# Profinite Groups and Cohomology

Anthi Zervou

Supervisor

Jannis A. Antoniadis

Master Thesis

Department of Mathematics and Applied Mathematics
University of Crete

# Acknowledgements

This master thesis was presented at the Department of Mathematics and Applied Mathematics in 16 May 2017.

I would like to express my sincere gratitude to my supervisor Professor Jannis A. Antoniadis who helped me all the way to the completion of this master thesis and for the continuous support of my studies. Also, I would like to thank him for his patience, motivation, enthusiasm, and immense knowledge.
Besides my supervisor I would like to thank the rest of my committee members Professor Alexandros Kouvidakis and Assistant Professor Maria Loukaki.
Additionally, I would like to thank my colleagues Emmanouil Doulgerakis and Alexandros Galanakis for their patience to attend the lectures I gave in order to present in detail the content of my master thesis.

Master thesis examination committee:

- Prof. Jannis A. Antoniadis (Supervisor)
- Prof. Alexandros Kouvidakis, and
- Asst. Prof. Maria Loukaki

Anthi Zervou,
Heraklion, May 2017

To my mother,<br>
Arsinoi,<br>
who always supports my choices.

# Contents

**Introduction** **vii**

**1 Galois Theory for Infinite Extensions** **1**

1.1 Topological Prerequisites . . . . . . . . . . . . . . . . . . . . . . . . 1

1.2 Topological Groups . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

1.3 Finite Galois Theory and Krull Topology . . . . . . . . . . . . . . . 8

1.4 The Fundamental Theorem of Infinite Galois Theory . . . . . . . . 17

1.5 The use of Infinite Galois Theory . . . . . . . . . . . . . . . . . . . . 21

**2 Profinite groups** **23**

2.1 Category Theory . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 23

2.2 Projective and Direct Limit . . . . . . . . . . . . . . . . . . . . . . . 29

2.3 Profinite Groups . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 33

2.4 Limits and Functors . . . . . . . . . . . . . . . . . . . . . . . . . . . . 43

**3 Cohomology of Finite Groups** **55**

3.1 Differential Groups . . . . . . . . . . . . . . . . . . . . . . . . . . . . 55

3.2 G- modules . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 61

3.3 Definition of Cohomology Groups . . . . . . . . . . . . . . . . . . . . 70

3.4 Low Dimensional Cohomology Group . . . . . . . . . . . . . . . . . . 74

3.5 Cyclic Cohomology . . . . . . . . . . . . . . . . . . . . . . . . . . . . 80

3.6 Cohomology Theorems . . . . . . . . . . . . . . . . . . . . . . . . . . 91

**4 Cohomology of Profinite Groups** **95**

4.1 Discrete Modules . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 95

4.2 Construction of the Cohomology Groups . . . . . . . . . . . . . . . . 98

4.3 Compatible Pairs . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 100

4.4 Change of the group $G$ . . . . . . . . . . . . . . . . . . . . . . . . . 103

4.5 Special Mappings . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 111

**5 Some Applications of Cohomology** **115**

5.1 Group Extensions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 115

5.2 The Brauer Group . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 124

5.3 The Inverse Problem of Galois Theory . . . . . . . . . . . . . . . . . 126

**Bibliography** **131**

# Introduction

Galois theory is an elegant interaction between field theory and group theory. It gives a bijective correspondence between intermediate fields of a Galois extension and subgroups of the Galois group of this extension. For the case of finite Galois extensions, the fundamental theorem of Galois theory establishes the bijective correspondence between intermediate fields and subgroups. The fundamental theorem is useful in many situations because it allows us to find out informations about the intermediate fields of a Galois extension from the subgroups of the Galois group of the extension, and vice versa. For this reason we would like to extend this theorem to the case of infinite Galois extensions. In the first chapter we study the Galois theory for infinite extensions. Luckily, the definition of the Galois extension carries over without change from the finite case to the case of infinite algebraic extensions. Unfortunately, the main theorem doesn't hold for infinite Galois extensions. This was ascertained by R. Dedekind in 1897. But we can find out that there exists a fundamental theorem for infinite Galois extensions which is a generalization of the main theorem of the finite Galois theory. For its proof we are going to put a topology on the infinite Galois groups, the so called Krull topology, which we define. So the concept of "topological groups" will naturally arise and for this reason we study them.

The groups which occur as Galois groups of field extensions belong to a class of topological groups, the so-called profinite groups. This category of groups we investigate in the second chapter. These groups are fairly close relatives of finite groups. A profinite group is a topological group that can be realized as a projective limit of finite topological groups. For this reason we introduce the notion of projective limit. Also, we provide some useful characterizations of profinite groups. One of them asserts that a profinite group is a topological group which is Hausdorff, compact and totally disconnected. But these are actually very familiar properties. We have proved that a Galois group equipped with Krull topology has these properties too. So we have that Galois groups are profinite groups. In addition, we give some examples of profinite groups. Moreover, we define the dual construction of projective limit, which is the direct limit, and we prove some properties of projective and direct limits. For their proof we need some notions of category theory, which we define.

In the last decades cohomology of groups has played a central role in various branches of mathematics. Cohomology has a lot of applications in class field theory and it has played an important role for its development. In the third chapter we investigate the cohomology of finite groups. Firstly, we define the differential groups because they serve as an introduction to some of the basic techniques for studying the cohomology groups. Also, we present some general considerations about $G$-modules. In order to give the definition of cohomology group we introduce an extensive formalism of homomorphisms, modules and sequence, the so-called standard complex. Then we analyze the concrete meaning of the cohomology group. As seen in the definition of group cohomology, it is in general painful to find the $nth$ cohomology group for an arbitrary finite group $G$. We remark that in algebraic applications only the cohomology groups of low dimension appear, since for these groups we have a concrete algebraic interpretation. For this reason we study them completely. Moreover, we study the cohomology of cyclic groups in which we prove some essential statements of cohomology theory and we introduce the Herbrand Quotient. We present also a lot of important theorems of cohomology without their proof, such as Nakayama-Tate's theorem which is about the cohomological triviality. Another theorem is about the exactness of the cohomology sequence. For its proof we need some special mappings which we define.

In fourth chapter we study the cohomology of profinite groups. Their cohomology groups often contain important arithmetic information. We construct the cohomology group and for doing this we use the notion of discrete modules. So firstly we define discrete $G$-modules and we provide a characterization of them. Also, we calculate the cohomology groups in low dimension. Moreover, we investigate what happens to the cohomology groups $\mathcal{H}^q(G, A)$ if we change the group $G$, where $A$ is a discrete module. For doing this we need the notion of compatible pairs and some properties of them. Finally, we study some special homomorphisms of cohomology groups, such as the restiction and inflation, which they connect the cohomology group of a group $G$ with the cohomology group of a subgroup of $G$.

All this theory played an essential role in number theory. So in the last chapter we present the use of cohomology theory to solve problems in number theory. The cohomology theory help us to think about the extension problem of a group, since for an abelian group $A$ which is a $G$-module there is a natural bijective correspondence between the equivalence classes of extensions of A by $G$ and the elements of second cohomology group $\mathcal{H}^2$. This is the reason why we define the extension problem and we prove this correspondence. Moreover by the use of the second cohomology group $\mathcal{H}^2$ we can define the Brauer group. We have proved that Galois groups are profinite groups. A reasonable question is if the converse is true. It is an important result that any finite group is the Galois group of some field extension. This fact we can generalize to profinite groups. More precisely we prove that every profinite group is the Galois group of some field extension.

Heraklion, 16/5/2017

# Chapter 1

# Galois Theory for Infinite Extensions

Galois theory is an elegant interaction between field theory and group theory. It gives a bijective correspondence between intermediate fields of a Galois extension and subgroups of the Galois group of this extension. For the case of finite Galois extensions, the fundamental theorem of Galois theory establishes the bijective correspondence between intermediate fields and subgroups. Naturally, we wonder if this correspondence still holds in the case of infinite Galois extension. It is tempting to assume that this correspondence is true. Unfortunately, when the Galois extension is infinite then it isn't necessary a correspondence between the intermediate fields and subgroups of its Galois group.

## 1.1 Topological Prerequisites

***Definition* 1.1.1.** *A topological space $(X, \tau)$ is called $T_1$ space if for every $x \in X$ the singleton set $\{x\}$ is a closed set in $(X, \tau)$.*

***Definition* 1.1.2.** *A topological space $(X, \tau)$ is called **regular space** if for each $x \in X$ and each closed subset $K$ of $X$ with $x \notin K$ there exist open sets $A_1, A_2$ of $X$ satisfying the following*

$$K \subseteq A_1,\ x \in A_2 \ and\ A_1 \cap A_2 = \emptyset$$

***Definition* 1.1.3.** *A topological space $(X, \tau)$ is called **normal space** if for every closed subsets $K_1, K_2$ of $X$ with $K_1 \cap K_2 = \emptyset$, there exist open sets $A_1, A_2$ of $X$ satisfying the following*

$$K_1 \subseteq A_1,\ K_2 \subseteq A_2 \ and\ A_1 \cap A_2 = \emptyset$$

***Theorem* 1.1.4.** *Every compact Hausdorff topological space $(X, \tau)$ is a regular space.*

*Proof.* Let $A$ be a closed subset of $X$ and $x \in X \setminus A$, then for each $y \in A,\ x \neq y$. Since $X$ is Hausdorff space, implies that there exist open sets $U_y, V_y$ satisfying

$$x \in U_y,\ y \in V_y \ and\ U_y \cap V_y = \emptyset$$

We know that every closed subset of a compact space is compact, so $A$ is a compact set. Here $A \subseteq \bigcup_{y \in A} V_y$. That is $\{V_y : y \in A\}$ is an open cover for the compact set $A$. Therefore there exist $n \in \mathbb{N}$ and $y_1, \dots y_n \in A$ such that $A \subseteq \bigcup_{i=1}^{n} V_{y_i}$. Let $U := \bigcap_{i=1}^{n} U_{y_i}$ and $V := \bigcup_{i=1}^{n} V_{y_i}$. Then $U, V$ are open sets in $X$ satisfying $x \in U$, $A \subseteq V$ and

$$\begin{aligned} U \cap V &= U \cap (V_{y_1} \cup V_{y_2} \cup \dots \cup V_{y_n}) \\ &= (U \cap V_{y_1}) \cup (U \cap V_{y_2}) \cup \dots \cup (U \cap V_{y_n}) \\ &\subseteq (U_{y_1} \cap V_{y_1}) \cup (U_{y_2} \cap V_{y_2}) \cup \dots \cup (U_{y_n} \cap V_{y_n}) = \emptyset \end{aligned}$$

Thus, by definition, $(X, \tau)$ is a regular space. □

***Theorem* 1.1.5.** *Every compact Hausdorff topological space $(X, \tau)$ is a normal space.*

*Proof.* Let $A, B$ be closed subsets of $X$ such that $A \cap B = \emptyset$. Then for each $x \in A$, $x \notin B$. According to theorem 1.1.4 we have that the $(X, \tau)$ is a regular space. This implies that there exist open sets $U_x, V_x$ satisfying that $x \in U_x$, $B \subseteq V_x$ and $U_x \cap V_x = \emptyset$. Here $A \subseteq \bigcup_{x \in A} U_x$. That is $\{U_x : x \in A\}$ is an open cover for the compact set $A$. Therefore there exist $n \in \mathbb{N}$ and $x_1, \dots x_n \in A$ such that $A \subseteq \bigcup_{i=1}^{n} U_{x_i}$. Let $U := \bigcap_{i=1}^{n} U_{x_i}$ and $V := \bigcup_{i=1}^{n} V_{x_i}$. Then $U, V$ are open sets in $X$ satisfying $A \subseteq U$, $B \subseteq V$ and $U \cap V = \emptyset$. Indeed

$$\begin{aligned} U \cap V &= (U_{x_1} \cup \dots \cup U_{x_n}) \cap V \\ &= (U_{x_1} \cap V) \cup \dots \cup (U_{x_n} \cap V) \\ &\subseteq (U_{x_1} \cap V_{x_1}) \cup \dots \cup (U_{x_1} \cap V_{x_n}) = \emptyset \end{aligned}$$

□

***Proposition* 1.1.6.** *Let $X$ a topological space, $Y$ a Hausdorff topological space and $f$, $g$ are continuous maps from $X$ to $Y$, then the set*

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

*is a closed subset of $X$.*

*Proof.* Let $x \in X$ such that $f(x) \neq g(x)$. Since the $Y$ is Hausdorff, then we have that there are two open neighborhoods $U_1$, $U_2$ of $Y$, such that $f(x) \in U_1$, $g(x) \in U_2$ and $U_1 \cap U_2 = \emptyset$. The map $f$ is continuous at the point $x \in X$ and $U_1$ is an open neighborhood of $f(x)$, there is an open neighborhood of $x$, $V_1$, such that $f(V_1) \subset U_1$. Similarly, since the map $g$ is continuous at the point $x \in X$ and since $U_2$ is an open neighborhood of $g(x)$, then there is an open neighborhood of $x$, $V_2$, such that $f(V_2) \subset U_2$. We define $V := V_1 \cap V_2$. The set $V$ is open as the intersection of open sets, and $x \in V$, because $x \in V_1$ and $x \in V_2$. Moreover, $V \cap E = \emptyset$, whereas $f(V_1) \subset U_1$, $g(V_2) \subset U_2$ and $U_1 \cap U_2 = \emptyset$. But the complement of E, $X \setminus E$, in X will be the union of these sets $V$. So the $X \setminus E$ is an open set. Hence, the $E$ is a closed subset of $X$. □

***Proposition* 1.1.7.** *If $f : X \to Y$ is a continuous and bijective map where $X$ is compact topological space and $Y$ is Hausdorff topological space, then $f$ is homeomorphism.*

*Proof.* It suffices to show that $f$ is a closed map, since $f$ is a continuous and bijective map. Let $A$ be a closed subset of the topological space $X$. Then it is known that $A$ is compact, since $X$ is compact space. Thus the image $f(A)$ is compact subset of $Y$, since $f$ is continuous. But $Y$ is Hausdorff topological space, so $f(A)$ is a closed subset of $Y$. Therefore $f$ is a closed map, and then $f$ is homeomorphism. □

***Remark* 1.1.8.** *If the set $X \neq \emptyset$ is finite and $X$ is a topological space equipped with any topology $\tau$, then the topological space $(X, \tau)$ is compact.*

*Proof.* Let $\mathcal{U} = \{A\}$ be an open cover of $X$, that is $X = \cup A$. Then for every $x \in X$, there exists $A_x \in \mathcal{U}$, with $x \in A_x$. If for every $x \in X$ we take only one $A_x \in \mathcal{U}$ such that $x \in A_x$, then we construct a finite subfamily, $(A_x)_{x \in A}$, of $\mathcal{U}$ that covers $X$. This means that every open cover of $X$ has a finite subcover. Therefore $(X, \tau)$ is compact. □

***Definition* 1.1.9.** *A map $f : A \to B$, where $A$ is a topological space and $B$ is a set, is called locally constant if for every $a \in A$ there exists an open neighborhood $U$ of $a$ such that $f$ is constant on $U$.*

Every constant function is locally constant. Also, if $f : A \to B$ is locally constant, then $f$ is constant on any connected component of $A$. The converse is true for locally connected spaces.

***Proposition* 1.1.10.** *Let $f : A \to B$, where $A$ is a topological space and $B$ is a discrete space. Then $f$ is continuous if and only if $f$ is locally constant.*

*Proof.* Since $B$ is a discrete space, then $\mathcal{B} = \{\{b\}, b \in B\}$ is a basis of $B$.
" $\Rightarrow$ " We assume that $f$ is continuous. Thus, $f^{-1}(\{b\})$ is open on $A$ for every $b \in B$. In particular, if $f(a) = b$, then $a \in f^{-1}(\{b\})$ and $f^{-1}(\{b\})$ is open. That is there exists an open neighborhood $f^{-1}(\{b\})$ of $a$ such that $f$ constant on $f^{-1}(\{b\})$. This is true for every $a \in A$. Thus, $f$ is locally constant.
" $\Leftarrow$ " Let $f$ is locally constant. This means that for every $a \in A$ there exists an open neighborhood $U$ of $a$ such that $f$ is constant on $U$, that is $f(x) = y \in B$ for every $x \in U$. Thus, $f(U) = \{y\}$. Therefore, for every open neighborhood $W$ of $f(a)$ there exists an open neighborhood of $a$ such that $f(U) \subseteq W$, so then $f$ is continuous in $a$. This is true for every $a \in A$. Consequently, $f$ is continuous. □

## 1.2 Topological Groups

In order to put a topology to infinite Galois groups we will need to define the topological groups and look into some properties of them as well.

***Definition* 1.2.1.** *A group $(G, \cdot)$ is called topological group if it is a topological space equipped with topology $\tau$, the multiplication map*

$$\delta_1 : G \times G \to G, \ (x, y) \mapsto xy$$

*is continuous, where $G \times G$ is equipped with product topology, and the inverse map*

$$\delta_2 : \ G \to G, \ x \mapsto x^{-1}$$

*is also continuous.*

***Comment* 1.2.2.** *1) If the group operation is addition instead of multiplication, then $xy$ and $x^{-1}$ should be regarded as $x + y$ and $-x$, respectively. The identity of a multiplicative group will be denoted by $e := 1$ and that for an additive group by $0$.*
*2) A homomorphism between two topological groups is a continuous group homomorphism and an isomorphism between two topological groups is a homeomorphic group isomorphism.*

We will mention some examples of topological groups.

***Example* 1.2.3.** *1) $G = \{e\}$*
*2) $G = \mathbb{R}$ equipped with Euclidean topology. Similarly, if $G = \mathbb{R}^n$.*
*3) $G = \mathbb{C}$ equipped with Euclidean topology. Similarly, if $G = \mathbb{C}^n$.*
*4) Let $K = \mathbb{R}$ or $\mathbb{C}$ and we consider $G = GL_n(K) = \{A \in M_n(K) \,|\, detA \neq 0\}$. Since $M_n(K) \subseteq \mathbb{R}^{n\times n}$, the topology on $GL_n(K)$ is the subspace topology.*
*5) $G = SL_n(K) = \{A \in M_n(K) \,|\, detA = 1\}$*
*6) $G = SO_n(\mathbb{R}) = \{A \in SL_n(\mathbb{R}) \,|\, A^T A = AA^T I_n\}$*
*7) If $G$ is any group equipped it with the discrete topology, then it is a topological group. We call this kind of topological groups discrete groups. For example $G = \mathbb{Z}$.*

Let $G$ a topological group and $U, V$ are subsets of $G$, then we denote by $UV := \{xy : x \in U, y \in V\}$ and $U^{-1} := \{x^{-1} : x \in U\}$. Similarly, in the additive case we can define $U + V$ and $-U$. The continuity of the maps $\delta_1$ and $\delta_2$ can be expressed as follows: $\delta_1$ is continuous in $x$ if and only if for each neighborhood $W$ of $xy$ there exists a neighborhood $U$ of $x$ such that $Uy \subseteq W$. Similarly, $\delta_1$ is continuous in $y$ if and only if for each neighborhood $W$ of $xy$ there exists a neighborhood $V$ of $y$ such that $xV \subseteq W$. Additionally, $\delta_1$ is continuous in both $x$ and $y$ if and only if for each neighborhood $W$ of $xy$ there exist a neighborhood $U$ of $x$ and a neighborhood $V$ of $y$ such that $UV \subseteq W$. Similarly, $\delta_2$ is continuous in $x$ if and only if for each neighborhood $W$ of $x^{-1}$ there exists a neighborhood $U$ of $x$ such that $U^{-1} \subseteq W$.

***Theorem* 1.2.4.** *Let $G$ be a topological group and $a \in G$ be a fixed element of $G$. Then the mappings*

$$r_a : G \to G, \ x \mapsto xa$$

*and*

$$l_a : G \to G, \ x \mapsto ax$$

*are homeomorphisms of $G$. Also, the inverse map $\delta_2$ and the inner automorphisms*

$$G \to G, \ \ x \mapsto axa^{-1}$$

*are homeomorphisms of $G$.*

*Proof.* It is clear that $r_a, l_a$ are bijective maps. Also, we will show that $r_a$ is a continuous map. Let $W$ be an open neighborhood of $xa$. Since $G$ is a topological group, there exists a neighborhood $U$ of $x$ such that $Ua \subseteq W$. Thus, $r_a$ is continuous in $x$, where $x$ is an arbitrary element of $G$ and so $r_a$ is continuous. Moreover, it is easy to see that the inverse of $r_a$ which is the $r_a^{-1} : G \to G, \ x \mapsto xa^{-1}$, is also continuous by the same argument as above. Thus, $r_a$ is homeomorphism. Similarly, we can prove that $l_a$ is homeomorphism. For the inverse map $\delta_2$ it is clear that $\delta_2$ is an injective, surjective and continuous map. Since $\delta_2^{-1}(x) = x^{-1}$ is also continuous, then we have that $\delta_2$ is a homeomorphism. Every inner automorphism is a homeomorphism as it is the composition of two homeomorphisms $x \mapsto ax$ and $a \mapsto xa^{-1}$. □

***Corollary* 1.2.5.** *Let $F$ be a closed, $P$ an open, $A$ any subset of a topological group $G$ and $a \in G$. Then $aF, Fa, F^{-1}$ are closed and $aP, Pa, P^{-1}, AP, PA$ are all open.*

*Proof.* Since $F$ is closed and $l_a, r_a$ and the inverse map are homeomorphisms, then $aF, Fa, F^{-1}$ are closed. Also, $aP, Pa, P^{-1}$ are open, because $P$ is open and the inverse map is homeomorphism. It is clear that $AP = \bigcup_{a \in A} aP$ and $PA = \bigcup_{a \in A} Pa$ and the union of open sets is open. □

***Definition* 1.2.6.** *A subset $U$ of a group $G$ is said to be symmetric if $U = U^{-1}$. In case $G$ is an additive group, $U$ is symmetric if $U = -U$.*

***Proposition* 1.2.7.** *In a topological group there exists a base $\{U\}$ of symmetric neighborhoods of $e$.*

*Proof.* Let $\{V\}$ be a base of open neighborhoods of $e$. Since $e = e^{-1}$ and we can prove that the map $f : G \to G, \ x \mapsto x^{-1}$ is an homeomorphism because $G$ is a topological group. So for every $V \in \{V\}$, we have that $V^{-1}$ is an open neighborhood of $e$. But $U = V \cap V^{-1}$ is a symmetric neighborhood of $e$ because $U^{-1} = V \cap V^{-1} = U$. Therefore, each $V$ contains a $U$. On the other hand, $\{V\}$ is a base of open neighborhoods of $e$, so then each open neighborhood $A$ of $e$ contains a $V$, that is $U \subseteq V \subseteq A$. Hence $\{U\}$ is a base of symmetric neighborhoods of $e$. □

***Proposition* 1.2.8.** *Let $G$ a topological group and let $a \in G$, then for each neighborhood $V$ of $a$ there is a neighborhood, $U$, of $e$ such that*

$$V = aU$$

*Proof.* Let $U := a^{-1}V$. Since $a \in V$ then $e \in U$. Since $G$ is a topological group and $a \in G$, then $l_a : G \to G$, where $x \mapsto ax$ is a homeomorphism. Also $a^{-1} \in G$, so then $l_{a^{-1}}$ is a homeomorphism. Since $V$ is an open set, then $l_{a^{-1}}(V)$ is open, because the map $l_{a^{-1}}$ is continuous. Moreover $l_{a^{-1}}(V) = a^{-1}V = U$. Thus we have $e \in U$ and $U$ is open, that is $U$ is a neighborhood of $e$. Hence $U = a^{-1}V \Rightarrow V = aU$. □

***Lemma* 1.2.9.** *Let $G$ a topological group, let $F$ be a closed subset and $C$ a compact subset such that $F \cap C = \emptyset$. Then there is a neighborhood $V$ of $e$ such that $F \cap CV = \emptyset$.*

*Proof.* Let $x \in C$ such that $x \in G \setminus F$, where $G \setminus F$ is open. So $G \setminus F$ is an open neighborhood of $x$. There is a neighborhood $W_x$ of $e$ such that $W_x^2 \subseteq x^{-1}(G \setminus F)$, that is $xW_x^2 \subseteq G \setminus F$. According to proposition 1.2.8 we have that there exist a neighborhood $W_x$ of $e$ such that $G \setminus F = xW_x \Rightarrow W_x = x^{-1}(G \setminus F)$, but $W_x^2 \subseteq W_x$. Hence $W_x^2 \subseteq x^{-1}(G \setminus F)$. Then there is a set of points $x_i$, and a set of associated neighborhoods of $e$, $W_i$, such that $x_iW_i^2 \subseteq G \setminus F$ and $C \subseteq \cup_i x_iW_i$. Since $C$ compact we have there is finitely many of points $x_i$, $i = 1, \dots, n$ and a set of associated neighborhoods of $e$, $W_i$, such that $x_iW_i^2 \subseteq G \setminus F$ and $C \subseteq \bigcup_{i=1}^{n} x_iW_i$. Set $V = \bigcap_{i=1}^{n} W_i$. Now for any $x \in C$ then $x \in x_iW_i$ for some $i$, and $xV \subseteq x_iW_i^2 \subseteq G \setminus F$. Then $xV \cap F = \emptyset$. Thus, $CV \cap F = \emptyset$, and this complete the proof. □

***Definition* 1.2.10.** *Let $G$ a topological space. $G$ is homogeneous if for every pair of points $x, y \in G$, there exists a homeomorphism $f$ such that $f(x) = y$.*

***Proposition* 1.2.11.** *Every topological group is homogeneous.*

*Proof.* Let $G$ be a topological group and $x, y$ be a pair of points in the topological group $G$. We define $f : G \to G$, where $g \mapsto yx^{-1}g$. Then $f(x) = y$. Also, $f$ is a left multiplication by the element $yx^{-1}$, so then $f$ is a homeomorphism, according to theorem 1.2.4. Therefore, $f$ is a homomorphism satisfying that $f(x) = y$. This is true for every pair of points in $G$. Hence, $G$ is homogeneous. □

Homogeneity is one interesting property of topological groups, because it makes us able to examine every open neighborhood in the topological groups just by looking at the open neighborhood of the identity element $e := 1$.

With the use of the theorem 1.2.4 we can prove that if we know a base of neighborhoods of the identity in a topological group, then we can find a base of neighborhoods of any other point.

***Theorem* 1.2.12.** *If $\{U\}$ is a base of open neighborhoods of $1 := e$ in a topological group $G$, then $\{xU\}$ and $\{Ux\}$, where $x$ runs over $G$ and $U$ over $\{U\}$ form a basis of the topology of $G$.*

*Proof.* Let $a \in G$ and let $W$ be an open neighborhood of $a$. We know that $l_a^{-1} : G \to G$, where $x \mapsto a^{-1}x$ is a homeomorphism in $x$, according to theorem 1.2.4 and $l_a^{-1}(W) = a^{-1}W$ is an open set which contains $e$. So then there exists a $U \in \{U\}$ such that $U \subseteq a^{-1}W$. This implies that $aU \subseteq W$, which proves that $\{xU\}$ is a base of the topology on $G$. With the use of similar arguments we can prove that $Ux$ is also base of the topology on $G$. □

Since a topological group is not only a topological space but also a group, we wonder if a subgroup of a topological group is a topological group as well.

***Proposition* 1.2.13.** *Let $G$ a topological group. Then every subgroup $H$ of $G$ is also a topological group.*

*Proof.* Since $H \leq G$ then the multiplication map and the inverse map on $H$ are the multiplication map and inverse map on $G$ restricted to the subgroup $H$. So then both the multiplication map and the inverse map on $H$ are continuous. Consequently, $H$ is a topological group. □

***Proposition* 1.2.14.** *Let $G$ be a topological group.*

*(i) Every open subgroup of $G$ is closed in $G$.*

*(ii) Every closed subgroup of $G$ of finite index is open.*

*(iii) If $G$ is compact, then a subgroup of $G$ is open if and only if it is closed and of finite index.*

*Proof.* (i) Let $H$ be an open subgroup of $G$. Let also $a \in cl(H) = \bar{H}$. We have that $aH$ is open, since $H$ is. So then $aH$ is a neighborhood of $a$, since it is an open set containing $a$. Also, $aH \cap H \neq \emptyset$, since $a \in cl(H) = \bar{H}$. So there exists $h_1, h_2 \in H$, such that $h_2 = ah_1 \in aH \cap H$, and then $a = h_2 h_1^{-1} \in H$, since $H$ is a subgroup. Hence, $\bar{H} \subseteq H$, but $H \subseteq \bar{H}$, so $H = \bar{H}$. Consequently, $H$ is closed. (ii) We assume that $H$ is a closed subgroup of $G$ of finite index, then

$$G = g_1 H \cup g_2 H \cup \cdots \cup g_n H \quad (disjoint\ union)$$

where $g_1 = 1$. We have that $g_i H$, for every $i = 1, \cdots, n$, is closed, since $H$ is closed. So then $G$ is closed. Thus, $H$ being the complement of $\bigcup_{i=2}^{n} g_i H$ in $G$, is open.

(iii) Let $H$ be an open subgroup of $G$. Then from (i) $H$ is closed. In addition, we have that the cosets of $H$ provide an open covering of $G$ and since $G$ is compact, then $H$ can have only finitely many cosets in $G$. Therefore, $H$ is closed and of finite index. The converse is true by $(ii)$. □

## 1.3 Finite Galois Theory and Krull Topology

In this section we will remind some basics of the finite Galois theory and we will define the Krull topology.

***Definition* 1.3.1.** *The algebraic field extension $L/K$ is called Galois if it is normal and separable*

***Definition* 1.3.2.** *Let $L/K$ be a Galois field extension. The Galois group $Gal(L/K)$ is the set of all automorphisms on the field $L$ that fixes every element of the field $K$, that is $\sigma(x) = x$ for every $x \in K$ and $\sigma \in Gal(L/K)$.*

***Definition* 1.3.3.** *Let $H$ be a subset of $Aut(L/K)$, then we define the fixed field of $H$ which is denoted by*

$$\mathcal{F}(H) = \{a \in L : \tau(a) = a, \forall \tau \in H\}$$

*Then $\mathcal{F}(H)$ is a subfield of $L$.*
*Let $F$ be an intermediate field of $L/K$, that is $K \leqslant F \leqslant L$, then we define the fixed group of $F$ which is denoted by $\mathcal{G}(F)$ and is defined as*

$$\mathcal{G}(F) = \{\sigma \in Aut(L) \,|\, \sigma(a) = a, \forall a \in F\}$$

*and $\mathcal{G}(F) \leqslant Aut(L/K)$.*

Let $K$ be a field and $N/K$ be a Galois extension. Let also

$$G = G_{N/K} = \{\sigma \in Aut(N) : \sigma|_K = id_K\}$$

the Galois group of the extension $N/K$. We denote by $\{N : K\}$ the lattice of intermediate fields $L$, such that $K \leqslant L \leqslant N$, and $\{G : 1\}$ the lattice of subgroups $H$ of $G$.

***Theorem* 1.3.4 (Fundamental Theorem of Galois Theory).** *Let $N/K$ be a finite, normal and separable field extension and $G = Gal(N/K)$. Then $[N : K] = |Gal(N/K)|$ and there is a $1-1$ inclusion reversing correspondence between intermediate fields of $N/K$ and subgroups of $G$, given by*

$$\{N : K\} \underset{\psi}{\overset{\phi}{\rightleftarrows}} \{G : 1\}$$

*$\phi(L) = Gal(N/L) = \mathcal{G}(L)$ and $\psi(H) = \mathcal{F}(H)$, where $K \leqslant L \leqslant N$ and $H$ subgroup of $G$. That is the maps are inverse lattice anti-isomorphism. This means that $\psi \circ \phi = id_{\{N:K\}}$ and $\phi \circ \psi = id_{\{G:1\}}$.*
*Moreover, if $L \leftrightarrow H$, then $|\mathcal{G}(L)| = [N : L]$ and $[L : K] = [G : H]$.*
*Furthermore, $H$ is normal in $G$ if and only if $L/K$ is Galois. When this occurs, then $Gal(L/K) \cong G/G_{N/L}$.*

$$\begin{tikzcd}
N \arrow[r, leftrightarrow] \arrow[d, dash] & < id_N > \arrow[d, dash] \\
L \arrow[r, leftrightarrow] \arrow[d, dash] & Gal(N/L) = \mathcal{G}(L) \arrow[d, dash] \\
K \arrow[r, leftrightarrow] & G_{N/K} = Gal(N/K)
\end{tikzcd}$$

Let us assume now that the extension $N/K$ is not necessary finite. The maps $\psi, \phi$ are defined as above and it is clear that they are lattice anti-homomorphisms. In particular we have the following

***Proposition* 1.3.5.** *We assume that $N/K$ is not necessary finite and the maps $\psi, \phi$ are defined as above. Then*

$$\psi \circ \phi = id_{\{N:K\}}$$

*Proof.* Let $K \leqslant L \leqslant N$. Then $\psi(\phi(L)) = \psi(G_{N/L}) = \{x \in N \,|\, G_{N/L}x = x\}$. It is clear that $L \subseteq \psi(\phi(L))$, since $G_{N/L}x = x$, for $x \in L$. Let now $x \in N$ such that $G_{N/L}x = x$ then $x$ is the only conjugate of $x$. Thus $x \in L$ and then $\psi(\phi(L)) \subseteq L$ . Therefore, $L = \psi(\phi(L))$. □

***Corollary* 1.3.6.** *The map $\phi$ is injective and $\psi$ is surjective.*

*Proof.* It is clear from proposition 1.3.5. □

However in the general case if we have infinite extension, then the maps are not anti-isomorphism. It is possible to happen that different subgroups of $G_{N/K}$ have the same fixed field, which means that $\psi$ isn't injective. This will be illustrated in the following example.

***Example* 1.3.7.** *Let $K = \mathbb{F}_p$ be the finite field with $p \in \mathbb{P}$ elements. Let $l \neq 2$ be a prime number and we consider the sequence*

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$$

*where $K_i$ is the unique extension field of $K$ of order $[K_i : K] = l^i$. Let*

$$N = \bigcup_{i=1}^{\infty} K_i = \bar{\mathbb{F}}_p$$

*It is clear that $K_i = \{x \in N \,|\, x^{p^{l^i}} - x = 0\}$. The extension $N/K$ is Galois and let $G := Gal(N/K)$. We consider the Frobenius $K$-automorphism $\phi : N \to N$, with $\phi(x) = x^p$, for every $x \in N$. We set $H := \{\phi^n \,|\, n \in \mathbb{Z}\} \leqslant G$.*
*We shall prove that:*

*i) The groups $H$ and $G$ have the same fixed field, that is $\psi(G) = \psi(H)$,*
*ii) $H \neq G$.*
*So then $\psi$ isn't injective. Firstly, we will prove (i): It is obvious that$\psi(G) = K$. It suffices to show that $\psi(H) = K$. Let $x \in \psi(H)$, that is $x \in N$ and $Hx = x$. But $\phi \in H$, so then $\phi(x) = x$. Also, $\phi(x) = x^p$. So $x^p = x$, which implies that $x \in K$. Thus, $\psi(H) \subseteq K$. Clearly $K \subseteq \psi(H)$. Therefore, $\psi(H) = K$. For $(ii)$ we will prove that $H \neq G$. We will construct a $K$-automorphism $\sigma$ of $N$, which is not contained in $H$. We define $k_i := 1 + l + \cdots + l^{i-1}$, for each $i = 1, 2, ...$ and we consider the $K$-automorphisms $\phi^{k_i}$ of $N$. If $x \in K_i$, then*

$$\begin{aligned}\phi^{k_{i+1}}(x) &= \phi^{1+l+\cdots+l^{i-1}+l^i}(x) = \phi^{1+l+\cdots+l^{i-1}}(\phi^{l^i}(x)) \\ &= \phi^{1+l+\cdots+l^{i-1}}(x^{p^{l^i}}) = \phi^{1+l+\cdots+l^{i-1}}(x) = \phi^{k_i}(x)\end{aligned}$$

*Thus,*

$$\phi^{k_{i+1}}|_{K_i} = \phi^{k_i}|_{K_i} \qquad (1.1)$$

*Now we define $\sigma : N \to N$, with $\sigma(x) = \phi^{k_i}(x)$, for every $x \in K_i$. We have that $\sigma$ is well-defined, since $l^i \mid l^{i+1}$, then $K_i \subseteq K_{i+1}$. If $x \in K_i$, then $x \in K_{i+1}$ etc, and so $\sigma(x) = \phi^{k_i}(x)$, $\sigma(x) = \phi^{k_{i+1}}(x)$. But from equation (1.1) we have that $\phi^{k_{i+1}}(x) = \phi^{k_i}(x)$. In addition, it is clear that $\sigma$ is an automorphism. Now, if $\sigma \in H$, then there is $n \in \mathbb{Z}$ such that $\sigma = \phi^n$. Hence, for every $i = 1, 2, ...$ we have $\sigma|_{K_i} = \phi^n|_{K_i} = \phi^{k_i}|_{K_i}$ and then*

$$\begin{aligned}\phi^n|_{K_i} = \phi^{k_i}|_{K_i} &\Leftrightarrow \phi^{n-k_i}|_{K_i} = id_{K_i} \\ ord(\phi|_{K_i}) \mid n - k_i &\Leftrightarrow l^i \mid n - k_i \\ n \equiv k_i \mod l^i & \qquad (1.2)\end{aligned}$$

*since $[K_i : K] = l^i$ and $G_{K_i/K} =< \phi|_{K_i} >$ Then we multiply the equation (1.2) by $(l-1)$ and we obtain that*

$$(l-1)n \equiv (l-1)k_i \mod l^i$$

*But $(l-1)k_i = (l-1)(1 + l + \cdots + l^{i-1}) = l^i - 1$. Therefore,*

$$(l-1)n \equiv -1 \mod l^i \ for\ every\ i = 1, 2, ...$$

*which is impossible if $l \neq 2$.*

The idea in this example is the following: we will see later that the Galois group $G = Gal(N/\mathbb{F}_p)$ is isomorphic with the additive group $\mathbb{Z}_l$ of $l$-adic integers. The Frobenius automorphism $\phi$ corresponds to $1 \in \mathbb{Z}_l$. So $H \cong \mathbb{Z} \subsetneq \mathbb{Z}_l$. The elements of $G$ which aren't in $H$ correspond to the $l$-adic integers which are not in $\mathbb{Z}$, (in our case $\sigma = 1 + l + l^2 + \cdots$).

Although the above example shows that the Fundamental theorem of Galois theory (Theorem 1.3.4) does not hold for infinite Galois extensions, it suggest us a way of modifying the theorem so that it will be valid even in those cases. The map $\sigma$ of the above example is approximated by the maps $\phi^{k_i}$, since it coincides with $\phi^{k_i}$ on $K_i$ which becomes larger with increasing $i$ and $N = \bigcup_{i=1}^{\infty} K_i$. This leads to the idea of defining a topology in $G$ such that $\sigma = \lim_i \phi^{k_i}$. Then $\sigma$ would belong to the closure of $H$. Now one could hope that there is a bijective correspondence between the intermediate fields of $N/K$ and the closed subgroups of Galois group $G$.

Now we will define a topology in Galois group. We remind that $L \in \{N : K\}$ means that $K \leqslant L \leqslant N$ and we set

$$\mathcal{F} = \{L/K : K \leqslant L \leqslant N, \, L/K \, is \, finite \, Galois\}$$

Also, we set

$$\mathcal{B}_1 = \{G_{N/L} \,|\, L/K \, finite \, Galois \, extension, \, L \in \{N : K\}\}$$

***Lemma* 1.3.8.** *Let $G_{N/K}$ for some Galois extension $N/K$ and let*

$$\mathcal{F} = \{L/K : K \leqslant L \leqslant N, \, L/K \, is \, finite \, Galois\}$$

*Then $\bigcap_{L/K \in \mathcal{F}} G_{N/L} = \{1\}$ and for all $\sigma \in G$ we have that $\bigcap_{L/K \in \mathcal{F}} \sigma G_{N/L} = \{\sigma\}$*

*Proof.* Let $\sigma \in \bigcap_{L/K \in \mathcal{F}} G_{N/L}$, then $\sigma$ is an $L$-automorphism of $N$ for every $L$ such that $K \leqslant L \leqslant N$, $L/K$ is a finite Galois extension. Let also $a \in N$ then there exists an $E \in \mathcal{F}$ such that $a \in E$. Thus $\sigma \in G_{N/E}$ because $\sigma \in \bigcap_{L/K \in \mathcal{F}} G_{N/L}$ and then $\sigma$ fixes $E$, so $\sigma(a) = a$. Hence, for every $a \in N$ we have $\sigma(a) = a$, and therefore $\sigma = 1$. So $\bigcap_{L/K \in \mathcal{F}} G_{N/L} = \{1\}$.

If $\tau \in \bigcap_{L/K \in \mathcal{F}} \sigma G_{N/L}$, then $\tau\sigma^{-1} \in \bigcap_{L/K \in \mathcal{F}} G_{N/L}$, so $\tau\sigma^{-1} = 1 \Rightarrow \sigma = \tau$. Thus, $\bigcap_{L/K \in \mathcal{F}} \sigma G_{N/L} = \{\sigma\}$. □

***Lemma* 1.3.9.** *If $G_{N/L_1}, G_{N/L_2} \in \mathcal{B}_1$, then $G_{N/L_1} \cap G_{N/L_2} \in \mathcal{B}_1$.*

*Proof.* Since $L_1/K, L_2/K$ are finite Galois, so is $L_1L_2/K$ and then $L_1L_2 \in \{N : K\}$. However $G_{N/L_1L_2} = Gal(N/L_1L_2) = G_{N/L_1} \cap G_{N/L_2}$, since $\sigma \in G_{N/L_1} \cap G_{N/L_2} \Leftrightarrow \sigma_{L_1} = 1_{L_1}$ and $\sigma|_{L_2} = 1|_{L_2} \Leftrightarrow L_1, L_2 \subseteq \mathcal{F}(\sigma) \Leftrightarrow L_1L_2 \subseteq \mathcal{F}(\sigma) \Leftrightarrow \sigma \in G_{N/L_1L_2}$. Therefore $G_{N/L_1} \cap G_{N/L_2} = G_{N/L_1L_2} \in \mathcal{B}_1$. □

***Lemma* 1.3.10.** *Let $N/K$ be an infinite Galois extension with Galois group $G_{N/K} = Gal(N/K)$. Then*

$$\mathcal{B}_\sigma = \{\sigma G_{N/L} \,|\, L/K \, finite \, normal \, extension, \, L \in \{N : K\}\}$$

*forms a basis for a topology on G.*

*Proof.* Each open set is a union of cosets $\sigma G_{N/L}$ hence an arbitrary union of open sets is also a union of such cosets, so in this topology an arbitrary union of open sets is open. Also, $G_{N/K}$ is open, since $K/K$ is a finite Galois extension of degree 1. In addition we will check that open sets are closed under finite intersections. It suffices to check that for two elements of the basis. If $\tau_1 G_{N/L_1}$ and $\tau_2 G_{N/L_2}$ are two basis elements and let $\tau \in \tau_1 G_{N/L_1} \cap \tau_2 G_{N/L_2}$, then from lemma 1.3.9 we have that $G_{N/L_1} \cap G_{N/L_2} \in \mathcal{B}_1$, thus $\tau(G_{N/L_1} \cap G_{N/L_2})$ is open. Finally we will show that $\emptyset$ is open. Indeed, for some $G_{N/L} \in \mathcal{B}_1$ with $G_{N/L} \neq G_{N/K}$ we choose $\tau_1, \tau_2 \in G_{N/K}$ such that $\tau_1 G_{N/L} \neq \tau_2 G_{N/L}$ (which we can do, otherwise $G_{N/L} = G_{N/K}$). Then $\tau_1 G_{N/L} \cap \tau_2 G_{N/L} = \emptyset$ and so $\emptyset$ is open. Therefore $\mathcal{B}_\sigma$ is indeed the basis for a topology on $G_{N/K}$. □

Now we can define the following.

***Definition* 1.3.11.** *Let $N/K$ be an infinite Galois extension and $G = G_{N/K}$. The set*

$$\mathcal{B}_\sigma = \{\sigma G_{N/L} \,|\, L/K \, finite\ normal\ extension,\ L \in \{N : K\}\}$$

*forms a basis of open neighborhoods of $\sigma \in G$. The topology which is defined by $\mathcal{B}_\sigma$, that is has basis $\mathcal{B}_\sigma$, is called the* ***Krull topology*** *on $G$.*

We can show that

$$\mathcal{B}_1 = \{G_{N/L} \,|\, L/K \, finite\ normal\ extension,\ L \in \{N : K\}\}$$

forms a basis of open neighborhoods of $1 \in G$.

We have that $G_{N/L} \trianglelefteq G_{N/K} = G$, since $L/K$ is a finite Galois extension. Moreover, if $G_{N/L}$ is such that $L/K$ is a finite Galois extension with $K \leqslant L \leqslant N$, then $[G_{N/K} : G_{N/L}] < \infty$. Thus, there are $\sigma_1, \dots, \sigma_{n-1}$ such that $G = H \cup \sigma_1 H \cup \dots \cup \sigma_{n-1} H$. This means that $G \setminus \sigma G_{N/L}$ is a union of finite number of cosets of $G_{N/L}$, which are open sets. So, $\sigma G_{N/L}$ is both open and closed set. Thus the Krull topology has a basis of sets which are both closed and open.

***Proposition* 1.3.12.** *Let $N/K$ be an infinite Galois extension and $G = G_{N/K}$. The Galois group $G$ equipped with Krull topology is a topological group.*

*Proof.* Let $\delta_1 : G \times G \to G$, with $(\sigma, \tau) \mapsto \sigma\tau$. It suffices to show that $\delta_1^{-1}(A)$ is open neighborhood of $G \times G$ for every open neighborhood $A$ of $G$. Let $A$ be an open neighborhood of $G$, then $A = \cup \sigma G_{N/L}$ and $\delta_1^{-1}(\cup \sigma G_{N/L}) = \cup \delta_1^{-1}(\sigma G_{N/L})$. We have that

$$\begin{aligned} \delta_1^{-1}(\sigma\tau G_{N/L}) &= \{(g_1, g_2) \in G \times G : g_1 g_2 \in \sigma\tau G_{N/L}\} \\ &= \{(g_1, g_2) \in G \times G : \tau^{-1}\sigma^{-1} g_1 g_2 \in G_{N/L}\} \end{aligned}$$

and

$$\begin{aligned}\sigma G_{N/L} \times \tau G_{N/L} &= \{(g_1, g_2) \in G \times G : g_1 \in \sigma G_{N/L}, g_2 \in \tau G_{N/L}\} \\ &= \{(g_1, g_2) \in G \times G : \sigma^{-1} g_1 \in G_{N/L}, \tau^{-1} g_2 \in G_{N/L}\}\end{aligned}$$

Let $(g_1, g_2) \in \sigma G_{N/L} \times \tau G_{N/L}$. Since $\sigma^{-1} g_1 \in G_{N/L}$, then there is $g \in G_{N/L}$ such that $\sigma^{-1} g_1 = g$. So $\tau^{-1}\sigma^{-1} g_1 g_2 = \tau^{-1} g g_2$ and we have that $g_2 \in \tau G_{N/L}$, which implies that there exists $g'$ such that $g_2 = \tau g'$, and then $\tau^{-1}\sigma^{-1} g_1 g_2 = \tau^{-1} g \tau g'$. But $\tau^{-1} g \tau g' = g''$, since $G_{N/L} \trianglelefteq G$ and $g'' \in G_{N/L}$.Thus, $\tau^{-1}\sigma^{-1} g_1 g_2 = g'' g' \in G_{N/L}$, that is $(g_1, g_2) \in \delta_1^{-1}(\sigma\tau G_{N/L})$. Hence, $\sigma G_{N/L} \times \tau G_{N/L} \subseteq \delta_1^{-1}(\sigma\tau G_{N/L})$. Also it is clear that $\sigma G_{N/L} \times \tau G_{N/L}$ is an open neighborhood as for product topology of $G \times G$ and $(\sigma, \tau) \in \sigma G_{N/L} \times \tau G_{N/L}$. Therefore, for every $(\sigma, \tau) \in \delta_1^{-1}(\sigma\tau G_{N/L})$ there exists an open neighborhood $\sigma G_{N/L} \times \tau G_{N/L}$ of $(\sigma, \tau)$ such that $\sigma G_{N/L} \times \tau G_{N/L} \subseteq \delta_1^{-1}(\sigma\tau G_{N/L})$. This implies that $\delta_1^{-1}(\sigma\tau G_{N/L})$ is an open neighborhood of $G \times G$ and so $\delta_1^{-1}(\sigma G_{N/L})$ is open for every $G_{N/L} \in \mathcal{B}_\sigma$. Moreover, we have that $A = \cup \sigma G_{N/L}$ is an open as a union of open sets. Thus, $\delta_1$ is a continuous map. Furthermore, we will show that $\delta_2 : G \to G$, with $\sigma \mapsto \sigma^{-1}$ is a continuous map. It suffices to show that $\delta_2^{-1}(A)$ is open neighborhood of $G$ for every open neighborhood $A$ of $G$. Let $A$ be an open neighborhood of $G$, then $A = \cup \sigma G_{N/L}$ and $\delta_2^{-1}(\cup \sigma G_{N/L}) = \cup \delta_2^{-1}(\sigma G_{N/L})$. We have that

$$\begin{aligned}\delta_2^{-1}(\sigma^{-1} G_{N/L}) &= \{g \in : g^{-1} \in \sigma^{-1} G_{N/L}\} \\ &= \{g \in G : \sigma g^{-1} \in G_{N/L}\}\end{aligned}$$

$$\sigma G_{N/L} = \{g \in G : g = \sigma g', g' \in G_{N/L}\}$$

Let $g \in \sigma G_{N/L}$, then $g = \sigma g'$, $g' \in G_{N/L}$. So $\sigma g^{-1} = \sigma g'^{-1} \sigma^{-1} = g'' \in G_{N/L}$, since $G_{N/L} \trianglelefteq G$. This means that $\sigma G_{N/L} \subseteq \delta_2^{-1}(\sigma^{-1} G_{N/L})$. Thus, $\sigma G_{N/L}$ is an open neighborhood of $\sigma$. This implies that for every $\sigma \in \delta_2^{-1}(\sigma^{-1} G_{N/L})$ there is an open neighborhood $\sigma G_{N/L}$ of $\sigma$ satisfying that $\sigma G_{N/L} \subseteq \delta_2^{-1}(\sigma^{-1} G_{N/L})$. So $\delta_2^{-1}(\sigma^{-1} G_{N/L})$ is an open neighborhood of $G$ and then $\delta_2^{-1}(\sigma G_{N/L})$ is open for every $G_{N/L} \in \mathcal{B}_\sigma$. Hence, we have that $A = \cup \sigma G_{N/L}$ is an open as a union of open sets. Thus, $\delta_2$ is a continuous map. Therefore the Galois group $G$ equipped with Krull topology is a topological group. □

***Remark* 1.3.13.** *1) If $N/K$ is finite Galois extension , then the Krull topology of $G_{N/K}$ is discrete, since every subgroup of $G_{N/K}$ is open but this is the definition of discrete topology.*
*2) Let $\sigma, \tau \in G_{L/K}$. Then $\tau \in \sigma G_{N/L} \Leftrightarrow \sigma^{-1}\tau \in G_{N/L} \Leftrightarrow (\sigma^{-1} \circ \tau)(x) = x$, for every $x \in L$, that is $\sigma(x) = \tau(x)$, for every $x \in L$, this means that two elements of $G_{N/L}$ "are near" if they coincide on a large field L.*

***Theorem* 1.3.14.** *Let $N/K$ be an infinite Galois extension and $G = G_{N/K}$. Then the topological group $G$ equipped with Krull topology is*

*i) Hausdorff*

*ii) compact*

*iii) totally disconnected*

*Proof.* i) To show that $G$ is Hausdorff, it suffices to show that for any two distinct elements $\sigma, \tau \in G$, there is a neighborhood $U$ of $\sigma$ and neighborhood $V$ of $\tau$ such that $U \cap V = \emptyset$. Let

$$\mathcal{F} = \{L/K : K \leqslant L \leqslant N,\, L/K\, is\, finite\, Galois\}$$

and we have that the set

$$\mathcal{B}_1 = \{G_{N/L} \,|\, L/K\, finite\, normal\, extension,\ L \in \{N : K\}\}$$

forms a basis of open neighborhoods of $1 \in G$. So according to lemma 1.3.8 we have that $\bigcap\limits_{L/K \in \mathcal{F}} G_{N/L} = \{1\}$. Since $\sigma, \tau$ are distinct elements in $G$, then $\sigma \neq \tau \Rightarrow \sigma^{-1}\tau \neq 1$. Thus, there is $U_0 \in \mathcal{B}_1$ such that $\sigma^{-1}\tau \notin U_0 \Rightarrow \tau \notin \sigma U_0$, and then $\sigma U_0 \cap \tau U_0 = \emptyset$ because $U_0 \trianglelefteq G$. We know that $U_0$ is an open neighborhood of 1, then according to proposition 1.2.8 we have that $\sigma U_0$ is an open neighborhood of $\sigma$ and $\tau U_0$ is open neighborhood of $\tau$. Thus, $G$ is Hausdorff.

It suffices to notice that

$$\bigcap_{L/K \in \mathcal{F}} G_{N/L} = \{1\} \Rightarrow N = \bigcup_{L/K \in \mathcal{F}} L$$

Indeed,

$$\begin{tikzcd}
N \arrow[r, leftrightarrow] \arrow[d, dash] & < id_N > \arrow[d, dash] \\
L \arrow[r, leftrightarrow] \arrow[d, dash] & Gal_{N/L} \arrow[d, dash] \\
K \arrow[r, leftrightarrow] & G_{N/K}
\end{tikzcd}$$

We set $G_i = G_{N/L_i}$

$$\begin{tikzcd}
 & N \arrow[d, dash] & \\
 & L_1L_2 \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] \\
 & K &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & <id> \arrow[d, equal] & \\
 & G_1 \cap G_2 \arrow[dl, dash] \arrow[dr, dash] & \\
G_1 \arrow[dr, dash] & & G_2 \arrow[dl, dash] \\
 & G &
\end{tikzcd}$$

But $G_1 \cap G_2 = \{1\}$ and $L_1L_2 \longleftrightarrow G_1 \cap G_2$, so $N = L_1L_2$. In general case $\bigcap\limits_{L/K \in \mathcal{F}} G_{N/L} =< id >$, so then $N = \prod\limits_{L/K \in \mathcal{F}} L$. Clearly, $\bigcup\limits_{L/K \in \mathcal{F}} L \subseteq N = \prod\limits_{L/K \in \mathcal{F}} L$. Let $x \in N = \prod\limits_{L/K \in \mathcal{F}} L$. Then $x = l_1 l_2 \cdots \in L_1 \subseteq \bigcup\limits_{L/K \in \mathcal{F}} L$. Therefore, $N = \bigcup\limits_{L/K \in \mathcal{F}} L$.

ii) We define the map

$$\begin{aligned} h: \quad G \quad &\to \quad \prod_{L/K \in \mathcal{F}} G_{L/K} = P \\ \sigma \quad &\mapsto \quad \prod_{L/K \in \mathcal{F}} \sigma|_L \end{aligned}$$

We notice that $P$ is compact according to Tychonoff's theorem since every $G_{L/K}$ is compact as it is a discrete finite topological group. We will show that $h$ is a homeomorphism from $G$ to $h(G)$ and $h(G)$ is a closed in the product space $\prod\limits_{L/K \in \mathcal{F}} G_{L/K} = P$. Then we will have that $G$ is compact.

Firstly, we will show that $h: G \to h(G)$ is a homeomorphism. We will prove that $h$ is injective. Let $\sigma \in G$ such that $h(\sigma) = 1$. This means that $\sigma|_L = 1$, for every $L$ with $L/K \in \mathcal{F}$. We have that $\sigma(x) = x$, for every $x \in N$, since $N = \bigcup\limits_{L/K \in \mathcal{F}} L$. So $\sigma = 1$ and then $h$ is injective. Also, we will show that $h$ is continuous. It suffices to show that $g_{L/K} \circ h$ is continuous, for every $g_{L/K}$, where $g_{L/K}$ is the projection of $P$ at $G_{L/K}$.

$$\begin{tikzcd}
G \arrow[r, "h"] & P \arrow[r, "g_{L/K}"] & G_{L/K} \\
\sigma \arrow[r, mapsto] & h(\sigma) \arrow[r, mapsto] & \sigma|_L
\end{tikzcd}$$

Indeed, if $g_{L/K} \circ h$ is continuous for every $g_{L/K}$, then for every open set $A$ of $G_{L/K}$ we have that $(h^{-1} \circ (g_{L/K}))^{-1}(A)$ is an open set of $G$. From the definition of product topology we have that

$$\mathcal{Y} = \{g_{L/K}^{-1}(A_L) |\, L/K \in \mathcal{F}\, and\, A_L\, is\, open\, in\, G_{L/K}\}$$

is a subbase of product topology. This means that $h^{-1}(V)$ is open set in $G$, for every $V \in \mathcal{Y}$. Thus, $h$ is continuous. It remains to show that $g_{L/K} \circ h$ is continuous. It suffices to show that for every open set in $G_{L/K}$ we have that $(g_{L/K} \circ h)^{-1}(A)$ is an open set in $G$. It is clear that all singletons $\{\sigma\}$ with $\sigma \in G_{L/K}$ are open, since $G_{L/K}$ is a topological group equipped with discrete topology, and we know that $\mathcal{B} = \{\{\sigma\}, \sigma \in G_{L/K}\}$ forms a basis of discrete topological space $G_{L/K}$. Let $A$ be an open set in $G_{N/L}$, then $A = \bigcup\limits_i B_i$, with $B_i \in \mathcal{B}$. So, $(g_{L/K} \circ h)^{-1}(A) = (g_{L/K} \circ h)^{-1}(\bigcup\limits_i B_i) = \cup(g_{L/K} \circ h)^{-1}(B_i)$. Clearly,

$$\begin{aligned}(g_{L/K} \circ h)^{-1}(\{1\}) &= \{x \in G : (g_{L/K} \circ h)(x) = 1\} \\ &= \{x \in G : x|_L = 1\} \\ &= \{x \in G : x \in G_{N/L}\} = G_{N/L} \in \mathcal{B}_1\end{aligned}$$

Similarly, $(g_{L/K} \circ h)^{-1}(\{\sigma\}) = \sigma G_{N/L} \in \mathcal{B}_\sigma$, so then $(g_{L/K} \circ h)^{-1}(B_i)$ is open for every $B_i \in \mathcal{B}$. Thus $A = \cup_i B_i$ is open as union of open sets in $G$, so then $g_{L/K} \circ h$ is continuous.

Now we will prove that $h(G)$ is closed in the $P$ and the map $h : G \to h(G)$ is an open map. We consider the set

$$M_{L_1/L_2} = \{ \prod_{L/K \in \mathcal{F}} \sigma|_L \ : \ \sigma_{L_1}|_{L_2} = \sigma_{L_2}\}$$

where $K \leqslant L_2 \leqslant L_1 \leqslant N$, $L_i/K \in \mathcal{F}$ and $\sigma_{L_i} = \sigma|_{L_i}$, for $i = 1, 2$. The set $M_{L_1/L_2}$ is closed in $P$, because it is a union of finite number of closed sets. Indeed, if $G_{L_2/K} = \{\sigma_1, \sigma_2, \dots, \sigma_r\}$ and $S_i$ is the set of all extensions of $\sigma_i$ at $L_1$, that is $S_i = \{\tau \in G_{L_1/K} \,|\, \tau_{L_2} = \sigma_i\}$ Then

$$M_{L_1/L_2} = \bigcup_{i=1}^{r} \left( \prod_{\substack{L \neq L_1, L_2 \\ L/K \in \mathcal{F}}} G_{L/K} \times S_i \times \{\sigma_i\} \right)$$

where $\prod\limits_{\substack{L \neq L_1, L_2 \\ L/K \in \mathcal{F}}} G_{L/K} \times S_i \times \{\sigma_i\}$ is closed on $P$.

Now we will prove that

$$h(G) = \bigcap_{L_2 \subseteq L_1} M_{L_1/L_2}, \ \textit{where}\ L_i/K \in \mathcal{F}$$

It is clear that $h(G) \subseteq \bigcap\limits_{L_2 \subseteq L_1} M_{L_1/L_2}$, since if $x = \prod\limits_{L/K \in \mathcal{F}} \sigma|_L \in h(G)$ and let $K \subseteq L_2 \subseteq L_1 \subseteq N$, $L_i/K \in \mathcal{F}$, $\sigma_{L_i} = \sigma|_{L_i}$, then $\sigma_{L_1}|_{L_2} = \sigma_{L_2}$. So $x \in$

$M_{L_1/L_2}$ and $L_1, L_2$ are arbitrary and then $x \in \bigcap\limits_{L_2 \subseteq L_1} M_{L_1/L_2}$. Let now $\prod\limits_{L/K \in \mathcal{F}} \sigma|_L \in \bigcap\limits_{L_2 \subseteq L_1} M_{L_1/L_2}$. We can consider a $K$-automorphism $\sigma : N \mapsto N$ defined by $\sigma(x) = \sigma_L(x)$, if $x \in L$, so that $h(\sigma) = \prod\limits_{L/K \in \mathcal{F}} \sigma|_L$ is well-defined since $\prod\limits_{L/K \in \mathcal{F}} \sigma|_L \in \bigcap\limits_{L_2 \subseteq L_1} M_{L_1/L_2}$. Therefore $h(G) = \bigcap\limits_{L_2 \subseteq L_1} M_{L_1/L_2}$. Hence, $h(G)$ is closed in $P$ as an intersection of closed sets.
Finally $h$ is open into $h(G)$, since if $L/K \in \mathcal{F}$ then

$$h(G_{N/L}) = h(G) \bigcap ( \prod_{\substack{L' \neq K \\ \\ L/K \in \mathcal{F}}} G_{L'/K} \times \{1\})$$

Thus, $h(G_{N/L})$ is open in $h(G)$ and since $G_{N/L}$ is an open neighborhood of 1 then $h$ is open in $h(G)$.
Hence, $h$ is a homeomorphism from $G$ to closed subset $h(G)$ of compact space $P$. Therefore, $h(G)$ is compact and then $G$ is compact.

iii) We only need to show that the connected component $H$ of 1 is the one-point set $H = \{1\}$, since $G$ is a topological group and so $G$ is homogeneous. For every $U \in \mathcal{B}_1$ let $U_H = U \cap H$, then $U_H \neq \emptyset$, since $1 \in U_H$, for every $U \in \mathcal{B}_1$, and $U_H$ is open in $H$. Let

$$V_H := \bigcup_{x \in H \setminus U_H} xU_H$$

We have that $xU_H$ is open, so then $V_H$ is open in $H$. Clearly, $V_H \cap U_H = \emptyset$ (by definition of $V_H$) and $H = U_H \cup V_H$. But $U_H \neq \emptyset$ and $H$ is the connected component of 1, so then $V_H = \emptyset$. That is $U_H = H$, which means that $U \cap H = H$ for every $U \in \mathcal{B}_1$, Then $H \subseteq \bigcap_{U \in \mathcal{B}_1} U = \{1\}$. Therefore, $G$ is totally disconnected. □

It worths to note that it is true the following: A compact topological group is totally disconnected if and only if the intersection of all compact neighborhoods of 1 is equal to $\{1\}$. A proof of this can be found in [9].

## 1.4 The Fundamental Theorem of Infinite Galois Theory

In this section we will state and prove the fundamental theorem for infinite Galois theory. In fact, the main theorem of the infinite Galois theory is a generalization of the fundamental theorem of the finite Galois theory.
For its proof we will require just one more proposition, which we state and prove now.

***Proposition* 1.4.1.** *Let $N/K$ be a Galois extension. The open subgroups of $G = G_{N/K}$ are just the groups $G_{N/L}$ where $L/K$ is a finite subextension of $N/K$. The closed subgroups are precisely the intersections of open subgroups.*

*Proof.* Let $L$ with $K \subseteq L \subseteq N$ such that $L/K$ is a finite extension. So then $L/K$ is finitely generated extension, that is $L = K(\alpha_1, \dots, \alpha_n)$. Let $f(x) = \prod_{i=1}^{n} Irr(\alpha_i, K)$.

$$\begin{tikzcd}
\bar{L} \arrow[d, dash] \\
L = K(\alpha_1, \dots, \alpha_n) \arrow[d, dash] \\
K
\end{tikzcd}$$

where $\bar{L}$ is the separable closure of $K$, so $\bar{L}/K$ is separable and then $L/K$ is also separable. Let $\tilde{L}$ be the splitting field of $f$, which is separable. Thus $\tilde{L}/K$ is Galois. Also $\tilde{L}/K$ is finite, since $L/K$ is. So $K \leq L \leq \tilde{L} \leq N$. We choose a finite normal extension $\tilde{L}/K$ such that $K \leq L \leq \tilde{L} \leq N$. Then $G_{N/\tilde{L}} \leq G_{N/L} \leq G_{N/K} = G$

$$\begin{tikzcd}
N \arrow[r, leftrightarrow] \arrow[d, dash] & < id_N > \arrow[d, dash] \\
\tilde{L} \arrow[r, leftrightarrow] \arrow[d, dash] & Gal_{N/\tilde{L}} \arrow[d, dash] \\
L \arrow[r, leftrightarrow] \arrow[d, dash] & Gal_{N/L} \arrow[d, dash] \\
K \arrow[r, leftrightarrow] & G_{N/K}
\end{tikzcd}$$

So, $G_{N/L} = \bigcup_{\sigma \in G_{N/L}} \sigma G_{N/\tilde{L}}$, and then $G_{N/L}$ is open as a union of open sets. Conversely, let now $H$ be open subgroup of $G$. Then there is a finite Galois extension $\bar{L}/K$ such that $G_{N/\tilde{L}} \leq H \leq G$. We consider the epimorphism

$$\begin{array}{ccc} G & \rightarrow & G/\tilde{N} \\ \sigma & \mapsto & \sigma|_{\tilde{L}} \end{array}$$

which is the restriction of $G$ in $G_{\tilde{L}/K}$ and $G/G_{N/\tilde{L}} \cong G_{\tilde{L}/K}$, so its kernel is $G_{N/\tilde{L}}$. The image of $H$ under this restriction is a subgroup of $G_{\tilde{L}/K}$ and since $\tilde{L}/K$ is finite, then the image of $H$ under this restriction is of the form $G_{\tilde{L}/L}$, for some field $L$ such that $K \leq L \leq \tilde{L}$. Thus,

$$H = \{\sigma \in G : \ \sigma|_L = id_L\} = G_{N/L}$$

Therefore we proved that the open subgroups of $G = G_{N/K}$ are just the groups $G_{N/L}$ where $L/K$ is a finite subextension of $N/K$.

Every open subgroup of $G$ is also closed, since it is the complement of a union of cosets of $G$ which are open, that is

$$G = G_{N/L} \cup ( \bigcup_{\sigma \in G \setminus G_{N/L}} )$$

So the intersections of open groups $G_{N/L}$ are also closed subgroups. Conversely, we assume that $H$ is closed subgroup of $G$. Clearly, $H \subseteq HU$, for every $U \in \mathcal{B}_1$, and then

$$H \subseteq \bigcap_{U \in \mathcal{B}_1} HU$$

On the other hand, let $\sigma \in \bigcap_{U \in \mathcal{B}_1} HU$. We have that $\sigma U \in \mathcal{B}_\sigma$, since $U \in \mathcal{B}_1$. So there is a $U_0 \in \mathcal{B}_1$ such that $\sigma \in HU_0$, that is $\sigma = \sigma_1\sigma_2$, with $\sigma_1 \in H$ and $\sigma_2 \in U_0$, then $\sigma U = \sigma_1\sigma_2 U = \sigma_1 U$ and $\sigma_1 = \sigma_1 \cdot 1 \in \sigma U$. Thus, $\sigma U \cap H \neq \emptyset$, for every $U \in \mathcal{B}_1$. This means that for every open neighborhood $V$ of $\sigma$ we have that $V \cap H \neq \emptyset$, that is $\sigma \in cl(H) = \bar{H}$. But $H$ is closed, so then $\sigma \in \bar{H} = H$. Hence, $H = \bigcap_{U \in \mathcal{B}_1} HU$ and then $H$ is the intersection of the open subgroups $HU$. □

***Comment* 1.4.2.** *In proposition 1.4.1 we assume that $L/K$ is finite but it isn't necessary $L/K$ are Galois like in proposition 1.3.5.*

Now we are ready to state and prove the fundamental theorem for infinite Galois extensions.

***Theorem* 1.4.3** (Krull's Theorem)**.** *Let $N/K$ be a (finite or infinite) Galois extension and let $G = G_{N/K}$. Let $\{N : K\}$ be the lattice of intermediate fields $K \subseteq L \subseteq N$ and let $\{G : 1\}$ be the lattice of closed subgroups of $G$. If $L \in \{N : K\}$ we define*

$$\phi(L) = \{\sigma \in G \,|\, \sigma|L = id_L\} = G_{N/L}$$

*Then $\phi$ is a lattice anti-isomorphism of $\{N : K\}$ and $\{G : 1\}$. Moreover, $L \in \{N : K\}$ is a Galois extension of $K$ if and only if $\phi(L)$ is a normal subgroup of $G$. If this is the case then*

$$G_{L/K} \cong G/\phi(L)$$

*Proof.* By assumption we have that $N/K$ is Galois, so is the $N/L$. Then according to theorem 1.3.14 we have that $\phi(L) = G_{N/L}$ is compact. So $G_{N/L}$ is closed in $G$. This implies that $\phi$ is in fact a map into $\{G : 1\}$. We define

$$\psi : \quad \{G : 1\} \quad \rightarrow \quad \{N : K\}$$

which defined by

$$\psi(H) = \{x \in N : \ Hx = x\}$$

We have already proved that $\psi \circ \phi = id_{\{N:K\}}$. It remains to show that $\phi \circ \psi = id_{\{G:1\}}$. If $L/K$ is finite, then

$$\begin{aligned} \phi(\psi(G_{N/L})) &= \phi(\psi(\phi(L))) = \phi(\psi \circ \phi(L)) \\ &= \phi(id(L)) = \phi(L) = G_{N/L} \end{aligned}$$

If $H \in \{G : 1\}$, then according to proposition 1.4.1 we have that

$$H = \bigcap G_{N/L}$$

where $L$ is running through a collection of $L$ such that $K \subseteq L \subseteq N$ with $L/K$ is finite. Then

$$\begin{aligned} \phi(\psi(H)) &= \phi(\psi(\cap G_{N/L})) = \phi(\cup \psi(G_{N/L})) \\ &= \cap(\phi \circ \psi)(G_{N/L}) = \cap G_{N/L} = H \end{aligned}$$

That is $\phi \circ \psi = id_{\{G:1\}}$.

Let now $L/K$ be Galois extension and $H = \phi(L) = G_{N/L}$. We will show that $H \trianglelefteq G$, that is $\sigma H \sigma^{-1} = H$, for every $\sigma \in G$. Since $L/K$ is Galois then $\sigma(L) = L$, for every $\sigma \in G$ and we know that if $\sigma \in G$ then $\phi(\sigma(L)) = \sigma\phi(L)\sigma^{-1}$. Then:

$$\begin{aligned} \psi(\phi(\sigma(L))) &= \psi(\sigma\phi(L)\sigma^{-1}) \Rightarrow \\ \sigma(L) &= \psi(\sigma H \sigma^{-1}) \end{aligned}$$

In addition, $L = \psi(H)$. But

$$\begin{aligned} & L = \sigma(L) \Rightarrow \psi(\sigma H \sigma^{-1}) = \psi(H) \\ \Rightarrow \ & \sigma H \sigma^{-1} = H, \ for \ every \ \sigma \\ \Rightarrow \ & H \trianglelefteq G \end{aligned}$$

Conversely, suppose $H \trianglelefteq G$ and $\psi(H) = L$. Then $\sigma H \sigma^{-1} = H$, for every $\sigma \in G$, that is $\psi(\sigma H \sigma^{-1}) = \psi(H)$, for every $\sigma \in G$, So $\sigma(L) = L$, for every $\sigma \in G$, and then $L/K$ is normal extension and also $L/K$ is separable since $N/K$ is. Thus, $L/K$ is Galois.

Finally, since every $K$-automorphism of $N$ at $L$ is a $K$-automorphism of $L$, since $L/K$ is Galois.

$$\begin{tikzcd} N \arrow[r, "\tau"] \arrow[d, dash] & N \arrow[d, dash] \\ L \arrow[r] \arrow[d, dash] & L \arrow[d, dash] \\ K \arrow[r, "id"] & K \end{tikzcd}$$

Let $\tau \in G_{N/K}$. Then $\tau|_L : L \to \bar{K}$ such that $\tau_K = id$ and $\tau_L$ is a homomorphism. But $\tau(L) = L$, so then $\tau|_L : L \to L$ with $\tau|_K = id$, which means that $\tau_L$ is a $K$-automorphism. Thus, the restriction of every $K$-automorphism of $N$ in $L$ is a $K$-automorphism of $L$. We consider the map

$$\begin{array}{rccc} rest: & G & \to & G_{L/K} \\ & \sigma & \mapsto & \sigma|_L \end{array}$$

According to the above we have that the map $rest$ is well-defined. Moreover, the $rest$ is a surjection map. If $\tau \in G_{L/K}$ then $\tau : L \to L$ is a $K$-automorphism. Since $N/K$ is Galois then $N$ is the splitting field of $f(X) \in K[X]$ and $K \subseteq L \subseteq N$. So $\tau(f) = f$, since $\tau \in G_{L/K}$. Thus, according to isomorphism extension theorem there exists an isomorphism $\sigma : N \to N$ such that $\sigma|_L = \tau$. The $\sigma$ is an automorphism of $N$ and $\sigma|_K \tau|_K = id$. This means that for every $\tau \in G_{L/K}$ there is $\sigma \in G_{N/K}$ such that $\sigma|_L = \tau$. Consequently, the $rest$ is a surjection map and the kernel of this restriction is

$$Ker(rest) = \{\sigma \in G : \sigma|_L = id\} = G_{N/L} = \phi(L)$$

Therefore, according to first isomorphism theorem of groups we have that

$$G/\phi(L) \cong G_{L/K}$$

□

So we ascertain that it is indeed possible to extend the fundamental theorem of finite Galois extensions to infinite algebraic extensions. This new theorem does indeed extend the old one. If $L/K$ is a finite Galois extension, then the Krull topology on $Gal(L/K)$ is discrete. This occurs because $L/K$ is a finite Galois extension, thus $Gal(L/L) = \{1\}$ is open. Hence every subgroup of $Gal(L/K)$ is closed, so then we obtain our original correspondence between intermediate fields and subgroups.

## 1.5 The use of Infinite Galois Theory

We have defined a fundamental theorem for infinite Galois extensions. An appropriate question to pose is whether this new theorem is at all useful. It would be the case that infinite Galois extensions are rarely encountered, so the study of their Galois groups would be in many ways fruitless. But there are occasions in which we would like to study infinite extensions. We know from elementary field theory that every algebraic extension of either field of characteristic 0 or a finite field is separable. Thus, when our field $F$ is in one of these categories, the field extension $\bar{K}/K$ is separable. Clearly, $\bar{K}/K$ is normal since $\bar{K}$ contains all roots of every polynomial $f(X) \in F[X]$, and hence is Galois. However, there are cases when $\bar{K}/K$ is not a separable extension as we shall see in the following example, so $\bar{K}/K$ cannot be Galois.

***Example* 1.5.1.** *Let $K = \mathbb{F}_2(t)$, where $t$ is transcendental. Then $\sqrt{t} \in \bar{K}$ because $\sqrt{t}$ is a root of the polynomial $X^2 - t$ over $K$. But $X^2 - t = (X - \sqrt{t})^2$ is not separable. Therefore, $\bar{K}/K$ is not a separable extension, so it cannot be Galois.*

***Definition* 1.5.2.** *Let $L/K$ be a field extension. The separable closure of $K$ in $L$ denoted by $K^{sep}$, is*

$$K^{sep} = \{x \in L \mid x \, is \, separable \, over \, K\}$$

*When $K^{sep}$ is written without reference to a particular extension field L of $K$, we will mean the separable closure of $K$ in $\bar{K}$.*

We can show the following proposition

***Proposition* 1.5.3.** *Let $K$ be a field, $\bar{K}$ its algebraic closure, and $K^{sep}$ its separable closure in $\bar{K}$. Then $K^{sep}/K$ is a Galois extension, and $Gal(\bar{K}/K) \cong Gal(K^{sep}/K)$.*

The proof of this extension can be found in [10].

***Definition* 1.5.4.** *The group $G = Gal(K^{sep}/K)$ is the absolute Galois group of the field $K$.*

***Example* 1.5.5.** *If $K = \mathbb{Q}$, then $\mathbb{Q}^{sep} = \bar{\mathbb{Q}}$, then the absolute Galois group of $\mathbb{Q}$ is $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.*

As a rule the extension $K^{sep}/K$ is an infinite extension. However, it does have the advantage of collecting all finite Galois extensions of $K$. So it is reasonable to develop the Galois theory for infinite extensions. This theory would help us to understand the Galois extension $\bar{\mathbb{Q}}/\mathbb{Q}$ and in turn, any understanding of the Galois group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ would be indispensable in number theory.

# Chapter 2

# Profinite groups

The groups which occur as Galois groups of field extensions belong to a class of topological groups, the so-called profinite groups. In this chapter we are going to investigate the profinite groups. These groups are fairly close relatives of finite groups. For the precise description of profinite groups we need the notion of *projective limit* which we will introduce as well.

## 2.1 Category Theory

Eilenberg and Mac Lane invented categories and functors in the 1940s by distilling ideas that had arisen in Algebraic Topology. Categorical notions have proven to be important in purely algebraic contexts. Category theory will force us to think in general case and categories are the context for discussing general properties of systems, such as groups, rings, vector spaces, modules, sets and topological spaces. Imagine a Set Theory whose primitive terms, instead of set and elements, are set and function. Then with the help of category theory we can define bijection, cartesian product, union and intersection. In this section we will study categories because they are an essential ingredient in the definition of functor, which will be useful in next sections.

In Set Theory there are well-known set-theoretic “paradoxes” showing that contradictions arise if we are not careful about how the undefined terms set and element are used. For example, Russell’s Paradox give a contradiction arising from regarding every collection as a set. From this we conclude that some conditions are needed to determine which collections are allowed to be sets. Such conditions are given in Zermelo-Fraenkel axioms for Set Theory.

***Definition* 2.1.1.**

- *A **class** is a collection whose elements are also classes.*
- *Every class (except from zero class) has elements but a class isn’t required to be an element of another class.*
- *If a class $\mathcal{A}$ is an element of some class $\mathcal{B}$ then the class $\mathcal{A}$ is called set.*

*For example,*

- *The class of all groups.*
- *The class of all group homomorphisms.*
- *The class of all sets.*
- *The class of all rings.*

Now we will define the categories.

***Definition* 2.1.2.** *Let $\mathcal{X}$ be a class and $obj(\mathcal{X})$ is the class of objects of $\mathcal{X}$. We assume that $\mathcal{X}$ is equipped with two maps, as follows*

*i) The first map assigns for every ordered pair of objects $(X, Y)$ a set of morphisms $Hom_{\mathcal{X}}(X, Y) = Hom(X, Y)$.*

*ii) The second one assigns for every ordered triple of objects $(X, Y, Z)$ a map*

$$Hom(Y, Z) \times Hom(X, Y) \to Hom(X, Z)$$

*denoted by $(g, f) \mapsto g \circ f$ for every morphisms $f : X \to Y$ and $g : Y \to Z$. The morphism $g \circ f$ is called composition of $g, f$.*

*The class $\mathcal{X}$ equipped with the above two maps will be called* ***category*** *if it also verifies the following axioms*

*1) Composition is associative. If $h : Z \to W$, $g : Y \to Z$, and $f : X \to Y$ are morphisms of $\mathcal{X}$, then $h \circ (g \circ f) = (h \circ g) \circ f$.*

*2) For each object $Y$ in $\mathcal{X}$ there exists an identity morphism $1_Y : Y \to Y$ such that*

$$if\, f : X \to Y\; then\, 1_Y \circ f = f$$

$$if\, g : Y \to Z\; then\, g \circ 1_Y = g$$

***Example* 2.1.3.** *i) $\mathcal{X} = \mathbb{Sets}$ the category of all sets. The objects in this category are sets, $Hom(X, Y) = \{f : X \to Y |\, f\, function\}$ and composition $g \circ f$ is the usual composition of functions.*
*ii) $\mathcal{X} = \mathbb{Groups}$ the category of all groups. The objects in this category are groups, morphisms are homomorphisms, that is $Hom(X, Y) = \{f : X \to Y |\, f\, homomorphism\}$ and composition $g \circ f$ is te usual composition of homomorphisms.*
*iii) $\mathcal{X} = \mathbb{Rings}$ the category of all rings. The objects in this category are rings, morphisms are homomorphisms of rings, that is $Hom(X, Y) = \{f : X \to Y |\, f\, homomorphism\ of\ rings\}$ and composition $g \circ f$ is the usual composition of homomorphisms.*
*iv) $\mathcal{X} = {}_R\mathbb{Mod}$ the category of all left R-modules over a ring R. The objects in this category are left R-modules, morphisms are $R - homomorphisms$, that is $Hom(X, Y) = \{f : X \to Y |\, f\, R - homomorphism\}$ and composition $g \circ f$ is*

*the usual composition.*
*If $R = \mathbb{Z}$, then we write ${}_R\mathbb{Mod} = \mathbb{Ab}$ to remind ourselves that $\mathbb{Z}$-modules are just abelian groups.*
*v) $\mathcal{X} = \mathbb{Mod}_{\mathbb{R}}$ the category of all right $R$-modules over a ring $R$. The objects in this category are right $R$-modules, morphisms are $R - homomorphisms$, that is $Hom(X,Y) = \{f : X \to Y | \, f \, R - homomorphism\}$ and composition $g \circ f$ is the usual composition.*
*The Hom sets in $\mathbb{Mod}_R$ are also denoted by $Hom_R(a,b)$.*
*vi) $\mathcal{X} = \mathbb{Top}$ the category of all topological spaces. The objects in this category are topological spaces, morphisms are all continuous functions, that is $Hom(X,Y) = \{f : X \to Y | \, f \, continuous\}$ and composition $g \circ f$ is the usual composition.*

Now we can define **functors**.

***Definition* 2.1.4.** *If $\mathcal{X}$ and $\mathcal{X}'$ are categories, then a functor $\mathcal{F} : \mathcal{X} \to \mathcal{X}'$ is a function such that*
*i) if $X \in obj(\mathcal{X})$, then $\mathcal{F}(X) = X' \in obj(\mathcal{X}')$*
*ii) if $f : X \to Y$ is a morphism in $\mathcal{X}$, then $\mathcal{F}(f) : \mathcal{F}(X) \to \mathcal{F}(Y)$ is a morphism in $\mathcal{X}'$.*
*iii) for every $X \in obj(\mathcal{X})$, then $\mathcal{F}(1_X) = 1_{\mathcal{F}(X)}$*
*iv) if $f : X \to X'$ and $g : X' \to X''$ are morphisms in $\mathcal{X}$, then*

$$\mathcal{F}(X) \overset{\mathcal{F}(f)}{\to} \mathcal{F}(X') \overset{\mathcal{F}(g)}{\to} \mathcal{F}(X'')$$

*in $\mathcal{X}'$ and*

$$\mathcal{F}(g \circ f) = \mathcal{F}(g) \circ \mathcal{F}(f)$$

***Definition* 2.1.5.** *Let $\mathcal{F}$ and $\mathcal{G}$ be functors from any category $\mathcal{X}$ to the category of sets, $\mathbb{Sets}$. The functor $\mathcal{G}$ will be called subfunctor of $\mathcal{F}$, when*
*i) For every $X \in \mathcal{X}$ the $\mathcal{G}(X)$ is a subset of $\mathcal{F}(X)$.*
*and*
*ii) For every morphism $f$ of $\mathcal{X}$ the $\mathcal{G}(f)$ is the restriction of $\mathcal{F}(f)$ to $\mathbb{Sets}$.*

***Example* 2.1.6.** *1) If $\mathcal{X}$ is a category, then the identity functor $1_{\mathcal{X}} : \mathcal{X} \to \mathcal{X}$ is defined by $1_{\mathcal{X}}(X) = X$ for every $X \in obj(\mathcal{X})$ and $1_{\mathcal{X}}(f) = f$ for every morphism $f$*

*2) Let $\mathcal{X}$ be a category and $A \in obj(\mathcal{X})$, then the Hom functor $T_A : \mathcal{X} \to \mathbb{Sets}$ is defined by $T_A(B) = Hom(A,B)$ for every $B \in obj(\mathcal{X})$*
*and if $f : B \to B'$ in $\mathcal{X}$, then*

$$\begin{array}{rccc} T_A(f) : & Hom(A,B) & \to & Hom(A,B') \\ & h & \mapsto & f \circ h \end{array}$$

*Then the $T_A(f)$ is called induced map and is denoted by*

$$f_* = T_A(f)$$

*We will show that $f_* = T_A(F)$ is a functor. By definition of $T_A(f) = Hom(A, B)$ we have that $Hom(A, B)$ is a set and so $T_A(f) \in obj(\mathbb{Sets})$. We notice that the composition $f \circ h$ makes sense.*

$$\begin{tikzcd} A \arrow[r, "h"] \arrow[rr, bend right, "f\circ h"'] & B \arrow[r, "f"] & B' \end{tikzcd}$$

*Let now that $g: B' \to B''$. Then,*

$$B \xrightarrow{f} B' \xrightarrow{g} B''$$

$$Hom(A, B) \xrightarrow{f_*} Hom(A, B') \xrightarrow{g_*} Hom(A, B'')$$

*and $(g \circ f)_* : Hom(A, B) \to Hom(A, B'')$.*

*Let $h \in Hom(A, B)$, then*

$$(g \circ f)_*(h) = (g \circ f) \circ h$$

*On the other hand,*

$$\begin{array}{ccccc} Hom(A, B) & \xrightarrow{f_*} & Hom(A, B') & \xrightarrow{g_*} & Hom(A, B'') \\ h & \longmapsto & f \circ h & \longmapsto & g \circ (f \circ h) \end{array}$$

*Clearly, $g \circ (f \circ h) = (g \circ f) \circ h$, because $\mathbb{Sets}$ is a category. Thus, $(g \circ f)_* = g_* \circ f_*$. Finally, $1_B : B \to B$, then $(1_B)_* : Hom(A, B) \to Hom(A, B)$, where $h \mapsto 1_B \circ h = h$. That is $(1_B)_*(h) = h$, for every $h \in Hom(A, B)$. So, $(1_B)_* = 1_{Hom(A,B)}$. Therefore, the $T_A(f) = f_*$ is a functor.*

*We can easily prove that $T_A$ preserves products, that is*

$$T_A(\prod_i B_i) \cong \prod_i T_A(B_i)$$

*We usually denote $T_A$ by $Hom(A, \Box)$.*

*3) Let R be a commutative ring and A is a R-module. Then it is clear that $Hom_R(A, B)$ is a R-module as well. We will show that if $f :, B \to B'$, then*

$$\begin{array}{cccc} f_* : & Hom_R(A, B) & \to & Hom_R(A, B') \\ & h & \mapsto & f \circ h \end{array}$$

*is a R-homomorphism. Indeed, $f_*$ is additive map. If $h, h' \in Hom_R(A, B)$, then for each $a \in A$,*

$$\begin{aligned} f_*(h + h')(a) &= (f \circ (h + h'))(a) = f(h(a) + h'(a) \\ &= f(h(a)) + f(h'(a)) = (f_*(h) + f_*(h'))(a) \end{aligned}$$

*Also, $f_*$ preserves scalars. We remind that if $r \in R$ and $h \in Hom_R(A, B)$, then $rh(a) = hr(a)$. Then, $f_*(rh)(a) = (f \circ rh)(a) = f(rh(a)) = f(h(ra))$ and $rf_*(h)(a) = r(f \circ h(a)) = f(r(h(a))) = f(h(ra))$. Thus $f_*(rh) = rf_*(h)$. Hence, $f_*$ is a R-homomorphism. Similarly with $(2)$ of the example, we can prove that $Hom_R(A, \Box)$ is a functor.*

*4) Let $\mathcal{X}$ be a category and $A \in obj(\mathcal{X})$. We define $T : \mathcal{X} \to \mathcal{X}$, with $T(C) = A$, for each $C \in obj(\mathcal{X})$ and $T(f) = 1_A$ for every morphism $f$ in $\mathcal{X}$. Then $T$ is a functor. Indeed, we have that $T(C) \in obj(\mathcal{X})$, for every $C \in obj(\mathcal{X})$. Also, let $1_C : C \to C$, with $C \in obj(\mathcal{X})$, then $T(1_C) = 1_A = 1_{T(C)}$. Finally, let $f : C \to C'$ and $g : C' \to C''$, then $T(g \circ f) = 1_A = 1_A \circ 1_A = T(g) \circ T(f)$. Therefore, $T$ is a functor, which is called constant functor at $A$.*

The second type of functor reverses the direction of arrows.

***Definition* 2.1.7.** *If $\mathcal{X}$ and $\mathcal{X}'$ are categories, then a contravariant functor $e : \mathcal{X} \to \mathcal{X}'$ is a function such that*
*i) if $X \in obj(\mathcal{X})$, then $e(X) = X' \in obj(\mathcal{X}')$*
*ii) if $f : X \to Y$ is a morphism in $\mathcal{X}$, then $e(f) : e(Y) \to e(X)$ is a morphism in $\mathcal{X}'$.*
*iii) for every $X \in obj(\mathcal{X})$, then $e(1_X) = 1_{e(X)}$*
*iv) if $f : X \to Y$ and $g : Y \to Z$ are morphisms in $\mathcal{X}$, then*

$$e(X) \overset{e(f)}{\leftarrow} e(Y) \overset{e(g)}{\leftarrow} e(Z)$$

*in $\mathcal{X}'$ and*

$$e(g \circ f) = e(f) \circ e(g)$$

The functors defined earlier are often called covariant functors.

***Definition* 2.1.8.** *If $\mathcal{F}$ and $\mathcal{G}$ are functors from any category $\mathcal{X}$ to the category $\mathcal{X}'$, then natural transformation $\tau : \mathcal{F} \to \mathcal{G}$ is a function which for every $X \in obj(\mathcal{X})$ there is morphism $\tau_X : \mathcal{F}(X) \to \mathcal{G}(X)$ of $\mathcal{X}'$ such that for every morphism $f : X \to Y$ the following diagram commutes*

$$\begin{tikzcd}
\mathcal{F}(X) \arrow[r, "\tau_X"] \arrow[d, "\mathcal{F}(f)"'] & \mathcal{G}(X) \arrow[d, "\mathcal{G}(f)"] \\
\mathcal{F}(Y) \arrow[r, "\tau_Y"'] & \mathcal{G}(Y)
\end{tikzcd}$$

***Example* 2.1.9.** *1) Let $\mathcal{X}$ be a category and $B \in obj(\mathcal{X})$, then the contravariant functor $T^B : \mathcal{X} \to \mathbb{Sets}$ is defined by $T^B(C) = Hom(C, B)$ for every $C \in obj(\mathcal{X})$ and if $f : C \to C'$ in $\mathcal{X}$, then*

$$\begin{array}{cccc} T^B(f) : & Hom(C', B) & \to & Hom(C, B) \\ & h & \mapsto & h \circ f \end{array}$$

*Then the $T^B(f)$ is called induced map and is denoted by*

$$f_* = T^B(f)$$

*We will show that $f^* = T^B(F)$ is a contravariant functor. By definition of $T^B(f) = Hom(C, B)$ we have that $Hom(C, B)$ is a set and so $T^B(f) \in obj(\mathbb{Sets})$. We notice that the composition $h \circ f$ makes sense.*

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[rr, bend right, "h \circ f"'] & C' \arrow[r, "h"] & B \end{tikzcd}$$

*Let now that $f : C \to C'$ and $g : C' \to C''$ and $(g \circ f)^* : Hom(C'', B) \to Hom(C', B)$, where $(g \circ f)^*(h) = h \circ (g \circ f)$, for $h \in Hom(C'', B)$ On the other hand,*

$$\begin{tikzcd} Hom(C'', B) \arrow[r, "g^*"] & Hom(C', B) \arrow[r, "f^*"] & Hom(C, B) \\ h \arrow[r, mapsto] & h \circ g \arrow[r, mapsto] & (h \circ g) \circ f \end{tikzcd}$$

*Clearly, $h \circ (g \circ f) = (h \circ g) \circ f$, because $\mathbb{Sets}$ is a category. Thus, $(g \circ f)^* = g^* \circ f^*$. Finally, $1_C : C \to C$, then $(1_C)_* : Hom(C, B) \to Hom(C, B)$, where $h \mapsto h \circ 1_C = h$. That is $(1_C)_*(h) = h$, for every $h \in Hom(C, B)$. So, $(1_B)^* = 1_{Hom(A,B)}$. Therefore, the $T^B(f) = f^*$ is a contravariant functor.*

*We can easily prove that $T^B$ converts sums to products, that is*

$$T^B(\bigoplus_i A_i) \cong \prod_i T^B(A_i)$$

*We usually denote $T^B$ by $Hom(\Box, B)$.*

*2) Let R be a commutative ring and B is a R-module. Then it is clear that $Hom_R(A, B)$ is a R-module as well. We will show that if $f :, C \to C'$ is $R-homomorphism$, then*

$$\begin{array}{cccc} f_* : & Hom_R(C', B) & \to & Hom_R(C, B') \\ & h & \mapsto & h \circ f \end{array}$$

*is a $R-homomorphism$ of $R-modules$. Indeed, $f^*$ is an additive map. If $g, h \in Hom_R(C', B)$, then for each $c' \in C'$,*

$$\begin{aligned} f^*(g+h)(a) &= ((g+h) \circ f)(c') = (g+h) \circ f(c') \\ &= g(f(c')) + h(f(c')) = (f^*(g) + f^*(h))(c') \end{aligned}$$

*Also, $f^*$ preserves scalars. We remind that if $r \in R$ and $h \in Hom_R(A, B)$, then $rh(a) = hr(a)$. Then, $f^*(rh)(c) = (rh \circ f)(c) = rh(f(c)) = h(r(f(c))) = h(f(rc)) = rf^*(h)(c)$ Thus $f^*(rh) = rf^*(h)$. Hence, $f^*$ is a R-homomorphism. Similarly with (2) of this example, we can prove that $Hom_R(\Box, B)$ is a contravariant functor.*

## 2.2 Projective and Direct Limit

The notions of projective, respective direct limit, generalize the operations of intersection, respective union, of a family of sets. If $(X_i)_{i\in I}$ is a family of subsets of a topological space $X$ which for any two sets $X_i, X_j$ also contains the set $X_i \cap X_j$, (resp. $X_i \cup X_j$), then the projective (resp. direct) limit of this family simply defined by

$$\varprojlim_{i\in I} X_i = \bigcap_{i\in I} X_i \quad \text{(rexp.} \quad \varinjlim_{i\in I} X_i = \bigcup_{i\in I} X_i)$$

Writing $i \leq j \quad \Leftrightarrow \quad X_j \subseteq X_i$ (resp. $X_i \subseteq X_j$) makes the indexing set $I$ into a *directed set*, this means that $I$ has a partial order $\leq$ such that for any $i, j \in I$, there is a $k \in I$ with $i \leq k$ and $j \leq k$. In the case at hand, such a $k$ is given by $X_k = X_i \cap X_j$ (resp. $X_k = X_i \cup X_j$). For $i \leq j$ we denote the inclusion $X_j \hookrightarrow X_i$ (resp. $X_i \hookrightarrow X_j$) by $\varphi_{ij}$ and then we obtain a system $\{X_i, \varphi_{ij}\}$ of sets and maps. The operations of intersection and union are now generalized by replacing the inclusions $\varphi_{ij}$ with arbitrary maps.

***Definition* 2.2.1.** *Let $I$ be a partial ordered set which is a directed set, too. A projective system over $I$ is a family*

$$\{(X_i, \varphi_{ij}) \,|i, j \in I, \ i \leq j\}$$

*of topological spaces $X_i$ and continuous maps $\varphi_{ij} : X_j \to X_i$ such that*
*i) If $i = j$, then $\varphi_{ii} = Id_{X_i}$*
*ii) If $i \leq j \leq k$, then $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$, that is the following diagram commutes:*

$$\begin{tikzcd}
& X_k \arrow[dl, "\varphi_{jk}"'] \arrow[dr, "\varphi_{ik}"] & \\
X_j \arrow[rr, "\varphi_{ij}"'] & & X_i
\end{tikzcd}$$

***Definition* 2.2.2.** *The projective limit of the projective system $\{(X_i, \varphi_{ij}) \,|i, j \in I, \, i \leq j\}$ is defined to be the following subset of the direct product $\prod_{i\in I} X_i$*

$$\varprojlim_{i\in I} X_i = \{(x_i)_{i\in I} \in \prod_{i\in I} X_i \ |\varphi_{ij}(x_j) = x_i, \textit{for} \ \ i \leq j\}$$

***Comment* 2.2.3.** *If we consider the $X_i$ as subsets of a topological space, then the subsets $X_i$ are topological spaces equipped with the subspace topology. Also, the product $\prod_{i\in I} X_i$ is a topological space equipped with the product topology.*

***Remark* 2.2.4.** *If the topological spaces $X_i$ are Hausdorff, then so is the product. In this case the projective limit $\varprojlim_{i\in I} X_i$ is a closed subspace of $\prod_{i\in I} X_i$.*

*Proof.* Indeed, the $\varprojlim_{i\in I} X_i$ can be written as

$$\varprojlim_{i\in I} X_i = \bigcap_{\substack{i \leq j\\ i,j\in I}} X_{ij}\,,$$

where $X_{ij} = \{(x_k)_{k\in I} \in \prod_{k\in I} X_k \mid \varphi_{ij}(x_j) = x_i\}$. It suffices to show that the sets $X_{ij}$ with $i \leq j$, $i, j \in I$ are close. Writing $p_i : \prod_{i\in I} X_i \to X_i$ for the $i$–th projection, the map $g = p_i$ is continuous. Also, the map $\varphi := \varphi_{ij} \circ p_j$, with $i \leq j$ is continuous as it is a composition of continuous maps.

$$\begin{tikzcd}
\prod_{k\in I} X_k \arrow[r, "p_j"] & X_j \arrow[r, "\varphi_{ij}"] & X_i \\
(x_k)_{k\in I} \arrow[r, mapsto, "p_j"] & x_j \arrow[r, mapsto, "\varphi_{ij}"] & x_i
\end{tikzcd}$$

Then, we can write $X_{ij} = \{x \in \prod_{k\in I} X_k \mid g(x) = \varphi(x)\}$. Since we have that $X_i$ is Hausdorff and the maps $\varphi$, $g$ are continuous, then $X_{ij}$ is a closed subset, according to Proposition 1.1.6. Thus, the $\varprojlim_{i\in I} X_i = \bigcap_{\substack{i \leq j\\ i,j\in I}} X_{ij}$ is also closed as an intersection of closed sets. □

***Theorem* 2.2.5.** *The projective limit $\varprojlim_{i\in I} X_i$ of nonempty compact topological spaces $X_i$ is nonempty and compact.*

*Proof.* Since for every $i \in I$ we have that the spaces $X_i$ are compact, then the product $\prod_{i\in I} X_i$ is also compact, by Tychonoff's theorem. Thus, the $\varprojlim_{i\in I} X_i$ is compact set, since it is a closed subset of the compact space $\prod_{i\in I} X_i$. Furthermore, $\varprojlim_{i\in I} X_i = \bigcap_{\substack{i \leq j\\ i,j\in I}} X_{ij}$ cannot be the empty set if all the $X_i$ are nonempty. In fact, as the product $\prod_{i\in I} X_i$ is compact, if $\varprojlim_{i\in I} X_i = \emptyset$, that is $\bigcap_{\substack{i \leq j\\ i,j\in I}} X_{ij} = \emptyset$, then there is an intersection of finitely many $X_{ij}$ which is empty. But this is impossible, since all indices entering into this finite intersection satisfy that are less than or equal to a natural number n, as the indexing set $I$ is directed, and then $x_n \in X_n$. If we choose

$x_i = \varphi_{in}(x_n)$ for $i \leq n$, and arbitrarily for all other $i$, then the element $(x_i)_{i\in I}$ belongs to this intersection. ↯
Hence, $\varprojlim\limits_{i\in I} X_i = \bigcap\limits_{i\leq j} X_{ij} \neq \emptyset$ □

Let $(G_i, \varphi_{ij})$ be a projective system of topological groups. Then the projective limit

$$G = \varprojlim_{i\in I} G_i$$

is a topological group as well. The multiplication in the projective limit is induced by the componentwise multiplication in the product $\prod\limits_{i\in I} G_i$. The projections

$$p_i : \prod_{i\in I} G_i \to G_i$$

induce a family of continuous homomorphisms

$$\varphi_i : G = \varprojlim_{i\in I} G_i \to G_i$$

such that $\varphi_i = \varphi_{ij} \circ \varphi_j$, for every $i \leq j$. This family has the following universal property.

***Theorem* 2.2.6.** *(Universal Property) If $H$ is a topological group and $(G_i, \varphi_{ij})$ be a projective system of topological groups. Let also*

$$h_i : H \to G_i \; \forall i \in I$$

*a family of continuous homomorphisms such that*

$$h_i = \varphi_{ij} \circ h_j \; for \; i \leq j,$$

*then there exists a unique continuous homomorphism*

$$h : H \to G = \varprojlim_{i\in I} G_i$$

*satisfying $h_i = \varphi_i \circ h$ for all $i \in I$.*

*Proof.* For $i \leq j$

$$\begin{tikzcd}
G = \varprojlim\limits_{i\in I} G_i \arrow[dr, "\varphi_j"] \arrow[ddr, "\varphi_i"'] & & H \arrow[ll, "h"'] \arrow[dl, "h_j"'] \arrow[ddl, "h_i"] \\
& G_j \arrow[d, "\varphi_{ij}"] & \\
& G_i &
\end{tikzcd}$$

Let $\alpha \in H$ and $h_i(\alpha) = g_i$, for every $i \in I$. We define $h(\alpha) = (g_i)_{i\in I}$. We have that $h_i(\alpha) = (\varphi_{ij} \circ \varphi_j \circ h)(\alpha)$. Indeed, $(\varphi_{ij} \circ \varphi_j \circ h)(\alpha) = (\varphi_{ij} \circ \varphi_j)(h(\alpha)) = (\varphi_{ij} \circ \varphi_j)(g_i) = \varphi_{ij}(\varphi_j(g_i)) = \varphi_{ij}(g_j) = g_i = h_i(\alpha)$, which is the desired. Also, this map $h$ is unique. Indeed, if there exist a map $h'$ such that $h_i = \varphi_i \circ h'$, then $\varphi_i \circ h' = h_i = \varphi_i \circ h$ for every $i \in I$, and so $h = h'$.

□

***Definition* 2.2.7.** *A morphism between two projective systems $(G_i, \varphi_{ij})$ and $(G'_i, \varphi'_{ij})$ of topological groups is a family of continuous homomorphisms $f_i : G_i \to G'_i$, $i \in I$, such that the diagram*

$$\begin{tikzcd}
G_j \arrow[r, "f_j"] \arrow[d, "\varphi_{ij}"'] & G'_j \arrow[d, "\varphi'_{ij}"] \\
G_i \arrow[r, "f_i"'] & G'_i
\end{tikzcd}$$

*commutes for $i \leq j$. Such a family $(f_i)_{i\in I}$ defines a mapping*

$$\begin{array}{rccc} f: & \prod_{i\in I} G_i & \to & \prod_{i\in I} G'_i \\ & (g_i)_{i\in I} & \mapsto & (f_i(g_i))_{i\in I} \end{array}$$

*which induces a homomorphism between of the projective limits*

$$f : \varprojlim_{i\in I} G_i \to \varprojlim_{i\in I} G'_i$$

In this way the projective limit, $\varprojlim$, becomes a functor. A particular important property of this functor is its so-called "exactness". The projective limit is not exact in complete generality, but only for compact groups, so we have the next proposition.

***Proposition* 2.2.8.** *Let $\alpha : (G'_i, \varphi'_{ij}) \to (G_i, \varphi_{ij})$ and $\beta : (G_i, \varphi_{ij}) \to (G''_i, \varphi''_{ij})$ be morphisms between projective systems of compact topological groups such that the sequence*

$$G'_i \xrightarrow{\alpha_i} G_i \xrightarrow{\beta_i} G''_i$$

*is exact for every $i \in I$. Then the sequence*

$$\varprojlim_{i\in I} G'_i \xrightarrow{\alpha} \varprojlim_{i\in I} G_i \xrightarrow{\beta} \varprojlim_{i\in I} G''_i$$

*is again an exact sequence of compact topological groups.*

*Proof.* Let $x = (x_i)_{i\in I} \in \varprojlim_{i\in I} G_i$ such that $x \in Ker\beta$, so that $\beta(x) = 1$ which means that $\beta_i(x_i) = 1$, $\forall\, i \in I$. Thus, $x_i \in Ker\beta_i$, $\forall\, i \in I$. But $Im\alpha_i = Ker\beta_i$ for every $i \in I$. So $x_i \in Im\alpha_i$ for all $i \in I$. We consider the sets $Y'_i := \alpha_i^{-1}(x_i) \subset G'_i$, for every $i \in I$. We have that $x_i \in Im\alpha_i \Rightarrow Y_i' \neq \emptyset$, $\forall\, i \in I$. The set $\{x_i\}$ is closed in $G_i$. The maps $\alpha_i$ are continuous for every $i \in I$. So we have that $Y_i'$ is closed in $\varprojlim_{i\in I} G_i'$, and then $Y_i'$ is compact for every $i \in I$. The $(Y_i', \varphi_{ij}|_{Y_i})$ form a projective system of nonempty closed, and hence compact subsets of the $G_i'$. According to theorem 2.2.5, this means that the projective limit $\varprojlim_{i\in I} Y_i' \subseteq \varprojlim_{i\in I} G_i'$ is nonempty. For every $y = (y_i)_{i\in I} \in \varprojlim_{i\in I} Y_i'$ we have that $\alpha(y) = x$. Since $\alpha_i(y_i) = x_i$ then we have that $Im\alpha = Ker\beta$. Hence the sequence is exact. □

## 2.3 Profinite Groups

***Definition* 2.3.1.** *A profinite group is a topological group that can be realized as a projective limit of finite topological groups.*

***Example* 2.3.2.** *Let $p$ a prime number and for every natural number $n$ we define $G_n := \mathbb{Z}/p^n\mathbb{Z}$. If $n \geq m$, then $p^m | p^n$ and so we can define the maps:*

$$\begin{array}{cccc} \varphi_{mn}: & \mathbb{Z}/p^n\mathbb{Z} & \to & \mathbb{Z}/p^m\mathbb{Z} \\ & a \mod p^n & \mapsto & a \mod p^m \end{array}$$

*Then the family $\{(G_n, \varphi_{mn}) | m \leq n\}$ form a projective system and the projective limit is defined as $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$, that is the ring of p-adic integers.*

***Example* 2.3.3.** *The rings $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$, form a projective system with respect to the projections $\varphi_{nm} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, with $n|m$, where the ordering on $\mathbb{N}$ is given by divisibility, that is $n \leq m \Leftrightarrow n|m$, with $n, m \in \mathbb{N}$. Then the projective limit*

$$\hat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$$

*was originally called* ***Prüfer ring****.*

Let $G := \varprojlim_{n\in\mathbb{N}} G_n$, where $G_n$ are finite groups with discrete topology. Then, every group $G_n$ is Hausdorff, so the $G$ is Hausdorff, as well. Also, every group $G_n$ is compact, then so is $G$, according to theorem 2.2.5. In addition, every group $G_n$ is totally disconnected, so the group $G$ is totally disconnected, too. Thus, in other words, we have proved the following theorem:

***Theorem* 2.3.4.** *Every profinite group is a Hausdorff, compact and totally disconnected topological group.*

Thereafter we will see that the vice versa of the above theorem is also true.

The following result gives a criterion for a group to be profinite.

***Theorem.*** *If G is a profinite group and if N varies over the open normal subgroups of G. Then*

$$G \cong \varprojlim_{N} G/N$$

*algebraically and topologically.*

For the proof of above theorem we will need the following lemmata.

***Lemma* 2.3.5.** *Let $X$ be a compact and Hausdorff topological space. Let $x \in X$ and $\{U_q | q \in Q\}$ be the family of all compact open subsets of $X$ which contain x. Then*

$$A := \bigcap_{q \in Q} U_q$$

*is connected.*

*Proof.* We assume that $A = U \cup V,\ U \cap V = \emptyset$, where $U, V$ are non-empty closed sets. Clearly $U, V$ are also open sets. Since $X$ is compact and Hausdorff space, then from theorem 1.1.5 we have that $X$ is a normal space. So, there exist open sets $U', V'$ such that $U \subseteq U',\ V \subseteq V'$ *and* $U' \cap V' = \emptyset$. Thus,

$$\{X \setminus (U' \cup V')\} \cap A = \emptyset \Rightarrow$$

$$\{X \setminus (U' \cup V')\} \cap (\bigcap_{q \in Q} U_q) = \emptyset \Rightarrow$$

$$\bigcap_{q \in Q} (\{X \setminus (U' \cup V')\} \cap U_q) = \emptyset$$

The set $X \setminus (U' \cup V')$ is compact because it is a closed subset of the compact space $X$, so then the sets $\{X \setminus (U' \cup V')\} \cap U_q$ are compact and then they are closed subsets of compact space $X$. We know that in a compact space, for every family of closed sets with empty intersection there exist at least a finite subfamily with empty intersection. Thus, there exist finite subfamily $Q' \subseteq Q$ satisfying

$$\bigcap_{q \in Q'} (\{X \setminus (U' \cup V')\} \cap U_q) = \emptyset \Rightarrow$$

$$[X \setminus (U' \cup V')] \cap (\bigcap_{q \in Q'} U_q) = \emptyset$$

Let $B := \bigcap_{q \in Q'} U_q$. Then $B$ is open, as intersection of finite number of open sets, and compact because it is closed subset of compact space $X$. Let $x \in B$ and $B = B \cap (U' \cup V') = (B \cap U') \cup (B \cap V')$. So, either $x \in B \cap U'$ or $x \in B \cap V'$. Say $x \in B \cap U'$. Since $B, U'$ are compact and open then $B \cap U'$ is open and compact containing $x$. So $A \subseteq B \cap U' \subseteq U'$ and then $A \cap V \subseteq A \cap V' = \emptyset$, because $A \subseteq U'$ and $U' \cap V' = \emptyset$. But $A \cap V = (U \cup V) \cap V = V$. Thus, $V = \emptyset$. But this is impossible since $V \neq \emptyset$. Similarly if $x \in B \cap V'$. Hence $A$ is connected. □

***Lemma* 2.3.6.** *Let $G$ be compact, Hausdorff and totally disconnected topological group. Then every neighborhood of $1 := e$ contains an open normal subgroup. Moreover this subgroup has finite index in $G$.*

*Proof.* Let $\{U_q \,|\, q \in Q\}$ be the family of all compact open sets containing 1. Then from lemma 2.3.5 we have that $1 \in A = \bigcap_{q\in Q} U_q$ is connected. But $G$ is totally disconnected, so then $A = \{1\}$. Let now $U$ be an open neighborhood of 1. We intend to show that there exist $H \trianglelefteq G$ and $H$ is open such that $H \subseteq U$. As $U$ is open then $G \setminus U$ is closed subset of compact space $G$, so then $G \setminus U$ is compact and

$$(G \setminus U) \cap (\bigcap_{q\in Q} U_q) = \emptyset \Rightarrow \bigcap_{q\in Q} (G \setminus U) \cap U_q = \emptyset$$

Since $G$ is compact and $(G \setminus U) \cap U_q$ is a family of closed sets with empty intersection, then there exists a finite subfamily of them with finite intersection. So, there exists a finite subset $Q' \subseteq Q$ such that

$$\bigcap_{q\in Q'} (G \setminus U) \cap U_q = \emptyset \quad \Rightarrow$$

$$(G \setminus U) \cap (\bigcap_{q\in Q'} U_q) = \emptyset \tag{2.1}$$

Let $A' := \bigcap\limits_{q\in Q'} U_q$. Then $A'$ is open as intersection of finite number of open sets, and compact because it is closed subset of compact space $G$. So then $A'$ is a compact open neighborhood of 1. Also, $A' \subseteq U$ according to equation (2.1). Let $F := (G \setminus A') \cap A'^2$. Since $A'$ is compact, so is $A'^2$, hence $F$ is closed. We have $F$ closed, $A'$ compact and $F \cap A' = \emptyset$, so then from lemma 1.2.9 we have that there exists a neighborhood $U'$ of 1 satisfying $F \cap A'U' = \emptyset$. But according to proposition 1.2.8, we have that there exists a symmetric neighborhood $V_1$ of 1 such that $V_1 \subseteq U'$, and then $F \cap A'V_1 = \emptyset$. In addition $A'$ is an open neighborhood of 1, so from proposition 1.2.8 there exists a symmetric neighborhood $V_2$ of 1 such that $V_2 \subseteq A'$. Set $V = V_1 \cap V_2$. Then $V \subseteq U'$, $V \subseteq A'$ $F \cap A'V = \emptyset$ and $V$ is symmetric because $V_1$, $V_2$ are symmetric. Thus, there exists a symmetric open neighborhood $V$ of 1 such that $A'V \cap F = \emptyset$ and $V \subseteq A'$. Since $A'V \subseteq A'A' = A'^2$, it implies that

$$A'V \cap F = \emptyset \Leftrightarrow A'V \cap (G \setminus A') \cap A'^2 = \emptyset \Leftrightarrow$$

$$A'V \cap (G \setminus A') = \emptyset$$

That is

$$A'V \subseteq A'$$

Inductively we can prove that

$$A'V^n \subseteq A' \; \forall n \in \mathbb{N}$$

Hence, $K := \bigcup_{n} V^n \subseteq A'$ is an open subgroup[1] of $G$ contained in $A'$. Since $G$ is compact, then $K$ has only finite number of cosets in $G$, say $G = \bigcup_{i=1}^{r} x_i K$. The subgroup $K$ may not be a normal subgroup, for this reason we set

$$H = \bigcap_{x \in G} xKx^{-1} = \bigcap_{i=1}^{r} x_i K x_i^{-1}$$

The subgroup $H$ is a normal subgroup of $G$, because $gHg^{-1} = g(\bigcap_{i=1}^{r} x_i K x_i^{-1})g^{-1}$ $= \bigcap_{i=1}^{r} g x_i K x_i^{-1} g^{-1} = H$, as $gx_i \in G$. Thus, $H$ is an open normal subgroup of $G$ with finite index, as $G$ is compact, then $H$ has only finite number of cosets in $G$. Also, $H \subseteq K \subseteq A' \subseteq U$. It is clear that $H$ is the desired open normal subgroup of finite index.

□

***Proposition* 2.3.7.** *Let $G$ compact, Hausdorff and totally disconnected topological group. Then the family of all open normal subgroups of $G$ form a basis of open neighborhood of* 1.

*Proof.* Let $\{N_i \leqslant G : N_i \trianglelefteq G \textit{ and } N_i \textit{ is open}\}$. It suffices to show that (i) $N_i$ is an open neighborhood of 1, and (ii) For every open neighborhood $A$ of 1, there exist $N_i$ such that $N_i \subseteq A$. Indeed $N_i$ is an open neighborhood of 1, because $N_i$ is open and $1 \in N_i$. Also, since $G$ is compact, Hausdorff and totally disconnected topological group, then according to lemma 2.3.6 we have that for every open neighborhood $A$ of 1, there exist $N_i \leq G$ where $N_i \trianglelefteq G$ and $N_i$ is open such that $N_i \subseteq A$. Thus the family of all open normal subgroups of $G$ formed a basis of open neighborhood of 1. □

***Remark* 2.3.8.** *Let $G$ compact, Hausdorff and totally disconnected topological group. Then*

$$\bigcap_{i \in I} N_i = \{1\}$$

*where $\{N_i\}$ is the family of all open normal subgroups of $G$.*

*Proof.* From proposition 2.3.7 we have that $\{N_i \leqslant G : N_i \trianglelefteq G \textit{ and } N_i \textit{ is open}\}$ forms a basis of open neighborhood of 1. Let there exist $x \neq 1$. Since $G$ is Hausdorff, then there exist open set $A \subseteq G \setminus \{x\}$ where $1 \in A$ and $x \notin A$. Also, $A$ is an open neighborhood of 1 because $1 \in A$ and $A$ is open. But $\{N_i \leqslant G : N_i \trianglelefteq G \textit{ and } N_i \textit{ is open}\}$ forms a basis of open neighborhood of 1, so then there exist an open normal subgroup, $N_{i_0}$, of $G$ such that $N_{i_0} \subseteq A$. Since $x \notin A$, then $x \notin N_{i_0}$. Thus, $x \notin \bigcap_{i \in I} N_i$. Hence $\bigcap_{i \in I} N_i = \{1\}$. □

[1] We need V be symmetric in order to be K a subgroup.

Now we are able to prove the following theorem.

***Theorem* 2.3.9.** *If $G$ is a profinite group and if $N$ varies over the open normal subgroups of $G$. Then*

$$G \cong \varprojlim_{N} G/N$$

*algebraically and topologically.*

*Proof.* $G$ is a profinite group, so then $G$ is a Hausdorff, compact and totally disconnected topological group. We consider the family

$$\mathcal{N} := \{N_i \leq G \,|\, N_i \trianglelefteq G,\; N_i \, is \, open\}$$

We define $i \leq j \Leftrightarrow N_j \subseteq N_i$. In this way the set $I$ is directed set. Indeed, $N_i \cap N_j \subseteq N_i$ and $N_i \cap N_j \subseteq N_j$ for arbitrary $i, j \in I$. But $N_i \cap N_j \trianglelefteq G$ and $N_i \cap N_j$ is open. So there exist $k \in I$ such that $N_k = N_i \cap N_j$. Then $N_k \subseteq N_i$ and $N_k \subseteq N_j$ which implies that $i \leq k$ and $j \leq k$ for every $i, j \in I$.
We will prove that $\{(G_i = G/N_i, \varphi_{ij}), i, j \in I, i \leq j\}$, where $\varphi_{ij} : G/N_j \to G/N_i$ is the natural map, forms a projective system of finite topological groups. Indeed, if $N_i$ open normal subgroup of $G$, then $gN_i$ is open, since $G$ is topological group. Also, $G = \bigcup\limits_{g \in G} gN_i$, that is an open cover of $G$. But $G$ is compact, so then $G$ contains a finite open subcover, which means that there exist a finite number of cosets that cover $G$. So, $[G : N_i] = |G/N_i| < \infty$ and then $G/N_i$ are topological spaces equipped them with discrete topology.
Thereafter we will define the maps $\varphi_{ij} : G/N_j \to G/N_i$. Let $\pi_i : G \to G/N_i$, where $g \mapsto gN_i$ be the natural projection. Clearly, $Ker\pi_i = N_i$, and so $N_j \subseteq Ker\pi_i$, because $N_j \subseteq N_i$. Thus, $\pi_i$ induces a homomorphism

$$\varphi_{ij} : G/N_j \to G/N_i$$

More precisely, $\varphi_{ij}$ is surjection as $\pi_i$ is surjection. Also $\varphi_{ij}$ are continuous from their construction. In addition, $\varphi_{ii} : G/N_i \to G/N_i$, $gN_i \mapsto gN_i$, that is $\varphi_{ii} = Id_{G/N_i}$ and if $i \leq j \leq k$ then $\varphi_{ij}(\varphi_{jk}(gN_k)) = \varphi_{ij}(gN_i) = \varphi_{ik}(gN_k)$. Hence we have that $\{(G_i = G/N_i, \varphi_{ij}), i, j \in I, i \leq j\}$ is a projective system. Since $G$ is profinite group, which means that $G$ is Hausdorff, compact and totally disconnected topological group, then according to proposition 2.3.7 we have that the family

$$\mathcal{N} := \{N_i \leq G \,|\, N_i \trianglelefteq G,\; N_i \, is \, open\}$$

forms a basis of open neighborhood of $1 \in G$. The family of continuous homomorphisms

$$\pi_i : G \to G/N_i,\; i \in I$$

satisfies that $\varphi_{ij} \circ \pi_j = \pi_i$. Then according to theorem 2.2.6 there exists a unique continuous homomorphism

$$\varphi : G \to \varprojlim_{i \in I} G/N_i \subseteq \prod_{i \in I} G/N_i$$

$$\begin{tikzcd}
G = \varprojlim_{i\in I} G/N_i \arrow[dr, "\varphi_j"] \arrow[ddr, "\varphi_i"'] & & G \arrow[ll, "\varphi"'] \arrow[dl, "\pi_j"'] \arrow[ddl, "\pi_i"] \\
& G/N_j \arrow[d, "\varphi_{ij}"] & \\
& G/N_i &
\end{tikzcd}$$

We will show that $\varphi$ is isomorphism of groups and homeomorphism of topological spaces. Firstly, we will show that $\varphi$ is injective. Indeed, $Ker\varphi = \{g \in G : \varphi(g) = (1)\} = \{g \in G : g \in N_i, \forall\, i \in I\} = \bigcap\limits_{i\in I} N_i = \{1\}$, the last equality arising from remark 2.3.8. Thus $\varphi$ is injective. Then, we will show that $\varphi$ is continuous. It suffices to show that $P_i \circ \varphi$ is continuous for every $N_i \trianglelefteq G$, $N_i = open$ where $P_i$ is the projection.

$$G \xrightarrow{\varphi} \varprojlim_{i\in I} G/N_i \subseteq \prod_{i\in I} G/N_i \xrightarrow{\mathrm{P_i}} G/N_i$$

For the proof of the above statement it suffices to show that for every open set $A$ in $G/N_i$ we have that $(P_i \circ \varphi)^{-1}(A)$ is an open set in $G$. Since the group $G/N_i$ is finite topological group with discrete topology then all her subsets are open. In addition the $\mathcal{B} = \{\{gN_i\}, gN_i \in G/N_i\}$ forms a basis of topological space $G/N_i$. So then it suffices to investigate if the inverse image of the elements of $\mathcal{B}$ is open set in $G$ under $P_i \circ \varphi$. Indeed,

$$\begin{aligned}
(P_i \circ \varphi)^{-1}(\{N_i\}) &= \{x \in G : (P_i \circ \varphi)(x) = N_i\} = \{x \in G : x|_{N_i} = N_i\} \\
&= \{x \in G : x \in N_i\} = N_i = open
\end{aligned}$$

Similarly,

$$\begin{aligned}
(P_i \circ \varphi)^{-1}(\{gN_i\}) &= \{x \in G : (P_i \circ \varphi)(x) = gN_i\} = \{x \in G : x|_{N_i} = gN_i\} \\
&= \{x \in G : g^{-1}x|_{N_i} = N_i\} = \{x \in G : x \in gN_i\} \\
&= gN_i = open
\end{aligned}$$

Thus, for every $\{gN_i\} \in \mathcal{B}$ we have that the $(P_i \circ \varphi)^{-1}(\{gN_i\})$ is open in $G$. If $A$ is open set in $G/N_i$, then $A = \cup\{gN_i\}$, so then $(P_i \circ \varphi)^{-1}(A) = (P_i \circ \varphi)^{-1}(\cup\{gN_i\}) = \cup((P_i \circ \varphi)^{-1}(\{gN_i\}))$ which is open set in $G$ as it is union of open sets. Consequently, the map $P_i \circ \varphi$ is continuous for every $P_i$, and then $\varphi$ is continuous. Moreover, we will show that $\varphi$ is surjective. We have that $G$ is compact, then $G$ is closed since $G$ is Hausdorff. Also, the map $\varphi$ is continuous, so then $\varphi(G)$ is closed, that is $\overline{\varphi(G)} = \varphi(G)$. We will show that $\varphi(G)$ is dense in $\varprojlim_{i\in I} G/N_i$, because then $\overline{\varphi(G)} = \varprojlim_{i\in I} G/N_i$. Thus, $\varphi(G) = \varprojlim_{i\in I} G/N_i$ and then $\varphi$ is surjective. Now we have to show that $\varphi(G)$ is dense in $\varprojlim_{i\in I} G/N_i$. It suffices to show that for every $x \in \varprojlim_{i\in I} G/N_i$ then $x \in \overline{\varphi(G)}$, that is for every open neighborhood of $x$ then $V \cap \varphi(G) \neq \emptyset$. Let $x = (x_i)_{i\in I} \in \varprojlim_{i\in I} G/N_i$ and let $U_S = \prod_{i\notin S} G/N_i \times \prod_{i\in S}\{1_{G/N_i}\}$, where $S \subseteq I$ and $S$ is finite. The $U_S$ are normal subgroups of $\prod_{i\in I} G/N_i$ and then $U_S$ form a basis of open neighborhood of 1 in $\prod_{i\in I} G/N_i$. Also the normal subgroups $U_S \cap \varprojlim_{i\in I} G/N_i$ form a basis of open neighborhood of 1 in $\varprojlim_{i\in I} G/N_i$. We have that $x(U_S \cap \varprojlim_{i\in I} G/N_i)$ is open neighborhood of $x$, since $U_S$ open. In addition, $S$ is a finite directed set. We consider $N_k = \bigcap_{i\in S} N_i$, then $N_k \subseteq N_i \Leftrightarrow i \leq \ \forall i \in S$. Let $y \in G$ such that $\pi_k : G \to G/N_k$, $\pi_k(y) = x_k$. Also we have that $\varphi_{ik}(x_k) = x_i$ for every $i \in S$ with $i \leq k$. For $i \in S$ we have $y \mod N_i = x_i$, because

$$\begin{tikzcd} G \arrow[r, "\pi_k"] & G/N_k \arrow[r, "\varphi_{ik}"] & G/N_i \\ y \arrow[r, mapsto] & x_k \arrow[r, mapsto] & x_i \end{tikzcd}$$

Thus, $\varphi(y) \in x(U_S \cap \varprojlim_{i\in I} G/N_i)$. We have that the $x(U_S \cap \varprojlim_{i\in I} G/N_i)$ form a basis of open neighborhood of $x$ in $\prod_{i\in I} G/N_i$, since the normal subgroups $U_S \cap \varprojlim_{i\in I} G/N_i$ form a basis of open neighborhood of 1 in $\varprojlim_{i\in I} G/N_i$ and $\varprojlim_{i\in I} G/N_i$ is a topological group. Hence, for every open neighborhood $V$ of $x$ there exist a $y \in G$ such that $\varphi(y) \in V$, which means that for every open neighborhood $V$ of $x$ we have that $V \cap \varphi(G) \neq \emptyset$. Consequently, $\varphi(G)$ is dense in $\varprojlim_{i\in I} G/N_i$.

Furthermore, we will show that $\varphi$ is closed map. Let $A$ a closed set in $G$, and then $A$ is compact since $G$ is compact. But $\varphi$ is continuous, so then $\varphi(A)$ is compact subset of $\varprojlim_{i\in I} G/N_i$. We have that $\varprojlim_{i\in I} G/N_i$ is a Hausdorff space. Indeed, firstly, we have that $G/N_i$ is Hausdorff, since if $g_1N_i, g_2N_i \in G/N_i$ with $g_1N_i \neq g_2N_i$. But $\{g_1N_i\}$, $\{g_2N_i\}$ are open neighborhoods of $G/N_i$ with $\{g_1N_i\} \cap \{g_2N_i\} = \emptyset$. So then the product $\prod_{i\in I} G/N_i$ is Hausdorff, and so is $\varprojlim_{i\in I} G/N_i \subseteq \prod_{i\in I} G/N_i$. Thus, from the above we have that $\varphi(A)$ is closed. Consequently, $\varphi$ is closed map. Finally, $\varphi$ is homomorphism from her construction. Hence, the map $\varphi$ is isomorphism of groups and homeomorphism of topological spaces. □

Now we will provide some useful characterizations of profinite groups.

***Theorem* 2.3.10.** *Let $G$ a topological group. Then the following conditions are equivalent:*
*i) $G$ is a profinite group*
*ii) $G$ is a Hausdorff, compact group which has a basis of open neighborhood of $1$ consisting of normal subgroups.*
*iii) $G$ is a Hausdorff, compact and totally disconnected group.*

*Proof.* $(\,i) \Rightarrow iii))$ Let $G$ be a profinite group. Then according to theorem 2.3.4 we have that $G$ is a Hausdorff, compact and totally disconnected group, which is the desired.
$(\,iii) \Rightarrow ii))$ Let $G$ be a Hausdorff, compact and totally disconnected group. Also from proposition 2.3.7 we have that the family of all open normal subgroups of $G$ forms a basis of open neighborhood of $1$.
$(\,ii) \Rightarrow i))$ Let $G$ be a Hausdorff, compact group which has a basis of open neighborhood of $1$ consisting of normal subgroups. We will show that $G$ is a profinite group. It suffices to show that $G$ is the projective limit of finite topological groups. Since $G$ is a Hausdorff, compact group which has a basis of open neighborhood of $1$ consisting of normal subgroups, then according to proof of theorem 2.3.9 we can prove that

$$G \cong \varprojlim_{i \in I} G/N_i$$

algebraically and topologically. Thus $G$ is a profinite group.
Consequently, we proved the theorem. □

Now we will refer some examples of profinite groups.

### *Examples of profinite groups*

***Example* 2.3.11.** *If $K$ is a field and $\bar{K}$ is a separable closure of $K$. Then the absolute Galois group $\bar{K}/K$ is a profinite group.*

*Let $G_K := Gal(\bar{K}/K)$. When $L/K$ run through the finite normal subextensions of $\bar{K}/K$, then $Gal(\bar{K}/L)$ run through the open, normal subgroups of $G_K$, according to definition of Krull topology.*

$$\begin{tikzcd}
\bar{K} \arrow[r, leftrightarrow] \arrow[d, dash] & <id> \arrow[d, dash] \\
L \arrow[r, leftrightarrow] \arrow[d, dash] & Gal(\bar{K}/L) \arrow[d, dash] \\
K \arrow[r, leftrightarrow] & G_K = Gal(\bar{K}/K)
\end{tikzcd}$$

*Thus, according to theorem 2.3.9 we have that*

$$G_K \cong \varprojlim_{L} G_K/Gal(\bar{K}/L)$$

*where $L$ satisfying that $K \leqslant L \leqslant \bar{K}$ and $L/K$ be a finite Galois extension. Since $Gal(\bar{K}/L) \trianglelefteq G_K$ then the extension $L/K$ is a finite Galois extension and so*

$$Gal(L/K) \cong G_K/Gal(\bar{K}/L)$$

*Therefore,*

$$G_K = Gal(\bar{K}/K) \cong \varprojlim_{L} Gal(L/K)$$

*where $L$ satisfying that $K \leqslant L \leqslant \bar{K}$ and $L/K$ be a finite Galois extension.*

*In particular*

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \cong \varprojlim_{K} Gal(K/\mathbb{Q})$$

*where $K$ such that $\mathbb{Q} \leqslant K \leqslant \bar{\mathbb{Q}}$ and $K/\mathbb{Q}$ be a finite Galois extension.*

***Example* 2.3.12.** *We have seen in example 2.3.3 that*

$$\hat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$$

*The **Prüfer ring** $\hat{\mathbb{Z}}$ is important in number theory. If $n = \prod_{p\in\mathbb{P}} p^{v_p}$ where $v_p \geq 0$ with almost all of them are $0$ and $\mathbb{P}$ is the set of all prime numbers. Then from Chinese theorem we have that $\mathbb{Z}/n\mathbb{Z} \cong \prod_{p\in\mathbb{P}} \mathbb{Z}/p^{v_p}\mathbb{Z}$. We know that the projective limit preserves the direct product. Therefore,*

$$\begin{aligned} \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} &\cong \varprojlim_{v_p}(\prod_{p\in\mathbb{P}} \mathbb{Z}/p^{v_p}\mathbb{Z}) \\ &\cong \prod_{p\in\mathbb{P}}(\varprojlim \mathbb{Z}/p^{v_p}\mathbb{Z}) \\ \Rightarrow \hat{\mathbb{Z}} &\cong \prod_{p\in\mathbb{P}} \mathbb{Z}_p \end{aligned}$$

***Remark* 2.3.13.** *If the family $(R_i, \varphi_{ij}), i, j \in I, i \leq j$ is a projective system of rings $R_i$ with identity elements $1_i$ and $\varphi_{ij}$ are ring homomorphisms*

$$\varphi_{ij} : R_j \to R_i, \text{ such that } \varphi_{ij}(1_j) = 1_i$$

*then the projective limit*

$$R := \varprojlim_{i\in I} R_i$$

*is a ring with identity as well.*

*Moreover,*

$$R^* = \varprojlim_{i\in I} R_i^*$$

***Example* 2.3.14.** *We consider that $G_n := (\mathbb{Z}/n\mathbb{Z})^*$, then*

$$\hat{\mathbb{Z}}^* = \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/n\mathbb{Z})^*$$

*Similarly,*

$$\mathbb{Z}_p^* = \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/p^n\mathbb{Z})^*$$

*We know that $(\mathbb{Z}/p^n\mathbb{Z})^* = \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$, since $(\mathbb{Z}/p^n\mathbb{Z})^*$ is abelian group of order $\varphi(p^n) = p^{n-1}(p-1)$. Therefore,*

$$\begin{aligned} \mathbb{Z}_p^* &= \varprojlim_{n\in\mathbb{N}}(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}) \\ &\cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/(p-1)\mathbb{Z} \times \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^{n-1}\mathbb{Z} \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \end{aligned}$$

***Example* 2.3.15.** *Let a finite field $\mathbb{F}_q$ with q elements. We know that for every $n \in \mathbb{N}$ the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is cyclic Galois extension of degree $n$ and cyclic Galois group with generator the Frobenius automorphism*

$$\begin{array}{cccc} \varphi : & \mathbb{F}_{q^n} & \to & \mathbb{F}_{q^n} \\ & x & \mapsto & x^q \end{array}$$

*So then we get isomorphisms*

$$Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$$

*by mapping the Frobenius automorphism to $1 \mod n\mathbb{Z}$. Therefore,*

$$\begin{aligned} Gal(\bar{\mathbb{F}_q}/\mathbb{F}_q) &\cong \varprojlim_{n\in\mathbb{N}} Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \\ &= \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}} \end{aligned}$$

*and this isomorphism $Gal(\bar{\mathbb{F}_q}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$ sends the Frobenius automorphism $\varphi \in Gal(\bar{\mathbb{F}_q}/\mathbb{F}_q)$ to $\mathbb{1} \in \hat{\mathbb{Z}}$ and the subgroup $< \varphi >= \{\varphi^n | n \in \mathbb{Z}\} \cong \mathbb{Z} \leqslant \hat{\mathbb{Z}}$ onto the dense but not closed subgroup $\mathbb{Z}$ of $\hat{\mathbb{Z}}$. In the beginning of the chapter 1 we were able to construct an element $\psi \in Gal(\bar{\mathbb{F}_q}/\mathbb{F}_q)$ such that $\psi \notin < \varphi >$. This isomorphism $Gal(\bar{\mathbb{F}_q}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$ explain us that*

$$(0, \dots, 0, 1_l, 0, \dots, 0) \in \prod_{p\in\mathbb{P}} \mathbb{Z}_p = \hat{\mathbb{Z}}$$

*which does not belongs to $\mathbb{Z}$.*

***Example* 2.3.16.** *We consider the extension $\mathbb{Q}^{ab}/\mathbb{Q}$. According to Kronecker-Weber Theorem, we have that*

$$\mathbb{Q}^{ab} = \mathbb{Q}(\{\zeta_n \mid n \in \mathbb{N}\})$$

*Clearly $\mathbb{Q}(\{\zeta_n \mid n \in \mathbb{N}\})$ is the splitting field of the collection of separable polynomials $\{X^n - 1 \mid n \in \mathbb{N}\}$ over $\mathbb{Q}$. Thus, the extension $\mathbb{Q}^{ab}/\mathbb{Q}$ is Galois. For every $\sigma \in G = Gal(\mathbb{Q}^{ab}/\mathbb{Q})$ if the value of $\sigma(\zeta_n)$ is known for every $n \in \mathbb{N}$, then $\sigma$ will be completely determined on all of $\mathbb{Q}^{ab}$. For fixed $n \in \mathbb{N}$, we know from classical Galois theory that*

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

*where $(\mathbb{Z}/n\mathbb{Z})^*$ is the multiplicative group of units of $\mathbb{Z}/n\mathbb{Z}$. So we have that*

$$\begin{aligned} G &= Gal(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \varprojlim Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ &\cong \varprojlim (\mathbb{Z}/n\mathbb{Z})^* = \hat{\mathbb{Z}}^* \end{aligned}$$

## 2.4 Limits and Functors

So far we have referred in projective systems of topological spaces. We can speak of projective systems of groups, modules or commutative rings as well.

The next result says that the functor $Hom_R(A, \square)$ preserves projective limits.

***Proposition* 2.4.1.** *Let $M_i$ be left $R$-modules and $\{(M_i, \varphi_{ij}), i, j \in I, i \leq j\}$ be a projective system. Then*

$$Hom_R(A, \varprojlim_{i \in I} M_i) \cong \varprojlim_{i \in I} Hom_R(A, M_i)$$

*for every left $R$-module $A$.*

*Proof.* Firstly we will show that the $\{(Hom_R(A, M_i), (\varphi_{ij})_*), i, j \in I, i \leq j\}$ forms a projective system, where $(\varphi_{ij})_*$ is the induced map, that is

$$\begin{array}{rccc} (\varphi_{ij})_* : & Hom_R(A, M_j) & \to & Hom_R(A, M_i) \\ & h & \mapsto & \varphi_{ij} \circ h \end{array}$$

This is valid since the functor $Hom_R(A, \square)$ is covariant. We know that $Hom_R(A, M_i)$ is a left $R$-module, because $M_i$ are left $R$-modules. Also the maps $(\varphi_{ij})_*$ are homomorphisms. Moreover, $(\varphi_{ii})_*(h) = \varphi_{ii} \circ h = Id_{M_i} \circ h = h$, that is $(\varphi_{ii})_* = Id_{Hom_R(A, M_i)}$. For $i \leq j \leq k$

$$\begin{tikzcd} Hom_R(A, M_j) \arrow[rr, "(\varphi_{ij})_*"] & & Hom_R(A, M_i) \\ & Hom_R(A, M_k) \arrow[ul, "(\varphi_{jk})_*"] \arrow[ur, "(\varphi_{ik})_*"'] & \end{tikzcd}$$

Then $(\varphi_{ij})_* \circ (\varphi_{jk})_*(h) = (\varphi_{ij})_*(\varphi_{jk} \circ h) = \varphi_{ij} \circ \varphi_{jk} \circ h = \varphi_{ik} \circ h = (\varphi_{ik})_*(h)$, since $(M_i, \varphi_{ij})$ is a projective system. Thus the $\{(Hom_R(A, M_i), (\varphi_{ij})_*), i, j \in I, i \leq j\}$ is a projective system, so that $\varprojlim_{i\in I} Hom_R(A, M_i)$ makes sense.

This statement follows from the fact that the projective limit has the universal mapping property. Indeed we consider the diagram,

$$\begin{tikzcd}
\varprojlim_{i\in I} Hom_R(A, M_i) \arrow[dr, "\beta_i"] \arrow[ddr, "\beta_j"'] & & Hom_R(A, \varprojlim_{i\in I} M_i) \arrow[ll, dashed, "\theta"'] \arrow[dl, "(\varphi_i)_*"'] \arrow[ddl, "(\varphi_j)_*"] \\
& Hom_R(A, M_i) & \\
& Hom_R(A, M_j) \arrow[u, "(\varphi_{ij})_*"'] &
\end{tikzcd}$$

where $\beta_i : \varprojlim_{i\in I} Hom_R(A, M_i) \to Hom_R(A, M_i)$ such that $\beta_i = (\varphi_{ij})_* \circ \beta_j$, for every $i \leq j$.

We intend to show that there exist such a map $\theta$ which is an isomorphism. We know that $Hom_R(A, \varprojlim_{i\in I} M_i)$ is a module. Also, $(M_i, \varphi_{ij})$ is a projective system, so then there exists a family of homomorphisms $\varphi_i : \varprojlim_{i\in I} M_i \to M_i$ such that $\varphi_i = \varphi_{ij} \circ \varphi_j$, for each $i \leq j$. Then the induced homomorphism is the following

$$\begin{array}{cccc} (\varphi_i)_* : & Hom_R(A, \varprojlim_{i\in I} M_i) & \to & Hom_R(A, M_i) \\ & h & \mapsto & \varphi_i \circ h \end{array}$$

such that $(\varphi_{ij})_* \circ (\varphi_j)_* = (\varphi_i)_*$. So, according to universal property of projective limit (Theorem 2.2.6) there exists a unique homomorphism

$$\theta : Hom_R(A, \varprojlim_{i\in I} M_i) \to Hom_R(A, M_i)$$

such that $(\varphi_i)_* = \beta_i \circ \theta$.

Thereafter, we will show that $\theta$ is injective. Suppose that $f : A \to \varprojlim_{i\in I} M_i$ and $\theta(f) = 0$. Then $\beta_i \circ \theta(f) = 0 \Rightarrow (\varphi_i)_*(f) = 0 \Rightarrow \varphi_i \circ f = 0$, for every $i$. So we have the following diagram

$$\begin{tikzcd}
\varprojlim_{i\in I} M_i \arrow[dr, "\varphi_i"] \arrow[ddr, "\varphi_j"'] & & A \arrow[ll, "f"'] \arrow[dl, "h_i:=\varphi_i\circ f"'] \arrow[ddl, "h_j:=\varphi_j\circ f"] \\
& M_i & \\
& M_j \arrow[u, "\varphi_{ij}"'] &
\end{tikzcd}$$

The above diagram commutes, since $\varphi_i \circ f = 0$ for every $i$, then $\varphi_{ij} \circ h_j = \varphi_{ij} \circ \varphi_j \circ f = 0 = \varphi_i \circ f = h_i$. Thus, according to universal property of projective limits (Theorem 2.2.6) the map $f$ is unique. But if we take the zero map in place of $f$, then the above diagram commutes as well. So the uniqueness of such a map gives that $f = 0$, that is $\theta$ is injective.
It remains to show that $\theta$ is a surjective map. Let $g \in \varprojlim_{i\in I} Hom_R(A, M_i)$. For every $i$ there is a map $\beta_i(g) \in Hom_R(A, M_i)$ with $\varphi_{ij} \circ \beta_j(g) = \beta_i(g)$ for $i \leq j$. Indeed, we know that $\beta_i = (\varphi_{ij})_* \circ \beta_j$, $\forall i \leq j$ and $\beta_i(g) \in Hom_R(A, M_i)$, so then $\varphi_{ij} \circ \beta_j(g) = (\varphi_{ij})_* \circ \beta_j(g) = \beta_i(g)$.

$$\begin{tikzcd}
\varprojlim_{i\in I} M_i \arrow[dr, "\varphi_i"] \arrow[ddr, "\varphi_j"'] & & A \arrow[ll, dashed, "g'"'] \arrow[dl, "\beta_i(g)"'] \arrow[ddl, "\beta_j(g)"] \\
& M_i & \\
& M_j \arrow[u, "\varphi_{ij}"'] &
\end{tikzcd}$$

Therefore, according to universal mapping property of projective limit there exists a unique homomorphism

$$g' : A \to \varprojlim_{i\in I} M_i$$

satisfying that $\varphi \circ g' = \beta_i(g)$ for every $i$. So then $(\varphi_i)_*(g') = \beta_i(g), \forall i \Rightarrow \beta_i(\theta(g')) = \beta_i(g), \forall i \Rightarrow \theta(g') = g$. Thus, $\theta$ is surjective.
Hence, the map $\theta$ is isomorphism, that is

$$Hom_R(A, \varprojlim_{i\in I} M_i) \cong \varprojlim_{i\in I} Hom_R(A, M_i)$$

□

We now consider the dual construction of projective limit, which is the direct limit. Firstly, we will define the direct system, then we will define the direct limit and finally we will investigate the dual of the proposition 2.4.1.

***Definition* 2.4.2.** *Let $I$ be a partially ordered set which is also directed. A direct system over $I$ is a family*

$$\{(M_i, \varphi_{ij})\,|i, j \in I,\, i \leq j\}$$

*of left $R$-modules $M_i$ and homomorphisms*

$$\varphi_{ij} : M_i \to M_j,\ i \leq j$$

*satisfying that:*
*1) If $i = j$, then $\varphi_{ii} = Id_{M_i}, \forall i$*
*2) If $i \leq j \leq k$ then $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$*

$$\begin{tikzcd}
M_i \arrow[rr, "\varphi_{ik}"] \arrow[dr, "\varphi_{ij}"'] & & M_k \\
& M_j \arrow[ur, "\varphi_{jk}"'] &
\end{tikzcd}$$

We can also speak for direct system of groups or topological spaces.

***Definition* 2.4.3.** *Let $I$ be a partially ordered set which is also directed. Let also $(M_i, \varphi_{ij})$ a direct system of left $R$-modules over $I$. The direct limit $\varinjlim_{i\in I} M_i$ is a left $R$-module and a family of $R$-homomorphisms $\varphi_i : M_i \to \varinjlim_{i\in I}$, $i \in I$, such that:*
*i) $\varphi_i = \varphi_j \circ \varphi_{ij}$, $i \leq j$*
*ii) For every module $X$ having maps $f_i : M_i \to X$ such that $f_i = f_j \circ \varphi_{ij}$ for every $i \leq j$, then there exists a unique homomorphism*

$$\theta : \varinjlim_{i\in I} M_i \to X$$

*such that the following diagram commutes:*

$$\begin{tikzcd}
\varinjlim\limits_{i\in I} M_i \arrow[rr, "\theta"] & & X \\
& M_i \arrow[ul, "\varphi_i"] \arrow[ur, "f_i"'] \arrow[d, "\varphi_{ij}"] & \\
& M_j \arrow[uul, "\varphi_j"] \arrow[uur, "f_j"'] &
\end{tikzcd}$$

*that is* $f_i = \theta \circ \varphi_i$.

From the definition of the direct limit we understand that it has the universal mapping property. So the direct limit of a direct system is unique (up to isomorphism) if it exists. We can prove that the direct limit of any direct system $(M_i, \varphi_{ij})$ of left $R$-modules over a partially ordered index set $I$, which is also directed, exists.

***Proposition* 2.4.4.** *Let* $(A_i, \varphi_{ij})$ *be a direct system of abelian groups, where* $I$ *is directed and* $A = \varinjlim_{i\in I} A_i$. *Let also the family of* $\mathbb{Z}$*-homomorphisms* $\varphi_i : A_i \to A$. *Then*

$$A = \bigcup_{i\in I} \varphi_i(A_i)$$

*Proof.* $(A_i, \varphi_{ij})$ is a direct system, so $\varphi_{ij} : A_i \to A_j$ such that $\varphi_{ik} = \varphi_{jk} \circ \varphi_{ij}$ and $\varphi_i : A_i \to A$ such that $\varphi_j \circ \varphi_{ij} = \varphi_i$. It is clear that $\bigcup_{i\in I} \varphi_i(A_i) \subseteq A$. Let now $a \in A$. From construction of direct limit there exists a $i \in I$ such that $a = \varphi_i(x)$ with $x \in A_i$. This means that $a \in \bigcup_{i\in I} \varphi_i(A_i)$. □

***Proposition* 2.4.5.** *If* $(M_i, \varphi_{ij})$ *be a direct system of left R-modules, then:*

$$Hom_R(\varinjlim_{i\in I} M_i, B) \cong \varprojlim_{i\in I} Hom_R(M_i, B)$$

*for every left R-module B.*

*Proof.* Firstly, we will show that $\{(Hom_R(M_i, B), (\varphi_{ij})_*), \, i, j \in I, \, i \le j\}$ form a projective system. We know that the functor $Hom_R(\Box, B)$ is a contravariant functor. So the induced map is

$$\begin{array}{rccc} (\varphi_{ij})_* : & Hom_R(M_j, B) & \to & Hom_R(M_i, B) \\ & h & \mapsto & h \circ \varphi_{ij} \end{array}$$

We know that the $Hom_R(M_i, B)$ are left $R$-modules, since $M_i$ are left $R$-modules. Also, $(\varphi_{ij})_*$ are homomorphisms, as $\varphi_{ij}$, $h$ are homomorphisms. In addition, $(\varphi_{ii})_*(h)$ $= h \circ \varphi_{ii} = h \circ Id_{M_i} = h$, that is $(\varphi_{ii})_* = Id_{M_i}$. For $i \le j \le k$

$$\begin{tikzcd}
Hom_R(M_j, B) \arrow[rr, "(\varphi_{ij})_*"] & & Hom_R(M_i, B) \\
& Hom_R(M_k, B) \arrow[ul, "(\varphi_{jk})_*"] \arrow[ur, "(\varphi_{ik})_*"'] &
\end{tikzcd}$$

$(\varphi_{ij})_* \circ (\varphi_{jk})_*(h) = (\varphi_{ij})_*(h \circ \varphi_{jk}) = h \circ \varphi_{jk} \circ \varphi_{ij} = h \circ \varphi_{ik} = (\varphi_{ik})_*(h)$.
Thus, the $\{(Hom_R(M_i, B), (\varphi_{ij})_*), \, i, j \in I, \, i \le j\}$ is a projective system, so that $\varprojlim_{i\in I} Hom_R(M_i, B)$ makes sense.

This statement follows from the fact that the direct limit has the universal mapping property. Indeed, we consider the diagram,

$$\begin{tikzcd}
\varprojlim_{i\in I} Hom_R(M_i,B) \arrow[dr, "\beta_i"] \arrow[ddr, "\beta_j"'] & & Hom_R(\varinjlim_{i\in I} M_i,B) \arrow[ll, dashed, "\theta"'] \arrow[dl, "(\varphi_i)_*"'] \arrow[ddl, "(\varphi_j)_*"] \\
 & Hom_R(M_i,B) & \\
 & Hom_R(M_j,B) \arrow[u, "(\varphi_{ij})_*"'] &
\end{tikzcd}$$

where $\beta_i : \varprojlim_{i\in I} Hom_R(M_i,B) \to Hom_R(M_i,B)$ such that $\beta_i = (\varphi_{ij})_* \circ \beta_j$, for every $i \leq j$.

We intend to show that there exists such a map $\theta$ which is an isomorphism. We know that $Hom_R(\varinjlim_{i\in I} M_i,B)$ is an $R$-module. We have that $(M_i,\varphi_{ij})$ is a direct system, so then there exists a family of homomorphisms $\varphi_i : M_i \to \varinjlim_{i\in I} M_i$ such that $\varphi_i = \varphi_j \circ \varphi_{ij}$ with $i \leq j$. Then the induced homomorphism is the following

$$\begin{array}{cccc}
(\varphi_i)_* : & Hom_R(\varinjlim_{i\in I} M_i,B) & \to & Hom_R(M_i,B) \\
 & h & \mapsto & h\circ\varphi_i
\end{array}$$

such that $(\varphi_{ij})_* \circ (\varphi_j)_* = (\varphi_i)_*$. So, according to universal property of direct limit there exists a unique homomorphism

$$\theta : Hom_R\left(\varinjlim_{i\in I} M_i, B\right) \to \varprojlim_{i\in I} Hom_R(M_i,B)$$

such that $(\varphi_i)_* = \beta_i \circ \theta$.

Thereafter, we will show that the map $\theta$ is injective. Let $f \in Hom_R(\varinjlim_{i\in I} M_i,B)$ such that $\theta(f)=0$. Then $\beta_i\circ\theta(f) = 0 \Rightarrow (\varphi_i)_*(f) = 0 \Rightarrow f\circ\varphi_i = 0$, $\forall i$. So we have the following diagram

$$\begin{tikzcd}
\varinjlim_{i\in I} M_i \arrow[rr, "f"] & & B \\
 & M_i \arrow[ul, "\varphi_i"'] \arrow[ur, "h_i:=f\circ\varphi_i"'] \arrow[d, "\varphi_{ij}"] & \\
 & M_j \arrow[uul, "\varphi_j"] \arrow[uur, "h_j:=f\circ\varphi_j"'] &
\end{tikzcd}$$

Since $f \circ \varphi_i = 0$, $\forall i$ then $h_j \circ \varphi_{ij} = f \circ \varphi_j \circ \varphi_{ij} = 0 = f \circ \varphi_i = h_i$. So then the diagram commutes and $f$ is unique according to universal mapping property of direct limit. But if we take the zero map in place of $f$, then the above diagram commutes as well. So the uniqueness of such a map gives that $f = 0$, that is $\theta$ is injective.

It remains to show that $\theta$ is a surjective map. Let $g \in \varprojlim_{i\in I} Hom_R(M_i, B)$. For every $i$ there exists $\beta_i(g) \in Hom_R(M_i, B)$ with $\beta_j(g) \circ \varphi_{ij} = \beta_i(g)$, for $i \leq j$. Indeed, we know that $\beta_i = (\varphi_{ij})_* \circ \beta_j$ for every $i \leq j$. We have that $\beta_i(g) \in Hom_R(M_i, B)$ and $\beta_j(g)\varphi_{ij} = (\varphi_{ij})_* \circ \beta_j(g) = \beta_i(g)$

$$\begin{tikzcd}
\varinjlim_{i\in I} M_i \arrow[rr, dashed, "g'"] & & B \\
 & M_i \arrow[ul, "\varphi_i"'] \arrow[ur, "\beta_i(g)"'] \arrow[d, "\varphi_{ij}"] & \\
 & M_j \arrow[uul, "\varphi_j"] \arrow[uur, "\beta_j(g)"'] &
\end{tikzcd}$$

Thus, according to universal mapping property of $\varinjlim_{i\in I} M_i$ there is a unique homomorphism $g' : \varinjlim_{i\in I} M_i \to B$ such that $g' \circ \varphi_i = \beta_i(g)$ for every $i$. So then $g' \circ \varphi_i = \beta_i(g)$, $\forall i \Rightarrow (\varphi_i)_*(g') = \beta_i(g)$, $\forall i \Rightarrow \beta_i(\theta(g')) = \beta_i(g)$, $\forall i \Rightarrow \theta(g') = g$. Hence, $\theta$ is surjective.

Therefore, $\theta$ is isomorphism. That is

$$Hom_R\left(\varinjlim_{i\in I} M_i, B\right) \cong \varprojlim_{i\in I} Hom_R(M_i, B)$$

□

Now we will prove that the functor $A \otimes \square$ preserves direct limits. For this proof we will need another proposition which we will prove first.

***Proposition* 2.4.6.** *Let a commutative diagram with exact rows of $R$-modules. We assume also that the map $f$ is surjective and the map $g$ is isomorphism*

$$\begin{tikzcd} A' \arrow[r, "i"] \arrow[d, "f"'] & A \arrow[r, "p"] \arrow[d, "g"] & A'' \arrow[r] \arrow[d, "h"] & 0 \\ B' \arrow[r, "j"] & B \arrow[r, "q"] & B'' \arrow[r] & 0 \end{tikzcd}$$

*then there exists a unique isomorphism $h : A'' \to B''$ such that $q \circ g = h \circ p$.*

*Proof.* If $a'' \in A''$, then there is $a \in A$ with $p(a) = a''$, since $p$ is surjective. We define $h(a'') = q \circ g(a)$. Firstly, we will show that $h$ is well-defined. If $u \in A$ such that $p(u) = a''$, then $h(p(u)) = h(a'') \Rightarrow qg(u) = h(a'') \Rightarrow q \circ \circ g(u) = q \circ g(a)$. Then $p(a) = p(u) \overset{\text{p is homomorphism}}{\Longrightarrow} p(a{-}u) = 0 \Rightarrow a{-}u \in Kerp$. But $Kerp = Imi$, since rows are exact, so then $a{-}u \in Imi$, that is $a{-}u = i(a')$, with $a' \in A'$. Thus, $q \circ g(a-u) = q \circ g \circ i(a') = q \circ j \circ f(a') = q(j(f(a'))) = 0$, because the diagram commutes then we have that $g \circ i = j \circ f$ and $j(f(a')) \in Imj = Kerq$. Hence, $q{\circ}g(a{-}u) = 0 \Rightarrow q{\circ}g(a){-}q{\circ}g(u) = 0 \Rightarrow h(p(a)) = h(p(u))$. So then $h$ is a well-defined map. From the definition of $h$ we have that the second square commutes, that is $h \circ p = q \circ g$. Thereafter, we will show that $h$ is unique. We assume that there exist $h' : A'' \to B''$ satisfying that $h' {\circ} p = q {\circ} g$. If $a'' \in A''$ we choose $a \in A$ with $p(a) = a''$. Then $h'(a'') = h'(p(a)) = q(g(a)) = h(a'')$. Thus, $h$ is unique. In addition, we will show that $h$ is injective. Let $a'' \in A''$ such that $h(a'') = 0$, with $a'' = p(a)$, since $p$ is surjective. Then, $h(a'') = 0 \Rightarrow q(g(a)) = 0 \Rightarrow g(a) \in Kerq = Imj$. So there exists $b' \in B'$ such that j(b')=g(a). Because of $f$ is surjective, there is $a' \in A'$ such that $f(a') = b'$. Thus $j(f(a')) = g(a) \Rightarrow g(i(a')) = g(a)$, but $g$ is injective, so then $i(a') = a \Rightarrow p \circ i(a') = p(a) \Rightarrow p \circ i(a') = a''$. But $p \circ i(a') = 0$, since $i(a') \in Kerp = Imi$, so then $a'' = 0$. Hence, $h$ is injective. Moreover, we will prove that $h$ is surjective. Let $b'' \in B''$. There is a $b \in B$ such that $q(b) = b''$, because $q$ is surjective. Also, there exist $a \in A$ such that $g(a) = b$. So, $q \circ g(a) = b'' \Rightarrow h(p(a)) = b''$. Consequently, $h$ is surjective. Hence, $h$ is isomorphism. □

***Theorem* 2.4.7.** *If $A$ is a right $R$-module and $\{(B_i, \varphi_{ij}), i, j \in I,\ i \leq j\}$ is a direct system of left $R$-modules, then*

$$A \otimes_R \varinjlim_{i \in I} B_i \cong \varinjlim_{i \in I} (A \otimes_R B_i)$$

*Proof.* Firstly we will prove that $\{(A \otimes_R B_i, 1 \otimes \varphi_{ij}), i, j \in I,\ i \leq j\}$ forms a direct system. We know that $A \otimes_R B_i$ is $\mathbb{Z}$-module and $\varphi_{ij}$, 1 are homomorphisms. So then there exists a unique homomorphism of $\mathbb{Z}$-modules

$$1 \otimes \varphi_{ij} : A \otimes_R B_i \to A \otimes_R B_j$$

such that $(1 \otimes \varphi_{ij})(\alpha \otimes b_i) = \alpha \otimes b_j$ and we extend it linearly. Also if $i = j$ then $(1 \otimes \varphi_{ii})(\alpha, b_i) = \alpha \otimes b_i$, that is $1 \otimes \varphi_{ii} = Id_{A \otimes_R B_i}$. For $i \leq j \leq k$ then $(1 \otimes \varphi_{jk}) \circ (1 \otimes \varphi_{ij}) = 1 \otimes (\varphi_{jk} \circ \varphi_{ij}) = 1 \otimes \varphi_{ik}$. Therefore, $\{(A \otimes_R B_i, 1 \otimes \varphi_{ij}),\, i, j \in I,\ i \leq j\}$ is a direct system, and then $(\varinjlim_{i \in I} A \otimes_R B_i)$ makes sense. For the proof of this statement we will construct $\varinjlim_{i \in I} B_i$ as the cokernel[2] of a special map. For every pair $i, j \in I$ with $i \leq j$, where $I$ is a partially ordered set which is also directed, we define a module $B_{ij}$ satisfying that the following map

$$\begin{array}{cccc} \lambda : & B_i & \to & B_{ij} \\ & b_i & \mapsto & b_{ij} \end{array}$$

is a module isomorphism. Let $\lambda_i$ be the injection of $B_i$ into the sum $\oplus_i B_i$ for each $i \in I$. We define

$$D = (\oplus_i B_i)/S$$

where $S$ be the submodule of $\oplus_i B_i$ generated by all elements $\lambda_j \circ \varphi_{ij}(b_i) - \lambda_i(b_i)$ with $b_i \in B_i$, $i \leq j$. Now we define

$$\begin{array}{cccc} \alpha_i : & B_i & \to & D \\ & b_i & \mapsto & \lambda_i(b_i) + S \end{array}$$

Then $\alpha_j \circ \varphi_{ij}(b_i) = \lambda_j \circ \varphi_{ij}(b_i) + S$ for $i \leq j$ and $\alpha_i(b_i) = \lambda_i(b_i) + S$. But it is plain that $\lambda_j \circ \varphi_{ij}(b_i) - \lambda_i(b_i) \in S \Leftrightarrow \lambda_j \circ \varphi_{ij}(b_i) + S = \lambda_i(b_i) + S \Leftrightarrow \alpha_j \circ \varphi_{ij}(b_i) = \alpha_i(b_i)$. That is $\alpha_j \circ \varphi_{ij} = \alpha_i$ for every $i \leq j$. Let $X$ be a module and $f_i : B_i \to X$ such that $f_j \circ \varphi_{ij} = f_i$ for every $i \leq j$. Then we define

$$\begin{array}{cccc} \theta : & D & \to & X \\ & \lambda_i(b_i) + S & \mapsto & f_i(b_i) \end{array}$$

and the following diagram commutes.

$$\begin{tikzcd}
D \arrow[rr, "\theta"] & & X \\
& B_i \arrow[ul, "\alpha_i"'] \arrow[ur, "f_i"] \arrow[d, "\varphi_{ij}"] & \\
& B_j \arrow[uul, "\alpha_j"] \arrow[uur, "f_j"'] &
\end{tikzcd}$$

Indeed, $\theta(\alpha_i(b_i)) = \theta(\lambda_i()b_i) + S) = f_i(b_i)$. Moreover, the map $\theta$ is the unique map $D \to X$ such that the above diagram is commutative for every $i \leq j$. If there is another one map $\varphi : D \to X$ satisfying that the above diagram is commutative,

[2] Let $M, N$ modules and let a map $f : M \to N$, then cokernel of $f$ is $coker(f) = \frac{N}{Imf}$

that is $\varphi \circ \alpha_i = f_i$. But we have that $f_i = \theta \circ \alpha_i$. Therefore, $\varphi \circ \alpha_i = \theta \circ \alpha_i$, $\forall i$ and then $\varphi = \theta$. Thus, the properties of direct limit are satisfied, and so

$$D \cong \varinjlim_{i \in I} B_i$$

Furthermore, we define

$$\begin{array}{cccc} \sigma : & \oplus_{ij} B_{ij} & \to & \oplus_i B_i \\ & b_i & \mapsto & \lambda_j \varphi_{ij}(b_i) - \lambda_i(b_i) \end{array}$$

We notice that $Im\sigma = S$. Hence, $coker\sigma = \oplus_i B_i / Im\sigma = (\oplus_i B_i)/S \cong \varinjlim_{i \in I} B_i$ and then there exists the below exact sequence

$$\oplus_{ij} B_{ij} \overset{\sigma}{\to} \oplus_i B_i \overset{\tau}{\to} \varinjlim_{i \in I} B_i \to 0 \tag{2.2}$$

Indeed, we have that $Ker\tau = Im\sigma = S$ as $\varinjlim_{i \in I} B_i \cong (\oplus_i B_i)/S$ and it is plain that $\tau$ is a surjection map. Now we act in the sequence 2.3 with the functor $A \otimes_R \square$ and then the sequence

$$A \otimes_R (\oplus_{ij} B_{ij}) \overset{1 \otimes \sigma}{\to} A \otimes_R (\oplus_i B_i) \overset{1 \otimes \tau}{\to} A \otimes_R \left( \varinjlim_{i \in I} B_i \right) \to 0 \tag{2.3}$$

is also exact, since $A \otimes_R \square$ is a right exact functor. Moreover, we have that the map

$$\begin{array}{cccc} \tau : & A \otimes_R (\oplus_i B_i) & \to & \oplus_i (A \otimes_R B_i) \\ & a \otimes (b_i) & \mapsto & (a \otimes b_i) \end{array}$$

is an isomorphism of $\mathbb{Z}-$modules. Indeed, $\tau(a \otimes (b_i) + a \otimes (b_i')) = \tau(a \otimes (b_i + b_i')) = (a \otimes (b_i + b_i')) = (a \otimes b_i + a \otimes b_i') = (a \otimes b_i) + (a \otimes b_i') = \tau(a \otimes (b_i)) + \tau(a \otimes (b_i'))$ and $\tau(\lambda a \otimes (b_i)) = \tau(a \otimes (\lambda b_i)) = (a \otimes (\lambda b_i)) = \lambda(a \otimes b_i) = \lambda \tau(a \otimes (b_i))$ with $\lambda \in \mathbb{Z}$. So $\tau$ is a homomorphism. Also, $\tau$ is an injective, since $\tau(a \otimes (b_i)) = (0) \Leftrightarrow (a \otimes b_i) = (0) \Leftrightarrow a \otimes b_i = 0$, $\forall i$, and then $a \otimes (b_i) = 0$. In addition, we will show that $\tau$ is a surjective map. Let $(a \otimes b_i) \in \oplus_i (A \otimes_R B_i)$. Then $\tau(a \otimes (b_i)) = (a \otimes b_i)$, and so $\tau$ is surjective. Thus, $\tau$ is an isomorphism of $\mathbb{Z}-$modules. Then,

$$\begin{tikzcd}
A \otimes_R (\oplus_{ij} B_{ij}) \arrow[r, "1 \otimes \sigma"] \arrow[d, "\tau'"'] & A \otimes_R (\oplus_i B_i) \arrow[r] \arrow[d, "\tau"] & A \otimes_R \left( \varinjlim_{i \in I} B_i \right) \arrow[r] \arrow[d] & 0 \\
\oplus (A \otimes_R B_{ij}) \arrow[r, "\tilde{\sigma}"] & \oplus (A \otimes_R B_i) \arrow[r] & \varinjlim_{i \in I} (A \otimes_R B_i) \arrow[r] & 0
\end{tikzcd}$$

where

$$\begin{array}{rccc} \tilde{\sigma}: & \oplus(A\otimes_R B_{ij}) & \to & \oplus(A\otimes B_i) \\ & (a\otimes b_{ij}) & \mapsto & (1\otimes\lambda_j)(a\otimes\varphi_{ij}(b_i))-(1\otimes\lambda_i)(a\otimes b_i) \end{array}$$

and $\tau'$ is an isomorphism (which can be proved like $\tau$). We will prove that $\tilde{\sigma}\circ\tau' = \tau\circ(1\otimes\sigma)$. Indeed, $\tau((1\otimes\sigma)(a\otimes b_i)) = \tau(a\otimes\sigma(b_i)) = \tau(a\otimes(\lambda_j\circ\varphi_{ij}(b_i)-\lambda(b_i))) = (a\otimes(\lambda_j\circ\varphi_{ij}(b_i)-\lambda_i(b_i)))$ and $\tilde{\sigma}\circ\tau'(a\otimes(b_{ij})) = \tilde{\sigma}(s\otimes b_{ij}) = (1\otimes\lambda_j)(a\otimes\varphi_{ij}(b_i))-(1\otimes\lambda_i)(a\otimes b_i) = (a\otimes\lambda_j\circ\varphi_{ij}(b_i))-(a\otimes\lambda_i(b_i)) = (a\otimes(\lambda_j\circ\varphi_{ij}(b_i)-\lambda_i(b_i))$. So we have the desired. In addition, it is plain that the sequence

$$\oplus(A\otimes_R B_{ij}) \xrightarrow{\tilde{\sigma}} \oplus(A\otimes_R B_i) \to \varinjlim_{i\in I}(A\otimes B_i)\to 0 \tag{2.4}$$

is an exact sequence. Similarly we can prove that

$$(\oplus(A\otimes B_i))/Im\tilde{\sigma} \cong \varinjlim_{i\in I}(A\otimes B_i)$$

Thus, the rows are exact sequences and the diagram commutes. Therefore, there exists a unique isomorphism

$$h:\ A\otimes\varinjlim_{i\in I}B_i \to \varinjlim_{i\in I}(A\otimes B_i)$$

making the augmented diagram commute, according to proposition 2.4.6. Hence,

$$A\otimes_R\varinjlim_{i\in I}B_i \cong \varinjlim_{i\in I}(A\otimes_R B_i)$$

□

In general it is not true that the tensor product $\square\otimes_{\mathbb{Z}} B$ commutes with the projective limit. This will be illustrated in the following example. We know that

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

Also we have that

$$\mathbb{Z}_p\otimes_{\mathbb{Z}}\mathbb{Q} = \mathbb{Q}_p$$

Then

$$(\varprojlim_{n\in\mathbb{N}}\mathbb{Z}/p^n\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Q} = \mathbb{Z}_p\otimes_{\mathbb{Z}}\mathbb{Q} = \mathbb{Q}_p$$

On the other hand, we have that

$$\mathbb{Z}/p^n\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q} = 0,\ for\ every\ n$$

and so

$$\varprojlim_{n\in\mathbb{N}}\mathbb{Z}/p^n\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q} = 0$$

Therefore,

$$(\varprojlim_{n\in\mathbb{N}}\mathbb{Z}/p^n\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Q} \neq \varprojlim_{n\in\mathbb{N}}\mathbb{Z}/p^n\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q}$$

Hence, the tensor product doesn't commute with the projective limit.

# Chapter 3

# Cohomology of Finite Groups

## 3.1 Differential Groups

Differential groups serve as a convenient starting point for studying the cohomology of groups, since they serve as an introduction to some of the basic techniques and as a tool for arriving at the infinite cohomology sequence.

***Definition* 3.1.1.** *A **differential group** is a pair $(A, d)$ where $A$ is an abelian group (which we shall usually write additively) and $d : A \to A$ is an endomorphism of $A$ such that $d^2 = d \circ d = 0$ (The $d$ is called **differential operator**).*
*This means that $Imd \subseteq Kerd$. Then we may form the group*

$$H(A) = \frac{Kerd}{Imd}$$

*which called **derived group** of $(A, d)$.*
*Let $(A_1, d_1)$ and $(A_2, d_2)$ are differential groups and $f : A_1 \to A_2$ is a homomorphism of groups. Then $f$ is said to be **admissible** when the following diagram*

$$\begin{tikzcd} A_1 \arrow[r, "f"] \arrow[d, "d_1"'] & A_2 \arrow[d, "d_2"] \\ A_1 \arrow[r, "f"'] & A_2 \end{tikzcd}$$

*is commutative, i.e $f \circ d_1 = d_2 \circ f$*

In this section all differential operators will be denoted by $d$.

***Proposition* 3.1.2.** *Every admissible homomorphism $f : (A, d) \to (B, d)$ of differential groups induces a homomorphism of groups*

$$f_* : H(A) \to H(B)$$

*given by*

$$f_*(a + dA) = f(a) + dB, \ where \ da = 0$$

*If $f, g : (A, d) \to (B, d)$ are admissible homomorphisms, then $f \pm g$ is also admissible and*

$$(f \pm g)_* = f_* \pm g_*$$

*If $f : (A, d) \to (B, d)$ and $g : (B, d) \to (C, d)$ are admissible homomorphisms, then $g \circ f$ is also admissible homomorphism and*

$$(g \circ f)_* = g_* \circ f_*$$

*Proof.* Firstly we will show that $f_*$ is well defined. Let $a + da_1$ another representative of the class $a + dA$, with $a_1 \in A$, then

$$\begin{aligned} f(a + da_1) &= f(a) + f(da_1) = f(a) + (f \circ d)(a_1) \\ &= f(a) + (d \circ f)(a_1), \ \textit{since } f \textit{ is admissible} \\ &= f(a) + d(f(a_1)) \in f(a) + dB \end{aligned}$$

Then $f_*(a + da_1 + dA) = f(a) + d(f(a_1)) + dB = f(a) + dB$. Thus $f_*$ is well-defined. Also, $f_*$ is a homomorphism, since

$$\begin{aligned} f_*(a + b + dA) &= f(a + b) + dB = f(a) + f(b) + dB \\ &= f(a) + dB + f(b) + dB = f_*(a + dA) + f_*(b + dB) \end{aligned}$$

Similarly we can prove the remaining assertions. □

***Corollary* 3.1.3.** *We have that*

$$0_* = 0 \textit{ and } 1_* = 1$$

*In more details if $0$ is the trivial map $(A, d) \to (B, d)$ then $0_*$ is the trivial map $H(A) \to H(B)$, and if $1 : A \to A$ is the identity map, then $1_* : H(A) \to H(A)$ is the identity.*

***Theorem* 3.1.4.** *Suppose that*

$$0 \to A \overset{i}{\to} B \overset{j}{\to} C \to 0$$

*is a short exact sequence of differential groups and $i, j$ are admissible homomorphisms.*
*I) Then there exists a homomorphism $d_* : H(C) \to H(A)$ such that the following triangle is exact*

$$\begin{tikzcd} H(C) \arrow[rr, "d_*"] & & H(A) \arrow[dl, "i_*"] \\ & H(B) \arrow[ul, "j_*"] & \end{tikzcd}$$

*II) Moreover, if*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d] & B \arrow[r, "j"] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r, "i'"] & B' \arrow[r, "j'"] & C' \arrow[r] & 0
\end{tikzcd}$$

*is a commutative diagram of differential groups with exact rows and all maps are admissible homomorphisms, then the following prism has exact triangles and commutative faces*

$$\begin{tikzcd}
H(C) \arrow[rr, "d_*"] \arrow[dd, "h_*"] & & H(A) \arrow[dl, "i_*"] \arrow[dd, "f_*"] \\
& H(B) \arrow[ul, "j_*"] \arrow[dd, "g_*"] & \\
H(C') \arrow[rr, "d'_*"] & & H(A') \arrow[dl, "i_*"] \\
& H(B') \arrow[ul, "j'_*"] &
\end{tikzcd}$$

*Proof.* I) $\rightsquigarrow$ Definition of $d_*$:
Let $\gamma \in H(C)$ that is $\gamma = c + dC$, with $d(c) = 0$. Then there exists $b \in B$ such that $j(b) = c$, since $j$ is surjective. We have that

$$j(db) = d(j(b)) = d(c) = 0 \Rightarrow d(b) \in Kerj \Rightarrow d(b) \in Imi$$

which means that there exists $a \in A$ such that $i(a) = d(b)$. So then

$$d(i(a)) = d^2(b) = 0 \Rightarrow d(i(a)) = 0 \Rightarrow i(d(a)) = 0$$

since $i$ is admissible, and this implies that $d(a) = 0$, because $i$ is injective, which means that $a \in Kerd$. Thus $a$ determines an element $\alpha = a + d(A) \in H(A)$. We define $d_*(\gamma) = \alpha$. In other words

$$d_*(\gamma) = a + dA, \ \ where \ j(b) = c \, and \, i(a) = d(b)$$

$\rightsquigarrow$ $d_*$ is well-defined:

Firstly, we will show that if $\gamma = 0 \in H(C)$, then $\alpha = 0$. That is if $c = d(c_1)$, with $c_1 \in C$, then we will show that $a = d(a_1)$. Now if $c = d(c_1)$ then there exists $b_1 \in B$ such that $j(b_1) = c_1$, since $j$ is surjective. So $j(b - d(b_1)) = j(b) - j(d(b_1)) = j(b) - d(j(b_1)) = j(b) - d(c_1) = 0$ which means that $b - d(b_1) \in Kerj = Imi$. Hence there exists $a_1 \in A$ such that $i(a_1) = b - d(b_1)$ and so $b = i(a_1) + d(b_1)$. Then $i(a) = d(b) = d(i(a_1) + d(b_1)) = d(i(a_1)) + d^2(b_1) = d(i(a_1)) = i(d(a_1))$. Therefore $i(a) = i(d(a_1))$ and since $i$ is injective then $a = d(a_1)$. In addition it is clear from its definition that $d_*$ is additive. So then it follows that $d_*$ is a well-defined homomorphism $H(C) \to H(A)$.

In order to show that the exactness of the triangle it remains to prove the six kernel-image relations.

$\rightsquigarrow$ $Imi_* \subseteq Kerj_*$:
We have that $j_* \circ i_* = (j \circ i)_* = 0_* = 0$.

$\rightsquigarrow$ $Imj_* \subseteq Kerd_*$:
If $b + dB \in H(B)$, with $db = 0$. Then

$$\begin{aligned} d_*(j_*(b + dB)) &= d_*(jb + dC) = d_*(c + dC) \\ &= d_*(\gamma) = \alpha = a + dA \end{aligned}$$

where $ia = db = 0$, which implies that $a = 0$, since $i$ is an injective map. Thus, $a + dA = 0 \in H(A)$ and therefore $d_* \circ j_* = 0$.

$\rightsquigarrow$ $Imd_* \subseteq Keri_*$:

$$\begin{aligned} i_*(d_*(c + dC)) &= i_*(a + dA) = i(a) + dB \\ &= d(b) + dB = 0 + dB = 0 \in H(B) \end{aligned}$$

Thus, $i_* \circ d_* = 0$ which means that $Imd_* \subseteq Keri_*$.

$\rightsquigarrow$ $Kerj_* \subseteq Imi_*$:
Let $b + dB \in Kerj_*$, that is $d(b) = 0$ and $j_*(b + dB) = j(b) + dC = 0 \in H(C)$. Then there exists $c \in C$ such that $j(b) = d(c)$. We choose $b_1 \in B$ such that $j(b_1) = c$, since $j$ is surjective, and

$$\begin{aligned} & j(b - d(b_1)) = j(b) - j(d(b_1)) = j(b) - d(j(b_1)) = d(c) = d(c) = 0 \\ \Rightarrow\ & b - d(b_1) \in Kerj = Imi \\ \Rightarrow\ & \exists a \in A \ such\ that\ i(a) = b - d(b_1) \\ \Rightarrow\ & d(i(a)) = d(b) - d^2(b_1) \Rightarrow i(d(a)) = 0 \\ \Rightarrow\ & d(a) = 0,\ since\ i\ is\ injective \end{aligned}$$

and

$$i_*(a + dA) = i(a) + dB = b - d(b_1) + dB = b + dB$$

Thus, $b + dB \in Imi_*$

$\rightsquigarrow$ $Kerd_* \subseteq Imj_*$:
Suppose that $c + dC \in Kerd_*$, that is $d(c) = 0$ and $d_*(c + dC) = a + dA = 0 \in H(A)$. So that $a \in dA$, that is $a = d(a_1)$, with $a_1 \in A$. We put $b_1 = b - i(a_1)$, where $c = j(b)$ and $i(a) = d(b)$. Then $j(b_1) = j(b - i(a_1)) = j(b) - j(i(a_1)) = j(b) = c$ and $d(b_1) = d(b) - d(i(a_1)) = i(a) - i(a) = 0$. Thus, $j_*(b_1 + dB) = j(b_1) + dC = c + dC$, that is $c + d) \in Imj_*$. Therefore, $Kerd_* \subseteq Imj_*$.

$\rightsquigarrow$ $Keri_* \subseteq Imd_*$:
Let $a + dA \in Keri_*$, that is $d(a) = 0$ and $i_*(a + dA) = i(a) + dB = 0 \in H(B)$. So $i(a) = d(b)$, with $b \in B$. We set $c = j(b)$. Thus, we have that $d(c) = d(j(b)) = j(d(b)) = j(i(a)) = 0$. Therefore, $d_*(c + dC) = a + dA$ which means that $a + dA \in Imd_*$

Therefore we proved that $Kerj_* = Imi_*$, $Kerd_* = Imj_*$, $Keri_* = Imd_*$ and then the triangle is exact.

II) From the above we have that

$$g_* \circ i_* = i'_* \circ f_* \; and \; h_* \circ j_* = j'_* \circ g_*$$

Since $g \circ i = i' \circ f$ then

$$(g \circ i)_* = (i' \circ f)_* \Rightarrow g_* \circ i_* = i'_* \circ f_*$$

Similarly, $h \circ j = j' \circ g \Rightarrow (h \circ j)_* = (j' \circ g)_* \Rightarrow h_* \circ j_* = j'_* \circ g_*$. It remains to show that $d'_* \circ h_* = f_* \circ d_*$. Indeed, $(f_* \circ d_*)(c + dC) = f_*(a + dA) = f(a) + dA'$, where $d(c) = 0$, $j(b) = c$ and i(a)=d(b). On the other hand $(d'_* \circ h_*)(c + dC) = d'_*(h_*(c + dC)) = d'_*(h(c) + dC'$. We have that $h(c) = h(j(b)) = (j' \circ g)(b) = j'(g(b))$ and $d'(g(b)) = g(d'(b)) = g(i(a)) = i'(f(a))$. So then $(d'_* \circ h_*)(c + dC) = d'_*(h(c) + dC') = f(a) + dA'$. Therefore the faces are commutative. This complete the proof. □

We assume that $(A, d)$ is a differential group. Let also $\{A_n\}$ be an infinite sequence of abelian groups and homomorphisms $d_n = d|_{A_n} : A_n \to A_{n+r}$ such that $d_{n+r} \circ d_n = 0$, where $r = \pm 1$, for every $n \in \mathbb{Z}$. So we get an infinite sequence

$$\cdots \to A_{n-r} \overset{d_{n-r}}{\to} A_n \overset{d_n}{\to} A_{n+r} \overset{d_{n+r}}{\to} A_{n+2r} \to \cdots \quad (*)$$

In this case we will denote by $(A, d, r)$, where $A = \sum_{-\infty}^{+\infty} \oplus A_n$ and it will be called differential graded group. The case $r = 1$, that is $(A, d, 1)$, is called **cohomology**, while the case $r = -1$, that is $(A, d, -1)$, is called **homology**. This distinction is highly artificial in that if $(A, d, 1)$ is a differential graded group of cohomology type, then we may put $A'_n = A_{-n}$ and $d'_n = d_{-n}$ and then $(A', d', -1)$ is a differential graded group of homological type. That is

$$\cdots \to A_{-2} \overset{d_{-2}}{\to} A_{-1} \overset{d_{-1}}{\to} A_0 \overset{d_0}{\to} A_1 \overset{d_1}{\to} A_2 \to \cdots$$

$$\cdots \to A'_2 \overset{d'_2}{\to} A'_1 \overset{d'_1}{\to} A'_0 \overset{d'_0}{\to} A'_{-1} \overset{d'_{-1}}{\to} A'_{-2} \to \cdots$$

Now we consider the differential graded group $(A, d, 1)$. For each $n \in \mathbb{Z}$, the group $A_n$ is called the **group of n-cochains**. The operator $d$ determines for each $n \in \mathbb{Z}$ the groups

$$\mathcal{C}_n := A_n \cap Kerd_n$$

which is called the **group of n-cocycles** and

$$\mathcal{B}_n = A_n \cap d_{n-1}(A_{n-1})$$

which is called the **group of n-coboundaries**. Let the chain

$$\cdots \to A_{-2} \overset{d_{-2}}{\to} A_{-1} \overset{d_{-1}}{\to} A_0 \overset{d_0}{\to} A_1 \overset{d_1}{\to} A_2 \to \cdots$$

For example $\mathcal{C}_2 = A_2 \cap Kerd_2 = Kerd_2$ and $\mathcal{B}_2 = A_2 \cap d_1(A_1) = d_1(A_1) = Imd_1$, so then $\mathcal{B}_2 \subseteq \mathcal{C}_2$, since $Imd_1 \subseteq Kerd_2$. In general we have that $\mathcal{B}_n \subseteq \mathcal{C}_n$, because $d_{n-1}(A_{n-1}) \subseteq Kerd_n$.

***Definition* 3.1.5.** *The group*

$$H_n(A) = \frac{\mathcal{C}_n}{\mathcal{B}_n}$$

*will be called the **nth cohomology group of A**.*

***Definition* 3.1.6.** *Let $(A, d, 1)$ and $(B, d, 1)$ are differential graded groups and $f : A \to B$ is a homomorphism of groups. Then $f$ is said to be an admissible map for the $(A, d, 1)$ and $(B, d, 1)$ when $f \circ d = d \circ f$ and $f$ maps $A_n$ into $B_n$ for every $n \in \mathbb{Z}$. It is clear that for the induced map $f_* : H(A) := \sum_{-\infty}^{+\infty} \oplus H_n(A) \to H(B) := \sum_{-\infty}^{+\infty} \oplus H_n(B)$ we have that*

$$f_* : H_n(A) \to H_n(B), \ for\ every\ n \in \mathbb{Z}$$

*and $f_n = f|_{A_n} : A_n \to B_n$ such that $f_{n+1} \circ d = d \circ f_n$ for every $n \in \mathbb{Z}$. This means that*

$$\begin{tikzcd}
\cdots \arrow[r] & A_{-2} \arrow[r, "d_{-2}"] \arrow[d, "f_{-2}"] & A_{-1} \arrow[r, "d_{-1}"] \arrow[d, "f_{-1}"] & A_0 \arrow[r, "d_0"] \arrow[d, "f_0"] & A_1 \arrow[r, "d_1"] \arrow[d, "f_1"] & A_2 \arrow[r] \arrow[d, "f_2"] & \cdots \\
\cdots \arrow[r] & B_{-2} \arrow[r, "d_{-2}"] & B_{-1} \arrow[r, "d_{-1}"] & B_0 \arrow[r, "d_0"] & B_1 \arrow[r, "d_1"] & B_2 \arrow[r] & \cdots
\end{tikzcd}$$

*where $d_n$ are differential operators, $f_n : A_n \to B_n$ such that $f_{n+1} \circ d = d \circ f_n$ for every $n \in \mathbb{Z}$.*

***Proposition* 3.1.7.** *We consider the following commutative diagram of differential graded groups, all of cohomological type, with exact rows and all maps admissible*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"] & B \arrow[r, "j"] \arrow[d, "g"] & C \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & A' \arrow[r, "i'"] & B' \arrow[r, "j'"] & C' \arrow[r] & 0
\end{tikzcd}$$

*Then the following diagram is commutative with exact rows.*

$$\begin{tikzcd}
\cdots \arrow[r] & H_{n-1}(C) \arrow[r, "d_*"] \arrow[d, "h_*"] & H_n(A) \arrow[r, "i_*"] \arrow[d, "f_*"] & H_n(B) \arrow[r, "j_*"] \arrow[d, "g_*"] & H_n(C) \arrow[r, "d_*"] \arrow[d, "h_*"] & H_{n+1}(A) \arrow[r] \arrow[d, "f_*"] & \cdots \\
\cdots \arrow[r] & H_{n-1}(C') \arrow[r, "d_{-2}"] & H_n(A') \arrow[r, "i'_*"] & H_n(B') \arrow[r, "j'_*"] & H_n(C') \arrow[r, "d_*"] & H_{n+1}(A') \arrow[r] & \cdots
\end{tikzcd}$$

*Proof.* According to theorem 3.1.4 we have that the diagram is commutative with exact rows. Also we notice that $d_*$ raises dimension by 1, since it is of cohomological type. □

## 3.2 G- modules

***Definition* 3.2.1.** *Let $M \neq \emptyset$ and $R$ be a ring (not necessary commutative with identity). The $M$ will be called left $R$-module, when $M$ is an additive abelian group equipped with a scalar multiplication*

$$\begin{array}{ccc} R \times M & \to & M \\ (r, m) & \mapsto & rm \end{array}$$

*such that*

- *$(r_1 + r_2)m = r_1 m + r_2 m$, for every $m \in M$ and $r_1, r_2 \in R$*
- *$r(m_1 + m_2) = rm_1 + rm_2$, for every $r \in R$ and $m_1, m_2 \in M$*
- *$r_1(r_2 m) = (r_1 r_2)m$, for every $r_1, r_2 \in R$ and $m \in M$*

*If also $R$ be a ring with identity element $1$, such that $1 \cdot m = m$, for every $m \in M$, then $M$ is called unitary left $R$-module.*
*Similarly, we can define the right $R$-module (In general left $R$-modules and right $R$-modules are different). We denote the left $R$-module $M$ by ${}_R M$ and the right $R$-module $M$ by $M_R$.*

Let $G$ be a finite group.

***Definition* 3.2.2.** *A $G$-module $A$ is an additive abelian group equipped with a scalar multiplication*

$$\begin{array}{ccc} G \times A & \to & A \\ (g, a) & \mapsto & ga \end{array}$$

*such that the following axioms holds for every $\sigma, \tau \in G$ and $a, b \in M$*

- $1 \cdot a = a$*, for every* $a \in M$
- $\sigma(a+b) = \sigma(a) + \sigma(b)$
- $\sigma(\tau a) = (\sigma\tau)(a)$

We can interpret $G$-modules as modules over rings by introducing the integer group ring of $G$. For every finite group $G$ we construct the integer group ring of $G$,

$$\mathbb{Z}[G] = \{\sum_{\sigma \in G} n_\sigma \sigma \mid n_\sigma \in \mathbb{Z}\}$$

that is $\mathbb{Z}[G]$ is a free abelian group with base $G$. The operations of ring $\mathbb{Z}[G]$ are defined as follow: the addition is defined by

$$\sum_{\sigma \in G} n_\sigma \sigma + \sum_{\sigma \in G} m_\sigma \sigma = \sum_{\sigma \in G} (n_\sigma + m_\sigma)\sigma$$

and the multiplication is defined by

$$\begin{array}{rcl} (\sum_{\sigma \in G} n_\sigma \sigma)(\sum_{\sigma \in G} m_\sigma \sigma) & = & \sum_{\sigma \in G}(\sum_{zp=\sigma} m_z n_p)\sigma \\ & = & \sum_{\sigma \in G}(\sum_{z \in G} m_z n_{z^{-1}\sigma})\sigma \end{array}$$

We may identify the elements of $G$, say $\sigma$, with the elements $1 \cdot \sigma$ of $\mathbb{Z}[G]$ , and then we may view $G$ as embedded in $\mathbb{Z}[G]$. Now the $G$-module $A$ becomes $\mathbb{Z}[G]$-module with the operation which defined by

$$(\sum_{\sigma \in G} n_\sigma \sigma)(a) = \sum_{\sigma \in G} n_\sigma(\sigma a)$$

In addition, if $A$ is a left $\mathbb{Z}[G]$-module, then $G$ is embedded in $\mathbb{Z}[G]$, so then $A$ becomes $G$-module.

For example, let $G$ be a finite group and we define the action of $G$ on $A$ to be the trivial, that is $G \times \mathbb{Z} \to \mathbb{Z}$, where $(\sigma, n) \mapsto \sigma \cdot n = n$. Then $\mathbb{Z}$ becomes a $G$-module. Similarly, $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are also $G$-modules with the trivial action. Moreover, the additive group $\mathbb{Z}[G]$ is a $G$-module.

Now we will define two useful ideals of the ring $\mathbb{Z}[G]$. The first ideal

$$I_G = \{\sum_{\sigma\in G} n_\sigma \sigma \in \mathbb{Z}[G] \mid \sum_{\sigma\in G} n_\sigma = 0\}$$

which is called *augmentation ideal* of $\mathbb{Z}[G]$. We have that $I_G$ is an ideal of $\mathbb{Z}[G]$ because it is the kernel of the homomorphism

$$\begin{array}{cccc} \epsilon : & \mathbb{Z}[G] & \to & \mathbb{Z} \\ & \sum_{\sigma\in G} n_\sigma \sigma & \mapsto & \sum_{\sigma\in G} n_\sigma \end{array}$$

The homomorphism $\epsilon$ is called *augmentation map*. Also, we denote by

$$N_G = \sum_{\sigma\in G} \sigma$$

the norm (or trace) of $\mathbb{Z}[G]$. For every $\tau \in G$ we have that $\tau N_G = \tau \sum_{\sigma\in G} \sigma = \sum_{\sigma\in G} \tau\sigma = \sum_{\sigma\in G} \sigma = N_G$. Therefore, $\mathbb{Z}N_G$ is an ideal of $\mathbb{Z}[G]$ as well, where

$$\mathbb{Z}N_G = \{n \sum_{\sigma\in G} \sigma \mid n \in \mathbb{Z}\}$$

The map

$$\begin{array}{cccc} \mu : & \mathbb{Z} & \to & \mathbb{Z}[G] \\ & n & \mapsto & nN_G \end{array}$$

is called *coaugmentation* of $\mathbb{Z}[G]$. Finally, we set

$$J_G = \mathbb{Z}[G]/\mathbb{Z}N_G$$

So then we have constructed two short exact sequences of rings with homomorphism of rings as follow

$$0 \to I_G \overset{i}{\hookrightarrow} \mathbb{Z}[G] \overset{\epsilon}{\to} \mathbb{Z} \to 0 \quad (1a)$$

$$0 \to \mathbb{Z} \overset{\mu}{\to} \mathbb{Z}[G] \overset{j}{\to} J_G \to 0 \quad (1b)$$

Indeed, the sequence $(1a)$ is exact, since $\epsilon$ is surjective, $i$ is injective and $Ker\epsilon = Imi$. In the same way we have that the sequence $(1b)$ is exact as well. If now we consider the rings as additive groups, then we have the following theorem:

***Theorem* 3.2.3.** *i) The ideal $I_G$ is a free abelian group with $\mathbb{Z}$-base $\{\sigma - 1 \mid \sigma \in G \setminus \{1\}\}$.*
*ii) $J_G$ is a free abelian group that is generated by $\{\sigma \mod \mathbb{Z}N_G,\ \sigma \neq 1\}$*
*Finally, we have that a) $\mathbb{Z}[G] = I_G \oplus \mathbb{Z}\cdot 1 \cong I_G \oplus \mathbb{Z}$ and*
*b) $\mathbb{Z}[G] = (\sum_{\sigma\in G\setminus\{1\}} \mathbb{Z}\sigma) \oplus \mathbb{Z}N_G \cong J_G \oplus \mathbb{Z}$*

*Proof.* i) If $\sum\limits_{\sigma \in G} n_\sigma \sigma \in I_G$, then $\sum\limits_{\sigma \in G} n_\sigma = 0$. Additionally,

$$\sum_{\sigma \in G} n_\sigma \sigma = \sum_{\sigma \in G \setminus \{1\}} n_\sigma (\sigma - 1)$$

This means that the $\mathbb{Z}$-module $I_G$ is generated by $\{\sigma - 1 \mid \sigma \in G \setminus \{1\}\}$. It remains to show that $I_G$ is a free group. If $\sum\limits_{\sigma \in G \setminus \{1\}} n_\sigma (\sigma - 1) = 0 \Rightarrow \underbrace{\sum\limits_{\sigma \in G} n_\sigma \sigma - \sum\limits_{\sigma \in G} n_\sigma \cdot 1}_{\in \mathbb{Z}[G]} = 0$

Then $n_\sigma = 0$, for every $\sigma \neq 1$ and $\sum\limits_{\sigma \in G} n_\sigma = 0$, since $\mathbb{Z}[G]$ is a free abelian group. Hence, $I_G$ is a free abelian group which is generated by $\{\sigma - 1 \mid \sigma \in G \setminus \{1\}\}$. Every element $\sum\limits_{\sigma \in G} n_\sigma \sigma \in \mathbb{Z}[\mathbb{G}]$ can be written uniquely in the form

$$\sum_{\sigma \in G} n_\sigma \sigma = \sum_{\sigma \in G} n_\sigma (\sigma - 1) + (\sum_{\sigma \in G} n_\sigma) \cdot 1$$

Thus, $\mathbb{Z}[G] = I_G \oplus \mathbb{Z} \cdot 1 \cong I_G \oplus \mathbb{Z}$.

ii) Let $\sum\limits_{\sigma \in G} n_\sigma \sigma \mod \mathbb{Z}N_G \in J_G$. This can be written as

$$\begin{aligned}\sum_{\sigma \in G} n_\sigma \sigma &= \sum_{\sigma \in G \setminus \{1\}} (n_\sigma - n_1)\sigma + n_1 \sum_{\sigma \in G} \sigma \\ &\equiv \sum_{\sigma \in G \setminus \{1\}} (n_\sigma - n_1)\sigma \mod \mathbb{Z}N_G\end{aligned}$$

This implies that the $J_G$ as a $\mathbb{Z}$-module is generated by $\{\sigma \mod \mathbb{Z}N_G,\ \sigma \neq 1\}$. Moreover,

$$\begin{aligned}\sum_{\sigma \in G \setminus \{1\}} n_\sigma \sigma \in \mathbb{Z}N_G &\Rightarrow \sum_{\sigma \neq 1} n_\sigma \sigma = n \sum_{\sigma \in G} \sigma \\ &\Rightarrow n \cdot 1 + \sum_{\sigma \in G \setminus \{1\}} (n - n_\sigma)\sigma = 0\end{aligned}$$

and then $\sum\limits_{\sigma \in G} \nu_\sigma \sigma \in \mathbb{Z}[G]$, so $\nu_\sigma = 0$, for every $\sigma \in G$, that is $n_\sigma = 0$, for every $\sigma \neq 1$. Therefore, $J_G$ is a free abelian group which is generated by $\{\sigma \mod \mathbb{Z}N_G,\ \sigma \neq 1\}$. Finally, every element $\sum\limits_{\sigma \in G} n_\sigma \sigma \in \mathbb{Z}[\mathbb{G}]$ can be written uniquely in the form

$$\sum_{\sigma \in G} n_\sigma \sigma = \sum_{\sigma \in G \setminus \{1\}} (n_\sigma - n_1)\sigma + n_1 N_G$$

Hence, $\mathbb{Z}[G] = (\sum\limits_{\sigma \in G \setminus \{1\}} \mathbb{Z}\sigma) \oplus \mathbb{Z}N_G \cong J_G \oplus \mathbb{Z}$. □

***Definition* 3.2.4.** *Let $R$ be a ring and $I$ is an ideal of $R$, then the annihilator of $I$ is defined by*

$$Ann(I) = \{a \in R \,|\, aI = 0\}$$

The ideals $I_G$ and $\mathbb{Z}N_G$ of $\mathbb{Z}[G]$ are dual to each other in the following sense.

***Theorem* 3.2.5.** *We have that: 1) $I_G = Ann(\mathbb{Z}N_G)$ and 2) $\mathbb{Z}N_G = Ann(I_G)$*

*Proof.* 1) Let $a = \sum\limits_{\sigma \in G} n_\sigma \sigma \in \mathbb{Z}[G]$ such that $a \in Ann(\mathbb{Z}N_G)$. That is

$$(\sum_{\sigma \in G} n_\sigma \sigma)(\mathbb{Z}N_G) = 0 \Rightarrow (\sum_{\sigma \in G} n_\sigma \sigma)N_G = 0 \Rightarrow \sum_{\sigma \in G} n_\sigma(\sigma N_G) = 0$$
$$\Rightarrow \sum_{\sigma \in G} n_\sigma N_G = 0 \Rightarrow (\sum_{\sigma \in G} n_\sigma)N_G = 0 \Rightarrow \sum_{\sigma \in G} n_\sigma = 0$$

so then $a \in I_G$. Clearly, the converse is also true. Thus, $I_G = Ann(\mathbb{Z}N_G)$.
2) Let $a = \sum\limits_{\tau \in G} n_\tau \tau \in \mathbb{Z}[G]$ such that $a \in Ann(I_G)$. That is

$$\sum_{\tau \in G} n_\tau \tau \in Ann(I_G) \Leftrightarrow (\sum_{\tau \in G} n_\tau \tau)(\sigma - 1) = 0, \ \forall \sigma \in G$$
$$\Leftrightarrow \sum_{\tau \in G} n_\tau \tau\sigma = \sum_{\tau \in G} n_\tau \tau, \ \forall \sigma \in G \Leftrightarrow n_\tau = n_1, \ \forall \tau \in G$$
$$\sum_{\tau \in G} n_\tau \tau = n_1 \sum_{\tau \in G} \tau = n_1 N_G \in \mathbb{Z}N_G$$

Hence, $\mathbb{Z}N_G = Ann(I_G)$. □

For every $G$-module A we can construct the following subgroups

$$A^G = \{a \in A \mid \sigma(a) = a, \forall \sigma \in G\}$$

which is called the group of fixed elements of $A$.

$$N_G A = \{N_G a = \sum_{\sigma \in G} \sigma a \mid a \in A\}$$

$$_{N_G}A = \{a \in A \,|\, N_G a = 0\}$$
$$I_G A = \{\sum_{\sigma \in G} n_\sigma(\sigma a_\sigma - a_\sigma) \mid a_\sigma \in A\}$$

That is $I_G A$ is generated by the elements of the form $\sigma a - a$, with $\sigma \in G$ and $a \in A$. Also, $I_G = {}_{\mathbb{Z}}{<}\sigma - 1 \mid \sigma \in G \setminus \{1\} >$ and then $A^G = \{a \in A \mid I_G a = 0\}$ According to theorem 3.2.5 we have that $N_G A \leqslant A^G$ and $I_G A \leqslant {}_{N_G}A$.

$\rightsquigarrow$ $N_GA \leqslant A^G$

Let $a \in A$ such that $N_Ga \in N_GA$, so $N_Ga = \sum_{\sigma \in G} \sigma a$, with $a \in A$ then $\tau(N_Ga) = \sum_{\sigma \in G} \tau\sigma a = \sum_{\sigma \in G} \sigma a = N_Ga$, for every $\tau \in G$ and $N_Ga \in A$, since $A$ is a $G$-module.

$\rightsquigarrow$ $I_GA \leqslant {}_{N_G}A$

Let $\beta = \sum_{\sigma \in G} n_\sigma(\sigma a_\sigma - a_\sigma) \in I_GA$. We will show that $N_G\beta = 0$. Then

$$\mathbb{Z}N_G\beta = Ann(I_G)\beta = 0 \Rightarrow N_G\beta = 0$$

Thus we are able to construct the quotient groups $A^G/N_GA$ and ${}_{N_G}A/I_GA$. We will see that they are the cohomology group of order $-1$ and $0$, respectively.

Let $A$ be a $G$-module and $H \leqslant G$. It is clear that $A$ is a $H$-module. If $H \trianglelefteq G$, then the module of fixed elements $A^H = \{a \in A \mid ha = a, \forall h \in H\}$ becomes a $G/H$-module. Indeed, $A^H$ is an additive group, since $A$ is, and $G/H$ acts on $A^H$ as follow

$$\begin{array}{ccc} G/H \times A^H & \to & A^H \\ (gH, a) & \mapsto & (gH)a = gHa = ga \end{array}$$

Now if $A, B$ are $G$-modules, then

$$Hom(A,B) = \{f \mid f : A \to B,\ f\, is\, homomorphism\, of\, groups\}$$

***Definition* 3.2.6.** *We define the set of G-homomorphism*

$$Hom_G(A,B) = \left\{ \begin{array}{c} f \mid f : A \to B, f\, is\, homomorphism\, of\, groups \\ such\, that\ f(\sigma a) = \sigma f(a),\ \forall \sigma \in G \end{array} \right\}$$

***Proposition* 3.2.7.** *1) The additive group $Hom(A,B)$ becomes a G-module when the action of G is defined by*

$$f^\sigma = \sigma(f) = \sigma \circ f \circ \sigma^{-1},\ where\ f \in Hom(A,B),\ \sigma \in G$$

*2) $Hom_G(A,B)$ is a subgroup of $Hom(A,B)$. In fact,*

$$Hom_G(A,B) = \{f \in Hom(A,B) \mid f^\sigma = f\ \forall \sigma \in G\}$$

*Proof.* 1) It is clear that $(f_1+f_2)^\sigma = \sigma(f_1+f_2) = \sigma \circ (f_1+f_2) \circ \sigma^{-1} = \sigma \circ f_1\sigma^{-1} + \sigma \circ f_2\sigma^{-1} = f_1^\sigma + f_2^\sigma$. Also, $f^{\sigma\tau} = \sigma\tau(f) = \sigma\tau \circ f \circ \tau^{-1}\sigma^{-1} = \sigma \circ \tau(f) \circ \sigma^{-1} = \sigma \circ f^\tau \circ \sigma^{-1} = \sigma(f^\tau) = (f^\tau)^\sigma$ and $f^1 = 1f = f$. Thus,

$Hom(A,B)$ is a $G$-module.
2)

$$\begin{aligned} Hom_G(A,B) &= \{f \in Hom(A,B) \,:\, f(\sigma a) = \sigma f(a)\} \\ &= \{f \in Hom(A,B) \,:\, f \circ \sigma = \sigma \circ f,\, \forall \sigma \in G\} \\ &= \{f \in Hom(A,B) \,:\, \sigma \circ f \circ \sigma^{-1} = f,\, \forall \sigma \in G\} \\ &= \{f \in Hom(A,B) \,:\, f^{\sigma} = f,\, \forall \sigma \in G\} \end{aligned}$$

Moreover, it is plain that $Hom_G(A,B)$ is a subgroup of $Hom(A,B)$, since $1 \in Hom_G(A,B)$, $f+g \in Hom_G(A,B)$ for every $f,g \in Hom_G(A,B)$ and $-f \in Hom_G(A,B)$. □

***Proposition* 3.2.8.** *Let $A, A_1, A_2, B, B_1, B_2$ be G-modules. Then:*

1. *If $\varphi \in Hom(A_1,A)$ and $\psi \in Hom(B,B_1)$, then we may define a homomorphism of additive groups*

$$(\varphi,\psi) \,:\, Hom(A,B) \to Hom(A_1,B_1)$$

*by putting for $f \in Hom(A,B)$*

$$(\varphi,\psi)(f) = \psi \circ f \circ \phi$$

2. *If in addition $\phi_1 \in Hom(A_2,A_1)$ and $\psi_1 \in Hom(B_1,B_2)$, then*

$$(\phi_1,\psi_1) \circ (\phi,\psi) = (\phi \circ \phi_1, \psi_1 \circ \psi)$$

3. *$(\phi,\psi)$ is additive in each variable*
*$(\phi,0)$ and $(0,\psi)$ are $0$-maps*
*$(1,1)$ is the identity map.*

4. *If $\phi$ and $\psi$ are both G-homomorphisms, then $(\phi,\psi)$ is a G-homomorphism, symbolically*

$$(\phi,\psi) \in Hom_G(Hom(A,B), Hom(A_1,B_1)$$

5. *If $\phi$ and $\psi$ are both G-homomorphisms, then $(\phi,\psi)$ maps $Hom_G(A,B) \to Hom_G(A_1,B_1)$, symbolically*

$$(\phi,\psi) \in Hom(Hom_G(A,B), Hom_G(A_1,B_1)$$

*Proof.* Straightforward verification. □

***Proposition* 3.2.9.** *Let $A, B, C$ and $\mathbb{Z}$ be G-modules, where, as usual, the action of G on $\mathbb{Z}$ is the trivial, and we define $\widehat{A} = Hom(A,\mathbb{Z})$. Then* *(i)* $\hat{A}$ *is a G-module*

*(ii) If* $A$ *is a G-free with finite base, then so is* $\hat{A}$.

*(iii) If* $f \in Hom(A, B)$ *and* $\hat{f} = (f, 1)$, *then* $\hat{f} \in Hom(\hat{B}, \hat{A})$. *If moreover* $f \in Hom_G(A, B)$, *then* $\hat{f} \in Hom_G(\hat{B}, \hat{A})$.

*(iv) If* $f, f_1, f_2 \in Hom(A, B)$ *and* $g \in Hom(B, C)$, *then* $\hat{f}_1 + \hat{f}_2 = \widehat{f_1 + f_2}$, $\widehat{g \circ f} = \hat{f} \circ \hat{g}$, $\hat{1} = 1$, $\hat{0} = 0$.

*(v) If* $f \in Hom(A, B)$ *is an epimorphism, then* $\hat{f}$ *is a monomorphism.*

*Proof.* (i) It follows from proposition 3.2.7

(ii) $A$ is a $G$-module, and then $A$ is a $\mathbb{Z}[G]$-module with the action $(\sum_{\sigma\in G} n_\sigma \sigma)a = \sum_{\sigma\in G} n_\sigma(\sigma a)$. So $A = \sum_{i=1}^{n} \oplus \mathbb{Z}Ga_i$, thus $A = \sum_{i=1}^{n} \oplus_{\sigma\in G}\mathbb{Z}(\sigma a_i)$. This means that $A$ is a free $\mathbb{Z}$-module with base $\{\sigma a_i \,|\, i = 1, \dots, n,\ \sigma \in G\}$. For $i = 1, \dots, n$ we define $f_i \in \hat{A} = Hom(A, \mathbb{Z})$ as follows

$$f_i(\sigma a_j) = \begin{cases} 1, & if\ \sigma = 1,\ i = j \\ 0, & otherwise \end{cases}$$

and we extend linearly from $\mathbb{Z}$-basis to all of $A$. The set

$$\{f_i^\tau \,|\, \tau \in G, i = 1, \dots, n\}$$

is a $\mathbb{Z}$-basis of $\hat{A}$, because

$$f_i^\tau(\sigma a_j) = \tau \circ f_i \circ \tau^{-1} \circ \sigma a_j \begin{cases} 1, & if\ \sigma = \tau,\ i = j \\ 0, & otherwise \end{cases}$$

$g(\sigma a_i) = \sum_{i=1}^{n}\sum_{\tau\in G} m_{\tau,j} f_j^\tau(\sigma a_i) = m_{\sigma,i}$. Therefore, $\{f_i^\tau \,|\, \tau \in G, i = 1, \dots, n\}$ is a $\mathbb{Z}[G]$-base of $\hat{A}$, since

$$\hat{A} = \sum_{i=1}^{n} \oplus_{\sigma\in G} \mathbb{Z} f_i^\sigma = \sum_{i=1}^{n} \oplus_{\sigma\in G} f_i^{\mathbb{Z}\sigma} = \sum_{i=1}^{n} \oplus f_i^{\mathbb{Z}[G]} = \sum_{i=1}^{n} \oplus \mathbb{Z}[G] f_i$$

Thus, $\hat{A}$ is a free $\mathbb{Z}[G]$-module with base $\{f_i, i = 1, \dots, n\}$

(iii) We have that $f \in Hom(A, B)$ and $1 : \mathbb{Z} \to \mathbb{Z}$. Then $\hat{f} = (f, 1) : Hom(B, \mathbb{Z}) \to Hom(A, \mathbb{Z})$. If $f \in Hom_G(A, B)$, then according to proposition 3.2.8(4) we have that $(f, 1) \in Hom_G(\hat{B}, \hat{A})$.

(iv) It follows from the properties of symbol $(\varphi, \psi)$.

(v) We have that $f(A) = B$, since $f$ is epimorphism. We suppose that $\hat{f}(\tau) = 0$ for some $\tau \in \hat{B} = Hom(B, \mathbb{Z})$. That is

$$(f, 1)(\tau) = 0 \Rightarrow 1 \circ \tau \circ f = 0 \Rightarrow \tau \circ f = 0$$

and since $f(A) = B$ this implies that

$$(\tau \circ f)(A) = 0 \Rightarrow \tau(B) = 0$$

hence $\tau = 0$. Therefore, $\hat{f}$ is monomorphism. □

***Proposition* 3.2.10.** *Let $A$ be a $G$-module. Then we have the following isomorphisms:*

1. *$Hom_G(\mathbb{Z}[G], A) \cong A$, as additive groups*
2. *$Hom(\mathbb{Z}, A) \cong A$, as G-modules*
3. *$\hat{\mathbb{Z}} \cong \mathbb{Z}$, as G-modules*

*Proof.* 1. Let $f \in Hom_G(\mathbb{Z}[G], A)$, then we have that $f(\sum n_\sigma \sigma) = \sum n_\sigma f(\sigma \cdot 1) = \sum n_\sigma \sigma(f(1)) = (\sum n_\sigma \sigma) f(1)$. So any $f \in Hom_G(\mathbb{Z}[G], A)$ is determined by $f(1)$. Thus, for every $a \in A$ there exists $f \in Hom_G(\mathbb{Z}[G], A)$ such that $f(1) = a$. We define

$$\begin{array}{rccc} \phi : & Hom_G(\mathbb{Z}[G], A) & \rightarrow & A \\ & f & \mapsto & f(1) \end{array}$$

which is an isomorphism of groups. Indeed, $\phi$ is surjective, since for every $a \in A$ there exists $f \in Hom_G(\mathbb{Z}[G], A)$such that $f(1) = a$. In addition, $\phi$ is injective, since if $f(1) = g(1)$, then

$$(f - g)(1) = 0 \Rightarrow f - g = 0 \Rightarrow f = g$$

and it is plain that $\phi$ is homomorphism.
2. In the same way with $(1)$ we have that the map

$$\begin{array}{rccc} \psi : & Hom_G(\mathbb{Z}, A) & \rightarrow & A \\ & f & \mapsto & f(1) \end{array}$$

is an isomorphism of groups. Also, $\psi(f^\sigma) = f^\sigma(1) = (\sigma \circ \sigma^{-1})(1) = \sigma \circ f(1)$, since $\mathbb{Z}$ is a $G$-module with the trivial action. So then $\psi(f^\sigma) = \psi(\sigma(f)) = (\sigma \circ f)(1) = \sigma\psi(f)$, this means that $\psi$ is a $G$-homomorphism.
3. From $(2)$ we have that $Hom_G(\mathbb{Z}, A) = Hom(\mathbb{Z}, A)$ □

## 3.3 Definition of Cohomology Groups

***Definition* 3.3.1.** *Let $G$ be a finite group. A complete free resolution of group $G$ (or of $G$-module $\mathbb{Z}$ with the trivial action) is defined to be the complex*

$$\begin{tikzcd}
\cdots & X_{-3} \arrow[l] & X_{-2} \arrow[l, "d_{-2}"'] & X_{-1} \arrow[l, "d_{-1}"'] & & X_0 \arrow[ll, "d_0"'] \arrow[dl, "\epsilon"'] & X_1 \arrow[l, "d_1"'] & X_2 \arrow[l, "d_2"'] & \cdots \arrow[l] \\
& & & & \mathbb{Z} \arrow[ul, "\mu"] \arrow[dl] & & & & \\
& & & 0 & & 0 \arrow[ul] & & &
\end{tikzcd}$$

*where*

*(i)* $X_q$ *are free $G$-modules,* $q \in \mathbb{Z}$

*(ii)* $\epsilon, \mu, d_q$ *are $G$-homomorphisms*

*(iii) The triangle is commutative, that is* $d_0 = \mu \circ \epsilon$

*(iv) The sequence is exact at every term.*

*So then a complete free resolution of $G$ (or $G$-complex) can be broken up into two exact sequences of $G$-modules and $G$-homomorphisms, namely*

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\epsilon} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \longleftarrow \cdots$$

*which is called the positive part. From this arose the cohomology.*

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} X_{-1} \xrightarrow{d_{-1}} X_{-2} \xrightarrow{d_{-2}} X_{-3} \longrightarrow \cdots$$

*which is called negative part and from this arose the homology. Conversely, if we are given a positive part and negative part, then they can be combined (by putting* $d_0 = \mu \circ \epsilon$*) to form a $G$-complex.*

The positive and negative part combined by Tate and this combination is very important because it leads to comprehensive study of them. For every group $G$ we can construct at least one complete free resolution of $G$. We construct one complete free resolution as follow which is called standard complete free resolution or standard complex of $G$:

For every $q \geq 1$ we define symbols $[\sigma_1, \dots, \sigma_q]$ consisting of ordered $n$-tuples of elements $\sigma_i \in G$, and we call them $q$-cells. The $q$-cells will be used as free generators of $G$-modules, that is we put

$$X_q = X_{-q-1} = \sum_{\sigma_1,\dots,\sigma_q \in G} \oplus \mathbb{Z}[G][\sigma_1, \dots, \sigma_q]$$

For $q = 0$ we put $X_0 = X_{-1} = \mathbb{Z}[G][1]$, so that $X_0$ is a finite free $\mathbb{Z}[G]$-module with a basis consisting of a single element $1 \in \mathbb{Z}[G]$ and the $[1]$ is called empty cell. So from the definition we have that $\dots, X_{-2}, X_{-1}, X_0, X_1, X_2, \dots$ are free $G$-modules and the maps

$$\epsilon : X_0 \to \mathbb{Z},\ with\ \epsilon(\sum_{\sigma \in G} n_\sigma \sigma) = \sum_{\sigma \in G} n_\sigma$$

which is called augmentation map and

$$\mu : \mathbb{Z} \to X_{-1},\ where\ \mu(n) = nN_G$$

which is called co-augmentation, are $G$-homomorphisms. Thereafter we will define the homomorphisms $d_q$. It suffices to give the values of $d_q$ on the free generators $[\sigma_1, \dots, \sigma_q]$. Now we define:

$\rightsquigarrow$ $d_0([1]) = N_G$, for $q = 0$

$\rightsquigarrow$ $d_1([\sigma]) = \sigma[1] - [1]$, for $q = 1$

$$\begin{aligned} \rightsquigarrow d_q([\sigma_1, \dots, \sigma_q]) &= \sigma_1[\sigma_2, \dots, \sigma_q] \\ &+ \sum_{i=1}^{q-1} (-1)^i [\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma_{i+1}, \sigma_{i+2}, \dots, \sigma_q] \\ &+ (-1)^q [\sigma_1, \dots, \sigma_{q-1}],\ for\, q > 1 \end{aligned}$$

$\rightsquigarrow$ $d_{-1}([1]) = \sum_{\sigma \in G} (\sigma^{-1}[\sigma] - [\sigma]),\ for\, q = -1$

$$\begin{aligned} \rightsquigarrow d_{-q-1}([\sigma_1, \dots, \sigma_q]) &= \sum_{\sigma \in G} \sigma^{-1}[\sigma, \sigma_1, \dots, \sigma_q] + \\ &+ \sum_{\sigma \in G} \sum_{i=1}^{q} (-1)^i [\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma, \sigma^{-1}, \sigma_{i+1}, \dots, \sigma_q] \\ &+ \sum_{\sigma \in G} (-1)^{q+1} [\sigma_1, \dots, \sigma_q, \sigma],\ for\ -q-1 < -1 \end{aligned}$$

According to the above definition we have construct the complex

$$\begin{tikzcd}
\cdots & X_{-3} \arrow[l] & X_{-2} \arrow[l, "d_{-2}"'] & X_{-1} \arrow[l, "d_{-1}"'] & & X_0 \arrow[ll, "d_0"'] \arrow[dl, "\epsilon"] & X_1 \arrow[l, "d_1"'] & X_2 \arrow[l, "d_2"'] & \cdots \arrow[l] \\
& & & & \mathbb{Z} \arrow[ul, "\mu"] \arrow[dl] & & & & \\
& & & 0 & & 0 \arrow[ul] & & &
\end{tikzcd}$$

which is called **standard complex** of $G$. We can prove that $(X, d, \epsilon, \mu)$ forms a complete free resolution of $G$. By construct of standard complex of $G$ we have that $X_q$ are free $G$-modules, the maps $\epsilon, \mu, d_q$ are $G$-homomorphisms and $d_0 = \mu \circ \epsilon$, since $\mu \circ \epsilon(1) = \mu(1) = N_G = d_0([1])$. It remains to show that the sequence is exact. For its proof we use algebraic topology. Its proof is complicated so we skip it. Thus if we have a group $G$, we can construct at least one $G$-complex which is the standard $G$-complex and from this we define the cohomology groups.

### Cohomology group of $G$-module A

Let $G$ be a finite group and $A$ be a $G$-module. Let also $(X, d, \epsilon, \mu)$ be a $G$-complex. We define

$$A_q := Hom_G(X_q, A), \ q \in \mathbb{Z}$$

The elements of $A_q$ are $G$-homomorphisms from $X_q$ to $A$ and they are called $q$-cochains of $A$. From the exact sequence

$$\cdots \longleftarrow X_{-3} \xleftarrow{d_{-2}} X_{-2} \xleftarrow{d_{-1}} X_{-1} \xleftarrow{d_0} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \longleftarrow \cdots$$

is defined the sequence

$$\cdots \longrightarrow A_{-3} \xrightarrow{\partial_{-2}} A_{-2} \xrightarrow{\partial_{-1}} A_{-1} \xrightarrow{\partial_0} A_0 \xrightarrow{\partial_1} A_1 \xrightarrow{\partial_2} A_2 \xrightarrow{\partial_3} \cdots$$

where $d : X \to X, 1 : A \to A$ are $G$-homomorphisms and $\partial = (d, 1)$. According to proposition 3.2.8 we have that $\partial = (d, 1)$ is an endomorphism of $Hom_G(X, A)$. Since $d_q \circ d_{q+1} = 0$, then we have that $\partial_{q+1} \circ \partial_q(\varphi) = \partial_{q+1}(\partial_q(\varphi)) = \partial_{q+1}(1 \circ \varphi \circ d_q) = \partial_{q+1}(\varphi \circ d_q) = 1 \circ \varphi \circ d_q \circ d_{q+1} = \varphi \circ 0 = 0$. That is $\partial_{q+1} \circ \partial_q = 0$ and then $Im\partial_q \subseteq Ker\partial_{q+1}$. Also from the above we have that $(Hom_G(X, A), \partial, +1)$ is a differential graded group of cohomological type.

***Definition* 3.3.2.** *We define*

$$\mathcal{C}_q = \mathcal{C}^q(G, A) = Ker\partial_{q+1}$$

*the group of* ***q-cocycles*** *of G in $A$ and*

$$\mathcal{B}_q = \mathcal{B}^q(G, A) = Im\partial_q$$

*the group of* ***q-coboundaries*** *of G in $A$.*

Now we can define the cohomology group of $G$ in $A$.

***Definition* 3.3.3.** *The qth derived group*

$$\mathcal{H}^q(G, A) = \mathcal{C}_q / \mathcal{B}_q$$

*is known as* ***qth cohomology group of G in A***.

Strictly speaking, the cohomology groups should be denoted in such a way as to indicate their dependence on the $G$-complex. It can be shown that the cohomology groups are independent (up to isomorphism) of the choice of $G$-complex.

Now we try to analyze the sense of cohomology group. The group of $q$-cochains $A_q = Hom_G(X_q, A)$ is the set of all $G$-homomorphisms $f : X^q \to A$. Since the $q$-cells $[\sigma_1, \dots, \sigma_q]$ are free generators of $X_q$, then the $G$-homomorphism $f : X_q \to A$ is determined by the values of $f$ in $q$-cells $[\sigma_1, \dots, \sigma_q]$. Thus, we can consider every cochain as a function $f : \underbrace{G \times \dots \times G}_{q-times} \to A$. According to proposition 3.2.10 we have that

$$A_0 = Hom_G(X_0, A) = Hom_G(\mathbb{Z}[G], A) \cong A$$

as additive groups. Similarly,

$$A_{-1} = Hom_G(X_{-1}, A) \cong A$$

since $X_{-1} = \mathbb{Z}[G]$. From the definition of $d_q$ we have that the maps $\mathfrak{d}_q$ in the sequence

$$\cdots \longrightarrow A_{-3} \xrightarrow{\mathfrak{d}_{-2}} A_{-2} \xrightarrow{\mathfrak{d}_{-1}} A_{-1} \xrightarrow{\mathfrak{d}_0} A_0 \xrightarrow{\mathfrak{d}_1} A_1 \xrightarrow{\mathfrak{d}_2} A_2 \xrightarrow{\mathfrak{d}_3} \cdots$$

verify the following:

$\rightsquigarrow$ $\mathfrak{d}_0(f) = f \circ d_0 = N_G f, \ f \in A_{-1} \cong A$

$$\begin{aligned} \rightsquigarrow (\mathfrak{d}_1 f)[\sigma] &= (f \circ d_1)[\sigma] = f(\sigma[1] - [1]) \\ &= \sigma f - f, \ \ \forall f \in A_0 = A, \forall \sigma \in G \end{aligned}$$

$$\begin{aligned} \rightsquigarrow (\mathfrak{d}_q f)([\sigma_1, \dots, \sigma_q]) &= \sigma_1 f([\sigma_2, \dots, \sigma_q]) \\ &+ \sum_{i=1}^{q+1} (-1)^i f([\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma_{i+1}, \sigma_{i+2}, \dots, \sigma_q]) \\ &+ (-1)^q f([\sigma_1, \dots, \sigma_{q-1}]), \ \ for\ q > 1, f \in A_{q-1} \end{aligned}$$

$\rightsquigarrow$ $(\mathfrak{d}_{-1} f)([1]) = \sum_{\sigma \in G} \sigma^{-1} f([\sigma]) - f([\sigma]), \ \ for\ f \in A_{-2}$

$$\begin{aligned} \rightsquigarrow (\mathfrak{d}_{-q-1} f)([\sigma_1, \dots \quad , \sigma_{q-1}]) &= \sum_{\sigma \in G} \sigma^{-1} f([\sigma, \sigma_1, \dots, \sigma_{q-1}]) + \\ &+ \sum_{\sigma \in G} \sum_{i=1}^{q} (-1)^i f([\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma, \sigma^{-1}, \sigma_{i+1}, \dots, \sigma_{q-1}]) \\ &+ \sum_{\sigma \in G} (-1)^{q+1} f([\sigma_1, \dots, \sigma_{q-1}, \sigma]), \ \ for\ q > 0, f \in A_{-q-2} \end{aligned}$$

## 3.4 Low Dimensional Cohomology Group

As seen in the definition of group cohomology, it is in general painful to find the $nth$ cohomology group for an arbitrary finite group $G$. In general the low dimension cohomology groups are useful in algebraic applications.

$\rightsquigarrow$ **The group** $\mathcal{H}^{-1}(G,A)$

We know that $\mathcal{H}^{-1}(G,A)=\mathcal{C}_{-1}/\mathcal{B}_{-1}$ where

$$\begin{aligned}\mathcal{C}_{-1} &= Ker\mathfrak{d}_0=\{a\in A_{-1}=A:\ \mathfrak{d}_0(a)=0\}\\ &= \{a\in A:\ N_G a=0\}={}_{N_G}A\end{aligned}$$

and

$$\begin{aligned}\mathcal{B}_{-1} &= Im\mathfrak{d}_{-1}=\{a\in A_{-1}=A:\ a=\mathfrak{d}_{-1}(f),\, f\in A_{-2}\}\\ &= \{a\in A:\ a=\sum_{\sigma\in G}[\sigma^{-1}f[\sigma]-f[\sigma]],\, f\in A_{-2}\}=I_G A\end{aligned}$$

Thus,

$$\mathcal{H}^{-1}(G,A)={}_{N_G}A/I_G A$$

***Corollary* 3.4.1.** *If $G$ is a finite group with order $n$, then*

$$\mathcal{H}^{-1}(G,\mathbb{Z})=<0>$$

*Proof.* It is clear that $\mathcal{H}^{-1}(G,\mathbb{Z})={}_{N_G}\mathbb{Z}/I_G A\mathbb{Z}$ and

$$\begin{aligned}{}_{N_G}\mathbb{Z} &= \{a\in\mathbb{Z}\mid N_G a=0\}=\{a\in\mathbb{Z}\mid\sum_{\sigma\in G}\sigma a=0\}\\ &= \{a\in\mathbb{Z}\mid\sum_{\sigma\in G}a=0\}\end{aligned}$$

since the action of $G$ in $\mathbb{Z}$ is the trivial, and then ${}_{N_G}\mathbb{Z}=\{a\in\mathbb{Z}\,|\,na=0\}$, where $n$ is the order of $G$, so ${}_{N_G}\mathbb{Z}=<0>$ and

$$I_G\mathbb{Z}=\{\sum_{\sigma\in G}n_\sigma(\sigma a_\sigma-a_\sigma),\, a_\sigma\in\mathbb{Z}\}=\{\sum_{\sigma\in G}n_\sigma(a_\sigma-a_\sigma),\, a_\sigma\in\mathbb{Z}\}$$

since the action of $G$ in $\mathbb{Z}$ is the trivial, and then $I_G\mathbb{Z}=<0>$. Therefore,

$$\mathcal{H}^{-1}(G,\mathbb{Z})=<0>$$

□

***Corollary* 3.4.2.** *If $G$ is a finite group with order $n$, then*

$$\mathcal{H}^{-1}(G,\mathbb{Q}/\mathbb{Z})=(\frac{1}{n}\mathbb{Z})/\mathbb{Z}$$

*Proof.* We have that $\mathcal{H}^{-1}(G,A) = {}_{N_G}A/I_GA$, where $A = \mathbb{Q}/\mathbb{Z}$. Then

$$\begin{aligned} {}_{N_G}A &= \{a \in A : N_Ga = 0\} = \{a \in \mathbb{Q}/\mathbb{Z} : N_Ga \in \mathbb{Z}\} \\ &= \{a \in \mathbb{Q}/\mathbb{Z} : \sum_{\sigma \in G} \sigma a \in \mathbb{Z}\} = \{a \in \mathbb{Q}/\mathbb{Z} : \sum_{\sigma \in G} a \in \mathbb{Z}\} \\ &= \{a \in \mathbb{Q}/\mathbb{Z} : na \in \mathbb{Z}\} = \{a \in \mathbb{Q}/\mathbb{Z} : a \in \frac{1}{n}\mathbb{Z}\} \\ &= \{a \in \mathbb{Q}/\mathbb{Z} : a = \frac{1}{n}\mathbb{Z} + \mathbb{Z}\} = (\frac{1}{n}\mathbb{Z}/\mathbb{Z}) \end{aligned}$$

and

$$I_GA = \{\sum_{\sigma \in G} n_\sigma(\sigma a_\sigma - a_\sigma),\, a_\sigma \in \mathbb{Q}/\mathbb{Z}\} = \{\sum_{\sigma \in G} n_\sigma(a_\sigma - a_\sigma),\, a_\sigma \in A\} =< 0 >$$

Hence,

$$\mathcal{H}^{-1}(G,A) = {}_{N_G}A/I_GA = (\frac{1}{n}\mathbb{Z})/\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$$

□

$\rightsquigarrow$ **The group** $\mathcal{H}^0(G,A)$

We have that

$$\mathcal{H}^0(G,A) = \mathcal{C}_0/\mathcal{B}_0$$

where

$$\begin{aligned} \mathcal{C}_0 &= Ker\mathfrak{d}_1 = \{a \in A_0 = A : \mathfrak{d}_1(a) = 0\} \\ &= \{a \in A : \sigma a - a = 0, \forall \sigma \in G\} = \{a \in A : \sigma a = a, \forall \sigma \in G\} = A^G \end{aligned}$$

and

$$\begin{aligned} \mathcal{B}_0 &= Im\mathfrak{d}_0 = \{a \in A_0 = A : a = \mathfrak{d}_0(f),\ f \in A_{-1} = A\} \\ &= \{a \in A : a = N_Gf,\ f \in A\} = N_GA \end{aligned}$$

Therefore,

$$\mathcal{H}^0(G,A) = A^G/N_GA$$

which is called norm residue group and it is very important in class field theory.

***Corollary* 3.4.3.** *Let $G$ be a finite group of order $n$ and $A$ be a $G$-module where the action of $G$ on $A$ is the trivial, then*

$$\mathcal{H}^0(G,A) = A/nA$$

*In particular $\mathcal{H}^0(G,\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ and $\mathcal{H}^0(G,\mathbb{Q}/\mathbb{Z}) = (\mathbb{Q}/\mathbb{Z})/n(\mathbb{Q}/\mathbb{Z}) =< 0 >$*

*Proof.* We have that

$$\mathcal{H}^0(G,A) = A^G/N_G A$$

where $A^G = A$ and

$$\begin{aligned} N_G A &= \{N_G a \,|\, a \in A\} = \{\sum_{\sigma\in G} \sigma a \mid a \in A\} \\ &= \{\sum_{\sigma\in G} a \,|\, a \in A\} = \{na \,|\, a \in A\} = nA \end{aligned}$$

Hence,

$$\mathcal{H}^0(G,A) = A/nA$$

and therefore, $\mathcal{H}^0(G,\mathbb{Z}) = \mathbb{Z}/nA\mathbb{Z}$ and $\mathcal{H}^0(G,\mathbb{Q}/\mathbb{Z}) = (\mathbb{Q}/\mathbb{Z})/n(\mathbb{Q}/\mathbb{Z}) =< 0 >$ □

We note that $\mathcal{H}^0(G,\mathbb{Q}/\mathbb{Z}) = \mathcal{H}^{-1}(G,\mathbb{Z})$ and $\mathcal{H}^0(G,\mathbb{Z}) = \mathcal{H}^{-1}(G,\mathbb{Q}/\mathbb{Z})$. In general, it can be proved that $\mathcal{H}^r(G,\mathbb{Q}/\mathbb{Z}) \cong \mathcal{H}^{r-1}(G,\mathbb{Z})$ and $\mathcal{H}^r(G,\mathbb{Z}) \cong \mathcal{H}^{r-1}(G,\mathbb{Q}/\mathbb{Z})$.

We assume that $L/K$ is a finite extension of order $n$ and $\sigma$ is a $K$-automorphism of $L$. If $L/K$ is a Galois extension then $G = Gal(L/K)$ and the fixed field of $G$ $\mathcal{F}(G) = \mathcal{F}ix(G) = K$.

***Corollary* 3.4.4.** *Let $K, L$ be fields and $L/K$ be a Galois extension with Galois group $G = Gal(L/K)$ then*

$$\mathcal{H}^0(G,L^*) \cong K^*/N_{L/K}(L^*)$$

*where $N_{L/K}(L^*) = \{\prod_{\sigma\in G} \sigma(a) \mid a \in L^*\}$ and $L^*$ becomes $G$-module with the natural action.*

*Proof.* We know that

$$\mathcal{H}^0(G,A) = A^G/N_G A$$

So

$$\mathcal{H}^0(G,L^*) = L^{*G}/N_G L^*$$

But $L^{*G} = K^*$, since $L/K$ is Galois and we have that $N_G L^* = \{N_G a \,|\, a \in L^*\} = \{(\prod_{\sigma\in G} \sigma)a \mid a \in L^*\} = \{\prod_{\sigma\in G} \sigma(a) \mid a \in L^*\}$. Thus, $N_G L^* = N_{L/K}(L^*)$ and therefore

$$\mathcal{H}^0(G,L^*) \cong K^*/N_{L/K}(L^*)$$

□

$\rightsquigarrow$ **The group** $\mathcal{H}^1(G,A)$

We know that

$$\mathcal{H}^1(G,A) = \mathcal{C}_1/\mathcal{B}_1$$

where

$$\begin{aligned}\mathcal{C}_1 &= Ker\mathfrak{d}_2 = \{f : G \to A \,|\, \mathfrak{d}_2(f) = 0\} \\ &= \{f : G \to A \,|\, (\mathfrak{d}_2 f)[\sigma,\tau] = \sigma f([\tau]) - f([\sigma\tau]) + f([\sigma]) = 0\} \\ &= \{f : G \to A \,|\, \sigma f(\tau) - f(\sigma\tau) + f(\sigma) = 0\}\end{aligned}$$

***Definition* 3.4.5.** *Let A be a G-module. The map $f : G \to A$ will be called* ***crossed homomorphism*** *if $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$, for every $\sigma, \tau \in G$*

Thus, $\mathcal{C}_1 = \{crossed\ homomorphisms\}$.
and

$$\begin{aligned}\mathcal{B}_1 &= Im\mathfrak{d}_1 = \{f : G \to A \mid \exists a \in A\ such\ that\ \mathfrak{d}_1(a) = f\} \\ &= \{f : G \to A \mid \exists a \in A\ such\ that\ (\mathfrak{d}_1 a)([\sigma]) = f([\sigma])\} \\ &= \{f : G \to A \mid \exists a \in A\ such\ that\ \sigma a - a = f(\sigma),\ \forall \sigma \in G\}\end{aligned}$$

***Definition* 3.4.6.** *Let A be a G-module. The map $f : G \to A$ will be called* ***principal crossed homomorphism*** *if $f(\sigma) = \sigma a - a$, for every $\sigma \in G$ and $a \in A$.*

Hence, $\mathcal{B}_1 = \{principal\ crossed\ homomorphisms\}$ and therefore

$$\mathcal{H}^1(G,A) = \frac{\{f : G \to A \,|\, f\, crossed\ homomorphism\}}{\{f : G \to A \mid f\, principal\ crossed\ homomorphism\}}$$

***Remark* 3.4.7.** *1) If G acts trivially on A, then*

$$\mathcal{H}^1(G,A) = Hom(G,A)$$

*2) If $A = \mathbb{Q}/\mathbb{Z}$ then*

$$\mathcal{H}^1(G,\mathbb{Q}/\mathbb{Z}) = \chi(G)$$

*where $\chi(G)$ is the character group of G.*

*Proof.* 1) $\mathcal{B}_1 =< 0 >$ and

$$\begin{aligned}\mathcal{C}_1 &= \{f : G \to A \mid f(\sigma\tau) = \sigma f(\tau) + f(\sigma),\ \forall \sigma,\tau \in G\} \\ &= \{f : G \to A \mid f(\sigma\tau) = f(\tau) + f(\sigma),\ \forall \sigma,\tau \in G\} = Hom(G,A)\end{aligned}$$

2) G acts trivially on $A$, so then we have that

$$\mathcal{H}^1(G,A) = Hom(G,\mathbb{Q}/\mathbb{Z}) = \chi(G)$$

□

***Theorem* 3.4.8.** *Let $L/K$ Galois extension and $G = Gal(L/K)$, then*

$$\mathcal{H}^1(G, L^*) =< 1 >$$

*This means that every crossed homomorphism is a principal crossed homomorphism.*

*Proof.* A proof of this can be found in my diploma thesis [21], Chapter 2. □

***Corollary* 3.4.9.** *(Hilbert's theorem 90) Let $L/K$ is a cyclic extension of degree $n$ with Galois group $G = Gal(L/K) =< \sigma >$. If $a \in L$, then $N_{L/K}(a) = 1$ if and only if there exists $\beta \in L^*$ such that $a = \frac{\sigma(\beta)}{\beta}$, where $N_{L/K} = \prod\limits_{\sigma \in G} \sigma(a)$.*

*Proof.* A proof of this can be found in my diploma thesis [21], Chapter 2. □

***Corollary* 3.4.10.** *Let $L/K$ is a Galois extension with Galois group $G = Gal(L/K)$, then*

$$\mathcal{H}^{-1}(G, L^*) = \frac{\{a \in L^* \,|\, N_{L/K}(a) = 1\}}{\{\prod\limits_{\sigma \in G} a_\sigma^{\sigma - 1} \,|\, a_\sigma \in L^*\}}$$

*If $L/K$ is a cyclic extension then $\mathcal{H}^{-1}(G, L^*) = 0$.*

*Proof.* We know that

$$\mathcal{H}^{-1}(G, L^*) = {}_{N_G}L^*/I_G L^*$$

We have that

$$\begin{aligned} {}_{N_G}L^* &= \{a \in L^* \,:\, N_G a = 1\} = \{a \in L^* \,:\, \prod_{\sigma \in G} \sigma(a) = 1\} \\ &= \{a \in L^* \,:\, N_{L/K}(a) = 1\} \end{aligned}$$

since $(L^*, \cdot)$ is a $G$-module, and

$$I_G L^* = \{\prod_{\sigma \in G} a_\sigma^{\sigma - 1} \,|\, a_\sigma \in L^*\} = \{\prod_{\sigma \in G} \frac{\sigma(a_\sigma)}{a_\sigma} \,|\, a_\sigma \in L^*\}$$

according to corollary 3.4.9

If now $L/K$ is cyclic extension, then

$$\begin{aligned} \{a \in L^* \,:\, N_{L/K}(a) = 1\} &= \{a \in L^* \,|\, a = \frac{\sigma(\beta)}{\beta}, \beta \in L^*\} \\ &\subseteq \{\prod_{\sigma \in G} \frac{\sigma(a_\sigma)}{a_\sigma} \,|\, a_\sigma \in L^*\} \end{aligned}$$

Thus, $\mathcal{H}^{-1}(G, L^*) = 0$ □

$\rightsquigarrow$ **The group** $\mathcal{H}^2(G, A)$

We know that

$$\mathcal{H}^2(G, A) = \mathcal{C}_2/\mathcal{B}_2$$

where

$$\begin{aligned} \mathcal{C}_2 &= Ker\mathfrak{d}_3 = \{f : G \times G \,|\, \mathfrak{d}_3(f) = 0\} \\ &= \{f : G \times G \,|\, \sigma f(\tau, \rho) + f(\sigma, \tau\rho) = f(\sigma\tau, \rho) + f(\sigma, \tau), \, \forall \sigma, \tau, \rho \in G\} \end{aligned}$$

***Definition*** **3.4.11.** *Let* $A$ *be a* $G$*-module. The map* $f : G \times G \to A$ *such that* $\sigma f(\tau, \rho) + f(\sigma, \tau\rho) = f(\sigma\tau, \rho) + f(\sigma, \tau)$*, for every* $\sigma, \tau, \rho \in G$*, will be called* ***factor sets****.*

Thus,

$$\mathcal{C}_2 = \{f : G \times G \,|\, f \ factor \ sets\}$$

In addition, $f \in \mathcal{B}_2 = Im\mathfrak{d}_2$ if and only if there exists $g : G \to A$ such that $\mathfrak{d}_2(g) = f$ if and only if there exists $g : G \to A$ such that $\sigma g(\tau) - g(\sigma\tau) + g(\sigma) = f(\sigma, \tau)$.

***Definition*** **3.4.12.** *Let* $A$ *be a* $G$*-module. The map* $f : G \times G \to A$ *satisfying that there exists* $g : G \to A$ *such that* $\sigma g(\tau) - g(\sigma\tau) + g(\sigma) = f(\sigma, \tau)$ *will be called* ***splitting factor sets****.*

Therefore,

$$\mathcal{H}^2(G, A) = \frac{\{factor \ sets\}}{\{splitting \ factor \ sets\}}$$

If we denote $f(\sigma, \tau)$ as $a_{\sigma,\tau}$ and we consider the $G$-module $A$ multiplicative, then we have that

$$\{factor \ sets\} = \{\{a_{\sigma,\tau} \,|\, a^{\sigma}_{\tau,\rho} a_{\sigma,\tau\rho} = a_{\sigma\tau,\rho} a_{\sigma,\tau}\}$$

and

$$\{splitting \ factor \ sets\} = \left\{ \begin{array}{cc} \{a_{\sigma,\tau}\} & | \ there \ exists \ a \ map \\ & \{b_p\} \ such \ that \ b^{\sigma}_{\tau} b^{-1}_{\sigma\tau} b_{\sigma} = a_{\sigma\tau} \end{array} \right\}$$

The $3rd$ cohomology group $\mathcal{H}^3(G, A)$ was calculated (for the first time) by Teichmüller (1940). Moreover it has been proved that

$$\mathcal{H}^{-2}(G, \mathbb{Z}) = G/[G, G]$$

where $[G, G]$ is the commutator subgroup of $G$.

## 3.5 Cyclic Cohomology

So far we have defined the basic cohomological maps and have studied some properties of them. Now we will prove some central theorems of cohomology theory. In this section we assume that $G$ is a finite cyclic group.

***Proposition* 3.5.1.** *Let $G$ is a cyclic group of order $n$ with generator $g$. If*

$$0 \to A \overset{i}{\to} B \overset{j}{\to} C \to 0$$

*is an exact sequence of G-modules and G-homomorphisms, then we have an exact hexagon*

$$\begin{tikzcd}
 & \mathcal{H}^0(G,A) \arrow[r, "f_1"] & \mathcal{H}^0(G,B) \arrow[dr, "f_2"] & \\
\mathcal{H}^{-1}(G,C) \arrow[ur, "f_6"] & & & \mathcal{H}^0(G,C) \arrow[dl, "f_3"] \\
 & \mathcal{H}^{-1}(G,B) \arrow[ul, "f_5"] & \mathcal{H}^{-1}(G,A) \arrow[l, "f_4"'] &
\end{tikzcd}$$

*Proof.* We have proved that $\mathcal{H}^0(G,A) = A^G/N_GA$ and $\mathcal{H}^{-1}(G,A) = {}_{N_G}A/I_GA$. We must show that $f_i$ is well-defined homomorphisms for every $i = 1, \dots, 6$ and $Kerf_{i+1} = Imf_i$, with $i = 1, \dots, 5$, $Kerf_1 = Imf_6$. The maps $f_i$ with $i = 1, \dots, 6$ are defined as follows:

$$\begin{array}{llcl} \rightsquigarrow f_1: & \mathcal{H}^0(G,A) \cong A^G/N_GA & \to & \mathcal{H}^0(G,B) \cong B^G/N_GB \\ & \quad a + N_GA & \mapsto & \quad i(a) + N_GB \end{array}$$

$f_1$ is well-defined, since if $a_1 + N_GA = a_2 + N_GA$, then $a := a_1 - a_2 \in N_GA$. We would like to show that $f_1(a_1 + N_GA) = f_1(a_2 + N_GA)$, that is $i(a_1) + N_GB = i(a_2) + N_GB$ and then $i(a) = i(a_1 - a_2) \in N_GB$. So it suffices to show that if $a \in N_GA$, then $i(a) \in N_GB$, with $a \in A^G$. Let $a \in A^G$, which means that $ga = a$. Then, $i(a) = i(ga) = gi(a)$, that is $i(a) \in B^G$. If $a \in N_GA$, then $a = \sum_{\sigma \in G} \sigma(t)$, with $t \in A$. So

$$\begin{aligned} f_1(a + N_GA) &= i(a) + N_GB = \sum_{\sigma \in G} i(\sigma(t)) + N_GB \\ &= \sum_{\sigma \in G} \sigma(i(t)) + N_GB = N_GB \end{aligned}$$

since $i(t) \in B$. Also, $f_1$ is homomorphism, since

$$\begin{aligned} f_(a + N_GA + b + N_GA) &= f_1(a + b + N_GA) = i(a+b) + N_GB \\ &= i(a) + N_GB + i(b) + N_GB \\ &= f_1(a + N_GA) + f_1(b + N_GA) \end{aligned}$$

$$\begin{array}{lrcl} \rightsquigarrow f_2: & \mathcal{H}^0(G,B) & \to & \mathcal{H}^0(G,C) \\ & b+N_GB & \mapsto & i(b)+N_GC \end{array}$$

Similar to $f_1$ we can show that $f_2$ is a well-defined homomorphism.

$$\begin{array}{lrcl} \rightsquigarrow f_4: & \mathcal{H}^{-1}(G,A) & \to & \mathcal{H}^{-1}(G,B) \\ & a+I_GA & \mapsto & i(a)+I_GB \end{array}$$

We will show that $f_4$ is well-defined. It suffices to show that if $a \in I_GA$, then $i(a) \in I_Gb$, with $a \in {}_{N_G}A$

$$a \in {}_{N_G}A \Rightarrow N_GA = 0 \Rightarrow \sum_{\sigma\in G} \sigma a = 0$$

Then $N_Gi(a) = \sum_{\sigma\in G}\sigma(i(a)) = \sum_{\sigma\in G} i(\sigma(a)) = i(\sum_{\sigma\in G}\sigma(a)) = i(0) = 0$, which means that $i(a) \in a \in {}_{N_G}B$. If $a \in I_GA$, then $a = \sum_{\sigma\in G}(\sigma t - t)$, with $t \in A$. So

$$\begin{aligned} f_4(a+I_GA) &= i(a)+I_GB = i(\sum_{\sigma\in G}(\sigma t - t)) + I_GB \\ &= \sum_{\sigma\in G}[i(\sigma t) - i(t)] + I_GB \\ &= \sum_{\sigma\in G}[\sigma i(t) - i(t)] + I_GB = I_GB \end{aligned}$$

since $i(t) \in B$

In addition, $f_4$ is homomorphism, since

$$\begin{aligned} f_4(a+I_GA+b+I_GA) &= f_4(a+b+I_GA) = i(a+b)+I_GB \\ &= i(a)+I_GB+i(b)+I_GB \\ &= f_4(a+I_GA)+f_4(b+I_GA) \end{aligned}$$

$$\begin{array}{lrcl} \rightsquigarrow f_5: & \mathcal{H}^{-1}(G,B) & \to & \mathcal{H}^{-1}(G,C) \\ & b+I_GB & \mapsto & j(b)+I_GC \end{array}$$

Similar to $f_4$, we can prove that $f_5$ is a well defined homomorphism.

$$\begin{array}{lccc} \rightsquigarrow f_3: & \mathcal{H}^0(G,C) \cong C^G/N_GC & \to & \mathcal{H}^{-1}(G,A) \cong {}_{N_G}A/I_GA \\ & c+N_GC & \mapsto & a+I_GA \end{array}$$

is defined as follows: Let $c \in C^G$. Then there exists $b \in B$ such that $j(b) = c$, since

$j$ is surjective. Also, $j(gb-b) = gj(b) - j(b) = gc - c = 0$ and

$$\begin{aligned} N_G(gb-b) &= \sum_{g'\in G} g'(gb-b) = \sum_{g'\in G} g'(gb) - \sum_{g'\in G} g'b \\ &= \sum_{g'\in G} (g'g)b - \sum_{g'\in G} g'b \\ &= \sum_{g'\in G} g'b - \sum_{g'\in G} g'b = 0 \end{aligned}$$

since $G$ is a finite group. We have that $j(gb-b) = 0$ , which means that $gb - b \in Kerj = Imi$, so then there exists $a \in A$ such that $i(a) = gb - b$. Now we define

$$f_3(c + N_G C) = a + I_G A$$

with $j(b) = c, b \in B$, $j(gb-b) = 0$ and $i(a) = gb - b$. We will show that $f_3$ is well-defined. It suffices to show that if $c \in N_G C$, then $a \in I_G A$. Then, $N_G(i(a)) = N_G(gb-b) = 0$ and this implies that $i(N_G a) = 0$, so then $N_G a = 0$, since $i$ is injective. Thus, $a \in {}_{N_G}A$. If $c \in N_G C$, then $c = N_G t = \sum_{\sigma\in G} \sigma t$, with $t \in C$. So there exists $b \in B$ such that $j(b) = c$, since $j$ is surjective, and $f_3(c + N_G C) = a + I_G A$, where i(a)=gb-b, by construction of $f_3$. Since $t \in C$, then $t = j(v)$, for some $v \in B$, which implies that $j(b) = c = \sum_{\sigma\in G} \sigma t = \sum_{\sigma\in G} \sigma j(v) = j(\sum_{\sigma\in G} \sigma u)$, so then

$$j(b) = j(\sum_{\sigma\in G} \sigma u) \Rightarrow j(\sum_{\sigma\in G} \sigma u - b) = 0$$

This means that $\sum_{\sigma\in G} \sigma u - b \in Kerj = Imi$, which implies that there exists $x \in A$ such that $i(x) = \sum_{\sigma\in G} \sigma u - b = v + gv + \cdots + g^{n-1}v - b$. Then $i(gx) = gv + g^2v + \cdots + v - gb$. So, $i(x) - i(gx) = gb - b = i(a)$ and then $x - gx = a$, since $i$ is injective, which means that $a \in I_G A$. Thus, $f_3(c + N_G C) = a + I_G A = I_G A$. It remains to show that $f_3$ is homomorphism. Let $c, d \in C^G$.

$$f_3(c + N_G C + d + N_G C) = f_3(c + d + N_G C) = a + I_G A$$

Since, $c + d \in C^G$ we have that there exists $b \in B$ such that $j(b) = c + d$ and $j(gb-b) = 0$, $i(a) = gb - b \quad (I)$. Also, since $c, d \in C^G$ there exist $b_c, b_d \in B$ such that $j(b_c) = c$ and $j(b_d) = d$. We know that $j$ is homomorphism, so then

$$\begin{aligned} &j(b_c + b_d) = j(b_c) + j(b_d) = c + d = j(b) \\ &\Rightarrow j(b_c - b_d - b) = 0 \Rightarrow b_c - b_d - b \in Kerj = Imi \end{aligned}$$

This means that there exists $a' \in A$ such that

$$i(a') = b_c - b_d - b \quad (II)$$

In addition, $j(gb_c - b_c) = j(gb_d - b_d) = 0$, which implies that there exists $a_d \in A$ such that $i(a_d) = gb_d - b_d$, and then $i(a_c + a_d) = g(b_c - b_c + gb_d - b_d) = g(b_c + b_d) - (b_c + b_d)$. We multiply the equation $(II)$ by $g$ and then

$$\begin{aligned}
& gb_c - gb_d - gb = gi(a') \Rightarrow g(b_c - b_d) - gb = gi(a') \\
& \Rightarrow i(a_c + a_d) + b_c + b_d - gb = gi(a') \\
& \overset{(II)}{\Rightarrow} i(a_c + a_d) + i(a') + b - gb = gi(a') \\
& \overset{(I)}{\Rightarrow} i(a_c + a_d) + i(a') + b - i(a) - b = gi(a') \\
& \Rightarrow i(a_c + a_d) - i(a) = i(ga') - i(a') \\
& \Rightarrow i(a_c + a_d - a) = i(ga' - a')
\end{aligned}$$

This implies that $a_c + a_d - a = ga' - a'$, since $i$ is injective, and then $a_c + a_d - a \in I_G A$, which implies that $a_c + a_d + I_G A = a + I_G A$. Hence, $f_3(c + N_G C) + f_3(d + N_G C) = f_3(c + N_G C + d + N_G C)$.

$\rightsquigarrow f_6 : \quad \mathcal{H}^{-1}(G, C) \cong {}_{N_G}C/I_G C \quad \rightarrow \quad \mathcal{H}^0(G, A) \cong A^G/N_G A$

Firstly we will define the $f_6$. Let $c \in {}_{N_G}C$, then there exists $b \in B$ such that $j(b) = c$. We have that $j(N_G b) = N_G(j(b)) = N_G(c) = 0$, which means that $N_G b \in Kerj = Imi$. So there exists $a \in A$ such that $i(a) = N_G b$. Hence, we define $f_6(c + I_G C) = a + N_G A$, where $j(b) = c, b \in B$ and $i(a) = N_G b$. We will prove that $f_6$ is well-defined. It suffices to show that if $c \in I_G C$, then $a \in N_G A$. We have that $a \in A^G$ and

$$\begin{aligned}
i(ga) &= gi(a) = g(N_G b) = g\sum_{\sigma\in G}\sigma b \\
&= \sum_{\sigma\in G} g\sigma b = \sum_{\sigma\in G}\sigma b = N_G b = i(a)
\end{aligned}$$

This implies that $i(ga) = i(a)$ and then $ga = a$, since $i$ is injective, that is $a \in A^G$. If $c \in I_G C$, then $c = \sum_{\sigma\in G}(\sigma t - t)$ for some $t \in C$, so there exists $v \in B$ such that $j(v) = t$, since $j$ is surjective. Thus,

$$\begin{aligned}
& j(b) = c = \sum_{\sigma\in G}(\sigma t - t) = \sum_{\sigma\in G}(\sigma j(v) - j(v)) = j(\sum_{\sigma\in G}(\sigma v - v)) \\
& \Rightarrow j(\sum_{\sigma\in G}(\sigma v - v) - b) = 0 \Rightarrow -\sum_{\sigma\in G}(\sigma v - v) + b \in Kerj = Imi
\end{aligned}$$

This means that there exists $x \in A$ such that

$$i(x) = b - \sum_{\sigma\in G}(\sigma v - v) \quad (*)$$

We apply $N_G$ on both sides of equation $(*)$, so

$$\begin{aligned}
N_G i(x) &= N_G(b - \sum_{\sigma\in G}(\sigma v - v)) \Rightarrow \\
i(N_G x) &= N_G(b) - \sum_{\sigma\in G}[N_G(\sigma v) - N_G(v)]
\end{aligned}$$

But $N_G v = \sum_{\sigma \in G} \sigma v = v + gv + \cdots + g^{n-1}v$, $N_G(gv) = gv + g^2 v + \cdots + v$ and $i(a) = N_G b$. Thus, $i(N_G x) = i(a)$, which implies that $N_G x = a$, since $i$ is injective, so then $a \in N_G A$. Therefore, if $c \in I_G C$, then

$$f_6(c + I_G C) = a + N_G A = N_G A$$

It remains to show that $f_6$ is homomorphism. Let $c, d \in {}_{N_G}C$. Then

$$f_6(c + {}_{N_G}C + d + {}_{N_G}C) = f_6(c + d + {}_{N_G}C) = a + N_G A$$

where $i(a) = N_G b, j(b) = c + d$.
Since $c, d \in {}_{N_G}C$, then there exists $b_c \in B$ and $b_d \in B$ such that $j(b_c) = c$, $j(b_d) = d$ and $f_6(c + {}_{N_G}C) = a_c + N_G A$, where $N_G b_c = i(a_c)$, $(j(b_c) = c)$, $f_6(d + {}_{N_G}C) = a_d + N_G A$, where $N_G b_d = i(a_d)$. We claim that $a_c + a_d - a \in N_G A$. Indeed,

$$i(a) = N_G b = \sum_{\sigma \in G} \sigma b = b + gb + ... + g^{n-1}b \quad (III)$$

Then

$$j(b_c) + j(b_d) = j(b_c + b_d) = c + d = j(b)$$
$$\Rightarrow j(b_c + b_d) = j(b) \Rightarrow b_c + b_d - b \in Kerj = Imi$$

This implies that there exists $a' \in A$ such that

$$i(a') = b_c + b_d - b \quad (IV)$$

Additionally,

$$i(a_c) = N_G b_c = b_c + gb_c + ... + g^{n-1}b_c \quad (V)$$

$$i(a_d) = N_G b_d = b_d + gb_d + ... + g^{n-1}b_d \quad (VI)$$

From the equations $(III)$, $(V)(VI)$ we have that

$$i(a_c + a_d - a) = b_c + b_d - b + g(b_c + b_d - b) + ... + g^{n-1}(b_c + b_d - b)$$
$$\overset{(IV)}{\Rightarrow} i(a_c + a_d - a) = i(a') + gi(a') + ... + g^{n-1}i(a') = N_G i(a') = i(N_G a')$$
$$\Rightarrow i(a_c + a_d - a) = i(N_G a')$$

Thus, $a_c + a_d - a = N_G a'$, since $i$ is injective, that is $a_c + a_d - a \in N_G A \Rightarrow a_c + a_d + N_G A = a + N_G A$. Hence, $f_6(c + {}_{N_G}C) + f_6(d + {}_{N_G}C) = f_6(c + d + {}_{N_G}C)$

Therefore all homomorphisms are well-defined. It remains to show the exactness.

$\rightsquigarrow Kerf_1 = Imf_6$

Let $a \in A^G$ such that $f_1(a + N_G A) = 0 \Rightarrow i(a) + N_G B = N_G B \Rightarrow i(a) \in$

$N_GB \Rightarrow i(a) = \sum_{\sigma\in G} gb,\ b \in B$. Let $j(b) = c$, then $f_6(c + I_GC) = a + N_GA$, by the definition of $f_6$. Thus, $Kerf_1 \subseteq Imf_6$. Let now $a + N_GA \in Imf_6$, then there exists $c \in {}_{N_G}C$ such that $f_6(c + I_GC) = a + N_GA$, where $j(b) = c, b \in B$ and $i(a) = N_Gb$. So

$$\begin{aligned} &f_1(a + N_GA) = i(a) + N_GB = N_Gb + N_GB = N_GB \\ &\Rightarrow a + N_GA \in Kerf_1 \end{aligned}$$

that is $Imf_6 \subseteq Kerf_1$

$\rightsquigarrow Kerf_2 = Imf_1$

Let $b + N_GB \in Kerf_2$ so then

$$\begin{aligned} &f_2(b + N_GB) = N_GC \Rightarrow j(b) + N_GC = N_GC \\ &\Rightarrow j(b) \in N_GC \Rightarrow j(b) = \sum_{\sigma\in G} \sigma c \end{aligned}$$

Since $j$ is surjective there exists $b' \in B$ such that $c = j(b')$. So then $j(b) = j(\sum_{i=1}^{n-1} g^ib')$, which implies that $b-\sum_{i=1}^{n-1} g^ib' \in Kerj = Imi$. Thus there exists $a \in A$ such that $i(a) = b-\sum_{i=1}^{n-1} g^ib'$. Then $f_1(a+N_GA) = i(a)+N_GB = b-\sum_{i=1}^{n-1} g^ib' + N_GB = b + N_GB$, that is $b + N_GB \in Imf_1$. Consequently, $Kerf_2 \subseteq Imf_1$. Let now $b + N_GB \in Imf_1$. This means that $f_1(a + N_GA) = b + N_GB$, with $a \in A^G$. Then $f_2(b+N_GB) = f_2(f_1(a+N_GA)) = f_2(i(a)+N_GB) = j(i(a))+N_GC = 0 + N_GC = N_GC$, that is $b + N_GB \in Kerf_2$. Hence, $Imf_1 \subseteq Kerf_2$.

$\rightsquigarrow Kerf_3 = Imf_2$

Let $c + N_GC \in Kerf_3$. That is

$$f_3(c + N_GC) = I_GA \Rightarrow a + I_GA = I_GA \Rightarrow a \in I_GA$$

where $j(b) = c, b \in B,\ j(gb - b) = 0$ and $i(a) = gb - b$. We have that $f_2(b + N_GB) = j(b) + N_GC = c + N_GC$, that is $c + N_GC \in Imf_2$. So then $Kerf_3 \subseteq Imf_2$. Conversely, let $c+N_GC \in Imf_2$, that is $f_2(b+N_GB) = c+N_GC$, for some $b \in B^G$, where $j(b) = c$. Then $f_3(c+N_GC) = a+I_GA$, where $j(b) = c, b \in B^G$, $j(gb - b) = 0$ and $i(a) = gb - b = 0$, since $b \in B^G$, so then $a = 0$, since $i$ is injective. Thus,

$$f_3(c + N_GC) = I_GA \Rightarrow c + N_GC \in Kerf_3$$

That is $Imf_2 \subseteq Kerf_3$.

$\rightsquigarrow Kerf_4 = Imf_3$

Let $a + I_GA \in Kerf_4$, that is $f_4(a + J_GA) = I_GB$. Let $j(b) = c$ then $f_3(c + N_GC) = a' + I_GA$, where $i(a') = gb - b$, $j(gb - b) = 0$. So $f_4(a' + I_GA) = i(a') + I_GB = gb - b + I_GB = I_GB$. This implies that

$$\begin{aligned} &f_4(a + J_GA) = f_4(a' + I_GA) \Rightarrow f_4(a - a' + I_GA) = I_GB \\ &\Rightarrow a - a' + I_GA = I_GA \Rightarrow a + I_GA = a' + I_GA \end{aligned}$$

Thus, $f_3(c + N_GC) = a + I_GA$, that is $a + I_GA \in Imf_3$ and then $Kerf_4 \subseteq Imf_3$. For the converse, let $a + I_GA \in Imf_3$, this means that $f_3(c + N_GC) = a + I_GA$, where $j(b) = c, b \in B$, $i(a) = gb - b$ and $j(gb - b) = 0$. Then, $f_4(a+I_GA) = i(a)+I_GB = gb-b+I_GB = I_GB$, which means that $a+I_GA \in Kerf_4$. Hence, $Imf_3 \subseteq Kerf_4$.

$\rightsquigarrow Kerf_5 = Imf_4$

Let $b + I_GB \in Kerf_5$, that is

$$f_5(b + J_GB) = I_GC \Rightarrow j(b) + I_GC = I_GC \Rightarrow j(b) \in I_GC$$

We have that ${}_{N_G}B \subseteq N_GB \subseteq B^G$. So, $b \in B^G$, which means that $gb = b$, and then $j(gb) = j(b)$. Since, $j(b) \in I_GC$ then $j(b) = \sum_{\sigma\in G}(\sigma c - c) = \sum_{\sigma\in G} \sigma j(b') - j(b')$, with $b' \in B$. Thus,

$$j(b) = j(\sum_{\sigma\in G} \sigma b' - b') \Rightarrow j(\sum_{\sigma\in G} \sigma b' - b' - b) = 0$$

We multiply the last expression with $g$ and then

$$\begin{aligned} &gj(\sum_{\sigma\in G} \sigma b' - b' - b) = 0 \Rightarrow j(\sum_{\sigma\in G} g\sigma b' - gb' - gb) = 0 \\ &\Rightarrow j(\sum_{\sigma\in G}()gb' - gb') - gb) = 0 \Rightarrow j(gb) = 0 \Rightarrow j(b) = 0 \end{aligned}$$

Hence, we have that $j(b) = \sum_{\sigma\in G}[\sigma j(b') - j(b')] = \sum_{\sigma\in G}[\sigma j(i(a')) - j(i(a'))] = 0$, which means that $b \in Kerj = Imi$. This means that there exists $a \in A$ such that $i(a) = b$. Then $f_4(a + I_GA) = i(a) + I_GB = b + I_GB$, that is $b + I_GB \in Imf_4$. So $Kerf_5 \subseteq Imf_4$. Conversely, let $b + I_GB \in Imf_4$, this means that $f_4(a + I_GA) = i(a) + I_GB = b + I_GB$, where $b = i(a)$ for some $a \in {}_{N_G}A$. Then, $f_5(b + I_GB) = j(b) + I_GC = j(i(a)) + I_GC = I_GC$, that is $b + I_GB \in Kerf_5$. Consequently, $Imf_4 \subseteq Kerf_5$.

$\rightsquigarrow Kerf_6 = Imf_5$

Let $c+I_GC \in Kerf_6$, which means that $f_6(c+I_GC) = N_GA$. But $f_6(c+I_GB) = a + N_GA$, where $j(b) = c, b \in B$, $i(a) = N_Gb$, then

$$a + N_GA = N_GA \Rightarrow a \in N_GA$$

So $f_5(b + I_GB) = j(b) + I_GC = c + I_GC$, that is $c + I_GC \in Imf_5$ and then $Kerf_6 \subseteq Imf_5$. For the converse, let $c + I_GC \in Imf_5$, that is there exist $b \in B$ such that $j(b) = c$. Thus, $f_5(b + I_GB) = j(b) + I_GC = c + I_GC$ and then $f_6(c+I_GC) = a+N_GA$, where $j(b) = c$, $i(a) = N_Gb$, for some $b \in {}_{N_G}B$, that is

$$N_Gb = 0 \Rightarrow i(a) = 0 \Rightarrow a = 0$$

Therefore, $f_6(c+I_GC) = a+N_GA = N_GA$, which implies that $c+I_GC \in Kerf_6$, that is $Imf_5 \subseteq Kerf_6$. □

***Definition* 3.5.2.** ***(Herbrand Quotient)*** *Let G be a finite cyclic group and A is a G-module. Then* ***Herbrand Quotient*** *of A is*

$$h(G, A) = \frac{|\mathcal{H}^0(G, A)|}{|\mathcal{H}^{-1}(G, A)|}$$

*provided that both orders $|\mathcal{H}^0(G, A)|$, $|\mathcal{H}^{-1}(G, A)|$ are finite.*

***Example* 3.5.3.** *1)Let $L = \mathbb{Q}(i)$ and $G = \{1, \sigma\} =< \sigma >$, where $\sigma$ sends any element to its complex conjugate. The extension $L/\mathbb{Q}$ is Galois and $G = Gal(L/\mathbb{Q})$. Then $(L^*, \cdot)$ is a G-module.*
*We have that*
*$(L^*)^G = \mathbb{Q}$, since $L/\mathbb{Q}$ is Galois.*
$N_GL^* = \{N_G(a + bi) \mid a + bi \in L^*\} = \{a + bi + a - bi \mid a + bi \in L^*\} \cong 2\mathbb{Q}$

$$\begin{aligned} {}_{N_G}L^* &= \{a + bi \in L^* \mid N_G(a + bi) = 0\} = \{a + bi \in L^* \mid 2a = 0\} \\ &= \{ib \in L^* \mid b \in \mathbb{Q}\} = i\mathbb{Q} \cong \mathbb{Q} \end{aligned}$$

$I_GL^* = \{\sum_{\sigma\in G} n_\sigma(\sigma a - a),\ a \in L^*\} = \{-2n_\sigma ib,\ n\sigma \in \mathbb{Z}, b \in \mathbb{Q}\} \cong 2\mathbb{Q}$
*Thus,*

$$h(G, L^*) = \frac{|\mathcal{H}^0(G, L^*)|}{|\mathcal{H}^{-1}(G, L^*)|} = \frac{|L^*)^G/N_GL^*|}{|{}_{N_G}L^*/I_GL^*|} = 1$$

*2) $K = \mathbb{F}_3(i)$, $K/\mathbb{F}_3$ Galois with $G = Gal(K/\mathbb{F}_3) = \{1, \sigma\}$, where $\sigma$ sends any element to its complex conjugate modulo 3. Then $K^*$ is a G-module. We have*
$(K^*)^G = \mathbb{F}_3$
$N_GK^* = \{N_G(a+bi) \mid a+bi \in K^*\} = \{a+bi+a-bi = 2a \mid a+bi \in L^*\} \cong \mathbb{F}_3$

$$\begin{aligned} {}_{N_G}K^* &= \{a + bi \in K^* \mid N_G(a + bi) = 0\} = \{a + bi \in K^* \mid 2a = 0\} \\ &= \{ib \in K^* \mid b \in \mathbb{F}_3\} \cong \mathbb{F}_3 \end{aligned}$$

$I_GK^* = \{\sum_{\sigma\in G} n_\sigma(\sigma a - a),\ a \in K^*\} = \{-2n_\sigma ib,\ n\sigma \in \mathbb{Z}, b \in \mathbb{F}_3\} \cong \mathbb{F}_3$
*Thus,*

$$h(G, K^*) = \frac{|\mathcal{H}^0(G, K^*)|}{|\mathcal{H}^{-1}(G, K^*)|} = \frac{|K^*)^G/N_GK^*|}{|{}_{N_G}K^*/I_GK^*|} = 1$$

A reasonable question has been arisen is if the Herbrand quotient exists, is it always an integer?

***Lemma* 3.5.4.** ***(Herbrand Lemma)*** *Let* $0 \to A \to B \to C \to 0$ *be a short exact sequence of G-modules where at least two of* $h(G, A), h(G, B)$ *and* $h(G, C)$ *are defined then*

$$\frac{h(G, A)h(G, C)}{h(G, B)} = 1$$

*Proof.* From proposition 3.5.1 we have that the hexagon is exact. Let $n_i := |Imf_i|$. Then $\mathcal{H}^0(G, A)/Kerf_1 \cong Imf_1$, so

$$|\mathcal{H}^0(G, A)| = |Kerf_1||Imf_1| = |Imf_6|n_1 = n_6 n_1$$

Similarly, $|\mathcal{H}^0(G, B)| = n_1 n_2$, $|\mathcal{H}^0(G, C)| = n_2 n_3$, $|\mathcal{H}^{-1}(G, A)| = n_3 n_4$, $|\mathcal{H}^{-1}(G, B)| = n_4 n_5$, $|\mathcal{H}^{-1}(G, C)| = n_5 n_6$. Then,

$$\begin{aligned} n_1 n_6 n_2 n_3 n_4 n_5 &= n_1 n_2 n_3 n_4 n_5 n_6 \Rightarrow \\ |\mathcal{H}^0(G, A)||\mathcal{H}^0(G, C)||\mathcal{H}^{-1}(G, B)| &= |\mathcal{H}^0(G, B)||\mathcal{H}^{-1}(G, A)||\mathcal{H}^{-1}(G, C)| \end{aligned}$$

If two Herbrand quotients of $h(G, A), h(G, B)$ and $h(G, C)$ are defined, then

$$|\frac{\mathcal{H}^0(G, A)|}{|\mathcal{H}^{-1}(G, A)|} \frac{|\mathcal{H}^{-1}(G, B)|}{|\mathcal{H}^0(G, B)|} \frac{|\mathcal{H}^0(G, C)|}{|\mathcal{H}^{-1}(G, C)|} = 1$$

□

Herbrand Lemma and the exact hexagon in proposition 3.5.1 can be extended to n number of groups.

***Proposition* 3.5.5.** *If A is a finite G-module, then*

$$h(G, A) = 1$$

*Proof.* The sequence

$$0 \to A^G \overset{i}{\to} A \overset{j}{\to} I_G A \to 0$$

where $f(a = ga - a)$, is exact sequence, since $i : A^G \to A, a \mapsto a$ is injective with $Imi = A^G$ and f is surjective with $Kerf = Imi$. In addition, the sequence

$$0 \to {}_{N_G}A \overset{j}{\to} A \overset{h}{\to} N_G A \to 0$$

where $h(a) = N_G a$, is exact sequence, since $j : {}_{N_G}A \to A$ is injective, $h$ is surjective and $Imj = Kerh$. Thus, we have that

$$A/Kerf \cong I_G A \ and \ A/Kerh \cong N_G A$$

This implies that $|A| = |I_G A||Kerf| = |I_G A||Imi| = |I_G A||A^G|$ and $|A| = |N_G A||Kerh| = |N_G A||Imj| = |N_G A||{}_{N_G}A|$. Hence,

$$h(G, A) = \frac{\mathcal{H}^0(G, A)}{\mathcal{H}^{-1}(G, A)} = \frac{|A^G/N_G A|}{|{}_{N_G}A/I_G A|} = 1$$

□

Since we use $\mathcal{H}^{-1}$ only in cyclic cohomology, it has a cohomlogical meaning only when $G$ is finite cyclic group. In this case we have the following:

***Proposition* 3.5.6.** *We have that*

$$\mathcal{H}^{-1}(G,A) \cong \mathcal{H}^{1}(G,A)$$

*Proof.* We assume that $G =< g >$ of order n. We have proved that

$$\mathcal{H}^{1}(G,A) = \frac{\{f : G \to A \,|\, f\, crossed\ homomorphism\}}{\{f : G \to A \mid f\, principal\ crossed\ homomorphism\}}$$

We define

$$\begin{array}{rccc} \varphi : & \mathcal{C}_1(G,A) & \to & {}_{N_G}A \\ & f & \mapsto & f(g) \end{array}$$

Firstly, we will show that $\varphi$ is well-defined. Let $f \in \mathcal{C}_1(G,A)$, that is $f$ is a crossed homomorphism. We will show that $f(g) \in {}_{N_G}A$, that is $N_G f(g) = 0$. We have proved that if $f$ is a crossed homomorphism, then

$$f(g^k) = \sum_{i=0}^{k-1} g^i f(g)$$

and if $G =< g >$ of order n, then

$$\sum_{i=0}^{n-1} g^i f(g) = 0 \Rightarrow f(g^n) = 0 \Rightarrow f(1) = 0$$

Thus,

$$N_G f(g) = \sum_{i=0}^{n-1} g^i f(g) = 0 \Rightarrow f(g^n) = 0 \Rightarrow f(g) \in {}_{N_G}A$$

Also, it is clear that $\varphi$ is a homomorphism. In addition, we will show that $\varphi$ is surjective. Let $a \in {}_{N_G}A$, then $N_G a = 0$. Let also $h$ such that $h(g) = a$ and $h(g^m) = \sum_{i=0}^{m-1} g^i h(g) = \sum_{i=0}^{m-1} g^i a$. So $h$ is a crossed homomorphism and therefore $h$ is surjective. Clearly, $\varphi$ is injective, since $f \in Ker\varphi$, then we have that $\varphi(f) = 0$ which is equivalently with $f(g) = 0$ and then $f = 0$. Therefore, $\varphi$ is an isomorphism. Furthermore, if $f \in \mathcal{B}_1(G,A)$, then $f(g) = ga - a$, for some $a \in A$, that is $f(g) \in I_G A$. Then $\varphi$ is an isomorphism between $\mathcal{C}_1(G,A)/\mathcal{B}_1(G,A)$ and ${}_{N_G}A/I_G A$. This means that $\mathcal{C}_1(G,A)/\mathcal{B}_1(G,A) \cong {}_{N_G}A/I_G A$. This complete the proof. □

***Proposition* 3.5.7.** *Let $G =< g >$ is a finite cyclic group. Then*

$$\mathcal{H}^q(G,A) \cong A^G/N_GA = \mathcal{H}^0(G,A),\ \ for\ every\ even\ q \geq -1$$

*and*

$$\mathcal{H}^q(G,A) \cong {}_{N_G}A/I_GA = \mathcal{H}^{-1}(G,A),\ \ for\ every\ odd\ q \geq -1$$

*Proof.* According to proposition 3.5.6 we have that $\mathcal{H}^{-1}(G,A) \cong \mathcal{H}^1(G,A)$. We assume that $|G| = m$ and $N := N_G = 1 + g + g^2 + \cdots + g^{m-1}$, then $N$ can be thought as a map $\mathbb{Z}[G] \to \mathbb{Z}[G]$. Also, $N(g-1) = (g-1)N = g^m - 1 = 0$ where the multiplication by $g-1$ is another map from $\mathbb{Z}[G] \to \mathbb{Z}[G]$. Since $G$ is a finite cyclic group we can construct a free resolution of $G$-module $\mathbb{Z}$

$$\cdots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{N} \cdots \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0 \qquad (*)$$

That is

$$\begin{tikzcd}
\cdots \arrow[r, "d_3"] & X_2 \arrow[r, "d_2"] & X_1 \arrow[r, "d_1"] & X_0 \arrow[r, "d_0"] \arrow[dr, "\epsilon"'] & X_{-1} & \\
& & & & \mathbb{Z} \arrow[dr] & \\
& & & & & 0
\end{tikzcd}$$

where $d_i = \begin{cases} N, & i = even \\ g-1, & i = odd \end{cases}$

$d$ is $G$-homomorphism with $d^2 = 0$ and $X_i = \mathbb{Z}[G]$ are free $G$-modules. We will show the exactness of the above sequence $(X, d, -1)$. Let $G = \{1, g, \ldots, g^{m-1}\}$, $N = \sum_{n=0}^{m-1} g^i$ and $\gamma \in \mathbb{Z}[G]$, that is $\gamma = \sum_{n=0}^{m-1} c_i g^i$, $c_i \in \mathbb{Z}$. We have that $Imd \subseteq Kerd$, since $d^2 = 0$. It remains to show the converse. If $n$ is odd, then

$$\begin{aligned} \gamma \in Ker(g_1) & \Leftrightarrow g\gamma = \gamma \\ \Rightarrow \sum_{i=0}^{m-1} c_i g^i = \sum_{i=0}^{m-1} c_i g^{i+1} & \Rightarrow c_i = c,\ \forall i = 0, \ldots, m-1 \end{aligned}$$

so $\gamma = Nc$, which means that $\gamma \in ImN$. If $n$ is even, then

$$\gamma \in KerN \Rightarrow N\gamma = 0 \Rightarrow N(\sum_{i=0}^{m-1} c_i g_i) = 0$$

$$\Rightarrow (\sum_{i=0}^{m-1} c_i)N = 0 \Rightarrow \sum_{i=0}^{m-1} c_i = 0$$

so $\gamma = \sum_{i=0}^{m-1} c_i g_i = \sum_{i=0}^{m-1} c_i(g_i - 1)$, which means that $\gamma \in Im(g-1)$. Thus, $Im(g-1) = KerN$. For the augmentation map

$$\epsilon : \mathbb{Z}[G] \to \mathbb{Z},\ where\ \sum_{\sigma \in G} n_\sigma \sigma \mapsto \sum_{\sigma \in G} n_\sigma$$

we have that $\mu \circ \epsilon(1) = d_0(1)$. Hence, $(X, d, -1)$ is a free resolution. In the sequence $(*)$ we apply $Hom_G(X_q, A)$. We have proved that $Hom_G(\mathbb{Z}[G], A) \cong A$, $Hom_G(\mathbb{Z}, A) \cong A$. So,

$$0 \to Hom_G(\mathbb{Z}, A) \overset{(\epsilon,1)}{\to} Hom_G(X_0, A) \overset{(d_1,1)}{\to} \cdots$$

That is

$$0 \to A \overset{(\epsilon,1)}{\to} A \overset{(d_1,1)}{\to} \cdots$$

Then

$$0 \to A \overset{(d_1,1)}{\to} A \overset{(d_2,1)}{\to} \cdots$$

We set $\mathfrak{d}_q = (d_q, 1)$. We have that

$$\mathcal{H}^q(G, A) = \mathcal{C}_q/\mathcal{B}_q = Ker\mathfrak{d}_{q+1}/Im\mathfrak{d}_q$$

For $q \geq 1$ : If $q$ is even then

$$Ker\mathfrak{d}_{q+1} = \{a \in A : \ (d_{q+1}, 1)a = 0\} = \{a \in A : \ (g-1, 1)a = 0\} = A^G$$

and

$$Im\mathfrak{d}_q = Im(d_q, 1) = Im(N, 1) = (N, 1)A = N_G A$$

Thus, $\mathcal{H}^q(G, A) = A^G/N_G A$.
If $q$ is odd then

$$\begin{aligned} Ker\mathfrak{d}_{q+1} &= Ker(N, 1) = \{a \in A : \ (N, 1)a = 0\} \\ &= \{a \in A : \ Na = 0\} = {}_{N_G}A \end{aligned}$$

and

$$Im\mathfrak{d}_q = Im(d_q, 1) = Im(g-1, 1) = (g-1, 1)A = I_G A$$

Thus, $\mathcal{H}^q(G, A) = {}_{N_G}A/I_G A$. This complete the proof. □

In particular we have that $\mathcal{H}^q(G, A) \cong \mathcal{H}^{q+2}(G, A)$, for every $q \geq -1$.

## 3.6 Cohomology Theorems

Now we will mention some theorems of cohomology without their proofs. For their proofs see [19].

***Theorem* 3.6.1.** *(Dimension Shifting) Let $A$ be a $G$-module. Then there exists $G$-modules $A^+$ and $A^-$ such that for every subgroup $H$ of $G$*

$$\mathcal{H}^{n-1}(H, A^-) \cong \mathcal{H}^n(H, A) \cong \mathcal{H}^{n+1}(H, A^+)$$

*for every $n \in \mathbb{Z}$.*

***Theorem* 3.6.2.** *Let*

$$0 \longrightarrow A \overset{i}{\longrightarrow} B \overset{j}{\longrightarrow} C \longrightarrow 0$$

*be an exact sequence of G-modules and G-homomorphisms. Then the induced infinite sequence*

$$\begin{aligned} \cdots \longrightarrow\ & \mathcal{H}^q(G,A) \longrightarrow \mathcal{H}^q(G,B) \longrightarrow \mathcal{H}^q(G,C) \overset{\delta}{\longrightarrow} \\ & \mathcal{H}^{q+1}(G,A) \longrightarrow \mathcal{H}^{q+1}(G,B) \longrightarrow \mathcal{H}^{q+1}(G,C) \longrightarrow \cdots \end{aligned}$$

*where $\delta$ is the connecting homomorphism, is also exact. It is called the exact cohomology sequence.*

***Definition* 3.6.3.** *Let G be a finite group and $M$ be a G-module. The G-module $M$ is called cohomologically trivial if and only if $\mathcal{H}^r(S,M) = \{0\}$ for every $r \in \mathbb{Z}$ and $S \leqslant G$.*

***Theorem* 3.6.4.** *(Nakayama-Tate) Let G be a finite group and $M$ is a G-module. Then $\mathcal{H}^r(S,M) = \mathcal{H}^{r+1}(S,M) = \{0\}$ if and only if M is cohomologically trivial.*

***Theorem* 3.6.5.** *Let $M$ be a G-module such that for every subgroup $S$ of G we have that $\mathcal{H}^1(S,M) = \{0\}$ and $\mathcal{H}^2(S,M)$ is cyclic of order $|G|$. Then for every subgroup $S$ of G and for every r we have that*

$$\mathcal{H}^r(S,M) = \mathcal{H}^{r-2}(S,\mathbb{Z})$$

*In particular, if $r = 0$ and $S = G$, then*

$$\mathcal{H}^0(G,M) = \mathcal{H}^{-2}(G,\mathbb{Z})$$

*That is*

$$M^G/N_G M \cong G/[G,G]$$

The last equality is very important in number theory. If $L/K$ is Galois extension of algebraic number fields and $G = Gal(L/K)$ then this equality give us the Artin reciprocity law.

***Theorem* 3.6.6.** *Let G be a finite group and $G_p$ is a p-Sylow subgroup of G, for every prime number p. If M is a G-module and $\mathcal{H}^r(G_p,M) = \{0\}$, for every $p \mid |G|$, then $\mathcal{H}^r(G,M) = \{0\}$*

Then we will mention some functions whose properties are important for the proof of theorems that we have mentioned above.
Also we will study the behavior of cohomology group if we change the group $G$.

Let $A$ be a $G$-module and $H$ is a subgroup of $G$. Clearly, $A$ is a $H$-module. If $H$ is a normal subgroup of $G$, then it is clear that $A^H$ is a $G/H$-module.

We wonder which is the relation between the cohomology groups

$$\mathcal{H}^r(G/H, A^H),\ \mathcal{H}^r(G, A),\ \mathcal{H}^r(H, A)$$

We have defined the homomorphism of pairs (definition 5.1.11)

$$(\lambda, f) : (G, A) \to (G', A')$$

In addition we have that if $(\lambda, f) : (G, A) \to (G', A')$ is a homomorphism of pairs, then for every $n$ there exists a homomorphism

$$(\lambda, f)_* : \mathcal{H}^n(G, A) \to \mathcal{H}^n(G', A')$$

For $f = 1_A$ and $\lambda = i : H \hookrightarrow G$, we take the homomorphism of pairs

$$(i, 1) : (G, A) \to (H, A)$$

which induce the map

$$(i, 1)_* : \mathcal{H}^n(G, A) \to \mathcal{H}^n(H, A)$$

The map $(i, 1)_*$ will be called **restriction** of $G$ in $H$ and it denoted by $rest := rest_{G \to H}$. We can prove that the restriction is transitive, that is if $H' \leqslant H \leqslant G$, then

$$rest_{G \to H'} = rest_{H \to H'} \circ rest_{G \to H}$$

We assume now that H is a normal subgroup of G, then $A^H$ is a $G/H$-module. Let $\pi : G \to G/H$ be the natural projection and $i : A^H \hookrightarrow A$ be an injection. Then $A^H$ becomes a $G$-module under $\pi$. So,

$$(\pi, i) : (G/A, A^H) \to (G, A)$$

is a homomorphism of pairs and then we have

$$(\pi, i)_* : \mathcal{H}^n(G/A, A^H) \to \mathcal{H}^n(G, A),\ n \geq 1$$

The map $(\pi, i)_*$ is called **inflation** of $G/H$ in $G$ and is denoted by $inf := inf_{G/H \hookrightarrow G}$. Also, we can prove that the inflation is transitive, that is if $H_2 \leqslant H_1 \leqslant G$ and $H_1, H_2$ are normal subgroups of $G$ then the following diagram is commutative

$$\begin{tikzcd}
\mathcal{H}^n(G/H_1, A^{H_1}) \arrow[rr] \arrow[dr] & & \mathcal{H}^n(G/H_2, A^{H_2}) \arrow[dl] \\
& \mathcal{H}^n(G, A) &
\end{tikzcd}$$

$n \geq 1$

***Theorem* 3.6.7.** *If*

$$0 \to A \to B \to C \to 0$$

*is an exact sequence of G-modules and G-homomorphisms and if $H$ is a normal subgroup of G such that*

$$0 \to A^H \to B^H \to C^H \to 0$$

*is an exact sequence, then the following diagram is commutative*

$$\begin{tikzcd}
\mathcal{H}^n(G/H, C^H) \arrow[r] \arrow[d, "inf"] & \mathcal{H}^{n+1}(G/H, A^H) \arrow[d, "inf"] \\
\mathcal{H}^n(G, C) \arrow[r] & \mathcal{H}^{n+1}(G, A)
\end{tikzcd}$$

There exists a respective statement for the restrictions as well.
Now we will mention a basic theorem of cohomology.

***Theorem* 3.6.8.** *If $A$ is a G-module and $H$ is a normal subgroup of G, then the sequence*

$$0 \to \mathcal{H}^1(G/H, A^H) \to \mathcal{H}^1(G, A) \to \mathcal{H}^1(H, A)$$

*is exact sequence.*

If $A = \mathbb{Z}$, then the map

$$rest : \mathcal{H}^{-2}(G, \mathbb{Z}) \to \mathcal{H}^{-2}(H, \mathbb{Z})$$

induce the map

$$G/[G,G] \to H/[H,H]$$

which is called **transfer (Verlagerung)**.
If $H$ is a subgroup of $G$ and $[G : H] < \infty$, then we can define a map

$$\mathcal{H}^n(H, A) \to \mathcal{H}^n(G, A)$$

which is called **corestriction** and is denoted by $corest_{H \to G}$. In addition, we have the following

***Theorem* 3.6.9.** *If $[G : H] = n$, then*

$$corest_{H \to G} \circ rest_{G \to H} = nId$$

Let $G$ be a group and $\mathbb{Z}[G]$ is the integer group ring. If $A, B$ are $G$-modules then we can construct a $\mathbb{Z}$-module, the so called tensor product of $A, B$, which is denoted by $A \otimes_{\mathbb{Z}} B$. This can be $G$-module.

***Theorem* 3.6.10.** *(Shapiro's Lemma) Let $H$ be a subgroup of G and $M$ is a H-module, then $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$ is a left G-module and*

$$\mathcal{H}^n(G, Ind_H^G M) = \mathcal{H}^n(H, M)$$

*where $Ind_H^G M = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$.*

# Chapter 4

# Cohomology of Profinite Groups

In second chapter of this thesis we defined the profinite groups and in third chapter we investigated the cohomology group of finite groups. We wonder what happen if the group is profinite. For this reason in this chapter we will define the cohomology group of a profinite group and we will study some useful statements.

Let $K$ be a perfect field and $\bar{K}$ be the algebraic closure of $K$. We know that the extension $\bar{K}/K$ is an infinite extension. In particular, it is Galois and $Gal(\bar{K}/K)$ is a profinite group.

$$\begin{array}{ccc} \bar{K} & \longleftrightarrow & \{id\} \\ | & & | \\ K & \longleftrightarrow & Gal(\bar{K}/K) \end{array}$$

We know that

$$G = Gal(\bar{K})/K = \varprojlim_{\substack{N \\ N \trianglelefteq G, \\ N = open}} G/N = \varprojlim_{\substack{K \leq L \leq \bar{K}, \\ L/K\, is\, finite}} Gal(L/K)$$

It's worth noting that $\bar{K} = \varinjlim_{\substack{L/K\, is\, finite \\ and\, Galois}} L$

## 4.1 Discrete Modules

Let $G$ be a group and $R$ be a ring (not necessarily commutative ring). We have defined that a left $G$ module $A$ is an additive abelian group equipped with a scalar multiplication

$$\begin{array}{ccc} G \times A & \rightarrow & A \\ (\sigma, a) & \mapsto & \sigma a \end{array}$$

such that the following axioms holds for every $a, b \in A$ and $\sigma, \tau \in G$:
i) $\sigma(a + b) = \sigma(a) + \sigma(b)$
ii) $(\sigma + \tau)a = \sigma a + \tau a$
iii) $(\sigma\tau)(a) = \sigma(\tau(a))$

If also $1a = a$ for every $a \in A$, then $A$ is called unitary.

We assume that $G$ is a profinite group and $M$ is a unitary $G$-module. Then $G$ is a topological group and $M$, as an abelian group, can be considered as a topological group equipped with the discrete topology.

***Definition* 4.1.1.** *Let G a profinite group and $M$ a unitary G-module. We will call $M$ discrete G-module if the group action $G \times M \to M$ is continuous.*

It suffices to remark that if $G$ is a finite group, then the above definition of discrete $G$-module is the same with the common definition of a $G$-module.

***Theorem* 4.1.2.** *Let G be a profinite group and $M$ is a unitary G-module. Then the following are equivalent:*
*i) $M$ is a discrete G-module,*
*ii) For every $m \in M$, the stabilizer*

$$G_m = \{g \in G : gm = m\}$$

*is an open subgroup of G,*
*iii) If $\mathcal{B}(1)$ is a basis of open neighborhoods of* 1 *consisting of open normal subgroups of G. Then*

$$M = \bigcup_{H \in \mathcal{B}(1)} M^H$$

*where $M^H = \{m \in M : hm = m, \forall h \in H\}$.*

*Proof.* "$i) \Rightarrow ii)$" We assume that $M$ is a discrete $G$-module. Let $m \in M$. We take the singleton $\{m\}$ which is open because $M$ is a topological group with discrete topology. Also, we know that the map $f : G \times M \to M$ is continuous, so then the preimage of $\{m\}$ under f, $f^{-1}(\{m\})$, is open. Moreover, the preimage of $\{m\}$ under the restriction of $G \times M \to M$ to $G \times \{m\}$ is $G_m \times \{m\}$. Consequently, $G_m \times \{m\}$ is open, so then $G_m$ is open as well. Therefore, $G_m$ is open for each $m \in M$.
"$ii) \Rightarrow iii)$" We assume that for every $m \in M$, the stabilizer

$$G_m = \{g \in G : gm = m\}$$

is an open subgroup of $G$. Let $\mathcal{B}(1)$ be a basis of open neighborhood of 1 consisting of open normal subgroups of $G$. It is clear that $\bigcup_{H \in \mathcal{B}(1)} M^H \subseteq M$. Let now $m \in M$. Then $G_m = \{g \in G : gm = m\}$ is an open neighborhood of 1, because $1 \in G_m$ as $G_m$ acts on $M$, so $1 \in G_m$ because $1 \cdot m = m$. This implies that there exists $H \in$

$\mathcal{B}(1)$ satisfying that $H \subseteq G_m$. But $M^{G_m} = \{m' \in M : gm' = m', \forall g \in G_m\}$, so then $m \in M^{G_m} \subseteq M^H$, that is $m \in \bigcup_{H \in \mathcal{B}(1)} M^H$. Hence, $M = \bigcup_{H \in \mathcal{B}(1)} M^H$.

"$iii) \Rightarrow i)$" Let $\mathcal{B}(1)$ be a basis of open neighborhood of $1$ consisting of open normal subgroups of $G$. Then $M = \bigcup_{H \in \mathcal{B}(1)} M^H$. We will prove that $G$ is a discrete $G$-module. It suffices to show that $f : G \times M \to M$ with $(g, m) \mapsto gm$ is a continuous map. For this it suffices to show that for every open set $A$ in $M$, the preimage of $A$ under $f$, $f^{-1}(A)$, is an open set in $G \times M$. Let $a, b \in M$ and $g \in G$ such that $ga = b$. Since $b \in M$ we have that $b \in \bigcup_{H \in \mathcal{B}(1)} M^H$. This implies that there exists $H \in \mathcal{B}(1)$ such that $b \in M^H$, which means that $hb = b$ for each $h \in H$. Thus, $Hg \times \{a\}$ is an open neighborhood of $(g, a)$ and $f(Hg \times \{a\}) = \{b\}$, since $f(hg, a) = hga = hb = b$. Hence, $Hg \times \{a \subseteq f^{-1}(\{b\})\}$. That is for every $(g, a) \in f^{-1}(\{b\})$ there exists $U = Hg \times \{a\}$ which is an open neighborhood of $(g, a)$ such that $U = Hg \times \{a\} \subseteq f^{-1}(\{b\})$. Consequently, $f^{-1}(\{b\})$ is open. Moreover, we have that $M$ is a unitary $G-$module and it is a topological group equipped with the discrete topology. So $\mathcal{B} = \{\{b\}, b \in M\}$ form a basis of $M$. For this reason it suffices to check that $f^{-1}(\{b\})$ is open. Therefore, it is easy to see that $f^{-1}(A)$ is open in $G \times M$ for every open subset $A$ of $M$, since $A$ will be a union of sets that belong in base $\mathcal{B}$, that is $A = \bigcup_{b \in M} \{b\}$. But then $f^{-1}(A) = \bigcup_{b \in M} f^{-1}(\{b\})$ and $f^{-1}(\{b\})$ is open. Consequently, $f^{-1}(A)$ is open as a union of open sets. Hence, $f$ is continuous. □

Theorem 4.1.2 implies immediately that submodules and quotients of discrete $G$-modules are again discrete $G$-modules.

***Comment* 4.1.3.** *We say that G acts trivially on A if $\sigma a = a$ for all $a \in A$. Thus $A^G = A$ if and only if the action is trivial. When $\mathbb{Z}, \mathbb{Q}, \mathbb{Q}/\mathbb{Z}$ are considered as G-modules, this is with the trivial action, unless stated otherwwise.*

***Example* 4.1.4.** *Let $M$ be an abelian group and G is a profinite group that acts trivially on $M$. Then $M$ is a discrete G-module. Indeed, $M^G = M$. Let $\mathcal{B}(1)$ is a basis of open neighborhood of $1$ consisting of open normal subgroups of G. If $H \in \mathcal{B}(1)$, then $M^H = M$, because $M^G = M$ and $H \leqslant G$. Thus, $M = \bigcup_{H \in \mathcal{B}(1)} M^H$. So then according to theorem 4.1.2 we have that $M$ is a discrete G-module*

***Example* 4.1.5.** *Let $\mathbb{Q}_p$ be the field of rational p-adic numbers. Then*

$$a(b + \mathbb{Z}_p) = ab + \mathbb{Z}_p, \ for\, a \in \mathbb{Z}_p, b \in \mathbb{Q}_p$$

*defines a discrete $\mathbb{Z}_p$ structure on $\mathbb{Q}_p/\mathbb{Z}_p$.*

***Example* 4.1.6.** *In the following examples $\bar{K}$ denotes the separable closure of $K$.*

*1) Let $M := \bar{K}$ an additive abelian group, $\bar{K}/K$ Galois extension*

$$Gal(\bar{K}/K) \times \bar{K} \to \bar{K}$$

*The action of $Gal(\bar{K}/K)$ on $(\bar{K},+)$ defines the $M := \bar{K}$ as a discrete $Gal(\bar{K}/K)$-module.*
*It is clear that the $(\bar{K},+)$ is a unitary $Gal(\bar{K}/K)$-module and discrete as well. Indeed, we notice that $\bar{K} = \bigcup\limits_{L} L$ where $K \leqslant L \leqslant \bar{K}$ and $L/K$ is finite. Clearly, $\bigcup\limits_{L} L \subseteq \bar{K}$, where $K \leqslant L \leqslant \bar{K}$ and $L/K$ is finite. Also, let $\alpha \in \bar{K}$ then $\alpha$ is algebraic over $K$, and then $K(\alpha)/K$ is algebraic and finite. That is $\alpha \in L$ such that $L/K$ is finite. Thus, $\bar{K} = \bigcup\limits_{L} L = \bigcup\limits_{L} \bar{K}^{Gal(\bar{K}/L)}$ where $K \leqslant L \leqslant \bar{K}$ and $L/K$ is finite, so then from theorem 4.1.2 we have that $(\bar{K},+)$ is a discrete $G$-module*

*2) The $(\bar{K}^*,\cdot)$ is a discrete $G$-module, where $G = Gal(\bar{K}/K)$. Clearly, the $(\bar{K}^*,\cdot)$ is a unitary $G$-module and we can prove that $(\bar{K}^*,\cdot)$ is a discrete $G$-module in like way with the previous.*

*3) The roots of unity of $\bar{K}$, $\mu(\bar{K})$, is a discrete $G$-module, where $G = Gal(\bar{K}/K)$.*

*4) Let $E$ an elliptic curve over $K$, where $K$ is an algebraic number field. Then $E(\bar{K})$ is an additive abelian group. Also, it is a discrete $Gal(\bar{K}/K)$-module. Indeed, since $E(\bar{K}) = \bigcup\limits_{L} E(L)$, where $K \leqslant L \leqslant \bar{K}$ and $L/K$ is finite.*

## 4.2 Construction of the Cohomology Groups

Throughout this section $G$ will denote a profinite group and $M$ a discrete $G$-module.

For $q \geq 1$, let $C^q(G,M)$ denote the set of all continuous map from $G^q$ to $M$, that is

$$C^q(G,M) = \{x : G^q \to M \,|\, x\, is\, continuous\}$$

For $q \geq 1$ we define the homomorphisms of groups

$$\mathfrak{d}_{q+1} : C^q(G,M) \to C^{q+1}(G,M)$$

with

$$\begin{aligned}(\mathfrak{d}_{q+1}f)(g_1,\dots,g_{q+1}) &= g_1 f(g_2,\dots,g_{q+1}) \\ &+ \sum_{i=1}^{q}(-1)^i f(g_1,\dots,g_{i-1},g_i g_{i+1},g_{i+2},\dots,g_{q+1}) \\ &+ (-1)^{q+1} f(g_1,\dots,g_q)\end{aligned}$$

where $f \in C^q(G,M)$

For $q = 0$: we define $\eth_1 : C^0(G,M) \to C^1(G,M)$ with $\eth_1 f(g) = gf - f$, $f \in C^0(G,M)$.
We know that $C^0(G,M) = M$. The maps $\eth$ are called coboundary maps. Moreover we have proved that $\eth_{q+1} \circ \eth_q = 0$, $\forall q \geq 1$. Thus, the chain

$$0 \longrightarrow C^0(G,M) \xrightarrow{\eth_1} C^1(G,M) \xrightarrow{\eth_2} \cdots$$

is a cochain complex. We define the $q$-cocycles group of $G$ as follows

$$\mathcal{Z}^q(G,M) = Ker\eth_{q+1}$$

and the $q$-coboundaries group of $G$ by

$$\mathcal{B}^q(G,M) = Im\eth_q, \; for\, q \geq 1$$

and

$$\mathcal{B}^0(G,M) := \{0\}$$

In this case the cocycles and the coboundaries are continuous maps in contrast with the case of finite groups. Thus we define the $q$-**cohomology group** of $G$ by

$$\mathcal{H}^q(G,M) = \frac{\mathcal{Z}^q(G,M)}{\mathcal{B}^q(G,M)}$$

We denote the elements of $\mathcal{H}^q(G,M)$ by $[f] = f + \mathcal{B}^q(G,M)$.

We can calculate the cohomology groups of low dimension.

***Proposition* 4.2.1.** *Let G a profinite group and $M$ discrete G-module. Then*

$$\mathcal{H}^0(G,M) = M^G$$

*Proof.* By definition we have that $\mathcal{H}^0(G,M) = \frac{\mathcal{Z}^0(G,M)}{\mathcal{B}^0(G,M)}$. Also, it is clear that $\mathcal{B}^0(G,M) = \{0\}$ and $\mathcal{Z}^0(G,M) = Ker\eth_1 = \{m \in M : gm - m = 0, \forall g \in G\} = M^G$. □

***Proposition* 4.2.2.** *Let G a profinite group and $M$ discrete G-module. Then the first cohomology group of $M$ is defined as*

$$\mathcal{H}^1(G,M) = \frac{\{f : G \to M, f\, is\, continuous, f\, is\, crossed\, homomorphism\}}{\{f : G \to M, f\, continuous, f\, principle\, crossed\, homomorpism\}}$$

*Proof.* By definition we have that $\mathcal{H}^1(G,M) = \frac{\mathcal{Z}^1(G,M)}{\mathcal{B}^1(G,M)}$. Also,

$$\begin{aligned} \mathcal{Z}^1(G,M) &= Ker\eth_2 = \{f : G \to M, f\, is continuous : \eth_2 f = 0\} \\ &= \{f : G \to M, f\, is\, continuous, f\, is\, crossed\, homomorphism\} \end{aligned}$$

□

***Proposition* 4.2.3.** *Let $G$ a profinite group and $M$ discrete G-module. Then the second cohomology group of $M$ is defined as*

$$\mathcal{H}^2(G,M)=\frac{\{continuous\, factor\, sets\}}{\{continuous\, splitting\, factor\, sets\}}$$

***Remark* 4.2.4.** *1) If the profinite group $G$ acts trivially on the discrete G-module $M$. Then $\mathcal{H}^0(G,M)=M$ (This is true for finite groups as well) and $\mathcal{H}^1(G,M)=Hom_{cont}(G,M)$.*
*2) If G is a profinite group and the sequence*

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

*is a short exact sequence of discrete G-modules, then the sequence*

$$\begin{aligned}0 \quad\longrightarrow\quad & \mathcal{H}^0(G,A)\longrightarrow\mathcal{H}^0(G,B)\longrightarrow\mathcal{H}^0(G,C)\xrightarrow{\delta}\\ & \mathcal{H}^1(G,A)\longrightarrow\mathcal{H}^1(G,B)\longrightarrow\mathcal{H}^1(G,C)\longrightarrow\cdots\end{aligned}$$

*is also exact.*

## 4.3 Compatible Pairs

In this section we will define the compatible pairs and we will study some useful propositions.

***Definition* 4.3.1.** *Let $\psi : G\to H$ be a continuous homomorphism of profinite groups. Let also $A$ be a discrete G-module and $B$ a discrete $H$-module. We assume that $\varphi: B\to A$ is a continuous homomorphism of topological groups. We say that the pair $(\psi,\phi)$ is compatible if*

$$\varphi(\psi(g)b)=g\varphi(b)$$

*for all $g\in G$ and $b\in B$*

***Proposition* 4.3.2.** *Let $\psi: G\to H$, $\varphi: B\to A$ be a compatible pair.*
*i) For every $q\geq 0$ there exists an induced homomorphism of $q-cochains$*

$$(\psi,\varphi)^*_q : C^q(H,B)\to C^q(G,A)$$

*where $(\psi,\varphi)^*_q(f)=\varphi\circ f\circ\psi$.*
*ii) For every $q\geq 0$ the following diagram is commutative*

$$\begin{tikzcd}
C^q(H,B) \arrow[r, "\mathfrak{d}_{q+1}"] \arrow[d, "f_q"'] & C^{q+1}(H,B) \arrow[d, "f_{q+1}"] \\
C^q(G,A) \arrow[r, "\mathfrak{d}_{q+1}"'] & C^{q+1}(G,A)
\end{tikzcd}$$

*where* $f_q = (\psi, \varphi)_q^*$.
*iii) For every* $q \geq 0$ *there exists an induced homomorphism*

$$\begin{array}{ccc} \mathcal{H}^q(H, B) & \rightarrow & \mathcal{H}^q(G, A) \\ [f] & \mapsto & [(\psi, \varphi)_q^*(f)] \end{array}$$

*which we also denote by* $(\psi, \varphi)_q^*$.

*Proof.* i) It is clear that $(\psi, \varphi)_q^*$ is a homomorphism of groups and also for every $f \in C^q(H, B)$ the $(\psi, \varphi)_q^*(f)$ is continuous as a composition of continuous maps.
ii) It's proof is a straightforward computation that follows from the definitions of the coboundary map and compatible pairs. It suffices to show that

$$(\psi, \varphi)_{q+1}^* \circ \mathfrak{d}_{q+1} = \mathfrak{d}_{q+1} \circ (\psi, \varphi)_q^*$$

$$\begin{aligned} & (\mathfrak{d}_{q+1} \circ (\psi, \varphi)_q^*(f))(g_1, \dots, g_{q+1}) = \\ = \;& g_1((\psi, \varphi)_q^*(f)(g_1, \dots, g_{q+1})) + \sum_{i=1}^{q} (-1)^i ((\psi, \varphi)_q^*(f))(g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_{q+1}) \\ + \;& (-1)^{q+1}((\psi, \varphi)_q^*(f))(g_1, \dots, g_q) \\ = \;& g_1(\varphi(f(\psi(g_1), \dots, \psi(g_{q+1})))) + \sum_{i=1}^{q} (-1)^i \varphi(f(\psi(g_1), \dots, \psi(g_{i-1}), \psi(g_i g_{i+1}), \psi(g_{i+2}), \dots, \psi(g_{q+1}))) \\ + \;& (-1)^{q+1}(\varphi(f(\psi(g_1), \dots, \psi(g_q))) \end{aligned}$$

In addition,

$$\begin{aligned} & (\psi, \varphi)_{q+1}^*(\mathfrak{d}_{q+1}(f(g_1, \dots, g_{q+1})) = \\ = \;& (\varphi \circ (\mathfrak{d}_{q+1} \circ f \circ \psi)(g_1, \dots, g_{q+1}) = \phi(\mathfrak{d}_{q+1}(f(\psi(g_1)), \dots, \psi(g_{q+1}))) \\ = \;& \varphi[g_1 f(\psi(g_2), \dots, \psi(g_{q+1})) + \sum_{i=1}^{q} (-1)^i f(\psi(g_1), \dots, \psi(g_{i-1}), \psi(g_i g_{i+1}), \psi(g_{i+2}), \dots, \psi(g_{q+1})) \\ + \;& (-1)^{q+1}(f(\psi(g_1), \dots, \psi(g_q))] \\ = \;& g_1 \varphi(f(\psi(g_2), \dots, \psi(g_{q+1}))) + \sum_{i=1}^{q} (-1)^i \varphi(f(\psi(g_1), \dots, \psi(g_{i-1}), \psi(g_i g_{i+1}), \psi(g_{i+2}), \dots, \psi(g_{q+1}))) \\ + \;& (-1)^{q+1} \varphi(f(\psi(g_1), \dots, \psi(g_q))) \end{aligned}$$

Thus, $(\psi, \varphi)_{q+1}^* \circ \mathfrak{d}_{q+1} = \mathfrak{d}_{q+1} \circ (\psi, \varphi)_q^*$
iii) Firstly we note that if $f \in \mathcal{Z}^q(H, B)$, then $\mathfrak{d}_{q+1}(f) = 0$. So then from (ii) we have that $\mathfrak{d}_{q+1}((\psi, \varphi)_q^*(f)) = (\psi, \varphi)_{q+1}^*(\mathfrak{d}_{q+1}(f)) = 0$. This means that if $f \in \mathcal{Z}^q(H, B)$, then $(\psi, \varphi)_q^*(f) \in Ker\mathfrak{d}_{q+1} = \mathcal{Z}^q(G, A)$. So the restriction of $(\psi, \varphi)_q^* : C^q(H, B) \rightarrow C^q(G, A)$ to $\mathcal{Z}^q(H, B)$ is the map $\mathcal{Z}^q(H, B) \rightarrow \mathcal{Z}^q(G, A)$. Let $\pi_q : \mathcal{Z}^q(G, A) \rightarrow \mathcal{H}^q(G, A)$ be the canonical projection. Then we have the following

$$\begin{array}{ccccc} \mathcal{Z}^q(H,B) & \overset{(\psi,\varphi)^*_q}{\rightarrow} & \mathcal{Z}^q(G,A) & \overset{\pi_q}{\rightarrow} & \mathcal{H}^q(G,A) = \frac{\mathcal{Z}^q(G,A)}{\mathcal{B}^q(G,A)} \\ f & \mapsto & (\psi,\varphi)^*_q(f) =: g & \mapsto & g + \mathcal{B}^q(G,A) \end{array}$$

Hence by composing $(\psi,\varphi)^*_q$ with $\pi_q$ we obtain a homomorphism

$$\varphi_q : \mathcal{Z}^q(H,B) \rightarrow \mathcal{H}^q(G,A)$$

where $\varphi_q := \pi_q \circ (\psi,\varphi)^*_q$. It suffices to show that $\mathcal{B}^q(H,B) \subseteq Ker\varphi_q$. Indeed, if $\mathcal{B}^q(H,B) \subseteq Ker\varphi_q$ then we know that there exists a unique homomorphism of groups

$$\frac{\mathcal{Z}^q(G,A)}{\mathcal{B}^q(G,A)} \rightarrow \mathcal{H}^q(G,A)$$

That is

$$\mathcal{H}^q(H,B) \rightarrow \mathcal{H}^q(G,A)$$

with $[f] \mapsto [(\psi,\varphi)^*_q(f)]$. It remains to show that $\mathcal{B}^q(H,B) \subseteq Ker\varphi_q$. Let $f \in \mathcal{B}^q(H,B) = Im\mathfrak{d}_q$. That is there exists $g \in C^{q-1}(H,B)$ such that $f = \mathfrak{d}_q(g)$. Then $(\psi,\varphi)^*_q(f) = (\psi,\varphi)^*_q(\mathfrak{d}_q(g)) = \mathfrak{d}_q((\psi,\varphi)^*_{q-1}(g)) \in \mathcal{B}^q(G,A)$. So $\pi_q \circ (\psi,\varphi)^*_q(f) = \pi_q(\mathfrak{d}_q((\phi,\psi)^*_{q-1}(g))) = \mathfrak{d}_q((\phi,\psi)^*_{q-1}(g)) + \mathcal{B}^q(G,A) = \mathcal{B}^q(G,A)$, which implies that $f \in Ker(\varphi_q) =$. Therefore, for every $q \geq 0$ induced a homomorphism

$$\begin{array}{ccc} \mathcal{H}^q(H,B) & \rightarrow & \mathcal{H}^q(G,A) \\ [f] & \mapsto & [(\psi,\varphi)^*_q(f)] \end{array}$$

□

The maps $(\psi,\varphi)^*_q$, that we have just constructed, behave functorially in the following sense.

***Proposition* 4.3.3.** *We assume that* $G_1 \overset{\psi_1}{\rightarrow} G_2 \overset{\psi_2}{\rightarrow} G_3$ *and* $A_3 \overset{\phi_2}{\rightarrow} A_2 \overset{\phi_1}{\rightarrow} A_1$ *are such that* $(\psi_1,\phi_1)$ *and* $(\psi_2,\phi_2)$ *are both compatible pairs. Then* $(\psi_2 \circ \psi_1, \phi_1 \circ \phi_2)$ *is compatible and for each* $q \geq 0$ *we have that* $(\psi_2 \circ \psi_1, \phi_1 \circ \phi_2)^*_q = (\psi_1,\phi_1)^*_q \circ (\psi_2,\phi_2)^*_q$.

*Proof.* Firstly we will show that $(\psi_2 \circ \psi_1, \phi_1 \circ \phi_2)$ is compatible. Since $(\psi_1,\phi_1)$ is compatible, then $\varphi_1(\psi_1(g_1)a_2) = g_1\varphi_1(a_2)$ for every $g_1 \in G_1$ and $a_2 \in A_2$. Similarly, $\varphi_2(\psi_2(g_2)a_3) = g_2\varphi_2(a_3)$ for every $g_2 \in G_2$ and $a_3 \in A_3$, because $(\psi_2,\phi_2)$ is compatible. Then, $\varphi_1 \circ \varphi_2(\psi_2 \circ \psi_1(g_1)a_3) = \varphi_1(\psi_1(g_1)\phi_2(a_3)) = g_1\phi_1 \circ \phi_2(a_3)$, for every $g_1 \in G_1, a_3 \in A_3$. Thus, $(\psi_2 \circ \psi_1, \phi_1 \circ \phi_2)$ is compatible. It remains to show that $(\psi_2 \circ \psi_1, \phi_1 \circ \phi_2)^*_q = (\psi_1,\phi_1)^*_q \circ (\psi_2,\phi_2)^*_q$. Indeed,

$$\begin{array}{l} (\psi_1,\phi_1)^*_q \circ (\psi_2,\phi_2)^*_q(f(g_1,\cdots,g_n)) = \\ \varphi_1 \circ (\psi_2,\phi_2)^*_q \circ f(\psi_1(g_1,\cdots,g_n)) = \\ \varphi_1 \circ (\psi_2,\phi_2)^*_q \circ f(\psi_1(g_1),\cdots,\psi_1(g_n)) = \\ \varphi_1 \circ \varphi_2 \circ f \circ \psi_2 \circ \psi_1(g_1,\cdots,g_n) = \\ (\psi_2 \circ \psi_1, \phi_1 \circ \phi_2)^*_q(f(g_1,\cdots,g_n)) \end{array}$$

□

***Remark* 4.3.4.** *If $\psi, \phi$ are identity maps, then the $(\psi, \phi)_q^*$ is identity map as well.*

*Proof.* It is clear that if $\psi, \phi$ are identity maps, then $(\psi, \phi)_q^*(f) = \phi \circ f \circ \psi = f$. □

## 4.4 Change of the group $G$

In this section we will study what happens to the cohomology group $\mathcal{H}^q(G, A)$ if we change the group $G$. If $\psi : G \to H$ is a continuous homomorphism of profinite groups and $\phi : B \to A$ is a group homomorphism, where $A$ is a discrete $G$-module and $B$ is a discrete $H$-module, then we have defined when $\psi, \phi$ are compatible pair. For such a compatible pair of homomorphisms we obtain a homomorphism of the groups of $q$-cochains

$$(\psi, \varphi)_q^* : C^q(H, B) \to C^q(G, A),\ for\, q \geq 0$$

given by $(\psi, \varphi)_q^*(f) = \varphi \circ f \circ \psi$. We have proved that $(\psi, \varphi)_q^*$ commutes with $\mathfrak{d}$ for every $q \geq 0$. Therefore, $(\psi, \varphi)_q^*$ induces homomorphisms

$$(\psi, \varphi)_q^* : \mathcal{H}^q(H, B) \to \mathcal{H}^q(G, A),\ for\, q \geq 0$$

of the cohomology groups. Also, we have proved that $(\psi, \varphi)_q^*$ behave functorially. In particular, for every $q \geq 0$ $\mathcal{H}^q$(A,-) is a functor from the category of discrete $G$-module to the category of abelian groups.

***Remark* 4.4.1.** *Let $I$ be a directed index set. Let also $(G_i, \pi_{ij})_I$ be a projective system of profinite groups and $(A_i, \lambda_{ij})$ be a direct system of abelian groups, where each $A_i$ is a discrete $G_i$-module, such that for each pair $i \leq j$ in $I$, the maps*

$$\pi_{ij} : G_j \to G_i \; and \; \lambda_{ij} : A_i \to A_j$$

*are compatible. Then for each $q \geq 0$, we obtain in a natural way that the family*

$$\{(\mathcal{H}^q(G_i, A_i), (\pi_{ij}, \lambda_{ij})_q^*), i \leq j,\, i, j \in I\}$$

*is a direct system.*

*Proof.* Since the maps

$$\pi_{ij} : G_j \to G_i \; and \; \lambda_{ij} : A_i \to A_j$$

are compatible, then according to proposition 4.3.2 there exists an induced homomorphism

$$(\pi_{ij}, \lambda_{ij})_q^* : \mathcal{H}^q(G_i, A_i) \to \mathcal{H}^q(G_j, A_j)$$

Additionally, if $i = j$, then

$$\begin{array}{rccc} (\pi_{ii}, \lambda_{ii})_q^* : & \mathcal{H}^q(G_i, A_i) & \rightarrow & \mathcal{H}^q(G_i, A_i) \\ & [f] & \mapsto & [\lambda_{ii} \circ f \circ \pi_{ii}] \end{array}$$

But $\pi_{ii}$ and $\lambda_{ii}$ are identity maps, so then $(\pi_{ii}, \lambda_{ii})_q^* = Id_{\mathcal{H}^q(G_i,A_i)}$. Moreover, if $i \leq j \leq k$ with $i, j, k \in I$ then

$$\begin{tikzcd} \mathcal{H}^q(G_i, A_i) \arrow[rr, "(\pi_{ik},\lambda_{ik})_q^*"] \arrow[dr, "(\pi_{ij},\lambda_{ij})_q^*"'] & & \mathcal{H}^q(G_k, A_k) \\ & \mathcal{H}^q(G_j, A_j) \arrow[ur, "(\pi_{jk},\lambda_{jk})_q^*"'] & \end{tikzcd}$$

$(\pi_{jk}, \lambda_{jk})_q^* \circ (\pi_{ij}, \lambda_{ij})_q^*([f]) = (\pi_{jk}, \lambda_{jk})_q^*([\lambda_{ij} \circ f \circ \pi_{ij}]) = [\lambda_{jk} \circ \lambda_{ij} \circ f \circ \pi_{ij} \circ \pi_{jk}] = [\lambda_{ik} \circ f \circ \pi_{ik}] = (\pi_{ik}, \lambda_{ik})_q^*([f])$ as $\pi_{ik} = \pi_{ij} \circ \pi_{jk}$ and $\lambda_{ik} = \lambda_{jk} \circ \lambda_{ij}$. Consequently, $\{(\mathcal{H}^q(G_i, A_i), (\pi_{ij}, \lambda_{ij})_q^*), i \leq j, \, i, j \in I\}$ is a direct system. □

Let

$$G = \varprojlim_I G_i \ and \ A = \varinjlim_I A_i$$

and let that $\pi_i : G \rightarrow G_i$ and $\lambda_i : A_i \rightarrow A$ are the homomorphisms which defined by the definition of projective and direct limit, respectively. Then $A$ can be considered as a discrete $G$-module in the following manner. Given $a \in A$ and $\sigma \in G$, then for some $i \in I$ and $a_i \in A_i$ one has $\lambda_i(a_i) = a$, then we define

$$\sigma(\alpha) = \lambda_i[\pi_i(\sigma)a_i]$$

This is a well defined continuous action of $G$ on $A$. It is clear that $\sigma(a) + \sigma(b) = \lambda_i[\pi_i(\sigma)a_i] + \lambda_i[\pi_i(\sigma)b_i] = \lambda_i[\pi_i(\sigma)(a_i + b_i)]\sigma(a + b)$, with $\lambda_i(a_i + b_i) = a + b$ as $\lambda_i(a_i) = a$ and $\lambda_i(b_i) = b$. Also, $(\sigma\tau)(a) = \lambda_i[\pi_i(\sigma\tau)a_i]$, $\lambda_i(a_i) = a$ and $\sigma(\tau(a)) = \sigma(\lambda_i[\pi_i(\tau)a_i])$, where $\lambda_i(a_i) = a$, then $\sigma(\tau(a)) = \sigma(\lambda_i[\pi_i(\tau)a_i]) = \lambda_i[\pi_i(\sigma)b_i]$. where $\lambda_i(b_i) = \lambda_i[\pi_i(\tau)a_i] \Rightarrow \lambda_i(b_i - \pi_i(\tau)a_i) = 0$ and then $b_i - \pi_i(\tau)a_i = 0$. So $\sigma(\tau(a)) = \lambda_i[\pi_i(\sigma)b_i] = \lambda_i[\pi_i(\sigma)\pi_i(\tau)a_i] = \lambda_i[\pi_i(\sigma\tau)a_i]$ with $\lambda_i(a_i) = a$. Thus, $\sigma(\tau(a)) = (\sigma\tau)(a)$. In addition, $1a = \lambda_i[\pi_i(1)a_i]$, where $\lambda_i(a_i) = a$, so ten $1a = \lambda_i(a_i) = a$. Moreover, it is clear that $\lambda_i$ is continuous homomorphism, because $A_i$ is a discrete space and every function from a discrete topological space to another topological space is continuous. Additionally, the action $G_i \times A_i \rightarrow A_i$ is continuous, as $A_i$ is a discrete $G_i$-module. Thus the action $G \times A \rightarrow A$ is continuous as composition of continuous maps. Therefore $A$ is a discrete $G$-module.

Now we are able to study the following general statement.

***Proposition* 4.4.2.** *Let $I$ be a directed index set. Let also $(G_i, \pi_{ij})_I$ be a projective system of profinite groups and $(A_i, \lambda_{ij})$ be a direct system of abelian groups, where each $A_i$ is a discrete $G_i$-module, such that for each pair $i \leq j$ in $I$, the maps*

$$\pi_{ij} : G_j \rightarrow G_i \ and \ \lambda_{ij} : A_i \rightarrow A_j$$

*are compatible. If* $G = \varprojlim_I G_i$ *and* $A = \varinjlim_I A_i$*, then for each* $q \geq 0$

$$\mathcal{H}^q(G, A) \cong \varinjlim_I \mathcal{H}^q(G_i, A_i)$$

*Proof.* According to remark 4.4.1 we have that the family

$$\{(\mathcal{H}^q(G_i, A_i), (\pi_{ij}, \lambda_{ij})^*_q), i \leq j, \, i, j \in I\}$$

is a direct system. So then $\varinjlim_I \mathcal{H}^q(G_i, A_i)$ makes sense. From the definition of cohomology we have that

$$\mathcal{H}^q(G, A) = \mathcal{H}^q(C^q(G, A))$$

and

$$\mathcal{H}^q(G_i, A_i) = \mathcal{H}^q(C^q(G_i, A_i))$$

Since $\varinjlim_{i\in I}$ is an exact functor in the category of abelian group, then we have that

$$\begin{aligned} \varinjlim_{i\in I} \mathcal{H}^q(G_i, A_i) &\cong \varinjlim_{i\in I} \mathcal{H}^q(C^q(G_i, A_i)) \\ &= \mathcal{H}^q(\varinjlim_{i\in I}(C^q(G_i, A_i))) \end{aligned} \tag{4.1}$$

where

$$\{(C^q(G_i, A_i), (\pi_{ij}, \lambda_{ij})^*_q), i \leq j, \, i, j \in I\}$$

is a direct system, and $\pi_{ij}, \lambda_{ij}$ are defined like the remark 4.4.1. That is $(G_i, \pi_{ij})$ is a projective system of profinite groups and $(A_i, \lambda_{ij})$ is a direct system of abelian groups, where $A_i$ are $G_i$-modules, such that for each pair $i \leq j$ in $I$, the maps

$$\pi_{ij} : G_j \to G_i \textit{ and } \lambda_{ij} : A_i \to A_j$$

are compatible. Then according to proposition 4.3.2 we have that for every $q \geq 0$ there exists an induced homomorphism

$$\begin{array}{cccc} (\pi_{ij}, \lambda_{ij})^*_q : & C^q(G_i, A_i) & \to & C^q(G_j, A_j) \\ & f & \mapsto & \lambda_{ij} \circ f \circ \pi_{ij} \end{array}$$

In addition, if $i = j$ then

$$(\pi_{ii}, \lambda_{ii})^*_q : C^q(G_i, A_i) \to C^q(G_i, A_i)$$

and $\pi_{ii}, \lambda_{ii}$ are identity maps. Thus, $(\pi_{ii}, \lambda_{ii})^*_q = Id_{C^q(G_i,A_i)}$. If $i \leq j \leq k, \;\; i, j, k \in I$, then

$$\begin{tikzcd}
C^q(G_i, A_i) \arrow[rr, "(\pi_{ik},\lambda_{ik})^*_q"] \arrow[dr, "(\pi_{ij},\lambda_{ij})^*_q"'] & & C^q(G_k, A_k) \\
& C^q(G_j, A_j) \arrow[ur, "(\pi_{jk},\lambda_{jk})^*_q"'] &
\end{tikzcd}$$

$(\pi_{jk}, \lambda_{jk})^*_q \circ (\pi_{ij}, \lambda_{ij})^*_q(f) = (\pi_{jk}, \lambda_{jk})^*_q(\lambda_{ij} \circ f \circ \pi_{ij}) = \lambda_{jk} \circ \lambda_{ij} \circ f \circ \pi_{ij} \circ \pi_{jk} = \lambda_{ik} \circ f \circ \pi_{ik} = (\pi_{ik}, \lambda_{ik})^*_q(f)$ as $\pi_{ik} = \pi_{ij} \circ \pi_{jk}$ and $\lambda_{ik} = \lambda_{jk} \circ \lambda_{ij}$.
Therefore $\{(C^q(G_i, A_i), (\pi_{ij}, \lambda_{ij})^*_q), i \leq j,\, i, j \in I\}$ form a direct system. So then $\varinjlim_{i \in I}(C^q(G_i, A_i))$ makes sense. In order to show that

$$\mathcal{H}^q(G, A) \cong \varinjlim_{I} \mathcal{H}^q(G_i, A_i)$$

it suffices to show that there exist isomorphisms

$$\varinjlim_{i \in I} C^q(G_i, A_i) \cong C^q(G, A),\ q \geq 0$$

which commute with the maps $\mathfrak{d}_q$. Then from equation 4.1 we have that

$$\begin{aligned}
\varinjlim_{i \in I} \mathcal{H}^q(G_i, A_i) &\cong \mathcal{H}^q(\varinjlim_{i \in I}(C^q(G_i, A_i))) \\
&\cong \mathcal{H}^q(C^q(G, A)) = \mathcal{H}^q(G, A)
\end{aligned}$$

For every $i \in I$ we define

$$f_i : C^q(G_i, A_i) \to C^q(G, A)$$

with $f_i(x_i) = \lambda_i \circ x_i \circ \pi_i$, where $f_i := (\pi_i, \lambda_i)^*_q$

$$\begin{tikzcd}
\varinjlim_{i \in I} C^q(G_i, A_i) \arrow[rr, dashed, "\theta"] & & C^q(G, A) \\
& C^q(G_i, A_i) \arrow[ul, "\varphi_i"'] \arrow[ur, "f_i"] \arrow[d, "\varphi_{ij}"] & \\
& C^q(G_j, A_j) \arrow[uul, "\varphi_j"] \arrow[uur, "f_j"'] &
\end{tikzcd}$$

where $\varphi_{ij} := (\pi_{ij}, \lambda_{ij})^*_q$. By definition of direct limit we have that $\varphi_i = \varphi_j \circ \varphi_{ij}$. Also,it is easy to see that $f_i = f_j \circ \varphi_{ij}$. Indeed, for $i \leq j$ then $f_j \circ \varphi_{ij}(x_i) = f_j((\pi_{ij}, \lambda_{ij})^*_q(x_i) = f_j(\lambda_{ij} \circ x_i \circ \pi_{ij}) = \lambda_j \circ \lambda_{ij} \circ x_i \circ \pi_{ij} \circ \pi_j = \lambda_i \circ x_i \circ \pi_i = f_i(x_i)$, as $\pi_i = \pi_{ij} \circ \pi_j$ and $\lambda_i = \lambda_j \circ \lambda_{ij}$. So then according to universal property of direct limit there exists a unique homomorphism

$$\theta : \varinjlim_{i \in I} C^q(G_i, A_i) \to C^q(G, A)$$

satisfying that $f_i = \theta \circ \varphi_i$. Thereafter we will show that $\theta$ commutes with $\eth$ in the following sense: for every $i \in I$ the diagram

$$\begin{tikzcd} C^q(G_i, A_i) \arrow[r, "\eth_{q+1}"] \arrow[d, "(\pi_i,\lambda_i)^*_q"'] & C^{q+1}(G_i, A_i) \arrow[d, "(\pi_i,\lambda_i)^*_{q+1}"] \\ C^q(G, A) \arrow[r, "\eth_{q+1}"'] & C^{q+1}(G, A) \end{tikzcd}$$

commutes. But the above diagram is commutative according to proposition 4.3.2. It remains to show that $\theta$ is injective and surjective.
For the injectivity, let $x \in \varinjlim_{i \in I} C^q(G_i, A_i)$ with $\theta(x) = 0$. From proposition 2.4.4 we have that

$$\varinjlim_{i \in I} C^q(G_i, A_i) = \bigcup_{i \in I} \varphi_i(C^q(G_i, A_i))$$

Thus there is $k \in I$ such that $\varphi_k(x_k) = x$ with $x_k \in C^q(G_k, A_k)$. For $i \geq k$ let $x_i = \varphi_{ki}(x_k)$. Then $0 = \theta(x) = \theta(\varphi_k(x_k)) = \theta \circ \varphi_k(x_k) = f_k(x_k) = f_i \circ \varphi_{ki}(x_k) = f_i(x_i) = (\pi_i, \lambda_i)^*_q(x_i) = \lambda_i \circ x_i \circ \pi_i$, that is for $i \geq k$ $\lambda_i \circ x_i \circ \pi_i = 0$.
For $i \geq k$ we define

$$X = \{\sigma_i = (\sigma_{i_1}, \dots, \sigma_{i_q}) \in G_i^q \,|\, x_i(\sigma_i) \neq 0\}$$

We will show that for some $i \geq k, \;\; X_i = \emptyset$, this implies that $x_i(\sigma) = 0$, for every $\sigma \in X_i$ and since $x_i$ is continuous then $x_i = 0$. Then $x_i = 0 \Rightarrow \varphi_{ki}(x_k) = 0 \Rightarrow \varphi_i \circ \varphi_{ki}(x_k) = 0 \Rightarrow \varphi_k(x_k) = 0 \Rightarrow x = 0$. This implies that $\theta$ is injective. It remains to show that for some $i \geq k, \; X_i = \emptyset$. We have that $G_i^q$ is compact from Tychonoff's theorem since $G_i$ is compact. So then, $x_i(G_i^q)$ is compact, because $x_i$ is continuous. In addition, the abelian groups $A_i$ are topological groups equipped with discrete topology, as it is a discrete $G_i$-modules. So then $x_i(G_i^q) \subseteq A_i$ is a topological space equipped with discrete topology. We assume that $x_i(G_i^q)$ is infinite. Then $x_i(G_i^q)$ is covered of infinite number of singleton sets. But then there isn't a finite subcover. This means that $x_i(G_i^q)$ isn't compact. But this is impossible, since $x_i(G_i^q)$ is compact. Thus, $x_i(G_i^q)$ is finite set and then $x_i$ takes only finite number of values. Hence $X_i$ is finite and therefore it is compact. On the other hand $i \geq j \geq k$ implies that

$$\pi_{ij}(X_i) \subseteq X_j$$

Indeed, if $\sigma_i \in X_i$, then $x_i(\sigma_i) \neq 0$. In our case $j \leq i$, so $\varphi_{ji}(x_j) = x_i$. Thus, $x_i(\sigma_i) \neq 0 \Rightarrow \varphi_{ji} \circ x_j(\sigma_i) \neq 0 \Rightarrow (\lambda_{ji} \circ x_j \circ \pi_{ji})(\sigma_i) \neq 0$ and since $\lambda_{ji}$ is a homomorphism then $x_j \circ \pi_{ji}(\sigma_i) \neq 0$. This means that $\pi_{ji}(\sigma_i) \in X_j$, that is $\pi_{ji}(X_i) \subseteq X_j$.

$$\begin{tikzcd}
X_j \arrow[rr, "\pi_{kj}"] & & X_k \\
& X_i \arrow[ul, "\pi_{ji}"] \arrow[ur, "\pi_{ki}"'] &
\end{tikzcd}$$

and $\pi_{kj} \circ \pi_{ji}(\sigma_i) = \pi_{kj}(\sigma_j) = \sigma_k = \pi_{ki}(\sigma_i)$.
Therefore,

$$\{(X_j, \pi_{ij}),\, i \geq j \geq k,\, i, j \geq k\}$$

form a projective system of compact spaces. If $\sigma = (\sigma_1, \dots, \sigma_q) \in \varinjlim_{i \geq k} X_i \subseteq G^q$, then it is clear that $(\theta(x))(\sigma) \neq 0$. Indeed,

$$\begin{aligned}
&(\theta(x))(\sigma) = (\theta(\varphi_k(x_k)))(\sigma) = (f_k(x_k))(\sigma) = \\
&(f_k(x_k))(\sigma) = ((f_i \circ \varphi_{ki})(x_k)(\sigma) = (f_i(x_i))(\sigma) = \\
&((\pi_i, \lambda_i)_q^*(x_i))(\sigma) = (\lambda_i \circ x_i \circ \pi_i)(\sigma) = \\
&(\lambda_i \circ x_i)(\sigma_i)
\end{aligned}$$

But $x_i(\sigma_i) \neq 0$ and $\lambda_i$ is a homomorphism, then $(\lambda_i \circ x_i)(\sigma_i) \neq 0$. So $(\theta(x))(\sigma) \neq 0$. But from our hypothesis we have that $\theta(x) = 0$. Hence, $\varinjlim_{i \geq k} X_i = \emptyset$. Therefore, according to theorem 2.2.5 there exists $i \geq k$ such that $X_i = \emptyset$. It remains to show that $\theta$ is surjective. Let $x \in C^q(G, A)$, that is $x : G^q \to A$ is continuous. We will prove that there exists $y \in \varinjlim_{i \in I} C^q(G_i, A_i)$ such that $\theta(y) = x$. We have known from proposition 2.4.4

$$\varinjlim_{i \in I} C^q(G_i, A_i) = \bigcup_{i \in I} \varphi_i(C^q(G_i, A_i))$$

Thus there is $k \in I$ such that $\varphi_k(x_k) = y$ with $x_k \in C^q(G_k, A_k)$. For $i \geq k$ let $x_i = \varphi_{ki}(x_k)$, then $\theta(y) = \theta(\varphi_k(x_k)) = f_k(x_k) = f_i \circ \varphi_{ki}(x_k) = f_i(x_i) = (\pi_i, \lambda_i)_q^*(x_i) = \lambda_i \circ x_i \circ \pi_i$. So it suffices to show that there exists a continuous map $x_i \in C^q(G_i, A_i)$ such that $x = \lambda_i \circ x_i \circ \pi_i$ for some $i \in I$. We have that $G^q$ is compact from Tychonoff's theorem since $G$ is compact. Also, $x(G^q)$ is compact, because $x$ is continuous. Thus, $x(G^q)$ is finite set, since $A$ is a discrete $G$-module, and then $x_i$ takes only finite number of values, say

$$x(G^q) = \{a_1, \dots, a_n\} \subseteq A$$

Then there exists $j \in I$ such that $\lambda_j(A_j) = x(G^q)$. Moreover, we have that $x : G^q \to A$ is continuous and $A$ is a discrete $G$-module, then $x$ is locally constant according to proposition 1.1.10. This means that for each $\sigma \in G^q$ there is an open neighborhood $U$ of $\sigma$ such that $x$ is constant on $U$. This implies that for each $g \in G$ there exists an open neighborhood $U'$ of $g$ in $G$ such that $x$ is constant on $U'^q$ of $G^q$. So for $g = 1$ there exists an open neighborhood $U'$ of $1$ in $G$ such that $x$ is constant on $U'^q$ of $G^q$. But $G$ is a profinite group and from lemma 2.3.6 there exists an open normal subgroup $U_l$ of $G$ with $U_l \subseteq U'$ such that $x$ is constant on $U_l^q$ of $G^q$. Additionally, $x$ is constant on the cosets of $U_l^q$ in $G^q$. Also, the set

$$\{\pi_k^{-1}(U_k),\, where\, U_k \trianglelefteq G_k, U_k = open, \forall k \in I\}$$

form a basis of open neighborhood of 1 in $G$. Hence, there exists $U_i \trianglelefteq G_i$, $U_i\ is\ open$ with $\pi_i^{-1}(U_i) = U \subseteq U_l$ for some $i$. So we can define $G/U$ and $(G/U)^q$ as well. We may assume that $i \geq j$. Then $x = \bar{x} \circ p$, where $p : G^q \to G^q/U^q$ is the natural projection and $\bar{x} : G^q/U^q \to A$ is defined by $\bar{x}(\sigma U^q) = x(\sigma)$. Clearly, $\bar{x}$ is well defined. Indeed, let $\sigma U^q = \tau U^q \Rightarrow \sigma\tau^{-1} \in U^q$. But $U^q \subseteq U_l^q \subseteq U'^q$, since $U \subseteq U_l \subseteq U'$. So $x(g') = x(1)$ for every $g' \in U'^q$ and then $x(g) = x(1)$ for every $g \in U^q$. Thus,

$$\begin{aligned} & x(\sigma\tau^{-1}) = x(1) \Leftrightarrow x(\sigma)x(\tau) = 1 \Leftrightarrow \\ & x(\sigma) = x(\tau) \Leftrightarrow \bar{x}(\sigma U^q) = \bar{x}(\tau U^q) \end{aligned}$$

The homomorphism $\pi_i$ induce the homomorphism $w_i^q : G^q \to G_i^q/U_i^q$ where $w_i^q(g_1, \dots, g_q) = (\pi_i(g_1), \dots, \pi_i(g_q)U_i^q$. Then,

$$\begin{aligned} Kerw_i^q &= \{(g_1, \dots, g_q) \in G^q : (\pi_i(g_1), \dots, \pi_i(g_q)) \in U_i^q\} \\ &= \{(g_1, \dots, g_q) \in G^q : (g_1, \dots, g_q) \in (\pi_i^{-1}(U_i))^q = U^q\} = U^q \end{aligned}$$

So then induced a homomorphism

$$\pi_i' : G^q/U^q \to G_i^q/U_i^q$$

where $\pi_i'((g_1, \dots, g_q)U^q) = (\pi_i(g_1), \dots, \pi_i(g_q))U_i^q$. In particular, $\pi_i'$ is injective, since

$$\begin{aligned} Ker\pi_i' &= \{(g_1, \dots, g_q)U^q \in G^q/U^q : (\pi_i(g_1), \dots, \pi_i(g_q)) \in U_i^q\} \\ &= \{(g_1, \dots, g_q)U^q \in G^q/U^q : (g_1, \dots, g_q) \in (\pi_i^{-1}(U_i))^q = U^q\} = U^q \end{aligned}$$

Let $\overline{x_i} : (G_i/U_i)^q \to A_i$ such that $\lambda_i \circ \overline{x_i} \circ \pi_i' = \bar{x}$.

$$\underbrace{G^q/U^q \xrightarrow{\pi_i'} G_i^q/U_i^q \xrightarrow{\bar{x}_i} A_i \xrightarrow{\lambda_i} A}_{\bar{x}}$$

We define $x_i = \bar{x} \circ \pi_i$, where $\pi_i : G_i^q \to G_i^q/U_i^q$ is the natural projection.

$$\underbrace{G_i^q \xrightarrow{p_i} G_i^q/U_i^q \xrightarrow{\bar{x}_i} A_i}_{x_i}$$

Clearly, $x_i$ is continuous, since $\bar{x}_i, p_i$ are continuous. Moreover, $x = \bar{x} \circ p = \lambda_i \circ \bar{x}_i \circ \pi_i' \circ p$ and $\lambda_i \circ x_i \circ \pi_i = \lambda_i \circ \bar{x}_i \circ p_i \circ \pi_i$.

$$G^q \xrightarrow{\pi_i} G_i^q \xrightarrow{\bar{x}_i} G_i^q/U_i^q\ and\ G^q \xrightarrow{p} G_i^q \xrightarrow{\pi_i'} G_i^q/U_i^q$$

and it is clear that $\pi_i' \circ p = p_i \circ \pi_i$, since

$$\pi_i'(p(g_1, \ldots, g_q)) = \pi_i'((g_1, \ldots, g_q)U^q) = (\pi_i(g_1), \ldots, \pi_i(g_q))U_i^q$$
$$p_i(\pi_i(g_1, \ldots, g_q)) = p_i(\pi_i(g_1), \ldots, \pi_i(g_q)) = (\pi_i(g_1), \ldots, \pi_i(g_q))U_i^q$$

Therefore $x = \lambda_i \circ x_i \circ \pi_i$. □

***Corollary* 4.4.3.** *Let $G$ be a profinite group and $A$ be a discrete $G$-module. Then*

$$\mathcal{H}^q(G, A) = \varinjlim_{U \in \mathcal{U}} \mathcal{H}^q(G/U, A^U)$$

*where $\mathcal{U}$ is the set of all open normal subgroups of $G$ and $A^U = \{b \in A \,|\, \sigma b = b, \forall \sigma \in U\}$.*

*Proof.* We have proved in theorem 2.3.9 that

$$G = \varprojlim_{U \in \mathcal{U}} G/U$$

Since $A$ is a discrete $G$-module then

$$A = \bigcup_{U \in \mathcal{U}} A^U = \varinjlim_{U \in \mathcal{U}} A^U$$

Also, the $A^U$ is a $G/U - module$ with the action

$$\begin{array}{ccc} G/U \times A^U & \to & A^U \\ (gU, a) & \mapsto & (gU)a = ga, \quad g \in G, a \in A^U \end{array}$$

Clearly, $(A^U, +)$ is an abelian group and also $(gU)(a+b) = g(a+b) = ga + gb = (gU)a + (gU)b$, $(g_iUg_2U)a = (g_1g_2U)a = g_1g_2a = g_1(g_2a) = g_1((g_2U)a) = (g_1U)((g_2U)a)$ and $(U)a = a$. Thus, $A^U$ is a unitary $G/U{-}module$. In addition, the action is continuous by construction. So then $A^U$ is a discrete $G/U$-module. Finally, it is plain that if $U \leqslant V$ with $U, V$ are open normal subgroups of $G$ and $A$ a discrete $G$-module, then there exists a normal inclusion of abelian groups

$$inc_{U,V} : A^V \hookrightarrow A^U$$

Moreover, the $p_{U,V} : G/U \to G/V$, where $gU \mapsto gV$, and the inclusion $inc_{U,V}$ are compatible maps. Indeed, let $gU \in G/U$ and $a \in A^V$ then

$$inc_{U,V}(p_{U,V}(gU)a) = inc_{U,V}((gV)a) = (gV)a =$$
$$ga = (gU)a = (gU)inc_{U,V}(a)$$

Therefore, according to proposition 4.4.2 we have that for each $q \geq 0$

$$\mathcal{H}^q(G, A) = \varinjlim_{U \in \mathcal{U}} \mathcal{H}^q(G/U, A^U)$$

□

## 4.5 Special Mappings

In this section we will study some special homomorphisms of cohomology groups, which they connect the cohomology group of a group $G$ with the cohomology group of a subgroup of $G$.

### ⤳ *The Inflation*

Let $N$ be a closed normal subgroup of a profinite group $G$, and let also $A$ be a discrete $G$-module. We have proved that the action of $G/N$ in $A^N$

$$\begin{array}{ccc} G/N \times A^N & \to & A^N \\ (\sigma N, a) & \mapsto & \sigma N = \sigma a, \quad \sigma \in G, a \in A^N \end{array}$$

is continuous. Thus, $A^N$ is a discrete $G/N$-module. It is plain that the projection $p_N : G \to G/N$, $g \mapsto gN$ and the inclusion $i_N$; $A^N \to A$ are compatible maps. Indeed, $A$ is a discrete $G$-module, $A^N$ is a discrete $G/N$-module, $i_N$ is a continuous homomorphism and $i_N(p_N(g)a) = gi_N(a)$ for $g \in G, a \in A^N$, since $i_N(p_N(g)a) = i_N((gN)a) = i_N(ga) = ga = gi_N(a)$. So then according to proposition 4.3.2 we have that for each $q \geq 0$ induced a homomorphism

$$(p_N, i_N)_q^* : \mathcal{H}^q(G/N, A^N) \to \mathcal{H}^q(G, A)$$

that is called *Inflation* and is denoted by

$$Inf = Inf_G^{G/N}$$

That is,

$$Inf = Inf_G^{G/N} : \mathcal{H}^q(G/N, A^N) \to \mathcal{H}^q(G, A)$$

In particular for $q = 0$:

$$Inf = Inf_G^{G/N} : \mathcal{H}^0(G/N, A^N) \to \mathcal{H}^0(G, A)$$

is the identity map, because $\mathcal{H}^0(G, A) = A^G$ and $\mathcal{H}^0(G/N, A^N) = A^G$.

We assume that $q > 0$ and $x \in \bar{x} \in \mathcal{H}^q(G/N, A^N)$, this means that $x : (G/N)^q \to A^N$ continuous $q-cocycle$. Then the $Inf(\bar{x})$ has as one of its representatives a continuous $q - cocycle$ $y : G^q \to A$ satisfying that $y(\sigma_1, \dots, \sigma_q) = x(\sigma_1 N, \dots, \sigma_q N)$.

**Proposition 4.5.1.** *If $f : G \to G_1$ and $g : G_1 \to G_2$ are surjective continuous homomorphisms, then*

$$Inf_G^{G_1} \circ Inf_{G_1}^{G_2} = Inf_G^{G_2}$$

*Proof.*

$$G \xrightarrow{f} G_1 \xrightarrow{g} G_2$$

where $G_1 = G/N$ and $G_2 = G/H$, $N \subseteq H$.

$$Inf_G^{G_1} : \mathcal{H}^q(G/N, A^N) \to \mathcal{H}^q(G, A)$$

$$Inf_{G_1}^{G_2} : \mathcal{H}^q(G/H, A^H) \to \mathcal{H}^q(G/N, A^N)$$

$$Inf_G^{G_2} : \mathcal{H}^q(G/H, A^H) \to \mathcal{H}^q(G, A)$$

Also, $A^H \overset{i_{H,N}}{\hookrightarrow} A^N \overset{i_N}{\hookrightarrow} A$. Thus, from proposition 4.3.3 we have that

$$(g \circ f, i_N \circ i_{H,N})_q^* = (f, i_N)_q^* \circ (g, i_{H,N})_q^* \Rightarrow$$

$$Inf_G^{G_1} \circ Inf_{G_1}^{G_2} = Inf_G^{G_2}$$

□

***Proposition* 4.5.2.** *Let $N$ be a closed normal subgroup of a profinite group $G$. Let also $f : A \to B$ be a $G$-homomorphism. Then $f$ induces a $G/N$-homomorphism*

$$f^N : A^N \to B^N$$

*and the following diagram*

$$\begin{tikzcd}
\mathcal{H}^q(G/N, A^N) \arrow[r, "(id, f^N)_q^*"] \arrow[d, "Inf"'] & \mathcal{H}^q(G/N, B^N) \arrow[d, "Inf"] \\
\mathcal{H}^q(G, A) \arrow[r, "(id, f)_q^*"'] & \mathcal{H}^q(G, B)
\end{tikzcd}$$

*commutes. That is $Inf$ is a morphism of the functors $\mathcal{H}^q(G/N, *^N)$ and $\mathcal{H}^q(G/N, *)$ on the functor of discrete $G$-modules, for every $q \in \mathbb{Z}$.*

*Proof.* We have that $f^N : A^N \to B^N$, $f^N(a) = f(a)$, for $a \in A$ and then $f^N((gN)a) = f^N(ga) = f(ga) = gf(a) = gf^N(a) = (gN)f^N(a)$. Thus, $f^N$ is a $G/N$-homomorphism. It remains to show that $Inf \circ (id, f^N)_q^* = (id, f)_q^* \circ Inf$. Indeed, let $g \in C^q(G/N, A^N)$, then $Inf \circ (id, f^N)_q^*([g]) = Inf([f^N \circ g \circ id]) = Inf([f^N \circ g]) = [i_N \circ f^N \circ g \circ p_N]$, since $Inf = (p_N, i_N)_q^*$, with $p_N : G \to G/N$, $g \mapsto gN$ and $i_N : B^N \hookrightarrow B$, $b \mapsto b$. Also, $Inf = (p_N, i'_N)_q^*$, where $p_N : G \to G/N$, $i'_N : A^N \hookrightarrow A$, so then $(id, f)_q^* \circ Inf([g]) = (id, f)_q^*([i'_N \circ g \circ p_N]) = [f \circ i_N \circ g \circ p_N \circ id] = [f \circ i'_N \circ g \circ p_N]$.

$$\begin{tikzcd}
A^N \arrow[r, "f^N"] \arrow[d, hook, "i'_N"'] & B^N \arrow[d, hook, "i_N"] \\
A \arrow[r, "f"'] & B
\end{tikzcd}$$

But $i_N \circ f^N(a) = f^N(a) = f(a) = i'_N(a)$ for every $a \in A^n$. So $Inf \circ (id, f^N)_q^*([g]) = (id, f)_q^* \circ Inf([g])$. □

***Proposition* 4.5.3.** *Let* $0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$ *be a short exact sequence of discrete G-modules and we assume that* $0 \longrightarrow A^n \xrightarrow{i^N} B^N \xrightarrow{j^N} C^N \longrightarrow 0$ *is also exact. Then the following diagram*

$$\begin{tikzcd}
\mathcal{H}^q(G/N, C^N) \arrow[r, "\delta"] \arrow[d, "Inf"'] & \mathcal{H}^{q+1}(G/N, A^N) \arrow[d, "Inf"] \\
\mathcal{H}^q(G, C) \arrow[r, "\delta"'] & \mathcal{H}^{q+1}(G, A)
\end{tikzcd}$$

*commutes of every* $q \geq 0$*, where* $\delta$ *is the connecting homomorphism.*

### $\rightsquigarrow$ ***The Restriction***

Let $S$ be a closed subgroup of a profinite group $G$. For each discrete $G$-module $A$ we have that $A^G \subseteq A^S$. This inclusion defines a homomorphism

$$\mathcal{H}^0(G, A) \to \mathcal{H}^0(S, A)$$

and this extends to a sequence of homomorphisms

$$Res := Res_S^G : \mathcal{H}^q(G, A) \to \mathcal{H}^q(S, A),', \forall q \geq 0$$

that are called restrictions[1].

We can describe these homomorphisms in terms of cochains as follows. Let $x : G^q \to A$ be a continuous $q$-cocycle, then a representative continuous $q - cocycle$ $y :, S^q \to A$ of $Rex(\bar{x}) \in \mathcal{H}^q(S, A)$ given by

$$y(\sigma_1, \sigma_2, \ldots, \sigma_q) = x(\sigma_1, \sigma_2, \ldots, \sigma_q) \in A, \ \sigma_1, \ldots, \sigma_q \in S$$

We notice that if $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is an exact sequence of discrete $G - modules$, then it is still exact when it considered as a sequence of discrete $S - modules$. Thus, by definition of restriction $Res$ we obtain that the following diagram

$$\begin{tikzcd}
\cdots \arrow[r] & \mathcal{H}^{q-1}(G, A) \arrow[r, "\delta"] \arrow[d, "Res"'] & \mathcal{H}^q(G, A) \arrow[r] \arrow[d, "Res"] & \mathcal{H}^q(G, B) \arrow[r] \arrow[d, "Res"] & \mathcal{H}^q(G, C) \arrow[r] \arrow[d, "Res"] & \cdots \\
\cdots \arrow[r] & \mathcal{H}^{q-1}(S, C) \arrow[r, "\delta"] & \mathcal{H}^q(S, A) \arrow[r] & \mathcal{H}^q(S, B) \arrow[r] & \mathcal{H}^q(S, C) \arrow[r] & \cdots
\end{tikzcd}$$

is commutative with exact rows.

[1] $Res = (incl, id)_q^*$, where $incl : \ S \hookrightarrow G$ and $id : \ A \to A$.

***Proposition* 4.5.4.** *Let $T \subseteq S \subseteq G$ be profinite groups. Then*

$$Res^S_T \circ Res^G_S = Res^G_T$$

*and $T \subseteq S$ closed subgroups of $G$.*

*Proof.*

$$Res^S_T : \mathcal{H}^q(S, A) \to \mathcal{H}^q(T, A)$$
$$Res^G_S : \mathcal{H}^q(G, A) \to \mathcal{H}^q(S, A)$$
$$Res^G_T : \mathcal{H}^q(G, A) \to \mathcal{H}^q(T, A)$$

$S \overset{i_1}{\hookrightarrow} G,\ A \overset{id}{\to} A,$
$T \overset{i_2}{\hookrightarrow} G,\ A \overset{id}{\to} A,$
$T \overset{i_3}{\hookrightarrow} S,\ A \overset{id}{\to} A$
The maps $(i_1, id), (i_3, id)$ are compatible maps. Thus according to proposition 4.3.3 we have that

$$(i_1 \circ i_3, id \circ id)^*_q = (i_3, id)^*_q \circ (i_1, id)^*_q$$
$$Res^S_T \circ Res^G_S = Res^G_T$$

. □

# Chapter 5

# Some Applications of Cohomology

## 5.1 Group Extensions

The extension problem in group theory is the classification of all extension groups of a given group A by a given group G. In this section we study the extension problem for the case of abelian groups and their connection with cohomology.

Let $A$ be an abelian multiplicative group and $G$ be an arbitrary multiplicative group. Every exact sequence

$$1 \to A \overset{i}{\to} U \overset{j}{\to} G \to 1 \tag{5.1}$$

will be called **group extension of A by G**. Since $i$ is an inclusion map then $i(A) \cong A \leqslant U$, but $i(A) = Kerj \trianglelefteq U$, so then $A \trianglelefteq U$ and $U/A \cong G$. We would like to determine the possible solutions of this problem, that is, we want to find all group extensions $U$ of $A$ such that $U/A \cong G$.

Now we consider the map $p: G \to U$ satisfying that for every $g \in G$ we choose a representative $u_g \in U$ so that $j(u_g) = g$, that is $j \circ p = 1_G$. The set

$$\{u_g \mid g \in G\}$$

will be called a **complete system of representatives** for $G$ in $U$ (or section for $G$ in $U$). (Of course, it is really the map $p: G \to U$, where $g \mapsto u_g$ which should be called section). We have that

$$\begin{aligned} &j(u_g u_\tau) = j(u_g)j(u_\tau) = g\tau = j(u_{g\tau}) \Rightarrow j(u_g u_\tau) = j(u_{g\tau}) \\ &\Rightarrow j(u_g u_\tau u_{g\tau}^{-1}) = 1 \Rightarrow u_g u_\tau u_{g\tau}^{-1} \in Kerj = Imi \end{aligned}$$

Thus there exists unique[1] $a_{g,\tau} \in A$ such that $u_g u_\tau u_{g\tau}^{-1} = a_{g,\tau}$, which implies that

$$u_g u_\tau = a_{g,\tau} u_{g\tau}, \ \forall g, \tau \in G \tag{5.2}$$

[1] Since $i$ is injective.

Clearly, $\{a_{g,\tau} \mid g, \tau \in G\}$ is a standard 2-cochain of $G$ in $A$.

For purposes of simplicity we assume that $A$ is an abelian group, because it suffices for our needs. Now, $U$ acts on $A$ by inner automorphisms, that is $U \times A \to A$, $(u, a) \mapsto a^u = uau^{-1}$. Since $A$ is abelian then $A$ acts trivially on $A$, so there is induced a "natural" action of $G$ on $A$. In more details we define the action

$$\begin{array}{ccll} G \times A & \to & A & \\ (g, a) & \mapsto & a^g = u_g a u_g^{-1} & \qquad (\star) \end{array}$$

***Proposition* 5.1.1.** *The abelian group $A$ equipped with the above action becomes a $G$-module.*

*Proof.* $(A, +)$ is an abelian group. Also, let $a, b \in A$ and $\sigma \in G$, then $(ab)^\sigma = u_\sigma ab u_\sigma^{-1} = u_\sigma a u_\sigma^{-1} u_\sigma b u_\sigma^{-1} = a^\sigma b^\sigma$. In addition, let $a \in A$ and $\sigma, \tau \in G$, then $(a^\tau)^\sigma = (u_\tau a u_\tau^{-1})^\sigma = u_\sigma u_\tau a u_\tau^{-1} u_\sigma^{-1} = u_\sigma u_\tau a (u_\sigma u_\tau)^{-1} \overset{5.2}{=} a_{\sigma,\tau} u_{\sigma\tau} a u_{\sigma\tau}^{-1} a_{\sigma,\tau}^{-1} = a_{\sigma,\tau} a^{\sigma\tau} a_{\sigma,\tau}^{-1} = a^{\sigma\tau}$. Finally, $a^1 = u_1 a u_1^{-1} = a$, since $u_1 \in A$. Therefore, $A$ is a $G$-module. □

***Proposition* 5.1.2.** *This action of $G$ on $A$ is independent of the choice of representatives $\{u_g\}$.*

*Proof.* Let $\{u_g,\, g \in G\}$ be a section of $G$ in $U$. Let also $\{v_\sigma \mid \sigma \in G\}$ be another section of $G$ in $U$. If $g \in G$, then $j(u_g) = g = j(v_g) \Rightarrow j(u_g) = j(v_g) \Rightarrow i(v_g u_g^{-1}) = 1 \Rightarrow v_g u_g^{-1} \in Ker j = Im i$. So then there exists a unique $a_\sigma \in A$ such that $i(a_\sigma) = v_g u_g^{-1}$, but $i(A) \cong A$ and so $i(a_g) = c_g \in A$. Thus, $c_g = v_g u_g^{-1} \Rightarrow v_g = c_g u_g$, with $c_g \in A$. Then, $a^g = v_g a v_g^{-1} = c_g u_g a u_g^{-1} c_g^{-1} = u_g a u_g^{-1}$, since $c_g, u_g a u_g^{-1} \in A$ and $A$ is abelian group. Therefore, the action is independent of the section. □

Thus, we can fix a section, say $\{u_g \mid g \in G\}$. Then, every $u \in U$ has a unique expression of the form

$$u = a u_g, \quad \textit{with } a \in A,\ g \in G$$

which is given by $j(u) = g$ and $a = u u_g^{-1}$. Also the action can be written as

$$a^g u_g = u_g a \tag{5.3}$$

It follows that the multiplication in $U$ can be described in terms of the multiplications in $A$ and in $G$, the action of $G$ on $A$ and the 2-cochain $\{a_{g,\tau}\}$. Hence, if $u, v \in U$ then there exists $a \in A$ such that $u = a u_g$, for some $g \in G$ and there exists $\beta \in A$ such that $u = \beta u_\tau$, for some $\tau \in G$. Then $uv = a u_g \beta u_\tau = a \beta^g u_g u_\tau = a \beta^g a_{g,\tau} u_{g\tau}$, that is

$$uv = a \beta^g a_{g,\tau} u_{g\tau}$$

Moreover, associativity in $U$, since $U$ is a group, leads to the below equality for every $g, \tau, \rho \in G$

$$(u_g u_\tau) u_\rho = (a_{g,\tau} u_{g\tau}) u_\rho = a_{g,\tau} (u_{g\tau} u_\rho) = a_{g,\tau} a_{g\tau,\rho} u_{g\tau\rho}$$

and

$$u_g(u_\tau u_\rho) = u_g(a_{\tau,\rho}u_{\tau\rho})u_g a_{\tau,\rho}u_{\tau\rho} = a^g_{\tau,\rho}u_g u_{\tau\rho} = a^g_{\tau,\rho}a_{g,\tau\rho}u_{g\tau\rho}$$

Therefore, for every $g, \tau, \rho \in G$

$$a_{g,\tau}a_{g\tau,\rho} = a^g_{\tau,\rho}a_{g,\tau\rho} \tag{5.4}$$

This formula is the multiplicative form of the factor sets. Thus, $\{a_{g,\tau}\}$ is a standard 2-cocycle of $G$ in $A$.

If now $\{v_g \mid g \in G\}$ is another section of $G$ in $U$, then $v_g = c_g u_g$, with $c_g \in A$. Additionally, $v_g v_\tau = \beta_{g,\tau}v_{g\tau}$ where $\{\beta_{g,\tau}\}$ is also a standard 2-cocycle of $G$ in $A$. One may wonder which is the connection between $\{a_{g,\tau}\}$ and $\{\beta_{g,\tau}\}$. From the equation

$$\begin{aligned} v_g v_\tau &= (c_g u_g)(c_\tau u_\tau) = c_g c^g_\tau u_g u_\tau = c_g c^g_\tau a_{g,\tau}u_{g\tau} \\ &= c_g c^g_\tau a_{g,\tau}c^{-1}_{g\tau}v_{g\tau} = c_g c^g_\tau c^{-1}_{g\tau}a_{g,\tau}v_{g\tau} \end{aligned}$$

This implies that $\beta_{g,\tau}v_{g\tau} = c_g c^g_\tau c^{-1}_{g\tau}a_{g,\tau}u_{g\tau}$ and then

$$\beta_{g,\tau}a^{-1}_{g,\tau} = c_g c^g_\tau c^{-1}_{g\tau}$$

Thus, $\{\beta_{g,\tau}a^{-1}_{g,\tau}\}$ is a 2-coboundary of $G$ in $A$, that is

$$\{\beta_{g,\tau}a^{-1}_{g,\tau}\} \in \mathcal{B}_2 \Leftrightarrow \{\beta_{g,\tau}\}\mathcal{B}_2 = a_{g,\tau}\mathcal{B}_2$$

This means that the cocycles $\{a_{g,\tau}\}$ and $\{\beta_{g,\tau}\}$ belong to the same cohomology class in $\mathcal{H}^2(G, A)$. It should be noted that the action of $G$ in $A$ which used for cohomology is derived from the short exact sequence (5.1) and is expressed by the formula $(\star)$.

We now suppose that $G$ is a multiplicative group, finite or infinite, and $A$ is a $G$-module with the action

$$\begin{array}{ccc} G \times A & \to & A \\ (g, a) & \mapsto & a^g \end{array}$$

By **a solution of the extension problem for the pair (G,A)** we mean an exact sequence of the form (5.1), that is a triple $(U, i, j)$ such that the action of $G$ on $A$ determined by short exact sequence (5.1) and expressed by the formula $(\star)$ coincides with the given action of $G$ on $A$. Then we say that the $(U, i, j)$ is an extension of $A$ by $G$. Therefore, we have proved that every extension, $(U, i, j)$, of $A$ by $G$ determines an element of $\mathcal{H}^2(G, A)$.

Our next step is to show that, conversely, an element $\alpha \in \mathcal{H}^2(G, A)$ determines a solution $(U, i, j)$ of the extension problem and such that the associated cohomology class in $\mathcal{H}^2(G, A)$ is precisely $\alpha \in \mathcal{H}^2(G, A)$. Let now $\{a_{g,\tau}\}$ be a 2-cocycle of $G$ in $A$ which belongs to the class $\alpha \in \mathcal{H}^2(G, A)$. In particular, the equation

$$a_{g,\tau}a_{g\tau,\rho} = a^g_{\tau,\rho}a_{g,\tau\rho}, \quad for\ every\ g, \tau, \rho \in G$$

holds. For $g = \tau = 1$ we have the following formula

$$a_{1,\rho} = a_{1,1} \ \ for\ every\ \rho \in G \tag{5.5}$$

For $\tau = \rho = 1$ we have that

$$a_{g,1} = a^g_{1,1} \tag{5.6}$$

For $\tau = g^{-1} = \rho^{-1}$ we have that

$$a_{g,g^{-1}}a_{1,1} = a^g_{g^{-1},g}a^g_{1,1} \tag{5.7}$$

Now, for every $g \in G$ we choose a formal symbol $u_g$ and let

$$U := \{(a, u_g) \mid a \in A, g \in G\} \tag{5.8}$$

and we define the multiplication in $U$ according to the rule

$$(a, u_g)(\beta, u_\tau) = (a\beta^g a_{g,\tau}, u_{g,\tau}), \ with\ a, \beta \in A, g, \tau \in G \tag{5.9}$$

***Proposition* 5.1.3.** *The $(U, \cdot)$ is a multiplicative group.*

*Proof.* It is clear that $U$ is closed under multiplication, since if $(a, u_g), (\beta, u_\tau) \in U$ then $(a, u_g)(\beta, u_\tau) = (a\beta^g a_{g,\tau}, u_{g,\tau}) \in U$. Also, the multiplication in $U$ is associative, since

$$((a, u_g)(\beta, u_\tau))(\gamma, u_\rho) = (a\beta^g a_{g,\tau}\gamma^{g\tau}a_{g\tau,\rho}, u_{g\tau\rho})$$

and

$$(a, u_g)((\beta, u_\tau)(\gamma, u_\rho)) = (a(\beta\gamma^\tau a_{\tau,\rho})^g a_{g,\tau\rho}, u_{g,\tau,\rho}) = (a\beta^g a_{g,\tau}\gamma^{g\tau}a_{g\tau,\rho}, u_{g\tau\rho})$$

In addition, let $(x, u_\rho) \in U$ be a left identity in $U$, then for every $a \in A$ and $g \in G$ we have that $(x, u_\rho)(a, u_g) = (a, u_g) \Rightarrow (xa^\rho a_{\rho,g}, u_{\rho g}) = (a, u_g)$, which implies that $xa^\rho a_{\rho,g} = a$ and $u_{\rho g} = u_g$. So then $\rho = 1$ and $xa^1 a_{1,g} = a \overset{5.5}{\Rightarrow} xaa_{1,1} = a \Rightarrow x = a^{-1}_{1,1}$. Thus, $(a^{-1}_{1,1}, u_1)$ is a left identity. Similarly,we can prove that $(a^{-1}_{1,1}, u_1)$ is a right identity. Thus, $(a^{-1}_{1,1}, u_1)$ is identity of $U$. Finally, given $(x, u_\rho) \in U$ then

$$(a^{-1}_{1,1}a^{-1}_{g^{-1},g}(a^{g^{-1}})^{-1}, u_{g^{-1}})(a, u_g) = (a^{-1}_{1,1}, u_1)$$

so then $(a^{-1}_{1,1}a^{-1}_{g^{-1},g}(a^{g^{-1}})^{-1}, u_{g^{-1}})$ is a left inverse of $(a, u_g)$. Similarly, this is and right inverse. Thus, $(a^{-1}_{1,1}a^{-1}_{g^{-1},g}(a^{g^{-1}})^{-1}, u_{g^{-1}})$ is inverse. Therefore, $(U, \cdot)$ is a multiplicative group. □

Now we define the maps

$$\begin{array}{rccc} i: & A & \rightarrow & U \\ & a & \mapsto & (aa_{1,1}^{-1}, u_1) \end{array}$$

and

$$\begin{array}{rccc} j: & U & \rightarrow & G \\ & (a, u_g) & \mapsto & g \end{array}$$

***Proposition* 5.1.4.** *The sequence*

$$1 \rightarrow A \xrightarrow{i} U \xrightarrow{j} G \rightarrow 1 \tag{5.10}$$

*is a short exact sequence.*

*Proof.* Firstly, $i$ is an monomorphism. It is clear that $i$ is a homomorphism. Also, $i(a) = 1_u \Leftrightarrow (aa_{1,1}^{-1}, u_1) = (a_{1,1}^{-1}, u_1) \Leftrightarrow a = 1$, which means $Ker i = \{1\}$.So $i$ is injective. In addition, $j$ is epimorphism. It is clear that $j$ is homomorphism, since $j((a, u_{g_1})(\beta, u_{g_2})) = g_1 g_2 = j(a, u_{g_1}) j(\beta, u_{g_2})$ and $j$ is surjective by construction, since $j(a, u_g) = g$. Finally, it remains to show that $Kerj = Imi$. Indeed, $Kerj = \{(a, u_g) \in U : j(a, u_g) = 1\} = \{(a, u_g) : g = 1\} = \{(a, u_1) \in U, a \in A\} = \{(aa_{1,1}a_{1,1}^{-1}) \in U, a \in A\} = Imi$. Therefore the sequence 5.10 is exact. □

***Proposition* 5.1.5.** *The action of G on A determined by the short exact sequence 5.10 coincides with the original action, that is*

$$i(a^g) = (1, u_g)(aa_{1,1}^{-1}, u_1)(1, u_g)^{-1}$$

*Proof.* We consider $\{(1, u_g), | \, g \in G\}$ be a section of $G$ in $U$. We must also verify that the 2-cocycle of $G$ in $A$ determined by this exact sequence coincides with the one from which the construction started. We must check that

$$(1, u_g)(1, u_\tau) = i(a_{g,\tau})(1, u_{g\tau})$$

Indeed, $(1, u_g)(1, u_\tau) = (a_{g,\tau}, u_{g\tau})$ and $i(a_{g,\tau})(1, u_{g\tau}) = (a_{g,\tau}a_{1,1}^{-1}, u_1)(1, u_{g\tau}) = (a_{g,\tau}a_{1,1}^{-1}a_{1,g\tau}, u_{g\tau}) = (a_{g,\tau}a_{1,1}^{-1}a_{1,1}, u_{g\tau}) = (a_{g,\tau,u_{g\tau}})$. Finally, it remains to show that $i(a^g) = (1, u_g)(aa_{1,1}^{-1}, u_1)(1, u_g)^{-1}$. We have that $i(a^g) = (a^g a_{1,1}^{-1}, u_1)$ and

$$\begin{aligned} (1, u_g)(aa_{1,1}^{-1}, u_1)(1, u_g)^{-1} &= ((aa_{1,1}^{-1})^g a_{g,1}, u_g)(1, u_g)^{-1} \\ &= (a^g(a_{1,1}^g)^{-1}a_{g,1}, u_g)(a_{1,1}^{-1}a_{g^{-1},g}^{-1}, u_{g^{-1}}) \\ &= (a^g(a_{1,1}^g)^{-1}a_{g,1}(a_{1,1}^g)^{-1}(a_{g^{-1},g}^g)^{-1}a_{g,g^{-1}}, u_1) \\ &\overset{5.6}{=} (a^g(a_{1,1}^g)^{-1}a_{1,1}^g(a_{1,1}^g a_{g^{-1},g}^g)^{-1}a_{g,g^{-1}}, u_1) \\ &\overset{5.7}{=} (a^g(a_{1,1}a_{g,g^{-1}})^{-1}a_{g,g^{-1}}, u_1) \\ &= (a^g a_{1,1}^{-1}a_{g,g^{-1}}^{-1}a_{g,g^{-1}}, u_1) \\ &= (a^g a_{1,1}^{-1}, u_1) = i(a^g) \end{aligned}$$

□

The foregoing discussion shows that a 2-cocycle $\{a_{g,\tau}\}$ belonging to the cohomology class $\alpha \in \mathcal{H}^2(G, A)$ leads to an extension $(U, i, j)$ of $A$ by $G$. If we take any other 2-cocycle $\{b_{g,\tau}\}$ belonging to the cohomology class $\alpha \in \mathcal{H}^2(G, A)$ then it also leads to a solution to extension problem. So it is desirable to compare solutions of the same extension problem and for this reason we are led to the following definition.

***Definition* 5.1.6.** *Let $(U, i, j)$ and $(U', i', j')$ be extensions of $A$ by $G$. We say that the extensions $(U, i, j)$ and $(U', i', j')$ are* ***equivalent*** *if there exists a homomorphism $\varphi : U \to U'$ such that the following triangles are commutative, this means that $j' \circ \varphi = j$ and $\varphi \circ i = i'$.*

$$\begin{tikzcd}
 & & U \arrow[rd, "j"] \arrow[dd, dashed, "\varphi"] & & \\
1 \arrow[r] & A \arrow[ru, "i"] \arrow[rd, "i'"'] & & G \arrow[r] & 1 \\
 & & U' \arrow[ru, "j'"'] & &
\end{tikzcd}$$

***Remark* 5.1.7.** *If there exists a homomorphism $\varphi : U \to U'$ as it was described in the above definition, then $\varphi$ is automatically an isomorphism.*

*Proof.* Firstly, it is clear that $\varphi$ is an injective, since

$$\begin{aligned} &u \in Ker\varphi \Leftrightarrow \varphi(u) = 1 \Leftrightarrow j'(\varphi(u)) = j'(1) = 1 \\ &\Rightarrow j(u) = 1 \Rightarrow u \in Ker j = Im i \end{aligned}$$

Thus, there exists $a \in A$ such that $i(a) = u$, so then $\varphi(u) = 1 \Rightarrow \varphi(i(a)) = 1 \Rightarrow i'(a) = 1$ and since $i'$ is injective then $a = 1$. It remains to show that $\varphi$ is surjective. Let $u' \in U'$, then $j'(u') = g$, $g \in G$. Since $j$ is surjective then there exists $u \in U$ such that $j(u) = g \Rightarrow j'(\varphi(u)) = j'(u') \Rightarrow j'(\varphi(u)u'^{-1}) = 1$. This means that $\varphi(u)u'^{-1} \in Ker j' = Im i'$, that is there exists $a \in A$ such that $i'(a) = \varphi(u)u'^{-1} \Rightarrow \varphi(u(i(a))^{-1}) = u'$, where $u(i(a))^{-1} \in U$. So then $\varphi$ is surjective. Therefore, $\varphi$ is isomorphism. □

***Comment* 5.1.8.** *$\varphi$ is called* ***equivalence*** *of $(U, i, j)$ and $(U', i', j')$.*

***Proposition* 5.1.9.** *Equivalent extensions of $A$ by $G$ determine the same cohomology class $\alpha \in \mathcal{H}^2(G, A)$ (in particular they determine the same cocycle).*

*Proof.* Let $(U, i, j)$ and $(U', i', j')$ be equivalent extensions of $A$ by $G$ and $\varphi : U \to U'$ is isomorphism. Let also $\{u_g, g \in G\}$ be a section of $G$ in $U$. Then $\{a_{g,\tau}\}$, which is defined by the formula

$$u_g u_\tau = a_{g,\tau} u_{g\tau}$$

is a 2-cocycle which belonging to $\alpha \in \mathcal{H}^2(G, A)$. We set now $u'_g := \varphi(u_g)$. Then $j'(u'_g) = j'(\varphi(u_g)) = j' \circ \varphi(u_g) = j(u_g) = g$ and so $\{u'_g = \varphi(u_g) \mid g \in G\}$ is a section of $G$ in $U'$. We have that $u'_g u'_\tau = \varphi(u_g)\varphi(u_\tau) = \varphi(u_g u_\tau) = \varphi(a_{g,\tau} u_{g\tau}) = \varphi(a_{g,\tau})\varphi(u_{g\tau}) = \varphi(a_{g,\tau})u'_{g\tau}$.

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "i"] \arrow[d, "id"] & U \arrow[r, "j"] \arrow[d, "\varphi"] & G \arrow[r] \arrow[d, "id"] & 1 \\
1 \arrow[r] & A \arrow[r, "i'"] & U' \arrow[r, "j'"] & G \arrow[r] & 1
\end{tikzcd}$$

Thus, $\varphi|_A = id$, since $\varphi$ is injective. Hence, $u'_g u'_\tau = \varphi(a_{g,\tau})u'_{g,\tau}$. This means that $\{a_{g,\tau}\}$ is a 2-cocycle belonging to $\alpha \in \mathcal{H}^2(G, A)$. Therefore equivalent extensions of $A$ by $G$ determine the same cohomology class $\alpha \in \mathcal{H}^2(G, A)$. □

It is also true that cocycles belonging to the same cohomology class $\alpha \in \mathcal{H}^2(G, A)$ determine equivalent extensions of $A$ by $G$. Its proof will follow.

We suppose that $(U, i, j)$ is an extension of $A$ by $G$ and $(U', i', j')$ is an extension of $A'$ by $G'$. Let also $f : A \to A'$ and $\lambda : G \to G'$ be homomorphisms, that is

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, hook, "i"] \arrow[d, "f"] & U \arrow[r, "j"] \arrow[d, dash, "\varphi"] & G \arrow[r] \arrow[d, "\lambda"] & 1 \\
1 \arrow[r] & A' \arrow[r, hook, "i'"] & U' \arrow[r, "j'"] & G' \arrow[r] & 1
\end{tikzcd}$$

We would like to decide if there exists a homomorphism $\varphi : U \to U'$ such that the squares of the above diagram are commutative. For this reason we choose $\{u_g \mid g \in G\}$ be a section of $U$ and $\{u'_{g'} \mid g' \in G'\}$ be a section of $U'$ and let $\{a_{g,\tau}\}$, $\{a'_{g'\tau'}\}$ be the corresponding 2-cocycles. We suppose that there exists such a homomorphism of groups $\varphi : U \to U'$ such that the squares are commutative. Then for any $u = au_g \in U$ we have $\varphi(u) = \varphi(a)\varphi(u_g) = f(a)\varphi(u_g)$, since $\varphi|_A = f$, so that $\varphi$ determined completely as soon as the values $\varphi(u_g)$ are prescribed. But $j'(\varphi(u_g)) = \lambda(j(u_g)) = \lambda(g) = j'(u'_{\lambda(g)}) \Rightarrow j'(\varphi(u_g)u'^{-1}_{\lambda(g)}) = 1 \Rightarrow \varphi(u_g)u'^{-1}_{\lambda(g)} \in Kerj' = Imi'$. So then there exists $c'_g \in A'$ such that $\varphi(u_g) = c'_g u'_{\lambda(g)}$, for every $g \in G$.

In the usual way we define the action of $G$ on $A'$ as follows

$$\begin{array}{ccc}
G \times A' & \to & A' \\
(g, a') & \mapsto & (a')^g = (a')^{\lambda(g)}
\end{array}$$

Thus we view $A'$ as a $G'$-module. Then $\{c'_g,\, g \in G\}$ is a standard 1-cochain of $G$ in $A'$ which, in virtue of $\varphi(u) = f(a)\varphi(u_g)$ and $\varphi(u_g) = c'_g u'_{\lambda(g)}$ , serves to describe $\varphi$.

***Proposition* 5.1.10.** *The map $f : A \to A'$ is a $G$-homomorphism, that is*

$$f(a^g) = f(a)^g$$

*Proof.*

$$\begin{aligned} f(a^g) &= \varphi(a^g) = \varphi(u_g a u_g^{-1}) = \varphi(u_g)\varphi(a)\varphi(u_g)^{-1} = c'_g u'_{\lambda(g)} f(a) u'^{-1}_{\lambda(g)} c'^{-1}_g \\ &= c'_g f(a)^{\lambda(g)} c'^{-1}_g = f(a)^{\lambda(g)} = f(a)^g \end{aligned}$$

□

Let us introduce the symbol $(G, A)$, which is called pair, to signify that $A$ is a $G$-module. Similarly, $(G', A')$-pair signify that $A'$ is a $G'$-module.

***Definition* 5.1.11.** *Let $(G, A)$ and $(G', A')$ be pairs. If we have a homomorphism $\lambda : G' \to G$ (so that $A$ becomes a $G'$-module) and a $G'$-homomorphism $f : A \to A'$ then the composite object $(\lambda, f)$ is called homomorphism of pairs and symbolically we write*

$$(\lambda, f) : (G, A) \to (G', A')$$

Note that if $G, G'$ are finite groups, $A$ is a $G$-module and $\lambda : G \to G'$ is a homomorphism. Then $A$ becomes a $G'$-module with the action $g'a = (\lambda g')a$, where $g' \in G'$ and $a \in A$.

Moreover according to the above definition and proposition we have that $(1, f) : (G, A) \to (G, A')$ and $(\lambda, 1) : (G', A') \to (G, A')$ are homomorphisms of pairs.

***Proposition* 5.1.12.** *If $\{a_{g,\tau}\}$ belongs to cohomology class $\alpha \in \mathcal{H}^2(G, A)$ and $\{a'_{g,\tau}\}$ belongs to cohomology class $\alpha' \in \mathcal{H}^2(G', A')$, then*

$$(1, f)_*(\alpha) = (\lambda, 1)_*(\alpha')$$

*(In particular, the last equality says that the $2$-cocycles $\{f(a_{g,\tau})\}$ and $\{a'_{\lambda(g),\lambda(\tau)}\}$ of $G$ in $A'$ differ by the coboundary of the $1$-cochain $\{c'_g\}$.)*

*Proof.* Indeed, we have that

$$\begin{aligned} \varphi(u_g u_\tau) &= \varphi(a_{g,\tau} u_{g\tau}) = \varphi(a_{g,\tau})\varphi(u_{g\tau}) \\ &= f(a_{g,\tau})\varphi(u_{g\tau}) = f(a_{g,\tau}) c'_{g\tau} u'_{\lambda(g\tau)} \end{aligned}$$

and

$$\begin{aligned} \varphi(u_g)\varphi(u_\tau) &= c'_g c_\tau'^{\lambda(g)} c'_\tau u'_{\lambda(\tau)} = c'_g c_\tau'^{\lambda(g)} u'_{\lambda(g)} u'_{\lambda(\tau)} \\ &= c'_g c_\tau'^g a'_{\lambda(g)\lambda(\tau)} u'_{\lambda(g)\lambda(\tau)} = c'_g c_\tau'^g a'_{\lambda(g)\lambda(\tau)} u'_{\lambda(g\tau)} \end{aligned}$$

But $\varphi$ is a homomorphism, so then $f(a_{g,\tau}) c'_{g\tau} u'_{\lambda(g\tau)} = c'_g c_\tau'^g a'_{\lambda(g)\lambda(\tau)} u'_{\lambda(g\tau)}$, which implies that

$$f(a_{g,\tau}) = a'_{\lambda(g)\lambda(\tau)} c'_g c_\tau'^g c'^{-1}_{g\tau}$$

□

***Theorem* 5.1.13.** *Let $(U, i, j)$ be an extension of $A$ by $G$ which determines $\alpha \in \mathcal{H}^2(G, A)$ and let $(U', i', j')$ be an extension of $A'$ by $G'$ which determines $\alpha' \in \mathcal{H}^2(G', A')$. We suppose that $f : A \to A'$ and $\lambda : G \to G'$ are homomorphisms and that $A'$ viewed as a $G$-module by putting $(a')^g = (a')^{\lambda(g)}$. Then there exists a homomorphism $\varphi : U \to U'$ such that the following diagram*

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"] & U \arrow[r, "j"] \arrow[d, dash, "\varphi"] & G \arrow[r] \arrow[d, "\lambda"] & 1 \\
1 \arrow[r] & A' \arrow[r, "i'"] & U' \arrow[r, "j'"] & G' \arrow[r] & 1
\end{tikzcd}$$

*is commutative diagram if and only if*

*(i)* *$f$ is a $G$-homomorphism*

*(ii)* *$f_*(\alpha) = (1, g)_*(\alpha) = (\lambda, 1)_*(\alpha')$. That is the $2$-cocycles $\{f(a_{g,\tau})\}$ and $\{a'_{\lambda(g),\lambda(\tau)}\}$ of $G$ in $A'$ differ by a coboundary.*

*Proof.* " $\Rightarrow$ " We have proved according to propositions 5.1.10 and 5.1.12.

" $\Leftarrow$ " We suppose that $(i)$ and $(ii)$ hold. We choose $\{u_g \mid g \in G\} \subseteq U$ and $u'_g \mid g' \in G' \subseteq U'$ be sections of $U$ and $U'$, respectively. If we write

$$u_g u_\tau = a_{g,\tau} u_{g\tau}, \quad u'_{g'} u'_{\tau'} = a\_g', \tau' u'_{g'\tau'}$$

then the cocycle $\{a_{g,\tau}\}$ belong to cohomology class $\alpha \in \mathcal{H}^2(G, A)$ and the cocycle $\{a'_{g',\tau'}\}$ belong to cohomology class $\alpha' \in \mathcal{H}^2(G', A')$. According to the condition $(i)$ we have that

$$f(a^g) = f(a)^g \tag{5.11}$$

and from condition $(ii)$ we have that there exists a 1-cochain $\{c'_g \in A'\}$ such that

$$f(a_{g,\tau}) = a'_{\lambda(g)\lambda(\tau)} c'_g c'^g_\tau c'^{-1}_{g\tau} \tag{5.12}$$

We define $\varphi : U \to U'$, by $\varphi(au_g) = f(a) c'_g u'_{\lambda(g)}$

Then $\varphi$ is a homomorphism, since

$$\begin{aligned}
\varphi(au_g bu_\tau) &= \varphi(ab^g u_g u_\tau) = \varphi(ab^g a_{g,\tau} u_{g\tau}) \\
&= f(ab^g a_{g,\tau}) c'_{g\tau} u'_{\lambda(g\tau)} = f(a) f(b^g) f(a_{g,\tau}) c'_{g\tau} u'_{\lambda(g\tau)}
\end{aligned}$$

and

$$\begin{aligned}
\varphi(au_g)\varphi(bu_\tau) &= f(a) c'_g u'_{\lambda(g)} f(b) c'_\tau u'_{\lambda(\tau)} \\
&= f(a) c'_g f(b)^{\lambda(g)} u'_{\lambda(g)} c'_\tau u'_{\lambda(\tau)} \\
&= f(a) f(b)^{\lambda(g)} c'_g c'^{\lambda(g)}_\tau u'_{\lambda(g)} u'_{\lambda(\tau)} \\
&= f(a) f(b)^g c'_g c'^g_\tau a'_{\lambda(g),\lambda(\tau)} u'_{\lambda(g\tau)} \\
&\overset{5.11}{\underset{5.12}{=}} f(a) f(b^g) f(a_{g,\tau}) c'_{g\tau} u'_{\lambda(g\tau)}
\end{aligned}$$

It remains to show that the above diagram is commutative. It suffices to show that $\lambda \circ j = j' \circ \varphi$ and $\varphi \circ i = i' \circ f$. Since $u_1 \in A$, we have that $1 = \varphi(1) = \varphi(u_1^{-1}u_1) = f(u_1^{-1})c'_1u'_{\lambda(1)} = f(u_1)^{-1}c'_1u'_1$ and therefore $f(u_1) = c'_1u'_1$. Also, $\lambda \circ j = j' \circ \varphi$, since $\varphi(i(a)) = \varphi(a) = \varphi(au_1^{-1})u_1 = f(au_1^{-1})c_1u'_1 = f(au_1^{-1})f(u_1) = f(a) = i'(f(a))$. In addition, $\varphi \circ i = i' \circ f$, since $\lambda \circ j(au_g) = \lambda(j(au_g)) = \lambda(g)$ and $j' \circ \varphi(au_g) = j'(\varphi(au_g)) = j'(f(a)c'_gu'_{\lambda(g)}) = \lambda(g)$. This complete the proof. □

***Definition* 5.1.14.** *By $\mathcal{E}(G, A) = Ext(G, A)$ will be denoted the set of equivalence classes of extensions of $A$ by $G$.*

***Theorem* 5.1.15.** *We suppose that the abelian group $A$ is a $G$-module, where $G$ is finite or infinite. Then there is a natural 1-1 correspondence between the elements of $\mathcal{E}(G, A)$ and the elements of $\mathcal{H}^2(G, A)$.*

*Proof.* It remains only to show that if $\{a_{g,\tau}\}$ and $\{b_{g,\tau}\}$ are 2-cocycles belonging to $\alpha \in \mathcal{H}^2(G, A)$ and $(U, i, j)$, $(U', i', j')$ are the extensions they determine according to our construction, then these extensions are equivalent. To do this we simply apply the theorem 5.1.13 with $A' = A$, $G' = G$, $\lambda = f = 1$ and $\alpha' = \alpha$

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f=1"] & U \arrow[r, "j"] \arrow[d, dash, "\varphi"] & G \arrow[r] \arrow[d, "\lambda=1"] & 1 \\
1 \arrow[r] & A \arrow[r] & U' \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

Since $f = 1$ then $f$ is a $G$-homomorphism and also the 2-cocycles $\{f(a_{g,\tau})\} = \{a_{g,\tau}\}$ and $\{a'_{\lambda(g),\lambda(\tau)}\} = \{a'_{g,\tau}\}$ of $G$ in $A'$ differ by a coboundary. So then according to 5.1.13 there exists a homomorphism $\varphi : U \to U'$ such that the above diagram is commutative. This means that there exists a homomorphism $\varphi : U \to U'$ such that the following diagram is commutative,

$$\begin{tikzcd}
 & & U \arrow[dr, "j"] & & \\
1 \arrow[r] & A \arrow[ur, "i"] \arrow[dr] & & G \arrow[r] & 1 \\
 & & U' \arrow[ur] & &
\end{tikzcd}$$

and then we have proved that $\varphi$ is isomorphism. This complete the proof. □

## 5.2 The Brauer Group

***Definition* 5.2.1.** *Let $K$ be a field. The ring $A$ is called* $\mathbf{K-algebra}$ *when $A$ is also a $K$-vector space and for every $\lambda \in K$ and $a, b \in A$ holds that*

$$(\lambda a)b = a(\lambda b) = \lambda(ab)$$

*(The addition in $A$ as a vector space is the addition as a ring.)*

*The* **dimension** *of $K$-algebra $A$, $dim_K A$, is the dimension of $A$ as a $K$-vector space.*

***Definition* 5.2.2.** *The* **center** *of the $K$-algebra $A$ is defined as follows*

$$\mathcal{Z}(A) = \{a \in A \mid ab = ba, \forall b \in A\}$$

***Definition* 5.2.3.** *The $K$-algebra $A$ will be called* **simple** *when the only two-sided ideals are the $< 0 >$ and $A$.*

***Proposition* 5.2.4.** *Let $K$ be a field and $A$ be a finite dimensional simple $K$-algebra. Then the center of $A$, $\mathcal{Z}(A)$, is a field.*

*Proof.* For its proof see ([6], proposition 5.3, p.12). □

***Definition* 5.2.5.** *The $K$-algebra $A$ is called* **division algebra** *over the field $K$ if for any element $\alpha \in A$ with $\alpha \neq 0$, there exists its multiplicative inverse in $A$.*

***Proposition* 5.2.6.** *For every division $K$-algebra $D$ it is hold that*

$$\mathcal{Z}(D) \cong \mathcal{Z}(M_n(D)), \ \forall n > 0$$

*Proof.* For its proof see ([6], proposition 5.3, p.12). □

Let $K$ be a field and $A$ be a $K$-algebra. Without loss of generality we can assume that $K \subset A$. Then, in general $K \subset \mathcal{Z}(A)$.

***Definition* 5.2.7.** *The $K$-algebra $A$ will be called* $\mathbf{central\ K-algebra}$ *when*

$$K = \mathcal{Z}(A)$$

***Definition* 5.2.8.** *An* $\mathbf{Azumaya-algebra}$ *over that field $K$ is a finite dimensional, central, simple $K$-algebra.*

***Definition* 5.2.9.** *Two Azumaya algebras $A$ and $B$ are equivalent, and it is denoted by $A \sim B$, if there exist $r, s \in \mathbb{N}$ such that*

$$A \otimes_K M_r(K) \cong B \otimes_K M_s(K)$$

*This relation is an equivalence relation.*

***Definition* 5.2.10.** *The* **Brauer group**, *$Br(K)$, is defined as the set of all similarity classes*

$$[A] = \{B \mid B\ is\ Azumaya-algebra\ over\ the\ field\ K\ and\ B \sim A\}$$

*endowed with the multiplication*

$$[A][B] = [A \otimes_K B]$$

If now $L/K$ is an extension of fields, then the map

$$\begin{array}{cccc} r_{L/K}: & Br(K) & \to & Br(L) \\ & [A] & \mapsto & [A \otimes_K L] \end{array}$$

is a group homomorphism.

***Definition* 5.2.11.** *Let $A$ be an Azumaya-algebra over the field $K$ and $L/K$ is a field extension. The field $L$ is a* **splitting field** *for the algebra $A$ when*

$$[A] \in Ker(r_{L/K})$$

*The group*

$$Br(L/K) := Ker(r_{L/K})$$

*is called relative Brauer subgroup of $K$ over $L$.*

Finally, if the extension $L/K$ is Galois extension, then we have that

$$\mathcal{H}^2(Gal(L/K), L^*) \cong Br(L/K)$$

For its proof see ([6], Theorem 14.3, p.15).

## 5.3 The Inverse Problem of Galois Theory

Let $N/K$ be a finite or infinite Galois extension. We have proved that the Galois group $Gal(N/K)$ equipped with Krull topology is a topological group. Moreover, we have proved that $Gal(N/K)$ is compact, Hausdorff and totally disconnected. Therefore, according to theorem 2.3.10 we have that the Galois group $Gal(N/K)$ equipped with Krull topology is a profinite group. In particular we can describe the Galois group of even an infinite Galois extension as a projective limit of finite Galois groups. More precisely if $N/K$ is a Galois extension, then

$$Gal(N/K) \cong \varprojlim_{L} Gal(L/K)$$

where $L/K$ is a finite Galois extension with $K \subseteq L \subseteq N$.

An easy result in Galois Theory is the following:

***Proposition* 5.3.1.** *Every finite group is isomorphic to the Galois group of some field extension.*

*Proof.* **The Ideas of the proof :**
Let $G$ be the finite group of order $n$. Then according to Cayley's theorem we have that $G \leqslant S_n$. We consider $K = K(t_1, \dots, t_n)$ and $F = K(s_1, \dots, s_n)$ where $t_1, \dots, t_n$ are the roots of general polynomial of degree $n$

$$g(X) = X^n - s_1X^{n-1} + s_2X^{n-2} + \cdots + (-1)^n s_n \in K(s_1, s_2, \dots, s_n)[X]$$

and $s_1, \dots, s_n$ are the elementary symmetric functions of $t_1, \dots, t_n$. Then we have that $L/F$ is Galois extension and $Gal(L/K) \cong S_n$.

$$\begin{tikzcd}
L \arrow[r, leftrightarrow] \arrow[d, dash] & < id_N > \arrow[d, dash] \\
E = \mathcal{F}(G) \arrow[r, leftrightarrow] \arrow[d, dash] & G \arrow[d, dash] \\
F \arrow[r, leftrightarrow] & Gal(L/F) \cong S_n
\end{tikzcd}$$

According to fundamental theorem of Galois theory we have that $L/E$ is a Galois extension and

$$G \cong Gal(L/E)$$

This means that $G$ is realizable as Galois group of some extension. □

We now generalize this fact to profinite groups. More precisely we will prove that every profinite group is the Galois group of some field extension. For doing this we will require just one more lemma, which we state and prove now.

***Lemma* 5.3.2.** *Let $F$ be a field and $G$ be a profinite group of automorphisms of $F$ such that for every $x \in F$, the stabilizer*

$$S(x) = \{\sigma \in G \mid \sigma(x) = x\}$$

*is an open subgroup of $G$. Then*

$$G = Gal(F/F^G)$$

*where $F^G = \{x \in F \mid \sigma(x) = x, \ \forall \sigma \in G\}$.*

*Proof.* Let $x_1, \dots, x_n \in F$. Then the group $H = \bigcap_{i=1}^{n} S(x_i)$ is open in $G$, by hypothesis. Also $G$ is compact, since $G$ is profinite, and $H$ is open, so then according to proposition 1.2.14, $(iii)$ we have that $H$ is closed of finite index. We consider the group $N := \bigcap_{g \in G} gHg^{-1}$. Since $H$ is closed, so is $gHg^{-1}$, and then $N$ is closed as well. It is clear that $N$ is a normal subgroup. Thus, $N$ is closed of finite index, which implies that $N$ is open according to proposition 1.2.14, $(iii)$. This means that $G/N$ is finite. Let $L := F^G(Gx_1, \dots, Gx_n)$, where $Gx_i = \{\sigma(x_i) \mid \sigma \in G\}$. We have that

$$F^G \subseteq L \subseteq F$$

The action of $G/N$ on $L$ is the following

$$\begin{array}{ccc} G/N \times L & \to & L \\ (gN, l) & \mapsto & (gN)(l) \end{array}$$

and then it is clear that $(gN)(F^G) = F^G$ and $(gN)(Gx_i) = Gx_i$. In addition, this action is faithful, since if $(g_1N)(Gx_i) = (g_2N)(Gx_i)$, for every $i = 1, 2, \dots, n$, then we have that

$$\begin{aligned}
&(g_1N)(\sigma x_i) = (g_2N)(\sigma x_i),\ \forall\sigma \in G\\
&\Rightarrow g_1\sigma H\sigma^{-1}(\sigma x_i) = g_2\sigma H\sigma^{-1}(\sigma x_i),\ since\ N = \bigcap_{g\in G} gHg^{-1}\\
&\Rightarrow g_1\sigma Hx_i = g_2\sigma Hx_i\\
&\Rightarrow (g_1\sigma)(x_i) = (g_2\sigma)(x_i),\ \forall\sigma \in G,\ \forall i = 1, \dots, n\\
&\Rightarrow (g_2^{-1}g_1)(\sigma(x_i)) = \sigma(x_i)\\
&\Rightarrow (\sigma^{-1}g_2^{-1}g_1\sigma)(x_i) = x_i,\ \forall\sigma \in G,\ \forall i = 1, \dots, n
\end{aligned}$$

This means that

$$\sigma^{-1}g_2^{-1}g_1\sigma \in S(x_i),\ \forall\sigma \in G,\ \forall i = 1, \dots, n$$

which implies that

$$\begin{aligned}
&\sigma^{-1}g_2^{-1}g_1\sigma \in \bigcap_{i=1}^{n} S(x_i) = H\\
&\Rightarrow g_2^{-1}g_1 \in \sigma H\sigma^{-1},\ \forall\sigma \in G
\end{aligned}$$

Thus $g_2^{-1}g_1 \in \bigcap_{g\in G} gHg^{-1} = N \Rightarrow g_1N = g_2N$. Hence, the finite group $G/N$ can be regarded as an automorphism group of the field $L$ and the fixed field of $G/N$ is $F^G$. A result of Artin in classical Galois theory asserts that if $K$ be a field and $G$ be a finite group of automorphisms of $K$, then $K/K^G$ is a finite Galois extension, $G = Gal(K/K^G)$ and $|G| = [K : K^G]$. In our case we have that $G/N$ is a finite group of automorphisms of $L$, so then according to Artin's result we have that $L/F^G$ is a finite Galois extension, $G/N = Gal(L/F^G)$ and $|G/N| = [L : F^G]$. The field $F$ is the union of the above $L$ and $\{N\}$ are open normal subgroups of $G$. So then

$$G \cong \varprojlim_N G/N = \varprojlim_L Gal(L/F^G) = Gal(F/F^G)$$

□

We are now able to prove the following result.

***Theorem* 5.3.3.** *(Waterhouse, 1974) Every profinite group is the Galois group of some field extension.*

*Proof.* Let $G$ be a profinite group and let

$$S = \dot{\bigcup_N} G/N,\ where\ N \trianglelefteq G, N\ is\ open\quad (disjoint\ union)$$

Let $K$ be any field. We can take the elements of $S$ as indeterminates and form the purely transcendetal extension $L = K(S)$. The natural action of $G$ on $S$

$$\begin{array}{ccc} G \times S & \to & S \\ (\sigma, \tau N) & \mapsto & \sigma(\tau N) = \sigma\tau N \end{array}$$

is well defined, since $S$ is the disjoint union. Also the action of $G$ on $S$ is faithful, since if $\sigma_1(\tau N) = \sigma_2(\tau N)$, then

$$\sigma_1\tau N = \sigma_2\tau N \Rightarrow \tau^{-1}\sigma_2^{-1}\sigma_1\tau \in N$$
$$\Rightarrow \sigma_2^{-1}\sigma_1 \in \tau N\tau^{-1} = N$$

Thus $\sigma_2^{-1}\sigma_1 \in N$, for every open normal subgroup $N$ of $G$, which implies that $\sigma_2^{-1}\sigma_1 \in \bigcap N = \{1\}$ and so $\sigma_1 = \sigma_2$. In addition let $\tau N \in S$, then

$$\begin{array}{rcl} S(\tau N) & = & \{g \in G \mid g(\tau N) = \tau N\} = \{g \in G \mid g\tau N = \tau N\} \\ & = & \{g \in G \mid \tau^{-1}g\tau N = N\} = \{g \in G \mid \tau^{-1}g\tau \in N\} \\ & = & \{g \in G \mid g \in \tau N\tau^{-1}\} = \{g \in G \mid g \in G\} = N \end{array}$$

The action of $G$ on $S$ as a group of permutations induces a homomorphism $\theta$ from $G$ to the group of field $K$-automorphisms of $L$, that is

$$\theta : \; G \to Aut_K(L), \; \sigma \mapsto \theta(\sigma)$$

where $\theta(\sigma)(s) = \sigma(s)$, for every $s \in S$. Furthermore, $\theta$ is injective, since the action of $G$ on $S$ is faithful and therefore $G \leqslant Aut_K(L)$. It remains to show that the stabilizer $S(u)$, for every $u \in L$ is an open subgroup of $G$. Let $u \in L$ then we have that $u \in K(s_1, \dots, s_r)$, for some $r$, where $s_i = \tau_i N_i$, for $i = 1, \dots, r$. We have that

$$S(\tau_1 N_1) \cap \dots \cap S(\tau_r N_r) \leqslant S(u) \Rightarrow N_1 \cap \cdots \cap N_r \leqslant S(u)$$

So $S(u)$ is open for every $u \in L$, since $N_1 \cap \cdots \cap N_r \leqslant S(u)$ and $N_1 \cap \cdots \cap N_r$ is open. Hence, according to lemma 5.3.2 we have that the extension $L/L^G$ is a Galois extension and

$$G \cong Gal(L/L^G)$$

This means that $G$ is realizable as Galois group of some extension. □

Although this proof let us choose any field $K$ we like, we have no way to control $L^G$.

One of the most famous conjecture in group theory is the so called

**Inverse Problem of Galois Theory.** Given a finite group G, does there exist a finite Galois extension $K$ of $\mathbb{Q}$ such that $Gal(K/\mathbb{Q}) \cong G$?

An important result about Inverse Problem of Galois Theory is due to Shafarevich. We wish to mention here the following result of Shafarevich about solvable groups.

***Theorem* 5.3.4.** *Every finite solvable group is realizable over $\mathbb{Q}$ as a Galois group of some extension.*

Its proof is very difficult. It uses Algebraic Number Theory and Cohomology of Profinite Groups (see [13], Chapter IX, §6). In the special case where the given finite group G is of odd order the same result has been proven by J. Neukirch (see [12], p. 135-164).

More can be read about the Inverse Galois Problem in [17].

Finally, we will mention a conjecture about the Galois group of the extension $\bar{\mathbb{Q}}/\mathbb{Q}^{ab}$ and this conjecture is due to Shafarevich.

**Shafarevich Conjecture**:
The absolute Galois group of $\mathbb{Q}^{ab}$, $Gal(\bar{\mathbb{Q}}/\mathbb{Q}^{ab})$ is a free profinite group of countable rank. Here $\mathbb{Q}^{ab}$ is the maximal abelian extension over $\mathbb{Q}$.

If the conjecture has a positive answer, then the Inverse Problem of Galois Theory over $\mathbb{Q}^{ab}$ has an affirmative answer.

# Bibliography

[1] Frederick Butler. *Infinite Galois Theory, Master Thesis, University of Pennsylvania, 2001*.

[2] Michael D. Fried and Moshe Jarden. *Field Arithmetic*. Third Edition. Vol. 11. Springer-Verlag, Berlin, 2008.

[3] Taqdir Husain. *Introduction to Topological Groups*. Huntington, New York: Robert E. Krieger Publishing Company, 1981.

[4] G. Karpilovsky. *Topics in Field Theory*. North-Holland, New York, 1989.

[5] Christos Karyofyllis and Charikleia Konstantilaki-Savvopoulou. *Topology II*. in greek. Thessaloniki: Ziti Pablications, 1986.

[6] Ina Kersten. *Brauergruppen von Körpern*. Vieweg, Braunschweig, 1990.

[7] Helmut Koch. *Galois Theory of p-Extensions*. Springer, Berlin, 2002.

[8] Megan Meguire. *Cohomology of Profinite Groups*.

[9] Dean Montgomery and Leo Zippin. *Topological transformation groups*. Interscience Tracts in Pure and Applied Mathematics, 1955.

[10] Patrick Morandi. *Field and Galois Theory*. Springer, New York,1986.

[11] Jürgen Neukirch. *Class Field Theory- The Bonn Lectures- Edited by Alexander Schmidt*. Springer-Verlag, Berlin, 2013.

[12] Jürgen Neukirch. *On solvable Number Fields, Inventiones Mathematicae, Vol. 53, (135-164)*. 1979.

[13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Second Edition. Springer-Verlag, Heidelberg, 2008.

[14] Luis Ribes. *Introduction to Profinite Groups*. Queen's University, Kingston, Ontario, Canada, 1970.

[15] Luis Ribes and Pavel Zalesskii. *Profinite Groups*. Springer, Berlin, 2000.

[16] Joseph J. Rotman. *Advanced Modern Algebra*. Second Edition. Vol. 114. American Mathematical Society, 2010.

[17] Helmut Volklein. *Groups as Galois Groups: An introduction*. Cambridge University Press, Cambridge UK, 1996.

[18] William C. Waterhouse. «Profinite Groups are Galois Groups». In: *Proceedings of the American Mathematical Society* Volume 42, (639-640).Number 2 (Feb. 1974).

[19] Edwin Weiss. *Cohomology of Groups*. Academic Press, New York, 1969.

[20] John S. Wilson. *Profinite Groups*. Oxford University Press, Oxford, 1999.

[21] Anthi Zervou. *Polynomials and Galois Theory, Diploma Thesis*. in greek, Heraklion. 2015.