Pontificia Universidad Javeriana

Carrera de Matemáticas

Facultad de Ciencias

An Introduction to Local Class Field Theory: Cohomology

Author:
Juan Sebastián Gaitán Escarpeta

Advisor:
Jorge Andrés Plazas Vargas

July 3, 2021

"*Sharing knowledge is the most fundamental act of friendship. Because it is a way you can give something without loosing something*"

Richard Stallman.

Acknowledgments

As almost all academic texts, this one has been the product not only of my work but also the contribution of numerous people without whom this would have been impossible.

I owe a very special thanks to my parents for being with me on every step of my personal and academic education, their life lessons have been invaluable through this process. I am also grateful to Daniela for her infinite patience and understanding. I would also like to acknowledge the strong support of my professors Jorge Andrés Plazas Vargas, Mario Andrés Velásquez Mendez and Germán Combariza Gonzalez who have been key in the development of this work. A final word of thanks goes to my friends Steven, Thomas, Felipe and David, without whom, this work would have been done much quicker.

Introduction

Cohomology theory is a powerful tool initially proposed by Hurewicz in a topological context, and it has proven to be quite useful in many different contexts of mathematics. In this work, we will discuss how cohomology theory provides us a way to attack the problem of computing Galois groups of local field extensions through class field theory.

Class field theory has been a very important topic in modern algebra and number theory, started by Gauss with his proof the quadratic reciprocity and developed by some of the greatest mathematicians like Noether, who, together with Artin laid the foundations of modern algebra, Hilbert, who conjectured the fundamental theorems of abelian class field theory that were later proven by Takagi, and in more recent times, John Tate, Jürgen Neukirch and Iwasawa, whose advancements in mathematics have been essential to the development of class field theory.

The goal of this work is to provide a general idea of the motivations and fundamental concepts of local class field theory and state some of its main results.

Contents

Chapter 1

Background In Algebraic Number Theory

In this chapter we will introduce some language, and state some theorems that will be usefull in the folowing chapters. All proofs that are not included in this chapter, can be found in [7], chapter 3.

1.1 Preliminary Notions

Discrete valuation rings

Definition 1.1. A *discrete valuation ring* is an integral domain A such that

- A is Noetherian,
- A is integrally closed, and
- A has exactly one nonzero prime ideal.

△

Definition 1.2. A *Dedekind domain* is an integral domain such that

- A is Noetherian,
- A is integrally closed, and
- every nonzero prime ideal is maximal.

△

From the above definitions, one can prove that an integral domain is a discrete valuation ring if and only if it is a local Dedekind domain. Now we will justify the name *discrete valuation ring*.

Definition 1.3. A *discrete valuation* on a field K is a nontrivial group homomorphism $v : K^\times \to \mathbb{Z}$ such that $v(a+b) \geq \min(v(a), v(b))$. △

Proposition 1.4. *Let v be a discrete valuation on K. Then the set*

$$A := \{a \in K \mid v(a) \geq 0\}$$

is a discrete valuation ring with maximal ideal

$$\mathfrak{m} := \{a \in K \mid v(a) > 0\}.$$

If $v(K^\times) = m\mathbb{Z}$, then $\mathfrak{m}$ is generated by every element π such that $v(\pi) = m$.

Example 1.5. Let $p \in \mathbb{N}$ be a prime number, define a function $v_p : \mathbb{Z}^\times \to \mathbb{Z}$ as follows:

$$v_p(n) = \max\{e \in \mathbb{Z} \mid p^e | n\}$$

Note that for each pair of $n, m \in \mathbb{Z}^\times$, one has $v_p(n \cdot m) = v_p(n) + v_p(m)$. The functions v_p can be extended to $\mathbb{Q}^\times$ defining:

$$v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b)$$

for each $a, b \in \mathbb{Z}^\times$. The reader can check that this is in fact a discrete valuation over $\mathbb{Q}$, hence the rings $\mathbb{Z}_{(p)}$ (the localization of $\mathbb{Z}$ at p, not to be confused with $\mathbb{Z}/p\mathbb{Z}$) are discrete valuation rings. ◇

Lattices

Definition 1.6. Let V be a finite dimensional vector space over $\mathbb{R}$. A *lattice* Λ in V is the free abelian group generated by some linearly independent elements of V. △

Proposition 1.7. *Let V be a finite dimensional vector space over $\mathbb{R}$. A subgroup Λ of V is discrete if and only if is a lattice.*

1.2 Prime factorization of Ideals

Lemma 1.8. *Let A be a ring, every ideal $\mathfrak{a}$ in A contains a product of nonzero prime ideals.*

Proof. We procced by contradiction, so let $\mathfrak{a}$ be a maximal couterexample of the statement. The ideal $\mathfrak{a}$ itself can not be prime, so there are elements x and y such that $xy \in \mathfrak{a}$ but $x \notin \mathfrak{a}$ and $y \notin \mathfrak{a}$. Therefore, the ideals $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ strictly contain $\mathfrak{a}$ but their product is contained in $\mathfrak{a}$. As $\mathfrak{a}$ is a maximal counterexample, both $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ contain a product of prime ideals, so $\mathfrak{a}$ also does. □

Lemma 1.9. *Let $\mathfrak{p}$ be a maximal ideal of an integral domain A, and define $\mathfrak{q} \coloneqq \mathfrak{p}A_{\mathfrak{p}}$. Then the map:*

$$\begin{aligned} A/\mathfrak{p}^m &\to A_{\mathfrak{p}}/\mathfrak{q}^m \\ a + \mathfrak{p}^m &\mapsto a + \mathfrak{q}^m \end{aligned} \tag{1.10}$$

is an isomorphism for all $m \in \mathbb{N}$.

Theorem 1.11. *Let A be a Dedekind domain. Every proper nonzero ideal of A can be written in the form*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n},$$

with $\mathfrak{p}_i$ prime ideals of A.

Proof. As in 1.8, the ideal $\mathfrak{a}$ contains an ideal $\mathfrak{b} \subseteq \mathfrak{a}$ such that

$$\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$$

and we may choose the $\mathfrak{p}_i$ distinct. Then

$$A/\mathfrak{b} \cong A/\mathfrak{p}_1^{r_1} \times \cdots \times A/\mathfrak{p}_m^{r_m} \cong A_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times \cdots \times A_{\mathfrak{p}_n}/\mathfrak{q}_m^{r_m},$$

the first isomorphism is given by the Chinese remainder theorem and the second one is given by 1.9. Under this isomorphism, $\mathfrak{a}/\mathfrak{b}$ corresponds to $\mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \cdots \times \mathfrak{q}_m^{s_m}/\mathfrak{q}_m^{r_m}$ for some $s_i \leq r_i$ because the rings A_{p_i} are discrete valuation rings. As this ideal also corresponds to $\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ then $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ in $A/\mathfrak{b}$ but as both of these ideals contain $\mathfrak{b}$, then $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ in A.

To complete the proof, we still have to prove the uniqueness of this factorization. Suppose that there are two factorizations of $\mathfrak{a}$, after adding factors with 0 exponent we may suppose that the same prime ideals occur in both factorizations. So following the notation of the proof:

$$\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} = \mathfrak{a} = \mathfrak{p}_1^{t_1} \cdots \mathfrak{p}_m^{t_m},$$

and following the proof,

$$\mathfrak{q}_i^{s_i} = \mathfrak{a} A_{p_i} = \mathfrak{q}_i^{t_i}$$

where $\mathfrak{q}_i$ is the maximal ideal of $A_{\mathfrak{p}_i}$. This implies $s_i = t_i$ for all i. □

Corollary 1.12. *Let A be a Dedekind domain and $\mathfrak{a}$,$\mathfrak{b} \subseteq A$ be ideals, then $\mathfrak{a} \subset \mathfrak{b}$ if and only if $\mathfrak{a}A_{\mathfrak{p}} \subset \mathfrak{b}A_{\mathfrak{p}}$ for all nonzero prime ideals $\mathfrak{p} \subset A$.*

Proof. The 'if' part is obvius. For the 'only if', factor $\mathfrak{a}$ and $\mathfrak{b}$ (adding prime ideals with 0 exponent if necessary) as follows:

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}, \quad \mathfrak{b} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}, \quad r_i, s_i \geq 0.$$

Then $\mathfrak{a}A_{\mathfrak{p}_i} \subset \mathfrak{b}A_{\mathfrak{p}_i}$ if and only if $r_i \geq s_i$. □

Corollary 1.13. *Let A be an integral domain with finitely many prime ideals, then A is a Dedekind domain if and only if A is a principal ideal domain.*

Proof. If A is a Dedekind domain, by 1.11 it is sufficient to prove that the prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_m \subset A$ are principal. Let $x_1 \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$, by the Chinese remainder theorem, there is an element $x \in A$ such that

$$x \equiv x_1 \mod \mathfrak{p}_1^2, \quad x \equiv 1 \mod \mathfrak{p}_i, \quad i \neq 1.$$

The ideals $\mathfrak{p}_1$ and (x) generate the same ideal in $A_{\mathfrak{p}_i}$ and therefore they are equal in A by 1.12. □

Corollary 1.14. *Let $\mathfrak{b} \subseteq \mathfrak{a}$ be ideals in a Dedekind domain A. Then $\mathfrak{a} = \mathfrak{b} + (a)$ for some $a \in A$*

Proof. Using 1.11, let $\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$ and $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ with $r_i, s_j \geq 0$. As $\mathfrak{b} \subseteq \mathfrak{a}$, $s_i \leq r_i$ for all i. For each $1 \leq i \leq m$ choose x_i such that $x_i \in \mathfrak{p}_i^{s_i}$, $x_i \notin \mathfrak{p}_i^{s_i+1}$. By the Chinese Remainder Theorem, there is an $a \in A$ such that

$$a = x_i \mod \mathfrak{p}_i^{r_i}, \text{ for all } i.$$

Note that $\mathfrak{b} + (a) = a$ (look at the ideals they generate in $A_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p}$.

□

Let A be a Dedekind domain with field of fractions K, and B its integral closure in a finite separable extension L of K. A prime ideal $\mathfrak{p}$ of A is factored in B:

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \quad e_i > 0.$$

If each $e_i = 1$, then we say that $\mathfrak{p}$ is *not ramified* in B (or L). If some $e_i > 1$, we say that p is *ramified* and e_i is called the *ramification* index.

Example 1.15. Take the Gaussian rational numbers $\mathbb{Q}[i]$ as a field extension of $\mathbb{Q}$. The prime ideal $(2) \subset \mathbb{Z}$ is ramified in $\mathbb{Q}[i]$:

$$\mathbb{Z}[i](2) = (1-i)^2$$

with ramification index 2. ◇

Definition 1.16. With the above notation, L is said to be an *unramified extension* of K if evey prime ideal of A is not ramified in B. △

1.3 Local Fields

Definition 1.17. An *absolute value* on a field K is a function

$$\begin{aligned} |\cdot| : K &\to \mathbb{R} \\ x &\mapsto |x| \end{aligned} \tag{1.18}$$

such that

- $|x| \geq 0$ and $|x| = 0$ only if $x = 0$.
- $|xy| = |x||y|$,
- $|x + y| \leq |x| + |y|$ (triangle inequality).

If the stronger version of the triangle inequality $|x + y| \leq \max\{|x|, |y|\}$ holds, then $|\cdot|$ is called a *nonarchimedian absolute value*. △

Example 1.19. Define the function $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ as follows:

$$|q|_p = \begin{cases} p^{-v_p(q)} & \text{if } q \neq 0 \\ 0 & \text{if } q = 0, \end{cases}$$

where v_p is as defined in example 1.5. From the definition it follows that this function constitutes a nonarchimeidan absolute value on $\mathbb{Q}$. ◇

Proposition 1.20. *Let $|\cdot|$ be a nontrivial nonarchimedian absolute value and define $v(x) := -\log|x|$, for $x \neq 0$. Then $v : K^\times \to \mathbb{R}$ satisfies the following conditions*

- $v(xy) = v(x) + v(y)$,
- $v(x+y) \geq \min\{v(x), v(y)\}$,
- *if $v(K^\times)$ is discrete in $\mathbb{R}$, then v is a multiple of a discrete valuation $w : K^\times \twoheadrightarrow \mathbb{Z} \subset \mathbb{R}$.*

An absolute value $|\cdot|$ such that $|K^\times|$ is a discrete subgroup of $\mathbb{R}$. is called a *discrete* absolute value.

Proof. The first two statements are clear, for the last one, note that $v(K^\times)$ is a subgroup of $\mathbb{R}$, if it is a discrete subgroup, then it is a lattice by 1.7, which means that $v(K^\times) = \mathbb{Z}c$ for some $c \in \mathbb{R}$. Now, the function $w := c^{-1} \cdot v$ is a discrete valuation. □

Proposition 1.21. *Let $|\cdot|$ be a nonarchimedian absolute value, then*

- $A := \{a \in K \mid |a| \leq 1\}$ *is a subring of K, wih*
- $U := \{a \in K \mid |a| = 1\}$ *as its group of units, and*
- $\mathfrak{m} := \{a \in K \mid |a| < 1\}$ *its unique maximal ideal.*
- *The absolute value $|\cdot|$ is discrete if and only if $\mathfrak{m}$ is principal, in which case A is a discrete valuation ring.*

Proof. Combine 1.4 and 1.20. □

Definition 1.22. A *local field* is a field K with a nontrivial absolute value $|\cdot|$ such that K is locally compact with the topology induced by $|\cdot|$. Throughout this text, we will restrict to nonarchimedean local fields with a discrete absolute value. With the notation of 1.20, A is called the *ring of integers* of K and is denoted $\mathcal{O}_K$, U is called the group of units of K and is denoted U_K, $\mathfrak{m}$ is denoted $\mathfrak{m}_K$ and its generators are called prime elements of K. The *residue field* k is defined as $k := \mathcal{O}_K/\mathfrak{m}_K$. △

Example 1.23. The completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$ is a local field and its ring of integers is $\mathbb{Z}_{(p)}$. This completion is denoted $\mathbb{Q}_p$. ◇

Proposition 1.24. *Let $L : K$ be an unramified extension of a local field K, then L is unique up to K-isomorphism and* $\mathrm{Gal}(L : K)$ *is a cyclic group.*

Proposition 1.25. *Let $L : K$ be a finite unramified Galois extension with Galois group G, then the induced field extension of residue fields $l : k$ is also Galois and*

$$\mathrm{Gal}(L : K) \cong \mathrm{Gal}(l : k).$$

Chapter 2

Covering Spaces in Topology

In this chapter, we will start exploring the relation between the fundamental group of a path-connected topological space and the Galois group. This relation will be further explained in chapter 3.

2.1 Galois Correspondence for Covering Spaces

Definition 2.1. Let X be a topological space. A *space over* X is a topological space Y together with a continuous map $p : Y \to X$. A morphism between two spaces $p_i : Y_i \to X$ $(i = 1, 2)$ over X is given by a continuous map $f : Y_1 \to Y_2$ such that the diagram

$$\begin{array}{ccc} Y_1 & \xrightarrow{f} & Y_2 \\ & \searrow^{p_1} & \downarrow{\scriptstyle p_2} \\ & & X \end{array}$$

commute. An isomorphism of spaces over X is a morphism such that f is a homeomorphism of topological spaces.
A *covering space* (or just *covering* for short) is a space Y over X such that

- For each $x \in X$ there is an open neighborhood of x in X, V_x, such that $p^{-1}(V_x)$ can be decomposed as a disjoint union $\coprod U_i$ of open subsets.
- $p|_{U_i}$ is a homeomorphism onto V_x.

A covering space $p : Y \to X$ is often noted as $Y|X$. △

Example 2.2. The classic example of a covering space is given by the function $p : \mathbb{R} \to S^1$ such that $\theta \mapsto e^{i\theta}$, and it is used in the standard proof of $\pi_1(S^1) = \mathbb{Z}$. ◇

Note that for any given topological space X, and a discrete topological space I, $I \times X$ seen as a space over X with the natural projection is also a covering space of X. Such covering spaces are called trivial and we will prove that any covering space is locally trivial.

Lemma 2.3. *Let Y be a space over X with a projection $p : Y \to X$, then p is a covering space of X if and only if for each $x \in X$ there is an open neighborhood of x in X, V such that $p_{|p^{-1}(V)}$ is isomorphic as a space over V to a trivial cover.*

Proof. First, suppose that p is a covering space and let $x \in X$, using definition 2.1, $p^{-1}(V_x) = \coprod_{i\in I} U_i$, for some index set I, one can endow I with the discrete topology and define the function: $f : \coprod_{i\in I} U_i \to I \times V$ such that for $u_i \in U_i$, $f(u_i) = (i, p(u_i))$, which is also a homeomorphism and therefore one has an isomorphism of spaces over X.
Conversely, let $x \in X$, suppose there is an open neighborhood V of x in X such that $p_{|p^{-1}(V_x)}$ is isomorphic to a trivial cover, say $q : I \times X \to X$; therefore $p^{-1}(V)$ is homeomorphic to $I \times X$, let $\Phi : I \times V \to p^{-1}(V)$ be a homeomorphism. Let $i, j \in I$ with $i \neq j$, as Φ is a homeomorphism and $\{i\} \times V \cap \{j\} \times V = \varnothing$, one has $\Phi(\{i\} \times V) \cap \Phi(\{j\} \times V) = \varnothing$, and as Φ is surjective:

$$p^{-1}(V) = \coprod_{i\in I} \Phi(\{i\} \times V).$$

The set $\Phi(\{i\} \times V)$ is open for any $i \in I$ because the set $\{i\} \times V$ is open and Φ sends open sets into open sets, so the first condition of 2.1 checks out. To verify the second condition, note that $V \cong \{i\} \times V \overset{\Phi}{\cong} \Phi(\{i\} \times V)$. □

Lemma 2.4. *Let $p : Y \to X$. be a covering space, Z a connected topological space and $f, g : Z \to Y$ two continuous maps such that $p \circ f = p \circ g$. If there is a point $z \in Z$ with $f(z) = g(z)$ then $f = g$.*

Proof. Let $y = f(z)$, then there is a connected neighborhood V of $p(y)$ satisfying the definition 2.1. Let U_i be the component of $p^{-1}(V)$ which contains

y. Using the continuity of f and g and the fact that p is a local homeomorphism, there is an open set $W \subseteq Z$ with $W = f^{-1}(U_i) = g^{-1}(U_i)$ and using the fact that $p \circ f = p \circ g$ and $p|_{U_i}$ is a homeomorphhism onto V we have $f|_W = g|_W$.
Now, suppose there is $z' \in Z$ with $f(z') \neq g(z')$ then there is an open neighborhood V of $p \circ f(z') = p \circ g(z')$ satisfying the definition 2.1. Let U_f be the component of $p^{-1}(V)$ which contains $f(z)$ and U_g the component of $p^{-1}(V)$ which contains $g(z)$. Using once again the continuity of f and g we conclude that $f^{-1}(U_f)$ and $g^{-1}(U_g)$ are open sets of Z with $z' \in f^{-1}(U_f) \cap g^{-1}(U_g) \neq \varnothing$ and for each $z_0 \in f^{-1}(U_f) \cap g^{-1}(U_g)$, and $f(z_0) \neq g(z_0)$. This proves that the set $\{z \in Z \mid f(z) = g(z)\}$ is a non-empty set which is is both open and closed and therefore is the whole space. □

Definition 2.5. Let $p : X \to Y$ a covering space, an automorphism of $X|Y$ is a topological automorphism ϕ of Y such that $\phi \circ p = p$. The set of all such automorphism will be denoted $\mathsf{Aut}(Y|X)$. △

For any given any covering space $p : Y \to X$, p can be factor as follows

$$Y \longrightarrow \mathsf{Aut}(Y|X) \setminus Y \xrightarrow{\overline{p}} X, \qquad p : Y \to X$$

The set $\mathsf{Aut}(Y|X) \setminus Y$ is the set of all orbits of Y under the action of $\mathsf{Aut}(Y|X)$ and the function between Y and $\mathsf{Aut}(Y|X) \setminus Y$ is the natural projection. Using this notation we can define the following.

Definition 2.6 (Galois covering)**.** A covering space $p : Y \to X$ is said to be Galois if Y is connected and the induced map $\overline{p} : \mathsf{Aut}(Y|X) \setminus Y \to X$ is a homeomorphism. △

The above definition looks familiar to that of a Galois extension of fields and we shall prove a theorem similar to the main theorem of Galois theory for finite extensions.

Proposition 2.7. *A connected covering space $p : Y \to X$ is a Galois covering if and only if $\mathsf{Aut}(Y|X)$ acts transitively on each fibre of p.*

Proof. As the set $\mathbf{Aut}(Y|X) \setminus Y$ is the set of all orbits of Y under the action of $\mathbf{Aut}(Y|X)$, so the function $\overline{p}$ is injective if and only if the group $\mathbf{Aut}(Y|X)$ acts transitively on each fibre of p. □

Definition 2.8. Let G be a group with a left continuous action over a topological space Y. The action of G over Y is said to be *even* if each $y \in Y$ has an open neighborhood U such that the open sets gU are pairwise disjoint for $g \in G$. △

Lemma 2.9. *For any given covering space $q : Z \to X$ and a continuous map $f : Y \to Z$ where Z and Y are connected if $q \circ f : Y \to X$ is a covering space, then so is $f : Y \to Z$.*

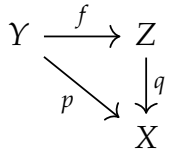
Proof. Let $z \in Z$, $x = q(z)$ and $V_x \subseteq X$ an open neighborhood of x satisfying definition 2.1 for both q and $q \circ f$. This induces two decompositions $\coprod U_{xi} = (q \circ f)^{-1}(V_x)$ and $\coprod W_{xi} = q^{-1}(V_x)$. For each $U_i \subseteq Y$, $f(U_i)$ is a connected subset of Z mapped by q onto V_x, therefore $f(U_i) \subseteq V_j$ for each j. Furthermore $f(U_i)$ and W_j are homeomorphic because both of them are homeomorphically mapped onto V_x, from this, one can deduce that $f(Y)$ is an open set in Z.

To prove that f is surjective, we will prove that $f(Y)$ is also closed and non empty and as Z is a connected space this implies $f(Y) = Z$.
Let $z \in Z \setminus f(Y)$ and let V_x be an open neighborhood of $x = q(z)$ satisfying definition 2.1. The component W_j of $q^{-1}(V_x)$ containing z and $f(Y)$ must be disjoint. This implies that $Z \setminus f(Y)$ is an open set, therefore $f(Y)$ is both open and closed. □

Lemma 2.10. *Let G be a group acting evenly over a connected space Y, then the natural projection $p_G : Y \to G \setminus Y$ turns Y into a covering space of $G \setminus Y$.*

Proof. It is clear that p_G is a surjective map, furthermore, for every $x \in G \setminus Y$ there is an open set $V = p_G(U)$ with U as in definition 2.8. It is easy to see that V satisfies definition 2.1. □

Theorem 2.11. *Let $p : Y \to X$ be a Galois covering space. For each subgroup H of $G := \mathbf{Aut}(Y|X)$ the projection p induces a natural map $\overline{p}_H : H \setminus Y \to X$ which turns $H \setminus Y$ into a covering space X.*
Conversely, if $Z \to X$ is a connected covering space fitting into a commutative diagram



then $f : Y \to Z$ is a Galois covering space and actually $Z \cong H \setminus Y$ for the subgroup $H = \mathrm{Aut}(Y|Z)$ of G. The maps $H \mapsto H \setminus Y$, $Z \mapsto \mathrm{Aut}(Y|Z)$ induce a bijection between subgroups of G and intermediate covering spaces Z as above.

Proof. The function p cna factor through H as follows:

$$Y \overset{p_H}{\to} H \setminus Y \overset{\overline{p}_H}{\to} X.$$

The function $\overline{p}_H$ is continuous because both p and p_H are continous (p_H is a local homeomorphism by 2.10). By lemma 2.3 one can find subsets V of X such that $p^{-1}(V) \cong F \times V$ where F is a discrete topological space on which H acts. The set $\overline{p}_H^{-1}(V)$ can be written as $H \setminus F \times V$. Using lemma 2.3, the space $H \setminus Y$ is a covering space of X.

To prove the converse statement, apply the lemma 2.9 to see that $f : Y \to Z$ is a covering space, now we will see that it is also Galois. By proposition 2.7, it will be enough to prove that the set $H \coloneqq \mathrm{Aut}(Y|Z)$ acts transitively on each fiber of f. Let $z \in Z$ and let y_1 and y_2 be two points in $f^{-1}(z)$. As the diagram in the statement commute, both y_1 and y_2 are cointained in the fibre $p^{-1}(q(z))$, so there is a $\phi \in G$ such that $\phi(y_1) = y_2$ (because $Y|X$ is Galois). The only thing left to prove is that $\phi \in H$, which is equivalent to the statement that $f = f \circ \phi$ □

2.2 The Universal Covering Space

We will now define the equivalent to the absolute Galois group in covering space, the proofs in this sections are outside the reach of this document and will be referenced.

Definition 2.12. Let X be a path-connected topological space, and let $p : Y \to X$ be a covering space such that Y is simply connected, then p (or Y) is called *an universal covering* of X. △

One can prove that any two given universal coverings of a topological space are isomorphic, so we can call an universal cover *the* universal cover. A proof of this fact can be found in [2].

One of the most important properties of the universal cover, is that it gives us another way to calculate the fundamental group of the base topological space, this is how the standard proof of the fact that $\pi_1(S^1) = \mathbb{Z}$ is justified. We will state this property and a proof of it can also be found in [2].

Theorem 2.13. *Let $p : \tilde{X} \to X$ be the universal covering space for some path-connected space X, then*

$$\mathrm{Aut}\,(\tilde{X}|X) \cong \pi_1(X).$$

Chapter 3

Fundamental Groups of Algebraic Curves

The goal of this chapter is to provide a strong motivation to study the Galois groups of certain field extensions and its importance in algebraic geometry.

3.1 Introduction to Affine Curves

In this section we will define an algebraic affine curve and prove some properties of it. In this section k will denote an algebraically closed field and we denote $\mathbb{A}^n := \{(x_1, \cdots, x_n) \,|\, x_i \in k\}$.

Proposition 3.1. *Let k be a field and A be a domain with transcendence degree 1 over k, then every proper nonzero prime ideal of A is maximal.*

Proof. Let $\mathfrak{p} \subset A$ be a nonzero prime ideal. Using Noether normalization lemma we can write A as an integral extension of the polynomial ring $k[x]$, the prime ideal $\mathfrak{p} \cap k[x]$ of $k[x]$ is nonzero because every nonzero element t of $\mathfrak{p}$ satisfies a monic polynomial equation $t^n + a_{n-1}t^{n-1} + \cdots + a_0 = 0$ with $a_i \in k[x]$ and $a_0 \neq 0$, therefore $-a_0 \in k[x] \cap \mathfrak{p}$. All nonzero prime ideals in $k[x]$ are maximal, therefore $\mathfrak{p} \cap k[x]$ is maximal and therefore $\mathfrak{p}$ is maximal. □

Definition 3.2. Given an ideal $I \subseteq k[x_1, \cdots, x_n]$ the subset defined as $V(I) := \{(x_1, \cdots, x_n) \in \mathbb{A}^n \mid p(x_1, \cdots, x_n) = 0 \text{ for all } p \in I\}$ is called the *Affine closed set* definded by I. △

Note that affine closed sets have the following properties:
Let $I_1, I_2, I_\lambda (\lambda \in \Lambda)$ be ideals in $k[x_1, \cdots, x_n]$, then the following properties hold:

1. $I_1 \subseteq I_2 \Rightarrow V(I_1) \supseteq V(I_2)$.
2. $V(I_1) \cup V(I_2) = V(I_1 \cap I_2) = V(I_1 I_2)$.
3. $V(\langle I_\lambda | \lambda \in \Lambda \rangle) = \bigcap_{\lambda \in \Lambda} V(I_\lambda)$.

This induces a topology in $\mathbb{A}^n$, known as the *Zariski topology* whose closed sets are given by affine closed subsets of $\mathbb{A}^n$. A basis for the Zarizki topology of $\mathbb{A}^n$ can be given by the open subsets defined as follows: $D(f) \coloneqq \{P \in \mathbb{A}^n \mid f(P) \neq 0\}$ where f is any fixed polynomial in $k[x_1, \cdots, x_n]$.

If in a given affine closed set $X = V(I)$ we have $I = \sqrt{I}$ then X and I determine each other and we call X an *affine variety*. Affine varieties have the subspace topology induced by the Zarisky topology of $\mathbb{A}^n$.

Definition 3.3. Let $X = V(I)$ be an affine variety, we define the *coordinated ring of* X as the set $O(X) \coloneqq k[x_1, \cdots, x_n]/I$. It's elements are *regular functions* over X. The images $\overline{x}_i$ of the x_i are called coordinate functions on X. △

Definition 3.4. Given an affine variety $Y = V(J)$, a morphism or regular map $\phi : Y \to \mathbb{A}^m$ is a m-tuple $\phi = (f_1, \cdots, f_m) \in O(Y)^m$. Given another affine variety $X \subseteq \mathbb{A}^m$, morphism $\phi : Y \to X$ is a morphism $\phi : Y \to \mathbb{A}^m$ such that $\phi(p) = (f_1(p), \cdots, f_m(p)) \in \mathbb{A}^m$ lies in X for all $p \in Y$. △

Note that a morphism between affine varieties $\phi : Y \to X$ induces a morphism of algebras $\phi^* : O(X) \to O(Y)$ such that $\phi^*(f) = f \circ \phi$. One can also note that morphisms are continous with respect to Zarizki topology:

$$\phi^{-1}(D(f)) = D(\phi^*(f)).$$

Proposition 3.5. *Let $X = V(I)$ an affine variety and $p \in X$, the set $\mathfrak{m}_p \coloneqq \{f \in O(X) | f(p) = 0\}$ is a maximal ideal.*

Proof. Let $h \in O(X)$ such that $h \notin \mathfrak{m}_p$. We will now proof that $\langle \mathfrak{m}_p, h \rangle = O(X)$. Let $f \in O(X)$ and define g as follows:

$$g = f - \frac{f\,h}{h(p)}.$$

One can easily check that $f = g + \frac{fh}{h(p)}$. Note that $g \in \mathfrak{m}_p$, therefore $f \in \langle \mathfrak{m}_p, h \rangle$. □

Every maximal ideal $\mathfrak{m}$ is radical ($\sqrt{\mathfrak{m}} = \mathfrak{m}$) and therefore $\mathfrak{m}$ and $V(\mathfrak{m})$ determine each other, this implies that for every maximal ideal $\mathfrak{m}$, the set $V(\mathfrak{m})$ is a singleton.

If $X = V(I)$ is an affine variety such that $O(X)$ is an integral domain we call X an integer affine variety. In this case we denote by $K(X)$ the fraction field of $O(X)$. The transcendence degree of the extension $K(X) : k$ is called the *dimension* of X. An affine variety of dimension 1 is called an *affine curve*.

Theorem 3.6. *All proper closed subsets of an integral affine algebraic curve are finite.*

Proof. In a Noetherian ring every proper ideal satisfying $\sqrt{I} = I$ is a finite intersection of prime ideals. For each ideal $L \subseteq O(X)$ we have $\sqrt{L} = \bigcap_{i=1}^{r} \mathfrak{p}_i$ and by theorem 3.1 each of the $\mathfrak{p}_i$ are maximal ideals, therefore the algebraic sets $V(\mathfrak{p}_i)$ are singletons. Note that

$$V(L) = V\left(\sqrt{L}\right) = V\left(\bigcap_{i=1}^{r} \mathfrak{p}_i\right) = \bigcup_{i=1}^{r} V(\mathfrak{p}_i)$$

and therefore $V(L)$ is a finite set. □

3.2 The Fundamental Group of Affine Schemes

We will now extend the concept of an affine curve to an arbitrary base field. The theory of the last section can't be applied to a non-algebraically closed field because in this case some ideals of polynomials will not have any zeros in the affine space. To solve this we will now introduce the concept of sheaf.

Definition 3.7. Let X be a topological space. A *presheaf* of sets (or rings, grups...) $\mathcal{F}$ is a rule that for every open set $U \subseteq X$ assings a set $\mathcal{F}(U)$ (in which elements are called *sections*) such that for every inclusion of open sets $V \subseteq U$ one has a morphism $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$ where $\rho_{UU} = id_{\mathcal{F}(U)}$ and for every chain of open sets $W \subseteq V \subseteq U$ the following equality holds: $\rho_{VW} \circ \rho_{UV} = \rho_{UW}$. △

One can define *morphism* between presheaves as follows, let $\mathcal{F}$ and $\mathcal{G}$ be sheaves, a morphisms Φ between $\mathcal{F}$ and $\mathcal{G}$ is a collection of maps (or morphisms) $\Phi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ such that for every inclusion $V \subseteq U$ the following diagram:

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\Phi_U} & \mathcal{G}(U) \\ {\scriptstyle \rho^{\mathcal{F}}_{UV}}\downarrow & & \downarrow{\scriptstyle \rho^{\mathcal{G}}_{UV}} \\ \mathcal{F}(V) & \xrightarrow{\Phi_V} & \mathcal{G}(V) \end{array}$$

commutes.

Example 3.8. Let X be a topological space and for each U let $\mathcal{F}(U)$ be the additive group of continous functions from U to $\mathbb{R}$. In this case, it is easy to see that for each inclusion $V \subseteq U$ of open sets the map ρ_{UV} can be defined as follows: For $s \in \mathcal{F}(U)$, $\rho_{UV}(s) = s_{|V}$. ◇

Keeping the last example in mind we will use the notation $s_{|V}$ refering to $\rho_{UV}(s)$ when the inclusion $V \subseteq U$ is clear.

Definition 3.9. A *sheaf* over a topological space X is a presheaf $\mathcal{F}$ satisfying the following conditions:

1. For a given non empty open set U and an open cover $\{U_i \mid i \in I\}$ of U of non empty sets if two sections $s, t \in \mathcal{F}(U)$ satisfy $s_{|U_i} = t_{|U_i}$ for all $i \in I$ then $s = t$.

2. For any given cover like in property 1 with a section system $\{s_i \in \mathcal{F}(U_i) \mid i \in I\}$ such that:

$$s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$$

whenever $U_i \cap U_j \neq \varnothing$ there is a section $s \in \mathcal{F}(U)$ such that $s_{|U_i} = s_i$ for every $i \in I$.

Using property 1 one can easily check that the section s from part 2 is unique. △

One can define morphisms of sheaves as morphisms of presheaves. With the previous definition now we can define our last tool to study curves over a general base field.

Definition 3.10 (Ringed space)**.** A ringed space is a topological space X together with a sheaf of rings $\mathcal{F}$ over X. △

Remark 3.11. Note that for any open set $U \subseteq X$ one has the following inclusion: $\varnothing \subseteq U$ and therefore for every sheaf $\mathcal{F}$ over X there is a morphsm $\mathcal{F}(U) \to \mathcal{F}(\varnothing)$. If $\mathcal{F}$ is a sheaf of rings, $\mathcal{F}(\varnothing)$ is the terminal object of the category of rings, i.e. $\mathcal{F}(\varnothing) = \{0\}$.

Let $\mathcal{O}$ be a ring with fraction field K and let $X \coloneqq \mathsf{Spec}(\mathcal{O})$ be the set of prime ideals in $\mathcal{O}$, and endow X with the topology on which closed sets are:

$$V(\mathfrak{a}) = \{\mathfrak{p} \mid \mathfrak{p} \supseteq \mathfrak{a}\}$$

for $\mathfrak{a}$ an ideal in $\mathcal{O}$.

For any given open subset $U \subseteq X$, define:

$$\mathcal{O}(U) \coloneqq \left\{ \frac{f}{g} \quad | \quad g(\mathfrak{p}) \neq 0 \quad \text{for all } \mathfrak{p} \in U \right\},$$

as a subset of K, note that:

$$\mathcal{O}(U) = \bigcap_{\mathfrak{p} \in U} \mathcal{O}_{\mathfrak{p}}. \tag{3.12}$$

Proposition 3.13. *The topological space X together with the sheaf of rings $\mathcal{O}(\cdot)$ is a ringed space, given two open subsets $U, V \subset X$ such that $V \subset U$, the morphisms ρ_{UV} is the inclusion $\mathcal{O}(U) \hookrightarrow \mathcal{O}(V)$ induced by equation 3.12.*

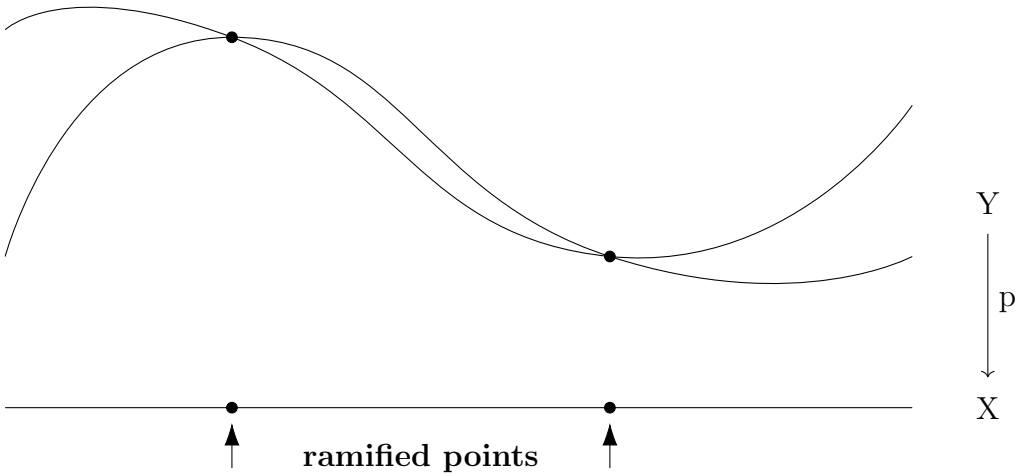
The proof of the above proposition, follows directly from the definitions, the ringed space $(X, \mathcal{O})$ is called an *affine scheme*.

Let o be a Dedekind domain with field of fractions K. Let $L|K$ be a finite separable extension of index n, and $\mathcal{O}$ its integral closure in in L. Let $X = \mathsf{Spec}\,(o)$, $Y = \mathsf{Spec}\,(\mathcal{O})$, and let $p : Y \to X$ the morphism of sheaves induced by the inclusion $X \hookrightarrow Y$.

In this case, the function p plays a similar role to the notion of a covering space induced in chapter 2. If any given maximal ideal $\mathfrak{p} \subseteq o$ has a prime descomposition

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$$

the morphism p is called a *ramified covering*. The following figure, shows how the ramification of prime ideals affects the "covering" in the case where the residue class fields of o are algebraically closed:



If that is the case, the fundamental identity($\sum_{i=1}^{r} e_i f_i = n$) tells us that for each point $\mathfrak{p} \in X$ there are exactly n points on Y lying above it if p is not ramified in $\mathcal{O}$. At a ramified point, many points in $\mathcal{O}$ can coincide (the graph makes evident the name "*ramify*".

If $L|K$ is a Galois extension with $G \coloneqq \mathrm{Gal}(L|K)$, then each $\sigma \in G$ via $\sigma_{|\mathcal{O}}$ defines an automorphism of ringed spaces $\tilde{\sigma} : X \to X$, and as $\mathcal{O} \subseteq K$, then the following diagram

$$\begin{array}{ccc} X & \xrightarrow{\quad\sigma\quad} & X \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle f} & \\ & Y & \end{array}$$

commutes. This automorphism is again analogue to the automorphisms of covering spaces in chapter 2, son one would like to define an equivalent to the universal cover space to define the fundamental grup of an affine scheme.

This universal covering space can be constructed as the spectrum of the integral closure of $\mathcal{O}$ in the composite of all unramified extensions, say $\tilde{K}$ inside an algebraic closure of K. For an explicit construction, the reader can refer to [6], chapter 7. If $\tilde{X}$ is the universal cover mentioned above, one can now define the fundamendal group of X:

$$\pi_1(X) \coloneqq \mathrm{Gal}(\tilde{K}|K).$$

Chapter 4

Cohomology of Groups

4.1 G-modules

Definition 4.1. Let G be a group. A G-module is an abelian group M together with a map

$$\begin{aligned} G \times M &\to M \\ (g, m) &\mapsto gm \end{aligned}$$

such that for each $g, g' \in G$ and $m, m' \in M$,

- $g(m + m') = gm + gm'$
- $(gg')(m) = g(g'm)$
- $1m = m$.

A G-homomorphism is a map between G-modules $\alpha : M \to N$ such that

- $\alpha(m + m') = \alpha(m) + \alpha(m')$.
- $\alpha(gm) = g(\alpha(m))$, for all $g \in G$, $m \in M$.

$\triangle$

Definition 4.2. Let G be a group and $H \subseteq G$ a subgroup. Let M be a H-module, the *induced G-module*, denoted $\mathrm{Ind}_H^G(M)$ is the set of all functions ϕ from G to M such that $\phi(hg) = h\phi(g)$ for each $h \in H$. The set $\mathrm{Ind}_H^G(M)$ has a G-module structure with the followng operations.

- $(\phi + \phi')(x) = \phi(x) + \phi'(x)$
- $(g\phi)(x) = \phi(xg)$.

If $H = 1$, then a H-module is just an abelian group, so we drop H from the notation $\mathrm{Ind}_H^G(M)$, therefore

$$\mathrm{Ind}^G(M) = \{\phi : G \to M_0\}$$

△

Definition 4.3. Let G be a group and M a G-module. The *group algebra of G*, denoted $\mathbb{Z}[G]$ is the free abelian group with basis the elements of G together with the product defined as follows:

$$\left(\sum_i n_i g_i\right)\left(\sum_j n'_j g'_j\right) = \sum_{i,j} n_i n'_j \left(g_i g'_j\right).$$

△

Note that if $H = 1$ then the set $\mathrm{Ind}_G^H(M)$ is the set of all function from G to M which can be also identified with the set $\mathrm{Hom}_{\mathrm{Ab}}(\mathbb{Z}[G], M)$.

Lemma 4.4. *For every G-module M and H-module N, one has the following isomorphism*

$$\mathrm{Hom}_G\left(M, \mathrm{Ind}_H^G(N)\right) \cong \mathrm{Hom}_H(M, N).$$

Proof. For any given G-homomorphism $\alpha : M \to \mathrm{Ind}_H^G(N)$. Define the map:

$$\begin{aligned} \beta : M &\to N \\ m &\mapsto \alpha(m)(1_G). \end{aligned}$$

Therefore, for every $g \in G$, $\beta(gm) \overset{\text{def}}{=} (\alpha(gm))(1_G) = (g(\alpha(m)))(1_G) = \alpha(m)(g)$. As $\alpha \in \mathrm{Ind}_H^G(N)$, when $g \in H$ we have $\alpha(m)(g) = g(\alpha(m)(1_G)) = g(\beta(m))$ and it follows that β is a H-homomorphism $M \to N$.

Conversely, given an H-homomorphism $\beta : M \to N$ we define:

$$\begin{aligned} \alpha : M &\to \mathrm{Ind}_H^G(N) \\ m &\mapsto \alpha(m) : G \to N \\ & \qquad g \mapsto \beta(gm). \end{aligned}$$

And therefore α is a G-homomorphism. One can check that the maps $\alpha \mapsto \beta$ and $\beta \mapsto \alpha$ are inverse and it follows that both are isomorphisms. □

Lemma 4.5. *The functor*

$$\mathrm{Ind}_H^G(\,) : \mathrm{Mod}_H \to \mathrm{Mod}_G$$

is exact.

Proof. Consider a short exact sequence of H modules:

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0. \tag{4.6}$$

This induces the short sequence of G-modules:

$$0 \longrightarrow \mathrm{Ind}_H^G(M) \xrightarrow{\overline{f}} \mathrm{Ind}_H^G(N) \xrightarrow{\overline{g}} \mathrm{Ind}_H^G(P) \longrightarrow 0 \tag{4.7}$$

where $\overline{f}$ and $\overline{g}$ are induced by f and g as follows:

$$\begin{aligned} \overline{f} : \mathrm{Ind}_H^G(M) &\to \mathrm{Ind}_H^G(N) \\ \phi &\mapsto f \circ \phi \end{aligned}$$

$$\begin{aligned} \overline{g} : \mathrm{Ind}_H^G(N) &\to \mathrm{Ind}_H^G(P) \\ \varphi &\mapsto g \circ \varphi. \end{aligned}$$

We will now prove that the second sequence is exact. First we will prove that $\overline{f}$ is injective: let $\phi, \gamma \in \mathrm{Ind}_H^G(M)$ with $\overline{f}(\phi) = \overline{f}(\gamma)$, that is $f \circ \phi = f \circ \gamma$. As f is injective, there exists a left inverse f^{-1} and therefore $f^{-1} \circ f \circ \phi = f^{-1} \circ f \circ \gamma$ which implies $\phi = \gamma$.

To prove that the diagram 4.7 is exact in its second position, let $\phi \in \mathrm{Ind}_H^G(M)$, then $\overline{g} \circ \overline{f}(\phi) = g \circ f \circ \phi$ and as $f(M) = \ker g$, we have $g \circ f$

is the trivial homomorphism an therefore $\overline{g} \circ \overline{f}(\phi)$ is zero; from this we can deduce that $\overline{f}\left(\mathrm{Ind}_H^G(M)\right) \subseteq \ker \overline{g}$.
Now, let $\varphi \in \ker \overline{g}$ we know that for each $x \in G$, $\overline{g}(\varphi)(x) = 1$, that is $g \circ \varphi(x) = g\left(\varphi(x)\right) = 0$ which implies $\varphi(x) \in \ker g$ and using the exactness of diagram 4.6, $\varphi(x) \in f(M)$ which can be written as follows: For every $x \in G$ there exists a $m_x \in M$ with $\varphi(x) = f(m_x)$ Using this notation, we define the function $\pi : G \to M$ such that $\pi(x) = m_x$, now let $x \in G$ with $\pi(x) = m_x$ and $y \in H$, we have:

$$\begin{aligned} \varphi(yx) &\overset{4.1}{=} y\varphi(x) \\ &= yf(m_x) \\ &\overset{4.1}{=} f(ym_x) \end{aligned}$$

which by definition of π implies that $\pi(yx) = ym_x = y\pi(x)$, this is the requirement of definition 4.1 and therefore $\pi \in \mathrm{Ind}_H^G(M)$. One can easily check that $\varphi = f \circ \pi$ (as showed in the diagram)

$$\begin{array}{ccc} G & \overset{\pi}{\dashrightarrow} & M \\ & \searrow^{\varphi} & \downarrow f \\ & & N \end{array}$$

and it follows that $\overline{f}(\pi) = \varphi$, or written in another way: $\varphi \in \overline{f}(M)$ which proves the exactness of 4.7 in its second position.

Now we have to prove that $\overline{g}$ is surjective. Let $\omega \in \mathrm{Ind}_H^G(P)$, as g is surjective it has a right inverse , let g^{-1} be its right inverse. One can easily check that $g^{-1} \circ \omega$ is a preimage of ω. □

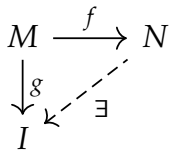
For a G-module M, define the set

$$M^G = \{m \in M | gm = m \text{ for all } g \in G\}.$$

4.2 Definition of the Cohomology of Groups

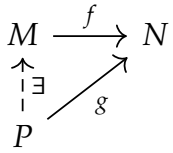
Definition 4.8. Let I be a G-module. The G-module I is said to be *injective* if for any G-modules M, N, with an injective G-homomorphism $f : M \longrightarrow N$

and a G-homomorphism $g : M \to I$, there exists a G-homomorphism such that de diagram:



commutes. △

Definition 4.9. Let P be a G-module. The G-modle P is said to be *projective* if for any two G-modules M, N, with a surjective G-homomorphism $f : M \to N$ and any G-homomorphism $g : P \to N$, there is a G-homomorphism such that the diagram:



commutes. △

Lemma 4.10. *Let G be a group and I be an injective abelian group, the G-module $\mathrm{Ind}^G(I)$ is injective.*

Proof. Let M and N be G-modules with $N \subseteq M$ and $\Phi : N \to \mathrm{Ind}^G(I)$ be a G-homomorphism. Note that Φ defines a homomorphism of abelian groups $\phi : N \to I$ such that $\phi(n) = \Phi(n)(1_G)$. As I is an injective abelian group, the homomorphism ϕ can be extended to an homomorphism $\tilde{\phi}$ defined over M. Now we define the G-homomorphism $\tilde{\Phi} : M \to \mathrm{Ind}^G(I)$, $m \mapsto \alpha_m$ such that $\alpha_m(g) = \tilde{\phi}(gm)$. The reader should be able to check easily that $\tilde{\Phi}$ extends Φ to all M.

□

Lemma 4.11. *The category of $G-$modules has enough injective objects.*

Proof. The claim means that every G-module M can be embedded into an injective G-module, $M \hookrightarrow I$. If $G = 1$, the category of Mod_G is the category of abelian groups, which is known to have enough injectives. Let M be a G-module and M_0 an abelian group, M_0 can be embeded into an injective abelian group, say $M_0 \hookrightarrow I$. If the functor $\mathrm{Ind}^G(\cdot)$ is appied, we get an

inclusion $\mathrm{Ind}^G(M_0) \hookrightarrow \mathrm{Ind}^G(I)$ of G-modules. One can define an inclusion of G-modules

$$\begin{aligned} M &\hookrightarrow \mathrm{Ind}^G(M_0) \\ m &\mapsto \alpha \end{aligned} \tag{4.12}$$

such that $\alpha(g) = gm$ and therefore we have an inclusion $M \hookrightarrow \mathrm{Ind}^G(I)$, the last of which is injective by lemma 4.10.

□

Lemma 4.13. *The functor* $(\cdot)^G : \mathrm{Mod}_G \to \mathrm{Ab}$ *is left exact.*

Proof. Let

$$0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

be an exact sequence, we will now prove that the sequence

$$0 \longrightarrow M'^G \xrightarrow{\phi^G} M^G \xrightarrow{\psi^G} M''^G$$

is exact, where $\phi^G := \phi_{|M'^G}$ and $\psi^G := \psi_{|M^G}$. The exactness in M'^G is clear (if ϕ is injective, then ϕ^G is also injective). Now, the fact that $\mathrm{Im}\,\phi^G \subseteq \ker\psi^G$ is also clear, it comes form the exactness of the first sequence at M. We will prove that $\mathrm{Im}\,\phi^G \supseteq \ker\psi^G$, let $x \in \ker\psi^G$, then $x \in \ker\psi$ and therefore $x \in \mathrm{Im}\,\phi$, so let $y \in M'$ such that $\phi(y) = x$, as $x \in M^G$ we have for each $g \in G$, for each $g \in G$ we have $gx = g\phi(y) = \phi(gy) = x$ and as ϕ is injective, $y = gy$, therefore $y \in M'^G$ so $x \in \mathrm{Im}\,\phi^G$. □

Definition 4.14. Let M be a G-module, a *relsolution* of M is an exact sequence of G-modules.

$$\cdots \xrightarrow{d_{n+1}} E_n \xrightarrow{d_n} \cdots \xrightarrow{d_3} E_2 \xrightarrow{d_2} E_1 \xrightarrow{d_1} E_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

A *coresolution* of M is an exact sequence of G-modules:

$$0 \longrightarrow M \xrightarrow{\varepsilon} C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \xrightarrow{d^2} \cdots \xrightarrow{d^{n-1}} C^n \xrightarrow{d^n} \cdots.$$

A coresolution in which the objects C_i are injective is called an *injective resolution of* M, a resolution in which the objects E_i are projective, is called a *projective resolution of* M.

△

Definition 4.15. Let M be a G-module. Let

$$0 \longrightarrow M \longrightarrow I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots$$

be an injective resolution (which exists by 4.11), as the functor $(\cdot)^G$ is left exact, then the complex

$$0 \xrightarrow{d^{-1}} \left(I^0\right)^G \xrightarrow{d^0} \left(I^1\right)^G \xrightarrow{d^1} \left(I^2\right)^G \xrightarrow{d^2} \cdots$$

is not necessarily exact, we define the *cohomology* of G with coefficients in M as

$$H^r(G, M) \coloneqq \frac{\ker\left(d^r\right)}{\operatorname{Im}\left(d^{r-1}\right)}.$$

△

We will now study some of the properties of these groups.

Remark 4.16. These groups have the following properties:

1. $H^0(G, M) = M^G$ because $0 \longrightarrow M^G \longrightarrow \left(I^0\right)^G \xrightarrow{d^0} \left(I^1\right)^G$ is exact, therefore $\ker d^0 \cong M^G$.
2. If M is an injective module, then $H^r(G, I) = 0$ for all $r > 0$ because $0 \to I \to I \to 0 \to \cdots$ is an injective resolution for I.
3. Let $M \to I^\bullet$ and $N \to J^\bullet$ be two injective resolutions of G-modules M and N, then any homomorphism $\alpha : M \to N$ of G-modules, can be extended to a map of chain complexes such that the diagram

$$\begin{array}{ccccccc} M & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & \cdots \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha^0} & & \downarrow{\scriptstyle \alpha^1} & & \\ N & \longrightarrow & J^0 & \longrightarrow & J^1 & \longrightarrow & \cdots \end{array}$$

commutes. If this property is applied to the identity map $I_M : M \to M$, one concludes that the groups $H^r(G, M)$ don't depend of the choice of the injctive resolution and therefore are well defined. With this notation, the group $H^r(G, M)$ will also be written as $H^r(I^\bullet)$ if $I^\bullet$ is an injective resolution of M.

4. Any short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

induces a long exact sequence.

$$0 \to H^0\left(G, M'\right) \to \cdots \to H^r(G, M) \to H^r\left(G, M''\right) \xrightarrow{\delta^r} H^{r+1}\left(G, M'\right) \to \cdots.$$

Proposition 4.17. *For any G-modules M_i,*

$$H^r\left(G, \prod_i M_i\right) \simeq \prod_i H^r\left(G, M_i\right)$$

Proof. The reader can easily prove that a product of exact sequences of abelian groups is again exact, and therefore $I \coloneqq \prod I_i$ is injective if the I_i are injective. Let $M_i \to I_i^\bullet$ be an injective resolution of M_i. Then $\prod M_i \to \prod I_i^\bullet$ is an injective resolution of $\prod M_i$, and

$$\begin{aligned} H^r\left(G, \prod_i M_i\right) &\simeq H^r\left(\left(\prod_i I_i^\bullet\right)^G\right) \\ &\simeq H^r\left(\prod_i \left(I_i^{\bullet G}\right)\right) \\ &\simeq \prod_i H^r\left(I_i^{\bullet G}\right) \\ &\simeq \prod_i H^r\left(G, M_i\right). \end{aligned} \tag{4.18}$$

□

Lemma 4.19 (Shapiro)**.** *Let H be a subgroup of G and N and H-module. There is an isomorphism*

$$H^r(G, \mathrm{Ind}_H^G(N)) \xrightarrow{\cong} H^r(H, N)$$

for all $r \geq 0$.

Proof. For $r = 0$, note that a homomorphism $\alpha : \mathbb{Z} \to M$ is uniquely determined by $\alpha(1)$, and $n \in N$ is the image of 1 under a G-homomorphism $\mathbb{Z} \to N$ if and only if it is fixed by G, therefore

$$\mathrm{Hom}_G(\mathbb{Z}, M) \cong M^G, \tag{4.20}$$

hence:

$$N^H \overset{4.20}{\cong} \mathrm{Hom}_H(\mathbb{Z}, N) \overset{4.4}{\cong} \mathrm{Hom}_G\left(\mathbb{Z}, \mathrm{Ind}_H^G(N)\right) \overset{4.20}{\cong} \mathrm{Ind}_H^G(N)^G \tag{4.21}$$

For an arbitrary r, let $N \to I^\bullet$ be an injective resolution of N. Applying the functor $\mathrm{Ind}_H^G(\cdot)$, the result is an injective resolution $\mathrm{Ind}_H^G(N) \to \mathrm{Ind}_H^G(I^\bullet)$ because the the functor $\mathrm{Ind}_H^G(\cdot)$ is exact 4.5 and preserves injectives (4.10). Therefore

$$H^r\left(G, \mathrm{Ind}_H^G(N)\right) = H^r\left(\left(\mathrm{Ind}_H^G(I^\bullet)\right)^G\right) \overset{4.21}{\cong} H^r\left(I^{\bullet H}\right) = H^r(H, N)$$

□

4.3 Cohomology and Cochains

Let $P_\bullet \to \mathbb{Z}$ be a projective resolution of $\mathbb{Z}$ seen as a trivial G-module. Let M be a G-module, as the functor $\mathrm{Hom}_G(-, M)$ is a left exact contravariant functor, the above resolution defines the following complex:

$$\mathrm{Hom}_G(\mathbb{Z}, M) \cong M^G \xrightarrow{d_0} \mathrm{Hom}_G(P_1, M) \xrightarrow{d_1} \mathrm{Hom}_G(P_2, M) \xrightarrow{d_2} \cdots,$$

which no longer needs to be exact. This motivates the following definition.

Definition 4.22. With the above notation, we define:

$$H^r(\mathrm{Hom}_G(P_\bullet, M)) = \frac{\mathrm{Ker}\, d_r}{\mathrm{Im}\, d_{r-1}}.$$

△

Define P_r, $r \geq 0$ as the free abelian group with basis the set of $r+1$-tuples $(g_0, \cdots, g_r)$ of elements on G, seen as a $\mathbb{Z}$ modules (in the future it will be useful to see them as $\mathbb{Z}(G)$-modules), with G acting as follows:

$$g(g_0, \cdots, g_r) \coloneqq (gg_0, \cdots, gg_r).$$

Define the homomorphism $d_r : P_r \to P_{r-1}$ as follows:

$$d_r(g_0, \cdots, g_r) = \sum_{i=0}^{r} (-1)^i (g_0, \cdots, \hat{g}_i, \cdots, g_r), \tag{4.23}$$

where $\hat{\cdot}$ means that $\cdot$ is ommited. Finally, define the morphism $\epsilon : P_0 \to \mathbb{Z}$ such that ϵ sends each basis element of P_0 to 1.

Lemma 4.24. *The sequence* $P_\bullet \xrightarrow{\epsilon} \mathbb{Z} \to 0$ *is exact.*

Proof. Choose $h \in G$, let $k_r : P_r \to P_{r+1}$ be defined as follows:

$$k_r\left(g_0, \cdots, g_r\right) = \left(h, g_0, \cdots, g_r\right).$$

Note that $d_{r+1} \circ k_r + k_{r-1} \circ d_r = \mathrm{Id}_{P_r}$:

$$\begin{aligned}
d_{r+1} \circ k_r + k_{r-1} \circ d_r \left(g_0, \cdots, g_r\right) &= \sum_{i=0}^{r+1} (-1)^i (h, g_0, \cdots, \hat{g}_{i-1}, \cdots, g_r) \\
&\quad + k_{r-1}\left(\sum_{i=0}^{r} (-1)^i (g_0, \cdots, \hat{g}_i, \cdots, g_r)\right) \\
&= \sum_{i=0}^{r+1} (-1)^i (h, g_0, \cdots, \hat{g}_{i-1}, \cdots, g_r) \\
&\quad + \sum_{i=0}^{r} (-1)^i (h, g_0, \cdots, \hat{g}_i, \cdots, g_r) \\
&= (g_0, \cdots, g_r) \\
&\quad + \sum_{i=1}^{r+1} (-1)^i (h, g_0, \cdots, \hat{g}_{i-1}, \cdots, g_r) \\
&\quad + \sum_{i=0}^{r} (-1)^i (h, g_0, \cdots, \hat{g}_i, \cdots, g_r) \\
&= (g_0, \cdots, g_r) \\
&\quad + \sum_{i=0}^{r} (-1)^{i+1} (h, g_0, \cdots, \hat{g}_i, \cdots, g_r) \\
&\quad + \sum_{i=0}^{r} (-1)^i (h, g_0, \cdots, \hat{g}_i, \cdots, g_r) \\
&= (g_0, \cdots, g_r).
\end{aligned}$$

Therefore, $d_r(x) = 0$ implies $x = d_{r+1}(k_r(x))$. The fact that $d_r \circ d_{r+1} = 0$ comes dicectly from equation 4.23. □

Proposition 4.25. *For any G-module M:*

$$H^r(G, M) \cong H^r\left(\mathrm{Hom}_G\left(P_\bullet, M\right)\right).$$

Proof. For any G-module M, $\mathrm{Hom}_G(\mathbb{Z}, M) = M^G$, so $H^0(G, \cdot)$ and $\mathrm{Hom}_G(\mathbb{Z}, \cdot)$ agree, therefore so do their right derived functors. □

Seen as a $\mathbb{Z}$-module, every element in $\mathrm{Hom}_G(P_\bullet, M)$ can be caracterized by a function $\phi : G^{r+1} \to M$ with the following property:

$$\phi(gg_0, \cdots, gg_r) = g\phi(g_0, \cdots, g_r), \tag{4.26}$$

the set of all the function with the above property is called the set of *homogeneous r-cochain of G with values in M* and will be denoted as $\tilde{C}^r(G, M)$. Define the boundary maps as follows:

$$\begin{aligned} \tilde{d}^r : \tilde{C}^r(G, M) &\to \tilde{C}^{r+1}(G, M) \\ \phi &\mapsto \tilde{d}^r(\phi) \end{aligned}$$

of groups such that the diagram: as induced by 4.23:

$$\tilde{d}^r(\phi)(g_0, \cdots, g_{r+1}) = \sum (-1)^i \phi(g_0, \cdots, \hat{g}_i, \cdots, g_{r+1})$$

Proposition 4.25 tells us that

$$H^r(G, M) \cong \frac{\mathrm{Ker}(\tilde{d}^r)}{\mathrm{Im}(\tilde{d}^{r-1})}.$$

The set $\mathrm{Hom}_G(P_\bullet, M)$ can also be seen as a $\mathbb{Z}[G]$-module, any G-homomorphism between P_r and M can be seen as a map (any map) $\phi : G^{r+1} \to M$. Let $C^r(G, M)$ the set of all maps $G^r \to M$. For any given map $\phi \in C^r(G, M)$ define the function $d^r : C^r(G, M) \to C^{r+1}(G, M)$ such that $d^r(\phi)(g_1, \cdots, g_{r+1}) =$

$$g_1\phi(g_2, \cdots, g_{r+1}) + \sum_{j=1}^{r} (-1)^j \phi(g_1, \cdots, g_j g_{j+1}, \cdots, g_{r+1}) + (-1)^{r+1} \phi(g_1, \cdots, g_r). \tag{4.27}$$

And define $Z^r(G, M) = \mathrm{Ker}(d^r)$ (group of r-cocicles) and $B^r(G, M) = \mathrm{Im}(d^{r-1})$ (group of r-coboundaries).

Proposition 4.28. *The sequence of maps*

$$C^0(G,M) \xrightarrow{d^0} C^1(G,M) \xrightarrow{d^1} \cdots \xrightarrow{d^{r-1}} C^r(G,M) \xrightarrow{d^r} C^{r+1}(G,M)\cdots$$

is a complex and there is a canonical isomorphism:

$$H^r(G,M) \cong \frac{Z^r(G,M)}{B^r(G,M)}.$$

Proof. Let $\Phi : \tilde{C}^r(G,M) \to C^r(G,M)$ be defined as follows:

$$\Phi(\phi)(g_1,\cdots,g_r) = \phi(1, g_1, g_1g_2, \ldots, g_1\cdots g_r).$$

The function Φ is a $\mathbb{Z}[G]$-isomorphism transforming the boundary maps in $\tilde{C}^\bullet(G,M)$ into the boundary maps in $C^\bullet(G,M)$. □

4.4 The Cohomology of L and $L^\times$

Example 4.29. Let G be a group and M a G-module. If $r = 1$, a map $\phi \in \mathrm{Ker}(d^1)$, following equation 4.27, has the followng property:

$$g_1\phi(g_2) - \phi(g_1g_2) + \phi(g_1) = 0,$$

this is:

$$\phi(g_1g_2) = g_1\phi(g_2) + \phi(g_1)$$

A function with this property is called an *crossed homomorphism*. Note that for each $m \in M$, the function $\sigma \mapsto \sigma m - m$ is a crossed homomorphism, a map that can be written like this will be called a *principal crossed homomorphism*; one can also check that if $\phi \in \mathrm{Im}(d^0)$ then ϕ is a principal crossed homomorphism (recall $G^0 = \{1\}$). This implies that

$$H^1(G,M) = \frac{\{\text{Crossed homomorphisms}\}}{\{\text{Principal crossed homomorphisms}\}}.$$

◇

Theorem 4.30 (Hilbert 90, Noether Generalization)**.** *Let $L : k$ be a finite Galois extension with Galois group G. Then $H^1(G, L^\times) = 0$.*

Proof. Using example 4.29 we will prove that every crossed homomorphism ϕ is principal, with multiplicative notation, this is

$$\phi(\sigma)\tau = \sigma\phi(\tau)\cdot\phi(\sigma)$$

and we must find $c \in L^\times$ such that $\phi(\sigma) = \frac{\sigma c}{c}$. Let $a \in L^\times$ and

$$b = \sum_{\sigma\in G} \phi(\sigma)\cdot\sigma a.$$

if $b \neq 0$, then

$$\begin{aligned}\tau b &= \sum_{\sigma\in G} \tau\phi(\sigma)\cdot\tau\sigma a \\ &= \sum_{\sigma\in G} \phi(\tau)^{-1}\phi(\tau\sigma)\tau\sigma a \\ &= \phi(\tau)^{-1} b.\end{aligned}$$

And therefore

$$\phi(\tau) = \frac{b}{\tau b}.$$

Now we have to prove that there is an a such that $b \neq 0$. By Dedekind's theorem on the independence of characters, the map $\sum_\sigma \phi(\sigma)\sigma$ is not the zero map, so there exists an a such that $b \neq 0$. □

Proposition 4.31. *Let $L : K$ be a finite Galois extension with Galois group G. Then $H^r(G, L) = 0$ for all $r > 0$.*

Proof. From Galois Theory, one knows that there exists $\alpha \in L$ such that the set $\{\sigma\alpha \mid \sigma \in G\}$ is a basis for L as a K-vector space. Hence, the function

$$\begin{aligned}\Phi : \mathrm{Ind}_{\{1\}}^{G}(K) &\longrightarrow L \\ \varphi &\longmapsto \sum_{\sigma\in G} \varphi(\sigma)\sigma(\alpha)\end{aligned}$$

is an isomorphism of G-modules, therefore using Shapiro's lemma (4.19), $H^r(G, L) \cong H^r(\{1\}, K) = 1$ for $r > 1$. □

4.5 Homology of Groups

Definition 4.32. Let G be a group and M a G-module, the set M_G is the largest quotient of M on which G acts trivially, that is, M_G is the quotient of M by the submodule generated by

$$\{gm - m \mid g \in G, m \in M\}. \tag{4.33}$$

△

Lemma 4.34. *The functor* $(\cdot)_G : \mathrm{Mod}_G \to \mathrm{Ab}$ *is right exact.*

Proof. Take the following exact sequence:

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

We will check that the following sequence is also exact:

$$M'_G \xrightarrow{f'} M_G \xrightarrow{g'} M''_G \longrightarrow 0.$$

If the function g is surjective, the function induced in M_G is also surjective. To check that the last sequence is exact in it's second position, take $[x] \in M_G$ □

Let G be a group and M be a $G-$module. Take a projective resolution $P^\bullet \to M$ of M. Note that the sequence

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \longrightarrow 0$$

is exact and as the functor $(\cdot)_G$ is right exact, the sequence:

$$\cdots \longrightarrow (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \xrightarrow{d_0} M_G \longrightarrow 0$$

is notnecessarily exact, so the sets

$$H_r(G, M) \coloneqq \frac{\mathrm{Ker}(d_r)}{\mathrm{Im}(d_{r+1})} \tag{4.35}$$

are not necessarily trivial. The set defined above in 4.35 is called *the r-th homology group of G with coefficients in M*. These groups have the following properties:

Remark 4.36. The homology groups are characterized by the following properties:

1. $H_0(G, M) = M_G$
2. If the P is projective, the sets $H_r(G, P) = 0$ for all r.
3. Let $P_\bullet \to M$ and $Q_\bullet \to N$ be two projetive resolutions of G-modules M and N, then any homomorphism $\alpha : M \to N$ of G-modules, extends to homomorphisms of groups $\alpha_2, \alpha_1, \dots$ such that the diagram:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M \\ & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha} \\ \cdots & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \longrightarrow & N \end{array}$$

   commutes. If the above property is applied to the identity map $I_M : M \to M$, then one can conclude that the groups $H_r(G, M)$ do dot depend of the choice of the projective resolution and therefore are well defined.

4. A short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

   induces a long exact sequence:

$$\cdots \to H_r(G, M) \to H_r(G, M'') \xrightarrow{\delta_r} H_{r-1}(G, M') \to \cdots \to H_0(G, M'') \to 0$$

We will now compute the group $H_1(G, \mathbb{Z})$ using only the properties listed above. Define the *augmentation map* as follows:

$$\begin{aligned} \mathbb{Z}[G] &\to \mathbb{Z} \\ \sum_g n_g g &\mapsto \sum_g n_g. \end{aligned}$$

And we define the *augmentation ideal* as the kernel of the augmentation map, this set will be denoted I_G. The reader can check tat the set I_G a free $\mathbb{Z}$-submodule with basis $\{g - 1 \mid g \in G,\ g \neq 1\}$ and therefore, the set $I_G M$ is the denominator in equation 4.35, so we now have

$$M/I_G M = M_G \cong H_0(G, M). \tag{4.37}$$

From the definition of I_G one has the following short exact sequence:

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

the second arrow is an inclusion and the third one is the augmentation map. From 4.36,(4) we have the following long exact sequence:

$$\cdots \to H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G]) \to \cdots. \tag{4.38}$$

Note that $\mathbb{Z}[G]$ is a projective G-module as it is a free $\mathbb{Z}[G]$-module, so the sets $H_r(G, \mathbb{Z}[G])$ are the trivial group (by 4.36 (2)). Now, taking $M = I_G$ and $M = \mathbb{Z}[G]$ in equation 4.37, we get $H_0(G, I_G) \cong {I_G}/{I_G}^2$ and $H_0(G, \mathbb{Z}[G]) \cong \mathbb{Z}[G]/I_G$. These facts turn the long exact sequence in equation 4.38 into the following exact sequence:

$$0 \to H_1(G, \mathbb{Z}) \to {I_G}/{I_G}^2 \to \mathbb{Z}[G]/I_G \to H_0(G, \mathbb{Z}) \to 0.$$

As the map in the middle is induced by the inclusion $I_G \hookrightarrow \mathbb{Z}[G]$, the map induced in the quotient is the zero map. And therefore the map:

$$H_1(G, \mathbb{Z}) \to {I_G}/{I_G}^2$$

is an isomorphism.

4.6 The Tate Groups

For this section, G will denote a finite group.

Definition 4.39. Let G be a finite group and M a G-module. The *norm map* $\mathrm{Nm}_G : M \to M$ is defined as follows:

$$m \mapsto \sum_{g \in G} gm.$$

△

Note that for any given $h \in G$, $h(\mathrm{Nm}_G(m)) = \mathrm{Nm}_G(m) = \mathrm{Nm}_G(hm)$ and therefore $\mathrm{Im}(\mathrm{Nm}_G(m)) \subset M^G$. Also, as $\mathrm{Nm}_G(gm - m) = 0$, one has

$I_G M \subseteq \mathrm{Ker}(\mathrm{Nm}_G)$. These properties induce the following exact commutative diagram:

$$\begin{array}{ccccccccc} & & & & M & \xrightarrow{\mathrm{Nm}_G} & M & & \\ & & & & \downarrow{\scriptstyle \text{quotient}} & & \uparrow & & \\ 0 & \longrightarrow & \mathrm{Ker}(\mathrm{Nm}_G)/I_G M & \hookrightarrow & M/I_G M & \longrightarrow & M^G & \twoheadrightarrow & M^G/\mathrm{Nm}_G(M) \longrightarrow 0 \end{array}$$

Where $M/I_G M \to M^G$, $[m] \mapsto \sum_{g\in G} gm$. To prove that this function is well defined, let $[m] = [n] \in M/I_G M$, then:

$$\begin{aligned} m &= n + (hl - l) \\ \sum_{g\in G} gm &= \sum_{g\in G} g(n + (hl - l)) \\ &= \sum_{g\in G} gn + \sum_{g\in G} g(hl - l) \\ &= \sum_{g\in G} gn + \sum_{g\in G} g(hl) - \sum_{g\in G} gl \\ &= \sum_{g\in G} gn + \sum_{g\in G} gl - \sum_{g\in G} gl \\ &= \sum_{g\in G} gn. \end{aligned}$$

Note that $H_0(G, M) = M/I_G M$ and $H^0(G, M) = M^G$, so the bottom row of the commutative diagram can be written as follows:

$$0 \to \mathrm{Ker}(\mathrm{Nm}_G)/I_G M \hookrightarrow H_0(G, M) \to H^0(G, M) \twoheadrightarrow M^G/\mathrm{Nm}_G(M) \to 0.$$

Using the above fact and remark 4.36, for any short exact sequence of G-modules, one has the diagram:

$$\begin{array}{ccccccccccc} \cdots \to H_1(G, M'') & \to & H_0(G, M') & \to & H_0(G, M) & \to & H_0(G, M'') & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \\ 0 \longrightarrow & & H^0(G, M') & \to & H^0(G, M) & \to & H^0(G, M'') & \to & H^1(G, M') \to \cdots, \end{array}$$

which, when applying the snake lemma transforms into the following sequence

$$\cdots \longrightarrow H_2(G,M'') \longrightarrow H_1(G,M') \longrightarrow H_1(G,M)$$
$$H_1(G,M'') \longrightarrow \operatorname{Ker}(\operatorname{Nm}_G)/I_G M' \to \operatorname{Ker}(\operatorname{Nm}_G)/I_G M \to \operatorname{Ker}(\operatorname{Nm}_G)/I_G M'' \xrightarrow{\delta}$$
$$\to M^G/\operatorname{Nm}_G(M') \to M^G/\operatorname{Nm}_G(M) \to M^G/\operatorname{Nm}_G(M'') \longrightarrow H^1(G,M')$$
$$H^1(G,M) \longrightarrow H^1(G,M'') \longrightarrow H^2(G,M') \longrightarrow \cdots.$$

We can write the above sequence as:

$$\cdots \to H_T^r\left(G,M'\right) \to H_T^r(G,M) \to H_T^r\left(G,M''\right) \to H_T^{r+1}(G,M) \to \cdots,$$

where:

$$H_T^r(G,M) \coloneqq \begin{cases} H^r(G,M) & r>0 \\ M^G/\operatorname{Nm}_G(M) & r=0 \\ \operatorname{Ker}(\operatorname{Nm}_G)/I_G M & r=-1 \\ H_{-r-1}(G,M) & r<-1, \end{cases}$$

the groups defined above are called the *Tate groups* of G with coefficients in M.

Proposition 4.40. *Let G be a cyclic group of finite order. A choice of a gnerator of G determines isomorphisms*

$$H^r(G,M) \xrightarrow{\cong} H_T^{r+2}(G,M).$$

Theorem 4.41 (Tate)**.** *Let G be a finite group and let C be a G-module. Suppose that for all subgroups $H \subseteq G$,*

- $H^1(H,C)=0$, *and*
- $H^2(H,C)$ *is a cyclic group of order equal to* $(H:1)$.

Then, for all r, there is an isomorphism

$$H_T^r(G,\mathbb{Z}) \to H_T^{r+2}(G,C)$$

depending only on the choice of a generator for $H^2(G,C)$.

Proposition 4.42. *Let M be a finite G-module with G a cyclic group, then*

$$\left|H_T^0(G,M)\right| = \left|H_T^1(G,M)\right|$$

Proof. Consider the following exact sequences:

$$0 \to M^G \to M \to^{g-1} M \to M_G \to 0$$

and

$$0 \to H_T^{-1}(G,M) \to M_G \xrightarrow{\mathrm{Nm}_G} M^G \to H_T^0(G,M) \to 0$$

where g is a generator of G. From the first exact sequence, $|M_G| = \left|M^G\right|$, and therefore from the second one one has the wanted result. □

Chapter 5

The Brauer Group of a Field

5.1 Lemmas on Algerbas

Let k be a field. All k-algebras considered in this section are unital, in particular we have a monomorphism $k \hookrightarrow A$ given by $x \mapsto 1x$

Definition 5.1. Let k be a field. A k-algebra is central if the center of A is the image of $k \hookrightarrow A$. △

Definition 5.2. For any given k-algebra A we denote by A^{op} the algebra obtained by reversing multiplication in A. △

Lemma 5.3. *Let A be a simple ring with unit. Let $M \subseteq A$ an ideal seen as right A-module, then A coincides with the biconmutant of M.*

Proof. Let $A' \coloneqq \mathrm{End}_A(M)$ now we can see M as a left A'-module. Let $A'' \coloneqq \mathrm{End}_{A'}(M)$, we take A'' as an algebra such that M is a right A''-module. Let $R : A \to A''$ be the natural homomorphism given by $mR(a) = ma$. R is injective because $R(1) = \mathrm{Id}_M$ and A doesn't have any non trivial two-sided ideals. $R(M)$ is a right side ideal of A'':

$$R(m)a'' = R(ma'')$$

for any $a'' \in A''$ and $m \in M$ because multiplication by any element in M represents an element in A'' and hence we have $(nm)a'' = m(ma'')$ for $n \in M$. Finally, as the product AM is a two-sided ideal, one must have $AM = A$ and therefore $R(A) = R(A)R(M)$, therefore $R(A)$ is a right ideal that contains the identity so $R(A) = A''$. □

Recall that a k-algebra is said to be finite if it is finite dimensional as a vector space over k.

Lemma 5.4. *Let A be a k-algebra. If A is finite, then:*

1. *A has a simple module.*
2. *Every non trivial A-module contains a simple A-module.*
3. *A simple A-module has finite dimension over k.*
4. *If M is a simple A-module, then $\mathsf{End}_A(M)$ is a skew-field.*

Proof. (1) is a direct consecuence of (2) because A is a non-zero module. To prove (2), any submodule of minimal degree over k is simple (as long as it has finite dimension). If M is simple, then $mA \subseteq M$ is a submodule and as A is finite and M is simple, we have (3). If M is simple, every non-zero element of $\mathsf{End}_A(M)$ is an isomorphism, therefore (4). □

Theorem 5.5 (Wedderburn)**.** *Let A be a finite simple k-algebra, then A is a matrix algebra over some skew field L that is also a k-algebra.*

Proof. Let $M \subseteq A$ be a simple submodule and define $L \coloneqq \mathsf{End}_A(M)$. By lemma 5.4, L is a skew field and by 5.3 we have $A = \mathsf{End}_L(M)$. As L is a skew field and M has finite dimension over k, M must be free and finite as right L-module, thus we conclude that $A \cong \mathbb{M}_{n\times n}\left(L^{\mathrm{op}}\right)$. □

Lemma 5.6. *Let A and A' be k-algebras. Let $B \subseteq A$ and $B' \subseteq A'$ subalgebras with centralizers C and C'. The centralizer of $B \otimes_k B'$ in $A \otimes_k A'$ is $C \otimes_k C'$.*

Proof. Let $C'' \subseteq A \otimes_k A'$ be the centralizer of $B \otimes_k B'$. Clearly $C \otimes_k C' \subseteq C''$. As each element of C'' commutes with $B \otimes_k 1$, we have $C'' \subseteq C \otimes_k A$. Similarly each elements of C'' commutes with $1 \otimes_k B$ and therefore $C'' \subseteq A \otimes_k C$. So we have

$$C'' \subseteq C \otimes_k A \cap A \otimes_k C' = C \otimes_k C'.$$

□

Lemma 5.7. *Let A be a k-algebra. Let L be a k-algebra that is also a skew field, then any ideal $I \subseteq A \otimes_k L$ can be written as $J \otimes_k L$ for some two sided $J \subseteq A$.*

Proof. Define $J := \{a \in A | a \otimes 1 \in I\}$. This is a two-sided ideal of A and $J \otimes_k L \subseteq I$. Let $w \in I$ such that $w = \sum^n a_i \otimes l_i$ is non zero and n is minimal. If $n = 1$, $(a \otimes l)l^{-1} \in I$ and therefore $(a \otimes l)l^{-1}l = a \otimes l \in I$. If $n > 1$, for any $c \in L$ we have $wc - cw = \sum_{i=1}^n a_i \otimes (l_i c - c l_i)$ if we assume $l_1 = -1$ (by right multiplying by l^{-1}) we have:

$$wc - cw = \sum_{i=2}^{n} a_i \otimes (l_i c - c l_i) \in I.$$

By by the minimality of n one must have $l_i c - c l_i = 0$ and therefore the l_i lie in the center of L, but the center of L is k so $w = (a_1 + \sum l_i a_i) \otimes 1$, contradicting the minimality of n. □

Lemma 5.8. *1. Let R be a ring, define $R_n := \mathbb{M}_n(R)$, every rwo sided ideal $J \subseteq R_n$ can be written as IR_n for some two-sided ideal $I \subseteq R$.*

2. The functors $M \mapsto M^{\oplus n}$ and $N \mapsto Ne_{11}$ define quasi-inverse equivalences between the categories $\mathbf{Mod}_R \leftrightarrow \mathbf{Mod}_{R_n}$.

Proof. If $J \subseteq R_n$ is a two-sided ideal, then $J = \bigoplus e_{ii} J e_{jj}$ where the elements of the direct sum are equal to each other and each of them is a two-sided ideal of R. Part (1) is clear. □

Lemma 5.9. *Let A and A' be two finite central k-algebras, then $A \otimes_k A'$ is simple.*

Proof. By 5.5, let $A' = \mathbb{M}_n(L)$ for some skew field L. The center of L is k and we conclude that $A \otimes L$ is simple by lemma 5.7. Finally, $A \otimes_k A' = \mathbb{M}_n(A \otimes_k L)$ is simple by 5.8. □

Lemma 5.10. *The tensor product of central finite simple k-algebras is central finite simple.*

Proof. This is clear by 5.6 and 5.9. □

Lemma 5.11. *Let A be a finite simple k-algebra. If $A = \mathbb{M}_n(K)$ with K a finite skew field extension of k, then $M := K^{\oplus n}$ is a simple A-module and $\mathbf{End}_A(M) = K^{op}$.*

Proof. Note that K is a simple K-module so its image under the equivalence defined in 5.8 must also be simple. Note also that $\mathbf{End}_A(M) = \mathbf{End}_K(K) = K^{\mathrm{op}}$. □

Lemma 5.12. *Let A be a finite central simple algebra over a field k. One has $A \otimes_k A^{op} \cong \mathbb{M}_n(k)$ where $n = [A : k]$.*

Proof. By Lemma 5.9, the algebra $A \otimes_k A^{\mathrm{op}}$ is simple. Therefore the map

$$A \otimes_k A^{\mathrm{op}} \longrightarrow \mathrm{End}_k(A),\ a \otimes a' \longmapsto (x \mapsto axa')$$

is injective (because is not null), and as both sides of the arrow have the same dimension, this function is an isomorphism. □

5.2 Morita Equivalence and the Brauer Group

Definition 5.13. Let k be a field. Let A and B be finite central simple k-algebras. We say that A and B are similar if there exist $n, m \in \mathbb{N}$ such that $\mathbb{M}_n(A) \cong \mathbb{M}_m(B)$. △

Lemma 5.14. *Morita equivalence.*

1. *Similarity defines an equivalence relation on the set of isomorphism classes of finite central simple algebras over k.*
2. *Every similarity class contains a unique (up to isomorphism) finite central skew field extension of k.*
3. *If $A = \mathbb{M}_n(K)$ and $B = \mathbb{M}_m K'$ for some finite central skew fields K, K' over k then A and B are similar if and only if $K \cong K'$ as k-algebras.*

Proof. Note that by Wedderburn's theorem (Theorem 5.5) we can always write a finite central simple algebra as a matrix algebra over a finite central skew field. Hence it suffices to prove the third assertion. To see this it suffices to show that if $A = \mathbb{M}_n(K) \cong \mathbb{M}_m K' = B$ then $K \cong K'$. To see this note that for a simple module M of A we have $\mathrm{End}_A(M) = K^{\mathrm{op}}$, see Lemma 5.11. Hence $A \cong B$ implies $K^{\mathrm{op}} \cong (K')^{\mathrm{op}}$. □

For any two finite simple central k-algebras A and B, the tensor product $A \otimes_k B$ is also finite simple and central (this can be easily proved using 5.6 and 5.9). Furthermore if A is similar to A', then $A \otimes_k B$ is similar to $A' \otimes_k B$ because taking tensor product and matrix algebra commute. Finally, the tensor product $A \otimes_k A^{\mathrm{op}}$ is isomorphic to a matrix algebra of k an therefore it belongs to the class of k.

Definition 5.15. The *Brauer group* of a field k is the abelian group of similarity classes of finite central simple k-algebras with the product $\otimes_k$ (the above discussion proves that this is in fact a group) and is denoted $\mathbf{Br}(k)$.

$\triangle$

Let $K : k$ be an algebraic extension, then the rule $A \mapsto A \otimes_k K$ defines a homomorphism $\mathbf{Br}(k) \to \mathbf{Br}(K)$. The kernel of this homomorphism is denoted $\mathbf{Br}(K : k)$ and provides a way to calculate a cohomology group:

Theorem 5.16. *Let $K : k$ be a finite Galois extension with Galois group G, there is an isomorphism:*

$$H^2(G, K^\times) \xrightarrow{\cong} \mathbf{Br}\,(K : k).$$

Chapter 6

Local Class Field Theory

So far, we have introduced enough theory to state the main theorems of local class field theory, however, some proofs are still outside the reach of this text.

6.1 Cohomology of Unramified Extensions

In this section, we will discuss the behaivior of unramified extentions of local fields. The term "local field" will refer to a locally compact field with respect to a nonarchimedean discrete absolute value (recall the notation introduced in 1.22).

Definition 6.1. Let $L : K$ be a Galois extension with Galois group G. The *norm* map is the function:

$$\begin{aligned} \mathrm{Nm}_{L:K} : L &\longrightarrow K \\ \alpha &\longmapsto \prod_{\sigma \in G} \sigma(\alpha). \end{aligned}$$

And the *trace* map:

$$\begin{aligned} \mathrm{Tr}_{L:K} : L &\longrightarrow K \\ \alpha &\longmapsto \sum_{\sigma \in G} \sigma(\alpha). \end{aligned}$$

Note that both of these functions are particular cases of the norm map defined in 4.39, with $L^\times$ seen as a multiplicative G-module for $\mathrm{Nm}_{L:K}$ and L seen as an additive G-module for $\mathrm{Tr}_{L:K}$. △

Lemma 6.2. *Let $L : K$ be a finite Galois unramified extension, then the maximal ideal of $\mathcal{O}_L$ can be generated by an element of $\mathcal{O}_K$.*

Proof. Let $\mathfrak{m}_K$ be the maximal ideal of $\mathcal{O}_K$, as $\mathfrak{m}_K$ is not ramified in $\mathcal{O}_L$, using theorem 1.11 one can write:

$$\mathfrak{m}_K \mathcal{O}_L = \mathfrak{m}_L,$$

where $\mathfrak{m}_L$ is the maximal ideal of $\mathcal{O}_L$, therefore any generator of $\mathfrak{m}_K$ also generates $\mathfrak{m}_L$. □

Lemma 6.3. *As in 1.22 let U_L be the group of units of $\mathcal{O}_L$, let $m > 0$ and define $U_L^{(m)} := 1 + \mathfrak{m}_L^m$. Then*

$$\begin{aligned} U_L / U_L^{(1)} &\xrightarrow{\cong} l^\times \\ U_L^{(m)} / U_L^{(m+1)} &\xrightarrow{\cong} l, \end{aligned} \tag{6.4}$$

where $l = \mathcal{O}_L / \mathfrak{m}_L$ is the residue field of L.

Proof. Let π be a generator of $\mathfrak{m}_K$ and $\mathfrak{m}_L$, which exist by 6.2, therefore $U_L^{(m)} = \{1 + a\pi^m \mid a \in O_L\}$ and the maps:

$$\begin{aligned} U_L &\longrightarrow l^\times \\ u &\longmapsto u \bmod \mathfrak{m}_L \end{aligned}$$

and

$$\begin{aligned} U_L^{(m)} &\longrightarrow l \\ 1 + a\pi^m &\longmapsto a \bmod \mathfrak{m}_L \end{aligned}$$

induce the isomorphisms. □

Lemma 6.5. *Let $L : K$ be a finite Galois unramified extension of local fields, with Galois group G and residue fields l and k, then for all r, $H_T^r(G, l^\times) = 0$, in particular the norm map $l^\times \to k^\times$ is surjective.*

Proof. By Hilbert's 90 (4.30), $H^1(G, l^\times) = 0$ and as $l^\times$ is finite, using 4.42, $H^2(G, l^\times) = 0$, which implies that all Tate groups are trivial by 4.40. □

Lemma 6.6. *Let $L : K$ be a finite Galois unramified extension of local fields, with Galois group G and residue fields l and k, then the cohomology groups satisfy $H_T^r(G, l) = 0$ for all r. In particular, the trace function is surjective.*

Proof. For $r > 0$, see 4.31, and by 4.40 the result holds for all r. □

Lemma 6.7. *Let $L : K$ be a finite Galois unramified extension, the norm map $\mathrm{Nm}_{L:K} : U_L \to U_K$ is surjective.*

Proof. One has the following commutative diagrams:

$$\begin{array}{ccc} U_L & \longrightarrow & l^\times \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Nm}} \\ U_K & \longrightarrow & k^\times \end{array} \qquad \begin{array}{ccc} U_L^{(m)} & \longrightarrow & l \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ U_K^{(m)} & \longrightarrow & k \end{array}$$

Let $u \in U_K$. As the norm map $l^\times \to k^\times$ is surjective, there is a $v_0 \in U_L$ such that $\mathrm{Nm}(v_0)$ and u have the same image in $k^\times$, hence the image of $u/\mathrm{Nm}(v_0)$ in $k^\times$ is 1 and therefore $u/\mathrm{Nm}(v_0) = 1 + a\pi$, which implies $u/\mathrm{Nm}(v_0) \in U_L^{(1)}$. In a similar fashion, as the trace map Tr is surjective, there exists $v_1 \in U_L^{(1)}$ such that $\mathrm{Nm}(v_1)$ and $u/\mathrm{Nm}(v_0)$ have the same image in k, hence $u/\mathrm{Nm}(v_0)\mathrm{Nm}(v_1) = u/\mathrm{Nm}(v_0v_1) \in U_K^{(2)}$. Continuing in the same way, one gets a sequence of elements $v_0 \in U_L^{(0)}, \ldots, v_i \in U_L^{(i)}$ such that $u/\mathrm{Nm}\,(v_0 \cdots v_i) \in U_K^{(i+1)}$. Define $v := \lim_{m\to\infty} \prod_{i=1}^m v_i$, then $u/\mathrm{Nm}(v) \in \bigcap_i U_K^{(i)} = \{1\}$, hence v is the preimage of u. □

Theorem 6.8. *Let $L : K$ be a finite Galois unramified extension with Galois group G, and let U_L be the group of units in L. Then*

$$H_T^r(G, U_L) = 0, \quad \textit{for all } r.$$

Proof. Let π be a generator of the maximal ideal of $\mathcal{O}_K$, which by lemma 6.2 can be chose to be in L. Then each element of $\alpha \in L^\times$ can be writen as $u\pi^n$, $u \in U_L, n \in \mathbb{Z}$, thus:

$$L^\times = U_L \cdot \pi^{\mathbb{Z}} \cong U_L \times \mathbb{Z}.$$

As $\pi \in K$, then for each $\sigma \in G$, $\sigma\alpha = \sigma(u\pi^n) = (\sigma u)\pi^n$, therefore the descomposition above is a descomposition of G-modules where G acts trivially on $\pi^{\mathbb{Z}} \cong \mathbb{Z}$. By proposition 4.17, $H^r(G, U_L)$ is a direct summand of $H^r(G, L^\times)$. By Hilbert's 90 (4.30), $H^1(G, L^\times) = 0$, and therefore $H^1(G, U_L) = 0$. As G is cyclic by proposition 1.24, using propositions 4.40 and lemma 6.7 the result is proven. □

6.2 Statements of the Main Theorems

Theorem 6.9. *Let K be a local field an K^{al} an algebraic closure, there exists an isomorphism*

$$\mathrm{inv}_K : H^2\left(\mathrm{Gal}\left(K^{al} : K\right), \left(K^{al}\right)^\times\right) \to \mathbb{Q}/\mathbb{Z},$$

called the invariant map and coming from the long cohomology sequence induce d by the short exact sequence of trivial G-modules $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, and if L is a finite extension of K with degree n, there is an isomorphism:

$$\mathrm{inv}_{L:K} : H^2(\mathrm{Gal}(L : K), L^\times) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Corollary 6.10. *The Brauer group of a local field is isomorphic to $\mathbb{Q}/\mathbb{Z}$.*

Let L be a Galois extension of K with Galois group G. The *fundamenal class* $u_{L:K}$ of the extension is the element of $H^2(\mathrm{Gal}(L : K), L^\times)$ such that

$$\mathrm{inv}_{L/K}\left(u_{L/K}\right) = \frac{1}{[L : K]} \bmod \mathbb{Z}.$$

the pair $(G, L^\times)$ satisfies the hypotesis of the Tate theorem (4.41), therefore one has:

Theorem 6.11 (Main theorem of local class field theory)**.** *Let $L : K$ be a finite Galois extensions of local fields, for all $r \in \mathbb{Z}$, there is an isomorphism*

$$H_T^r(\mathrm{Gal}(L : K), \mathbb{Z}) \xrightarrow{\cong} H_T^{r+2}\left(\mathrm{Gal}(L : K), L^\times\right),$$

defined by the rule $x \mapsto x \cup u_{L/K}$ (cup product), where $\mathbb{Z}$ is seen as a trivial $\mathrm{Gal}(L : K)$-module.

By taking $r = -2$, the main theorem provides a way to calculate the abelianized fundamental group of a given Galois extension of local fields, in terms of the arithmetic of the field itself (recall that the norm map can be calculated as a determinant without knowing the Galois group).

Theorem 6.12 (Local reciprocity law)**.** *Let $L : K$ be a finite Galois extension of local fields, there is an isomorphism:*

$$\mathrm{Gal}(L : K)^{ab} \xrightarrow{\cong} K^{\times} / \mathrm{Nm}_{L:K} L^{\times}.$$

Bibliography

[1] Tamás Szamuely, *Galois groups and fundamental groups*, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, Cambridge, 2009.

[2] Allen Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002. MR1867354

[3] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Student economy edition, Addison-Wesley Series in Mathematics, Westview Press, Boulder, CO, 2016.

[4] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[5] The Stacks Project Authors, *Stacks Project*, 2018.

[6] Jürgen Neukirch, *Algebraic number theory*, 1. Aufl. 1992. Nachdruck, Springer, 1999.

[7] J.S. Milne, *Algebraic Number Theory*, 2017.