

For the reverse inclusion, let $x \in \bar{P}$. Then every neighbourhood of x intersects P. Therefore xU^{-1} which is also a neighbourhood of x intersects P. This shows that $xy^{-1} = p$ for some $y \in U$ and $p \in P$ which implies $py = x \in PU$. Since the choice of U was arbitrary $x \in PU$ for all neighbourhood U of e. Thus $x \in \bigcap PU$, therefore $\bar{P} \subseteq \bigcap PU$. □

Definition 5.0.3. *A subset H of a topological group G is a subgroup of the topological group G if and only if H is a closed subset of G and a subgroup of the abstract group G.*

Proposition 5.0.4. *If H is a subgroup of G, then $\bar{H}$ is also a subgroup.*

Proof. Since $H \subseteq \bar{H}$, $\bar{H}$ is non-empty. Let $a, b \in \bar{H}$, we have to show that $ab^{-1} \in \bar{H}$. Let U be a neighbourhood of ab^{-1}. We know that the map $f : G \times G \to G$ such that $(x, y) \mapsto xy^{-1}$ is a continuous map, since G is a topological group. Thus there exists neighbourhoods A

and B of a and b respectively such that $f(A \times B) \subseteq U$. Since $a, b \in \bar{H}$, every neighbourhood of a and b intersects with H, thus $\exists x, y$ such that $x \in A \cap H$ and $y \in B \cap H$. Thus $f(x, y) = xy^{-1} \in U$ as well as $xy^{-1} \in H$ since H is a subgroup. Therefore U intersects H. Since we hav shown that any neighbourhood U of ab^{-1} intersects with H,$ab^{-1} \in \bar{H}$. □

Proposition 5.0.5. *if N is a normal subgroup of G, then $\bar{N}$ is also a normal subgroup.*

Proof. Since N is a subgroup , so is $\bar{N}$ from the previous proposition, therefore we have to show that $\bar{N}$ is normal in G. Let $x \in \bar{N}$ and $g \in G$, let O be a neighbourhood of gxg^{-1}, it will be of the form $Vgxg^{-1}$ for some neighbourhood V of e. Let $W = g^{-1}Vg$, since $e \in V$, $g^{-1}eg = e \in W$. Therefore W is a neighbourhood of e. Thus Wx which will be a neighbourhood of x will intersect with N, let $n \in Wx \cap N$. Since N is normal in G, $gng^{-1} \in N$, also $gng^{-1} \in gWxg^{-1} = gg^{-1}Vgxg^{-1} = Vgxg^{-1}$. Thus $gng^{-1} \in Vgxg^{-1} \cap N$. We have show that any neighbourhood of gxg^{-1} intersects with N, therefore $gxg^{-1} \in \bar{N}$. □

Proposition 5.0.6. *If a topological group G is T_1 then G is Hausdorff.*

Proof. Let $g, h \in G$ such that $g \neq h$, then $h^{-1}g \neq e$. Let U be a neighbourhood of e such that $h^{-1}g \notin U$, such a neighbourhood exists as G is a T_1 space. Now by a previous property (5), there exists a neighbourhood V of e such that $VV^{-1} \subseteq U$. Now gV and hV are neighbourhoods of g an h respectively. And $gV \cap hV = \emptyset$, as if not, then there exists $v_1, v_2 \in V$ such that $gv_1 = hv_2$. This gives us $h^{-1}g = v_2v_1^{-1} \in VV^{-1} \subseteq U$ which is a contradiction. □

Proposition 5.0.7. *If G is a T_1 space then G/H is T_1 space, π is a open map and G is Hausdorff.*

Proof. H is a closed subset of G, thus its image xH under the homeomorphism given in (2) is also closed. Therefore the set $G - xH = (xH)^c$ is open. Now $xH = \bar{x} \in G/H$ and $\pi^{-1}(G - \bar{x}) = G - xH = xH)^c$ is open, thus $\{\bar{x}\}$ is closed G/H. As singleton sets are closed in G/H, it is a T_1 space.

Now the natural surjection $\pi : G \to G/H$ is a continuous map. Let U be an open set in G. Then $\pi(U)$ in the coset space G/H is open if and only if $\pi^{-1}\pi(U)$ is open in G as G/H has the quotient topology. We note that $\pi^{-1}\pi(U) = OH$ which is open by (4). We have shown that π maps open sets to open sets, thus is a open map.

Now to show that G/H is Hausdorff (T_2). Let $\bar{g}$ and $\bar{k}$ be distinct points of G/H and let

$g, k \in G$ such that $\pi(g) = \bar{g}$ and $\pi(k) = \bar{k}$. We choose a neighbourhood U of e such that, $Ug \cap kH = \emptyset$. Such a neighbourhood exists as $g \notin kH = \bar{kH}$ as H is closed and so is kH, which implies $g \in \bar{kH}^c$ thus there exists a neighbourhood U of e such that $Ug \subseteq \bar{kH}^c$. This shows that $UgH \cap kH = \emptyset$, otherwise $\exists h_1, h_2 \in H$ and $\exists u \in U$ such that $ugh_1 = kh_2$ $\implies$ $ug = kh_2h_1^{-1} \in kH$ which is a contradiction. Now let V be a neighbourhood of e such that $V^{-1}V \subseteq U$(see (5)). $V^{-1}VgH \cap kH = \emptyset$ from which we get $VgH \cap VkH = \emptyset$. Otherwise $\exists h_1, h_2 \in H$ and $v_1, v_2 \in V$ such that $v_1gh_1 = v_2kh_2 \implies v_2^{-1}v_1gh_1 = kh_2 \in V^{-1}VgH \cap kH = \emptyset$ which is a contradiction. Therefore $\pi(Vg) \cap \pi(Vk) = \emptyset$. Now $g \in \pi(Vg)$ and $k \in \pi(Vk)$ are separated by open neighbourhoods as π is a open map. Thus G/H is Hausdorff.

□

Proposition 5.0.8. *If G is a topological group with H a normal subgroup, then G/H with the quotient topology is a topological group.*

Proof. We have to show that the map $\psi' : G/H \times G/H \to G/H$ such that $(x, y) \mapsto xy^{-1}$ $x, y \in G/H$ is continuous. Let $\psi : G \times G \to G$ such that $(g, k) \mapsto gk^{-1}$. Then ψ is continuous as G is a topological group. Now consider the following diagram.

$$\begin{tikzcd}
G \times G \arrow[r, "\pi \times \pi"] \arrow[d, "\psi"] & G/H \times G/H \arrow[d, "\psi'"] \\
G \arrow[r, "\pi"] & G/H
\end{tikzcd}$$

Form the diagram, we have $\pi\psi = \psi'(\pi \times \pi)$. Since G is a topological group both π and ψ are continuous and thus so is $\pi\psi$, which gives us that $\psi'(\pi \times \pi)$ is continuous. Now let U be a open set in G/H. $(\psi'(\pi \times \pi))^{-1}(U) = (\pi \times \pi)^{-1}\psi'^{-1}(U)$ is open, but $\pi \times \pi$ is a open map, thus $(\pi \times \pi)(\pi \times \pi)^{-1}\psi'^{-1}(U)$ is open, which gives us that $\psi'^{-1}(U)$ is open in $G/H \times G/H$. Therefore ψ' is continuous which gives us that G/H is a topological group. □

Proposition 5.0.9. *Let G be a compact topological group and H be it's subgroup then, H and G/H are both compact.*

Proof. Since H is a subgroup of the topological group G, H is closed in G, which gives us that H is compact, as closed subset of a compact space is compact. And G/H is the continuous image of a compact set G under the continuous map π, thus G/H is also compact. □

Chapter 6

Profinite groups and Pro-p groups

In this chapter we'll explore profinite groups, a notion of order and index of profinite group using supernatural numbers and Sylow theorem of profinite groups. Then we move to the cohomology of profinite groups and related results. This chapter is primarily based on results from [3], [6], [7]

Definition 6.0.1. *A topological group which is the inverse limit of a collection of finite groups, each given the discrete topology is called a profinite group.*

In other words $G = \varprojlim_{i \in I} G_i$, where $\{G_i, \phi_{ij}\}_{i \in I}$ is a inverse system of finite discrete topological groups.

Proposition 6.0.2. *If G is a profinite group, then G as a topological group is compact, Hausdorff and totally disconnected.*

Proof. Since G is a profinite group, $G = \varprojlim_{i \in I} G_i$ for some inverse system of finite discrete topological groups $\{G_i, \phi_{ij}\}_{i \in I}$. Now since each G_i is a finite group with discrete topology thus each of the G_i is compact and Hausdorff, which gives us that the product $\prod_{i \in I} G_i$ is compact (by Tychonoff'S theorem) and Hausdorff. Now if $p_i : \prod_{i \in I} G_i \to G_i$ is the natural projection and if $C \subseteq \prod_{i \in I} G_i$ is a connected component, then the image $p_i(C)$ is a connected component in G_i as p_i is a continuous map. But G_i has discrete topology, thus $p_i(C)$ should be a singleton set. Now $C = (p_i(C))_{i \in I}$, and since every $p_i(C)$ is a singleton $\forall i \in I$, C is a

singleton set in $\prod_{i\in I} G_i$ and thus, $\prod_{i\in I} G_i$ is totally disconnected.
Now $\varprojlim_{i\in I} G_i \subseteq \prod_{i\in I} G_i$ and is in fact a closed subgroup. The argument for why it is a closed subgroup is similar to the one in proposition 6.1.5. Since closed subset of a compact space is compact $\varprojlim_{i\in I} G_i$ is compact, Hausdorff and totally disconnected.

□

This gives us an idea of the topology of a profinite group. In fact the converse of proposition 6.0.2 also true, but to show it, we need a few results on topological space which we'll see below.For the sake of convenience we'll refer to a set which is both closed and open as clopen.

Lemma 6.0.3. *Let X be a compact Hausdorff topological space and lext $x \in X$. Then the connected component C_x of x is the intersection of all clopen neighbourhoods of x.*

Proof. Let $\{V_t \big| t \in T\}$ be the family of clopen neighbourhoods of x and let $B = \bigcap\limits_{t\in T} V_t$. Since every clopen neighbourhood of x contain it's connected component, we have $C_x \subseteq B$. To prove the equality of C_x and B, it is sufficient to show that B is connected. Suppose $B = U \cup V$ where both the sets are closed in B, and $U \cap V = \emptyset$. Since X is compact Hausdorff space and U and V are compact and disjoint subsets, we can find open sets $U' \supseteq U$ and $V' \supseteq V$, such that $U' \cap V' = \emptyset$. This gives us $(U' \cup V')^c \cap B = \emptyset$. Now $(U' \cup V')^c$ is closed hence compact and $\{V_t^c \big| t \in T\}$ forms an open cover of $(U' \cup V')^c$. Thus there exists a finite subset $T' \subseteq T$ such that $\bigcup\limits_{t\in T'} V_t^c$ covers $(U' \cup V')^c$, so that $(U' \cup V')^c \cap [\bigcap\limits_{t\in T'} V_t] = \emptyset$. Let $A = \bigcap\limits_{t\in T'} V_t$, this gives us $(U' \cup V')^c \cap A = \emptyset \implies A \subseteq (U' \cup V')$. Since A is a finite intersection of clopen sets, it is also clopen. Now $x \in (A \cap U') \cup (A \cap V') = A \cap (U' \cup V') = A$. Now $A \cap U'$ is open but is also closed since $A \cap U' = V'^c \cap A$ and both sets of RHS are closed. Thus $B = U \cup V \subseteq A \cap U' \subseteq U'$. This gives us $B \cap V \subseteq B \cap V' = \emptyset$ and thus $V = \emptyset$. □

Proposition 6.0.4. *Let X be a compact, Hausdorff and totally disconnected topological space, then for any $x \in X$, the set of all clopen sets containing x forms a neighbourhood basis of x.*

Proof. Let X be as above, from lemma 6.0.3 if $\{V_t \big| t \in T\}$ is the family of clopen neighbourhoods of x, then $C_x = \bigcap\limits_{t\in T} V_t$. But X is totally disconnected thus $C_x = \{x\}$, thus

$\bigcap\limits_{t\in T} V_t = \{x\}$. Now let W be a proper open neighbourhood of of x, we must show that W contains a clopen neighbourhood of x. Since W^c is closed and $\bigcap\limits_{t\in T} V_t = \{x\}$, the collection $\{V_t^c \big| t \in T\}$ forms a open cover of W^c, and since W^c compact there exists a finite $T' \subseteq T$, such that $\bigcup\limits_{t\in T'} V_t^c \supseteq W^c$. This gives us that $V = \bigcap\limits_{t\in T'} V_t \subseteq W$ which is the required clopen neighbourhood of x. □

Theorem 6.0.5. *The following statements are equivalent for a topological group G.*

1. *G is a profinite group.*
2. *G is a compact, Hausdorff and totally disconnected topological group.*

Proof. 1. $\implies$ 2. follows from proposition 6.0.2. Now to show that 2. $\implies$ 1.

Let G be a compact, Hausdorff and totally disconnected topological group. We claim that $1 \in G$ admits a base $\{N\}_{N\in\mathcal{N}}$ of neighbourhood system where $\mathcal{N}$ is the set of all open normal subgroups of G. By proposition 6.0.4, $1 \in G$ admits a base of clopen neighbourhoods. Therefore it is sufficient to show that any clopen neighbourhood V containing 1 contains a $N \in \mathcal{N}$.

We denote by X^n the set of all products $x_1 \dots x_n$, $x_i \in X$ and by X^{-1} the set of all elements x^{-1} such that $x \in X$. Let $F = (G - V) \cap V^2$. Since V is compact, so is V^2 as its the continuous image of $V \times V$ under the multiplication map. Let x be such that $x \in V$ and $x \notin F$, thus $x \in F^c$. By continuity of multiplication map in G, $\exists V_x, S_x$ open in G, such that $x \in V_x$ and $1 \in S_x$ and $V_x S_x \subseteq V$ and $V_x S_x \subseteq F^c$. Since V is compact, there are finitely many $x_1, \dots, x_n$ such that $V_{x_1}, \dots, V_{x_n}$ covers V. Now let $S = \cup_{i=1}^n S_i$ and take $W = S \cap S^{-1}$. W is a symmetric neighbourhood of 1. $W \subseteq V$ and $VW \subseteq \cup_{i=1}^n V_{x_i} S_{x_i} \subseteq F^c$, thus $VW \cap F = \emptyset$. Since $W \subseteq V$, we have $VW \subseteq V^2$, and since $VW \cap F = \emptyset$ we have $VW \subseteq V$. This gives us $VW^2 \subseteq VW \subseteq V$ and iteratively $VW^n \subseteq V$. Since W is symmetric $H = \bigcup\limits_{n\in\mathbb{N}} W^n$ forms an open subgroup of G and $H \subseteq V$. As H is open in G, it has a finite index in G thus has a finite number of conjugates. Now take $N = \cap g^{-1} H g$ intersection over all the finitely many conjugates of H, $N \subseteq H \subseteq V$ is the required open normal subgroup.

Now $\{G/N\}_{N\in\mathcal{N}}$ forms a inverse system of finite groups with the maps $\phi_{NN'} : G/N \to G/N'$ the natural surjections whenever $N \subseteq N'$. Thus we have a profinite group $\varprojlim (G/N)_{N\in\mathcal{N}}$. The continuous natural projections $\pi_N ; G \to G/N$ induces a continuous homomorphism $\psi : G \to \varprojlim (G/N)$, due to the universal property of inverse limits. This map is injective because if $x \in G$ and $\psi(x) = 1$ then $x \in N$ for all $N \in \mathcal{N}$, thus $x \in \cap_{N \in \mathcal{N}} N = \{1\}$. Thus $x = 1$, which shows that ψ is an injection.

Now let $(g_i N_i)_{N_i \in \mathcal{N}} \in \varprojlim(G/N)$. Let $g_1 N_1, \ldots, g_k N_k$ be an finite sub collection of $\{g_i N_i\}_{N_i \in \mathcal{N}}$. Since $\{G/N\}_{N \in \mathcal{N}}$ forms a inverse system, there exists j such that $g_j N_j \subseteq g_i N_i$ for all $1 \leq i \leq k$. Thus $g_j N_j \subseteq \bigcap_{i=1}^{k} g_i N_i$. Thus the collection $\{g_i N_i\}_{N_i \in \mathcal{N}}$ has the finite intersection property. Since G is compact, by finite intersection property $\bigcap_i g_i N_i \neq \emptyset$. Thus any $g \in \bigcap_i g_i N_i$ maps to $(g_i N_i)_{N_i \in \mathcal{N}}$ via ψ, thus ψ is a surjection.

□

Example 11. *The group $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$, $GL_n(\mathbb{Z}_p)$, $SL_n(\mathbb{Z}_P)$ are examples of profinite groups.*

6.1 Index

Definition 6.1.1. *A supernatural number is a formal product $n = \prod_p p^{n(p)}$, where p runs over all prime numbers and $n(p)$ is either a non-negative integer or ∞.*

We can do some operations and comparisons with supernatural numbers analogous to natural numbers.

If $n = \prod_p p^{n(p)}$ and $m = \prod_p p^{m(p)}$ are two supernatural numbers and if $m(p) \leq n(p) \quad \forall p$, then we say m divides n, and denote it by $m|n$.

If $\{n_i = \prod_p p^{n_i(p)} | i \in I$ are a family of supernatural numbers, we can define product, lcm and gcd in an analogous way to natural numbers.

- $\prod_{i \in I} n_i = \prod_p p^{n(p)}$ where $n(p) = \sum_{i \in I} n_i(p)$.
- $\gcd\{n_i\}_i = \prod_p p^{n(p)}$ where $n(p) = min\{n_i(p)\}$.
- $\text{lcm}\{n_i\}_i = \prod_p p^{n(p)}$ where $n(p) = max\{n_i(p)\}$.

Now we can define a notion of index of a subgroup of a profinite group using supernatural numbers.

Definition 6.1.2. *Let G be a profinite group, and H be a closed subgroup of G. Let $\mathcal{U}$ be the set of all open normal subgroups of G. We define the index $[G : H]$ of H in G to be the supernatural number*

$$[G : H] = lcm\{[G/U : HU/U]\big|U \in \mathcal{U}\}$$

Which is equivalent to $lcm\{[G/U : H/H \cap U]\big|U \in \mathcal{U}\}$

With this, we can define a notion of order of profinite groups.

Definition 6.1.3. *The order of a profinite group G, denoted by $\#G$ is defined to be $[G : 1]$, that is, $\#G = lcm\{[G : U]\big|U \in \mathcal{U}\}$.*

Proposition 6.1.4. *If H and K are closed subgroups of a profinite group G, such that $H \subseteq H \subseteq G$, then $[G : K] = [G : H][H : K]$.*

Proof. We have $[G : K] = lcm\{[G/U : KU/U]|U \in \mathcal{U}\} = lcm\{[G/U : HU/U][HU/U : KU/U]|U \in \mathcal{U}\}$, thus is equivalent to $lcm\{[G/U : H/H \cap U][H/H \cap U : K/K \cap U]|U \in \mathcal{U}\}$. Now $[H : K] = lcm\{[H/H\cap U : K/K\cap H\cap U]|U \in \mathcal{U}\} = lcm\{[H/H\cap U : K/K\cap U]|U \in \mathcal{U}\}$. Hence it suffices to show that

$$lcm\{[G/U : H/H \cap U][H/H \cap U : K/K \cap U]|U \in \mathcal{U}\} =$$
$$lcm\{[G/U : H/H \cap U]|U \in \mathcal{U}\}lcm\{[H/H \cap U : K/K \cap U]|U \in \mathcal{U}\}$$

Let p^n, p^{n_1}, p^{n_2} where $n, n_1, n_2 \in \mathbb{N} \cup \infty$ be the highest prime powers such that $p^n \big| lcm\{[G/U : H/H\cap U][H/H\cap U : K/K\cap U]|U \in \mathcal{U}\}$, $p^{n_1} \big| lcm\{[G/U : H/H\cap U]|U \in \mathcal{U}\}$ and $p^{n_2} \big| lcm\{[H/H\cap U : K/K \cap U]|U \in \mathcal{U}\}$. This gives us that $n \geq n_1, n \geq n_2$ and $n \leq n_1 + n_2$. If $n = \infty$ then $n = n_1 + n_2$ and thus we are done. So, suppose $n < \infty$. this gives us $n_1, n_2 < \infty$. There exist $U_1, U_2 \in \mathcal{U}$ such that $p^{n_1} \big| [G/U : H/H \cap U_1]$ and $p^{n_2} \big| [H/H \cap U_2 : K/K \cap U_2]$. Take $U' = U_1 \cap U_2$, thus $U' \in \mathcal{U}$, which give us that $p^{n_1+n_2} \big| [G/U : H/H\cap U'][H/H\cap U' : K/K\cap U']$, which implies that $n \geq n_1 + n_2$. Thus $n = n_1 + n_2$ and we are done. □

Proposition 6.1.5. *Let $\{X_i, \phi_{ij}\}$ be an inverse system of compact, Hausdorff, non-empty topological spaces over the directed poset I, then $\varprojlim_{i \in I} X_i$ is non empty.*

Proof. For each $j \in I$, let $Y_j = \{(x_i)_i \in \prod_i X_i | \phi_{jk}(x_j) = x_k, \text{for all } k \leq j\}$. Each Y_j is non empty. Now consider $\prod X_i - Y_j$, if $(x_i)_i \in \prod X_i - Y_j$ then there exists x_k such that $x_k \neq \phi_{jk}(x_j)$ for some $k \in I$. Since each X_i are compact and Hausdorff $\prod X_i$ is compact and Hausdorff. And since $x_k \neq \phi_{jk}(x_j)$ are distinct points, there exists neighbourhoods U and V of $\phi_{jk}(x_j)$ and x_k respectively such that $U \cap V = \emptyset$. As ϕ_{jk} is continuous there exists a neighbourhood U' of x_j in X_j such that $\phi_{jk}(U') \subseteq U$. Now consider $W = \prod W_i$ where $W_i = U'$ for $i = j$, $W_i = V$ for $i = k$ and $W_i = X_i$ otherwise. This makes W a open neighbourhood of $(x_i)_i$. Now if $(y_i)_i \in W$ then $\phi_{jk}(y_j) \neq y_k$, since $\phi_{jk}(y_j) \in U$ and $y_k \in V$, but $U \cap V = \emptyset$. Thus $(y_i)_i \in \prod X_i - Y_j$, which give us that $W \subseteq \prod X_i - Y_j$ so that $\prod X_i - Y_j$ is open, hence Y_j is closed. Since I is a poset, we observe that if $j \leq j'$ then $Y_j' \subseteq Y_j$. This observation along with the fact that I is a directed poset gives that the collection $\{Y_i\}_{i \in I}$ has the finite intersection property. Now since $\prod X_i$ is compact, $\bigcap\limits_{i \in I} Y_i \neq \emptyset$, but $\varprojlim X_i = \bigcap\limits_{i \in I} Y_i$ and thus we are done. □

Corollary 6.1.6. *The inverse limit of a inverse system of non empty finite sets is non empty.*

Each finite set in an inverse system of non empty finite sets can be given the discrete topology which makes it compact and Hausdorff, thus the result follows from proposition 6.1.5.

Definition 6.1.7. *A pro-p group is a profinite group such that every open normal subgroup of it has a p power index.*

Pro-p groups are in a way the counterpart of finite p-groups in the context of profinite groups. The following proposition captures this essence.

Proposition 6.1.8. *A group G is pro-p if and only if it is the inverse limit of a family of finite p-groups.*

A proof of the above proposition can be found in [5]. We say that H is a p-sylow subgroup of G, if H is pro-p and it's index $[G : H]$ is co prime to p. This leads us to the following theorem, which is analogous to the Sylow theorem of finite groups.

Theorem 6.1.9 (Sylow theorem of profinite groups)**.** *Let G be a profinite group and p a fixed prime number such that G has a open normal subgroup of p power index, then*

1. *G contains a p-sylow subgroup.*

2. *Any pro-p subgroup of G is contained in a p-sylow subgroup of G.*

3. *Any two p-sylow subgroups of G are conjugates.*

Proof. Without loss of generality we can assume G to be the inverse limit of the inverse system $\{G_i, \phi_{ij}\}_{i \in I}$, where I is a directed poset. Now let $\mathcal{K}_i$ be the set of all p-sylow subgroups of G_i. Then $\mathcal{K}_i$ is non empty. And since ϕ_{ij} are surjective, if $K_i \in \mathcal{K}$ is a p-sylow subgroup of G_i then $\phi_{ij(K_i)}$ is a p-sylow subgroup of G_j, thus $\phi_{ij}(\mathcal{K}_i) \subseteq \mathcal{K}_j$. Thus $\{\mathcal{K}_i, \phi_{ij}\}_{i \in I}$ forms an inverse system of non empty finite sets, hence from corollary 6.1.6, $\varprojlim \mathcal{K}_i$ exists and is non empty. Now if $(K_i)_i \in \varprojlim \mathcal{K}_i$, then for each $i \in I$, K_i is a p-sylow subgroup of G_i, and $\{K_i, \phi_{ij}\}_{i \in I}$ forms a inverse system of discrete finite groups. Thus $K = \varprojlim K_i$ is the required sylow-p subgroup of G. The proof of 2. and 3. are similar to above, in forming some inverse system of non empty finite groups and using it to get the desired object.

□

6.2 Cohomology of profinite groups

Cohomology of profinite groups G arise form it's action on special G-modules, which also considers the profinite group G's topological structure. A discrete G-module A is an abelian group with the discrete topology, on which G acts continuously. Consider the following diagram.

$$\cdots \to G^3 \to G^2 \to G$$

There are $n+1$ projective maps from G^{n+1} to G^n given by $d_i : G^{n+1} \to G^n$, $d_i : (g_0, \dots, g_n) \mapsto (g_0, \dots, \hat{g}_i, \dots, g_n)$, $0 \leq i \leq n$, where $\hat{g}_i$ indicates that g_i has been removed from the n+1 tuple. Now the set $X^n(G, A)$ of all continuous maps $x : G^{n+1} \to A$ together with the operation of point wise addition of the maps forms an abelian group. This has a G-module structure given by $(gx)(g_0, \dots, g_n) = gx(g^{-1}g_0, \dots, g^{-1}g_n)$. The maps d_i for each $0 \leq i \leq n$, induces the G-maps, $d_i^* : X^{n-1}(G, A) \to X^n(G, A)$, where $d*_i : x \mapsto xd_i$, from which we get a map, called the nth coboundary map $\partial^n : X^{n-1}(G, A) \to X^n(G, A)$ given by

$$(\partial^n x)(g_o, \dots, g_n) = \sum_{i=o}^{n} (-1)^i d_i^*(x(g_o, \dots, g_n)) = \sum_{i=o}^{n} (-1)^i x(g_0, \dots, \hat{g}_i, \dots, g_n)$$

. This gives us a sequence of G-modules,

$$0 \to A \xrightarrow{\partial^0} X^0(G, A) \xrightarrow{\partial^1} X^1(G, A) \xrightarrow{\partial^2} X^2(G, A) \to \cdots$$

where $\partial^0 A \to X^0(G, A)$ is the map which takes $a \in A$ to thee constant map $x_a(g) = a$ of $X^0(G, A)$

Proposition 6.2.1. *The above sequence of G-modules is an exact sequence.*

Proof. We have to show that the $\ker\partial^{n+1} = \mathrm{im}\partial^n$, for all $n \geq 0$. Consider the composition $\partial^{n+1}\partial^n x(g_o, \dots g_n)$ for a $x \in X^{n-1}(G, A)$. Then $\partial^{n+1}\partial^n x(g_o, \dots g_n) =$

$$\sum_{i=o}^{n+1} (-1)^i \sum_{j=o}^{i-1} (-1)^j x(g_0, \dots, \hat{g}_j, \dots, \hat{g}_i, \dots, g_n) + \sum_{i=o}^{n+1} (-1)^i \sum_{j=i+1}^{n+1} (-1)^j x(g_0, \dots, \hat{g}_i, \dots, \hat{g}_j, \dots, g_n)$$

$$= \sum_{i=o}^{n+1} \sum_{j=o}^{i-1} (-1)^{i+j} x(g_0, \dots, \hat{g}_j, \dots, \hat{g}_i, \dots, g_n) - \sum_{i=o}^{n+1} \sum_{j=i+1}^{n+1} (-1)^{i+j} x(g_0, \dots, \hat{g}_i, \dots, \hat{g}_j, \dots, g_n)$$

$$= \sum_{i=o}^{n+1} \sum_{j=o}^{i-1} (-1)^{i+j} x(g_0, \dots, \hat{g}_j, \dots, \hat{g}_i, \dots, g_n) - \sum_{j=o}^{n+1} \sum_{i=0}^{j-1} (-1)^{i+j} x(g_0, \dots, \hat{g}_i, \dots, \hat{g}_j, \dots, g_n)$$

$$= 0$$

Also $\partial^1\partial^0 a(g_0, g_1) = \partial^1 x_a(g_0, g_1) = x_a(g_0) - x_a(g_1) = a - a = 0$. Thus $\partial^{n+1}\partial^n x = 0$ for all $n \geq 0$. Which gives us that the sequence is a complex, so $im\partial^n \subseteq ker\partial^{n+1}$. Now we define the maps $D^n : X^{n+1}(G, A) \to X^n(G, A)$ given by $(D^n x)(g_0, \dots, g_n) = x(1, g_0, \dots, g_n)$ for all $n \geq 0$ and $D^{-1} : X^0 G, A \to A$ by $D^{-1}x = x(1)$. We get the relation $D^n\partial^{n+1} + \partial^n D^{n-1} = id$ which can be verified directly using the definitions of the respective maps. From this relation, we observe that if $x \in ker\partial^{n+1}$ then $\partial^n D^{n-1}x = x$, which implies that $x \in im\partial^n$. This gives us the opposite inclusion $ker\partial^{n+1} \subseteq im\partial^n$ for all $n \geq 0$, thus the sequence is exact. □

Now we define $C^n(G, A) = X^n(G, A)^G$, that is $x \in X^n(G, A)$, such that $(gx)(g_0, \dots, g_n) = gx(g^{-1}g_0, \dots, g^{-1}g_n) = x(g_0, \dots, g_n)$. These are precisely the maps $x \in X^n(G, A)$ such that

$x(gg_0, \ldots, gg_n) = gx(g_0, \ldots, g_n)$. This makes $C^n(G, A)$ the group of all G-maps from G^{n+1} to A. Thus we get the following cochain complex, called the homogeneous cochain complex of G with coefficients in A.

$$0 \to C^0(G, A) \xrightarrow{\partial^1} C^1(G, A) \xrightarrow{\partial^2} C^2(G, A) \to \cdots$$

Using this, we can define the cohomology groups of G with coefficients in A.

Definition 6.2.2. *We define $Z^n(G, A) = ker\partial^{n+1}$ to be the homogeneous n-cocycles and $B^n(G, A) = im\partial^n$ to be the homogeneous n-coboundaries of the above cochain complex, and for $n \geq 0$ we define $H^n(G, A) = Z^n(G, A)/B^n(G, A)$ to be the nth cohomology group of G with coefficients in A.*

Although this definition is relatively simpler, the way $C^n(G, A)$ is defined restricts the elements in it to continuous maps which are also G-maps. Thus redefining cohomology groups in the following way eases the restriction and makes calculations simpler to work with.

We define $\mathbb{C}^n(G, A)$ to be the abelian group of all continuous maps of the form $y : G^n \to A$ and $\mathbb{C}^0(G, A)$ to be A.

Proposition 6.2.3. *The abelian groups $C^n(G, A)$ and $\mathbb{C}^n(G, A)$ are isomorphic for all $n \geq 0$.*

The maps $\phi : C^n(G, A) \to \mathbb{C}^n(G, A)$, given by $x(g_0, \ldots, g_n) \mapsto y(g_1, \ldots, g_n)$, where $y(g_1, \ldots, g_n) = x(1, g_1, g_1g_2, \ldots, g_1 \cdots g_n)$ and $\psi : \mathbb{C}^n(G, A) \to C^n(G, A)$, given by $y(g_1, \ldots, g_n) \mapsto x(g_0, \ldots, g_n)$, where $x(g_0, \ldots, g_n) = g_0y(g_0^{-1}g_1, g_1^{-1}g_2, \ldots, g_{n-1}^{-1}g_n)$ are group homomorphisms and inverses of each other, which gives us the isomorphism.
With this we can define $\partial'^n : \mathbb{C}^n - 1(G, A) \to \mathbb{C}'^n(G, A)$ to be $\phi\partial^n\psi$. Thus for any $y \in \mathbb{C}^{n-1}(G, A)$

$$\begin{aligned}\partial'^n y(g_1, \ldots, g_n) = \phi\partial^n\psi y(g_1, \ldots, g_n) =& g_1y(g_2, \ldots, g_n)\\ &+ \sum_{i=1}^{n-1}(-1)^i y(g_1, \ldots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \ldots, g_n)\\ &+ (-1)^n y(g_1, \ldots, g_{n-1})\end{aligned}$$

This give us the following cochain complex, called the inhomogeneous cochain complex of G with coefficients in A.

$$0 \to \mathbb{C}^0(G, A) \xrightarrow{\partial'^1} \mathbb{C}^1(G, A) \xrightarrow{\partial'^2} \mathbb{C}^2(G, A) \to \cdots$$

Since the coboundary maps and the isomorphism between the terms of the two cochain complexes commute by definition, the two complexes are isomorphic and so are their respective cohomology groups.

Chapter 7

Golod Shafarevich inequality

In this chapter we will see how invariants of a group which arises from it's presentation such as generator rank of group can be interpreted in terms of it's cohomology groups. We'll also see the inequality relation between the relation rank and generator rank of finite pro p-group G, proved by E.S.Golod and I.R.Shafarvich. This chapter is primarily based on results from [8] and [9]

7.1 Presentation of a pro-p group

In this section assume G to be a pro-p group, unless specified otherwise.

Definition 7.1.1. *Let N be a normal subgroup of G. A system of generators of N as a normal subgroup of G, is a convergent subset $S \subseteq N$ such that, N is the smallest normal subgroup of G containing S.*

A convergent subset of N is a subset S such that, every open subgroup of N contains all but finitely many elements of S. If we consider the above definition taking $N = G$ to be a normal subgroup of itself, then S is the system of generators of G. We say a system of generator S of G is minimal, if no proper subset of S is a system of generators of G.

To give a presentation of a pro-p group, we need a free pro-p group analogous to the case of presentation of a finite group.

Definition 7.1.2. *Let F_S be the free group with S as its generators and p be a prime number. The pro-p completion F of F_S is called the free pro-p group with system of generators S, that is, $F = \varprojlim(F_S/N)_{N\in\mathcal{N}}$ where $\mathcal{N}$ is the set of all open normal subgroups of F_S with p power index.*

Thus we have the short exact sequence similar to the finite group case $1 \to R \to F \to G \to 1$, where G is a pro-p group with system of generator S, and F is the free pro-group with the system of generators S. Now if E is a system of generator of R, then E is called the system of relations of G. The cardinality of the minimal system of generators of G is called the generator rank of G , often denoted by $d(G)$ or d. Similarly the cardinality of the minimal system of relations is called the relation rank, denoted by $r(G)$ or r.

Proposition 7.1.3. *For a pro-p group G, the generator rank and relation rank of G are related to it's cohomology groups by $d(G) = dim_{\mathbb{F}_p}H^1(G,\mathbb{F}_p)$ and $r(G) = dim_{\mathbb{F}_p}H^2(G,\mathbb{F}_p)$*

7.2 Preliminary background required for proof

For the proof of the inequality we need additional structure on pro-p groups Let Λ be a compact commutative ring with unity. If G is a pro-p group with normal subgroups N, N' with $N \subseteq N'$, the the natural surjection $G/N \to G/N'$ can b extended to homomorphism $\Lambda[G/N] \to \Lambda[G/N']$ of group rings. Thus $\{\Lambda[G/N]\}_{N\in\mathcal{N}}$, where $\mathcal{N}$ is the set of all open normal subgroups of G, along with the homomorphisms as above forms an inverse system.

Definition 7.2.1. *The completed group $\Lambda[[G]]$ is defined to be the inverse limit $\varprojlim(\Lambda[G/N])_{N\in\mathcal{N}}$.*

We use a few results on completed group rings from [8], the proof of which can be found in the same.

Proposition 7.2.2. *If $\phi : G \to G'$ is a morphism of profinite groups, with $ker\phi = N$, then we have a induced morphism $\phi' : \Lambda[[G]] \to \Lambda[[G']]$ where $ker\phi' = I(N)$ is the closed ideal generated by all $n - 1$ such that $n \in N$.*

Definition 7.2.3. *Let Λ be a ring with identity. Then the Magnus algebra $\Lambda(x_1, \ldots, x_m)$ in variables $x_1, \ldots, x_m$ is the algebra of formal non-commutative associate power series in the variables $x_1, \ldots, x_m$ with coefficients from Λ.*

Proposition 7.2.4. *If F is a free pro-p group with the system of generators $\{s_1, \doteq, s_m\}$, then $\Lambda[[F]]$ is isomorphic to the ring $\Lambda(x_1, \ldots, x_m)$ by linearly extending the homomorphism $s_i \mapsto 1 + x_i$*

Definition 7.2.5. *Let F be a d-generated free pro-p group. For $\tau_1, \ldots, \tau_d \in \mathbb{Z}^+$, the Lazard valuation of type $(\tau_1, \ldots, \tau_d)$ on $\mathbb{F}_p(x_1, \ldots, x_d)$, is an additive function $\nu : \mathbb{F}_p(x_1, \ldots, x_d) \to \mathbb{Z} \cup \infty$ which has $x_i \mapsto \tau_i$ and the valuation on a monomial $x_{i_1} \ldots x_{i_k}$ is given by $\nu(x_{i_1} \ldots x_{i_k}) = \tau_{i_1} + \cdots + \tau_{i_k}$. Also $\nu(1) = 0$ and $\nu(0) = \infty$. The valuation on an element $\sum_k \lambda_k M_k$ where M_k are monomials is defined as $\nu(\sum_k \lambda_k M_k) = min\{\nu(M_k) | \lambda_k \neq 0\}$. This forms a valuation on $F_p(x_1, \ldots, x_d)$ as defined in the usual sense. That is for all $a, b \in F_p(x_1, \ldots, x_d)$*

$$\nu(ab) = \nu(a) + \nu(b) \qquad \textit{and} \qquad \nu(a + b) \geq min(\nu(a), \nu(b))$$

If $1 \to R \to F \xrightarrow{\psi} G \to 1$ is a minimal presentation of a pro-finite group G, then a valuation ν on $\mathbb{F}_p[[F]]$ identified with $\mathbb{F}_p(x_1, \ldots, x_d)$ induces a valuation on $\mathbb{F}_p[[G]]$ given by $\nu(b) = max\{\nu(a) \big| \psi(a) = b\}$ for $b \in \mathbb{F}_p[[G]]$ and where $a \in \mathbb{F}_p[[F]]$.

7.3 Proof of Golod Shafarevich inequality

Let $1 \to R \to F \xrightarrow{\psi} G \to 1$ be the minimal presentation of a finitely generated pro-p group. The map $\psi : F \to G$ induces the map $\psi : \mathbb{F}_p[[F]] \to \mathbb{F}_p[[G]]$ which we also denote by ψ for the sake of notational convenience. Let $d(G) = d$ and $r(G) = r$, let $\{s_1, \ldots, s_d\}$ be the lifts in F of the minimal system of generators of G and $\{\rho_1, \ldots \rho_r\}$ be the minimal system of relations for G.

Then using the results from the previous section, the kernel of $\psi : \mathbb{F}_p[[F]] \to \mathbb{F}_p[[G]]$ denoted by $I(R)$ is generated ρ_i, $1 \leq i \leq r$. For the sake of notational convenience let $A = F_p[[F]]$ and $B = \mathbb{F}_p[[G]]$. Again from using the results from previous section A can be identified with $\mathbb{F}_p(x_1, \ldots, x_d)$ by the isomorphism $s_i \mapsto x_i + 1$ and B with $A/I(R)$.Let $y_i = \psi(x_i)$.

Let ν be a Lazard valuation of type $(\tau_1, \ldots, \tau_d)$ on A. We can assume without loss of generality that $t_i \leq \tau_{i+1}$, and that system of relations are indexed in such a way that their levels are monotonically increasing. The valuation ν induces a valuation ν on B which gives us the filtration $I_n = \{b \in B \big| \nu(b) \leq n\}$, for $n \in \mathbb{Z}$ and we define $I_n = B$ for $n \leq 0$. Thus we can count generators and relations by level with d_n defined to be the cardinality of $\{x_i \big| \nu(x_i) = n\}$

and r_n define to be the cardinality of $\{\rho_i \big| \nu(\rho_i) = n\}$, which gives us $d = \sum d_n$ and $r = \sum r_n$.

Consider the following sequence $B^r \xrightarrow{\psi_1} B^d \xrightarrow{\psi_0} B \xrightarrow{\epsilon} \mathbb{F}_p \to 0$. The map ϵ is the augmentation map, or with the identification of B with $A/I(R)$ the map of evaluation at $(0, \ldots, 0)$. The map ψ_0 is given by $\psi_0(b_1, \ldots, b_d) = \sum\limits_{i=1}^{d} b_i y_i$.
We observe that $\rho_i - 1$ is inside the augmentation ideal of A and thus has zero constant term. Thus every $\rho_i - 1$ can be written as $\rho_i - 1 = \sum\limits_{j=1}^{d} z_{ij} x_j$, by grouping the monomials of the power series representing ρ_i based on their last free variable. With this the map ψ_1 is given by $\psi_1(b_1, \ldots, b_r) = \left(\sum\limits_{i=1}^{r} b_i \psi(z_{i1}), \ldots, \sum\limits_{i=1}^{r} b_i \psi(z_{id}) \right)$.

Proposition 7.3.1. *The sequence $B^r \xrightarrow{\psi_1} B^d \xrightarrow{\psi_0} B \xrightarrow{\epsilon} \mathbb{F}_p \to 0$ is exact.*

Proof. The augmentation map ϵ is surjective, thus the sequence is exact at $\mathbb{F}_p$. Th kernel of the augmentation map, when ϵ is interpreted as the evaluation at $(0, \ldots, 0)$ is the all power series $b \in B$ with zero constant term, which are generated by $y_i = \psi(x_i)$, and since $\psi_0(b_1, \ldots, b_d) = \sum\limits_{i=1}^{d} b_i y_i$, $im(\psi_0)$ is all the linear B combinations of y_i, we have $im\psi_0 = ker\epsilon$. This gives us that the sequence is exact at B. Now for the exactness at B^d, let $(b_1, \ldots, b_r) \in B^r$, then $\psi_0(\psi_1(b1, \ldots, b_r)) =$

$$\begin{aligned} &\sum_{j=1}^{d} \sum_{i=1}^{r} b_i \psi(z_{ij}) y_j = \sum_{j=1}^{d} \sum_{i=1}^{r} b_i \psi(z_{ij} x_j) \\ &= \sum_{i=1}^{r} b_i \sum_{j=1}^{d} \psi(z_{ij} x_j) = \sum_{i=1}^{r} b_i \psi(\rho_i - 1) \\ &= 0 \end{aligned}$$

This gives us that $im\psi_1 \subseteq ker\psi_0$. For the reverse inclusion, let $(b_1, \ldots, b_d) \in B^d$ such that $(b_1, \ldots, b_d) \in ker\psi_0$, then $\sum\limits_{j=1}^{d} b_j y_j = 0$. Take a_j to be the lifts of b_j in A, so that $0 = \sum\limits_{j=1}^{d} b_j y_j = \sum\limits_{j=1}^{d} \psi_0(a_j x_j)$, which gives us that $\sum\limits_{j=1}^{d} a_j x_j \in ker\psi$. But we know that $ker\psi$ is generated by $\rho_1 - 1, \ldots, \rho_r - 1$, thus we have $\sum\limits_{i=1}^{d} a_j x_j = \sum\limits_{i=1}^{r} a'_i \sum\limits_{j=1}^{d} z_{ij} x_j = \sum\limits_{j=1}^{d} \sum\limits_{i=1}^{r} a'_i z_{ij} x_j$.

Comparing coefficient of x_j we get $a_j = \sum\limits_{i=1}^{r} a_i' z_{ij}$. Therefore

$$\begin{aligned}\psi_1\big(\psi(a_1'), \dots, \psi(a_r')\big) &= \Big(\sum_{i=1}^{r} \psi(a_i' z_{i1}), \dots, \sum_{i=1}^{r} \psi(a_i' z_{id})\Big) = (\psi(a_1), \dots, \psi(a_d)) \\ &= (b_1, \dots, b_d)\end{aligned}$$

which give us that $(b_1, \dots, b_d) \in im\psi_1$, which implies $ker\psi_0 \subseteq im\psi_1$. Thus the sequence is exact at B^d. □

Now fix an integer n. The restriction of the sequence in proposition 7.3.1 gives us the sequence $\bigoplus\limits_{i=1}^{r} I_{n-\nu(\rho_i-1)} \xrightarrow{\psi_1} \bigoplus\limits_{i=1}^{d} I_{n-\nu(x_i)} \xrightarrow{\psi_0} I_n \to 0$. This restriction is a complex. Now we verify that the maps ψ_0 and ψ_1 land properly with the restrictions. Let $(b_1, \dots, b_d) \in \bigoplus\limits_{i=1}^{d} I_{n-\nu(x_i)}$. Then we have $\nu(b_i) \geq n - \nu(x_i)$ from the definition of the filtration I_n. $\psi_0(b_1, \dots, b_d) = \sum\limits_{i=1}^{d} b_i y_i$ thus $\nu(\psi_0(b_1, \dots, b_d)) = \nu(\sum\limits_{i=1}^{d} b_i y_i) \geq min\{\nu(b_i) + \nu(y_i)\}$. But $\nu(y_i) = \nu(\psi(x_i)) \geq \nu(x_i)$, which gives us $\nu(\psi_0(b_1, \dots, b_d)) \geq min\{\nu(b_i) + \nu(y_i)\} \geq n - \nu(x_i) + \nu(x_i) = n$. Thus $(b_1, \dots, b_d) \in I_n$. Similarly ψ_1 takes elements of $\bigoplus\limits_{i=1}^{r} I_{n-\nu(\rho_i-1)}$ to $\bigoplus\limits_{i=1}^{d} I_{n-\nu(x_i)}$.

Proposition 7.3.2. *The restriction of the map $\psi_0 : \bigoplus\limits_{i=1}^{d} I_{n-\nu(x_i)} \to I_n$ is surjective.*

Proof. Let $k \in I_n$. Let g be a lift of k in A such that $\nu(g) = \nu(k)$. Such a g exists as $\nu(h)$ is the maximum of $\nu(g)$ over all lift g of k in A. Now since $\nu(g) = \nu(k) \geq n$, we can write g uniquely as $\sum\limits_{i=1}^{d} g_i x_i$. We have $\nu(g_i x_i) \geq min\{\nu(g_i x_i)\} = \nu(g) \geq n$. Thus $\nu(g_i) + \nu(x_i) \geq n$ or $\nu(g_i) \geq n - \nu(x_i)$. Now take $k_i = \psi(g_i)$, which gives us $\nu(k_i) \geq n - \nu(x_i)$, so that and $(k_1, \dots, k_d) \in \bigoplus\limits_{i=1}^{d} I_{n-\nu(x_i)}$, and $\psi_0(k_1, \dots, k_d) = \sum\limits_{i=1}^{d} k_i y_i = \sum\limits_{i=1}^{d} \psi(g_i x_i) = \psi(g) = k$. □

Now consider the following commutative diagram.

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & & \\
\bigoplus_{i=1}^{r} I_{n-\nu(\rho_i-1)} \arrow[r, "\psi_1"] \arrow[d] & \bigoplus_{i=1}^{d} I_{n-\nu(x_i)} \arrow[r, "\psi_0"] \arrow[d] & I_n \arrow[r] \arrow[d] & 0 \arrow[d] & \\
B^r \arrow[r, "\psi_1"] \arrow[d] & B^d \arrow[r, "\psi_0"] \arrow[d] & B \arrow[r, "\epsilon"] \arrow[d] & \mathbb{F}_p \arrow[r] \arrow[d] & 0 \\
B^r/\bigoplus_{i=1}^{r} I_{n-\nu(\rho_i-1)} \arrow[r] \arrow[d] & B^d/\bigoplus_{i=1}^{d} I_{n-\nu(x_i)} \arrow[r] \arrow[d] & B/I_n \arrow[r] \arrow[d] & \mathbb{F}_p \arrow[r] \arrow[d] & 0 \\
0 & 0 & 0 & 0 &
\end{tikzcd}$$

The columns of this diagram are exact, the top row is a complex and the middle row is exact. The bottom row is also exact, which can be shown from the other exact sequences in the above commutative diagram by diagram chasing. If we define $c_n = dim_{\mathbb{F}_p} B/I_n$, then from the exactness of the bottom row, counting dimensions we get $\sum_{i=1}^{r} c_{n-\nu(\rho_i-1)} - \sum_{i=1}^{d} c_{n-\nu(x_i)} + c_n - 1 \geq 0$.

Consider the sum $\sum_{i=1}^{r} c_{n-\nu(\rho_i-1)}$. The value of $n-\nu(\rho_i-1)$ varies between 0 and $n-1$, as $n-\nu(\rho_i-1)$ cannot exceed $n-1$ and $c_{n-j}=0$ for $j \geq n$. The number of times c_{n-j} occurs in the sum is r_j times, thus $\sum_{i=1}^{r} c_{n-\nu(\rho_i-1)} = \sum_{j=1}^{n} r_j c_{n-j}$. Similarly $\sum_{i=1}^{d} c_{n-\nu(x_i)} = \sum_{j=1}^{n} d_j c_{n-j}$. Thus we get

$$\sum_{j=1}^{n} r_j c_{n-j} - \sum_{j=1}^{n} d_j c_{n-j} + c_n \geq 1$$

Since $d_0 = 0$ as $\nu(x_i) > 0$, and taking $r_0 = 1$ we get

$$\sum_{j=0}^{n} (r_j - d_j) c_{n-j} \geq 1$$

Proposition 7.3.3. *Let G be a finite pro-p group with r_i and d_i as above, then $\phi(t) = 1 + \sum_{n=1}^{\infty} (r_n - d_n) t^n$, converges for $0 < t < 1$ and $\phi(t) > 0$.*

Proof. We have $\sum\limits_{j=0}^{n}(r_j - d_j)c_{n-j} \geq 1$. Multiplying t^n on both sides and summing over all n we get

$$\sum_{n=0}^{\infty}\Big(\sum_{j=0}^{n}(r_j - d_j)c_{n-j}\Big)t^n \geq \sum_{n=0}^{\infty} t^n = 1/(1-t)$$

We observe that the LHS of the above inequality is of the form of Cauchy product of the two series $\sum\limits_{n=0}^{\infty}(r_n - d_n)t^n$ and $\sum\limits_{n=0}^{\infty} c_n t^n$. Therefore we have

$$\big(\sum_{n=0}^{\infty}(r_n - d_n)t^n\big)\big(\sum_{n=0}^{\infty} c_n t^n\big) \geq 1/(1-t)$$

Since G is finite, I_n will eventually become zero , thus $c_n = dim_{\mathbb{F}_p} B/I_n$ is bounded above, which gives us that $\sum\limits_{n=0}^{\infty} c_n t^n$ converges and is greater that 0. Since G is finite, d and r are finite, which makes all but finitely many d_n and r_n to be zero. Thus $\sum\limits_{n=0}^{\infty}(r_n - d_n)t^n$ is a polynomial and thus converges. Since $1/(1-t) > 0$ diving on both sides by $\sum\limits_{n=0}^{\infty} c_n t^n$ gives us that $\sum\limits_{n=0}^{\infty}(r_n - d_n)t^n > 0$. Now taking $n = 0$ term out of the summation we get $\phi(t) = 1 + \sum\limits_{n=1}^{\infty}(r_n - d_n)t^n > 0$. □

If the Lazard valuation is of type $(1, \ldots, 1)$, then the valuation of any generator $\nu(x_i) = 1$, Which gives us $d_1 = d$ and $d_i = 0$ otherwise. Also $r_1 = 0$, as any relation $\rho_i - 1$ with valuation $\nu(\rho_i - 1) = 1$ makes it a generator which, contradicts the minimality of the presentation of G. Thus $\phi(t) = 1 + \sum\limits_{n=1}^{\infty}(r_n - d_n)t^n$ becomes $\sum\limits_{n=2}^{\infty} r_n t^n - dt + 1 > 0$.

Proposition 7.3.4. *For a finite pro-p group G, with r, d and t as above $rt^2 - dt + 1 > 0$.*

Proof. Previously we have $\sum\limits_{n=2}^{\infty} r_n t^n - dt + 1 > 0$. Since $0 < r < 1$, we have $r^2 \geq r_n$ for all $n \geq 2$ and $\sum r_n = r$. Thus $rt^2 - dt + 1 \geq \sum\limits_{n=2}^{\infty} r_n t^n - dt + 1 > 0$. □

Theorem 7.3.5. *If G is a finite pro-p group, with generator rank $d(G) = d$ and relation rank $r(G) = r$, then $r > d^2/4$.*

Proof. Consider the following exact sequence $0 \to \mathbb{Z} \xrightarrow{p} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/p\mathbb{Z} \to 0$, where the map p is multiplication by p and π th natural surjection. We can extend this to a long exact sequence on cohomology group by theorem 4.0.8. But $H^1(G, \mathbb{Z}) = Hom(G, \mathbb{Z}) = 0$, as action of G on $\mathbb{Z}$ is trivial and G is finite. Thus the sequence gives us the following exact sequence

$$0 \to H^1(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z}) \to H^2(G, \mathbb{Z}) \to H^2(G, \mathbb{Z}/p\mathbb{Z})$$

Since we know that $dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/p\mathbb{Z}) = d$ and $dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z}) = r$, the above exact sequence gives us the inequality $-d + k - k + r \geq 0$ by counting dimensions , where k is the $\mathbb{F}_p$ dimension of $H^2(G, \mathbb{Z})$, which gives us that $d \leq r < 2r$ or $0 < d/2r < 1$. Substituting $t = d/2r$ in proposition 7.3.4, we get $r(d/2r)^2 - d(d/2r) + 1 > 0$, thus $-d^2/4r > -1$ or $d^2/4 < r$. □

Chapter 8

Conclusion

The primary aim of this project was to explore and understand a few standard tools of Homological algebra and related results. We first started with basic topics from category theory to better understand and get a broader perspective of the rest of the project. We explored projective, injective and flat modules and saw how the category of R-modules had enough projective and injective objects which allowed us to show that every R-module has a projective and injective resolution. We then explored cochain complexes and it cohomology groups in abstract and applying it to the case of projective resolution of a R-module and applying the contravariant hom functor which gave us the Ext groups. With the help of Ext groups, group cohomology were able to be realized as the Ext groups of $\mathbb{Z}G$-module projective resolutions of $\mathbb{Z}$.

We shifted our focus to Topological groups which helped us in understanding profinite and pro-p groups, whose cohomology was then explored. We were then able to interpret the relation rank and generator rank of a pro-p group in terms of their cohomology groups, which aided us in proving the Golod-Shfarevich inequality. There are many proofs in literature on Golod-Shfarevich inequality like the one by J.P. Serre's [3] and by Helmut Koch [8]. The one in this thesis is primarily based on Koch's proof with aid from [9].

Bibliography

[1] Joseph J. Rotman, *An Introduction to Homological Algebra*, Second edition, Springer, 2009.

[2] David S. Dummit and Richard M. Foote, *Abstract Algebra*, Third edition, Wiley, 2011.

[3] Jean P. Serre, *Galois Cohomology*, Springer, 1997.

[4] K. Chandrasekharan, *A Course on Topological Groups*, Hindustan Book Agency,1996.

[5] J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p Groups*, Second edition, Cambridge University Press, 1999.

[6] Luis Ribes and Pavel Zalesskii, *Profinite Groups*, Second edition, Springer, 2010.

[7] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg, *Cohomology of Number Fields*, Second edition, Springer, 2008.

[8] Helmut Koch, *Galois Theory of p-extensions*, Springer, 2002.

[9] Cameron McLeman, *A Golod-Shafarevich Equality and p-Tower Groups*, PhD thesis, University of Arizona, 2008.