Galois Cohomology

Seyfi Türkelli

June 15, 2004
Let $K/k$ be a Galois extension. Galois correspondence says that there is a 1-1 correspondence between the sub-extensions of $K/k$ and the subgroups of $Gal(K/k)$ in such a way that normal sub-extensions correspond to normal subgroups. In view of this result, which is usually called the fundamental theorem of Galois theory, understanding a Galois extension is the same as understanding its Galois group. As usual, we have cohomological invariants of Galois groups and its theory Galois cohomology. Galois groups are in fact profinite groups, namely $Gal(K/k) = \lim \leftarrow Gal(E/k)$ where the limit runs over the finite sub-extensions, and the converse is also true. Therefore, Galois cohomology is the cohomology of profinite groups which can be seen as the extension of cohomology of finite groups to the one of profinite groups with respecting the topological structure on profinite groups. In other words, finite groups are trivially profinite groups and, in this point of view, cohomology of profinite groups recovers that of finite groups.

Almost all of the results in this theory is due to Tate. Many deep results can be proven, with relative ease, by using cohomological machinery. For instance, the existence of Hasse invariant [Sh,p155] or Tsen’s theorem saying that the Brauer group $Br(K)$, which is a very important algebraic invariant of the field, of a function field $K$ in one variable over an algebraically closed field is trivial [Sh,p108]. In this text, our aim is to prove one of the most basic and important results of the theory, namely Hilbert’s theorem 90, and to give a few of its applications to the field theory. In chapter 1, we introduce profinite groups and prove Pontryagin duality, which is used very often like many other duality theorems -as an example see the proof Shafarevich-Golod’s theorem [Sh,p69]. In chapter 2, we define the cohomology of profinite groups and its elementary properties. In chapter 3, we introduce another very useful invariant, cohomological dimension of an extension, instead of that we don’t really use it in this text. In the last chapter, we show our theorem and its applications.
## Contents

1 Profinite Groups 3
   1. Structure of Profinite Groups ........................................ 3
   2. Pontryagin Duality .................................................... 6
   3. Subgroups .................................................................... 9
   4. Sylow $p$-Subgroups .................................................... 10

2 Cohomology 12
   1. Two Definitions of Cohomology and Their Equivalence ............ 12
   2. $Res$, $Cor$ and Functoriality ........................................ 16
   3. Induced Modules .......................................................... 18
   4. Cup Products ................................................................ 20
   5. Spectral Sequences ....................................................... 22

3 Cohomological Dimension 25
   1. Basic Properties .......................................................... 25
   2. Cohomological Dimension of Subgroups ............................... 27
   3. The Case Cohomological Dimension 1 ................................ 29

4 Galois Cohomology: An Application 31
   1. Hilbert’s Theorem 90 ...................................................... 31
   2. Some Applications: Cyclic Extensions ................................ 32
   3. Some Applications: Brauer Groups ................................... 33
Chapter 1

Profinite Groups

1. Structure of Profinite Groups

We say that a group $G$ equipped with a topology is a topological group if the maps $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are continuous. From the definition, it immediately follows that the maps $x \mapsto ax$, $x \mapsto xa$ and $x \mapsto x^{-1}$ are homeomorphisms. It is clear that $\{1\}$ is closed in $G$ if and only if $G$ is Hausdorff. Throughout the section we will assume that topological groups are Hausdorff.

A topological group $G$ has the following obvious properties:

i. Any open subgroup of $G$ is closed.

ii. Any closed subgroup of finite index is open.

iii. If a subgroup of $G$ contains an open subgroup then it is open.

iv. If $G$ is compact then the open subgroups are of finite index.

The isomorphism theorems hold for closed subgroups of topological groups if we assume that homomorphisms are closed and open [Pn, p 113]. This is automatic for compact groups [Pn, 115].

A partially ordered set $I$ is called directed if for any $i, j \in I$ there exists a $k \in I$ with $i \leq k$ and $j \leq k$. An inverse system of topological groups (sets) is a family $(G_i, \varphi_i^j)_{i,j \in I}$ of topological groups (sets) and continuous homomorphisms (maps)

$$\varphi_i^j : G_j \to G_i$$

such that for $k \leq i \leq j$, we have

$$\varphi_i^i = id \text{ and } \varphi_k^i \circ \varphi_i^j = \varphi_k^j.$$

By the inverse or projective limit of an inverse system of topological groups (sets) $(G_i, \varphi_i^j)$ we mean the group (set) $G = \{(x_i)_{i \in I} \in \prod G_i \mid x_i = \varphi_i^j(x_j), i, j \in I, i \leq j \}$ and denote it by $G = \varprojlim G_i$. Then $G$ is a closed subgroup of $\prod G_i$, in particular a topological group, and
the projections $\Pi_i : G \to G_i$ are continuous homomorphisms [Ri,p 3]. If we have another inverse system $(H_i, \psi_j^i)_{i,j \in I}$ and the continuous homomorphisms $\theta_i : G_i \to H_i$ which are compatible with $\varphi_i^j$ ’s and $\psi_j^i$ ’s then the map $\theta : G \to H$ induced by $\theta_i$ ’s is also a continuous homomorphism.

A profinite group $G$ is the inverse limit of an inverse system of finite groups endowed with the discrete topology. $G$ is clearly compact and its topology generated by $\Pi_i^{-1}(g_i), g_i \in G_i, i \in I$ [Fr, p 3]. Noting that $\Pi_i^{-1}(g_i)$’s are open and closed, it can be easily seen that $G$ is totaly disconnected. And, a basis for open neighborhoods of 1 given by the open normal subgroups of $G$. Open subgroups are precisely the closed subgroups of finite index, and their intersection is 1. Therefore, every closed subgroup $H$ is the intersection of open subgroups.

Indeed, $H = \bigcap G_i$ where $G_i$ is an open subgroup containing $H$. If $x \in \bigcap G_i$ then $x \in NH$ for all open subgroups $N$ of $G$ since $NH$ is an open normal subgroup containing $H$. So $xN \cap H \neq \emptyset$. Since $H$ is compact and any finite collection of them has nonempty intersection, $(\bigcap xN) \cap H \neq \emptyset$ and there exists $h \in H$ such that $h \in xN$ for all such $N$. Hence $x^{-1}h \in \bigcap N, x^{-1}h = 1$ and $x = h \in H$.

As we mentioned before, a profinite group is compact and totaly disconnected. Conversely:

**Theorem 1.1.** Any compact totaly disconnected group is profinite.

In order to prove this result, we need two lemmas.

**Lemma 1.2.** Let $G$ be a compact group and $\{N_i \mid i \in I\}$ be a family of normal closed subgroups of finite index satisfying

i. For every finite subset $J$ of $I$ there exists $i \in I$ such that $N_i \subseteq \bigcap_j N_j$,

ii. $\bigcap_i N_i = 1$.

Then $G = \varprojlim G/N_i$ is a profinite group.

**Proof.** Define the partial order $\leq$ on $I$ as follows: $i \leq j$ if and only if $N_i \supseteq N_j$. Let’s define the ”restrictions”, for $i \leq j$, $\varphi_i^j : G/N_j \to G/N_i$ as the natural quotient maps. By condition $i$, $I$ is a directed set. Note that $G/N_i$’s are finite groups endowed with the discrete topology so the restrictions are automatically continuous. We have the canonical map

$$\psi : G \to \varprojlim G/N_i,$$

defined by

$$g \mapsto (\Pi_i(g))_i$$

where $\Pi_i : G \to \varprojlim G/N_i$ is the projection. By condition $ii$, $\psi$ is injective. Since $\{\Pi_i^{-1}(g_i)\}_{i,g_i}$ forms a basis for the topology of $\varprojlim G/N_i$ and $g \in \Pi_i^{-1}(g_i)$ where $g_i = \Pi_i(g)$, $\psi(G)$ is dense in $\varprojlim G/N_i$. On the other hand, $\Pi_i$’s are continuous and so is $\psi$. Since $G$ is compact, $\psi$ is surjective and we are done.

**Lemma 1.3.** Open subgroups of totaly disconnected locally compact groups form a base for neighborhoods of 1.

4
Proof. See [PN, Thm 67].

Proof of Theorem 1.1. If $H$ is an open subgroup of $G$ then $[G : H] < \infty$ and the set \( \{ H^g \mid g \in G \} \) is finite; Thus \( \bigcap_{g \in G} H^g \) is an open normal subgroup of $G$. By lemma 1.3, open normal subgroups forms a basis for neighborhoods of 1 and the set \( \{ N_i \mid N_i \leq G, N_i \text{ is open} \} \) satisfies condition i in Lemma 1.2. Since $G$ is Hausdorff, \( \bigcap N_i = 1 \) i.e the second condition is also satisfied. Hence, by Lemma 1.2, we are done. \( \square \)

Note that profinite groups form a category in which morphisms are continuous homomorphisms, and products and inverse limits exist.

Corollary 1.4. A closed subgroup $H$ of a profinite group $G$ is profinite. If $H$ is also normal then $G/H$ is a profinite group.

Corollary 1.5. $\mathbb{Z}_p$, $p$-adic completion of $\mathbb{Z}$ or ring of integers of $\mathbb{Q}_p$, is a profinite group. Namely, $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ where $p$ is a prime number and $n \in \mathbb{N}$.

Corollary 1.6. An inverse limit of profinite groups is a profinite group.

Corollary 1.7. Any Galois group $G = \text{Gal}(E/K)$ is profinite. Indeed, $G = \varprojlim \text{Gal}(F/K)$ where $K \subseteq F \subseteq E$ and $F/K$ is a finite Galois extension.

Perhaps the theorem we have already proved gives us a good characterization of profinite groups. But we can give a more explicit description:

Theorem 1.8. Every profinite group is isomorphic to a Galois group of some Galois extension.

We need a lemma, which is a generalization of Artin’s Lemma:

Lemma 1.9. Let $G$ be a profinite group acting faithfully as automorphisms of a field $E$ such that $G_x = \{ g \in G \mid x^g = x \}$ is an open subgroup of $G$ for all $x \in E$. Then $E$ is the Galois extension of the fixed field $K = \{ x \in E \mid x^g = x \text{ for all } g \in G \}$.

Proof. In case $G$ is finite, this is Artin’s Lemma [La, p 264]. If $H = x_1^G \cap ... \cap x_n^G$ for $x_1, ..., x_n \in E$ then, by the assumption, $H$ is open in $G$ and $N = \bigcap_{g \in G} H^g$, which is a finite intersection, is an open normal subgroup of $G$. The set of such $N$’s satisfies the assumptions of Lemma 1.2 so $G = \varprojlim G/N$. On the other hand, finite group $G/N$ acts on $F = K(x_1^G \cap ... \cap x_n^G)$ faithfully with the fixed field $K$ (Observe that $x_i$’s are finite orbits). Thus, by Artin’s Lemma, $F$ is a Galois extension of $K$ and $G/N \cong \text{Gal}(F/K)$. Since this holds for all $x_1^G \cap ... \cap x_n^G \in E$, $E$ is the union of all such $F$’s and we have $\text{Gal}(E/K) = \varprojlim \text{Gal}(F/K)$. Hence, we get the isomorphism $\text{Gal}(E/K) = \varprojlim \text{Gal}(F/K) \cong \varprojlim G/N = G$ induced by the finite case. \( \square \)

Proof of Theorem 1.8. Let $\Gamma = \coprod G/N$ where the disjoint union runs over open normal subgroups of $G$ and $F$ be any field. Define the action of $G$ on the purely transcendental extension $F(\Gamma)$ by $g.(xN) := (gx)N$ for $xN \in \Gamma$ and $a^g = a$ for $a \in F$. Since $\Gamma$ is a set of formal objects, in other words set of algebraically independent elements over $F$, $G$ acts on
An element of \( F(\Gamma) \) is of the form \( y = f(x_1, ..., x_n, a_1, .., a_k) \) where \( x_i \in \Gamma \), \( a_i \in F \) and \( f \) is a function. On the other hand, \( G_{a_i} = G \) and \( G_x = N \) for \( x_i \in G/N \); In particular \( G_x \) is open. Therefore, \( G_x \cap ... \cap G_{x_n} \cap G_{a_1} \cap ... \cap G_{a_k} \) is open, and \( G_y \) is open since it contains \( G_x \cap ... \cap G_{a_k} \). Hence, by Lemma 1.9, we are done. □

2. Pontryagin Duality

A direct system of topological groups is a family \((A_i, \varphi^j_i)_{i,j \in I}\) of topological groups and continuous homomorphisms

\[ \varphi^j_i : A_i \to A_j \]

such that for \( k \leq i \leq j \), we have

\[ \varphi^i_i = id \] and \( \varphi^j_i \circ \varphi^i_k = \varphi^j_k \).

The direct or inductive limit of a direct system of topological groups \((A_i, \varphi^j_i)\) is the group \( A = \bigoplus_I A_i / \Gamma \) where \( \Gamma = \langle \varphi^j_i(x) - x \mid x \in A_i, i, j \in I \rangle \) and is denoted by \( A = \text{lim}_\rightarrow A_i \).

Given a torsion abelian group \( G \), its dual \( G^* = \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \) is a commutative profinite group with the topology given by pointwise convergence. Then we have the duality:

\[
\text{Torsion Abelian Groups} \iff \text{Commutative Profinite Groups}
\]

Formally speaking, we have:

**Theorem 1.10.**

i. If \( G \) is a profinite group then its dual \( G^* \) is a discrete torsion abelian group.

ii. Conversely, if \( G \) is a discrete torsion abelian group then \( G^* \) is a profinite group.

iii. If \( G \) is a profinite group or a discrete torsion abelian group then the homomorphism

\[ \alpha_G : G \to G^{**} \]

is an isomorphism.

It is clear that Pontryagin duality holds for cyclic groups, and so does for finite abelian groups since every finite abelian group is a sum of its cyclic components. In order to generalize this fact to profinite groups, we need some facts which state some basic properties of compact, discrete groups and inverse and direct limits.

**Lemma 1.11.**

i. Every proper closed subgroup of \( S^1 \) is finite.
ii. If \( G \) is a compact group then \( \text{Hom}_{TG}(G, S^1) \) is a discrete group where \( \text{Hom}_{TG} \) stands for topological group homomorphisms and similarly \( \text{Hom} \) stands for group homomorphisms.

iii. If \( G \) is a discrete then \( G \) is a compact group.

Proof. i. It immediately follows from the obvious fact that any infinite subgroup of \( S^1 \) is dense in \( S^1 \).

ii. Assume \( G \) is a compact group. It is enough to show that \( \varphi \in G^* \), \( \varphi(g) = 1 \) for all \( g \in G \), is isolated, i.e. There is no sequence \( (\psi_n)_n \) with \( \psi_n(g) \neq 1 \) for some \( g \in G \) for all \( n \in \mathbb{N} \) such that \( (\psi_n)_n \to \varphi \).

Suppose not! Let \( (\psi_n)_n \) be such a sequence. Then for all \( n \in \mathbb{N} \) there is \( g_n \in G \) with \( \psi_n(g_n) \in [e^{\pi i/2}, e^{3\pi i/2}] \). Since \( G \) is compact we may assume that \( \lim g_n = g \) exists. Then \( \lim \psi_n(g_n) = \varphi(g) = 1 \in [e^{\pi i/2}, e^{3\pi i/2}] \). A contradiction.

iii. \( G \) is discrete so \( \text{Hom}_{TG}(G, S^1) = \text{Hom}(G, S^1) \). It suffices to show that \( \text{Hom}_{TG}(G, S^1) \) is a closed subgroup of \( \prod_G S^1 \), which is a compact Hausdorff space. Let \( (\psi_n)_n \) be a sequence in \( \text{Hom}(G, S^1) \) with \( (\psi_n)_n \to \psi \) in \( \prod_G S^1 \). Then for \( g_1, g_2 \in G \) we have

\[
\psi(g_1g_2) = \lim \psi_n(g_1g_2) = \lim(\psi_n(g_1)\psi_n(g_2)) = \lim \psi_n(g_1) \lim \psi_n(g_2) = \psi(g_1)\psi(g_2)
\]

and we are done. \( \square \)

Lemma 1.12. Let \( G \) be a profinite group and \( f : G \to S^1 \) be a continuous homomorphism. Then \( f(G) \) is a finite subgroup of \( S^1 \) and \( f(G) < \mathbb{Q} \).

Proof. In view of Lemma 1.11, this is trivial. \( \square \)

Lemma 1.13.

i. Let \( \{G_i, \varphi_{ij}, I\} \) be a surjective inverse system of profinite groups over a directed set \( I \) and let \( G = \varprojlim_{i \in I} G_i \). Then there exists an isomorphism

\[
G^* = \text{Hom}_{TG}(\varprojlim_{i \in I} G_i, \mathbb{Q}/\mathbb{Z}) = \varprojlim \text{Hom}_{TG}(G_i, \mathbb{Q}/\mathbb{Z}) = \varprojlim G_i^*.
\]

ii. Let \( \{A_i, \varphi_{ij}, I\} \) be a direct system of discrete torsion abelian groups over a directed set \( I \) and let \( G = \varinjlim_{i \in I} A_i \) be its direct limit. Assume that the canonical homomorphism \( \varphi_i : A_i \to A \) are inclusion maps. Then there exists an isomorphism of profinite groups

\[
A^* = \text{Hom}_{TG}(\varinjlim_{i \in I} A_i, \mathbb{Q}/\mathbb{Z}) = \varinjlim \text{Hom}_{TG}(A_i, \mathbb{Q}/\mathbb{Z}) = \varinjlim A_i^*.
\]
Proof. i. Let $f : G \to \mathbb{Q}/\mathbb{Z}$ be a continuous homomorphism. Then $f(G)$ is finite by Lemma 1.12. Therefore, there exits $f_i : G_i \to \mathbb{Q}/\mathbb{Z}$ with $f = f_i \varphi_i$ where $\varphi_i : G \to G_i$ is the projection [Ri, p 13]. Then we have the isomorphism

$$\Phi : G^* \to \varprojlim G_i^*$$

defined by

$$f \mapsto (f_i)_i.$$

ii. Let $f : A \to \mathbb{Q}/\mathbb{Z}$ be a continuous homomorphism. Then we have the isomorphism of groups

$$\Psi : A^* :\to \varprojlim A_i^*$$

defined by

$$f \mapsto (f_i)_i$$

where $f = f_i \varphi_i$ and $\varphi_i : A_i \to A$ is the canonical homomorphism. It is clearly an isomorphism of groups. Since $A^*$ and $\varprojlim A_i^*$ are compact, it suffices to prove that $\Psi$ is continuous. Let $f^n \to f$ be a convergent sequence of such maps. We want to show that $f^n_i = f^n \varphi_i \to f_i = f \varphi_i$ for all $i$. But it means that $f^n(\varphi_i(a_i)) \to f(\varphi_i(a_i))$, which holds since $A$ is discrete i.e $f^n(a) = f(a)$ for sufficiently big $n > N_a$ and for all $a \in A$.

□

Proof of Theorem 1:10. (i) and (ii) follows from Lemma 1.11 and Lemma 1.12.

iii. Let $G$ be a profinite group, $G = \varprojlim G_i$ where $\{G_i, \varphi_{ij}, I\}$ is an inverse system of finite abelian groups. Then for each $i \in I$ we have the commutative diagram

$$\begin{array}{ccc}
G & \xrightarrow{\alpha_G} & G^{**} \\
\varphi_i \downarrow & & \varphi_i^{**} \\
G_i & \xrightarrow{\alpha_{G_i}} & G_i^{**}
\end{array}$$

By Lemma 1.13, we get the isomorphism $\alpha_G = \varprojlim \alpha_{G_i}$.

On the other hand, if $G$ is a discrete torsion abelian group then, by Lemma 1.13, $G = \varprojlim G_i$ where $G_i$'s are finite subgroups of $G$. Then we have the isomorphism

$$\alpha_G : G = \varprojlim G_i \to \varprojlim G_i^{**} = G^{**}$$

induced by

$$\alpha_{G_i} : G_i \to G_i^{**}.$$

□
3. Subgroups

**Lemma 1.14.** let $G$ be a compact group and $\{S_i\}_{i \in I}$ be a decreasing filtration of $G$ by closed subgroups. Let $S = \bigcap S_i$. Then the canonical map

$$\varphi : G/S \to \varprojlim G/S_i$$

is a homeomorphism.

*Proof.* Clearly, $\varphi$ is injective and continuous. And, $\varphi(G/S)$ is dense in $\varprojlim G/S_i$ since $\Pi_i^{-1}(U_i)$’s form a basis and $\varphi(g) \in \Pi_i^{-1}(U_i)$ where $\Pi_i(g) \in U_i$, $U_i$ is an open subset of $G/S_i$. Compactness of $G$ implies that $\varphi$ is a surjection and homeomorphism. $\square$

**Lemma 1.15.** Let $K \leq H$ be closed subgroups of a profinite group $G$ with $[H : K] < \infty$. Then there is a continuous section $s : G/H \to G/K$.

*Proof.* We know that open normal subgroups of $G$ forms a base for neighborhoods of 1. Since $H/K$ is finite, $K$ is open in $H$ and so there is an open subset $U$ of $G$ such that $U \cap H = K$. By the fact mentioned above, we may assume that $U$ is an open normal subgroup of $G$ with the assumption $U \cap H \subseteq K$. Then the canonical map $\Pi \downarrow_U : G/K \to G/H$ is an injection and, of course, a homeomorphism. Since $G = g_1U \sqcup \ldots \sqcup g_kU$, one can extend the inverse of this map to whole $G$ by translation continuously. This completes the proof. $\square$

**Theorem 1.16.** Let $K \leq H$ be arbitrary closed subgroups of $G$. Then there exits a continuous section $s : G/H \to G/K$.

*Proof.* Consider the set $Z = \{(U_i, s_i) \mid U_i$ is a closed subgroup of $H$ with $U_i \supseteq K$, $s_i : G/H \to G/U_i$ is a section $\}$. Let’s define an order on $Z$ as follows: $(U_i, s_i) \leq (U_j, s_j)$ if and only if $U_i \supseteq U_j$ and $s_i = p \circ s_j$ where $p : G/U_j \to G/U_i$ is the canonical map. By Lemma 1.14, $(U, s)$ is the maximal element of an ascending chain $(U_i, s_i)$ with $U = \bigcap U_i$ and $s = \bigcup s_i$. By Zorn’s lemma, there is a maximal element, call $(U, s)$. We claim that $U = K$.

Suppose not! Let $S$ be a proper subgroup of $U$ containing $K$ with $[U : K] < \infty$ (It exists because $K = \bigcap S_i$ where $S_i$’s are open subgroups, or equivalently closed subgroups of finite index). Then, by Lemma 1.15, there is a continuous section

$$p : G/U \to G/S.$$

Therefore, $(S, s') \in Z$ where $s' = p \circ s$ and $(U, s) \not\leq (S, s')$. A contradiction. $\square$
4. Sylow p-Subgroups

A supernatural number is a formal product $\prod p^{n_p}$ where $n_p \in \mathbb{N} \cup \{\infty\}$ and the product runs over the prime numbers. Product, $\text{lcm}$ and $\text{gcd}$ of supernatural numbers are in the obvious way.

Let $G$ be a group with a closed subgroup $H$. The index of $H$ in $G$, denoted by $(G : H)$, is the $\text{lcm}$ of the set of supernatural numbers $\{(G : U)/(HU : U) \mid U \leq G, \text{open}\}$. One can show that $(G : H) = \text{lcm}\{(G : V) \mid V \text{ is open subgroup of } G \text{ containing } H\}$.

Proposition 1.17.

i. If $K \subseteq H \subseteq G$ are profinite groups then $(G : K) = (G : H)(H : K)$,

ii. If $\{H^i\}_{i \in I}$ is a decreasing filtration of closed subgroups of $G$ with $H = \bigcap_i H^i$ then $(G : H) = \text{lcm}\{(G : H^i) \mid i \in I\}$,

iii. $H$ is open in $G$ if and only if $(G : H) \in \mathbb{N}$.

Proof. i. We claim that $(H : K) = \text{lcm}\{(H_U : K_U) \mid U \leq G, \text{open}\}$ where $H_U = HU/U$ and $K_U = KU/U$. The part ”$\geq$” is trivial. Let $V$ be an open subgroup of $H$. It suffices to find an open subgroup $U \leq G$ such that $(H_V : K_V)$ divides $(H_U : K_U)$. Since $V$ is open in $H$, there exists an open normal subgroup $U$ of $G$ with $U \cap H \subseteq V$. One can see that this is the required subgroup.

Now, for an open normal subgroup $U$ of $G$ we have

$$(G_U : K_U) = (G_U : H_U)(H_U : K_U)$$

and so

$$\text{lcm}\{(G_U : K_U)\} = \text{lcm}\{(G_U : H_U)\}\text{lcm}\{(H_U : K_U)\}.$$ 

By the claim we have already proved and the definitions, we get

$$(G : K) = (G : H)(H : K).$$

ii. The inequality ”$\geq$” is obvious by $i$. The equality follows from the fact that for an open normal subgroup $U$ of $G$ there is a $c \in \mathbb{N}$ such that $(G_U : H_U) = (G_U : H^n_U)$ for all $n > c$. 

iii. Trivial. \hfill \square

A profinite group is called profinite $p$-group if it is inverse limit of $p$-groups. A subgroup $H$ of $G$ is called Sylow $p$-subgroup if it is a profinite $p$-group and $(G : H)$ is coprime to $p$ (as a supernatural number). As we have done previous sections, we continue to generalize the theorems holding for finite groups. Here is the generalization of Sylow theorems; But we first need a lemma:

Lemma 1.18. Inverse limit of nonempty finite sets is nonempty.
Proof. Let $S = \lim S_i$ be the inverse limit of the nonempty finite sets with maps $\{\varphi^j_i : S_j \to S_i\}_{i, j \in I}$. Let’s equip the finite sets with the discrete topology. Define

$$C_k = \{(x_i)_{i} \in \prod_i S_i \mid x_i = \varphi^i_j(x_j), \forall i \leq j \leq k\}.$$ 

Clearly, by axiom of choice, $C_k$ is a closed nonempty subset of $\prod_i S_i$ for all $k \in I$. Since $I$ is a directed set, intersection of any finitely many $C_k$’s is nonempty. Hence, by compactness of $\prod_i S_i$, $\bigcap_i C_k = S$ is nonempty.

Proposition 1.19.

i. Every profinite group $G$ has a Sylow $p$-subgroup,

ii. Every $p$-subgroup of $G$ is contained in a Sylow $p$-subgroup,

iii. If $\varphi : G \to G'$ is an epimorphism and $H$ is a sylow $p$-subgroup then $\varphi(H)$ is a sylow $p$-subgroup.

Proof. i. By Lemma 1.2, we know that $G = \lim(G/U)$ where $U$ is an open normal subgroup of $G$. Let $H_U$ be a Sylow $p$-subgroup of $G/U$ for fixed $p$. Then $H = \lim(H_U)$ is a Sylow $p$-subgroup of $G$. Let $H' = \lim(H_U')$ be another Sylow $p$-subgroup of $G$ and $\Gamma_U = \{g_u \in G/U \mid H^g_u = H'\}$. Since $\Gamma_U$ is nonempty, by Lemma 1.18, $\lim(\Gamma_U)$ is nonempty and we are done.

ii. If $K$ is a $p$-subgroup of $G$ then $K_U$ is a $p$ is a subgroup of $G/U$ and is contained in a Sylow $p$-subgroup $H_U$. Hence $K = \lim(K_U) \subseteq \lim(H_U) = H$.

iii. One can prove it easily by using the same arguments.
Chapter 2

Cohomology

1. Two Definitions of Cohomology and Their Equivalence

Throughout the chapter $G$ will stand for a profinite group unless specified. In this section, we want to define cohomology of $G$ in two different ways and show their equivalence. We define cohomology of $G$ with coefficients in $A$, denoted by $H(G; A)$, only when $A$ is a discrete $G$ module, i.e. $A$ is a discrete abelian group on which $G$ acts continuously.

$C_G$, the category of discrete $G$ modules, is a full subcategory of the category of $G$ modules and so it is an abelian category in which direct limit exist. In this section we also show that $C_G$ has enough injectives, but not projectives. We know that the set of open subgroups of $G$ forms a fundemental system of neighborhoods of 1; we will denote this set by $\Omega$. For $A \in C_G$, we have

$$A = \bigcup_{\Omega} A^U \quad \text{where} \quad A^U = \{a \in A \mid a^g = a, \forall g \in U\} \quad (\ast)$$

where $U \in \Omega$. It is very easy to show that any $G$ module satisfying $(\ast)$ is discrete. The property $(\ast)$ allows us to generalize the facts in cohomology which exist for finite groups and because of this, it is defined only for discrete modules.

Let’s give our first definition of the cohomology, which we call continuous cohomology and denote by $H^*$. Let $A \in C_G$. One defines $C^n(G, A)$ as the set of continuous maps from $G^n$ to $A$ and the differentials, as usual,

$$d : C^{n-1}(G, A) \to C^n(G, A)$$

by

$$(df)(g_1, \ldots, g_n) = g_1f(g_2, \ldots, g_n) + \sum_{i=1}^{n-1} f(g_1, \ldots, g_ig_{i+1}, \ldots, g_n) + (-1)^n f(g_1, \ldots, g_{n-1}).$$

Thus, taking the cohomology, we get continuous cohomology of $G$ with coefficients in $A$. One can easily see that the definition recovers the standard definition of cohomology of finite
groups. Here is the most important theorem of this chapter, which summarize the idea of generalization of the cohomology of finite groups to that of profinite groups:

**Theorem 2.1.** Let \((G_i)_{i \in I}\) be an inverse system of profinite groups and \((A_i)_{i \in I}\) be a direct system of \(G_i\) modules in which the homomorphisms \(A_i \rightarrow A_j\) are compatible with the homomorphisms \(G_j \rightarrow G_i\). Then one has for each \(q \geq 0\)

\[
H^q_{\text{ct}}(G; A) = \lim_{\rightarrow} H^q(G_i; A_i)
\]

where \(A = \lim_{\rightarrow} A_i\) and \(G = \lim_{\leftarrow} G_i\).

**Proof.** We have the canonical homomorphism

\[
\Psi : \lim_{\rightarrow} C^*(G_i, A_i) \rightarrow C^*(G, A)
\]

defined by

\[
\Psi((f_i)_i)(g_i)_i := (f_i(g_i))_i.
\]

It suffices to show that \(\Psi\) is an isomorphism. Injectivity follows from a simple computation. Let \(f \in C^n(G, A)\). Then \(f(G)\) is finite and \(f\) factors through \(G_i\) for sufficiently big \(i\) i.e there exists \(f_i : G_i^n \rightarrow A_i\) in \(C^n(G_i, A_i)\) with \(f = f_i \phi_i^n\) [Ri, p 13]. This proves the surjectivity and completes the proof. \(\square\)

**Corollary 2.2.** Let \(A \in C_G\). Then one has

\[
H^q_{\text{ct}}(G; A) = \lim_{\rightarrow} H^q(G/U; A^U)
\]

where the limit runs over \(\Omega\). In fact, \(G = \lim_{\rightarrow} G/U\) and \(A = \lim_{\leftarrow} A^U\).

**Corollary 2.3.** For \(A \in C_G\), we have

\[
H^q_{\text{ct}}(G; A) = \lim_{\rightarrow} H^q(G; B)
\]

where \(B\) runs over the set of finitely generated submodules of \(A\).

**Corollary 2.4.** For \(q \geq 1\), \(H^q(G; A)\) is a torsion group.

**Proof.** In case \(G\) is finite, it is a classical result (see corollary 2.9). Then, it immediately follows from Corollary 2.2. \(\square\)

By using the results we already mentioned, one can reduce everything to the case of finite groups. For instance, one may deduce \(H^q(G; A)\) is trivial for \(q \geq 1\) is \(A\) is injective in \(C_G\).

Now we define the cohomology as the functor \(A \rightarrow H^q(G; A)\) which is the derived functor of the functor \(A \rightarrow A^G\). In other words, one defines \(H^q(G; A) := \text{Ext}^q(\mathbb{Z}, A)\) for \(A \in C_G\). We will show that \(C_G\) has enough injectives. Notice that \(C_G\) does not have enough projectives.
Indeed, $ZG \notin C_G$ by (*) and so any $ZG$ free module is not in $C_G$. Thus, $C_G$ has no $ZG$ projective module.

**Theorem 2.5.** $C_G$ has enough injective modules. Moreover, for each object $A \in C_G$ there is an injective resolution $A \rightarrow A^\bullet$ such that $A^\bullet = \bigcup_{U \in \Omega} A_U^\bullet$, where $A_U^\bullet$ is an injective resolution of $A^U$ in $G$-$\text{Mod}$.

**Lemma 2.6.** If $I$ is a injective $G$ module then $I^U$ is $G/U$- injective for all $U \in \Omega$. Conversely, for a direct system $(I_U, i_U^V)$ of $G/U$ modules, $I = \lim I_U$ is injective in $C_G$ if $i_U^V$ is injective for all $U \subseteq V$ in $\Omega$.

**Proof.** Let $I \in C_G$ be an injective module, $U \in \Omega$ and $A$ and $B$ be $G/U$-modules with an injective morphism $i : A \rightarrow B$. We can regard $A$ and $B$ as $G$-modules via the projection $G \rightarrow G/U$. Then, by $G$-injectivity of $I$, a morphism $\varphi : A \rightarrow I$ can be extended to a morphism $\tilde{\varphi} : B \rightarrow I$ via the map $i$. Since $U$ acts on $A$ and $B$ trivially, $Im(\varphi) \subseteq Im(\tilde{\varphi}) \subseteq I^U$ and $\tilde{\varphi}$ is an extension of $\varphi$ in $G/U$-$\text{Mod}$. Hence, $I^U$ is injective.

Now suppose that we are given such a direct system. Let $A$ and $B$ be in $C_G$ with an injective morphism $i : A \rightarrow B$ and $\alpha : A \rightarrow I$ be a $G$-morphism. In general, the module $A$ can be written as a union of its submodules, $A = \bigcup A_j$, such that $A_j^U$ is a finitely generated $G$-module for all $j$ and $U \in \Omega$. Indeed, $A = \lim \lim A_j^U$ where $A_j^U$ are finitely generated $G/U$-modules of $A^U$. If we find the extension of $\alpha \mid_{A_j} := \alpha_j$, say $\beta_j : B \rightarrow I$, for all $j$ then one takes the limit of extensions $\lim \beta_j = \beta : B \rightarrow I$ as the extension of $\alpha$ and complete the proof. So we may assume that $A^U$ is a finitely generated $G$ module for all $U \in \Omega$. Let $U \in \Omega$ and $\alpha \mid_{A^U} := \alpha_U : A^U \rightarrow I$. Then $Im(\alpha_U) \subseteq I_{V(U)}$ for some sufficiently small $V(U) \in \Omega$ since $A^U$ is finitely generated. We may assume that $V = V(U) \subseteq U$. If $U' \subseteq U$ then we have the correspondence $V' = V(U') \subseteq V = V(U)$ and the commutative diagram

$$
\begin{array}{ccc}
I_U & \xrightarrow{i_U^V} & I_{U'} \\
\downarrow{\alpha_U} & & \downarrow{\alpha_{U'}} \\
A^U & \xrightarrow{i_{U'}} & A_U^U \\
\end{array}
$$

Therefore, we may assume that $i_U^V, \beta_U = \beta_{U'}$ and this allows us to take the limit

$$
\lim \beta_U = \beta : B \rightarrow I
$$

which is the desired extension of $\alpha$. This completes the proof.

For a given unital ring $R$ and a (left) $R$-module $M$, we know that we can embed $M$ into an injective module $I_M$. Indeed, we have the isomorphism

$$
\text{Hom}_R(M, \text{Hom}_Z(R, \mathbb{Q}/\mathbb{Z})) \cong \text{Hom}_Z(M, \mathbb{Q}/\mathbb{Z})
$$

(2.1)

given by

$$
\varphi \mapsto \tilde{\varphi} \quad \text{where} \quad \tilde{\varphi}(x) = \varphi(x)(1)
$$

14
where $\text{Hom}_\mathbb{Z}(R, \mathbb{Q}/\mathbb{Z})$ is a $R$ module whose action defined by $(\lambda f)(x) = f(x\lambda)$ for $\lambda \in R$.

It is easy to show that $\text{Hom}_\mathbb{Z}(R, \mathbb{Q}/\mathbb{Z})$ is an injective module [Hi, p 190]. Clearly, for any $m \in M - \{0\}$ there is a $\phi_m \in \text{Hom}_\mathbb{Z}(R, \mathbb{Q}/\mathbb{Z})$ with $\phi_m(m) \neq 0$ by divisibility of $\mathbb{Q}/\mathbb{Z}$; And so, by (2.1), there is $\varphi_m \in \text{Hom}_R(M, \text{Hom}_\mathbb{Z}(R, \mathbb{Q}/\mathbb{Z})$ with $\varphi_m(m) \neq 0$. Now we have the injective $R$ module $\prod_{M - \{0\}} \text{Hom}_\mathbb{Z}(R, \mathbb{Q}/\mathbb{Z})$ and the embedding

$$\iota_M : M \hookrightarrow I_M = \prod_{M - \{0\}} \text{Hom}_\mathbb{Z}(R, \mathbb{Q}/\mathbb{Z})$$

defined by

$$\iota_M(x) = \prod \varphi_m(x).$$

Notice that the injectivity follows from the fact that $\varphi_m(m) \neq 0$.

Proof of Theorem 2.5. Let $A \in C_G$ and $U \in \Omega$. Then there is an injective $G/U$ module $I_U$ with the injection

$$\iota_{AU} : A^U \hookrightarrow I_U = \prod_{A - \{0\}} \text{Hom}_\mathbb{Z}(\mathbb{Z}[G/U], \mathbb{Q}/\mathbb{Z}).$$

And the projection $\Pi^U_V : G/V \to G/U$, for $V \subseteq U$ in $\Omega$, induces an monomorphism

$$i^U_V : (\Pi^U_V)^* : \text{Hom}_\mathbb{Z}(\mathbb{Z}[G/U], \mathbb{Q}/\mathbb{Z}) \to \text{Hom}_\mathbb{Z}(\mathbb{Z}[G/V], \mathbb{Q}/\mathbb{Z}).$$

Then we have the monomorphism induced naturally by $i^U_V$

$$i^U_V : I_{AU} \to I_{AV}.$$

In summary, we have the compatibility condition

$$\begin{array}{ccc}
A^U & \xrightarrow{\iota_{AU}} & I_{AU} \\
\downarrow \leq & & \downarrow \iota^U_V \\
A^V & \xrightarrow{\iota_{AV}} & I_{AV}
\end{array}$$

which allows us to take the limit over $\Omega$. By taking the direct limit and using lemma 2.6, we get the desired injective $G$ module and embedding

$$\iota_A = \varinjlim \iota_{AU} : A = \varinjlim A^U \to I_A = \varinjlim I_{AU}.$$

By the construction of the injective object, one can conclude the second point of the theorem and the proof. □

Corollary 2.7. Let $A \in C_G$. Then one has

$$H^\bullet(G; A) \cong \varinjlim H^\bullet(G/U; A^U) \cong H^\bullet_{ct}(G; A).$$
Proof. Suppose that we are given the injective resolutions $A^U \hookrightarrow I^U_*$ of $G/U$ modules. If $V \subseteq U$, we have the inclusion which induces a chain map

$$i^U_V : I^*_U \rightarrow I^*_V$$

and the unique map which is independent from the resolution, called inflation map,

$$(i^U_V)_* = \inf^U_H : H^*(G/U; A^U) \rightarrow H^*(G/V; A^V).$$

Therefore, $\lim \inf H^*(G/U; A^U)$ is well defined. $G$ acts on the injective resolution $\lim I^*_U = I^*$ in theorem 2.5, called standard injective resolution, componentwise and $d = \lim d_i$, we get the first identification

$$H^*(G; A) \cong \lim H^*(G/U; A^U).$$

By corollary 2.2, we are done. \qed

2. Res, Cor and Functoriality

From now on $H^*(G; A)$ will denote the cohomology in the both sense. Let $G'$ be a profinite group with a morphism $f : G \rightarrow G'$ and $A, A' \in C_G$ with a morphism $h : A' \rightarrow A$. Then, as usual, we have a induced map

$$(f, h) : H^*(G'; A') \rightarrow H^*(G; A).$$

In particular, if $H$ is a closed subgroup of $G$ then $H$ is profinite and we have the map induced by the inclusion $H \hookrightarrow G$, called Restriction,

$$\text{Res}^G_H : H^*(G; A) \rightarrow H^*(H; A).$$

Now we want to define a map called corestriction for profinite groups. Let $H$ be an open subgroup of $G$ of index $n$. In order to define this map

$$\text{Cor}^H_G : H^*(H; A) \rightarrow H^*(G; A)$$

we will use the limit process; In detail: Let $U \in \Omega$ be a normal subgroup and $\mathbb{Z} \leftarrow P_\bullet$ be a projective resolution of $G/U$ modules. Then $G/U$ and $H/H \cap U := H_U$ are finite groups and one has the Transfer map

$$T_{G/U, H_U} : \text{Hom}_{H_U}(P_\bullet, A^U) \rightarrow \text{Hom}_{G/U}(P_\bullet, A^U)$$

defined by

$$f \mapsto \sum_{s \in S} s.f \quad \text{and} \quad (s.f)(x) := sf(s^{-1}x)$$

16
where \( S \) is a set of representatives of the left coset space \((G/U)/(UH/U)\). Since \( f \) is \( H \) linear \( T_{G/U,H_U}(f) \) does not depend on the set of representatives. It is very easy to see that \( T_{G/U,H_U} \) commutes with the differentials and induces a homomorphism, namely corestriction,

\[
\Cor_{G/U}^{H_U}: H^\bullet(H/H \cap U; A^U) \to H^\bullet(G/U; A^U).
\]

By taking the limit, one gets

\[
\Cor_G^H = \lim_{\to} \Cor_{G/U}^{H_U}: H^\bullet(H; A) \to H^\bullet(G; A).
\]

**Proposition 2.8.** Let \( H \leq G \) be an open subgroup of index \( n \). Then \( \Cor_G^H \Res_G^H = n.id \).

**Proof.** Let \( A \in C_G \). By lemma 1.2, one has \( G = \lim G/U \) where \( U \) runs over open normal subgroups contained in \( H \). Let \( U \) be such a subgroup, \( Z \twoheadrightarrow \mathbb{P}^1_U \) be a projective resolution of \( G/U \) modules and \( f_u \in \Hom_{G/U} (\mathbb{P}^1_U, A^U) \). Then \( (G/U : UH/U) = n \), for any \( g \in G \) \( g.f_u = f_u \) and we have

\[
T_{G/U,H/H \cap U}(f_u) = \sum_{s \in S} s.f_u = \sum_{s \in S} f_u = (G/U : UH/U).f_u = n.f_u.
\]

Hence, \( \Cor_{G/U}^{H/H \cap U} \Res_{H/H \cap U}^G ([f_u]) = n.[f_u] \) and

\[
\Cor_G^H \Res_G^H ([f]) = \lim \Cor_{G/U}^{H/H \cap U} \Res_{H/H \cap U}^G ([f_u]) = \lim (n.[f_u])_u = n.[f]
\]

where \([f] = ([f_u])_u\). \( \square \)

**Corollary 2.9.** If \( G \) is finite then \( |G|.H^q(G; A) = 0 \) for any \( G \) module \( A \) and all \( q \geq 1 \). In particular, \( H^q(G; A) \) is torsion for all \( q \geq 1 \).

**Proof.** One takes \( H = 1 \) and use \( H^q(H; A) = 0 \) for all \( q \geq 1 \). \( \square \)

**Corollary 2.10.** If \( (G : H) = n \) then the kernel of \( \Res_G^H : H^\bullet(G; A) \to H^\bullet(H; A) \) is annihilated by \( n \).

**Corollary 2.11.** Let \( p \) be a prime number. If \( (G : H) \) is coprime to \( p \) then \( \Res_G^H \) is injective on the \( p \)-primary component of \( H^\bullet(G; A) \).

**Proof.** If \( (G : H) \) is finite then it follows from the proposition. Otherwise we can reduce the problem to this case as follows: Let \( A \in C_G \). One can show that \( \Res_G^H \) is induced by the maps

\[
\Res_{G/U,H/H \cap U}^G : H^\bullet(G/U; A^U) \to H^\bullet(UH/U).
\]

Since \( \lim H^\bullet(G/U; A^U) = H^\bullet(G; A) \) and \( \lim H^\bullet(H/H \cap U; A^U) = H^\bullet(H; A) \), it is enough to prove that \( \Res_{G/U,H/H \cap U}^G \) is injective on the \( p \)-primary component of \( H^\bullet(G/U; A^U) \) for all such \( U \). Observing \( (G/U : UH/U) = (G : H) /(UH : H) \), one gets that \( (G/U : UH/U) \) is coprime to \( p \) and completes the proof. \( \square \)
3. Induced Modules

Let \( H \) be a closed subgroup of \( G \) and \( A \in C_H \). Then the induced module is defined as
\[
A^* = M^H_G(A) := \{ a^* : G \to A \mid a^* \text{ is continuous and } H \text{ linear} \}.
\]

If \( H = 1 \) then one writes \( M_G(A) \) and calls the module induced\(^1\). \( M^H_G(A) \) is a \( G \) module on which the action of \( G \) is defined by \( (\lambda.f)(x) := f(x.\lambda) \) for \( x, \lambda \in G \). It is important to note that the actions of \( G \) and \( H \) commute. One can easily see that \( M^H_G(A) \in C_G \).

One defines a homomorphism \( M^H_G(A) \to A \) by \( a^* \mapsto a^*(1) \), that is compatible with the injection \( H \hookrightarrow G \); Hence gets the induced homomorphism
\[
H^\bullet(G; M^H_G(A)) \to H^\bullet(H; A).
\]

**Theorem 2.12.** The homomorphisms \( H^\bullet(G; M^H_G(A)) \to H^\bullet(H; A) \) are isomorphisms.

**Proof.** We first claim that if \( B \in C_G \) and \( A \in C_H \) then \( \text{Hom}_H(B, A) \cong \text{Hom}_G(B, M^H_G(A)) \).

Define the homomorphism \( \Psi : \text{Hom}_G(B, M^H_G(A)) \to \text{Hom}_H(B, A) \) by \( \Psi(f)(b) := f(b)(1) \) for \( b \in B \). Clearly, \( \Psi(f) \) is \( H \) linear. Let’s define the inverse
\[
\Psi^{-1} : \text{Hom}_H(B, A) \to \text{Hom}_G(B, M^H_G(A))
\]
by
\[
f \mapsto \hat{f} \text{ and } \hat{f}(b)(g) := f(g.b).
\]

Then, for \( g, x \in G \) and \( b \in B \), \( \hat{f}(gb)(x) = f(xgb) = \hat{f}(b)(xg) = g.(\hat{f}(b)(x)) \) and so \( \Psi^{-1}(f) = \hat{f} \) is \( G \)-linear. And, for \( f \in \text{Hom}_H(B, A) \) and \( b \in B \), \( \hat{f}(b) : G \to A \) is continuous because the action of \( G \) on \( A \) is continuous and so is \( f \) (since \( B \) is discrete). Obviously, \( \hat{f}(b) \) is \( H \) linear for all \( b \in B \). Therefore, \( \Psi^{-1} \) is well defined. Now:

For \( f \in \text{Hom}_H(B, A) \) and \( b \in B \),
\[
(\Psi\Psi^{-1})(f)(b) = \Psi(\Psi^{-1}(f))(b) = (\Psi^{-1}(f))(b)(1) = f(1.b) = f(b);
\]

For \( f \in \text{Hom}_H(B, M^H_G(A)) \), \( g \in G \) and \( b \in B \),
\[
(\Psi^{-1}\Psi)(f)(b)(g) = (\Psi^{-1}(f))(b)(g) = (\Psi(f))(g.b) = f(gb)(1) = (g.f(b))(1) = f(b)(1.g) = f(b)(g).
\]

Thus \( \Psi \) and \( \Psi^{-1} \) are inverse to each other and this proves our claim. Then it follows that \( M^H_G \) transforms injective objects to injective objects. Therefore, by a standard comparison theorem, it suffices to prove that \( M^H_G \) is an exact functor from \( C_H \) to \( C_G \).

We now claim that \( M^H_G \) is an exact functor. Let
\[
\begin{array}{cccc}
0 & \longrightarrow & A & \stackrel{\varphi}{\longrightarrow} & B & \stackrel{\psi}{\longrightarrow} & C & \longrightarrow 0
\end{array}
\]

\(^1\text{In the literature, the common terminology for this module is coinduced.}\)
be short exact sequence in $C_H$. Then we have the sequence
\[ 0 \longrightarrow M^H_G(A) \xrightarrow{\varphi_*} M^H_G(B) \xrightarrow{\psi_*} M^H_G(C) \longrightarrow 0 \]
in $C_G$. Obviously, $\varphi_*$ is injective. Let $f \in \text{Ker}(\psi_*)$. Since the given sequence is exact, for any $b \in B$ there is $a_b \in A$ with $\varphi(a_b) = b$. In particular, for any $g \in G$ there is $a_g \in A$ with $\varphi(a_g) = f(g)$. On the other hand, $f^{-1}(f(g)) = U_g$ is open in $G$ for all $g \in G$ and $U_{g_1} \cap U_{g_2} = \emptyset$ if $f(g_1) \neq f(g_2)$. Moreover, $\bigcup U_g = G$. Therefore, $f' : G \to A$ defined by $f'(g) := a_g$ is well defined, continuous and $\varphi_*(f')(g) = \varphi(f'(g)) = \varphi(a_g) = f(g)$ for $g \in U_g$. Thus, $\varphi_*(f') = f$ and the sequence is exact at $M^H_G(B)$. One uses the same arguments to prove the surjectivity of $\psi_*$ and completes the proof. 

**Corollary 2.13.** The cohomology of an induced module is zero of dimension $\geq 1$.

**Proof.** One takes $H = 1$ and uses $H^q(1; A) = 0$ for $q \geq 1$. 

Theorem 2.12, due to Faddeev and Shapiro, is very useful; It reduces the cohomology of a subgroup to that of the group. We can recover the homomorphisms in terms of Res and Cor as follows:

(i) Let $A \in C_G$. We have the injective $G$-homomorphism
\[ i : A \hookrightarrow M^H_G(A) \quad \text{defined by} \quad i(a)(g) = ga. \]

This induces a morphism on cohomology
\[ i_* : H^\bullet(G; A) \to H^\bullet(G; M^H_G(A)). \]

By composing with the isomorphism $\Psi : H^\bullet(G; M^H_G(A)) \to H^\bullet(H; A)$, we get
\[ \text{Res}^G_H : H^\bullet(G; A) \to H^\bullet(H; A). \]

Indeed, the map , for every $B \in C_G$, $B \xrightarrow{i} M^H_G(B) \xrightarrow{\psi} B$ defined by $b \mapsto i(b) \mapsto i(b)(1) = b.1 = b$ induces a map of cochain complexes: for an injective resolution $A \hookrightarrow I^\bullet$ of $G$ modules,
\[
\begin{array}{ccccccccc}
0 & \longrightarrow & \text{Hom}_G(\mathbb{Z}, A) & \xrightarrow{i_*} & \text{Hom}_G(\mathbb{Z}, I^0) & \xrightarrow{i_*} & \text{Hom}_G(\mathbb{Z}, I^1) & \longrightarrow & \\
& & \downarrow \psi_* & & \downarrow \psi_* & & \downarrow \psi_* & & \\
0 & \longrightarrow & \text{Hom}_G(\mathbb{Z}, M^H_G(A)) & \xrightarrow{} & \text{Hom}_G(\mathbb{Z}, M^H_G(I^0)) & \longrightarrow & \text{Hom}_G(\mathbb{Z}, M^H_G(I^1)) & \longrightarrow & \\
& & \downarrow \psi_* & & \downarrow \psi_* & & \downarrow \psi_* & & \\
0 & \longrightarrow & \text{Hom}_H(\mathbb{Z}, A) & \longrightarrow & \text{Hom}_H(\mathbb{Z}, I^0) & \longrightarrow & \text{Hom}_H(\mathbb{Z}, I^1) & \longrightarrow & \\
\end{array}
\]

This gives us a homomorphism $\alpha : H^\bullet(G; A) \to H^\bullet(H; A)$ by taking an $H$ injective resolution of $A$, lifting the map $A \xrightarrow{id} A$ (as $H$ modules) to the injective resolution and
composing this map with the map induced by the diagram above. Therefore, in order to show that \( \alpha = \text{Res}_G^G \), it suffices to show that \( \psi_\ast i_\ast \) are in fact natural inclusions and that is: for \( f \in \text{Hom}_G(\mathbb{Z}, I^*) \),

\[
(\psi_\ast i_\ast(f))(1) = \psi_\ast(i_\ast(f))(1) = (((i \circ f))(1))(1) = i(f(1))(1) = f(1).1 = f(1).
\]

(ii) Let \( H \leq G \) be an open subgroup of index \( n \), \( A \in C_G \) and \( S \) be a set of representatives of the left coset space \( G/H \). One defines a surjective homomorphism

\[
\Pi : M^H_G(A) \rightarrow A \quad \text{by setting} \quad \Pi(a^s) = \sum_{x \in S} x.a^s(x^{-1}).
\]

This map is independent of choice of the set of representatives since \( a^s \) is \( H \) linear. And, it induces a map on cohomology, that is actually

\[
\text{Cor}_G^H : H^\ast(H; A) \xrightarrow{\Psi^{-1}} H^\ast(G; M^H_G(A)) \xrightarrow{\Pi^\ast} H^\ast(G; A)
\]

where \( \Psi \) is the isomorphism constructed in theorem 2.12.

Indeed, as in (i), for the projective resolutions \( \mathbb{Z} \xleftarrow{\Pi} P^U \) of \( G/U \) modules it is enough to show that the map

\[
\text{Hom}_{H/U}(P^U, A^U) \xrightarrow{\Psi^{-1}} \text{Hom}_{G/U}(P^U, M^H_G(A^U)) \xrightarrow{\Pi^\ast} \text{Hom}_{G/U}(P^U, A^U)
\]

is the transfer map for every \( U \in \Omega \) which is contained in \( H \). Let \( U \) be such a open subgroup, \( f \in \text{Hom}_{H/U}(P^U, A^U) \), \( x \in P^U \) and \( S \) be a representative set of \( G/U \). Then we have:

\[
(\Pi(x)(f))(x) = \Pi(\Psi^{-1}(f)(x)) = \sum_{g \in S} g.\Psi^{-1}(f)(x)(g^{-1})
\]

\[
= \sum_{g \in S} g.f(g^{-1}x) = T_{G/U,H/U}(f)(x).
\]

4. **Cup Products**

Given a (any) group \( G \), \( H^\ast(G; \mathbb{Z}) \) can be endowed with a multiplicative structure which turns it into a commutative graded ring, i.e \( xy = (-1)^{pq}yx \) for \( x \in H^p(G; \mathbb{Z}) \) and \( y \in H^q(G; \mathbb{Z}) \). This multiplicative structure will be given by the cup product. We will define the product in a more general setting for our purposes in spite of that most interesting cases occur in case the \( G \) module is \( \mathbb{Z} \).

Let \( A, B, C \in C_G \) and \( \theta : A \times B \rightarrow C \) be a \( G \)-pairing, that is \( \theta \) is a bi-additive map satisfying \( \theta(\sigma a, \sigma b) = \sigma \theta(a, b) \) for all \( \sigma \in G \). Then \( \theta \) gives rise to a map, called "cup product"

\[
H^\ast(G; A) \times H^\ast(G; B) \rightarrow H^{\ast + \ast}(G; C).
\]

We can define "cup product" explicitly as follows: Let \( a \in H^\ast(G; A) \) and \( b \in H^\ast(G; B) \). Let \( f \in C^r(G, A) \) and \( g \in C^s(G, B) \) representing \( a \) and \( b \), respectively. Then one defines and denotes cup product of \( a \) and \( b \) by

\[
ab = [fg]
\]
where
\[ f g(x_1, \ldots, x_{r+s}) = \theta(f(x_1, \ldots, x_r), x_1 \ldots x_r g(x_{r+1}, \ldots, x_{r+s})). \]

One can easily check that the definition is well defined and can also prove the following theorem by doing long computations (or by just seeing [CE, ch 12] for a complete proof):

**Theorem 2.14.** Let the notation be as above. The cup product is a \( \mathbb{Z} \)-linear mapping uniquely determined by its value in dimension zero and the following fact: Given three exact sequences
\[
0 \to A' \to A \to A'' \to 0 \\
0 \to B' \to B \to B'' \to 0 \\
0 \to C' \to C \to C'' \to 0
\]
such that \( A \times B \to C, A'' \times B'' \to C'', A' \times B'' \to C', A'' \times B' \to C' \) under \( \theta \) for \( a \in H^r(G; A'') \) and \( b \in H^s(G; B'') \) we have
\[
\delta(ab) = \delta(a)b + (-1)^r a\delta(b).
\]

Moreover, when \( A = B \) the cup product is graded commutative, i.e
\[
ab = (-1)^{rs}ba
\]
and, in general, it is associative in the usual sense.

A \( G \)-pairing \( \theta \) yields an \( H \)-pairing for any closed subgroup \( H \leq G \). Of course, there is a corresponding cup product for that cohomology over \( H \) and the relationship between this cup product is given by

**Proposition 2.15.** Let \( G \) be a profinite group and \( H \leq G \) be an open subgroup. Let \( A, B, C \in C_G \) with a \( G \)-pairing \( \theta : A \times B \to C \). Then, for \( a \in H^r(H; A) \) and \( b \in H^s(G; B) \), one has
\[
\Cor^H_G(a. \Res^G_H(b)) = \Cor^G_H(a).b.
\]
That is, with respect to pairing on cohomology, the mappings \( \Cor^H_G, \Res^G_H \) are adjoint.

**Proof.** By theorem 2.14, it is enough check the equality in dimension zero, which is easy. \( \square \)

Let \( \tau : G' \to G \) be a homomorphism between profinite groups; \( A, B \in C_G \) and \( A', B' \in C_{G'} \) with morphisms of \( G' \) modules \( \alpha : A \to A' \) and \( \beta : B \to B' \). Then we have cup products given by tensor products (as pairings) and the following commutative diagram (One can check it easily):

\[
\begin{array}{ccc}
H^\bullet(G; A) \times H^\bullet(G; B) & \longrightarrow & H^\bullet(G; A \otimes B) \\
\downarrow_{(\tau, \alpha)^* \times (\tau, \beta)^*} & & \downarrow_{(\tau, \alpha \otimes \beta)^*} \\
H^\bullet(G'; A') \times H^\bullet(G'; B') & \longrightarrow & H^\bullet(G'; A' \otimes B')
\end{array}
\]

And so we have:
Proposition 2.16. Let $G$ be a profinite group and $H \leq G$ be a closed subgroup. Let $A, B \in C_G$ with the $G$--pairing $\theta : A \times B \to A \otimes B$. Then, for $a \in H^r(G; A)$ and $b \in H^s(G; B)$, one has

$$\text{Res}_H^G(ab) = \text{Res}_H^G(a) \text{Res}_H^G(b).$$

Proof. By the above commutative diagram, we have:

$$\text{Res}(ab) = (i, id_A \otimes id_B)^*(ab) = (i, id_A)^*(a)(i, id_B)^*(b) = \text{Res}(a) \text{Res}(b)$$

where $i : H \to G$ is the natural injection. \hfill $\square$

5. Spectral Sequences

In this section, we will define the machinery to compute (co)homology, namely spectral sequences, and show the existence of Hochschild-Serre spectral sequence as a particular case of Grothendick spectral sequence.

Let $K = (K^p, d)$ be a cochain complex with $p \geq 0$ and the differential $d$. A filtration $F$ on $K$ is an ordered family of subcomplexes

$$... \subseteq F^{p+1} \subseteq F^p \subseteq F^{p-1}...$$

with

$$dF^p K \subseteq F^p K.$$ We say that the filtration $F$ is bounded if for each $n$ there are integers $s \leq t$ such that $F^s K^n = K^n$ and $F^t K^n = 0$. The complex $K = (K^p, d)$ with its filtration is called filtered cochain complex. In this section, we will always assume that the filtration is bounded unless specified. Now, keeping the above notation, one defines its $(K^p, d, F)$'s ) associated graded complex

$$GrFK = GrK = \bigoplus_{p \geq 0} Gr^p K$$

where

$$Gr^p K = F^p K / F^{p+1} K$$

with the obvious differential. The filtration $F^p K$ on $K$ induces a filtration $F^p H^q(K)$ on the cohomology by

$$F^p H^q(K) = F^p Z^q / F^p B^q$$

where $Z^q$ is the cocycles of degree $q$ and $B^q$ is the set coboundaries of degree $q$. A spectral sequence is a sequence $\{E_r, d_r\}_{r \geq 0}$ of bigraded objects

$$E_r = \bigoplus_{p,q} E_r^{p,q}$$

together with differentials

$$d_r : E_r^{p,q} \to E_r^{p+r,q-r+1}$$
such that the cohomology of $E_r$ is $E_{r+1}$, that is
\[ H(E_r) = E_{r+1}. \]

In practice, one usually has $E_r = E_{r+1} = \ldots$ after some $r_0$. This limit object is denoted by $E_\infty$ and one says that the spectral sequence abuts to $E_\infty$ and denotes by $E_r \Rightarrow E_\infty$.

Due to Shatz, the central problem all this orgy of indices is meant to handle this: Given $K$ as above, compute $H^\bullet(K)$. Frequently, with relative ease, one can compute $H^\bullet(Gr(K))$.

The method of spectral sequences is an iterative procedure which passes from $H^\bullet(Gr(K))$ to $Gr(H^\bullet(K))$. This is weaker than finding $H^\bullet(K)$, but often ”just as good”. Hence, the whole machinery of spectral sequences is an analysis of the ”non-commutativity” of $Gr$ and $H^\bullet$.

**Proposition 2.17.** Let $FK$ be a filtered complex. Then there exits a spectral sequence $\{E_r\}_{r \geq 0}$ with
\[
E_0^{p,q} = F^pK^{p+q}/F^{p+1}K^{p+q}; E_1^{p,q} = H^{p+q}(Gr^p(K)); E_\infty^{p,q} = Gr^p(H^{p+q}(K)).
\]

**Proof.** See [La,p 815].

From our point of view, the application of proposition 2.17 is more important than its proof. It allows us to create a ”good” spectral sequence from a given filtration. The most important method of generating spectral sequences is the following:

**Theorem 2.18. (Grothendick Spectral Sequence)** Let $A, B$ and $C$ be abelian categories with enough injectives. Let $T : A \to B$ and $S : B \to C$ be covariant left exact functors such that if $I$ is injective in $A$ then $T(I)$ is $S$–acyclic, i.e $R^pS(T(I)) = 0$ for $p \geq 1$. Then for each $A \in A$ there is a spectral sequence $\{E_r(A)\}$ such that
\[ E_2^{p,q}(A) = R^pS(R^qT(A)) \]
and
\[ E_r^{p,q} \Rightarrow R^{p+q}(ST)(A). \]

**Proof.** See [La,p 821].

**Corollary 2.19. (Hochschild-Serre Spectral Sequence)** Let $G$ be a (any) group with a normal subgroup $N$. For each $G$–module $A$, there is a spectral sequence $\{E_r(A)\}$ with
\[ E_2^{p,q} = H^p(G/N; H^q(N; A)) \Rightarrow H^{p+q}(G; A). \]

**Proof.** Let’s take $S : G\text{-Mod} \to G/N\text{-Mod}$ defined by $S = Hom_N(\mathbb{Z}, -)$ and $T : G/N\text{-Mod} \to \text{Ab}$ be defined by $T = Hom_{G/N}(\mathbb{Z}, -)$. One can easily check that $T$ and $S$ satisfies the hypothesis of the theorem. Since $TS = Hom_G(\mathbb{Z}, -)$, the result is immediate.
Remark 2.20. In our case (in case $G$ is profinite), the existence of the Hochschild-Serre spectral sequence implies a continuous action of $G/N$ on $H^q(N;A)$ for each $q$. This is given by choosing $\alpha \in H^q(N;A)$, $\bar{\tau} \in G/N$ and representing them by a cocycle $f(\sigma_1, \ldots, \sigma_q)$ and an element $\tau \in G$, then by setting

$$f^\tau(\sigma_1, \ldots, \sigma_q) =\tau f(\tau^{-1} \sigma_1 \tau, \ldots, \tau^{-1} \sigma_q \tau).$$

One checks that $f^\tau$ is a cocycle whose class is independent of the representatives and moreover that $N$ acts trivially on the cohomology classes and that the induced $G/N$ action is continuous The exact sequence of terms of low degree yields an exact sequence, called inflation-restriction sequence,

$$0 \longrightarrow H^1(G/N; A^N) \xrightarrow{\text{inf}} H^1(G; A) \xrightarrow{\text{Res}} H^1(N; A) \xrightarrow{G/N} H^2(G/N; A^N) \xrightarrow{\text{inf}} H^2(G; A).$$
Chapter 3

Cohomological Dimension

In this chapter, we will define the cohomological dimension of a group and prove basic properties. And, we will also study the case cohomological dimension one. In what follows, $G$ will always stand for a profinite group unless specified.

1. Basic Properties

For a given group $G$ and prime number $p$, one defines ($p$-)cohomological dimension (resp. $cd_pG$) $cdG$ of $G$ as the minimum number $n$ such that (resp. $H^r(G; A, p) = 0$) $H^r(G; A) = 0$ for all $r > n$ and for all torsion $G$–modules $A$; and one defines ($p$-)strict cohomological dimension (resp. $scd_p G$) $scdG$ of $G$ as the minimum number $n$ such that (resp. $H^r(G; A, p) = 0$) $H^r(G; A) = 0$ for all $r > n$ and for all $G$–modules $A$ where $H^r(G; A, p)$ denotes the $p$–th primary component of $H^r(G; A)$.

It obviously follows from the definitions that

i. $cdG = \sup_p \{cd_p G\}$ and $scdG = \sup_p \{scd_p G\}$;

ii. $cdG \leq scdG$ and $cd_p G \leq scd_p G$ for all prime $p$.

Proposition 3.1. For every prime $p$ we have

$$cd_p G \leq scd_p G \leq cd_p G + 1$$

and consequently,

$$cdG \leq scdG \leq cdG + 1.$$ 

Proof. Let $p$ be a prime. We only need to prove that $scd_p \leq cd_p G + 1$. Let $A \in C_G$ and $tA$ be its torsion part. Then, one has the s.e.s in $C_G$ $0 \to tA \to A \to A/tA \to 0$ which induces the long exact sequence in cohomology

$$\cdots \to H^r(G; tA) \to H^r(G; A) \to H^r(G; A/tA) \to .$$
Let $cd_pG = n$. Since $H^r(G; tA, p) = 0$ for all $r > n$, it suffices to prove that $H^r(G; A/tA, p) = 0$ for all $r > n + 1$. Set $A/tA = B$. As $B$ is torsion free, we have the short exact sequence

$$0 \rightarrow B \xrightarrow{p} B \rightarrow B/pB \rightarrow 0$$

which induces the long exact sequence

$$\rightarrow H^{r-1}(G; B/pB) \rightarrow H^r(G; B) \xrightarrow{p} H^r(G; B) \rightarrow$$

Since $B/pB$ is a torsion module, $H^{r-1}(G; B/pB) = 0$ for all $r > n + 1$ and so the map $H^r(G; B, p) \xrightarrow{p} H^r(G; B, p)$ multiplication by $p$ is a monomorphism. Hence, as $H^r(G; B)$ is torsion, $H^r(G; B, p) = 0$ for all $r > n + 1$.

**Proposition 3.2.** Let $p$ be a prime, $A \in C_G$ be $p$–divisible and suppose $cd_pG = n$. Then $H^n(G; A)$ is $p$–divisible and $H^{n+1}(G; A) = 0$. If we omit $p$–divisibility of $A$, then the statement holds with $n$ replaced by $n + 1$.

**Proof.** We have the following short exact sequence

$$0 \rightarrow A_p \rightarrow A \xrightarrow{p} A \rightarrow 0$$

where $A_p = \{a \in A \mid pa = 0\}$ and the induced long exact sequence

$$H^n(G; A) \rightarrow H^n(G; A) \xrightarrow{p} H^{n+1}(G; A_p) = 0$$

which gives us $p$–divisibility of $H^n(G; A)$. And, the continuation of this sequence

$$0 = H^{n+1}(G; A_p) \rightarrow H^{n+1}(G; A) \xrightarrow{p} H^{n+1}(G; A)$$

gives us the triviality of $H^{n+1}(G; A, p)$. One considers the short exact sequence

$$0 \rightarrow A_p \rightarrow A \xrightarrow{p} A/pA \rightarrow 0,$$

uses proposition 3.1 and gets the rest of the proposition. \(\square\)

**Corollary 3.3.** If $cdG \leq n$ and $A \in C_G$ is divisible then $H^r(G; A) = 0$ for all $r > n$.

**Corollary 3.4.** If $cdG = n$ then $H^{n+1}(G; A)$ is divisible for any $A \in C_G$.

**Proposition 3.5.** Let $S$ be a closed subgroup of $G$ and $p$ be a prime number. Then, $cd_pS \leq cd_pG$ and $scd_pS \leq scd_pG$. We have the equality if $(G : S)$ is prime to $p$. In particular, $(s)cd_pG = (s)cd_pG_p = (s)cdG_p$ where $G_p$ is a Sylow $p$–subgroup of $G$.

**Proof.** First claims follow from theorem 2.12. Now, suppose that $(G : S)$ is prime to $p$. By proposition 2.8, $\text{Res} \circ \text{Cor} = (G : S)$ and so the map

$$\text{Res} : H^r(G; A, p) \rightarrow H^r(S; A, p)$$

is injective where $A \in C_G$ is torsion (resp. any module). This completes the proof. \(\square\)
Lemma 3.6. Let $G$ be a profinite $p$–group and $E$ be a finite simple $G$–module of $p$–power. Then $E = \mathbb{Z}/p\mathbb{Z}$ with trivial action.

Proof. Class equation implies that $E^G$ is a nontrivial submodule of $E$, which means that $E = E^G$ and $G$ acts trivially on $E$. The rest is a first-year-algebra problem. □

Lemma 3.7. Let $p$ be a prime and $n \in \mathbb{N} \cup \{\infty\}$ be the minimum number satisfying $H^{n+1}(G; E) = 0$ for all finite simple $G$–module $E$ of $p$–power order. Then $cd_p G = n$.

Proof. Trivially, $n \leq cd_p G$. Let $A \in C_G$ be a torsion $G$–module. Since $A = \varinjlim A_\alpha$ where the limit runs over finitely generated $G$–modules $A_\alpha$'s and the cohomology commutes with the direct limit, we may assume that $A$ is finite. We may also assume that $A$ is finite of $p$–power order as $H^r(G; A, p) = H^r(G; A_p)$ where $A_p$ stands for the $p$–part of $A$. Now, for $A$ we have the composition series

$$A > A_1 > \cdots > A_m = 0$$

whose factors are simple $G$–modules of $p$–power order. Induction on the length of the series and the cohomology sequence (and our assumption) imply that $H^{n+1}(G; A) = 0$. Hence, we are done. □

Theorem 3.8. Let $G$ be any profinite group, $p$ be a prime and $n \in \mathbb{N}$. Then, the followings are equivalent:

i. $cd_p G \leq n$
ii. $H^{n+1}(G; \mathbb{Z}/p\mathbb{Z}) = 0$.

Proof. Of course, the problem is that $ii \Rightarrow i$. By proposition 3.5, we may assume that $G$ is profinite $p$–group. Then, it immediately follows from lemma 3.6 and lemma 3.7. □

2. Cohomological Dimension of Subgroups

Proposition 3.9. (Serre) Let $cd_p G = n < \infty$. Then, $scd_p = n$ if and only if $H^{n+1}(S; \mathbb{Z}, p) = 0$ for every open subgroup $S$ of $G$.

Proof. The implication ($\Rightarrow$) is trivial. Let $A \in C_G$. Since $A = \varinjlim A_\alpha$ where $A_\alpha$'s are finitely generated, we may assume that $A$ is finitely generated, i.e $B = \langle b_1, ..., b_m \rangle$. Then, there exists an open subgroup $S$ of $G$ with the property that $S$ acts on $A$ trivially. So one can consider the short exact sequence of $\mathbb{Z}$ modules

$$0 \longrightarrow K \longrightarrow \mathbb{Z}^m \longrightarrow A \longrightarrow 0$$

in which $K$ is a torsion module and $m = rank_{\mathbb{Z}}(A)$. By applying cohomology over $S$, one gets

$$\cdots \longrightarrow H^{n+1}(S; K, p) \longrightarrow H^{n+1}(S; \mathbb{Z}, p)^m \longrightarrow H^{n+1}(S; A, p) \longrightarrow H^{n+2}(S; K, p) \longrightarrow$$

27
Since \( cd_p \leq n \), \( H^{n+1}(S; \mathbb{Z}, p) \xrightarrow{\sim} H^{n+1}(S; A, p) \) and, by hypothesis, we deduce that \( H^{n+1}(S; A, p) = 0 \). By theorem 2.12, we get

\[
H^{n+1}(G; M^S_S(A)) = 0.
\]

The norm map \( N : M^S_S(A) \to A \) defined by \( f \mapsto \sum_{\rho \in G/S} \rho f(\rho^{-1}) \) gives the short exact sequence

\[
0 \to \text{Ker}(N) \to M^S_S(A) \to A \to 0
\]

and this induces

\[
H^{n+1}(G; M^S_S(A), p) \to H^{n+1}(G; A, p) \to H^{n+2}(G; \text{Ker}(N), p) \to 0.
\]

Then, the fact that \( H^{n+1}(G; M^S_S(A)) = 0 \) and that \( scd_p G \leq cd_p G + 1 = n + 1 \) imply that \( H^{n+1}(G; A, p) = 0 \) and complete the proof.

**Proposition 3.10.** Let \( S \) be an open subgroup of \( G \) and suppose \( cd_p G = n < \infty \). Then \( cd_p S = cd_p G \).

**Proof.** By proposition 3.5, we may assume that \( G \) is a profinite \( p \)-group. By proposition 3.5 and theorem 3.8, it suffices to prove that \( H^n(S; \mathbb{Z}/p\mathbb{Z}) \neq 0 \). Since \( G \) acts trivially on \( \mathbb{Z}/p\mathbb{Z} \), \( A := M^S_S(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^{(G:S)} \) and so, by theorem 2.12, it is enough to prove that \( H^n(G; A) \neq 0 \). The short exact sequence

\[
0 \to A_1 \to A \to \mathbb{Z}/p\mathbb{Z} \to 0
\]

which induces the long exact sequence in cohomology

\[
\to H^n(G; A) \to H^n(G; \mathbb{Z}/p\mathbb{Z}) \to H^{n+1}(G; A_1) \to
\]

Now, \( H^{n+1}(G; A_1) = 0 \) as \( cd_p G = n \) and \( H^n(G; \mathbb{Z}/p\mathbb{Z}) \neq 0 \) by theorem 3.8. Hence, \( H^n(G; A) \neq 0 \) and we are done.

**Corollary 3.11.** If \( G \) is a \( p \)-group of cohomological dimension \( n < \infty \) then \( H^n(G; A) \neq 0 \) for any \( G \)-module of \( p \)-power order.

**Corollary 3.12.** If \( 0 < cd_p G < \infty \) then \( p^\infty \) divides \( |G| \). In particular, a finite group with nonzero Sylow \( p \)-subgroup has infinite \( p \)-cohomological dimension.

**Proof.** Since \( cd_p G = cd_p G_p \), we may assume that \( G \) is a profinite \( p \)-group. Assume not! Then, \( G \) is a finite group and \( \{1\} \) is an open subgroup. By proposition 3.10, \( cd_p G = cd_p \{1\} = 0 \). A contradiction.

This corollary shows that cohomological dimension is a trivial invariant for finite groups. Here, we have a very useful result:

**Theorem 3.13.** (Tower Theorem) Let \( N \) be a closed subgroup of \( G \). Then,

\[
\text{cd}_p G \leq \text{cd}_p G/N + \text{cd}_p N.
\]

**Proof.** See [Sh, p 61].
3. The Case Cohomological Dimension 1

First of all:

**Proposition 3.14.** For a given prime \( p \), one has

\[
\text{cd}_p G = 0 \text{ if and only if } G_p = 1
\]

and consequently,

\[
\text{cd} G = 0 \text{ if and only if } G = 1.
\]

**Proof.** We only need to prove that \( G_p = 1 \) when \( \text{cd}_p G = 0 \). Assume not! Let \( G \) be our counterexample. As usual, we may assume that \( G \) is a profinite \( p \)-group. Let \( S \) be an open subgroup with a nontrivial homomorphism \( \alpha : G/S \to \mathbb{Z}/p\mathbb{Z} \). Then, one can show that \([\alpha] \in H^1(G/S; \mathbb{Z}/p\mathbb{Z})\) and \([\alpha] \neq 0\). By first part of inflation-restriction sequence

\[
0 \longrightarrow H^1(G/S; \mathbb{Z}/p\mathbb{Z}) \overset{\text{inf}}{\longrightarrow} H^1(G; \mathbb{Z}/p\mathbb{Z})
\]

one concludes that \( H^1(G; \mathbb{Z}/p\mathbb{Z}) \neq 0 \) and gets a contradiction. \( \square \)

The proposition above is one of the reasons to study the case dimension is one. Another reason is that there are natural examples of groups which have dimension 1, for instance \( \hat{\mathbb{Z}} = \lim \leftarrow \mathbb{Z}/n\mathbb{Z} \). We will find an explicit criteria for such groups and we will prove that \( \text{cd} \hat{\mathbb{Z}} = 1 \).

An *extension* of \( G \) by an abelian group \( A \) for us is a short exact sequence

\[
0 \rightarrow A \rightarrow E \rightarrow G \rightarrow 0
\]

in which \( E \) is a topological group and the maps are continuous. Notice that \( E \) acts on \( A \) via inner automorphisms

\[
\sigma : a \mapsto \sigma a \sigma^{-1}
\]

In fact, this action is a \( G = E/A \)-action and it is continuous. Thus, \( A \in C_G \). Here, we have a classical result, for the proof see [Sh,p 63].

**Theorem 3.15.** Let \( A \) be an abelian group. Then isomorphism classes of extensions of \( G \) by \( A \) are in 1-1 correspondence with the elements of \( H^2(G; A) \).

**Theorem 3.16.** Let \( p \) be a prime. Then, TFAE:

i. \( \text{cd}_p G \leq 1 \)

ii. Every extension of \( G \) by a finite abelian \( p \)-group splits

iii. Every extension of \( G \) by a profinite \( p \)-group splits
Proof. The equivalence of (i) and (ii) follows from theorem 3.15 and theorem 3.8. (iii) clearly implies (ii). So, assume (ii). Let \( A \rightarrow E \xrightarrow{p} G \rightarrow 0 \) be an extension in which \( A \) is a profinite \( p \)-group. Define the Zorn’s set \( Z \) as the set of couples \( (A_\alpha, \iota_\alpha) \) in which \( A_\alpha \)'s are closed in \( A \) and normal subgroups of \( E \) with \( \iota_\alpha : G \rightarrow E/A_\alpha \) satisfying \( \tilde{p}_\iota\alpha = id \) where \( \tilde{p} \) is the map induced by \( p \). Clearly, \( (A, \tilde{p}^{-1}) \in Z \) and \( Z \) is not empty. By defining order in the usual way, one has an inductive poset and, by Zorn’s Lemma, \( Z \) has a maximal element, say \( (A_0, \iota_0) \). It is enough to prove that \( A_0 = 0 \). Note that \( E/A_0 \) acts on \( H^1(A_0; \mathbb{Z}/p\mathbb{Z}) \) continuously as: \( \varphi^\alpha(\tau) = \sigma \varphi(\sigma \tau \sigma^{-1}) = \varphi(\sigma \tau \sigma^{-1}) \). Continuity of the action implies that there are finitely many conjugacy classes, call the representatives as \( \varphi_1, ..., \varphi_n \). Notice that \( H^1(A_0; \mathbb{Z}/p\mathbb{Z}) \neq 0 \) because one can find a nontrivial morphism \( \varphi : A_0 \rightarrow \mathbb{Z}/p\mathbb{Z} \). Now, let’s set \( \hat{A} = \bigcap \ker(\varphi_i) \). Then it is clear that \( \hat{A} \) is normal in \( E \) and \( (A_0 : \hat{A}) < \infty \). The following short exact sequence

\[
0 \rightarrow A_0/\hat{A} \rightarrow E/\hat{A} \rightarrow E/A_0 \rightarrow 0
\]

and our assumption allows us to define \( \iota \) which satisfies \( (A_0, \iota_0) < (\hat{A}, \iota) \). A contradiction. 

Let \( G = \langle x_\alpha \rangle \) be any group and \( \Lambda = \{ S \triangleleft G \mid (G : S) < \infty \text{ and } S \text{ contains almost all } x_\alpha \} \). Then, one defines and denotes the profinite closure of \( G \) by \( \hat{G} = \underleftarrow{\lim}_\Lambda G/S \). For a prime \( p \), one considers the subset \( \Lambda_p \) of \( \Lambda \) containing the subgroups \( S \) with the property that \( (G : S) = p^n \) for some \( n \in \mathbb{N} \). Then, one defines and denotes the \( p \)-profinite closure of \( G \) by \( \hat{G}_p = \underleftarrow{\lim}_{\Lambda_p} G/S \). \((p-)Profinite closure of the free group \( F(X) \) on a set \( X \) is called free profinite \((p-)group on \( X \). If \( X \) contains only one element, then \( F(X) = \mathbb{Z} \) and \( \hat{F_p}(X) = \mathbb{Z}_p = p^{-1} \) adic integers.

**Proposition 3.17.** Let \( X \) be a set and \( F_p(X) \) be the free profinite \( p \)-group on \( X \). Then, the homomorphisms of \( F_p(X) \) into a discrete \( p \)-group \( A \) in 1-1 correspondence with set theoretic maps \( X \rightarrow A \) which send almost all \( x \in X \) to 0 in \( A \). Consequently, \( \cd_p F_p(X) \leq 1 \).

**Proof.** Easy. 

**Corollary 3.18.** \( H^1(F_p(X); \mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^{\vert X \vert} \). Consequently, \( \cd_p F_p(X) = \cd(F_p(X)) = 1 \).

**Corollary 3.19.** \( F_p(X) \cong F_p(Y) \) if and only if \( \vert X \vert = \vert Y \vert \).

**Corollary 3.20.** \( \cd \mathbb{Z}_p = \cd_p \mathbb{Z}_p = 1 \) and \( \cd(\hat{\mathbb{Z}}) = 1 \) where \( \hat{\mathbb{Z}} = \underleftarrow{\lim}_n \mathbb{Z}/n\mathbb{Z} \).
Chapter 4

Galois Cohomology: An Application

Many deep results, especially about Brauer groups, can be established cohomological machinery. In this chapter, we will present the most basic one, Hilbert’s theorem 90, with some important applications.

We will denote $H^r(Gal(K/k); A)$ by $H^r(K/k; A)$ for a Galois extension $K/k$ and a discrete $Gal(K/k)$-module $A$.

1. Hilbert’s Theorem 90

Theorem 4.1. (Hilbert’s Theorem 90) Let $K/k$ be a Galois extension. Then, for $r > 0$

$H^r(K/k; K^+) = 0$

and

$H^1(K/k; K^*) = 0$.

Proof. Since $H^r(K/k; K^+) = \varinjlim H^r(L/k; L^+)$ where the limit runs over the finite Galois extensions $L/k$, we may assume that $[K : k] < \infty$. Let’s denote $G(K/k) = G$. By the normal basis theorem [La, p312], there exists a $x \in K$ such that the set $\{\sigma x \mid \sigma \in G\}$ forms a basis of $K^+$ over $k$. If $f \in M^G_{\{1\}}(k^+)$, then the map

$T : M^G_{\{1\}}(k^+) \rightarrow K^+$

defined by

$T(f) = \sum_{\sigma \in G} f(\sigma^{-1}) \sigma x$

is a monomorphism. Noting that the action of $G$ on $M^G_{\{1\}}(k^+)$ is defined by $(\lambda f)(x) := f(x\lambda)$, it is trivial to verify that $T$ is a $G$–module monomorphism, and it is, in fact, an isomorphism of $G$–modules since $G$ is finite and so $f(\sigma^{-1})$ can take any value in $k$ for any $\sigma \in G$. Hence, we have $M^G_{\{1\}}(k^+) \cong K^+$ and, for $r > 0$

$H^r(K/k; K^+) = H^r(K/k; M^G_{\{1\}}(k^+)) \cong H^r(1; k^+) = 0$.
Now, in order to prove our second claim, let \( f : G \to K^* \) be a continuous map representing the cohomology class \( u \in H^1(K/k; K^*) \). We may continue to assume that \([K : k] < \infty\). For \( x \in K^* \), define

\[
c(x) = \sum_{\sigma \in G} f(\sigma) \sigma x.
\]

By the normal basis theorem, there exists a \( \xi \in K^* \) with \( c(\xi) \neq 0 \). Now, we have

\[
\sigma c(\xi) = \sigma \sum_{\tau \in G} f(\tau) \tau(\xi) = \sum_{\tau \in G} \sigma f(\tau) \sigma \tau(\xi)
\]

and by the cocycle condition,

\[
= \sum_{\tau \in G} \frac{f(\sigma \tau)}{f(\sigma)} (\sigma \tau)(\xi) = \frac{1}{f(\sigma)} c(\xi).
\]

Hence, for \( c = c(\xi)^{-1} \), \( f(\sigma) = \sigma c / c \) i.e \( f \) is a coboundary and we are done. \( \square \)

2. Some Applications: Cyclic Extensions

A finite Galois extension is said to be cyclic if its Galois group is cyclic. We can determine if the extension is cyclic by using Hilbert’s theorem 90. In this section, we will present two results.

**Theorem 4.2.** Let \( n > 0 \) be an integer which is prime to \( \text{char}(k) \). Assume that there is a primitive \( n \)-th root of unity in \( k \).

i. Let \( K/k \) be a cyclic extension of degree \( n \). Then there exists \( \alpha \in K \) such that \( K = k(\alpha) \) and \( \alpha^n - a = 0 \) for some \( a \in k \).

ii. Conversely, if there exists \( \alpha \in K \) with \( \alpha^n = a \in k \) then \( K(\alpha) \) is cyclic over \( k \) of degree \( d \) and \( \alpha^d \in k \).

**Proof.** Let \( G = \text{Gal}(K/k) \), \( \xi \in k \) be the \( n \)-th root of unity and \( \sigma \in G \) be a generator. Let \( f : G \to K^* \) be a continuous map with \( f(\sigma^r) = \xi^r \). One can see that \( f \) is a cocycle. By Hilbert’s theorem 90, there exists \( \alpha \in K^* \) with \( f(\sigma^r) = \sigma^r(\alpha) / \alpha \) for all \( r = 1, ..., n \), and so \( \sigma^r(\alpha) = \xi^r \alpha \). Since \( \xi \) is a primitive \( n \)-th root of unity in \( k \), the elements \( \sigma^r(\alpha) = \xi^r \alpha \)‘s are distinct and \([k(\alpha) : k] \geq n\); Thus \( k(\alpha) = K \). And, we have

\[
\sigma(\alpha^n) = \sigma(\alpha)^n = (\xi \alpha)^n = \alpha^n.
\]

As all the elements of \( G \) fixes \( \alpha^n \), \( \alpha^n \in k \) and the first claim is proven.

Let \( \xi \in k \) be again our primitive \( n \)-th root of unity. Then, the elements \( \xi^r \alpha \)’s are the roots of the polynomial \( x^n - a \). This implies that \( \alpha^d \in k \) where \( d = [k(\alpha) : k] \). And, clearly, \( \sigma \in G \) defined by \( \sigma(\alpha) = \xi \alpha \) generates \( G \). Hence, all is proven. \( \square \)
Theorem 4.3. (Artin-Schreier) Let \( k \) be a field of characteristic \( p \).

i. Let \( K/k \) be a cyclic Galois extension of degree \( p \) with the Galois group \( G \). Then there exists \( \alpha \in K \) such that \( K = k(\alpha) \) and \( \alpha \) satisfies the equation \( x^p - x - a = 0 \) with some \( a \in k \).

ii. Conversely, given \( a \in k \), the polynomial \( f(x) = x^p - x - a \) either has one root in \( k \), in which case all its roots are in \( k \), or it is irreducible. In this latter case, is \( \alpha \) is a root then \( k(\alpha) \) is cyclic of degree \( p \) over \( k \).

Proof. Let \( \sigma \) be a generator of \( G \). Clearly, the automatically-continuous map \( f : G \to K^+ \) defined by \( f(\sigma^r) = r \) is a cocyle. By Hilbert’s theorem 90, there exists \( \alpha \in K \) with \( \sigma^r(\alpha) - \alpha = f(\sigma^r) = r \) for all \( r = 0, \ldots, p - 1 \) or, in other words, \( \sigma^r(\alpha) = \alpha + r \). Therefore, \( \alpha \) has \( p \) distinct conjugates and \( [k(\alpha) : k] \geq p \); Thus \( K = k(\alpha) \). Noting that

\[
\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha,
\]

we get that \( \alpha^p - \alpha \) is fixed by \( G \) and lies in \( k \). Hence, by taking \( a = \alpha^p - \alpha \), we have proved the first claim.

If \( \alpha \) is a root of \( f \) then \( (\alpha + i)'s \) are all the roots of \( f \). Then, it follows from a simple analysis that \( f \) is irreducible when \( \alpha \) (or equivalently \( f \) has no root) is not in \( k \). As the roots of \( f \) are distinct and \( k(\alpha) \) is the splitting field of \( f \), \( k(\alpha)/k \) is a Galois extension. Since \( \alpha + 1 \) is a root of \( f \), there exists a \( \delta \in G \) with \( \delta(\alpha) = \alpha + 1 \). Hence, \( \delta^r(\alpha) = \alpha + i \) and \( \delta \) generates \( G \), and we are done. \( \square \)

3. Some Applications: Brauer Groups

The group \( H^2(k; k^*_s) \) where \( k_s \) is the separable closure of \( k \) is especially important, it is called Brauer Group of \( k \) and denoted by \( Br(k) \), after Richard Brauer who first studied in a different guise. This group is a subtle arithmetic invariant of the field \( k \). The group \( H^2(K/k; K^*_s) \) will be denoted by \( Br(K/k) \) and called the relative Brauer group of \( K/k \). We have important corollaries dealing with the Brauer group.

Theorem 4.4. Let \( k \subset K \subset L \) be Galois extensions. Then the sequence

\[
0 \rightarrow Br(K/k) \xrightarrow{\text{inf}} Br(L/k) \xrightarrow{\text{Res}} Br(L/K) \xrightarrow{K/k} H^3(K/k; K^*_s) \rightarrow H^3(L/k; L^*_s)
\]

is exact. In particular, the inflation maps \( Br(K/k) \rightarrow Br(k) \) are always injective; so the Brauer group of \( k \) is the union of all the relative Brauer groups of extensions \( K/k \) for which \( K/k \) is finite Galois.

Proof. This is the inflation-Restriction sequence in remark 2.20 induced by Hochschild-Serre spectral sequence

\[
H^p(K/k; H^q(L/K; L^*_s)) \Rightarrow H^{p+q}(L/k; L^*_s)
\]

because \( H^1(L/K; L^*_s) = 0 \) by Hilbert’s theorem 90. \( \square \)
We have also the following useful fact, for proof see [Sh,p96].

**Theorem 4.5.** Let $k$ be a field of characteristic $p > 0$. Then $cd_p k \leq 1$, and $Br(k)$ is divisible by $p$. 
References


