MINISTRY OF EDUCATION
AND TRAINING

VIETNAM ACADEMY OF
SCIENCE AND TECHNOLOGY

GRADUATE UNIVERSITY OF SCIENCE AND TECHNOLOGY

Đinh Ngọc Tùng

CLASS FIELD THEORY

MASTER THESIS IN MATHEMATICS

Hanoi - 2024

MINISTRY OF EDUCATION AND TRAINING

VIETNAM ACADEMY OF SCIENCE AND TECHNOLOGY

GRADUATE UNIVERSITY OF SCIENCE AND TECHNOLOGY

Đinh Ngọc Tùng

CLASS FIELD THEORY

MASTER THESIS IN MATHEMATICS

Major: *Algebra and Number Theory*

Code: 8460104

ADVISOR:

Dr. Nguyễn Chu Gia Vượng

Hanoi - 2024

BỘ GIÁO DỤC
VÀ ĐÀO TẠO

VIỆN HÀN LÂM KHOA HỌC
VÀ CÔNG NGHỆ VIỆT NAM

HỌC VIỆN KHOA HỌC VÀ CÔNG NGHỆ

Đinh Ngọc Tùng

LÝ THUYẾT TRƯỜNG CÁC LỚP

LUẬN VĂN THẠC SĨ TOÁN HỌC

Ngành: *Đại số và lý thuyết số*

Mã số: 8460104

NGƯỜI HƯỚNG DẪN KHOA HỌC :

Tiến sĩ Nguyễn Chu Gia Vượng

Hà Nội - 2024

Declaration

I declare that this thesis titled “Local Class Field Theory” has been composed solely by myself and it has not been previously included in a thesis or dissertation submitted for a degree or any other qualification at this graduate university or any other institution. Wherever the works of others are involved, every effort is made to indicate this clearly, with due reference to the literature. I will take responsibility for the above declaration.

Hanoi, 14th August 2024
Signature of Student

Dinh Ngoc Tung

Acknowledgements

First, I would like to express my deepest gratitude to Dr.Nguyen Chu Gia Vuong for his support and encouragement throughout the two past years, and his advice and guidance on the topic of my thesis.

I am thankful to the Graduate University of Science and Technology and the Institute of Mathematics for giving me a chance to study here. Learning mathematics there helps me to meet more mathematicians and friends who share the same interests. Participating in seminars and lectures there always motivates me to understand and study more mathematics.

I extend my deepest appreciation to Dr.Nguyen Duy Tan for his unwavering support and guidance throughout this academic journey.

I am grateful to Professor Phung Ho Hai for his help and guidance, especially in my early years learning algebraic geometry. His lectures and seminars on algebraic geometry play a key role in my algebraic geometry knowledge.

I would like to express my gratitude towards mathematicians in the Institute of Mathematics who always do not hesitate to answer my questions and encourage me to pursue advanced mathematics.

I would like to extend my sincere gratitude to my friends, Dr.Vo Quoc Bao and Nguyen Quang Khai, for their unwavering support throughout the development of this thesis.

Finally, I am indebted to my family for an obvious reason.

Hanoi, 14th August 2024
Signature of Student

Dinh Ngoc Tung

Contents

Introduction

The arithmetic of number fields or local fields are related to the field's Galois extensions through Class Field Theory. The theory for abelian extensions was established by Kronecker, Weber, Hilbert, Takagi, Artin, and others approximately between 1850 and 1927. With the work of Langlands, nonabelian extensions only saw significant advancement for the first time roughly 25 years ago. The present thesis is motivated by [1] and mainly focus on results on local fields.
This thesis is divided into three chapters:

1. Chapter 1 is an introduction to the classical theory of cohomology of groups and Tate cohomology. We present the notion of cup-product, a family of bi-additive pairings $H_T^r(G, M) \times H_T^s(G, N) \to H_T^{r+s}(G, M \otimes N)$. In this chapter, We also present two important results: the Hilbert's theorem (also known as Satz 90) and the Tate's theorem. Main references of this chapter are [2], [3] and [4].

2. The main focus of Chapter 2 is the construction of the Local Artin map. We also present the Local Reciprocity Law theorem. Main references of this chapter are [5] and [6].

3. Chapter 3 is devoted to Lubin-Tate theory. We give a summary of Lubin and Tate's works on Local Class Field Theory, namely the construction of the Lubin-Tate group laws, the Local Kronecker-Weber theorem and the Existence Theorem. This chapter is based on [7] and [8].

The literature on class field theory is fairly large. But, for the reader's convenience, we suggest two additional references: [9] for basic notions on algebraic number theory and [10] for basic notions and results on local fields.

Chapter 1

Cohomology of groups

1.1 Introduction of the first chapter

In this chapter, we will introduce the theory of cohomology of groups. Throughout this chapter, unless otherwise stated, we consider an abstract group G. The letter G' denotes a subgroup of G.

In particular, at the beginning of this chapter, we will first introduce the notion of a G-module, a module structure on some abelian group A which is similar to the class of left $\mathbb{Z}G$-modules. In this context, we can form a category of G-modules that possesses all the characteristics common to ring modules (for example, it has enough projectives and injectives). Thus, by means of G-modules, we can also build some structure of G-cohomology ($H^m(G,-)$) and G-homology ($H_m(G,-)$) as usual. However, the main focus of this paper is on the zeroth, first, and second cohomology groups.

Once we understand the basic notions of G-cohomology and G-homology, we would need to explore their relationships and how they interact with each other. For any (sometimes required normal) subgroup G' of G, a G-module A also has a G'-module structure. Therefore, the cohomology groups $H^m(G,A)$ and $H^m(G',A)$ share some similar structure. In particular, there are some special homomorphisms that illustrate this relation, such as

$$\mathrm{Res}: H^m(G,A) \to H^m(G',A), \quad \mathrm{Cor}: H^m(G',A) \to H^m(G,A)$$

and

$$\mathrm{Inf}: H^m(G/G', A^{G'}) \to H^m(G,A)$$

In the middle of this chapter, the notion of Tate cohomology will be introduced. Furthermore, when we examine the structures of G-cohomology and G-homology groups, we will notice their similarities, but they seem too discrete to be connected. This is where we introduce John Tate's work on uniting these two concepts. By applying the snake lemma and the technique called dimensional shifting, we can connect all cohomology and homology groups in one long exact sequence

$$\cdots \to H_T^m(G,A') \to H_T^m(G,A) \to H_T^m(G,A'') \xrightarrow{\sigma} H_T^{m+1}(G,A') \to \dots, \quad m \in \mathbb{Z}$$

where $H_T^m(G,-)$ denotes the m-th Tate cohomology group, which generalizes the notion of usual G-cohomology.

The goal of all the concepts about group cohomology is to support the theory of class field theory on local fields. By the end of this chapter, we can view G as a Galois group of a finite

Galois extension E/K of a local field K. The Tate Theorem will help us understand the relation of the Tate cohomology of a finite group. In particular, if G and its G-module C satisfy some special conditions (which will be explored further in the next chapter as the Galois group), then essentially we have

$$H_T^m(G,\mathbb{Z}) \cong H^{m+2}(G,C)$$

which corresponds to the cup-product (another notion that will be introduced in this chapter as well) with the selected element $\gamma \in H^2(G,C)$. It is, technically, a restriction of the map

$$\smile: H^2(G,C) \times H^m(G,\mathbb{Z}) \to H^{m+2}(G,C)$$

on $\{\gamma\} \times H^m(G,\mathbb{Z})$.

1.2 Cohomology of groups

We present here the classical construction of cohomology of groups as derived functors.

1.2.1 The category of $G-$modules

Let us first define the objects of the category of $G-$modules.

Definition 1.2.1 ($G-$modules)
A $G-$module is an abelian group A (noted additively), with a map

$$G \times A \to A : (g,a) \mapsto ga$$

so that for every elements $g, g_1, g_2 \in G$ and $a, a_1, a_2 \in A$, we have

(i) $g(a_1 + a_2) = ga_1 + ga_2$*;*

(ii) $(g_1g_2)(a) = g_1(g_2a)$, $1a = a$.

Note that, a $G-$module is an abelian group A together with a group homomorphism $G \to \mathrm{Aut}(A)$, where $\mathrm{Aut}(A)$ is the group of group automophisms of A.

Example 1.2.2

a. *Every abelian group A can be considered as a $G-$module by $ga = a$ for all $g \in G$ and $a \in A$. From now, we call this action trivial.*

b. *Let A be the set of binary quadratic forms and let $G = \mathrm{SL}_2(\mathbb{Z})$ be the group of 2 by 2 matrices with integer coefficients of determinant 1. Define, for $f(x,y) = ax^2 + bxy + cy^2$ and $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$,*

$$(g \cdot f)(x,y) = f((x,y)g^T) = f(\alpha x + \beta y, \gamma x + \delta y),$$

where g^T denotes the transpose of g. We can easily check that this formula defines an action of G on M. Then A, with the above action, becomes a $G-$module.

c. *Let E/K be a Galois extension of fields with Galois group $G = \mathrm{Gal}(E/K)$. Then $(E,+)$ and $(E^\times, \times)$ are $G-$modules with the natural Galois actions.*

We now introduce the morphisms in the category of $G-$modules.

Definition 1.2.3 ($G-$homomorphisms)
Let A, B be two $G-$modules. A homomorphism of $G-$modules (or a $G-$homomorphism) from A to B is a group homomorphism which is compatible with the $G-$actions; in other words, a map $\alpha : M \to N$ satifies

(i) $\alpha(a_1 + a_2) = \alpha(a_1) + \alpha(a_2)$ *for all* $a_1, a_2 \in A$*;*

(ii) $\alpha(ga) = g(\alpha(a))$ *for all* $g \in G, a \in A$.

We shall denote the set of $G-$homomorphisms from A to B by $\mathrm{Hom}_G(A, B)$.

The $G-$modules together with $G-$homomorphisms form a category, denoted by Mod_G. Moreover, routine calculations show that it's an abelian category. This fact also follows from the classical interpretations of the category of $G-$modules as the category of modules over its group rings that we recall below.

We define $\mathbb{Z}G$ to be the free abelian group over G, that is

$$\mathbb{Z}G := \{\sum_i n_i g_i : n_i \in \mathbb{Z}; g_i \in G; n_i = 0 \quad \text{for all but finitely many } i\}.$$

We then define the multiplication on $\mathbb{Z}G$ by the formula:

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

The abelian group $\mathbb{Z}G$ equipped with this multiplication is a ring.

Furthermore, any $G-$module can be identified with a left $\mathbb{Z}G-$module and any $G-$homomorphism can be identified with a morphism of $\mathbb{Z}G-$modules. Thus, the category of modules over the ring $\mathbb{Z}G$ can be identified with the category Mod_G of $G-$modules. Recall that the category of modules over a fixed ring is an abelian categories with enough injectives and enough projectives. In particular, Mod_G is an abelian category which has enough projectives and injectives.

Remark 1.2.4 (The $G-$module $\mathrm{Hom}(A, B)$)
Let A and B be $G-$modules, the set $\mathrm{Hom}(A, B)$ *of abelian group homomorphisms is again an abelian group. We can turns* $\mathrm{Hom}(A, B)$ *into a $G-$module by defining the action of G as follows: for any* $\varphi \in \mathrm{Hom}(A, B)$ *and* $a \in A$,

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

1.2.2 Induction and induced modules

Note that every $G-$module has a natural $G'-$module structure defined by restriction. Similarly, any $G-$homorphism between two $G-$modules is naturally an $G'-$homomorphism. It follows that the restriction of the action of G to that of G' is a functor, called restriction from G to G', denoted by $\mathrm{Res}^G_{G'}$ from the category Mod_G to the category Mod'_G. It is evident that $\mathrm{Res}^G_{G'}$ is an additive, exact functor.

Now, we introduce anathor functor, which goes in the opposite direction.

Definition 1.2.5 (Induced modules)
Let A be a $G'-$module A. We denote by $\operatorname{Ind}_{G'}^{G}(A)$ the set of maps $\varphi : G \to A$ such that $\varphi(g'g) = g'\varphi(g)$ for all $g' \in G$ and $g \in G$. We equip $\operatorname{Ind}_{G'}^{G}(A)$ with the regular right action of G: for all $g \in G$ and $\varphi \in \operatorname{Ind}_{G'}^{G}(A)$, we define the element $g\varphi \in \operatorname{Ind}_{G'}^{G}(A)$ by the formula:

$$(g\varphi)(x) = \varphi(xg)$$

for all $x \in G$. Eventually, $\operatorname{Ind}_{G'}^{G}(A)$ turns into a $G-$module with structures

$$(\varphi + \varphi')(x) = \varphi(x) + \varphi'(x) \text{ and } (g\varphi)(x) = \varphi(xg)$$

. The set $\operatorname{Ind}_{G'}^{G}(A)$, which is an abelian group with the natural addition law, becomes a $G-$module.

Remark 1.2.6 (Induced homomorphisms)
We also note that a $G'-$homomorphism $\alpha : A \to A'$ induces a $G-$homomorphism

$$\varphi \mapsto \alpha \circ \varphi : \operatorname{Ind}_{G'}^{G}(A) \to \operatorname{Ind}_{G'}^{G}(A').$$

Let us check that $\operatorname{Ind}_{G'}^{G} : \operatorname{Mod}_{G'} \to \operatorname{Mod}_{G}$ is a functor:

(i) On objects, $\operatorname{Ind}_{G'}^{G} : A \mapsto \operatorname{Ind}_{G'}^{G}(A)$, sends a $G'-$module A to $\operatorname{Ind}_{G'}^{G}(A)$, a $G-$module.

(ii) On morphisms, $\operatorname{Ind}_{G'}^{G} : (\alpha : A \to A') \mapsto (\varphi \mapsto \alpha \circ \varphi : \operatorname{Ind}_{G'}^{G}(A) \to \operatorname{Ind}_{G'}^{G}(A'))$. Therefore,

$$\operatorname{Ind}_{G'}^{G} : \operatorname{id}_A \mapsto (\varphi \mapsto \operatorname{id}_A \circ \varphi : \operatorname{Ind}_{G'}^{G}(A) \to \operatorname{Ind}_{G'}^{G}(A)) \equiv \operatorname{id}_{\operatorname{Ind}_{G'}^{G}(A)}$$

and for $G'-$homomorphisms $f : A \to B$ and $g : B \to C$

$$\operatorname{Ind}_{G'}^{G} : (g \circ f : A \to C) \mapsto (\varphi \mapsto (g \circ f) \circ \varphi \equiv \varphi \mapsto g \circ (f \circ \varphi) : \operatorname{Ind}_{G'}^{G}(A) \to \operatorname{Ind}_{G'}^{G}(C))$$

which is $\operatorname{Ind}_{G'}^{G}(g) \circ \operatorname{Ind}_{G'}^{G}(f)$

Moreover, the functor $\operatorname{Ind}_{G'}^{G}$ is clearly additive.

The functors $\operatorname{Res}_{G'}^{G}$ and $\operatorname{Ind}_{G'}^{G}$ are actually adjoint, as shown in the next lemma.

Lemma 1.2.7

(a) *For any $G'-$module B and $G-$module A, we have a natural abelian group isomorphism*

$$\operatorname{Hom}_G(A, \operatorname{Ind}_{G'}^{G}(B)) \cong \operatorname{Hom}_{G'}(A, B),$$

where on the right hand side, for simplicity, we denote A in stead of $Res_{G'}^{G}(A)$ the module A, viewed as a $G'-$module.

(b) *The functor*

$$\operatorname{Ind}_{G'}^{G} : \operatorname{Mod}_{G'} \to \operatorname{Mod}_{G}$$

is exact.

Proof:

(a) For a $G-$homomorphism $\alpha : A \to \operatorname{Ind}_{G'}^{G}(B)$, we construct a map $\beta : A \to B$ by setting

$$\beta(a) = \alpha(a)(1_G).$$

Hence, for every $g \in G$,

$$\beta(ga) = (\alpha(ga))(1_G) = (g(\alpha(a)))(1_G) = \alpha(a)(g).$$

Since $\alpha(a) \in \operatorname{Ind}_{G'}^{G}(B)$, for $g \in G'$, $\alpha(a)(g) = g(\alpha(a)(1_G)) = g(\beta(a))$. Thus, β is a $G'-$homomorphism from $A \to B$. The map $\alpha \mapsto \beta$ is obviously a group homomorphism. Conversely, given a $G'-$homomorphism $\beta : A \to B$, we define α to be the map $A \to \operatorname{Ind}_{G'}^{G}(A)$ such that $\alpha(a)(g) = \beta(ga)$. Then α is a G homomorphism. We can check that the mappings $\alpha \mapsto \beta$ and $\beta \mapsto \alpha$ are mutually inverse, thus they are isomorphisms. Note that the constructions of α and β are natural.

(b) Now we will prove the exactness of $\operatorname{Ind}_{G'}^{G}$. Consider a $G'-$exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

We have to show that

$$0 \to \operatorname{Ind}_{G'}^{G}(A) \xrightarrow{\operatorname{Ind}_{G'}^{G}(f)} \operatorname{Ind}_{G'}^{G}(B) \xrightarrow{\operatorname{Ind}_{G'}^{G}(g)} \operatorname{Ind}_{G'}^{G}(C) \to 0$$

is an $G-$exact sequence.

(i) The exactness at $\operatorname{Ind}_{G'}^{G}(A)$ is obvious: since f is injective, it's evident that the map $\operatorname{Ind}_{G'}^{G}(f) : \varphi \mapsto f \circ \varphi$ is also injective.

(ii) Exactness at $\operatorname{Ind}_{G'}^{G}(B)$.

$$\begin{aligned}
\operatorname{Ker}\operatorname{Ind}_{G'}^{G}(g) &= \{\varphi \in \operatorname{Ind}_{G'}^{G}(B) : g \circ \varphi \equiv 0\} \\
&= \{\varphi \in \operatorname{Ind}_{G'}^{G}(B) : g(\varphi(x)) = 0_C \ \forall x \in G\} \\
&= \{\varphi \in \operatorname{Ind}_{G'}^{G}(B) : \varphi(x) \in \operatorname{Ker}(g) \ \forall x \in G\} \\
&= \{\varphi \in \operatorname{Ind}_{G'}^{G}(B) : \varphi(x) \in \operatorname{Im}(f) \ \forall x \in G\} \\
&= \{\varphi \in \operatorname{Ind}_{G'}^{G}(B) : \varphi(x) = f(a) \text{ for some } a \in A,\ \forall x \in G\}.
\end{aligned}$$

Now for such φ, we fix a $a_x \in A$ such that $\varphi(x) = f(a_x)$ we define φ' as $\varphi'(x) = a_x$ for every $x \in G$. Hence, for all $x' \in G'$ and $x \in G$

$$f(a_{g'x}) = \varphi(g'x) = g'\varphi(x) = g'f(a_x) = f(g'a_x).$$

This implies $\varphi'(g'hx) = a_{g'x} = g'a_x = g'\varphi'(x)$ since f is injective. Thus, $\varphi'(x) \in \operatorname{Ind}_{G'}^{G}(A)$ and $\varphi = f \circ \varphi'$. In other words, $\varphi \in \operatorname{Im}\operatorname{Ind}_{G'}^{G}(f)$ or $\operatorname{Ker}\operatorname{Ind}_{G'}^{G}(g) \subset \operatorname{Im}\operatorname{Ind}_{G'}^{G}(f)$. The proof for the inclusion $\operatorname{Ker}\operatorname{Ind}_{G'}^{G}(g) \supset \operatorname{Im}\operatorname{Ind}_{G'}^{G}(f)$ is similar.

(iii) Exactness at $\operatorname{Ind}_{G'}^{G}(C)$. Let $G = \cup_{s\in S} G's$ where S is a set of representatives of the $G'-$ right cosets. Take any $\varphi \in \operatorname{Ind}_{G'}^{G}(C)$. For every $s \in S$, we choose an element $n(s) \in B$ that maps to $\varphi(s) \in C$ and define $\varphi'(g's) = g'n(s)$. We can check that $\varphi' \in \operatorname{Ind}_{G'}^{G}(B)$ and maps to φ.

□

One interesting feature of the induction functor lies in the following lemma.

Lemma 1.2.8
Let G be a group and a subgroup G' of finite index in G. The functor $\operatorname{Ind}_{G'}^{G} : \operatorname{Mod}_{G'} \to \operatorname{Mod}_G$ preserves injectives.

Proof: Let B be an injective $G'-$module. Then the functor $\operatorname{Hom}_{G'}(-, B)$ from $\operatorname{Mod}_{G'}$ to **Ab** (the category of abelian groups) is exact. By Lemma 1.2.7, we have a natural isomorphism between the functors $\operatorname{Hom}_G(-, \operatorname{Ind}_{G'}^{G}(B))$ and $\operatorname{Hom}_{G'}(-, B)$. Therefore the functor $\operatorname{Hom}_G(-, \operatorname{Ind}_{G'}^{G}(B))$ from Mod_G to **Ab** is also exact. Hence $\operatorname{Ind}_{G'}^{G}(B)$ is an injective $G-$module and therefore $\operatorname{Ind}_{G'}^{G}$ preserves injectives. □

When $G' = \{1_G\}$, an $G'-$module is simply an abelian group. In this scenario, we use the notation Ind^G instead of $\operatorname{Ind}_{G'}^{G}$. Therefore, we get the following homomorphisms of abelian groups

$$\operatorname{Ind}^G(A_0) = \{\varphi : G \to A_0\} = \operatorname{Hom}(\mathbb{Z}G, A_0).$$

Definition 1.2.9 (Induced $G-$modules)
A $G-$module A is deemed induced if it is isomorphic to $\operatorname{Ind}^G(A_0)$ for a certain abelian group A_0.

Remark 1.2.10 (Induced modules of finite groups)
Let's consider the case when G is a finite group. Recall that every abelian group has a natural $\mathbb{Z}-$module structure.

(a) *A $G-$module A is induced iff there exists an abelian group $A_0 \subset A$ so that*

$$A = \bigoplus_{g \in G} gA_0,$$

whereby there is an $G-$isomorphism

$$\varphi \mapsto \sum_{g \in G} g \otimes \varphi(g^{-1}) : \operatorname{Ind}^G(A_0) \to \mathbb{Z}G \otimes_{\mathbb{Z}} A_0$$

Where $\mathbb{Z}G \otimes_{\mathbb{Z}} A_0$ is a $G-$module by the structure $g(z \otimes a) = gz \otimes a$.

(b) *Let G' be a subgroup of G. An induced $G-$module, restricted to G', is also an induced $G'-$module.*

(c) *For a $G-$module A, if we refers to A_0 as A, considered as an abelian group, then*

$$\pi : \operatorname{Ind}^G(A_0) \to A, \ \varphi \mapsto \sum_{g \in G} g\varphi(g^{-1})$$

is a surjective $G-$homomorphism. It corresponds to the map

$$\mathbb{Z}G \otimes A_0 \to A, \ (\sum n_g g) \otimes a \mapsto \sum n_g ga.$$

Remark 1.2.11 (Tensor products of $G-$modules)
For two $G-$modules A and B, the operation

$$g(a\otimes b)=(ga)\otimes(gb)$$

defines $A\otimes_{\mathbb{Z}}B$ as a $G-$module. If A_0 refers to A as an abelian group then $\mathbb{Z}G\otimes_{\mathbb{Z}}A=\mathbb{Z}G\otimes_{\mathbb{Z}}A_0$ as abelian groups but not as $G-$modules. However,

$$g\otimes a\mapsto g\otimes ga:\mathbb{Z}G\otimes_{\mathbb{Z}}A_0\xrightarrow{\cong}\mathbb{Z}G\otimes_{\mathbb{Z}}A$$

is a $G-$isomorphism.

1.2.3 The cohomology $H^m(G,-)$

For any $G-$module A, we define its $G-$ fixed elements (or $G-$invariants)

$$A^G=\{a\in A:ga=a;\forall g\in G\}.$$

It is obvious that A^G is an abelian subgroup of A. Note that if $f:A\to B$ is a $G-$homomorphism then f sends any $G-$fixed element of A to a $G-$fixed element of B, thus induces a morphism of abelian groups: $A^G\to B^G$. In particular, the previous discussion show that $(-)^G:\mathrm{Mod}_G\to\mathrm{Ab}$ is a functor.

Lemma 1.2.12
The functor $(-)^G:\mathrm{Mod}_G\to\mathrm{Ab}$ is isomorphic to the functor $\mathrm{Hom}_G(\mathbb{Z},-)$. As a consequence, it is a left exact functor.

Proof: The functor $\mathrm{Hom}_G(\mathbb{Z},-):\mathrm{Mod}_G\to\mathrm{Ab}$ corresponds to the functor $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z},-):\mathbb{Z}G-\mathrm{Mod}\to\mathrm{Ab}$ which is a well-known left exact functor. Thus, we only need to prove that $(-)^G\cong\mathrm{Hom}_G(\mathbb{Z},-)$. Consider the natural transformation

$$\mu:\mu_A(A^G):A^G\to\mathrm{Hom}_G(\mathbb{Z},A),\ a\mapsto(1\mapsto a),$$

each μ_A is an isomorphism $A^G\to\mathrm{Hom}_G(\mathbb{Z},A)$. This implies the two functors are isomorphic. □

Definition 1.2.13 (The cohomology groups)
Let A be $G-$module. The functor $(-)^G:\mathrm{Mod}_G\to\mathrm{Ab}$ is left exact. Moreover, the category Mod_G has enough injectives. So it has right derived functors that we recall the constructions below. Let's choose an injective resolution (I^n) of A:

$$0\to A\to I^0\xrightarrow{d^0}I^1\xrightarrow{d^1}I^2\xrightarrow{d^2}\dots$$

By applying the functor $(-)^G$, we get the complex $(-)^G(I^n)$ of abelian groups:

$$0\xrightarrow{d^{-1}}(I^0)^G\xrightarrow{d^0}(I^1)^G\to\dots\xrightarrow{d^{r-1}}(I^r)^G\xrightarrow{d^r}(I^{r+1})^G\to\dots$$

For a non negative integer m, we define the m^{th} cohomology group of G with coefficients in A as

$$H^m(G,A):=\frac{\mathrm{Ker}(d^m)}{\mathrm{Im}(d^{m-1})}.$$

The abelian groups $H^m(G,A)$, $m=0,1,\dots,$ do not depend on the choice of (I^n).

Remark 1.2.14

1. *We have $H^0(G,A) = A^G$. Indeed, since $(-)^G$ is left exact,*

$$0 \to A^G \to (I^0)^G \xrightarrow{d^0} (I^1)^G$$

is exact, hence $H^0(G,A) = \frac{\operatorname{Ker} d^0}{\operatorname{Im} d^{-1}} = \operatorname{Ker} d^0 = A^G$.

2. *$H^m(G,I) = 0$ for all $m > 0$ if I is injective. This fact follows from the fact that for such a $G-$module, we always have a simple injective resolution*

$$0 \to I \to I \to 0 \to \dots$$

3. *Consider two injective resolutions of $G-$module $A \to (I^n)$ and $B \to (J^n)$. Any $G-$hormomorphism $\alpha : A \to B$ extends to a map of complexes:*

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\alpha"'] & (I^n) \arrow[d, "\alpha^\star"] \\
B \arrow[r] & (J^n)
\end{tikzcd}$$

and the homomorphisms between two cohomology groups:

$$H^m(\alpha^\star) : H^m(I^n) \to H^m(J^n)$$

are not dependent of the way we choose of $\alpha^\star$. Moreover, there are functors $A \to H^m(G,A) : \mathrm{Mod}_G \to \mathrm{Ab}$, called the right derived functors of $(-)^G$.

4. *Every $G-$exact sequence:*

$$0 \to A \to A' \to A'' \to 0$$

induces a long exact sequence of abelian groups

$$0 \to H^0(G,A') \to \dots \to H^m(G,A) \to H^m(G,A'') \xrightarrow{\delta^m} H^{m+1}(G,A') \to \dots$$

As we mentioned before, for a $G-$module A

$$\mathrm{Hom}_G(\mathbb{Z}, A) \cong A^G.$$

Lemma 1.2.15 (Shapiro's)
If $G' \le G$ and B be a $G'-$module, then we get natural homomorphisms

$$H^m(G, \mathrm{Ind}_{G'}^G(B)) \cong H^m(G', B)$$

for every $m \ge 0$.

Proof: In the case $m = 0$, the isomorphism is the composite:

$$B^{G'} \cong \mathrm{Hom}_{G'}(\mathbb{Z}, B) \cong \mathrm{Hom}_G(\mathbb{Z}, \mathrm{Ind}_{G'}^G(B)) \cong \mathrm{Ind}_{G'}^G(B)^G,$$

where the second isomorphism is given by Lemma 1.2.7. Recall that the functor $\mathrm{Ind}_{G'}^G : \mathrm{Mod}_{G'} \to \mathrm{Mod}_G$ is exact and preserves injectives. Consider an injective resolution $B \to (I^n)$ of B. We apply the functor $\mathrm{Ind}_{G'}^G$ to get an injective resolution $\mathrm{Ind}_{G'}^G(B) \to \mathrm{Ind}_{G'}^G(I^n)$. Hence,

$$H^m(G, \mathrm{Ind}_{G'}^G(B)) = H^m((\mathrm{Ind}_{G'}^G(I^n))^G) \cong H^m((I^n)^{G'}) = H^m(G', B).$$

□

This leads to an obvious consequence:

Corollary 1.2.16
Let A be an induced $G-$module i.e. $A = \mathrm{Ind}^G(A_0)$ then $H^m(G, A) = 0$ for all $m > 0$.

Remark 1.2.17

a) *Consider the exact sequence of $G-$module*

$$0 \to A \to C \to B \to 0.$$

If $H^m(G, C) = 0$ for every $m > 0$, then the following exact sequence is formed from the cohomology sequence .

$$0 \to A^G \to C^G \to A^G \to H^1(G, A) \to 0,$$

and the isomorphisms:

$$H^m(G, B) \xrightarrow{\cong} H^{m+1}(G, A),\ m > 0$$

b) *In general, the long exact sequence*

$$0 \to A \to C^1 \to \cdots \to C^n \to B \to 0$$

so that $H^m(G, C^i) = 0$ for every $m, i > 0$ specifies isomorphisms

$$H^m(G, B) \xrightarrow{\cong} H^{m+n}(G, A),\ \textit{for all}\, m \geq 1.$$

We divide the sequence into short, exact sequences in order to demonstrate this.

$$0 \to A \to C^1 \to B^1 \to 0,$$

$$0 \to B^1 \to C^2 \to B^2 \to 0,$$

$$0 \to B^{n-1} \to C^n \to B \to 0,$$

and obtain the isomorphisms

$$H^m(G, B) \cong H^{m+1}(G, B^{n-1}) \cong H^{m+2}(G, B^{n-2}) \cong \ldots$$

c) *Let*

$$0 \to A \xrightarrow{\epsilon} C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \to \ldots$$

be an exact sequence so that $H^m(G, J^n) = 0$ for every $n > 0$ and every $m \geq 0$. Then

$$H^m(G, A) = H^m((J^n)^G).$$

1.2.4 The cohomology group by means of cochains

We consider P_m $(m \geq 0)$ to be the free $\mathbb{Z}-$module with the $(m+1)-$ tuples $(g_0, \dots, g_m) \in G \times G \times \dots \times G$ as its basis, within the action of G:

$$g(g_0, \dots, g_m) = (gg_0, \dots, gg_m).$$

P_m is the free $\mathbb{Z}G-$module with basis $\{(1, g_1, \dots, g_m) | g_i \in G\}$ as well. We can define a $G-$homomorphism $d_m : P_m \to P_{m-1}$ By the rule

$$d_m(g_0, \dots, g_m) = \sum_{i=0}^{m} (-1)^i (g_0, \dots, \cancel{g_i}, \dots, g_m),$$

we define a homomorphism $d_m : P_m \to P_{m-1}$, where the g_i position is omitted. In other words, $(g_0, \dots, \cancel{g_i}, \dots, g_m)$ becomes a m-tuple. Let (P_n) be

$$\cdots \to P_m \xrightarrow{d_m} P_{m-1} \to \cdots \to P_0.$$

Lemma 1.2.18
The sequence defined by $\cdots \to P_m \xrightarrow{d_m} P_{m-1} \to \cdots \to P_0$ *forms a complex.*

Proof: We only need to check that $d_{m-1} \circ d_m = 0$. To avoid the confusion, let $m = 4$ and $(g_0, g_1, g_2, g_3, g_4)$ be an element in the basis of P_4. By the definition of d_4,

$$d_4(g_0, g_1, g_2, g_3, g_4) = (g_1, g_2, g_3, g_4) - (g_0, g_2, g_3, g_4) + (g_0, g_1, g_3, g_4) - (g_0, g_1, g_2, g_4) + (g_0, g_1, g_2, g_3)$$

then $d_3 \circ d_4(g_0, g_1, g_2, g_3, g_4) = (g_2, g_3, g_4) - (g_1, g_3, g_4) + (g_1, g_2, g_4) - (g_1, g_2, g_3) + \dots = 0$. For arbitrary $r \geq 0$. Note that the coefficient of $(g_0, \dots, \cancel{g_i}, \dots, \cancel{g_j}, \dots, g_m)$ is $(-1)^{i+1}(-1)^j + (-1)^{j+1}(-1)^{i+1} = 0$ (the first coefficient is from canceling g_i first and then g_j, the second coefficient is from canceling g_j first and then g_i). □

Lemma 1.2.19
The complex $(P_m) \xrightarrow{\varepsilon} \mathbb{Z} \to 0$ *is exact. Where* $\varepsilon : P_0 \to \mathbb{Z}$ *sends every basis element to* 1.

Proof: For a fixed $g \in G$, we define $k_m : P_m \to P_{m+1}$ by

$$k_m(g_0, \dots, g_m) = (g, g_0, \dots, g_m).$$

We will check that $d_{m+1} \circ k_m + k_{m-1} \circ d_m = 1$. Hence, if $d_m(x) = 0$, then $x = d_{m+1}(k_m(x))$. Let $(g_0, g_1, \dots, g_m)$ be a given basis element of P_m. We only need to prove that

$$(d_{m+1} \circ k_m + k_{m-1} \circ d_m)(g_0, g_1, \dots, g_m) = (g_0, g_1, \dots, g_m).$$

This is just straightforward implied from

$$(d_{m+1} \circ k_m)(g_0, g_1, \dots, g_m) = \sum_{i=-1}^{m} (-1)^{i+1} (g_{-1}, g_0, \dots, \cancel{g_i}, \dots, g_m)$$

where $g_{-1} = g$ and

$$(k_{m-1} \circ d_m)(g_0, g_1, \dots, g_m) = \sum_{i=0}^{m} (-1)^i (g, g_0, \dots, \cancel{g_i}, \dots, g_m).$$

□

Proposition 1.2.20
For any $G-$module A,

$$H^m(G, A) \cong H^m(\mathrm{Hom}_G((P_m), A)).$$

Proof: Note that the category of $G-$module Mod_G has enough projectives and injectives. For a $G-$module M, the functor $\mathrm{Hom}(\mathbb{Z}, -)$ and $H^0(G, -)$ are the same. Thus, their right derived functors also agree:

$$\mathrm{Ext}^m_G(\mathbb{Z}, A) \cong H^r(G, A).$$

Thus, we can choose a projective resolution of $\mathbb{Z}$ and define $H^m(G, A)$. □

Remark 1.2.21

1. *Any $\overline{\varphi} \in \mathrm{Hom}(P_m, A)$ can be viewed the same as $\varphi : G^{m+1} \to A$ and φ is invariant by the action of G iff*
$$\varphi(gg_0, \dots, gg_m) = g(\varphi(g_0, \dots, g_m)).$$
2. $\mathrm{Hom}_G(P_m, A)$ *is the same with $\tilde{C^r}(G, A)$ of φ's satisfying above conditions, which we may denote by $\tilde{C^r}(G, A)$.*
3. *The homomorphism d_{m+1} induced the boundary map $\tilde{d^m} : \tilde{C}^m(G, A) \to \tilde{C}^{m+1}(G, A)$. In particular,*
$$(\tilde{d^m}\varphi)(g_0, \dots, d_{m_1}) = \sum (-1)^i \varphi(g_0, \dots, \cancel{g_i}, \dots, g_{m+1}).$$
4. *On applying Proposition 1.2.20, we can say that:*
$$H^m(G, A) \cong \frac{\mathrm{Ker}(\tilde{d^m})}{\mathrm{Im}(\tilde{d}^{m-1})}.$$

Definition 1.2.22 (Group of inhomogeneous $m-$cochain of G with value in A)
The group $C^m(G, A)$ consisting of all maps $\varphi : G^m \to A$ is said to be group of inhomogeneous $m-$cochain of G with value in A. We consider $G^0 = \{1_G\}$ sao $C^0(G, A) = A$. Define

$$d^m : C^m(G, A) \to C^{m+1}(G, A).$$

by

$$(d^m\varphi)(g_1, \dots, g_{m+1}) = g_1\varphi(g_2, \dots, g_{m+1}) + \sum_{j=1}^{m} (-1)^j \varphi(g_1, \dots, g_j g_{j+1}, \dots, g_{m+1}) + (-1)^{m+1}\varphi(g_1, \dots, g_m).$$

Let $Z^m(G, A) = \mathrm{Ker}(d^m)$ be the group of $m-$cocycles and $B^m(G, A) = \mathrm{Im}(d^{m-1})$ be the group of $m-$coboundaries.

Proposition 1.2.23
The following sequence is a complex:

$$C^0(G,A) \xrightarrow{d^0} C^1(G,A) \xrightarrow{d^1} \dots \xrightarrow{d^{m-1}} C^m(G,A) \xrightarrow{d^m} \dots$$

Furthermore,

$$H^m(G,A) \cong \frac{Z^m(G,A)}{B^m(G,A)}.$$

Proof: For any $\varphi \in \tilde{C}^m(G,A)$, we say

$$\varphi'(g_1,\dots,g_m) := \varphi(1, g_1, g_1g_2, \dots, g_1\dots g_m).$$

The map $\varphi \mapsto \varphi' : \tilde{C}^m(G,A) \to C^m(G,A)$ is a bijection. □

Example 1.2.24 (Crossed homomorphism and normalized 2−cocyle)

1. *We say $\varphi : G \to A$ to be a cross homomorphism if it satisfies*

$$\varphi(\sigma\tau) = \sigma\varphi(\tau) + \varphi(\tau),\ \forall \tau, \sigma \in G.$$

2. *For every $a \in A$, the map $\sigma \mapsto \sigma a - a$ is a crossed homomorphism and we call it a principal crossed homomorphism. Hence,*

$$H^1(G,A) = \frac{\text{“ } G\text{−module of all crossed homomorphism ”}}{\text{“its submodule of all principal crossed homomorphisms”}}.$$

3. *In the case G acts trivially on A, a crossed homomorphism is said to be a homomorphism $G \to A$ and principal crossed homomorphisms are trivial as well. Therefore,*

$$H^1(G,A) \cong \mathrm{Hom}(G,A).$$

4. *Let A be a $G-$module. For $a \in A$, let $\varphi_a : G \to A$ be the constant map $\sigma \mapsto a$. Then*

$$(d^1\varphi_a)(\sigma,\tau) = \sigma a - a + a = \sigma a.$$

In particular, $(d^1\varphi_a)(1,1) = a$. Hence, every class in $H^2(G,A)$ is represented by a $2-$cocycle φ with $\varphi(1,1) = 0$. Such a $2-$cocycle is said to be normalized.

5. *Let $\varphi : G \to A$ be a crossed homomorphism. For every $\sigma \in G$:*

$$\varphi(\sigma^f) = \sigma^{f-1}\varphi(\sigma) + \dots + \sigma\varphi(\sigma) + \varphi(\sigma).$$

Thus, if $G = \langle\sigma\rangle$ with order f then a crossed homomorphism φ is defined by its value (say a) on σ such that:

$$\sigma^{f-1}a + \dots + \sigma a + a = 0.$$

Conversely, if $a \in A$ satisfies such equation, the map $\varphi(\sigma^i) = \sigma^{i-1}a + \dots + \sigma a + a$ determines a homomorphism $\varphi : G \to A$ and

$$\varphi \text{ is principal} \Leftrightarrow a = \sigma x - x \text{ for some } x \in A.$$

6. *Let* $\mathrm{Nm} : A \to A, a \mapsto \sum_{\sigma \in G} \sigma a$ *and* $\sigma - 1 : A \to A, m \mapsto \sigma a - a$*. When* G *is cyclic with* $|G| < \infty$*, the map* $\varphi \mapsto \varphi(\sigma)$ *induces*

$$H^1(G, A) \overset{\cong}{\to} \frac{\mathrm{Ker}(\mathrm{Nm}_G)}{(\sigma - 1)a}.$$

7. *Consider an* $G-$*exact sequence:* $0 \to A \to B \to C \to 0$*. The boundary map*

$$\delta^r : H^m(G, C) \to H^{m+1}(G, A)$$

can be described as follows: Take any $\gamma \in H^m(G, C)$ *be represented by the* $m-$*cochain* $\varphi : G^m \to C$*; since* $B \to C \to 0$*, there is an* $m-$*cochain* $\tilde{\varphi} : G^m \to B$ *lifting* φ*;* $d\tilde{\varphi}$ *(which takes value in* A*) is the cocycle representing* $\delta^m \gamma$

1.2.5 The cohomology group of Galois extension field E and $E^\times$

Let E/K be the Galois extension such that $G = \mathrm{Gal}(E/K)$ is finite. Both E (under addition) and $E^\times$ are $G-$modules.

Lemma 1.2.25 (Dedekind)
Let E *be a field,* G' *be a group and* $f_1, \dots, f_n$ *be distinct homomorphisms* $G' \to L^\times$*. Then they are* $E-$*linearly independent.*

Proof: Let $n \geq 2$ be the minimal number such that there exists n distinct $E-$linearly dependent homomorphisms. Suppose

$$\alpha_1 f_1(h) + \cdots + \alpha_n f_n(h) = 0 \ \forall h \in G'$$

for $\alpha_n \neq 0$. Because f_1 and f_n are distinct, there exist $h_1 \in G'$ such that $f_1(h_1) \neq f_n(h_1)$. Hence,

$$0 = \alpha_1 f_1(h_1 h) + \cdots + \alpha_n f_n(h_1 h) = \alpha_1 f_1(h_1) f_1(h) + \dots \alpha_n f_n(h_1) f_n(h).$$

However,

$$\alpha_1 f_1(h_1) f_1(h) + \cdots + \alpha_n f_1(h_1) f_n(h) = 0.$$

Therefore, $\alpha_2(f_1(h_1) - f_2(h_1)) f_2(h) + \dots \alpha_n(f_1(h_1) - f_n(h_1)) f_n(h) = 0$ for all $h \in G'$ where $\alpha_n(f_1(h_1) - f_n(h_1)) \neq 0$. This means $f_2, \dots, f_n$ are $E-$linearly dependent, a contradiction to the minimality of n. ■

Theorem 1.2.26 (Hilbert's 90)

$$H^1(G, E^\times) = 0.$$

Proof: Recall that:

$$H^1(G, E^\times) = \frac{\{\text{crossed homomorphisms } G \to L^\times\}}{\{\text{principal crossed homomorphisms}\}}.$$

we need to show that every crossed homomorphism is principal. Let $\varphi : G \to E^\times$ be a crossed homomorphism:

$$\varphi(\sigma\tau) = \sigma\varphi(\tau).\varphi(\sigma), \ \forall \sigma, \tau \in G.$$

By Lemma 1.2.25, there exists $a \in E^\times$ so that

$$0 \neq \sum_{\sigma \in G} \varphi(\sigma).\sigma a = b.$$

Then

$$\tau b = \sum_{\sigma \in G} \tau\varphi(\sigma).\tau\sigma a = \sum_{\sigma \in G} \varphi^{-1}(\tau)\varphi(\tau\sigma).\tau\sigma a = \varphi(\tau)^{-1} b.$$

Hence,

$$\frac{\tau(b^{-1})}{b^{-1}} = \frac{b}{\tau b} = \varphi(\tau).$$

□

Corollary 1.2.27
In the case E/K is a cyclic extension, $G = \mathrm{Gal}(E/K)$ generated by σ. If $\mathrm{Nm}_{E/K}\, a = 1$ then $a = \frac{\sigma b}{b}$ for some b.

Proof: This is implied directly by the fact

$$H^1(G, E^\times) = \mathrm{Ker}(\mathrm{Nm}_G)/(\sigma - 1)E^\times.$$

□

Example 1.2.28
Let $K = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{-7})$. The Galois group $G = Gal(E/\mathbb{Q})$ is cyclic and moreover $|G| = 2$, and the non-trivial automorphism σ is given by:

$$\sigma(\sqrt{-7}) = -\sqrt{-7}.$$

Since $G = Gal(E/\mathbb{Q})$ is cyclic, the action of the automorphism σ on E is:

$$\sigma(p + q\sqrt{-7}) = p - q\sqrt{-7} \quad \text{for } p, q \in \mathbb{Q}.$$

By Hilbert's 90 theorem, for $x \in E^\times$, we have:

$$x - \sigma(x) \in \mathbb{Q}^\times.$$

Let $e = p + q\sqrt{-7} \in E^\times$, where $p, q \in \mathbb{Q}$. Then:

$$e - \sigma(e) = (p + q\sqrt{-7}) - (p - q\sqrt{-7}) = 2q\sqrt{-7}.$$

By Hilbert's 90 theorem, we know that $2q\sqrt{-7} \in \mathbb{Q}^\times$. Since $\sqrt{-7}$ is irrational, this implies that $q = 0$. Thus, $e = p$ for some $p \in \mathbb{Q}$.

Therefore, the only units in $E = \mathbb{Q}(\sqrt{-7})$ that are fixed by G are the rational numbers $x = \pm 1$. Thus,

$$\mathcal{O}_E^\times = \{\pm 1\}.$$

This is a simple example of how Hilbert's 90 theorem can be used to calculate the group of units in a finite Galois extension of $\mathbb{Q}$.

Proposition 1.2.29
Let E/K be Galois and finite, $G = \mathrm{Gal}(E/K)$. Then $H^m(G, E) = 0$ for every $m > 0$

Proof: For a normal basis $(\sigma\alpha)_{\sigma\in G}$ $(\alpha \in E)$, let

$$\sum_{\sigma\in G} a_\sigma \sigma \mapsto \sum_{\sigma\in G} a_\sigma \sigma\alpha : K[G] \to E$$

be an isomorphism of $G-$module. $K[G] = \mathrm{Ind}_{1_G}^G K$, by Lemma 1.2.15, $H^m(G,E) \cong H^m(1_G, K) = 0$ for all $m > 0$. □

1.2.6 Group cohomology operations and their functorial properties

Definition 1.2.30 (Product of $G-$modules)
Let $A = \prod A_i$ be a product of $G-$modules, we can make A turns into a $G-$module by the following action (soon we will call it diagonal):

$$\sigma(\dots, a_i, \dots) = (\dots, \sigma a_i, \dots).$$

Proposition 1.2.31 (The cohomology of products)
For any $G-$module A_i,

$$H^m(G, \prod A_i) = \prod H^m(G, A_i).$$

Proof: Let $I = \prod I_i$ be a product of injectives $G-$modules then I is injective itself, since

$$\mathrm{Hom}_G(-, I) \cong \prod \mathrm{Hom}_G(-, I_i).$$

is exact. Given an injective resolution of A_i $A_i \to I_i$. Afterwards, $\prod A_i \to \prod I_i$ is an injective resolution of $\prod A_i$. And then

$$H^m(G, \prod A_i) = H^m((\prod I_i)^G) = H^m(\prod (I_i)^G) = \prod H^m(I_i^G) = \prod H^m(G, A_i).$$

□

Definition 1.2.32 (Compatible homomorphisms)
Let A and A' represent G and $H-$ modules, respectively. We call the homomorphism $\alpha : G \to H$ and $\beta : A \to A'$ compatible when

$$\beta(\alpha(g)a) = g(\beta(a)).$$

It also induces a homomorphism

$$H^m(G, A) \to H^m(H, A'),$$

by complexes homomorphisms: $C^m(G, A) \to C^m(H, A') : \varphi \mapsto \beta \circ \varphi \circ \alpha^m$.

Remark 1.2.33 (Restriction, inflation homomorphisms and dimension shifting)

1. *For any $G'-$module A with $G' \leq G$, the homomorphism*

$$\mathrm{Ind}_{G'}^G(A) \to A : \varphi \mapsto \varphi(1_G)$$

is compatible within the map $G' \hookrightarrow G$. Moreover, its induced homomorphism

$$H^m(G, \mathrm{Ind}_{G'}^G(M)) \to H^m(G', A)$$

is the isomorphism appeared in Lemma 1.2.15.

2. *Let $\alpha : G' \hookrightarrow G$ and $\beta = \mathrm{id}_A : A \to A$. Thus, α and β are compatible, we get the restriction homomorphisms:*

$$\mathrm{Res} : H^m(G, A) \to H^m(G', A).$$

3. *When G' is a normal subgroup, $\alpha : G \to G/G'$ and $\beta : A^{G'} \hookrightarrow A$. Thus, α and β are compatible, we get the inflation homomorphisms:*

$$\mathrm{Inf} : H^m(G/G', A^{G'}) \to H^m(G, A)$$

4. *Given $g_0 \in G$ and $\alpha : G \to G, \sigma \mapsto g_0\sigma g_0^{-1}$ and $\beta : A \to A, a \mapsto g_0^{-1}a$ are compatible. We can check that*

$$H^m(G, A) \to H^m(G, A).$$

is identity, for every $m \geq 0$.

5. ***(Dimension shifting)** Given $g_0 \in G$ then $\alpha : G \to G, \sigma \mapsto g_0\sigma g_0^{-1}$ and $\beta : A \to A, a \mapsto g_0^{-1}a$ are compatible. Eventually, for all $m > 0$*

$$H^m(G, A) \to H^m(G, A)$$

are identity. For $m = 0$, the homomorphism becomes

$$a \mapsto g^{-1}a : A^G \to A^G$$

is an indentity as well. Given $m > 0$ and suppose that the statement holds till $m - 1$. Let $B = \mathrm{Ind}^G(A_0)$, the short exact sequence

$$0 \to A \to B \to C \to 0$$

gives us a commutative diagram:

$$\begin{tikzcd}
H^{m-1}(G, B) \arrow[r] \arrow[d] & H^{m-1}(G, C) \arrow[r] \arrow[d] & H^m(G, A) \arrow[r] \arrow[d] & 0 \\
H^{m-1}(G, B) \arrow[r] & H^{m-1}(G, C) \arrow[r] & H^m(G, A) \arrow[r] & 0.
\end{tikzcd}$$

The 0s at the right-hand side were obtained by the fact N is an induced module. The pair (α, β) defines the vertical maps. By induction, the map $H^{m-1}(G, C) \to H^{m-1}(G, C)$ is an identity. It suggests that the third vertical map is an identity as well.

6. *When $[G : G']$ is finite and $G = \cup_{s \in S} sG'$. Given a $G-$module A. For every $a \in A^{G'}$,*

$$\mathrm{Nm}_{G/G'}\, a := \sum_{s \in S} sa$$

is fixed by G and independent of the choice of S. Thus the map $\mathrm{Nm}_{G/G'} : A^{G'} \to A^G$ is a homomorphism. This extends to a corestriction:

$$\mathrm{Cor} : H^m(G', A) \to H^m(G, A),$$

for every m since: for every $G-$module A, there is a $G-$homomorphism

$$\mathrm{Ind}_H^G A \to A : \varphi \mapsto \sum_{s \in S} s\varphi(s^{-1}),$$

the mapping on cohomology, when combined with the isomorphism noted in Lemma 1.2.15, results in

$$\mathrm{Cor} : H^m(G', A) \overset{\cong}{\to} H^m(G, \mathrm{Ind}_{G'}^G A) \to H^m(G, A)$$

Proposition 1.2.34
For a subgroup G' of finite index in G. The composite homomorphism:

$$\mathrm{Cor} \circ \mathrm{Res} : H^m(G, A) :\to H^m(G, A)$$

is a multiplication by $[G : G']$ map.

Proof: By the definition, the map $\mathrm{Cor} \circ \mathrm{Res}$ is a cohomology map given by the composite of

$$A \to \mathrm{Ind}_{G'}^G(A) \to A, a \mapsto \varphi_a \mapsto \sum_{s \in S} s\varphi_a(s^{-1}) = \sum_{s \in S} a = [G : G']a.$$

□

Corollary 1.2.35
Let $n := |G|$ then $nH^m(G, A) = 0$ for every $m > 0$.

Proof: For all $m > 0$, $H^m(1, A) = 0$. The map $\mathrm{Cor} \circ \mathrm{Res}$ is the multiplication by $[G : G']$ map, by

$$H^m(G, A) \xrightarrow{\mathrm{Res}} H^m(1, A) \xrightarrow{\mathrm{Cor}} H^m(G, A),$$

we get $nH^m(G, A) = 0$. □

Corollary 1.2.36
If G is finite, let G_p be its Sylow $p-$subgroup then for every $G-$module A, the restriction:

$$\mathrm{Res} : H^m(G, A) \to H^m(G_p, A)$$

on the $p-$primary component of $H^m(G_p, A)$, is injective.

Proof: Since p does not divide $[G : G']$, the composite

$$\mathrm{Cor} \circ \mathrm{Res} : H^m(G, A) \to H^m(G_p, A) \to H^m(G, A)$$

is the multiplication by $[G : G']$. Hence, it is injective on the $p-$primary component of $H^m(G, A)$. □

Remark 1.2.37
When G' is normal.

1. *The restriction of an $m-$cocycle is the restriction of the map $f : G^m \to A$ to a map* $\mathrm{Res}(f) : (G')^m \to A$ *given by* $\mathrm{Res}(f)(h) : f(h)$ *for all $h \in (G')^m$.*
2. *The inflation of an $m-$cocycle is just* $\mathrm{Inf}(f)(g) = f(\overline{g})$ *for all $g \in G^m$ and its image* $\overline{g} \in (G/G')^m$.

Proposition 1.2.38 (The inflation-restriction exact sequence)
Consider $G' \trianglelefteq G$ and a $G-$module A. For a fixed $m > 0$, if $H^i(G', A) = 0$ for every $0 < i < m$ then we get the following exact sequence:

$$0 \to H^m(G/G', A^{G'}) \xrightarrow{\mathrm{Inf}} H^m(G, A) \xrightarrow{\mathrm{Res}} H^m(G', A).$$

Proof: For $m = 1$, the injectivity of inflation on cocycles is obvious from Remark 1.2.37. Let f be a cocycle in $Z^1(G/G', A^{G'})$. If $f(\overline{g}) = (g-1)a$ for some $a \in A$ and all $g \in G$, then $a \in A^{G'}$ as $f(\overline{1}) = 0$. Thus, Inf is injective and also $\mathrm{Res} \circ \mathrm{Inf}(f)(h) = f(\overline{h}) = 0$ for all $h \in G'$.
Let $f' \in Z^1(G, A)$ and suppose $\mathrm{Res}(f') = 0$. Then there exists $a \in A$ such that $f'(h) = (h-1)a$ for all $h \in G'$. Define $k \in Z^1(G, A)$ by $k(g) = f'(g) - (g-1)a$, then $k(h) = 0$ for all $h \in G'$. We have:

$$k(gh) = gk(h) + k(h) = k(g),$$

for all $g \in G$ and $h \in G'$, so k factors through G/G'. Also,

$$k(g) = k(gh) = k(gg^{-1}hg) = k(hg) = hk(g) + k(h) = hk(g),$$

so k has image in $A^{G'}$. Therefore, k is the inflation of a cocycle in $Z^1(G/G', A^{G'})$. This prove the exactness.
For $m > 1$, suppose the statement is true for $m-1$. Consider the exact sequence:

$$0 \to A \to B \to C \to 0,$$

where $B := \mathrm{Ind}^G(A_0)$ and $C := B/A$. Then

$$H^i(G', A) \cong H^{i+1}(G', A), \ i > 0$$

$,so\mathrm{H}^i(G', C) = 0$ for all $0 < i \leq m-1$. By induction, we get the exact sequence

$$0 \to H^{m-1}(G/G', C^{G'}) \xrightarrow{\mathrm{Inf}} H^{m-1}(G, C) \xrightarrow{\mathrm{Res}} H^{m-1}(G', C),$$

and it is isomorphic to

$$0 \to H^m(G/G', A^{G'}) \xrightarrow{\mathrm{Inf}} H^m(G, A) \xrightarrow{\mathrm{Res}} H^m(G', A).$$

□

Example 1.2.39
If $E \subset \Omega$ and Ω/K and E/K is Galois extensions then $G' := \mathrm{Gal}(\Omega/E)$ is a normal subgroup of $G := \mathrm{Gal}(\Omega/K)$. By the Theorem 1.2.26, $H^1(G', \Omega^\times) = 0$ and then the sequence

$$0 \to H^2(G/G', E^\times) \to H^2(G, \Omega^\times) \to H^2(G', \Omega^\times)$$

is exact.

1.3 Homology of group

1.3.1 The construction of group homology

Definition 1.3.1
For every $G-$module A, we say

$$A_G := A/\{ga - a : g \in G,\ a \in A\}$$

to be the largest quotient of A that G acts on trivially.

Remark 1.3.2
The functor $A \mapsto A_G : \mathrm{Mod}_G \to \mathrm{Ab}$ is equivalent to the functor $\mathbb{Z} \otimes_{\mathbb{Z}G} - : \mathbb{Z}G - \mathrm{Mod} \to \mathrm{Ab}$. Hence, it is a right exact functor. Moreover, we can simply define homology group by letting

$$H_n(G, M) = \mathrm{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, M).$$

Definition 1.3.3 (The homology group)
Recall that Mod_G has enough projectives, given a $G-$module A and consider its projective resolution:

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to A \to 0.$$

This induces a complex

$$\cdots \to (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \to 0.$$

We set

$$H_m(G, A) = \frac{\mathrm{Ker}(d_m)}{\mathrm{Im}(d_{m+1})}.$$

Example 1.3.4

1. *$H_0(G, A) = A_G$ because the sequence*

   $$(P_1)_G \to (P_0)_G \to A_G \to 0$$

   is exact, hence

   $$H_0(G, A) = \frac{\mathrm{Ker}(d_0)}{\mathrm{Im}(d_1)} = \frac{(P_0)_G}{\mathrm{Ker}((P_0)_G \to A_G)} = A_G.$$

2. *Consider a projective $G-$module P we have $H_m(G, P) = 0$ for every $m > 0$ since we have a simple projective resolution*

   $$\cdots \to P \to P \to 0.$$

3. *Consider two projective resolutions of $G-$modules $(P_n) \to A$ and $(Q_n) \to A$, every homomorphism $\alpha : A \to B$ of $G-$module extends to a complexes morphism:*

$$\begin{tikzcd}
(P_n) \arrow[r] \arrow[d, "\overline{\alpha}"] & A \arrow[d, "\alpha"] \\
(Q_n) \arrow[r] & B.
\end{tikzcd}$$

Hence, we get the homomorphisms

$$H_m(\overline{\alpha}) : H_m((P_n)) \to H_m((Q_n))$$

do not depend on the chosen $\overline{\alpha}$.

4. *The exact sequence of* $G-$*modules*

$$0 \to A' \to A \to A'' \to 0$$

induces the long exact sequence

$$\cdots \to H_m(G, A) \to H_m(G, A'') \to H_{m-1}(G, A') \to \cdots \to H_0(G, A'') \to 0.$$

5. $H_m(G, -) : \mathrm{Mod}_G \to \mathrm{Ab}$ *is a functor.*

1.3.2 Computing the group $H_1(G, \mathbb{Z})$

Definition 1.3.5 (Augmentation ideal)
We define the map

$$\mathbb{Z}G \to \mathbb{Z}, \sum n_g g \mapsto \sum n_g$$

as the augmentation map and the augmentation ideal I_G *is its kernel.*

Remark 1.3.6
Obviusly I_G *is a free* $\mathbb{Z}-$*submodule of* $\mathbb{Z}G$ *with basis* $\{g - 1 : g \in G\}$, *thus*

$$A/I_G A = A_G = H_0(G, A).$$

Lemma 1.3.7

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

Proof: By Remark 1.3.6, $H_0(G, I_G) = I_G/I_G^2, H_0(G, \mathbb{Z}G) = \mathbb{Z}G/I_G\mathbb{Z}G, H_0(G, \mathbb{Z}) = \mathbb{Z}/I_G\mathbb{Z} = \mathbb{Z}$. Moreover, $H_1(G, \mathbb{Z}G) = 0$ because $\mathbb{Z}G$ is a free (hence projective) $G-$module. Thus the exact sequence

$$0 \to I_G \to \mathbb{Z}G \to \mathbb{Z} \to 0$$

induces a homology groups exact sequence

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

The map $I_G/I_G^2 \to \mathbb{Z}G/I_G$ is induced by the map $I_G \hookrightarrow \mathbb{Z}G$ hence its a zero map. Therefore,

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

■

Lemma 1.3.8
Let $G^{ab} := G/[G, G]$. *The mapping* $g \mapsto (g - 1) + I_G^2 : G \to I_G/I_G^2$ *allows us to make an isomorphism*

$$G^{ab} \to I_G/I_G^2.$$

Proof: The mapping $g \mapsto (g-1) + I_G^2 : G \to I_G/I_G^2$ is a group homomorphism since

$$g_1g_2 - 1 = (g_1-1)(g_2-1) + (g_1-1) + (g_2-1) \equiv (g_1-1) + (g_2-1) \mod I_G^2.$$

Because $G/\operatorname{Ker}(g \mapsto (g-1) + I_G^2)$ is isomorphic to the abelian group I_G/I_G^2, there is a natural homomorphism

$$G^{\mathrm{ab}} := G/[G,G] \to G/\operatorname{Ker}(g \mapsto (g-1) + I_G^2) \xrightarrow{\cong} I_G/I_G^2.$$

Consider the inverse mapping

$$g - 1 \mapsto \overline{g} : I_G \to G^{\mathrm{ab}}.$$

From

$$(g_1-1)(g_2-1) = (g_1g_2 - 1) - (g_1-1) - (g_2-1)$$

we have $(g_1-1)(g_2-1) \mapsto \overline{g_1g_2}.\overline{g_1}^{-1}.\overline{g_2}^{-1} = \overline{1}$. So this induces a well-define homomorphism $I_G/I_G^2 \to G^{\mathrm{ab}}$.

■

Proposition 1.3.9

$$H_1(G, \mathbb{Z}) \cong G^{ab}.$$

Proof: This can be proved directly from Lemma 1.3.7 and Lemma 1.3.8. □

1.4 The Tate cohomology

1.4.1 Construction

In this subsection, we consider G to be finite and A as a $G-$module.

Definition 1.4.1 (The norm map)
We define a map $\mathrm{Nm}_G : A \to A$ *as*

$$a \mapsto \sum_{g \in G} ga,$$

and call it the norm map.

Remark 1.4.2
We have

$$\mathrm{Nm}_G(ga) = \mathrm{Nm}_G(a) = g(\mathrm{Nm}_G(a)).$$

Hence

$$I_GA \subset \operatorname{Ker}(\mathrm{Nm}_G), \ \operatorname{Im}(\mathrm{Nm}_G) \subset A^G.$$

As $H_0(G, A) = A/I_GA$ *and* $H^0(G, A) = A^G$*, that means* Nm_G *induces a homomorphism:*

$$\mathrm{Nm}_G : H_0(G, A) \to H^0(G, A).$$

Lemma 1.4.3
Every $G-$exact sequence of the form

$$0 \to A' \xrightarrow{f} A \to A'' \to 0$$

induces a commutative diagram :

$$\begin{tikzcd}
H_1(G,A'') \arrow[r] & H_0(G,A') \arrow[r] \arrow[d, "\mathrm{Nm}_G"] & H_0(G,A) \arrow[r] \arrow[d, "\mathrm{Nm}_G"] & H_0(G,A'') \arrow[r] \arrow[d, "\mathrm{Nm}_G"] & 0 \\
0 \arrow[r] & H^0(G,A') \arrow[r] & H^0(G,A) \arrow[r] & H^0(G,A'') \arrow[r] & H^1(G,A').
\end{tikzcd}$$

Proof: We rewrite $H_0(G,A) = A/I_GA$ and $H^0(G,A) = A^G$, similarly for A' and A''. We only need to prove the commutative of the first square, i.e., the diagram

$$\begin{tikzcd}
A'/I_GA' \arrow[r] \arrow[d, "\mathrm{Nm}_G"] & A/I_GA \arrow[d, "\mathrm{Nm}_G"] \\
A'^G \arrow[r] & A^G
\end{tikzcd}$$

is commutative. The homomorphism

$$A'/I_GA' \to A/I_GA \xrightarrow{\mathrm{Nm}_G} A^G$$

goes $a' + I_GA' \mapsto a + I_GA \mapsto \mathrm{Nm}_G(a)$, and the homomorphism

$$A'/I_GA' \to A'^G \to A^G$$

goes $a' + I_GA' \mapsto \mathrm{Nm}_G(a') \mapsto f(\mathrm{Nm}_G(a'))$. However,

$$f(\mathrm{Nm}_G(a')) = f\left(\sum_{g\in G} ga'\right) = \sum_{g\in G} gf(a') = \sum_{g\in G} ga = \mathrm{Nm}_G(a)$$

hence, the diagram is commutative. ■

Definition 1.4.4 (The Tate groups)
The middle part of the diagram in Lemma 1.4.1 induces a long exact sequence due to the snake lemma:

$$\cdots \to H_T^m(G,A') \to H_T^m(G,A) \to H_T^m(G,A'') \xrightarrow{\sigma} H_T^{m+1}(G,A') \to \dots, \; m \in \mathbb{Z}$$

where

$$H_T^m(G,A) := \begin{cases} H^m(G,A) & m > 0 \\ A^G/\mathrm{Nm}_G(A) & m = 0 \\ \mathrm{Ker}(\mathrm{Nm}_G)/I_GM & m = -1 \\ H_{-m-1}(G,A) & m < -1. \end{cases}$$

$H_T^m(G,A)$ is called the $m-$th Tate cohomology group.

Remark 1.4.5
Almost every result we represented for the groups $H^m(G,A)$ with $m \geq 0$ extends naturally to every $m \in \mathbb{Z}$, include

1. *The Shapiro lemma for the Tate cohomology groups.*

2. *The restriction, costriction, inflation homomorphisms:*

   (a) $\mathrm{Res} : H^m_T(G, A) \to H^m_T(G', A)$;

   (b) $\mathrm{Cor} : H^m_T(G', A) \to H^m_T(G, A)$;

   (c) $\mathrm{Inf} : H^m_T(G/G', A^{G'}) \to H^m_T(G, A)$ *(G' is normal).*

3. *The homomorphism* $\mathrm{Res} \circ \mathrm{Cor}$ *keeps being the multiplication by* $[G : G']$ *map and* $H^m_T(G, A)$ *becomes trivial when multiplying* $|G|$*, for every* m*, i.e.* $|G|H^r_T(G, A) = 0$.

4. $H^{-2}_T(G, \mathbb{Z}) = H_1(G, \mathbb{Z}) \cong G^{ab}$.

For the rest of this chapter, we will denote H^r_T by H^r since every cohomology from now is Tate cohomology.

Definition 1.4.6 (The Verlagerung map)
Let $G = \bigcup s_i G'$*, for* $g \in G$ *and index* i*, there exists* $g_i \in G'$ *and* s_j *so that*

$$gs_i = s_j g_i.$$

The map

$$g \mapsto \prod g_i \mod [G', G'] : G \to (G')^{ab}$$

is a group homomorphism and it induces the Verlagerung map $\mathrm{Ver} : G^{ab} \to (G')^{ab}$.

Proposition 1.4.7

1. *The homomorphism* $\mathrm{Res} : H^{-2}_T(G, \mathbb{Z}) \to H^{-2}_T(G', \mathbb{Z})$ *is equivalent to the Verlagerung map* $G^{ab} \to (G')^{ab}$.

2. *The homomorphism* $\mathrm{Cor} : H^{-2}_T(G', \mathbb{Z}) \to H^{-2}_T(G, \mathbb{Z})$*. represents the map* $(G')^{ab} \to G^{ab}$*. caused by inclusion* $G' \hookrightarrow G$.

Proof:

1. From Proposition 1.3.9 and dimension shifting, we obtain a commutative diagram:

$$\begin{tikzcd}
H^{-2}(G',\mathbb{Z}) \arrow[r, "\cong"] \arrow[d, "\mathrm{Cor}"] & I_{G'}/I_{G'}^2 \arrow[r, "\cong"] \arrow[d] & (G')^{\mathrm{ab}} \arrow[d] \\
H^{-2}(G,\mathbb{Z}) \arrow[r, "\cong"] & I_G/I_G^2 \arrow[r, "\cong"] & G^{\mathrm{ab}}.
\end{tikzcd}$$

   Here the second and third down-arrow are $(g'-1) + I^2_{G'} \mapsto (g'-1) + I^2_G$ and $g'[G', G'] \mapsto g'[G, G]$, respectively. This directly implies the correspondence.

2. Consider a diagram:

$$\begin{tikzcd}
H^{-2}(G,\mathbb{Z}) \arrow[r, "\mathrm{Res}"] \arrow[d, "\cong"] & H^{-2}(G',\mathbb{Z}) \arrow[r, "\mathrm{Cor}"] \arrow[d, "\cong"] & H^{-2}(G,\mathbb{Z}) \arrow[d, "\cong"] \\
G^{\mathrm{ab}} \arrow[r, "\mathrm{Ver}"] & (G')^{\mathrm{ab}} \arrow[r, "i_{G'}"] & G^{\mathrm{ab}},
\end{tikzcd}$$

here the second square is commutative and $i_{G'}$ is just $(G')^{\mathrm{ab}} \hookrightarrow G^{\mathrm{ab}}$. By Proposition 1.2.34, the map $\mathrm{Cor} \circ \mathrm{Res}$ is $[G : G']. \mathrm{id} : H^{-2}(G, \mathbb{Z}) \to H^{-2}(G, \mathbb{Z})$. For any $g[G, G] \in G^{\mathrm{ab}}$ and $gs_i = s_j g_i$ for $G = \bigcup s_i G'$,

$$\begin{aligned} i_{G'} \circ \mathrm{Ver}(g[G,G]) &= i_{G'}(\prod g_i[G',G']) \\ &= i_{G'}(\prod s_j g_i s_i^{-1}[G',G']) \\ &= \prod s_j g_i s_i^{-1}[G,G] \\ &= \prod g_i[G,G] \\ &= \prod s_j^{-1} g s_i[G,G] \\ &= g^{[G:G']}[G,G]. \end{aligned} \tag{1.1}$$

Hence, the big rectangle of the diagram is indeed commutative. Since $i_{G'}$ is injective, the first square is also commutative.

□

1.4.2 The cohomology of finite cyclic groups

Let $\mathbb{Z}$, $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{Q}$ to be $G-$modules that the actions of G on them are trivial.

Lemma 1.4.8
When G is finite

1. *$H_T^m(G, \mathbb{Q}) = 0$ for every m;*
2. *$H_T^m(G, \mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$ and $H^1(G, \mathbb{Z}) = 0$;*
3. *$H^2(G, \mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$.*

Proof:

1. Since $\mathbb{Q}$ is uniquely divisible, for any integer $a \neq 0$, the homomorphism $H^m(a) : H_T^m(G, \mathbb{Q}) \to H_T^m(G, \mathbb{Q})$ is an isomorphism since it is multiplication by a. Let $a := |G|$, the multiplication by a on $H^m(G, A)$ is an isomorphism and zero. This implies $H_T^m(G, A) = 0$.
2. We have $\mathbb{Z}^G = \mathbb{Z}$ and the norm map is mulplication by $|G|$ mapping. Thus $\mathbb{Z}/|G|\mathbb{Z} = H_T^0(G, \mathbb{Z})$. In addition, $H^1(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z}) = 0$ because $\mathbb{Z}$ is torsion-free.
3. The exact cohomology sequence of the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

is of the form

$$\begin{tikzcd} H^1(G,\mathbb{Q}) \arrow[r] \arrow[d, "="] & H^1(G,\mathbb{Q}/\mathbb{Z}) \arrow[r] \arrow[d, "\cong"] & H^2(G,\mathbb{Z}) \arrow[r] & H^2(G,\mathbb{Q}). \arrow[d, "="] \\ 0 & \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) & & 0 \end{tikzcd}$$

■

Proposition 1.4.9
In the case G is a finite cyclic group and A is a $G-$module. For all $m \in \mathbb{Z}$

$$H_T^m(G,A) \cong H_T^{m+2}(G,A),$$

and the isomorphism depends only on the choice of group generator.

Proof: Suppose $G = \langle \sigma \rangle$, the sequence

$$0 \to \mathbb{Z} \xrightarrow{a \mapsto a1_G} \mathbb{Z}G \xrightarrow{\sigma - 1} \mathbb{Z}G \xrightarrow{\sigma^i \mapsto 1} \mathbb{Z} \to 0$$

is exact. Since the groups in the sequence and I_G are free $\mathbb{Z}-$modules, when we take tensor product of the sequence with A, it stays exact. Hence we obtain the following exact sequence of $G-$module

$$0 \to A \to \mathbb{Z}G \otimes_{\mathbb{Z}} A \to \mathbb{Z}G \otimes_{\mathbb{Z}} A \to A \to 0$$

Recall that $\mathbb{Z}G \otimes_{\mathbb{Z}} A \cong \mathbb{Z}G \otimes_{\mathbb{Z}} A_0$ where A_0 denotes the abelian group A, thus $H^m(G, \mathbb{Z}G \otimes_{\mathbb{Z}} A) = 0$ for all m. Hence, the sequence induces an isomorphisms

$$H_T^m(G,A) \overset{\cong}{\to} H_T^{m+2}(G,A),$$

for every m. □

Remark 1.4.10
We know that

$$H^2(G,\mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$

Let $\gamma \in H^2(G,\mathbb{Z})$ corrresponding under the isomorphism to the map $G \to \mathbb{Q}/\mathbb{Z} : \sigma \mapsto 1/a$ where $G = \langle \sigma \rangle$. Therefore the homomorphism $H^m(G,A) \to H^{m+2}(G,A)$ is defined by $x \mapsto x \cup \gamma$.

Definition 1.4.11 (Herbrand quotient)
In the case G finite and cyclic and A is a $G-$module. We say the following quotient is the Herbrand quotient when the groups $H^m(G,A)$ are finite:

$$h(A) = \frac{\#H_T^0(G,A)}{\#H_T^1(G,A)}.$$

Lemma 1.4.12
Consider

$$0 \to H_0 \to H_1 \to \cdots \to H_r \to 0$$

as a sequence of finite groups. Therefore

$$\frac{\#H_0 \#H_2 \ldots}{\#H_1 \#H_3 \ldots} = 1.$$

Proof: In the case $r = 3$, the sequence becomes a short exact sequence, the statement is obvious. Moreover, it is possible to divide every exact sequence into these exact sequences:

$$0 \to H_0 \to H_1 \to C_1 \to 0;$$

$$0 \to C_1 \to H_2 \to C_2 \to 0;$$

$$\dots$$

$$0 \to C_{r-1} \to H_{r-1} \to H_r \to 0;$$

here $C_i = \mathrm{Coker}(H_{i-1} \to H_i) = \mathrm{Ker}(H_{i+1} \to H_{i+2})$. From here we can see that

$$1 = \frac{\#H_0\#C_1}{\#H_1} = \frac{\#H_0\#H_2}{\#H_1\#C_2} = \dots$$

This proves our statement. ■

Proposition 1.4.13
Consider an short exact sequence of $G-$module:

$$0 \to A' \to A \to A'' \to 0.$$

Any Herbrand quotient in $h(A'), h(A), h(A'')$ is defined if any two of the others are. In addition,

$$h(A) = h(A')h(A'').$$

Proof: The long exact sequence can be truncated as follows:

$$0 \to K \to H^0_T(A') \to H^0_T(A) \to H^0_T(A'') \to H^1_T(A') \to H^1_T(A) \to H^1_T(A'') \to K' \to 0,$$

here

$$K = \mathrm{Coker}(H^{-1}_T(A) \to H^{-1}_T(A'')) \cong \mathrm{Coker}(H^1_T(A) \to H^1_T(A'')) = K'.$$

This (with Lemma 1.4.12) proves the proposition. □

Proposition 1.4.14
We have $h(A) = 1$ when A is finite.

Proof: By directly checking, we can see that the sequence

$$0 \to A^G \to A \xrightarrow{\times(g-1)} A \to A_G \to 0$$

is exact, where $G = \langle g \rangle$, and then

$$0 \to H^{-1}_T(A) \to A_G \xrightarrow{\mathrm{Nm}_G} A^G \to H^0_T(A) \to 0$$

is also an exact sequence. From the first sequence we can see that $|A^G| = |A_G|$ and from the second that $|H^{-1}_T(A)| = |H^0_T(A)|$. This implies $h(A) = 1$. □

Corollary 1.4.15
For every $G-$homomorphism $\alpha : A \to B$ such that $\mathrm{Ker}\,\alpha$ and $\mathrm{Coker}\,\alpha$ are finite. If either $h(A)$ or $h(B)$ is defined then so also the other. Moreover, $h(A) = h(B)$.

Proof: Suppose that $h(B)$ is defined, we have two following canonical exact sequences:

$$0 \to \alpha(A) \to B \to \operatorname{Coker}(\alpha) \to 0$$

and

$$0 \to \operatorname{Ker}(\alpha) \to A \to \alpha(A) \to 0.$$

The notation $h(\alpha A)$ can be defined by the first exact sequence and it equals $h(B)$. Similarly, from the second sequence, we can also define $h(A)$ and it equals $h(\alpha A)$. Hence, $h(A) = h(B)$. □

1.4.3 Cup-products

Definition 1.4.16 (Tensor product)
For every pair of $G-$modules (X, Y), we denote $X \otimes Y$ as $X \otimes_{\mathbb{Z}} Y$, regarded as a $G-$module with

$$g(x \otimes y) = gx \otimes gy,$$

for any $(g, x, y) \in G \times X \times Y$

Definition 1.4.17 (Coaugmentation ideal)
The coaugmentation maps is

$$\mathbb{Z} \to \mathbb{Z}G, n \mapsto \sum_{g \in G} gn.$$

Its cokernel is denoted $J_G := \mathbb{Z}/\mathbb{Z}N_G$ is the coaugmentation ideal of $\mathbb{Z}G$, where $\mathbb{Z}N_G := \{\sum gn : n \in \mathbb{Z}\}$.

Definition 1.4.18
Consider any arbitrary $G-$module X, we define the $G-$modules

$$X^m = J_G \otimes \cdots \otimes J_G \otimes X,$$

for $m > 0$ with m times J_G and

$$X^{-m} = I_G \otimes \cdots \otimes I_G \otimes X$$

for $m > 0$ with m times I_G. We also consider $X^0 = X$.

There is an (unique) family of bi-additive pairings (called cup-product and we are going to construct it)

$$(x, y) \mapsto x \smile y : H_T^m(G, X) \times H_T^n(G, Y) \to H_T^{m+n}(G, X \otimes Y)$$

defined for all $G-$modules X, Y and all integers $m, n \in \mathbb{Z}$ that satisfy the following three conditions:

1. When the two sides are considered as covariant bifunctors on (X, Y), these maps transform into functor morphisms;

2. In the case $m = n = 0$, the map becomes

$$(x, y) \mapsto x \otimes y : X^G / \operatorname{Nm}_G(X) \times Y^G / \operatorname{Nm}_G(Y) \to (X \otimes Y)^G / \operatorname{Nm}_G(X \otimes Y).$$

3. For any $G-$short exact sequence $0 \to X' \to X \to X'' \to 0$ so that

$$0 \to X' \otimes Y \to X \otimes Y \to X'' \otimes Y \to 0$$

is also exact then

$$(\delta x'') \smile y = \delta(x'' \smile y),\ x'' \in H_T^m(G, X''),\ y \in H_T^n(G, Y).$$

Lemma 1.4.19
Let

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & X' \arrow[r] \arrow[d] & X \arrow[r] \arrow[d] & X'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Y' \arrow[r] \arrow[d] & Y \arrow[r] \arrow[d] & Y'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Z' \arrow[r] \arrow[d] & Z \arrow[r] \arrow[d] & Z'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

be a commutative diagram of $G-$module with all rows and columns be exact. Then the diagram

$$\begin{tikzcd}
H^{n-1}(G, Z'') \arrow[r, "\delta_{n-1}"] \arrow[d, "\delta_{n-1}"] & H^n(G, Z') \arrow[d, "-\delta_s"] \\
H^n(G, X'') \arrow[r, "\delta_s"] & H^{n-1}(G, X')
\end{tikzcd}$$

commutes.

<u>Proof:</u> Let $D = \ker(Y \to Z'')$, we obtain a well-known exact sequence:

$$0 \to D \to Y \to Z'' \to 0.$$

Define homomorphism of $G-$modules

$$i : X' \to X \oplus Y' : x' \mapsto (x, y'),$$

where x and y' are the images of x' in X and in Y', respectively.

$$j : X \oplus Y' \to D : (x, y') \mapsto d_1 - d_2,$$

where d_1 is the image of x in D and similarly for y' and d_2. Then we have an exact sequence

$$0 \to X' \xrightarrow{i} X \oplus Y' \xrightarrow{j} D \to 0,$$

and a commutative diagram

$$\begin{tikzcd}
X' \arrow[r] & X \arrow[r] & X'' \arrow[r] & Y'' \arrow[r] & Z'' \\
X' \arrow[u, "\mathrm{id}"] \arrow[r, "i"] \arrow[d, "-\mathrm{id}"] & X \oplus Y' \arrow[u, "\mathrm{id}\times 0"] \arrow[r, "j"] \arrow[d, "-\mathrm{id}\times 0"] & D \arrow[u] \arrow[r] \arrow[d] & Y \arrow[u] \arrow[r] \arrow[d] & Z'' \arrow[u, "\mathrm{id}"] \arrow[d, "\mathrm{id}"] \\
X' \arrow[r] & Y' \arrow[r] & Z' \arrow[r] & Z \arrow[r] & Z''.
\end{tikzcd}$$

In light of the exact sequence, we note that $\mathrm{im}(D \to Y'') \subset \mathrm{im}(X'' \to Y'')$. Given the injectivity of the map $X'' \to Y''$, it follows that we can introduce a homomorphism from D to X'', preserving the structure of the diagram. Similarly, by analogous reasoning, we extend the diagram with a homomorphism from D to Z'. The resulting extensions maintain commutativity within the diagram. Consequently, by applying dimension-shifting arguments, we obtain a commutative diagram of cohomology groups.

$$\begin{tikzcd}
H^{s-1}(G, Z'') \arrow[r, "\delta_{s-1}"] & H^s(G, X'') \arrow[r, "\delta_s"] & H^{s+1}(G, X') \\
H^{s-1}(G, Z'') \arrow[u, "\mathrm{id}"] \arrow[r, "\delta_{s-1}"] \arrow[d, "\mathrm{id}"] & H^s(G, D) \arrow[u] \arrow[r, "\delta_s"] \arrow[d] & H^{s+1}(G, X') \arrow[u, "\mathrm{id}"] \arrow[d, "-\mathrm{id}"] \\
H^{s-1}(G, Z'') \arrow[r, "\delta_{q-1}"] & H^s(G, Z') \arrow[r, "\delta_s"] & H^{s+1}(G, X').
\end{tikzcd}$$

■

Theorem 1.4.20

There exists an unique family of such bi-additive pairings.

Proof: First, for $m = n = 0$, we consider a map

$$X^G/\operatorname{Nm}_G(X) \times Y^G/\operatorname{Nm}_G(Y) \to (X \otimes Y)^G/\operatorname{Nm}_G(X \otimes Y) :$$

$$(x + \operatorname{Nm}_G(X), y + \operatorname{Nm}_G(Y)) \mapsto x \otimes y + \operatorname{Nm}_G(X \otimes Y).$$

This map is well-defined since:

1. For $x \in X^G, y \in Y^G$

   $$g(x \otimes y) = gx \otimes gy = x \otimes y \ \forall g \in G,$$

   hence $x \otimes y \in (X \otimes Y)^G$

2. For $x, x' \in X^G; y, y' \in Y^G$ such that $x - x' \in \operatorname{Nm}_G(X), y - y' \in \operatorname{Nm}_G(Y)$

   $$\begin{aligned} x \otimes y - x' \otimes y' &= x \otimes y - x \otimes y' + x \otimes y' - x' \otimes y' \\ &= x \otimes (y - y') + (x - x') \otimes y', \end{aligned} \tag{1.2}$$

   thus

   $$\begin{aligned} \sum_{g \in G} g(x \otimes y - x' \otimes y') &= x \otimes \sum g(y - y') + \sum g(x - x') \otimes y' \\ &= x \otimes 0 + 0 \otimes y' \\ &= 0. \end{aligned} \tag{1.3}$$

   Hence, $x \otimes y - x' \otimes y' \in \operatorname{Nm}_G(X \otimes Y)$.

Since the mapping above is well-defined, we proceed to define the cup product across any dimensions. Begin by observing that $X \otimes Y$ can be identified with $Y \otimes X$, and likewise, $X \otimes (Y \otimes Z)$ is identified with $(X \otimes Y) \otimes Z$ for G-modules X, Y, and Z. Accordingly, there are natural identifications for dimension-shifted modules: $X^m \otimes Y = (X \otimes Y)^m$ and $X \otimes Y^n = (X \otimes Y)^n$ for all $m, n \in \mathbb{Z}$. Given any $m, n \in \mathbb{Z}$, we thus consider the following diagram.

$$\begin{tikzcd}
H^0(G, X^m) \times H^0(G, Y^n) \arrow[r, "\smile"] \arrow[d, "\delta_m \times \mathrm{id}"] & H^0(G, X^m \otimes Y^n) \arrow[d, "\delta_m"] \\
H^m(G, X) \times H^0(G, Y^n) \arrow[r, "\smile"] \arrow[d, "\mathrm{id} \times \delta_n"] & H^n(G, X \otimes Y^n) \arrow[d, "\delta_n"] \\
H^m(G, X) \times H^n(G, Y) \arrow[r, "\smile"] & H^{m+n}(G, X \otimes Y).
\end{tikzcd}$$

We define the operation

$$\smile : H^m(G, X) \times H^n(G, Y) \to H^{m+n}(G, X \otimes Y)$$

as a natural homomorphism that extends the existing diagram into a commutative one. By this construction, it becomes clear that if $\smile$ fulfills property 3 of the theorem, then this definition of $\smile$ must be unique.

To show that $\smile$ satisfies property 3, we first provide explicit forms in the cases $(m, 0)$ and $(0, n)$ for $m, n \geq 0$. Specifically, we assert that

$$\smile : H^m(G, X) \times H^0(G, Y) \to H^m(G, X \otimes Y) : (\overline{x_m}, \overline{y_0}) \mapsto \overline{x_m \otimes y_0}$$

and

$$\smile : H^0(G, X) \times H^n(G, Y) \to H^n(G, X \otimes Y) : (\overline{x_0}, \overline{y_n}) \mapsto \overline{x_0 \otimes y_n}$$

give the explicit descriptions. This definition readily satisfies property 2, so it remains to verify property 3.

Assume we have the following exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & X' \arrow[r, "\varphi"] & X \arrow[r, "\psi"] & X'' \arrow[r] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
0 \arrow[r] & X' \otimes Y \arrow[r, "\varphi"] & X \otimes Y \arrow[r, "\psi"] & X'' \otimes Y \arrow[r] & 0.
\end{tikzcd}$$

It is necessary for us to demonstrate that the subsequent diagram commutes:

$$\begin{tikzcd}
H^m(G, X'') \times H^0(G, Y) \arrow[r, "\smile"] \arrow[d, "\delta_m \times \mathrm{id}"] & H^m(G, X'' \otimes Y) \arrow[d, "\delta_m"] \\
H^{m+1}(G, X') \times H^0(G, Y) \arrow[r, "\smile"] & H^{m+1}(G, X' \otimes Y)
\end{tikzcd}$$

Let $\overline{x''_m} \in H^m(G, X'')$ and $\overline{y_0} \in H^0(G, Y)$. Suppose x_m is such that $\psi(x_m) = x''_m$ and x_{m+1} satisfies $\varphi(x_{m+1}) = \delta_m(x_m)$. Then $\delta_m(\overline{x''_m}) = \overline{x_{m+1}}$. Therefore,

$$\delta_m(\overline{x''_m}) \smile \overline{y_0} = \overline{x_{m+1} \otimes y_0}.$$

Moreover, since δ_m is independent of the choice of preimage, we may select $x_m \otimes y_0$ as a preimage of $x''_m \otimes y_0$ under ψ. This choice yields $\varphi(x_{m+1} \otimes y_0) = \delta_{m+1}(x_m \otimes y_0)$, leading to the equality

$$\delta_m(\overline{x''_m} \smile \overline{y_0}) = \overline{x_{m+1} \otimes y_0} = \delta_m(\overline{x''_m}) \smile \overline{y_0}.$$

Hence, the diagram commutes, confirming property 3.
To address the general case, assume we have the exact sequences as outlined in the theorem's statement. This assumption gives rise to the following exact sequences.

$$\begin{tikzcd}
0 \arrow[r] & X^n \arrow[r] & (X')^n \arrow[r] & (X'')^n \arrow[r] & 0 \\
0 \arrow[r] & (X \otimes Y)^n \arrow[r] & (X' \otimes Y)^n \arrow[r] & (X'' \otimes Y)^n \arrow[r] & 0
\end{tikzcd}$$

which induce the diagram

$$\begin{tikzcd}
 & H^m(G,X'') \times H^0(G,Y^n) \arrow[rr] \arrow[dl] \arrow[dd] & & H^m(G,(X'' \otimes Y)^n) \arrow[dl] \arrow[dd] \\
H^{m+1}(G,X) \times H^0(G,Y^n) \arrow[rr, crossing over] \arrow[dd] & & H^{m+1}(G,(X \otimes Y)^n) & \\
 & H^m(G,X'') \times H^n(G,Y) \arrow[rr] \arrow[dl] & & H^{m+n}(G,X'' \otimes Y) \arrow[dl] \\
H^{m+1}(G,X) \times H^n(G,Y) \arrow[rr] & & H^{m+n+1}(G,X \otimes Y) \arrow[from=uu, crossing over] &
\end{tikzcd}$$

The left-hand faces of these cubes commute straightforwardly. The right-hand faces commute due to the composition of squares from Lemma 1.4.19. The front and back faces commute by the definition of the cup product, and based on the cases $(m,0)$ and $(0,n)$, the top faces also commute. Since all vertical maps are isomorphisms, it follows that the bottom faces must commute as well.
To verify the first property, let $f : X \to Y$ and $g : X' \to Y'$ be homomorphism of $G-$modules. Denote $f \otimes g$ the induced homomorphism

$$f \otimes g : X \otimes Y \to X' \otimes Y'$$

then we need to prove the diagram

$$\begin{tikzcd}
H^m(G,X) \times H^n(G,Y) \arrow[r, "\smile"] \arrow[d, "\overline{f} \times \overline{g}"] & H^{m+n}(G,X \otimes Y) \arrow[d, "\overline{f \otimes g}"] \\
H^m(G,X') \times H^n(G,Y') \arrow[r, "\smile"] & H^{m+n}(G,X' \otimes Y').
\end{tikzcd}$$

However, this immediate in case that $m = n = 0$ and the general case then follows via dimension shifting. □

Corollary 1.4.21
For every exact sequnce of $G-$modules $0 \to Y' \to Y \to Y'' \to 0$ so that

$$0 \to X \otimes Y' \to X \otimes Y \to X \otimes Y'' \to 0$$

is exact then

$$x \smile \delta y'' = (-1)^m \delta(x \smile y''),\ x \in H^m(G,X),\ y'' \in H^n(G,Y'').$$

Proof: The argument is similar to the proof of Theorem 1.4.20. □

Proposition 1.4.22
Let X, Y be $G-$modules and $G' \leq G$. Then for all $\overline{a} \in H^m(G,X)$ and $\overline{b} \in H^n(G,Y)$ we have the relations

1. $\mathrm{Res}(\overline{x}) \smile \mathrm{Res}(\overline{y}) = \mathrm{Res}(\overline{x} \smile \overline{y})$*;*
2. $\mathrm{Cor} \circ \mathrm{Res}(\overline{x} \smile \overline{y}) = \overline{x} \smile \mathrm{Cor}(\overline{y})$*.*

Proof: The general case follows from the case where $m = n = 0$ via dimension shifting. Now suppose that $m = n = 0$. The first formula is immediate. To prove the second formula, fix $x + \mathrm{Nm}_G(X) \in H^0(G,X) \cong X^G/\,\mathrm{Nm}_G(X)$ and $y + \mathrm{Nm}_G(Y) \in H^0(G,Y) \cong Y^G/\,\mathrm{Nm}_G(Y)$. By the definition of corestriction, we have

$$\begin{aligned}
\mathrm{Cor}((x + \mathrm{Nm}_G(X)) \smile (y + \mathrm{Nm}_G(Y))) &= \mathrm{Cor}(x \otimes y + \mathrm{Nm}_{G'}(X \otimes Y)) \\
&= \sum_{\sigma \in G/G'} \sigma(x \otimes y) + \mathrm{Nm}_G(X \otimes Y) \\
&= \left(\sum_{\sigma \in G/G'} x \otimes \sigma y \right) + \mathrm{Nm}_G(X \otimes Y) \qquad (1.4) \\
&= \overline{x} \smile \left(\sum_{\sigma \in G/G'} \sigma y \right) + \mathrm{Nm}_G(Y) \\
&= \overline{x} \smile \mathrm{Cor}(\overline{y}).
\end{aligned}$$

□

Proposition 1.4.23
Let X, Y, Z be $G-$modules. Suppose that $\overline{x} \in H^m(G,X), \overline{y} \in H^n(G,Y)$ and $\overline{Z} \in H^p(G,Z)$. Then

1. *The cup-product is anti commutative*

$$(-1)^{mn}(\overline{y} \smile \overline{x}) = \overline{x} \smile \overline{y}$$

under the canonical isomorphism

$$H^{m+n}(G, Y \otimes X) \cong H^{m+n}(G, X \otimes Y).$$

2. *The cup-product is associative*

$$(\overline{x} \smile \overline{y}) \smile \overline{z} = \overline{x} \smile (\overline{y} \smile \overline{z})$$

under the canonical isomorphism

$$H^{m+n+p}(G, X \otimes (Y \otimes Z)) \cong H^{m+n+p}(G, (X \otimes Y) \otimes Z).$$

Proof: The proposition follows immediately from the properties of the tensor product in dimensions $m = n = p = 0$ and then we can apply the dimension shifting principle for the general cases. □

Example 1.4.24
Let $G = \mathbb{Z}/2\mathbb{Z}$ generated by g and X is a $G-$module with trivial action. For simplicity, we take $X = \mathbb{Z}/2\mathbb{Z}$. The cohomology group $H^m(G, X)$ for $n \geq 0$ alternate between X and the trivial group 0. We have:

$$H^m(G, X) = \begin{cases} X & \textit{if } 2|n; \\ 0 & \textit{if } 2 \nmid n. \end{cases}$$

Now we compute the cup-product for classes in $H^0(G, X)$ and $H^2(G, X)$. Take $\alpha \in H^0(G, X) = \mathbb{Z}/2\mathbb{Z}$ and $\beta \in H^1(G, X) = \mathbb{Z}/2\mathbb{Z}$, which can be represented by the $2-$cocycle corresponding to the nontrivial central extension of G by X. The cup-product:

$$\alpha \cup \beta \in H^2(G, X),$$

since it was defined by the map

$$H^0(G, X) \times H^2(G, X) \to H^2(G, X)$$

Because both $\alpha, \beta \in \{0; 1\}$, we can compute their cup-product easily by multiplication:

1. *If $\alpha = \beta = 1$ then $\alpha \cup \beta = 1 \cdot 1 = 1 \in H^2(G, X)$;*

2. *If $\alpha = 0$ or $\beta = 0$ then $\alpha \cup \beta = 0$.*

Example 1.4.25
Let $G = \mathbb{Z}/2\mathbb{Z}$, and consider the trivial G-module $X = \mathbb{Z}$. We want to compute the cup product in

$$H^1(G, X) \times H^1(G, X) \to H^2(G, X).$$

1. *The group $G = \mathbb{Z}/2\mathbb{Z}$ has two elements: 1 and σ (with $\sigma^2 = 1$). A 1-cocycle $f : G \to \mathbb{Z}$ is a function such that:*

   $$f(\sigma\tau) = \sigma \cdot f(\tau) + f(\sigma)$$

   where $\sigma, \tau \in G$ and $\sigma \cdot x = x$ for any $x \in \mathbb{Z}$, because the action is trivial. In this context, the cocycle condition simplifies to:

   $$f(1) = 0 \quad \textit{and} \quad f(\sigma^2) = 2f(\sigma) = 0.$$

   Since $2f(\sigma) = 0$ in $\mathbb{Z}$, we conclude that $f(\sigma)$ can be any integer. Hence,

   $$H^1(G, A) = \mathbb{Z}/2\mathbb{Z},$$

   represented by $[f(\sigma) = 0]$ or $[f(\sigma) = 1]$.

2. *Consider two cocycles: - $f_1(\sigma) = 1$ mod 2 - $f_2(\sigma) = 1$ mod 2.*

   Both represent non-trivial elements in $H^1(G, A)$.

3. *The cup product of f_1 and f_2 is given by:*

$$f_1 \smile f_2 : G \times G \to \mathbb{Z},$$

and the value on (σ, τ) is:

$$(f_1 \smile f_2)(\sigma, \tau) = f_1(\sigma) \cdot \sigma \cdot f_2(\tau).$$

Since $\sigma \cdot f_2(\tau) = f_2(\tau)$ (the action is trivial), we have:

$$(f_1 \smile f_2)(\sigma, \sigma) = f_1(\sigma) \cdot f_2(\sigma).$$

Plugging in $f_1(\sigma) = 1$ and $f_2(\sigma) = 1$, we get:

$$(f_1 \smile f_2)(\sigma, \sigma) = 1 \cdot 1 = 1.$$

4. *The result 1 represents the cohomology class in $H^2(G, \mathbb{Z})$. For $G = \mathbb{Z}/2\mathbb{Z}$, this class corresponds to the non-zero element of*

$$H^2(G, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}.$$

Example 1.4.26
Let $G = \mathbb{Z}/n\mathbb{Z}$ and $X = \mathbb{Q}/\mathbb{Z}$ as a trivial G-module. We will compute the cup product in:

$$H^1(G, X) \times H^1(G, X) \to H^2(G, X).$$

1. *For $G = \mathbb{Z}/n\mathbb{Z}$, consider an element $g \in G$ with order n. The cohomology group $H^1(G, \mathbb{Q}/\mathbb{Z})$ can be identified with the group of homomorphisms from G to $\mathbb{Q}/\mathbb{Z}$:*

$$Hom(G, \mathbb{Q}/\mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}).$$

Since $G \cong \mathbb{Z}/n\mathbb{Z}$, we have:

$$Hom(G, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}.$$

An element of $H^1(G, \mathbb{Q}/\mathbb{Z})$ can be represented by a cocycle $f : G \to \mathbb{Q}/\mathbb{Z}$ where $f(g^k) = \frac{k}{n}$ mod 1.

2. *Let $f_1, f_2 \in H^1(G, \mathbb{Q}/\mathbb{Z})$ be cocycles defined as:*

$$f_1(g^k) = \frac{ak}{n} \quad \text{and} \quad f_2(g^k) = \frac{bk}{n},$$

where $a, b \in \mathbb{Z}$ are fixed integers.

3. *The cup product $f_1 \smile f_2$ is defined as:*

$$(f_1 \smile f_2)(g^i, g^j) = f_1(g^i) \cdot g^i \cdot f_2(g^j),$$

where $g^i \cdot f_2(g^j) = f_2(g^j)$ since the action on $\mathbb{Q}/\mathbb{Z}$ is trivial.

Substituting the values, we get:

$$(f_1 \smile f_2)(g^i, g^j) = f_1(g^i) \cdot f_2(g^j) = \frac{ai}{n} \cdot \frac{bj}{n} = \frac{ab \cdot ij}{n^2}.$$

4. *Now, let's compute this value modulo* 1. *Since* $i, j \in \{0, 1, \ldots, n-1\}$, *we consider:*

$$\frac{ab \cdot ij}{n^2} \in \mathbb{Q}/\mathbb{Z}.$$

This value represents an element of $H^2(G, \mathbb{Q}/\mathbb{Z})$. *For* $G = \mathbb{Z}/n\mathbb{Z}$, *we have:*

$$H^2(G, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}.$$

The cup product results in:

$$[f_1 \smile f_2] = \frac{ab}{n} \in \mathbb{Z}/n\mathbb{Z}.$$

5. *The cup product of two elements* $f_1, f_2 \in H^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ *is the cohomology class in* $H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ *corresponding to* $\frac{ab}{n}$, *where* a, b *are integers representing the chosen cocycles* f_1 *and* f_2.

1.4.4 Tate's Theorem

Lemma 1.4.27 (Tate's)
When G *is finite and* A *is a* $G-$*module. If*

$$H^1_T(G', A) = 0 = H^2_T(G', A)$$

for every $G' \leq G$, *then* $H^m_T(G, A) = 0$ *for every* $m \in \mathbb{Z}$.

Proof: This is clear if G is cyclic. Presume that G is solvable. In this instance, we will use induction on the size of finite group G to finish this lemma.
Assume that G/G' is cyclic and that G' is a proper subgroup of G. For every $m \in \mathbb{Z}$, $H^m_T(H, A) = 0$ since $|G'| < |G|$ and the pair (G', A) satisfy the lemma's hypotheses. Thus, we have exact sequences:

$$0 \to H^m_T(G/G', A^{G'}) \to H^m_T(G, A) \to H^m_T(G', A)$$

for every $m \geq 1$. Since $H^1_T(G, A) = 0 = H^2_T(G, A), H^1_T(G/G', A^{G'}) = 0 = H^2_T(G/G', A^{G'})$, and G/G' is cyclic, this leads to that $H^m_T(G/G', A^{G'}) = 0$ for every $m \in \mathbb{Z}$. Therefore, $H^m_T(G, A) = 0$ for all $m > 0$. We next show that $H^0(G, A) = 0$. Let $x \in A^G$, because $H^0_T(G/G', A^{G'}) = 0$, there is a $y \in A^{G'}$ so that $\mathrm{Nm}_{G/G'}(y) = x$. Moreover, since $H^0_T(G', A) = 0$, there is a $z \in A$ such that $\mathrm{Nm}_{G'}(z) = x$. We have

$$\mathrm{Nm}_G(z) = \mathrm{Nm}_{G/G'} \circ \mathrm{Nm}_{G'}(z) = x.$$

Therefore, $H^m_T(G, A) = 0$ for every $m \geq 0$. Now we consider the exact sequence

$$0 \to A \to \mathrm{Ind}^G(A_0) \to \mathrm{Ind}^G(A_0)/A \to 0$$

where A_0 is A as an abelian group. Because $\mathrm{Ind}^G(A_0)$ induced as an $G'-$module, $H^m_T(G', \mathrm{Ind}^G(A_0)) = 0$ for every $m \in \mathbb{Z}$ and every subgroup G' of G. Thus

$$H^m_T(G', A) = H^{m-1}_T(G', \mathrm{Ind}^G(A_0)/A)$$

for all m and all subgroup G'. Therefore, $\mathrm{Ind}^G(A_0)/A$ is satisfies the hypothesis of the theorem, and so $H_T^m(G, \mathrm{Ind}^G(A_0)/A) = 0$ for all $m \geq 0$:

$$0 = H_T^0(G, \mathrm{Ind}^G(A_0)/A) = H_T^{-1}(G, A).$$

We repeat the argument so $H_T^{-2}(G, A) = 0, H_T^{-3}(G, A) = 0, \ldots$. This demonstrates the lemma when we consider G as a solvable group.
Now we look at the general case for any finite group G. The lemma's hypotheses are satisfied by G_p and A as well, if G and A do, where G_p is a Sylow $p-$subgroup. For every $m \in \mathbb{Z}$ and all prime p, $H^m(G_p, A) = 0$. The $p-$primary component of $H^m(G, A)$ is zero for all m and all p, according to Corollary 1.2.36. This suggests that for any $m \in \mathbb{Z}$, $H^m(G, A) = 0$. ■

Theorem 1.4.28 (Tate's)
Let C be a $G-$module where G is a finite group. Suppose that for every G' subgroup of G, including $G' = G$,

1. *$H_T^1(G', C) = 0$, and*
2. *$H_T^2(G', C)$ is a cyclic group and its order equals to $|G'|$.*

Then for every $m \in \mathbb{Z}$, there exists an isomorphism

$$H_T^m(G, \mathbb{Z}) \xrightarrow{\cong} H_T^{m+2}(G, C).$$

Moreover, this isomorphism depends on how we choose the generator for $H^2(G, C)$.

Proof: Choose any generator γ from $H_T^2(G, C)$. Since the map $\mathrm{Cor} \circ \mathrm{Res} : H_T^2(G, C) \to H_T^2(G, C)$ is a multiplication by $[G : G']$, the group $H_T^2(H, C) = \langle \mathrm{Res}(\gamma) \rangle$ for each subgroup G' of G.
Let γ be represented by cocycle Φ. We say

$$C(\Phi) = C \oplus \bigoplus_{g \in G;\, g \neq 1} \mathbb{Z}[x_g]$$

and broaden the action of G on C to encompass $C(\Phi)$ by defining:

$$gx_t = x_{gt} - x_g + \Phi(g, t).$$

The notation x_1 should be understood as $\Phi(1, 1)$. This indeed establishes an action of G on $C(\Phi)$ since

$$rgx_t = x_{rgt} - x_{rg} + \Phi(rg, t)$$

and

$$\begin{aligned} r(gx_t) &= r(x_{gt} - x_g + \Phi(g, t)) \\ &= x_{rgt} - x_r + \Phi(r, gt) - (x_{rg} - x_r + \Phi(r, g)) + r\Phi(g, t) \\ &= x_{rgt} - x_{rg} + x_r + \Phi(r, gt) - \Phi(r, g) + r\Phi(g, t) \\ &= x_{rgt} - x_{rg} + \Phi(rg, t). \end{aligned} \tag{1.5}$$

The last equation comes from the cocycle condition

$$\Phi(r, gt) - \Phi(r, g) + r\Phi(g, t) = \Phi(rg, t).$$

The reason γ maps to $\overline{0} \in H_T^2(G, C(\Phi))$ is because Φ is the coboundary of the $1-$cochain $g \mapsto x_g$. This is the reason $C(\Phi)$ is referred to as γ's splitting module.
First, we will demonstrate that the hypotheses imply that, for all subgroups G' of G,

$$H_T^1(G', C(\Phi)) = 0 = H_T^2(G', C(\Phi))$$

We recall the following canonical exact sequence

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

where $I_G = \langle g - 1 | g \in G \rangle$. Because $\mathbb{Z}G$ is induced, $H_T^m(G', \mathbb{Z}G) = 0$ for all r, and so

$$\varphi(\tau) \cong H_T^0(G', \mathbb{Z}) \cong H_T^1(G', I_G)$$

and

$$H_T^2(G', I_G) \cong H_T^1(G', \mathbb{Z}) = 0$$

We define a additive mapping $\alpha : C(\Phi) \to \mathbb{Z}G$ so that $\alpha(x_g) = g - 1$ and $\alpha(c) = 0$ holds for all $c \in C(\Phi)$ Is is clear that the $G-$short sequece

$$0 \to C \to C(\Phi) \xrightarrow{\alpha} I_G \to 0$$

is exact. It induces the cohomology sequence

$$0 \to H_T^1(G', C(\Phi)) \to H_T^1(G', I_G) \to H_T^2(G', C) \xrightarrow{0} H_T^2(G', C(\Phi)) \to 0.$$

Because of $H_T^1(G', C) = 0$ and $H_T^2(G', I_G) = 0$, the zeros at the ends are used. Since $\text{Res}(\gamma)$ generates $H^2(G', C)$, the map $H_T^2(G', C) \to H_T^2(G', C(\Phi))$ is zero, and this maps to the restriction of the image of γ in $H_T^2(G, C(\Phi))$, which is also zero. Thus, $H_T^1(G', I_G) = H_T^2(G', C)$ is surjective, and hence it is an isomorphism. As a result, $H_T^1(G', C(\Phi))$ and $H_T^2(G', C(\Phi))$, its kernel and cokernel, are both zero.
Lemma 1.4.27 leads us to the conclusion that, for all m, $H_T^m(G', C(\Phi)) = 0$. We obtain an exact sequence by joining the two short exact sequences:

$$0 \to C \to C(\Phi) \to \mathbb{Z}G \to \mathbb{Z} \to 0$$

possessing the characteristic that, for all m, $H_T^m(G, C(\Phi)) = 0 = H_T^m(G, \mathbb{Z}G)$. The double boundary map is an isomorphism as a result

$$H_T^m(G, \mathbb{Z}) \xrightarrow{\cong} H_T^{m+2}(G, C).$$

□

Remark 1.4.29
The cup-product with the selected $\gamma \in H^2(G, C)$ is the map $H^m(G, \mathbb{Z}) \to H^{m+2}(G, C)$.

Chapter 2

Local Class Field Theory: Cohomology

2.1 Introduction of the second chapter

For the rest of this chapter, K is a non-Archimedean local field, $\mathcal{O}_K$ is its ring of integers (i.e., its valuation ring), $\mathfrak{m}_K$ is its maximal ideal, and k is its residue field.

The central construction in this chapter is the local Artin map, which is an isomorphism stated as follows:

$$\varphi_K : K^\times \overset{\cong}{\to} \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

or locally, for every finite abelian extension E/K:

$$\varphi_{E/K} : K^\times/\mathrm{N}_{E/K}(L^\times) \overset{\cong}{\to} \mathrm{Gal}(E/K).$$

In order to do that, we need to find out about the relation between Galois extensions of a local field and how they interact with their Galois groups. Initially, their relations will start with the unramified extensions - the most fundamental extensions of local fields. When we talk about the ramification of an extension of a local field, we are referring to how the extension behaves with respect to the valuation and the residue field. For some unramified extension E/K, the residue field of E is an extension of the residue field of K but does not introduce any new ramification. In other words, the extension of residue fields is purely algebraic and does not involve any new ramification behavior. In particular, $\mathrm{Gal}(E/K) = \mathrm{Gal}(e/k)$ where e is the residue field of E. For convenience, we can treat an unramified extension of a local field as a cyclic extension of a general abstract field.

Let U_K be the group of all unit elements in K and U_E be the group of all unit elements in E for some finite unramified extension E/K with the Galois group $G = \mathrm{Gal}(E/K)$, we see that U_E is a subgroup of $E^\times$ (and hence is a G-module) and moreover it is a compact subset of E in the natural topological sense. We will find that $H_T^m(G, U_E)$ is trivial for all integers m.

Next, the notion of the invariant map $\mathrm{inv}_{E/K} : H^2(E/K) \to \mathbb{Q}/\mathbb{Z}$ will be introduced. The construction of the invariant map typically begins by considering the Galois group of a finite, unramified extension L/K of a local field K. One then examines the corresponding ideal class group $\mathrm{Cl}(K)$ of the base field K. The invariant map takes an element of the Galois group $\mathrm{Gal}(L/K)$ and produces an element of the ideal class group $\mathrm{Cl}(K)$, reflecting how the Galois group permutes ideals in K.

Finally, the Local Reciprocity Law Theorem will warrant the existence of the Local Artin map.

2.2 The Cohomology of Uramified Extensions of Local Fields

2.2.1 Group cohomology of the ring of units

Proposition 2.2.1
An finite unramified extension of local fields E/K induces a surjective norm map

$$\mathrm{Nm}_{E/K} : U_E \to U_K.$$

To demonstrate this claim, we require the following lemmas:

Lemma 2.2.2
For $r > 0$, let $U_E^{(r)} := 1 + \mathfrak{m}_E^r$. Then

$$U_E/U_E^{(1)} \cong e^\times$$

and

$$U_E^{(r)}/U_E^{(r+1)} \cong e$$

as $G-$module.

Proof: Let $\mathfrak{m}_K = \pi\mathcal{O}_K$. In E, it is still prime, and

$$U_E^{(r)} = 1 + \pi^r\mathcal{O}_E.$$

The homomorphisms

$$u \mapsto u \mod \mathfrak{m}_E : U_E \to e^\times;$$
$$1 + a\pi^r \mapsto a \mod \mathfrak{m}_E : U_E^{(r)} \to e$$

induce the required isomorphisms. □

Lemma 2.2.3
$H_T^m(G, e^\times) = 0$, for every m. More specifically, there is a surjective norm map $e^\times \to k^\times$.

Proof: Let $G := \mathrm{Gal}(E/K)$, because E/K is unramified extension, G is also the Galois group of their residue fields extension e/k. Moreover, E/K is finite so G is cyclic. By Theorem 1.2.26, $H^1(G, e^\times) = 0$, and because $e^\times$ is finite so $H^2(G, e^\times) = 0$. Therefore by Proposition 1.4.9, $H_T^m(G, e^\times) = 0$ for all m. In particular,

$$0 = H_T^0(G, e^\times) = (e^\times)^G / \mathrm{Nm}_G(e\times) = k^\times / \mathrm{Nm}(e^\times)$$

so $k^\times = \mathrm{Nm}(e^\times)$ or the norm map $e^\times \to k^\times$ is surjective. □
Similarly, we have

Lemma 2.2.4
$H_T^m(G, e) = 0$ for every m. More specifically, there is a surjective trace map $e^\times \to k^\times$.

Proof: (of the proposition) Let $u \in U_K$. There is a $e_0 \in U_E$ so that $\mathrm{Nm}(e_0) \equiv u \mod U_k^{(1)}$, since $\mathrm{Nm}\, e^\times \to k^\times$ is surjective. For the same reason that the norm map $U_E^{(1)}/U_E^{(2)} \to U_K^{(1)}/U_K^{(2)}$ is surjective, so is the trace map $e \to k$, and so there is a $e_1 \in U_E^{(1)}$ such that $\mathrm{Nm}(e_1) \equiv u/\mathrm{Nm}(e_0) \mod U_K^{(2)}$. By following this pattern, we generate a sequence $e_0, e_1, e_2, \dots \in U_K^{(i)}$, so that $u/\mathrm{Nm}(e_0 \dots e_i) \in U_K^{(i+1)}$. Let $\overline{e} = \lim_{i\to\infty} \prod_{j=1}^{i} v_j$. Thus $u/\mathrm{Nm}(\overline{e}) \in \bigcap U_K^{(i)} = \{1\}$. □

Proposition 2.2.5
Consider extension E/K : finite, unramified with $G = \mathrm{Gal}(E/K)$. Then

$$H_T^m(G, U_E) = 0, \ \forall m \in \mathbb{Z}.$$

Proof: Let $\pi \in K$ be a prime and hence it is a prime in E as well. We get

$$E^\times \cong U_E \times \pi^{\mathbb{Z}}.$$

Thus, according to Proposition 1.2.31

$$H^m(G, E^\times) = H^m(G, U_E) \oplus H^m(G, \pi^{\mathbb{Z}})$$

since $H^1(G, E^\times) = 0$ (by Theorem 1.2.26), $H^1(G, U_E) = 0$. Given that G is cyclic, proving $H^0(G, U_E) = 0$ is sufficient to finish the proof. This can be done directly by Proposition 2.2.1. □

Remark 2.2.6
Let E/K be an unramified extension and $[E : K] = \infty$, for all $m \geq 0$,

$$H^m(\mathrm{Gal}(E/K), U_E) = \varinjlim_{L} H^m(\mathrm{Gal}(L/K), U_L),$$

where the limit is over the finite extensions L/K such that $L \subset E$. Thus,

$$H^m(\mathrm{Gal}(E/K), U_E) = 0$$

for all $m > 0$.

2.2.2 Constructing the invariant map

Definition 2.2.7 (Frobenius element)
Given a non-Archimedean local field K, let E be its finite unramified extension. Hence, E/K is Galois and for every $a \in \mathcal{O}_E$, there is one and only one $\sigma \in \mathrm{Gal}(E/K)$ so that $a^q = \sigma a$ (where $q = |k|$). Denoted as $\mathrm{Frob}_{E/K}$, this σ is known as the Frobenius element of $\mathrm{Gal}(E/K)$ and it generates $\mathrm{Gal}(E/K)$.

Definition 2.2.8
For any Galois extension E/K, let

$$H^2(E/K) = H^2(\mathrm{Gal}(E/K), E^\times).$$

In the case E/K is unramified and $G = \mathrm{Gal}(E/K)$. From the $G-$cohomology sequence

$$0 \to U_E \to E^\times \xrightarrow{\mathrm{ord}_E} \mathbb{Z} \to 0.$$

An isomorphism is obtained:

$$H^1(G, E^\times) \overset{\cong}{\to} H^1(G, \mathbb{Z}).$$

The $G-$short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

induces a long exact sequence of cohomology, it leads to the isomorphism

$$H^2(G, \mathbb{Z}) \overset{\cong}{\to} H^1(G, \mathbb{Q}/\mathbb{Z}).$$

Recall that

$$H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{Q}/\mathbb{Z}).$$

If the degree of the extension E/K is equal to r, then the group $G = \langle \mathrm{Frob}_{E/K} \rangle$ of order r. The mapping defined by

$$f \mapsto f(\mathrm{Frob}_{E/K}) : \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$$

illustrates the r-order of $\mathbb{Q}/\mathbb{Z}$. When $[E : K] = \infty$, the group G is topologically generated by $\mathrm{Frob}_{E/K}$. This indicates that $G = \mathrm{Cl}\{\mathrm{Frob}^j_{E/K} : j \in \mathbb{Z}\}$. Furthermore, the mapping $f \mapsto f(\mathrm{Frob}_{L/K})$ establishes an isomorphism from $\mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{Q}/\mathbb{Z})$ to an infinite subgroup of $\mathbb{Q}/\mathbb{Z}$.

Definition 2.2.9 (Invariant map)
The composite of

$$H^2(E/K) \overset{\cong}{\to} H^2(G, \mathbb{Z}) \overset{\cong}{\to} H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\mathrm{Frob}_{E/K})} \mathbb{Q}/\mathbb{Z}$$

is called the invariant map

$$\mathrm{inv}_{E/K} : H^2(E/K) \to \mathbb{Q}/\mathbb{Z}.$$

Example 2.2.10
In the case $K = \mathbb{Q}_5$, consider a finite abelian extension $E = \mathbb{Q}_5(\sqrt[3]{5})$ of K. Since this is a cyclic extension of degree 3, the Galois group $G = \mathrm{Gal}(E/K)$ is cyclic of order 3.
The invariant map in this case sends the generator σ of G to $\frac{1}{[E:K]} = \frac{1}{3} \in \mathbb{Q}/\mathbb{Z}$. In particular, Let $\sigma : \sqrt[3]{5} \mapsto \zeta\sqrt[3]{5}$, where ζ is a primitive cube root of unity. The invariant map

$$\mathrm{inv}_{E/K}(\sigma) = \frac{1}{3} \in \mathbb{Q}/\mathbb{Z}.$$

Therefore, each power of σ corresponds to a multiple of $\frac{1}{3}$:

1. $\mathrm{inv}_{E/K}(1_G) = 0$;
2. $\mathrm{inv}_{E/K}(\sigma) = \frac{1}{3}$;
3. $\mathrm{inv}_{E/K}(\sigma^2) = \frac{2}{3}$.

Proposition 2.2.11
When E/K is finite and $[E/K] = r$. Let K^{un} and E^{un} be the largest unramified extensions of K and E, respectively. The diagram:

$$\begin{tikzcd}
H^2(K^{\text{un}}/K) \arrow[r, "\text{Res}"] \arrow[d, "\text{inv}_K"] & H^2(E^{\text{un}}/E) \arrow[d, "\text{inv}_E"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "\times r"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

commutes.

Proof: Consider the map

$$\tau \mapsto \tau|_{K^{\text{un}}} : \text{Gal}(E^{\text{un}}/E) \to \text{Gal}(K^{\text{un}}/K)$$

because $E^{\text{un}} = L \cdot K^{\text{un}}$, it is injective. The restriction map is defined by the compatible homomorphism $\text{Gal}(E^{\text{un}}/E) \to \text{Gal}(K^{\text{un}}/K)$ and $(K^{\text{un}})^\times \to (E^{\text{un}})^\times$ Let $G_K = \text{Gal}(K^{\text{un}}/K)$ and $G_E = \text{Gal}(E^{\text{un}}/E)$. Consider the diagram:

$$\begin{tikzcd}
H^2(K^{\text{un}}/K) \arrow[r, "\cong"] \arrow[d, "\text{Res}"] & H^2(G_K, \mathbb{Z}) \arrow[r, "\cong"] \arrow[d, "r\,\text{Res}"] & H^1(G_K, \mathbb{Q}/\mathbb{Z}) \arrow[r] \arrow[d, "r\,\text{Res}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "fe"] \\
H^2(E^{\text{un}}/E) \arrow[r, "\cong"] & H^2(G_E, \mathbb{Z}) \arrow[r, "\cong"] & H^1(G_E, \mathbb{Q}/\mathbb{Z}) \arrow[r] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

The residue class degree and ramification index ofE/K are denoted by f and e in this case. The commutative square yields the square on the left.

$$\begin{tikzcd}
(K^{\text{un}})^\times \arrow[r, "\text{ord}_K"] \arrow[d] & \mathbb{Z} \arrow[d, "\times r"] \\
(E^{\text{un}})^\times \arrow[r, "\text{ord}_E"] & \mathbb{Z}
\end{tikzcd}$$

The restriction map and boundary map commute, as indicated by the second square. Here is the third square:

$$\begin{tikzcd}
\text{Hom}(G_K, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\text{Frob}_K"] \arrow[d, "\varphi \mapsto \varphi|_{G_E}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\times f"] \\
\text{Hom}(G_E, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\text{Frob}_E"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

Where Frob_K and Frob_E maps are $\varphi \mapsto \varphi(\text{Frob}_K)$ and $\varphi \mapsto \varphi(\text{Frob}_E)$, respectively. If $q = |k|$ and $q^f = |e|$, then the Frobenius elements induce $x \mapsto x^q$ and $x \mapsto x^{q^f}$ on the residue field. Therefore, $\text{Frob}_L |_K = \text{Frob}_K^f$. Because $n = rf$, the square commutes. □

2.3 Local Artin map

Remark 2.3.1 (Construction of Local Artin map)
Let $\overline{K}$ be the algebraic closure of K (in the case K has charateristic $p > 0$, we uniformize the notation $\overline{K}$ with K^{sep} - the separable closure of K) and $q = |k|$ (necessarily q is a power of a prime). Let K^{un} be the largest unramified extension of K which can be obtained by taking $\bigcup E$ where E runs over all finite unramified extensions of K. We can see that K^{un} is well-defined since $E \cdot F/K$ is unramified for every finite unramified E/K and F/K. The algebraic closure of the residue filed k of K is the residue field $\overline{k}$ of K^{un}.
All automorphisms σ of K^{un} that fix K preserves the field norm $|\cdot|$. Consequently, it induces an automorphism $\overline{\sigma}$ of $\overline{k}/k$ on K^{un}. The map

$$\mathrm{Gal}(K^{\mathrm{un}}/K) \to \mathrm{Gal}(\overline{k}/k) : \sigma \to \overline{\sigma}$$

is an isomorphism. Hence, $(x \mapsto x^q) : \overline{k} \to \overline{k}$ and $\alpha \mapsto \mathrm{Frob}_K^{\alpha} : \hat{\mathbb{Z}} \to \mathrm{Gal}(K^{\mathrm{un}}/K)$ are both induced by the unique element $\mathrm{Frob}_K \in \mathrm{Gal}(K^{\mathrm{un}}/K)$.

We will prove the existence of a group homomorphism (called **local Artin map**)

$$\varphi_K : K^{\times} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

with these two properties:

1. $\varphi_K(\pi)|_{K^{\mathrm{un}}} = \mathrm{Frob}_K$ for any prime element π of K;
2. The kernel of $a \mapsto \varphi_K(a)|_E$ contains $\mathrm{Nm}_{E/K}(E^{\times})$ for any E/K finite abelian, and φ_K induces
$$\varphi_{E/K} : K^{\times}/\,\mathrm{Nm}_{E/K}(L^{\times}) \to \mathrm{Gal}(E/K).$$

Lemma 2.3.2
Consider $L \subset E \subset K$ as a Galois extension tower. Then

$$\mathrm{Res}(u_{L/K}) = u_{L/E}$$

and

$$\mathrm{Inf}(u_{E/K}) = [L : E]u_{L/K}.$$

Proof: Let $[E : K] = n, [L : E] = m.$ Consider

$$\begin{tikzcd}
H^2(\overline{K}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"] & H^2(\overline{K}/E) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_L"] & H^2(\overline{K}/E) \arrow[d, "\mathrm{inv}_L"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "\times n"] & \mathbb{Q}/\mathbb{Z} \arrow[r, "\times m"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

Each of the vertical maps is an isomorphism. We get the following commutative diagram after applying the kernel-cokernel lemma to the rows:

$$\begin{tikzcd}
0 \arrow[r] & H^2(E/K) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\mathrm{inv}_{E/K}"] & H^2(L/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_{L}\,_{/K}"] & H^2(L/E) \arrow[d, "\mathrm{inv}_{L/E}"] \\
0 \arrow[r] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[r, "\mathrm{id}"] & \frac{1}{mn}\mathbb{Z}/\mathbb{Z} \arrow[r, "\times n"] & \frac{1}{m}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}$$

The fact that the two squares commute leads us to

$$\operatorname{Res}(u_{L/K}) = u_{L/E}$$

and

$$\operatorname{Inf}(u_{E/K}) = [L : E]u_{L/K}.$$

■

Proposition 2.3.3
Given a finite Galois extension E/K with a Galois group G, there is a canonical isomorphism exists for all m:

$$H_T^m(G, \mathbb{Z}) \to H_T^{m+2}(G, E^\times).$$

Proof: For every subgroup G' of G, it is straightforward to verify that

1. $H^1(G', E^\times) = 0$ by the Hilbert's Theorem 1.2.26.
2. $H^2(G', E^\times) = \langle u_{E/E^{G'}} = \operatorname{Res}(u_{E/K})\rangle$ and $|H^2(G', E^\times)| = |G'|$.

The conditions of Tate's theorem are fulfilled by the pair $(G, E^\times)$. Therefore

$$H_T^m(G, \mathbb{Z}) \to H_T^{m+2}(G, E^\times)$$

□

Corollary 2.3.4
In the case of a finite Galois extension of local fields with Galois group G denoted by E/K:

$$H_2(G, \mathbb{Z}) = H_T^{-2}(G, \mathbb{Z}) \to H_T^0(G, E^\times)$$

or

$$G^{ab} \cong K^\times / \operatorname{Nm}_{E/K}(E^\times).$$

Proof: This is directly implied by Proposition 2.3.3 by letting $m = 2$. □

Remark 2.3.5
*In the case of a finite abelian extension E/K, we can define the **local Artin map** as*

$$\varphi_{E/K} : K^\times / \operatorname{Nm}(E^\times) \to \operatorname{Gal}(E/K) = G^{ab}$$

by stipulating that it is the inverse of the isomorphism

$$G^{ab} \xrightarrow{\cong} K^\times / \operatorname{Nm}(E^\times).$$

Theorem 2.3.6 (Norm limitation)
Let E/K be finite Galois and L/K be maximal abelian among all $L \subset E$. We can state that

$$\operatorname{Nm}_{L/K}(L^\times) = \operatorname{Nm}_{E/K}(E^\times).$$

Proof: Let $G = \mathrm{Gal}(E/K)$. Since $\mathrm{Nm}_{E/K} = \mathrm{Nm}_{E/L} \circ \mathrm{Nm}_{L/K}$, it follows that $\mathrm{Nm}_{E/K}(E^\times)$ is contained within $\mathrm{Nm}_{L/K}(L^\times)$. In light of this, we have $\mathrm{Gal}(L/K) = \mathrm{Gal}(E/K)^{\mathrm{ab}} = G^{\mathrm{ab}}$, which means that the norm groups have the same index in $K^\times$, since by the Corollary 2.3.4,

$$K^\times / \mathrm{Nm}_{E/K}(E^\times) \cong G^{\mathrm{ab}} = (G^{\mathrm{ab}})^{\mathrm{ab}} \cong K^\times / \mathrm{Nm}_{L/K}(L^\times).$$

Consequently, this indicates that the norm groups are indeed equal. □

Proposition 2.3.7
In the case where $L \supset E \supset K$ forms a tower of finite ablian extensions of K, it follows that

$$\varphi_{L/K}(a)|_E = \varphi_{E/K}(a)$$

holds true for all $a \in K$.

Proof: The local Artin maps' definition allows us to directly check this by using $\mathrm{Inf}(u_{E/K}] = [L : E]u_{L/K}$. □

Remark 2.3.8
In the case where E/K is a finite unramified extension with $G = \mathrm{Gal}(E/K)$ and $n = [E : K]$, there exists an isomorphism given by

$$G = G^{ab} = H_T^{-2}(G, \mathbb{Z}) \to H_T^0(G, E^\times) = K^\times / \mathrm{Nm}(E^\times).$$

For every prime $\pi \in E$, $\alpha \in E^\times$ can be expressed uniquely in the form $\alpha = u\pi^t$ for some $u \in U_E$ and $t \in \mathbb{Z}$. Consequently,

$$E^\times = U \times \pi^{\mathbb{Z}} \cong U_E \times \mathbb{Z}.$$

As E is unramified over K, we have the freedom to select $\pi \in K$. This allows us to express $\tau\alpha$ as $\tau(u\pi^t) = (\tau u)\pi^t$ for $\tau \in \mathrm{Gal}(E/K)$, making the previous expression a decomposition of $G-$modules, with G acting on $\mathbb{Z} \cong \pi^{\mathbb{Z}}$ trivially.

Remark 2.3.9
Select an element $\sigma \in G$ to be the generator, and consider

$$f \in H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

as the element such that $f(\sigma^t) = \frac{t}{r} \mod \mathbb{Z}$ for all t. It is responsible for generating $H^1(G, \mathbb{Q}/\mathbb{Z})$. By using the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

and the fact that $H^m(G, \mathbb{Q}) = 0$ for all m, we can establish an isomorphism

$$\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z}).$$

In order to form δf, we select a lift of f to a $1-$cochain $\overline{f} : G \to \mathbb{Q}$. We define $\overline{f}$ as the function $\sigma^t \mapsto \frac{i}{r}$, where $0 \le t < r - 1$. Then

$$d\overline{f}(\sigma^t, \sigma^k) = \sigma^t \overline{f}(\sigma^k) - \overline{f}(\sigma^{t+k}) + \overline{f}(\sigma^k) = \begin{cases} 0 & \textit{if } t + k \le r - 1 \\ 1 & \textit{if } t + k > r - 1 \end{cases}$$

When $\mathbb{Z}$ is matched with $\pi^{\mathbb{Z}} \leq E^{\times}$, we can observe $u_{E/K} \in H^2(G, E^{\times})$ is depicted by the cocycle:

$$\varphi(\sigma^t, \sigma^k) = \begin{cases} 0 & \textit{if } t+k \leq r-1 \\ \pi & \textit{if } t+k > r-1 \end{cases}$$

The sequences

$$0 \to I \to \mathbb{Z}G \to \mathbb{Z} \to 0$$

and

$$0 \to E^{\times} \to E^{\times}(\varphi) \to I \to 0$$

yields

$$H_T^{-2}(G, \mathbb{Z}) \overset{\cong}{\to} H_T^{-1}(G, I)$$

$$H_T^{-1}(G, I) \overset{\cong}{\to} H_T^{0}(G, I)$$

Since both $\mathbb{Z}G$ and $E^{\times}(\varphi)$ exhibit trivial cohomology. In this context, $E^{\times}(\varphi)$ denotes the splitting module $E^{\times} \oplus \bigoplus_{\sigma \in G, \sigma \neq 1} \mathbb{Z}x_{\sigma}$ associated with φ.

Proposition 2.3.10
The composite of mapping in the following sequence

$$G \overset{\cong}{\to} H^{-2}(G, \mathbb{Z}) \to H^0(G, E^{\times}) \overset{\cong}{\to} K^{\times}/\operatorname{Nm}_G(E^{\times})$$

maps $\sigma \in G \mapsto \pi \mod \operatorname{Nm}_G(E)$.

Proof: $H^{-2}(G, \mathbb{Z}) \cong G$ indicates that under $H^{-2}(G, \mathbb{Z}) \to H^{-1}(G, I_G) \subset I_G/I_G^2$, the element σ is represented as $\sigma - 1$.
$H^{-1}(G, I_G) \to H^0(G, E^{\times})$ is determined by the snake lemma applied to

$$\begin{tikzcd}
 & & & H^{-1}(G, I_G) \arrow[d] & \\
 & (E^{\times})_G \arrow[r] \arrow[d] & E^{\times}(\varphi)_G \arrow[r] \arrow[d] & (I_G)_G \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & (E^{\times})^G \arrow[r] \arrow[d] & E^{\times}(\varphi)^G \arrow[r] & I^G & \\
 & H^0(G, E^{\times}) & & &
\end{tikzcd}$$

Where the vertical maps are $\operatorname{Nm}_G = \sum_{t=0}^{r-1} \sigma^t$ and $(\sigma - 1) + I_G^2$ is the image of $x_{\sigma} + I_G \cdot E^{\times}(\varphi)_G$ in $E^{\times}(\varphi)_G$ and $\operatorname{Nm}_G(x_{\sigma} + I_G \cdot E^{\times}(\varphi))$ is

$$\sigma x_{\sigma} = \varphi(\sigma, \sigma) + x_{\sigma^2} - x_{\sigma};$$

$$\sigma^2 x_{\sigma} = \varphi(\sigma, \sigma^2) + x_{\sigma^3} - x_{\sigma^2}$$

$$\ldots;$$

$$\sigma^{t-1} x_{\sigma} = x_1 - x_{\sigma^{t-1}} + \varphi(\sigma, \sigma^{t-1});$$

where $1 = \varphi(1,1) = x_\sigma$ and plus on the $E^\times$ of $E(\varphi)$ is "$\cdot$", thus

$$\mathrm{Nm}_G(x_\sigma) = \prod_{t=1}^{r-1} \varphi(\sigma, \sigma^t) = \pi.$$

□

Lemma 2.3.11
If the extension E/K is Galois with a finite degree n, then the group $H^2(E/K)$ contains a subgroup of order n.

Proof: Consider the diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(\mathrm{Res}) \arrow[r] \arrow[d] & H^2(K^{\mathrm{un}}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{Res}"] & H^2(E^{\mathrm{un}}/E) \arrow[d, "\mathrm{Res}"] \\
0 \arrow[r] & H^2(E/K) \arrow[r] & H^2(\overline{K}/K) \arrow[r, "\mathrm{Res}"] & H^2(\overline{K}/E)
\end{tikzcd}$$

The injectivity of the two restriction maps implies that the first vertical map is also injective. However, Proposition 2.2.11 demonstrates that the Ker(Res) on the first row is $\frac{1}{r}\mathbb{Z}/\mathbb{Z}$. □
Now we need to prove that the map $\frac{1}{r}\mathbb{Z}.\mathbb{Z} \hookrightarrow H^2(E/K)$ is an isomorphism.

Lemma 2.3.12
In the case where E/K is finite Galois and $G = \mathrm{Gal}(E/K)$, there exists $O \subset_{open} \mathcal{O}_E$, which remains stable under G and satisfies $H^m(G, O) = 0$ for every $m > 0$.

Proof: Consider $\{x_\sigma | \sigma \in G\}$ as a normal basis for E over K. The elements x_σ share a common denominator d in $\mathcal{O}_K$. By replacing each x_σ with $d \cdot x_\sigma$, we can assume that they belong to $\mathcal{O}_E$. Let $O = \sum \mathcal{O}_E x_\sigma$. Then it follows that

$$O \cong \mathcal{O}_E[G] = \mathrm{Ind}^G \mathcal{O}_E$$

and consequently $H^m(G, O) = 0$ for all $m > 0$. □

Lemma 2.3.13
An open subgroup O of U_E exists that is stable under G, and for all $m > 0$, it satisfies $H^m(G, O) = 0$.

Example 2.3.14
If char$K = 0$, then the power series

$$e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$$

converges for $\mathrm{ord}(p)/(p-1) < \mathrm{ord}(x)$. *It establishes an isomorphism between an open neighborhood of* 0 *in* E *and a neighborhood of* 1 *in* $E^\times$*, and its inverse is*

$$\log(x) = -\sum_{i=1}^{\infty} \frac{(1-x)^i}{i}.$$

It is evident that both mappings are compatible within the $G-$action. If O' is an open neighborhood of 0 as described in Lemma 2.3.12, then $\pi^M O'$ will possess the same properties, and we can choose $O = \exp(\pi^M O')$ where M is sufficiently large to ensure the exponential function is defined on $\pi^M O'$.

Lemma 2.3.15
In the case where E/K is finite Galois $[E : K] = r$, the order of $H^2(E/K)$ is also r.

Proof: We note that r divides $|H^2(E/K)|$ and $|H^2(E/K)| = r$ when E/K is cyclic. We will establish the lemma using induction on $[E : K]$. As $\mathrm{Gal}(E/K)$ is solvable, there is L/K Galois such that $E \supset L \supset K$. From the sequence

$$0 \to H^2(L/K) \to H^2(E/K) \to H^2(E/L)$$

we can conclude that

$$r = |H^2(L/K)| \times |H^2(E/L)| \geq |H^2(E/K)|.$$

□

Now we are prepared to demonstrate the main theorem:

Theorem 2.3.16
We can construct an isomorphism

$$\mathrm{inv}_K : H^2(\overline{K}/K) \to \mathbb{Q}/\mathbb{Z}$$

on every non-archimedean local field K. In addition, if $[E : K] = r$, then the diagram

$$\begin{tikzcd}
0 \arrow[r] & H^2(E/K) \arrow[r] & H^2(\overline{K}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"] & H^2(\overline{K}/E) \arrow[d, "\mathrm{inv}_E"] \\
0 \arrow[r] & \frac{1}{r}\mathbb{Z}/\mathbb{Z} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r, "\times r"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

is commutative, and thus defines a canonical isomorphism

$$\mathrm{inv}_{E/K} : H^2(E/K) \to \frac{1}{r}\mathbb{Z}/\mathbb{Z}.$$

Proof: We represent the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker(Res)} \arrow[r] \arrow[d] & H^2(K^{\mathrm{un}}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{Res}"] & H^2(E^{\mathrm{un}}/E) \arrow[d, "\mathrm{Res}"] \\
0 \arrow[r] & H^2(E/K) \arrow[r] & H^2(\overline{K}/K) \arrow[r, "\mathrm{Res}"] & H^2(\overline{K}/E)
\end{tikzcd}$$

For any E/K finite Galois, we observe that $H^2(E/K) \leq H^2(\overline{K}/K)$ and $H^2(E/K) \subset H^2(K^{\mathrm{un}}/K)$. This implies that $H^2(\overline{K}/K) = \bigcup H^2(E/K)$, demonstrating that the inflation map $H^2(K^{\mathrm{un}}/K) \to H^2(\overline{K}/K)$ forms an isomorphism. Consequently, the invariant map $\mathrm{inv}_K : H^2(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$ establishes an isomorphism $H^2(\overline{K}/K) \to \mathbb{Q}/\mathbb{Z}$. As a result of Lemma 2.3.11, it satisfies the necessary properties for the theorem. Furthermore, the Proposition 2.3.10 (with chosen σ)

demonstrates that the homomorphism possesses the necessary properties for 2.2.11. Therefore, the commutativity of the diagram can be directly inferred from Proposition 2.2.11. Let's now examine

$$L \supset E \supset K,$$

with L/K and E/K being uramified. The following diagram

$$\begin{tikzcd}
H^2(E/K) \arrow[r, "\mathrm{inv}_{E/K}"] \arrow[d, "\mathrm{Inf}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\cong"] \\
H^2(L/K) \arrow[r, "\mathrm{inv}_{L/K}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

is commutative, as inv and Inf being compatible.
Specifically, there exists a natural isomorphism

$$\mathrm{inv}_K : H^2(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$$

such that for every $E \subset K^{\mathrm{un}}$ with E/K finite, the map inv_K induces

$$\mathrm{inv}_{E/K} : H^2(E/K) \xrightarrow{\cong} \frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z}.$$

□

Theorem 2.3.17 (Local Reciprocity Law)
On a non-Archimedean local field K, we defined the local Artin map, denoted as

$$\varphi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$$

exists and it satisfies the following properties:

1. *For each prime number π in the field K, the restriction of the Frobenius map $\varphi_K(\pi)_{|K^{\mathrm{un}}}$ holds true.*

2. *Every finite abelian extension E of K has the property that $\mathrm{Nm}_{E/K}(E^\times)$ is included in the kernel of the map $a \mapsto \varphi_K(a)_{|E}$, and the function φ_K causes an one-to-one correspondence denoted by*
$$\varphi_{E/K} : K^\times/\,\mathrm{Nm}_{E/K}(E^\times) \to \mathrm{Gal}(E/K).$$

Proof: It's all clear now, except for 1. This is because in the case of an unramified extension E of K, $\varphi_{E/K}$ is consistent with the one defined, so we can simply use Proposition 2.3.10. □

Corollary 2.3.18
Let K be a nonarchimedean local field and$\varphi : K^\times \to \mathrm{Gal}(K^{ab}/K)$ is its local Artin map. Then

1. *The function that maps E to $\mathrm{Nm}(E^\times)$ forms an one-to-one correspondence between the collection of finite abelian extensions of K and the assortment of norm groups in $K^\times$.*

2. *$E \subset E' \iff \mathrm{Nm}(E^\times) \supset \mathrm{Nm}(E'^\times)$.*

3. *$\mathrm{Nm}((E \cdot E')^\times) = \mathrm{Nm}(E^\times) \cap \mathrm{Nm}((E')^\times)$.*

4. *$\mathrm{Nm}((E \cap E')^\times) = \mathrm{Nm}(E^\times) \cdot \mathrm{Nm}((E')^\times)$.*

5. *The statement is that any subgroup of $K^\times$ that includes a norm group is also a norm group itself.*

Proof: We note that the transitivity of norms can be expressed as

$$\mathrm{Nm}_{L/K} = \mathrm{Nm}_{E/K} \circ \mathrm{Nm}_{L/E}\,.$$

This implies that if $E \subset L$, then

$$\mathrm{Nm}(E^\times) \supset \mathrm{Nm}(L^\times)$$

Hence, it follows that $\mathrm{Nm}((E \cdot L)^\times)$ is a subset of $\mathrm{Nm}(E^\times) \cap \mathrm{Nm}(L^\times)$. On the other hand, if $a \in \mathrm{Nm}(E^\times) \cap \mathrm{Nm}(L^\times)$, then

$$\varphi_{E/K}(a) = 1 = \varphi_{L/K}(a).$$

In the given context, it is evident that $\varphi_{LE/K}(a)_{|E} = \varphi_{E/K}(a)$ and $\varphi_{LE/K}(a)_{|E} = \varphi_{L/K}(a)$. Since the mapping

$$\sigma \mapsto (\sigma_{|E}, \sigma_{|L}) : \mathrm{Gal}(LE/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(L/K)$$

is shown to be injective, it follows that $\varphi_{LE/K}(a) = 1$, thus implying that $a \in \mathrm{Nm}((E \cdot L)^\times)$. Now we establish 3. Next, we finalize the demonstration of 2. If $\mathrm{Nm}(E^\times) \supset \mathrm{Nm}(L^\times)$, then statement 3 transforms into

$$\mathrm{Nm}((LE)^\times) = \mathrm{Nm}(L^\times).$$

The norm group's index corresponds to the abelian extension's degree that defines it, and since $LE \supset L$, this means that $LE = L$. Therefore, $L \supset E$.
The mapping $E \mapsto \mathrm{Nm}(E^\times)$ is surjective, as per the definition, and it can be inferred from point 2 that it is also injective. This proves 1.
We will now establish 5. Suppose $N = \mathrm{Nm}(L^\times)$ and I contains N. Let M denote the field that is fixed by $\varphi_{E/K}(I)$, such that $\varphi_{L/K}$ bijectively maps I/N to $\mathrm{Gal}(E/M)$. We examine the commutative diagram,

$$\begin{tikzcd}
K^\times \arrow[r, "\varphi_{E/K}"] \arrow[d, "\cong"] & \mathrm{Gal}(E/K) \arrow[d] \\
K^\times \arrow[r, "\varphi_{M/K}"] & \mathrm{Gal}(M/K)
\end{tikzcd}$$

The kernel of $\varphi_{M/K}$ can be represented as $\mathrm{Nm}(M^\times)$. Conversely, the kernel of the sequence

$$K^\times \to \mathrm{Gal}(E/K) \to \mathrm{Gal}(M/K)$$

is equal to $\varphi_{E/K}^{-1}(\mathrm{Gal}(E/M))$, which equals to I.
At last, we demonstrate 4. There exists a bijective mapping that reverses the order between two sets in 1. Since $E \cap L$ represents the most extensive expansion of K that is present in both E and L, and $\mathrm{Nm}(E^\times) \cdot \mathrm{Nm}(L^\times)$ is the smallest subgroup that includes both $\mathrm{Nm}(E^\times)$ and $\mathrm{Nm}(L^\times)$ (as specified in 5), the two sets must correspond to each other. □

Example 2.3.19
In the case where K is an archimedean local field, $K = \mathbb{R}$ or $\mathbb{C}$. For $K = \mathbb{C}$, everything is trivial since $\overline{K} = K$ itself. If $K = \mathbb{R}$ then $\mathbb{R}$ and $\mathbb{C}$ are the only two abelian extensions of K, we have $\mathrm{Nm}(\mathbb{R}^\times) = \mathbb{R}^\times$ and $\mathrm{Nm}(\mathbb{C}^\times) = \mathbb{R}_{>0}$. Let $H \leq \mathbb{R}^\times$ with $(\mathbb{R}^\times : H) < \infty$ then H is either $\mathbb{R}^\times$ or $\mathbb{R}_{>0}$. Hence, the isomorphism

$$\mathbb{R}^\times/\mathbb{R}_{>0} \xrightarrow{\cong} \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cong} \mathrm{Gal}(\mathbb{C}/\mathbb{R})$$

is termed the local Artin map for $K = \mathbb{R}$.

Chapter 3

Local Class Field Theory: Lubin-Tate theory

3.1 Introduction of the third chapter

While researching Local Class Field theory, John Tate and Jonathan Lubin realized that the action of ramification groups of local field abelian extensions is extremely similar to a special class of formal group laws.

In the beginning of this chapter, we introduce the formal group laws (a class of formal power series ring $R[[X_1, X_2]]$). This is just formal algebra to soon support our theory of Lubin-Tate. After that, let R be the ring of integers of a non-Archimedean local field K. Within any fixed prime $\pi \in R$, we can define another special formal power series of the ring $R[[X]]$ and denote it by $\mathcal{F}_\pi$. By that mean, every $f \in \mathcal{F}_\pi$ can be seen as an endomorphism of a formal group law, soon denoted by F_f and called Lubin-Tate formal series.

After that, we construct K^{un} - the maximal unramified extension of K - by joining every cyclic extension of K that is generated by the $m-$th roots of unity. We need to construct an abelian extension of E of K large enough so we get an isomorphism which is similar to the local Artin map:

$$A^\times \cong \text{Gal}(E/K).$$

This field is soon denoted by K_π and it only depends on the way we choose the prime π.

In the last part, we will prove that K_π is actually the missing component of K^{un} in the Kronecker-Weber theorem:

$$K^{\text{ab}} = K_\pi \cdot K^{\text{un}}.$$

We also prove the statement (so-called the Existence Theorem) that when we view $K^\times$ as a topological group, then every open subgroup of it is actually of the form $\text{Nm}_{E/K}(E^\times)$ for some finite extension E/K.

3.2 The basic notion of formal group laws

Definition 3.2.1 (Formal group law)
We call a (one dimensional) commutative formal group law over a commutative ring R is a formal power series $F(X_1, X_2) \in R[[X_1, X_2]]$ in two variables with coefficients in R such that

1. $F(X_1, 0) = X_1$ *and* $F(0, X_2) = X_2$,

2. $F(X_1, F(X_2, X_3)) = F(F(X_1, X_2), X_3)$ *and*

3. $F(X_1, X_2) = F(X_2, X_1)$*.*

Definition 3.2.2 (Homomorphisms)
A homomorphism $h : F \to G$ *between two formal group laws* F *and* G *is a formal power series* $h(X) \in R[[X]]$ *such that* $h(0) = 0$ *and* $h(F(X_1, X_2)) = G(h(X), h(Y))$*. Moreover, it is an isomorphism if there exists* $h^{-1} : G \to F$ *such that* $h^{-1}(h(X)) = h(h^{-1}(X)) = X$*.*

Lemma 3.2.3 (Inverse of a formal power series)
The formal power series $h(X) = c_1X + \dots$ *has an inverse* h^{-1} *if and only if* $c_1 \in R^\times$*.*

Proof: Let $h^{-1}(X) = c_1^{-1}X + \dots$ with higher coefficients are determined uniquely by $h(X)$'s coefficients. ■

Remark 3.2.4 (Abelian group of homomorphisms)
The set $\mathrm{Hom}_R(F, G)$ *of homomorphisms between formal group laws* F *and* G *is an abelian group with respect to the addition* $(h_1 + h_2)(X) := G(h_1(X), h_2(X))$ *with zero element* 0*.*

Lemma 3.2.5
The formal group law $F(X, Y)$ *has a formal inverse in the sense that there is an unique formal power series* $i_F \in R[[X]]$ *such that* $i_F(X) = -x + \dots$ *and* $F(X, i_F(X)) = 0$*.*

Proof: We construct inductively an unique sequence $(i_j(X))_{j\geq1}$ of polynomials in $XR[X]$ such that $\deg i_j(X) \leq j$ and

$$F(X, i_j(X)) \equiv 0 \mod X^{j+1}R[[X]]$$

Let $i_1(X) = -X$. Suppose that $i_j(X)$ has been constructed already. Then

$$F(X, i_j(X)) \equiv c_{j+1}X^{j+1} \mod X^{j+2}R[X]$$

for an unique $c_{j+1} \in A$. We define $i_{j+1}(X) := i_j(X) - c_{j+1}X^{j+1}$. Then

$$F(X, i_{j+1}(X)) = F(X, i_j(X) - c_{j+1}X^{j+1}) \equiv F(X, i_j(X)) - c_{j+1}X^{j+1} \equiv 0 \mod X^{j+2}R[[X]].$$

It follows that $i_F(X) := -X - \sum_{j\geq2} c_jX^j \in R[[X]]$ satisfies $F(X, i_F(X)) = 0$. ■

Example 3.2.6
The multicative formal group law $\widehat{\mathbb{G}}_m(X_1, X_2) := (1 + X_1)(1 + X_2) - 1 = X_1 + X_2 + X_1X_2$ *has its inverse*

$$i_{\widehat{\mathbb{G}}_m}(X_1) = -\frac{X_1}{X_1 + 1} = \sum_{i\geq1} X_1^i.$$

Suppose $R = \mathcal{O}_K$. Any commutative formal group law F over R gives rise to actual abelian groups in the following way:

Definition 3.2.7
Let E *be any nonarchimedean local field extension of* K *and let* $\mathfrak{m}_E$ *be the maximal ideal of its ring of integers. For any two* $x, y \in \mathfrak{m}_E$*, the series*

$$x +_F y := F(x, y)$$

converges with the limit in $\mathfrak{m}_E$*. Thus* $(\mathfrak{m}_E, +_F)$ *is an abelian group in which the inverse of* x *is given by* $i_F(x)$*. Moreover, any* $h \in \mathrm{End}_{\mathcal{O}_K}(F)$ *induces the endomorphism* $x \mapsto h(x)$ *of* $(\mathfrak{m}_E, +_F)$

Example 3.2.8
Consider a formal group law denoted as G. We can define $f +_G g = G(f(T), g(T))$ for any f and g belonging to $TR[[T]]$. This transforms $TR[[T]]$ into an abelian group.

Remark 3.2.9
In the context of a formal group law over $\mathcal{O}_K$, if we have $f : F \to G$, it will establish

$$a \mapsto f(a) : (\mathfrak{m}_E, +_F) \to (\mathfrak{m}_E, +_G)$$

for any $E \supset K$.

Example 3.2.10
We define $F = \widehat{\mathbb{G}}_m(X_1, X_2) := X_1 + X_2 + X_1X_2 = (1 + X_1)(1 + X_2) - 1$, consider $f(T) = -1 + (1 + T)^p$ as an endomorphism of F since

$$F(f(X_1), f(X_2)) = (1 + X_1)^p(1 + X_2)^p - 1 = f(F(X_1, X_2))$$

It is worth noting that the diagram below is commutative,

$$\begin{tikzcd}
\mathfrak{m}_K \arrow[r, "f"] \arrow[d, "a\mapsto 1+a"] & \mathfrak{m}_K \arrow[d, "a\mapsto 1+a"] \\
1+\mathfrak{m}_K \arrow[r, "a\mapsto a^p"] & 1+\mathfrak{m}_K
\end{tikzcd}$$

When we match $(\mathfrak{m}_K, +_F)$ with $(1 + \mathfrak{m}_K, \times)$, f is then associated with the function $a \mapsto a^p$.

Example 3.2.11
The abelian group $(\mathfrak{m}_E, +_{\widehat{\mathbb{G}}_m})$ is isomorphic to the subgroup $1 + \mathfrak{m}_E$ of $E^\times$ under the map $x \to 1 + x$ for the multiplicative formal group.

3.3 The introduction of Lubin-Tate group laws

Let K be a nonarchimedean local field and $R = \mathcal{O}_K$ be its ring of integers and $k = \mathcal{O}_K/\mathfrak{m}_K$ be its residue field, choose a prime $\pi \in \mathcal{O}_K$

Definition 3.3.1
We denote $\mathcal{F}_\pi$ as the set of every formal power series $f(X) \in R[[X]]$ satisfies the following two conditions:

1. $f(X) = \pi X + \dots$;
2. $f(X) \equiv X^q \mod \pi$,

where the following terms after πX is of degree ≥ 2 and $q = |k|$.

Example 3.3.2
The polynomial $f(X) = \pi X + X^q$ belongs to $\mathcal{F}_\pi$.

Example 3.3.3
When K is $\mathbb{Q}_p$ then

$$f(X) = -1 + (1 + X)^p \in \mathcal{F}_p.$$

Lemma 3.3.4
In $\mathcal{F}_\pi$, consider forms f and g, and a linear form $\varphi_1(X_1,\ldots,X_r)$ with coefficients in R. There exists an unique $\varphi \in R[[X_1,\ldots,X_r]]$ so that

$$\varphi(X_1,\ldots,X_r) = \varphi_1 + \geq 2-\textit{degree}$$

and

$$f(\varphi(X_1,\ldots,X_r)) = \varphi(g(X_1),\ldots,g(X_r))$$

<u>Proof:</u> By using the method of induction on n, we can demonstrate that there exists an unique polynomial $\varphi_n(X_1,\ldots,X_r)$ of degree n, satisfying the conditions:

$$\varphi_n(X_1,\ldots,X_r) = \varphi_1 + \geq 2-\text{degree}$$

and

$$f(\varphi_n(X_1,\ldots,X_r)) = \varphi_n(g(X_1),\ldots,g(X_r)) + \geq n+1-\text{degree}.$$

The initial polynomial has a distinctive coordinate denoted as φ_1. This coordinate definitely fulfills the initial requirement. If we express φ_1 as $\sum a_i X_i$, the second requirement states that

$$\pi(\sum a_i X_i) = \sum a_i(\pi X_i) + \text{terms of degree} \geq 2$$

This condition also holds true. If $n \geq 1$, the definition of φ_{n+1} is required. Since φ_n is unique, φ_{n+1} should be equal to $\varphi_n + Q$ for a homogeneous polynomial Q of degree $n+1$ in $A[X_1,\ldots,X_r]$. It is necessary to have

$$f(\varphi_r(X_1,\ldots,X_r)) = \varphi_{n+1}(g(X_1),\ldots,g(X_r)) - \geq n+2-\text{degree}.$$

On the left side, we have

$$f(\varphi_r(X_1,\ldots,X_r)) + \pi Q(X_1,\ldots,X_r) + \geq n+2-\text{degree}$$

and on the right side, we have

$$\varphi_n(g(X_1),\ldots,g(X_r)) + Q(\pi X_1,\ldots,\pi X_r) + \geq n+2-\text{degree}.$$

Since Q is homogeneous of degree $n+1$, it follows that $Q(\pi X_1,\ldots,\pi X_r) = \pi^{n+1} Q(X_1,\ldots,X_r)$. Therefore, it is necessary for

$$(\pi^{n+1}-\pi)Q(X_1,\ldots,X_r) = f(\varphi_n(X_1,\ldots,X_r)) - \varphi_n(g(X_1),\ldots,g(X_r)) + \text{terms of degree} \geq n+2$$

The polynomial Q must be the only one that satisfies the following condition:

$$\frac{f(\varphi_n(X_1,\ldots,X_r)) - \varphi_n(g(X_1),\ldots,g(X_r))}{(\pi^n-1)\pi} = Q + \text{terms of degree} \geq n+2.$$

It is important to note that on the field of characteristic p,

$$f \circ \varphi_n - \varphi_n \circ g \equiv \varphi_n(X_1,\ldots,X_r)^q - \varphi_n(X_1^q,\ldots,X_r^q) \equiv 0 \mod \pi$$

The form Q has coefficients in the ring A since $\pi | (f \circ \varphi_n - \varphi_n \circ g)$, and $\pi^n - 1 \in R^\times$. Additionally, the function φ_n satisfies the induction hypothesis and indeed has degree $n+1$.
Once we have established the values of φ_n for $n = 1, 2\ldots$, and have observed that

$$\varphi_{n+1} = \varphi_n + \text{terms with a degree} \geq n+1$$

allows us to define φ as the only one power series for which

$$\varphi = \varphi_n + \text{terms with a degree} \geq n+1,$$

for all values of n. ■

Proposition 3.3.5
Any f belonging to $\mathcal{F}_\pi$ corresponds to only one formal group law F_f with coefficients in R that allows f to act as an endomorphism. We soon call this F_f the Lubin-Tate formal group law for f.

Proof: As per Lemma 3.3.4, there exists a singular power series $F_f(X_1, x_2)$ such that

$$\begin{cases} F_f(X_1, X_2) & = X_1 + X_2 + \geq 2\text{−degree} \\ f(F_f(X_1, X_2)) & = F_f(f(X_1), f(X_2)) \end{cases} \tag{3.1}$$

We still need to verify that this satisfies the requirements of a formal group law.
Commutativity: Let $G = F_f(X_2, X_1)$. Then

$$\begin{cases} G(X_1, X_2) & = X_1 + X_2 + \geq 2\text{−degree} \\ f(G(X_1, X_2)) & = f(F_f(X_2, X_1)) = F_f(f(X_2), f(X_1)) = G(f(X_1), f(X_2)) \end{cases} \tag{3.2}$$

Given that $F_f(X_1, X_2)$ is the only power series with these characteristics, we can conclude that $G(X_1, X_2) = F_f(X_1, X_2)$.
Regarding associativity, if we let $G_1(X_1, X_2, X_3) = F_f(X_1, F_f(X_2, X_3))$ and $G_2(X_1, X_2, X_3) = F_f(F_f(X_1, X_2), X_3)$. Then, for $i = 1, 2$:

$$\begin{cases} G_i(X_1, X_2, X_3) & = X_1 + X_2 + X_3 + \text{term of degree } \geq 2 \\ G_i(f(X_1), f(X_2), f(X_3)) & = f(G_i(X_1, X_2, X_3)) \end{cases} \tag{3.3}$$

Lemma 3.3.4 implies that only one power series fulfills these conditions. □

Example 3.3.6
Consider $K = \mathbb{Q}_p$ and let $\pi = p$. We have $f = (1+T)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} T^i$ satisfies all the conditions to be an element of $\mathcal{F}_p$, and the form $F = X_1 + X_2 + X_1 X_2$ has f as an endomorphism. Hence, we can write $F = F_f$.

Proposition 3.3.7
In the set $\mathcal{F}_\pi$, consider two elements f and g, and an element r belonging to R. Then, let $[r]_{g,f} \in R[[T]]$ such that

$$\begin{cases} [r]_{g,f}(T) & = rT + \geq 2\text{−}degree \\ g \circ [r]_{g,f} & = [r]_{g,f} \circ f. \end{cases}$$

and it induces a formal group laws homomorphism $[r]_{g,f} : F_f \to F_g$.

Proof: In Lemma 3.3.4, we are assured of the existence of $h = [r]_{g,f}$. Our task is to demonstrate that

$$h(F_f(X_1, X_2)) = F_g(h(X_1), h(X_2)).$$

Each term is clearly in the form $rX + rY +$ term of degree ≥ 2. Additionally,

$$h(F_f(f(X_1), f(X_2)) = (h \circ g)(F_f(X_1, X_2)) = g(h(F_f(X_1, X_2)))$$

and

$$F_g(h(f(X_1)), h(f(X_2))) = F_g(g(h(X_1)), g(h(X_2))) = g(F_g(h(X_1), h(X_2)))$$

and we again utilize the uniqueness in Lemma 3.3.4. □

Proposition 3.3.8
For any $r_1, r_2 \in R$,

$$[r_1 + r_2]_{g,f} = [r_1]_{g,f} +_{F_g} [r_2]_{g,f}$$

and

$$[r_1 r_2]_{h,f} = [r_1]_{h,g} \circ [r_2]_{g,f}.$$

Proof: We can readily verify the accuracy of the statement based on the definition of $[.]_{g,f}$. □

Corollary 3.3.9
For $f, g \in \mathcal{F}_\pi, F_f \approx F_g$.

Proof: Each element $r \in R^\times$ has inverse isomorphisms $[r]_{f,g}$ and $r^{-1}_{g,f}$. Specifically, there exists one and only one $h : F_f \xrightarrow{\cong} F_g$ such that $h(T) = T + \geq 2-$degree together with $g \circ h = h \circ g$, denoted as $[1]_{g,f}$. □

Corollary 3.3.10
For every element r in the set R, there exists one and only one endomorphism $[r]_f : F_f \to F_f$ in such a way that $[r]_f = rT +$ term of degree ≥ 2, and $[r]_f$ has the property of commuting with f. The function

$$r \mapsto [r]_f : R \hookrightarrow \operatorname{End}(F_f)$$

acts as a homomorphism of rings.

Proof: Consider $[r]_f = [r]_{f,f}$- it represents the unique series $rT + \geq 2-$degree, which commutes with f. This series serves as an endomorphism of F_f. The fact that $r \mapsto [r]_f$ forms a homomorphism of rings can be derived from Proposition 3.3.8, and $[1]_f = T$. □

Remark 3.3.11
Therefore, for any finite extension E of K, the abelian group $(\mathfrak{m}_E, +_{F_f})$ naturally possesses an $R-$module structure.

Example 3.3.12 (Lubin-Tate group law and its attached endomorphism on $\mathbb{Q}_p$)
When $K = \mathbb{Q}_p$, let $f = (1+T)^p - 1 == \sum_{i=1}^p \binom{p}{i} T^i \in \mathcal{F}_p$ (as we have shown before), so that $F_f = X_1 + X_2 + X_1 X_2$. For any $r \in \mathbb{Z}_p$, we can define

$$(1+T)^r = \sum_{r \geq 0} \binom{r}{m} T^r$$

The definitions coincide with the usual ones when $a \in \mathbb{Z}$, and if $(r_i)_{i \geq 1}$ is a sequence of integers converging to $r \in \mathbb{Z}_p$, then $\binom{r_i}{m} \to \binom{r}{m}$ as $i \to \infty$. In the case of $\binom{r}{m} \in \mathbb{Z}_p$, we have

$$[r]_f = (1+T)^r - 1$$

It is certain that $(1+T)^r - 1 = rT + \dots$, and

$$((1+T)^r - 1) \circ f = (1+T)^{rp} - 1 = f \circ ((1+T)^r - 1)$$

holds true for integer r, and due to continuity, it holds true for all $r \in \mathbb{Z}_p$.
When we consider the isomorphism $(\mathfrak{m}, +_{F_f}) \xrightarrow{t \mapsto 1+t} (1 + \mathfrak{m}, \times)$, the action of $[r]_f$ corresponds to the mapping of an element of $1 + \mathfrak{m}$ to its $r-$th power.

Example 3.3.13 (Lubin-Tate group law and its attached endomorphism on $\mathbb{F}_p((t))$) *In the case $K = \mathbb{F}_p((t))$, its ring of integers is $R = \mathbb{F}_p[[t]]$, its residue field is $\mathbb{F}_p$ and K now has characteristic p. We are going to define the Carlitz polynomial $[M](T)$.*

1. *By setting $[1](T) := T$ and $[t](T) := T^p + tT$, we define (for every $n \geq 2$):*

$$[t^n](T) := [t]([t^{n-1}](T)).$$

2. *For every $F = a_0 + a_1t + a_2t^2 + \cdots \in \mathbb{F}_p[[t]]$, let*

$$[F](T) = a_0T + a_1[t](T) + a_2[t^2](T) + \cdots \in \mathbb{F}_p[[t]][[T]].$$

Now, let $f = T^p + tT \in \mathcal{F}_p$, its Lubin-Tate group law is just $F(X_1, X_2) = X_1 + X_2$ and for all $F \in \mathbb{F}_p[[t]]$, we can define

$$[F]_f := [F](T).$$

Remark 3.3.14

1. *Note that $[\pi]_f = f$.*

2. *The mapping $r \mapsto [r]_f : R \mapsto \mathrm{End}(F_f)$ is an injective homomorphism, since the leading coefficient of $[r]_f$ allows for the recovery of r.*

3. *$[1]_{g,f} : F_f \overset{\cong}{\to} F_g$ preserves the actions of R on F_g and F_f as shown by the equation*

$$[1]_{g,f} \circ [r]_f = [r]_{g,f} = [r]_g \circ [1]_{g,f}.$$

3.4 Constructing the extension K_π/K

Recall that a non-archimedean local field K is either a finite extension of $\mathbb{Q}_p$ or a finite extension of $\mathbb{F}_p((t))$. In this subsection, we consider $R = \mathcal{O}_K$ as its ring of integers, $k = R/\mathfrak{m}$ as its residue field and $q = |k|$. It is well-known that q is a power of some prime number p.

Remark 3.4.1 (The construction of K^{un})
Let

$$\mu_m := \{\zeta \in \overline{K} : \zeta^m = 1\}$$

be the set of all $m-$th roots of unity in $\overline{K}$. When p is not a prime factor of m, the discriminant of the polynomial $P(X) = X^m - 1$

$$\mathrm{disc}(X^m - 1) = \prod_{i<j}(\zeta_i - \zeta_j)^2 = (-1)^{n(n+1)/2}m^m$$

is an unit in the ring $R = \mathcal{O}_K$ where $\zeta_i, \zeta_j \in \mu_m$. Let $K[\mu_m]$ be the extension of K generated by the $m-$roots of unity, since $\mathrm{Gal}(K[\mu_m]/K)$ is cyclic the extension is unramified. Additionally, the splitting field of $P(x)$ over k is the residue field k_m of $K[\mu_m]$. Moreover, k_m has exactly $q^{\mathrm{ord}_m(p)}$ elements. Consequently, we have

$$K^{\mathrm{un}} = \bigcup_{p \nmid m} K[\mu_m]$$

and the Galois group $\mathrm{Gal}(K^{\mathrm{un}}/K) \cong \widehat{\mathbb{Z}}$*. Where*

$$\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}.$$

We can also identify each $\overline{n} \in \widehat{\mathbb{Z}}$ *with a homomorphism* $\sigma_n \in \mathrm{Gal}(K[\mu_m]/K)$ *as: for each* $\zeta \in \mu_m$ *and every* $n_0 \in \mathbb{Z}$ *close enough to* $\overline{n}$ *(with canonical norm and only depends on* m*),*

$$\sigma_n \cdot \zeta := \zeta^{n_0}.$$

In other words, σ_n *can be seem as* $\mathrm{Frob}_K^{\overline{n}}$

Example 3.4.2 (The case $K = \mathbb{Q}_p$)
When K *is the field of* p*-adic numbers* $\mathbb{Q}_p$ *with* π *being the prime number* p*, an analogous structure for the extension* K_π *known as* $(\mathbb{Q}_p)_p$ *can be defined as the union of the fields* $\mathbb{Q}_p[\mu_{p^n}]$ *for all* n*. The mapping* $([m], \zeta) \to \zeta^m$ *from the group* $\mathbb{Z}/p^n\mathbb{Z} \times \mu_{p^n}$ *to* μ_{p^n} *transforms the group* u_{p^n} *into a free module over* $\mathbb{Z}/p^n\mathbb{Z}$ *with one generator. Considering that* $\mathbb{Z}/p^n\mathbb{Z}$ *is equivalent to* $\mathbb{Z}_p/p^n\mathbb{Z}_p$*, we can treat* μ_{p^n} *like a cyclic module over the* p*-adic integers* $\mathbb{Z}_p$*, similar to the cyclic group* $\mathbb{Z}/(p^n)$*. The* $\mathbb{Z}_p$*-action on* μ_{p^n} *allows for an isomorphism between the units of* $\mathbb{Z}_p/p^n\mathbb{Z}_p$ *and the Galois group* $\mathrm{Gal}(\mathbb{Q}_p[\mu_{p^n}]/\mathbb{Q}_p)$*. As we take the limit when* n *increases without bound, this results in an isomorphism between the units of the* p*-adic integers* $\mathbb{Z}_p^\times$ *and the Galois group* $\mathrm{Gal}((\mathbb{Q}_p)_p/\mathbb{Q}_p)$*.*

For the field extensions K^{un}/K *and* $(\mathbb{Q}_p)_p/\mathbb{Q}_p$*, we can concretely specify a set of elements that generate the extension, describe the Galois group in detail, and express precisely how the Galois group acts on these generators.*

Definition 3.4.3 (Similar results for general cases by Lubin-Tate groups)
The absolute value operator $|\cdot|$ *on the field* K *uniquely extends to any* $E \subset \overline{K}$ *with* E/K *finite and subsequently to the entire algebraic closure* $\overline{K}$*. Suppose* $f \in \mathcal{F}_\pi$*. For any* $\gamma, \delta \in \overline{K}$ *such that* $|\gamma|, |\delta| < 1$ *and* $r \in R$*, the series* $F_f(\gamma, \delta)$ *and* $[r]_f(r)$ *converge. As a result, we define* Λ_f *as the* $R-$*module satisfying*

$$\Lambda_f = \{\gamma\overline{K} | |\gamma| < 1\}$$
$$\gamma +_{\Lambda_f} \delta = \gamma +_{F_f} \delta = F_f(\gamma, \delta)$$
$$a \cdot \gamma = [a]_f(\delta).$$

We define $\Lambda_n \subset \Lambda_f$ *as submodule consisting of all elements annihilated by* $[\pi]_f^n$*.*

Remark 3.4.4
In light of the fact that $f(T) = [\pi]_f(T)$*, we can define* Λ_n *as the collection of roots of*

$$f \circ \cdots \circ f = f^{(n)} \text{ (}n\text{ times)}$$

in $\overline{K}$ *with a valuation of less than 1. To simplify, let's assume that* f *is* $T^q + \cdots + T^2 + \pi T$*. By Corollary 3.3.9, we can take* $f = T^q + \pi T$ *as sufficient. Then,*

$$(f \circ f)(T) = f(f(T)) = (T^q + \cdots + \pi T)^q + \cdots + \pi(T^q + \cdots + \pi T) = T^{q^2} + \cdots + \pi T^2$$

and

$$f^{(n)}(T) = \pi^n T + \cdots + T^{q^n}.$$

For the Newton polynomial of $f^{(n)}$, it is evident that all of its roots have a positive ord_K*, thus a valuation* < 1*. Therefore,* Λ_n *represents the collection of all roots of* $f^{(n)}$ *in* $\overline{K}$ *with the given commutative group structure*

$$\gamma +_{F_f} \delta = F_f(\gamma, \delta) = \gamma + \delta + \dots$$

along with the $R-$*module structure,*

$$[r]_f \alpha = r\gamma + \dots$$

Lemma 3.4.5
Consider an $R-$*module denoted as* A*, and define* A_m *as the kernel of the map* $\pi^m : A \to A$*. Assume that the following conditions are satisfied:*

1. $|A_1| = (A : (\pi))$*, and*
2. $\pi : A \to A$ *is onto map.*

The group A_m *is isomorphic to the quotient group* $R/(\pi^m)$*; therefore, it contains* q^m *elements.*

Proof: We will utilize induction on m. As $R/(\pi^m)$ has an order of q^m, when considering condition 1 and the structure theorem, we can conclude that A_1 is isomorphic to $R/(\pi)$. Let's examine the sequence

$$0 \to A_1 \to A_m \xrightarrow{\times\pi} A_{m-1} \to 0.$$

Condition 2 indicates that it is exact at A_{m-1}, and hence, exact in general. Consequently, A_m contains q^m elements. Additionally, if A_m is not cyclic, A_1 would not be too. Thus A_m is cyclic $R-$module with $|A_m| = q^m$ and $A_m \cong R/(\pi^m)$. ■

Proposition 3.4.6
The quotient $R/(\pi^m)$ *is isomorphic to the* $R-$*module* Λ_m*. Therefore* $\operatorname{End}_R(\Lambda_m) \cong R/(\pi^m)$ *as well as* $\operatorname{Aut}_R(\Lambda_m) \cong (R/(\pi^m))^\times$*.*

Proof: The existence of $h : F_f \xrightarrow{\cong} F_g$ results in $R-$homomorphism $\Lambda_f \xrightarrow{\cong} \Lambda_g$, making the choice of $f \in \mathcal{F}_\pi$ irrelevant. We take $f \in \mathcal{F}_\pi$ to be of the form of $T^q + \dots \pi T$. This polynomial is an Eisenstein polynomial and therefore possesses q distinct roots, each with a valuation less than 1. Let $\gamma \in \overline{K}$ have a valuation less than 1. Consider the Newton polynomial of

$$f(T) - \alpha = -\alpha + T^q + \dots + \pi T.$$

The roots have a valuation of less than 1 and therefore belong to Λ_f. As a result, we have confirmed that the assumptions of the lemma hold for Λ_f, meaning that $\Lambda_m \cong R/(\pi^m)$. Consequently, the impact of R on Λ_m causes an isomorphism $R/(\pi^m) \to \operatorname{End}_R(\Lambda_m)$. □

Lemma 3.4.7
Let E/K *be finite Galois with* $G = \operatorname{Gal}(E/K)$*. For any* $F \in \mathcal{O}_K[[X_1, \dots, X_n]]$ *and* $\gamma_1, \dots, \gamma_n \in \mathfrak{m}_E$*,*

$$F(\theta\gamma_1, \dots, \theta\gamma_n) = \theta F(\gamma_1, \dots, \gamma_n), \ \forall \theta \in G.$$

Proof: We know that θ is a field isomorphism preserving $\mathcal{O}_K$ implies that if F is a polynomial. It is known that θ preserves the valuation on E, so θ is continuous. Hence, it maintains boundaries: For

$$\lim_{i\to\infty} \alpha_i = E$$

it follows that

$$\lim_{i\to\infty} \tau\alpha_i = \tau E.$$

Suppose F_t is the polynomial with a degree of t, such that $F = F_t + \deg \geq t+1$. Thus

$$\theta(F(\gamma_1,\dots)) = \theta(\lim_{t\to\infty} F_t(\gamma_1,\dots)) = \lim_{t\to\infty} \theta F_m(\gamma_1,\dots) = \lim_{m\to\infty} F_m(\tau\gamma_1,\dots).$$

■

Theorem 3.4.8
Consider $K_{\pi,m} = K[\Lambda_m]$, a subfield of $\overline{K}$ created by the elements of Λ_m.

1. *For every m, $K_{\pi,m}/K$ is totally ramified of degree $(q-1)q^{m-1}$.*
2. *The action of R on Λ_m defines*

$$(R/\mathfrak{m}^m)^\times \xrightarrow{\cong} \mathrm{Gal}(K_{\pi,m}/K).$$

   Specifically, $K_{\pi,m}/K$ is abelian.

3. *For every $m \geq 1, \pi \in \mathrm{Nm}_{K_{\pi,m}/K}(K^\times_{\pi,m})$.*

Proof: It is reasonable to assume once more that $f \in \mathcal{F}_\pi$ is of the form $T^q + \cdots + \pi T$. Choose a nonzero root π_1 of $f(T)$ and a roots π_m of $f(T) - \pi_{m-1}$ (inductively) for 1 and 2. Consider

$$K[\Lambda_m] \supset K[\pi_m] \supset K[\pi_{m-1}] \supset \cdots \supset K[\pi_1] \supset K.$$

Eisenstein is used for each extension, with the degree indicated. Consequently, over K of degree $q^{m-1}(q-1)$, $K[\pi_m]$ is completely ramified.
Remember that $K[\Lambda_m]$ is the splitting field of $f^{(m)}$ since Λ_m is the set of roots of $f^{(m)}$ in $\overline{K}$. The image of $\mathrm{Gal}(K[\Lambda_m]/K)$ in $\mathrm{Sym}(\Lambda_m)$ is therefore contained in

$$\mathrm{End}_A(\Lambda_m) = (R/(\pi^m))^\times)$$

because $\mathrm{Gal}(K[\Lambda_m]/K)$ is an isomorphism between $A-$modules and can be associated with a subgroup of the group of permutations of the set Λ_m. Therefore

$$(q-1)q^{m-1} = [K[\Lambda_m] : K] = |\,\mathrm{Gal}(K[\Lambda_m]/K)| \leq (q-1)q^{m-1}.$$

The equalities hold iff $\mathrm{Gal}(K[\Lambda_m]/K) \cong (R/\mathfrak{m}^m)^\times$ and $K[\Lambda_m] = K[\pi_m]$.
For 3. Let $f^{[m]}(T) = \frac{f}{T} \circ f \circ \cdots \circ f$ (m terms), so

$$f^{[m]}(T) = T^{(q-1)q^{m-1}} + \cdots + \pi.$$

Then $0 = \cdots = f(\pi_1) = f^{[m-1]}(\pi_{m-1}) = f^{[m]}(\pi_m)$. Because $f^{[m]}$ is monic with $\deg f^{[m]} = (q-1)q^{m-1} = [K[\pi_m] : K]$, it is the minimal polynomial of π_m over K. Therefore,

$$\mathrm{Nm}_{K[\Lambda_m]/K}\, \pi_m = (-1)^{(q-1)q^{m-2}}\pi = \pi,$$

unless $q = 2$ and $m = 1$. Since $K[\Lambda_1] = K$ in the exceptional case, π is unquestionably a norm.
□

Remark 3.4.9
We now can define $K_\pi := \bigcup K_{\pi,m}$ *which is a abelian extension of* K*. The isomorphism*

$$(R/\mathfrak{m}^m)^\times \cong \mathrm{Gal}(K_{\pi,m}, K)$$

induced (by inverse limit) the isomorphism

$$R^\times \cong \mathrm{Gal}(K_\pi/K).$$

Example 3.4.10
Assume that $f = (T+1)^p - 1$ *and* $K = \mathbb{Q}_p$*. Select a primitive* ζ_p *and* $\zeta_{p^n}^p = \zeta_{p^{n-1}}$ *for each* n *by taking the* p^n-*th root* ζ_{p^n} *of* 1*. Then,* $(\mathbb{Q}_p)_{p,n} = \mathbb{Q}_p[\pi_n] = \mathbb{Q}_p[\zeta_{p^n}]$ *and* $\pi = \zeta_{p^n} - 1$ *follow. Additionally, the standard isomorphism is* $(\mathbb{Z}_p/(p^n))^\times \to \mathrm{Gal}(\mathbb{Q}_p[\zeta_{p^n}]/\mathbb{Q}_p)$*.*

3.5 An Introduction of Local Kronecker-Weber Theorem and its application

This section's primary purpose is the demonstration that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$.

3.5.1 Note on the ramification group of the field extension $K_{\pi,m}/K$

Let G be the Galois group of a finite Galois extension E/K. Remember that

$$G_i = \{g \in G |\, \mathrm{ord}_E(gr - r) \geq i + 1\ \forall r \in \mathcal{O}_E\}$$

is the $i-$th ramification group. In addition, for $i \geq 0$,

$$G_i = \{g \in G_0 |\, \mathrm{ord}_E(g\Pi - \Pi) \geq i + 1\}$$

where $\Pi \in E$ is prime. The normalized valuation $E^\times \to \mathbb{Z}$ is represented here by ord_E. Afterwards, $G/G_0 = \mathrm{Gal}(e/k)$, with the following inclusions:

$$(\Pi \mapsto g\Pi/\Pi \mod \Pi) : G_0/G_1 \hookrightarrow e^\times$$

$$(\Pi \mapsto (g\Pi - \Pi)/\Pi^{i+1} \mod \Pi) : G_i/G_{i+1} \hookrightarrow e$$

where k and e are the residue fields of K and E, respectively. Hence $(G_0 : G_1)|(q-1)$ and $(G_i : G_{i+1})|q$ for $i \geq 1$. Additionally, $G_i = \{1\}$ for i large enough. Consider

$$U^{(0)} = U = R^\times;$$

$$U^{(i)} = 1 + \mathfrak{m}^i, i \geq 1.$$

Then

$$U/U^{(m)} \supset U^{(1)}/U^{(m)} \supset \cdots \supset U^{(m)}/U^{(m)} = 0$$

on $R^\times/(1 + \mathfrak{m}^m) = U/U^{(m)}$.

Proposition 3.5.1
Under $R^\times/U^{(m)} \overset{\cong}{\to} G$ *of Theorem 3.4.8,* $U^{(i)}/U^{(m)} \to G_{q^i - 1}$ *is surjective.*

Proof: Let $f = \pi T + T^q$. As $G = G_0$, $U^{(0)}/U^{(m)} \twoheadrightarrow G_0$, without a doubt. Now, let $u \in U^{(i)} \setminus U^{(i+1)}$, and assume $i \geq 1$. Afterwards, $u = 1 + v\pi^i$ and

$$[u]_f(\pi_m) = [1]_f(\pi_m) + [v]_f[\pi^i]_f(\pi_m) = \pi_m + [v]_f(\pi_{m-i}) = \pi_m + (\text{unit})\pi_{m-i}.$$

For any $i \geq 1$, $\pi_i = \pi\pi_{i+1} + \pi_{i+1}^q = \pi_{i+1}^q \left(\frac{\pi\pi_{i+1}}{\pi_{i+1}^q} + 1\right) = \pi_{i+1}^q \times \text{unit}$. Since ord $\left(\frac{\pi}{\pi_{i+1}^{q-1}}\right) > 0$. Thus $\pi_{m-1} = \pi_m^{q^i} \times \text{unit}$, and

$$[u]_f(\pi_m) - \pi_m = \pi_m^{q^i} \times \text{unit}.$$

This indicates that, by definition, $[u]_f \in G_{q^i-1}$, and $[u]_f \notin G_{q^i}$. This states that $U^{(i)} \twoheadrightarrow G_{q^i-1}$ since it is true for all i. □

Remark 3.5.2
From the above arguments, we get

$$\begin{cases} G_0 & = G \\ G_{q-1} & = G_{q-2} = \cdots = G_1 \\ G_{q^2-1} & = G_{q^2-2} = \cdots = G_q \\ \cdots & \\ G_{q^m-1} & = 1 \end{cases}$$

3.5.2 Upper numbering on ramification groups

Let E/K be a finite Galois extension, with $G = \text{Gal}(E/K)$. We now define the notation G_r for all real number $r \geq -1$ by letting

$$G_r = G_i, \ \ \forall i = \lceil u \rceil$$

For $r > 0$, $G_r = \{g \in G_0 | \operatorname{ord}_E(g\Pi - \Pi) \geq i+1\}$ defines an unique continuous pairwise linear function

$$\pi : \mathbb{R}_{\geq 0} \to \mathbb{R}$$

satisfied:

$$\begin{cases} \varphi(0) & = 0 \\ \varphi'(u) & = (G_0 : G_r)^{-1} \text{ if } r \notin \mathbb{Z}. \end{cases}$$

We now letting $G^v = G_r$ if $v = \varphi(r)$, i.e., $G^v = G_{\varphi^{-1}(v)}$

Example 3.5.3
Let $E = K_{\pi,m}$. Then

$$G^{q-1} = \cdots = G_2 = G + 1, \ q - 1 = (G_0 : G_1)$$

The map φ' with respect to u is given by $\varphi'(u) = \frac{1}{q-1}$ for $0 < u < q-1$, and the initial segment of the graph of φ extends from the point $(0, 0)$ to $(q-1, 1)$. Consequently, G_1 is equivalent to G_{q-1}. Following this, we have $(G_{q-1} : G_q) = q$, and G_q is equal to G_{q+1}, continuing up to G_{q^2-1}. Therefore, within the interval $q - 1 < u < q^2 - 1$, it follows that $\varphi'(u) = \frac{1}{q(q-1)}$. The second portion of the graph representing φ extends from the point $(q-1, 1)$ to $(q^2 - 1, 2)$. As a result, we have $G^2 = G_{q^2-1}$. Proceeding in a similar fashion, we derive the diagram below:

$$\begin{tikzcd}
G_0 \supset \arrow[d, "\cong"] & G_{q-1} \supset \arrow[d, "\cong"] & G_{q^2-1} \supset \arrow[d, "\cong"] & \dots & G_{q^m-1} = \{1\} \arrow[d, "\cong"] \\
G^0 & G^1 & G^2 & \dots & G^m
\end{tikzcd}$$

Remark 3.5.4
Under $R^\times/U^{(m)} \overset{\cong}{\to} G$,

$$U^{(i)}/U^{(m)} \overset{\cong}{\to} G^i.$$

The upper numbering corresponds to the quotient and the lower numbering corresponds to the subgroup.

Proposition 3.5.5
Consider a tower of Galois extensions $L \supset E \supset K$, where $G = \mathrm{Gal}(L/K)$ and $G' = \mathrm{Gal}(L/E)$, and note that $G/G' = \mathrm{Gal}(E/K)$. We get

$$(G/G')^v = \mathrm{Im}(G^v \to G/G')$$

in other words, $(G/G')^v = G^vG'/G'$.

Proof: See Serre, Local Fields [6]. □
Consider Ω/K to be Galois with $[\Omega : K] = \infty$ with Galois group G, we define a filtration on G:

$$g \in G^v \iff g \in \mathrm{Gal}(E/K)^v, \ \forall E/K \text{ finite and Galois } \ E \subset \Omega.$$

Definition 3.5.6
*In a finite Galois extension E/K, a value v is termed a **jump** in the series $\{G^v\}$ if $G^v \neq G^{v+\epsilon}$ for every $\epsilon > 0$.*

Theorem 3.5.7 (Hasse-Arf)
All the jumps are integers in the case E/K is finite abelian. In other words, if $G_i \neq G_{i+1}$, then $\varphi(i) \in \mathbb{Z}$.

Proof: See Serre, Local Fields [6]. □
Therefore, in the case E/K finite abelian, the filtration on $G_0 = G^0$ takes the following structure

$$G^0 \supsetneq G^{j_1} \supsetneq G^{j_2} \dots \ \ j_n \in \mathbb{N}$$

.

3.5.3 The local Kronecker-Weber theorem

Let K be a nonarchimedean local field, and assume that all extensions of K are subfields within a designated separable algebraic closure $\overline{K}$ of K.

Lemma 3.5.8
Let E be an abelian totally ramified extension of K. If $E \supset K_\pi$, then $E = K_\pi$.

Proof: Let $G = \mathrm{Gal}(E/K)$ and $G' = \mathrm{Gal}(E/K_\pi)$, so that $G/G' = \mathrm{Gal}(K_\pi/K)$. Consider the diagram of abelian groups:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & G^{m+1} \cap G' \arrow[r] \arrow[d] & G^{m+1} \arrow[r] \arrow[d] & (G/G')^{m+1} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & G^{m} \cap G' \arrow[r] \arrow[d] & G^{m} \arrow[r] \arrow[d] & (G/G')^{m} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \frac{G^m \cap G'}{G^{m+1} \cap G'} \arrow[r] \arrow[d] & \frac{G^m}{G^{m+1}} \arrow[r] \arrow[d] & \frac{(G/G')^m}{(G/G')^{m+1}} \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

It is trivial that all the columns exact, and Proposition 3.5.5 demonstrates the exactness of two top rows and the snake lemma shows that the third row is also exact, hence

$$q \geq (G^m : G^{m+1}) = ((G/G')^m : (G/G')^{m+1})(G^m \cap G' : G^{m+1} \cap G').$$

This leads to the conclusion that $G^m \cap G' = G^{m+1} \cap G'$ for every m. Therefore,

$$G^{m+1} \cap G' = G^m \cap G' = \cdots = G^0 \cap G' = G'$$

Hence $G' \subset G^m$ for all m or $G' = \{1_G\}$ (since $\bigcap G^m = 1$). ■

Lemma 3.5.9
All finite unramified extensions of K_π are contained in $K_\pi \cdot K^{\text{un}}$.

Proof: Let E denote an unramified extension of K_π. It follows that E can be expressed as $K_\pi \cdot E'$, where E' represents an unramified extension of $K_{\pi,m}$ for a certain m. Furthermore, we observe that E' can be expressed as $K_{\pi,m} \cdot E''$, where E'' is an unramified extension of K. ■

Lemma 3.5.10
Let E/K be finite abelian extension with an exponent of k (i.e., $g^k = 1$ for all $g \in \mathrm{Gal}(E/K)$), and let K_k denote the unramified extension of K with a degree of k. It follows that there exists a totally ramified abelian extension E_t of K such that

$$E \subset E_t \cdot K_k = E \cdot K_k.$$

Proof: For any element $g \in \mathrm{Gal}(EK_k/K)$, the restriction of g to E is trivial, i.e., $g|_E = 1 = g^k_{|K_k}$, indicating that $\mathrm{Gal}(EK_k/K)$ remains an abelian group with exponent k. Suppose $g \in \mathrm{Gal}(EK_k/K)$ such that $g_{|K_k}$ represents the Frobenius automorphism. Then, g has order k, and we have

$$\mathrm{Gal}(E/K) =< g > \times G'$$

for some subgroup G'. Let $E_t = E^{<g>}$; consequently, E_t is totally ramified over K, and $E \cdot K_k = E_t \cdot K_k$. ■

Theorem 3.5.11 (Local Kronecker-Weber)

$$K_\pi \cdot K^{\text{un}} = K^{ab}$$

for every prime π of K.

Proof: Let E represent a finite abelian extension of K. Our objective is to establish that E is a subset of $K_\pi \cdot K^{\mathrm{un}}$. Lemma 3.5.8 remains applicable when K is replaced with K_π. Upon applying it to the extension $E \cdot K_\pi / K_\pi$, we infer the existence of a totally ramified extension E_t of K_π and an unramified extension E_u of K_π such that

$$E \cdot K_\pi \subset E_t \cdot E_u \subset (E_t \cdot K_\pi) \cdot E_u.$$

Additionally, Lemma 3.5.9 implies that $E_t \subset K_\pi$, and Lemma 3.5.10 implies that $E_u \subset K_\pi \cdot K^{\mathrm{un}}$. □

Corollary 3.5.12
Every finite abelian extension of $\mathbb{Q}_p$ is encompassed within a cyclotomic extension.

Corollary 3.5.13 (Calculating Gal(K^{ab}/K))

- $K^{\mathrm{ab}} \cong K_\pi \cdot K^{\mathrm{un}}$, *depends only on the choice of* π*;*
- $K_{\pi_K} \cap K^{\mathrm{un}} = K$*, hence*
- $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K^{\mathrm{un}}/K)$*;*
- $\mathrm{Gal}(K_\pi/K) \cong \mathcal{O}_K^\times$*;*
- $\mathrm{Gal}(K^{\mathrm{un}}/K) \cong \widehat{\mathbb{Z}} := \lim\limits_{\leftarrow} \mathbb{Z}/n\mathbb{Z}$*;*
- $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathcal{O}_K^\times \times \widehat{\mathbb{Z}}$*.*

3.6 The Existence Theorem

Let K represent a local field. It is worth recalling that a subgroup N of $K^\times$ is termed a norm group if there exists a finite abelian extension E/K such that $\mathrm{Nm}_{E/K}(E^\times) = N$. Since $K^\times/N \xrightarrow{\cong} \mathrm{Gal}(E/K)$, the group N is of finite index in $K^\times$ and, consequently, open.

Theorem 3.6.1 (Existence Theorem)
Every $O \subset_{open} K^\times$ and $O < K^\times$ there exists a finite abelian extension E/K such that $O = \mathrm{Nm}_{E/K}(E^\times)$.

Certainly, here are the proofs of the lemmas that we need:

Lemma 3.6.2
For all finite extension E/K, the norm map $E^\times \to K^\times$ has closed image and compact kernel.

Proof: Recall that $(K : N) = (K^\times : \mathrm{Nm}(E^\times)) < \infty$ and N is open in $K^\times$, therefore N is closed. $\mathrm{Ker}(\mathrm{Nm}_{E/K})$ is also closed since the norm map is continuous. We have

$$\mathrm{ord}_E(\mathrm{Nm}_{E/K}(a)) = [E : K]\,\mathrm{ord}_E(a) = f \cdot \mathrm{ord}_K(a)$$

so $N \subset U_K$ and then N is compact since U_K is compact ■
For convenience, let $H_K = \bigcap \mathrm{Nm}_{E/K}(E^\times)$ where E runs over the finite extensions of K.

Lemma 3.6.3

$$\operatorname{Nm}_{K'/K} H_{K'} = H_K$$

for every finite extension K'/K.

Proof: It is trivial that

$$\operatorname{Nm}_{K'/K} H_{K'} \subset H_K.$$

For every finite extension E/K and every $a \in K$, we consider the set:

$$T_E(a) = \operatorname{Nm}_{E/K}(E^\times) \cap \operatorname{Nm}^{-1}_{K'/K}(a).$$

We get a collection of sets:

$$T_{K'} = \{T_E(a)\},$$

where E runs over the finites extension of K' and a runs in K. We can check that those sets are nonempty and then compact since they are the intersection of two compact sets. Furthermore, $T_E(a)$ is obviously a subset of $H_{K'}$ due to their definitions and every $t \in T_E(a)$ has norm a. Hence,

$$\operatorname{Nm}_{K'/K} H_{K'} \supset H_K.$$

■

Lemma 3.6.4
The group H_K is divisible.

Proof: Let n be a positive integer greater than 1. The objective is to establish that $nH_K = H_K$. Let $a \in H_K$. For every E/K finite such that $\sqrt[n]{1_K} \in E$, we denote

$$D(E) = \{b \in K^\times | b^n = a,\ b \in \operatorname{Nm}_{E/K} E^\times\}.$$

This set is proven to be nonempty since $a = \operatorname{Nm}_{E/K} a'$ for some $a' \in H_E$, where $a' = c^n$ for some $c \in E$ (according to Proposition 3.5.1). Thus,

$$\operatorname{Nm}_{E/K}(c)^n = \operatorname{Nm}_{E/K}(a') = a.$$

Hence, $b := \operatorname{Nm}_{E/K}(c) \in D(E)$. Moreover, every set $D(E)$ is finite since E/K finite and $D(E) \cap D(E') \supset D(E \cdot E') \neq \emptyset$ for every finite extensions E and E' of K. This implies there exists $\bar{b} \in D(E) \cap D(E') \cap H_K$ has an n-th power of a. ■

Lemma 3.6.5
$H_K = \{1\}$.

Proof: Select a prime of K. Define $W_{m,n} = U^{(m)} \times \pi^{n\mathbb{Z}}$. It follows that $W_{m,n}$ constitutes an open subgroup of finite index in $K^\times$, and therefore encompasses H_K. Consequently, $H_K \subset \bigcap_{m,n} W_{m,n} = \{1\}$. ■

Lemma 3.6.6
Every subgroup J of $K^\times$ with finite index and containing U_K is a norm group.

Proof: Consider the map

$$\operatorname{ord}_K : K^\times \to \mathbb{Z},$$

which is surjective and $\operatorname{Ker}(\operatorname{ord}_K) = U_K$. Hence, every subgroup $J \subset K^\times$ is of the form $\operatorname{ord}_K^{-1}(m\mathbb{Z})$ for some integer $m \geq 1$. Let K_m/K be unramified extension with $[K_m : K] = m$. We know that $\operatorname{Nm}_{K_m/K}(K_m^\times)$ is a subgroup of $K^\times$ and it contains U_K. Moreover, $\operatorname{ord}_K \operatorname{Nm}_{K_m/K}(K_m^\times) = m\mathbb{Z}$. This proved our statement. ■

To proceed, we will now prove the theorem:

Proof: (of the Existence Theorem)
We denote $\mathcal{N}$ to be the set of all norm groups of $K^\times$, and define $\mathcal{H}_K = \bigcap_{N \in \mathcal{N}} N$. Suppose J is a finite index subgroup of $K^\times$. Since $\mathcal{H}_K$ is divisible, we have $J \supset \mathcal{H}_K$, which implies

$$\bigcap_{N \in \mathcal{N}} (N \cap U_K) \subset \bigcap_{N \in \mathcal{N}} N \subset J.$$

This leads to $(U_K \cap N) \setminus J = \emptyset$. Since all the sets are compact, there is a subfamily with empty intersection. As any two sets $N \cap U_K$ contain a third, it follows that $J \supset N \cap U_K$ for some N. Consider a norm group N such that $N \cap U_K \subset J$. Consequently, we have

$$I \supset N \cap (U_K \cdot (N \cap I)).$$

Each element from this intersection can be expressed as ab, where $a \in U_K$ and $b \in N \cap I$, with the property that $ab \in N$. According to the previous two lemmas, this means $a \in N$ and therefore $a \in N \cap U_K \subset I$, ensuring $ab \in I$. Given that $N \cap I$ has a finite index in $K^\times$, and this is also the case for both N and I, the quotient $K^\times / N \cap I$ embeds into $(K^\times/N) \times (K^\times/I)$. Thus, $U_K \cdot (N \cap I)$ represents a finite-index subgroup of $K^\times$ that includes U_K, qualifying it as a norm group, as per the previous lemma. Moreover, since $N \cap (U_K \cdot (N \cap I))$ is the intersection of two norm groups, it includes a norm group. This results in I containing a norm group, which shows that I itself is a norm group. □

Conclusion

In this thesis, we have presented the following.

1. The construction of Cohomology of groups and Homology of groups and their basic properties. Moreover, we gave constructions of the Tate groups and cup-product to prove the Tate's theorem - one of the most important result in Local Class Field theory.

2. The construction of Local Artin map and prove the Local Reciprocity Law theorem.

3. Finally, we gave proofs to the Local Kronecker-Weber theorem and the Existence theorem.

Bibliography

[1] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[2] Alejandro Adem and R James Milgram. *Cohomology of finite groups*, volume 309. Springer Science & Business Media, 2013.

[3] Kenneth S Brown. *Cohomology of groups*, volume 87. Springer Science & Business Media, 2012.

[4] Edwin Weiss. *Cohomology of Groups: Cohomology of Groups*. Academic Press, 1969.

[5] Serge Lang. *Topics in cohomology of groups*, volume 1625. Springer Science & Business Media, 1996.

[6] Jean-Pierre Serre. *Local fields*, volume 67. Springer Science & Business Media, 2013.

[7] Jean-Pierre Serre and Jean-Pierre Serre. Local class field theory. *Local Fields*, pages 188–203, 1979.

[8] Jürgen Neukirch et al. *Class field theory*, volume 280. Springer, 1986.

[9] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[10] John William Scott Cassels. *Local fields*, volume 3. Cambridge University Press Cambridge, 1986.