Abstract Class Field Theory

Mishty Ray

A dissertation submitted for the partial fulfilment
of BS-MS dual degree in Mathematics

Indian Institute of Science Education and Research Mohali
April 2017

Certificate of Examination

This is to certify that the dissertation titled **Abstract Class Field Theory** submitted by **Mishty Ray** (Reg. No. MS12089) for the partial fulfillment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Abhik Ganguli Dr. Varadharaj Srinivasan Dr. Aribam Chandrakant
(Supervisor)

Dated: April 21, 2017

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Aribam Chandrakant at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of work done by me and all sources listed within have been detailed in the bibliography.

Mishty Ray
(Candidate)
Dated: April 21, 2017

In my capacity as the supervisor of the candidates project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Aribam Chandrakant
(Supervisor)
Dated: April 21, 2017

Acknowledgment

I would like to extend my sincere gratitude to my supervisor, Dr. Aribam Chandrakant, for his patient support, motivation and guidance. In addition, I would like to thank the rest of my thesis committee members - Dr. Abhik Ganguli and Dr. Varadharaj Srinivasan for their kind feedback, and Professor Kapil for his general advice and insight.

I also thank my peers from the math department - Suman Ahmed, Neha Kwatra, and Jitendra Rathore for their participation and support during my presentations. I would like to thank my friends Boddu Satya Spandana, Jayanth Guhan, and Ketika Garg and for their moral support and encouragement. Lastly, I thank Anwesh Ray for his immense help, stimulating discussions and inspiration during the course of my work.

Abstract

Class field theory characterizes abelian extensions of number fields. Both local and global class field theory involve a canonical one to one correspondence between abelian field extensions $L|K$ and certain subgroups of a corresponding module A_K associated with the field K. At the heart of this correspondence lies a reciprocity law, which is a canonical isomorphism of the abelianization of the Galois group $G_{L|K}$ of the extension $L|K$ and the "norm residue group", $A_K/N_{L|K}A_L$, where $N_{L|K}A_L$ is the subgroup of A_K mentioned above. In this thesis, this theory has been studied and presented in utmost generality. A purely group theoretic machinery, which culminates in Tate's theorem, is described in the first chapter. This involves the study of cohomology of finite groups. The next chapter deals with the development of the notion of class formation. This is the main criterion which, when combined with Tate's theorem, yields the general reciprocity law or the main theorem of abstract class field theory. Following this, the class formation of unramified extensions of p-adic number fields is described, which provides a simple yet concrete instance where this theory holds.

Contents

Abstract **iv**

1 Background **1**

1.1 Preliminaries 1

1.2 Towards the canonical isomorphsim $G^{ab} \cong H^{-2}(G, \mathbb{Z})$ 5

1.3 Inflation, Restriction, and Corestriction 8

1.4 Towards Shapiro's lemma 11

1.5 Towards Tate's Theorem 14

2 Abstract Class Field Theory **17**

2.1 Abstract formalism 18

2.2 Towards the reciprocity map 18

2.3 Galois Cohomology 23

2.4 Class formation of unramified extensions 24

A Local fields and unramified extensions **31**

A.1 Discrete valuation rings 31

A.2 Factorization of prime ideals in extensions 33

A.3 Unramified extensions of a local field 34

Bibliography **37**

Chapter 1

Background

1.1 Preliminaries

In class field theory, we come across the action of Galois groups of Galois extensions of algebraic number fields $L|K$ on the set of units $L^\times$.

- Motivated by this, we consider the action of a **finite, multiplicatively written group, G** on an **additively written group A**. Let $a \in A$ and $\sigma, \tau \in G$. Through this action, A becomes a G-module under the following considerations:
  - $1a = a$
  - $\sigma(a + b) = \sigma a + \sigma b$
  - $(\sigma\tau)a = \sigma(\tau a)$
- Define the group ring $\mathbb{Z}[G]$ as $\mathbb{Z}$-linear combinations of elements of G:

  $$\mathbb{Z}[G] = \{\Sigma_{\sigma\in G} n_\sigma \sigma | n_\sigma \in \mathbb{Z}\}$$

  The action of G induces the action of $\mathbb{Z}[G]$ on A in a natural way - $\left(\sum_{\sigma\in G} n_\sigma\sigma\right) \cdot a = \sum_{\sigma\in G} n_\sigma(\sigma \cdot a)$ for $a \in A$.
- Consider the **augmentation map** $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ where,

  $$\varepsilon\left(\sum_{\sigma\in G} n_\sigma\sigma\right) = \sum_{\sigma\in G} n_\sigma.$$

This is a homomorphism of rings, and the kernel of this map is called the augmentation ideal, I_G.

- Consider the **coaugmentation map** $\mu : \mathbb{Z} \to \mathbb{Z}[G]$ where, $\mu(n) = n \cdot N_G$. This too is a ring homomorphism. We shall call $N_G = \sum_{\sigma \in G} \sigma$ the norm of the group G.

- Thus we have the following exact sequences of rings and ring homomorphisms:

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

$$0 \to \mathbb{Z} \xrightarrow{\mu} \mathbb{Z}[G] \to J_G \to 0.$$

- Throughout this exposition, we will consider $\mathbb{Z}$ as a G-module with the trivial action of G:

$$\begin{aligned} G \times A &\to A \\ (g, a) &\mapsto a, \qquad \forall g \in G \end{aligned}$$

- Let A and B be abelian groups. Then the set of all $\mathbb{Z}$ homomorphisms between them is denoted throughout by $Hom(A, B)$ and the tensor product over $\mathbb{Z}$ by $A \otimes B$. Both these new sets are $\mathbb{Z}$ modules.

Proposition 1.1. *Consider the group ring $\mathbb{Z}[G]$ as defined above.*

1. *The augmentation ideal I_G is a free group generated by the elements $\sigma - 1$, where $\sigma \in G$ and $\sigma \neq 1$.*

2. *$J_G = \mathbb{Z}[G]/\mathbb{Z} \cdot N_G$ is the free group generated by the elements σ mod $\mathbb{Z} \cdot N_G$, where $\sigma \neq 1$.*

Using the terms defined above, we define some important submodules of A. They are given as follows:

$A^G = \{a \in A \mid \sigma a = a\}$ (Fixed group under the G-action on A.)
$N_G A = \{\sum_{\sigma \in G} \sigma a \mid a \in A\}$ (Norm subgroup of A.)
${}_{N_G}A = \{a \in A \mid N_G a = 0\}$
$I_G A = \{\sum_{\sigma \in G} (\sigma - 1)a \mid a \in A\}$

Definition 1.1. *Let A, B be two G-modules. A homomorphism $f : A \to B$ is said to be a G* ***homomorphism*** *if $f(\sigma a) = \sigma f(a)$.*

Note that both the augmentation and the coaugmentation maps are G-homomorphisms. $Hom(A, B)$, which denote the set of all $\mathbb{Z}$-homomorphisms between the $\mathbb{Z}$-modules A and B form an abelian group under pointwise operation. This is a G-module under the following action of G:
Let $\sigma \in G$, and $f \in Hom(A, B)$. Then, $\sigma(f) = \sigma \circ f \circ \sigma^{-1}$. The set of all G-homomorphisms denoted by $Hom_G(A, B)$ is a subgroup of $Hom(A, B)$. In particular,

$$Hom_G(A, B) = Hom(A, B)^G$$

Definition 1.2. *A G-module is said to be G-free if it is the direct sum of G modules that are isomorphic copies of $\mathbb{Z}[G]$.*

Remark. *G-free modules are also $\mathbb{Z}$-free.*

Lemma 1.1. *Let $\cdots \to X_{q+1} \xrightarrow{d_q+1} X_q \xrightarrow{d_q} X_{q-1} \xrightarrow{d_{q-1}} \cdots$ be an exact sequence of $\mathbb{Z}$-free modules and $\mathbb{Z}$ homomorphisms and D be a $\mathbb{Z}$ module. Then the sequence $\cdots \to Hom(X_{q-1}, D) \to Hom(X_q, D) \to Hom(X_{q+1}, D) \to \cdots$ is exact. In other words, under these considerations, the $Hom(\_, D)$ functor is exact.*

Remark. *In general, the $Hom_G(\_, D)$ functor is not exact.*

Definition 1.3. *Let G be a finite group written multiplicatively. Then the* ***complete free resolution*** *of the G- module $\mathbb{Z}$ (defined by letting G act on $\mathbb{Z}$ trivially, i.e, as the identity) is the complex defined as follows:*

$$\cdots \xleftarrow{d_{-2}} X_{-2} \xleftarrow{d_{-1}} X_{-1} \xleftarrow{d_0} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \xleftarrow{d_3} \cdots \qquad (*)$$

$$\mu \nwarrow \quad \swarrow \varepsilon$$

$$\mathbb{Z}$$

$$\swarrow \quad \searrow$$

$$0 \qquad 0$$

such that the following properties are satisfied:

- *X_q are free G modules*
- *All maps are G-homomorphisms*

- $d_0 = \mu \circ \varepsilon$; ε, μ *are the augmentation and coaugmentation maps respectively.*
- *At every term we have exactness*

Set $X_q = X_{-q-1} = \bigoplus \mathbb{Z}[G](\sigma_1, \sigma_2, ..., \sigma_q)$, where $(\sigma_1, \sigma_2, ..., \sigma_q)$ is a q-tuple and $q \geq 1$ and $\sigma_i s$ run over all elements of G. This direct sum can be thought of as the set of all $\mathbb{Z}[G]$-linear combinations of elements from $\prod_{i=1}^{q} G$. For $q = 0$, we have $X_0 = X_{-1} = \mathbb{Z}[G]$.

Let A be a G module. Set $A_q = Hom_G(X_q, A)$. For any $x \in A_q = Hom(X_q, A)$, x can be thought of as a map $x : \prod_{i=1}^{q} G \to A$. Now from the exact sequence $(*)$, we get the complex:

$$\cdots \xrightarrow{\partial_{-2}} A_{-2} \xrightarrow{\partial_{-1}} A_{-1} \xrightarrow{\partial_0} A_0 \xrightarrow{\partial_1} A_1 \xrightarrow{\partial_2} A_2 \xrightarrow{\partial_3} \cdots \qquad (**)$$

This complex is not exact. From $(*)$, we have $d_q \circ d_{d+1} = 0$, $\forall q \in \mathbb{Z}$. Therefore, $\partial_{q+1} \circ \partial_q = 0$ $\forall q \in \mathbb{Z}$. Thus, $\forall q \in \mathbb{Z}$:

$$im\partial_q \subseteq ker\partial_{q+1}$$

Set $Z_q = ker\partial_{q+1}$ and $R_q = im\partial_q$. Elements of $\boldsymbol{Z_q}$ are called **q-cocycles** and those of $\boldsymbol{R_q}$ are called **q-coboundaries**.

We now define the maps d_q and ∂_q explicitly.

Definition 1.4. *The G-homomorphisms d_q as in $(*)$are defined as follows:*
$d_0 1 = N_G$;
$d_1(\sigma) = \sigma - 1$;
$d_{-1} 1 = \sum_{\sigma \in G} (\sigma^{-1}(\sigma) - (\sigma))$

$$d_q(\sigma_1, \sigma_2, ..., \sigma_q) = \sigma_1(\sigma_2, ..., \sigma_q) + \sum_{i=1}^{q-1} (-1)^i (\sigma_1, ..., \sigma_i \sigma_{i+1}, ..., \sigma_q) + (-1)^q (\sigma_1, \sigma_2, ..., \sigma_{q-1}); \qquad q > 1$$

$$d_{-q-1}(\sigma_1, \sigma_2, ..., \sigma_q) = \sum_{\sigma \in G} [\sigma^{-1}(\sigma, \sigma_1, \sigma_2, ..., \sigma_q) + \sum_{i=1}^{q} (-1)^i (\sigma_1, ..., \sigma_{i-1}, \sigma_i \sigma, \sigma^{-1}, \sigma_{i+1} ..., \sigma_q) + (-1)^{q+1} (\sigma_1, \sigma_2, ..., \sigma_q, \sigma)]; \qquad -q - 1 < -1$$

Definition 1.5. *The G-homomorphisms ∂_q as in $(**)$ are defined as follows:*
$\partial_0 x = N_G x;\ \ x \in A_{-1} = A$
$\partial_1 x(\sigma) = \sigma x - x;\ \ x \in A_0 = A$
$\partial_{-1} x = \sum_{\sigma \in G}(\sigma^{-1} x(\sigma) - x(\sigma));\ \ x \in A_{-2}$
For $q \geq 1$ we have,

$$\partial_q x(\sigma_1, \sigma_2, ..., \sigma_q) = \sigma_1 x(\sigma_2, ..., \sigma_q) + \sum_{i=1}^{q-1}(-1)^i x(\sigma_1, ..., \sigma_i\sigma_{i+1}, ..., \sigma_q) + (-1)^q x(\sigma_1, \sigma_2, ..., \sigma_{q-1}); \quad x \in A_{q-1}$$

$$\partial_{-q-1} x(\sigma_1, \sigma_2, ..., \sigma_q) = \sum_{\sigma \in G}[\sigma^{-1} x(\sigma, \sigma_1, \sigma_2, ..., \sigma_q) + \sum_{i=1}^{q}(-1)^i x(\sigma_1, ..., \sigma_{i-1}, \sigma_i\sigma, \sigma^{-1}, \sigma_{i+1}..., \sigma_q) + (-1)^{q+1} x(\sigma_1, \sigma_2, ..., \sigma_q, \sigma)]; \quad x \in A_{-q-2}$$

Definition 1.6. *The factor group*

$$H^q(G, A) = Z_q / R_q$$

is called the ***cohomology group of dimension q*** *($q \in \mathbb{Z}$) of the G-module A or the* ***q-th cohomology group with coefficients in*** *A.*

Computations of some general factor groups of low dimension are given below:

$H^{-1}(G, A) =_{N_G} A/I_G A$
$H^0(G, A) = A^G/N_G A$ (Norm residue group)
$H^1(G, A) = Z_1/R_1$ where, $Z_1 = \{x : G \to A \mid x(\sigma\tau) = \sigma x(\tau) + x(\sigma)\}$, and
$R_1 = \{\sigma a - a \mid a \in A\}$

1.2 Towards the canonical isomorphsim $G^{ab} \cong H^{-2}(G, \mathbb{Z})$

Theorem 1.1. *Let $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ be an exact sequence of G-modules and G-homomorphisms. This induces a sequence of cohomology factor groups,*

$$\cdots \to H^q(G, A) \xrightarrow{\bar{i_q}} H^q(G, B) \xrightarrow{\bar{j_q}} H^q(G, C) \xrightarrow{\delta_q} H^{q+1}(G, A) \to \cdots$$

which is also exact. It is called the exact cohomology sequence. Here $\bar{i_q}, \bar{j_q}$ are induced by the maps i_q and j_q respectively, and δ_q is the connecting homomorphism.

Corollary 1.1.1. *If $H^q(G,A) = 0$ for all q, $H^q(G,B) \cong H^q(G,C)$. Similarly, if $H^q(G,B) = 0$ (resp. $H^q(G,C) = 0$) for all q, $\delta_q : H^q(G,C) \to H^{q+1}(G,A)$ (resp. $\bar{i}_q : H^q(G,A) \to H^q(G,B)$) is an isomorphism.*

Definition 1.7. *A G-module A is said to be G-induced if there is a subgroup D of A such that*

$$A = \bigoplus_{\sigma \in G} \sigma D$$

Example: $\mathbb{Z}[G] = \bigoplus_{\sigma \in G} \sigma(\mathbb{Z} \cdot 1)$

Proposition 1.2. *Let X be a G-induced module, and A be an arbitrary G-module. Then $X \otimes A$ is a G-induced module.*

Proof. Recall that we have fixed the notation $X \otimes A$ to be the tensor product over $\mathbb{Z}$. As X is a G-induced module, we have $X = \bigoplus_{\sigma \in G} \sigma D$, where D is a subgroup of X. Thus,
$X \otimes A = \left(\bigoplus_{\sigma \in G} \sigma D\right) \otimes A \cong \bigoplus_{\sigma \in G} (\sigma D) \otimes (\sigma A) \cong \bigoplus_{\sigma \in G} \sigma(D \otimes A)$. □

Proposition 1.3. *Let A be a G-induced module, and K is a subgroup of G. Then A is a K induced K module. If K is normal in G, then A^K is a G/K - induced G/K module.*

Definition 1.8. *We say that a G module A has trivial cohomology if $H^q(K,A) = 0$ for all $q \in \mathbb{Z}$ and all subgroups $K \subseteq G$.*

Theorem 1.2. *Every G-induced module has trivial cohomology.*

Proof. By Proposition 1.3, it suffices to show that $H^q(G,A) = 0$. For each factor group to be trivial, we need to show that the sequence obtained from the exact sequence $(*)$,

$$\cdots \to Hom_G(X_q, A) \xrightarrow{\partial_q} Hom_G(X_{q+1}, A) \to \cdots$$

is exact. By hypothesis, A is G-induced, therefore $A = \bigoplus_{\sigma \in G} \sigma D$, where D is a subgroup of A. Let $\pi : A \to D$ be the natural projection of A onto D. Now, as each X_q is finitely generated, we have the isomorphism $Hom(X_q, A) = Hom(X_q, \bigoplus_{\sigma \in G} \sigma D \cong$

$\bigoplus_{\sigma \in G} Hom(X_q, \sigma D)$. Then the map $f \mapsto \pi \circ f$ induces an isomorphism between $Hom_G(X_q, A)$ and $Hom_{\mathbb{Z}}(X_q, D) = Hom(X_q, D)$. Therefore, it suffices to consider

$$\cdots \to Hom(X_q, D) \to Hom(X_{q+1}, D) \to \cdots$$

which is exact by Lemma 1.1.

Theorem 1.3. *There is a canonical isomorphism* $H^{-2}(G, \mathbb{Z}) \cong G^{ab}$

Proof. Consider the exact sequence,

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0.$$

From Theorem 1.1, we obtain the exact cohomology sequence:

$$\cdots \to H^q(G, I_G) \to H^q(G, \mathbb{Z}[G]) \to H^q(G, \mathbb{Z}) \xrightarrow{\delta_q} H^{q+1}(G, I_G) \to \cdots$$

We know that $\mathbb{Z}[G]$ is a G-induced module. Therefore, by Theorem 1.2,

$$H^q(G, \mathbb{Z}[G]) = 0, \quad \forall q \in \mathbb{Z}.$$

By Corollary 1.1.1, we have the isomorphism:

$$H^q(G, \mathbb{Z}) \cong H^{q+1}(G, I_G), \quad \forall q \in \mathbb{Z}.$$

In particular, we have the isomorphism $H^{-2}(G, \mathbb{Z}) \cong H^{-1}(G, I_G)$.
Note that $H^{-1}(G, I_G) = I_G / I_G^2$.
Therefore, it suffices to show that $G^{ab} \cong I_G / I_G^2$
Consider the map $\Phi : G \to I_G / I_G^2$ such that $\sigma \mapsto (\sigma - 1) + I_G^2$.
Φ is a homomorphism because:

$$\begin{aligned} \Phi(\sigma\tau) &= \sigma\tau - 1 + I_G^2 \\ &= (\sigma - 1) + (\tau - 1) + (\sigma - 1) \cdot (\tau - 1) + I_G^2 \\ &= (\sigma - 1) + (\tau - 1) + I_G^2 \\ &= \Phi(\sigma) + \Phi(\tau) \end{aligned}$$

The last two inequalities hold because we have seen in Proposition **??** that I_G is the additive free abelian group generated by the elements $\sigma - 1$ where $\sigma \in G - \{1\}$.

As I_G/I_G^2 is Abelian, the commutator subgroup $G^{'} \subseteq \ker\Phi$. Therefore we have the homomorphism:

$$log : G/G^{'} \to I_G/I_G^2$$

Now we claim that log is an isomorphism. To prove this claim, consider the map:

$$exp : I_G/I_G^2 \to G/G^{'}$$

such that $(\sigma - 1) + I_G^2 \mapsto \sigma G^{'}$. This map is a surjective homomorphism. Its a homomorphism because :

$$\begin{aligned} exp((\sigma-1)+(\tau-1)+I_G^2) &= exp((\sigma-1)+(\tau-1)+(\sigma-1)\cdot(\tau-1) \\ &\quad + I_G^2) \\ &= exp(\sigma\tau - 1) = (\sigma\tau)G^{'} \\ &= exp((\sigma-1)+I_G^2)\cdot exp((\tau-1)+I_G^2) \end{aligned}$$

Since, $(\sigma-1)\cdot(\tau-1) = (\sigma\tau-1)-(\sigma-1)-(\tau-1) \mapsto \sigma\tau\sigma^{-1}\tau^{-1}G^{'} = \bar{1}$, we have, $I_G^2 \subseteq ker\ exp$.
Observe that $log \circ exp = Id_{I_G/I_G^2}$, and $exp \circ log = Id_{G/G^{'}}$.
Thus the claim holds. This finishes the proof. □

1.3 Inflation, Restriction, and Corestriction

Lemma 1.2 (**Method of dimension shifting**). *Let A be a G- module. Then there exist G-modules indexed by m defined as follows:*

$$A^m = \begin{cases} (\otimes_{i=1}^m J_G) \otimes A & m \geq 0 \\ (\otimes_{i=1}^m I_G) \otimes A & m < 0 \end{cases}$$

with the property that the m-fold composition of the connecting homomorphism δ induces $\forall q \in \mathbb{Z}$ and every subgroup $K \subseteq G$ the isomorphism:

$$\delta^m : H^{q-m}(K, A) \to H^q(K, A), \qquad m \in \mathbb{Z}.$$

This is a crucial method employed to formally extend the definition of the inflation, restriction and corestriction maps from the dimension 0 to arbitrary dimensions. Before defining the aforesaid maps, we will state a simple application of dimension shifting in calculating cohomology factor groups, which will be useful later.

Theorem 1.4. *Let A be a G-module where G is a finite group. Then $H^q(G, A)$ is a torsion group and the orders of elements in $H^q(G, A)$ divide the order n of the group G:*

$$n \cdot H^q(G, A) = 0$$

Proof. We know that, $H^0(G, A) = A^G/N_G A$, and $N_G a = n \cdot a \ \forall a \in A$. Thus $n \cdot H^0(G, A) = 0$. From Lemma 1.2, we have the isomorphism $H^q(G, A) \cong H^0(G, A^q)$. The theorem follows from this □

Definition 1.9. *An abelian group A is said to be uniquely divisible if for every $a \in A$ and every $n \in \mathbb{N}$, we have a unique solutionto the equation $nx = a$ for x in A .*

Corollary 1.4.1. *A uniquely divisible G-module has trivial cohomology.*

In particular, the G-module $\mathbb{Q}$ with the trivial action of G has trivial cohomology, as $\mathbb{Q}$ is uniquely divisible.

Corollary 1.4.2. *There is a canonical isomorphism:*

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

where $\mathbb{Z}$ and $\mathbb{Q}/\mathbb{Z}$ are G-modules with the trivial action of G.

Proof. Consider the long exact cohomology sequence obtained from the following exact sequence:

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

$\mathbb{Q}$ is uniquely divisible, and thus from Corollary 1.4.1, we have $H^q(G, \mathbb{Q}) = 0, \ \forall q$. Therefore by Corollary 1.1.1 we have the isomorphism $H^q(G, \mathbb{Q}/\mathbb{Z}) \cong H^{q+1}(G, \mathbb{Z})$. Take $q = 1$ and the result follows. □

Definition 1.10. $\chi(G) := Hom(G, \mathbb{Q}/\mathbb{Z})$ *is called the* ***character group*** *of G.*

Definition 1.11 (**Inflation**)**.** *Let A be a G-module and K a normal subgroup of G. The homomorphism*

$$inf_q : H^q(G/K, A^K) \to H^Q(G, A), \qquad q \geq 1,$$

induced by the homomorphism from the q-th group of cochains of the G/K-induced module A^K to the q-th group of cochains of the G-module is called inflation.

Note that the *inf* map is defined only for normal subgroups and for positive dimensions.

Definition 1.12 (**Restriction**). *Let G be a finite group and K be a subgroup. Then* ***restriction*** *is the uniquely determined family of homomorphisms:*
$res_q : H^q(G, A) \to H^q(K, A), \quad q \in \mathbb{Z}$, *such that*

- $res_0 : H^0(G, A) \to H^0(K, A)$, $q \in \mathbb{Z}$
  $a + N_G A \mapsto a + N_K A \qquad (a \in A^G)$
- *For every exact sequence $0 \to A \to B \to C \to 0$ of G-modules and G homomorphisms, the following diagram is commutative:*

$$\begin{array}{ccc} H^q(G, C) & \xrightarrow{\delta} & H^{q+1}(G, A) \\ \downarrow{\scriptstyle res_q} & & \downarrow{\scriptstyle res_{q+1}} \\ H^q(K, C) & \xrightarrow[\delta]{} & H^{q+1}(K, C) \end{array}$$

The definition of restriction is extended to all dimensions from the zeroth dimension by the method of dimension shifting shown by the following commutative diagram:

$$\begin{array}{ccc} H^0(G, A^q) & \xrightarrow{\delta^q} & H^q(G, A) \\ \downarrow{\scriptstyle res_0} & & \downarrow{\scriptstyle res_q} \\ H^0(K, A^q) & \xrightarrow[\delta^q]{} & H^q(K, A) \end{array}$$

Definition 1.13 (**Corestriction**). *Let G be a finite group with a subgroup K and A a G-module Thencorestriction is the uniquely determined family of homomorphisms,*

$$cor_q : H^q(K, A) \to H^q(G, A), \qquad q \in \mathbb{Z},$$

with the properties:

- *If $q = 0$, then*

$$cor_0 : H^0(K, A) \to H^0(G, A), \qquad a + N_G A \mapsto N_{G/K} a + N_G A \qquad (a \in A^K)$$

- *For every exact sequence $0 \to A \to B \to C \to 0$ of G-modules and G-homomorphsims, the following diagram is commutative:*

$$\begin{array}{ccc} H^0(K, C) & \xrightarrow{\delta} & H^{q+1}(K, A) \\ {\scriptstyle cor_q}\downarrow & & \downarrow{\scriptstyle cor_{q+1}} \\ H^0(G, C) & \xrightarrow{\delta} & H^{q+1}(G, A) \end{array}$$

The definition of corestriction can be extended to arbitrary dimensions using the method of dimension shifting:

$$\begin{array}{ccc} H^0(K, A^q) & \xrightarrow{\delta^q} & H^q(K, A) \\ {\scriptstyle cor_0}\downarrow & & \downarrow{\scriptstyle cor_q} \\ H^0(G, A^q) & \xrightarrow{\delta^q} & H^q(G, A) \end{array}$$

An important property of inf, res and cor maps is that they commute with connecting homomorphisms and G-homomorphisms.

1.4 Towards Shapiro's lemma

Lemma 1.3. *Let $\{A_i | i \in I\}$ be a family of G-modules, and let X be another G-module. Then we have the canonical isomorphisms*

$$X \otimes (\bigoplus_i A_i) \cong \bigoplus_i (X \otimes A_i)$$

Moreover, if X is a finitely generated as an abelian group, then

$$X \otimes (\prod_i A_i) \cong \prod_i (X \otimes A_i)$$

Lemma 1.4. *Let $\{A_i | i \in I\}$ be a family of G-modules. Then,*

$$H^q(G, \bigoplus_i A_i) \cong \bigoplus_i H^q(G, A_i)$$

Definition 1.14. *Let G be a finite group and K be a subgroup. A G-module A is called **G/K-induced** if it has the following representation:*

$$A = \bigoplus_{\sigma \in G/K} \sigma D$$

where $D \subseteq A$ is a subgroup of A which is a K- module and σ ranges over a system of left coset representatives of K in G.

Theorem 1.5. ***Shapiro's Lemma**: Let $A = \bigoplus_{\sigma \in G} \sigma D$ be a G/K induced G module where K is a subgroup of G. Then,*

$$H^q(G, A) \cong H^q(K, D)$$

and this isomorphism is given by the composition:

$$H^q(G, A) \xrightarrow{res} H^q(K, A) \xrightarrow{\bar{\pi}} H^q(K, D)$$

where $\bar{\pi}$ is induced by the natural projection $\pi : A \to D$.

Proof. As A is a G/K-induced G-module, we have $A = \bigoplus_{i=1}^{m} \sigma_i D$, where σ_i ranges over a system of left coset representatives of G/K, in particular let $\sigma_i = 1$. For $q = 0$, define the following composition of maps:

$$A^G/N_G A \xrightarrow{res} A^K/N_K A \xrightarrow{\bar{\pi}} D^K/N_K D$$

Now define a map in the opposite direction of the above homomorphism:

$$\nu : D^K/N_K D \to A^G/N_G A$$

where $\nu(d+N_KD) = \sum_{i=1}^{m} \sigma_i d + N_G A$. We observe that $(\bar{\pi} \circ res) \circ \nu = id$ on $D^K/N_K D$ and $\nu \circ (\bar{\pi} \circ res) = id$ on $A^G/N_G A$, which makes $\pi \circ res$ bijective. Now, we set

$$\begin{array}{lll} A^q = (\otimes_{i=1}^{q} J_G) \otimes A & & A^q = \left(\otimes_{i=1}^{|q|} I_G\right) \otimes A \\ D_*^q = (\otimes_{i=1}^{q} J_G) \otimes D, & resp & D_*^q = \left(\otimes_{i=1}^{|q|} I_G\right) \otimes D \\ D^q = (\otimes_{i=1}^{q} J_K) \otimes D & & D^q = \left(\otimes_{i=1}^{|q|} I_K\right) \otimes D \end{array}$$

for $q \geq 0$ resp, $q < 0$. As $A = \bigoplus_{i=1}^{m} \sigma_i D$, we have,

$$J_G = J_K \oplus K_1 \quad resp \quad I_G = I_K \oplus K_{-1},$$

where K_1 and K_{-1} are K-induced modules as defined below:

$$K_1 = \bigoplus_{\tau \in K} \tau \left(\sum_{i=2}^{m} \mathbb{Z} \cdot \bar{\sigma}_i^{-1} \right) \quad resp \quad K_{-1} = \bigoplus_{\tau \in K} \left(\sum_{i=2}^{m} \mathbb{Z} \cdot (\sigma_i^{-1} - 1) \right)$$

Substituting these expressions for I_G and J_G in D^q and D_q^* respectively, and using Proposition 1.2 and Lemma 1.3, we obtain for all q the canonical K-module decomposition

$$D_*^q = D^q \oplus C^q$$

for some K-induced K-module C^q. Using the method of dimension shifting stated in Lemma 1.2, we then obtain the diagram,

$$\begin{array}{ccccccc} H^0(G, A^q) & \xrightarrow{res} & H^0(K, A^q) & \xrightarrow{\bar{\pi}_*} & H^0(K, D_*^q) & \xrightarrow{\bar{\rho}} & H^0(K, D^q) \\ \downarrow{\scriptstyle \delta_q} & & \downarrow{\scriptstyle \delta_q} & & & & \downarrow{\scriptstyle \delta_q} \\ H^q(G, A) & \xrightarrow[res]{} & H^q(K, A) & \xrightarrow{\bar{\pi}} & H^q(K, D) & \xrightarrow{id} & H^q(K, D) \end{array}$$

in which the map $\pi_* \circ res$ in the upper row in dimension 0 is bijective as shown above. From Lemma 1.4 $H^0(K, D^q) \cong H^0(K, D^q \bigoplus C^q) \cong H^0(G, D^q) \bigoplus H^0(G, C^q)$. As C^q is K-induced, we use Theorem 1.2 and Corollary 1.1.1 to conclude that $\bar{\rho}$ is bijective. Now we need to show that this diagram commutes. Since the composition $A^q \xrightarrow{\pi} D_*^q \xrightarrow{\rho} D^q$ is induced by the projection $A \xrightarrow{\pi} D$ and δ_q is an isomorphism, we see it does. As the upper map $\rho \circ \bar{\pi}_* \circ res$ is bijective, so is the lower map $\bar{\pi} \circ res$. $\square$

1.5 Towards Tate's Theorem

Definition 1.15 (**Cup Product**). *If A and B are G-modules, then there exists a uniquely determined family of bilinear mappings, the cup product*

$$H^p(G,A) \times H^q(G,B) \overset{\cup}{\to} H^{p+q}(G, A \otimes B)$$

with the following properties:

- *For $p = q = 0$, the cup product is given by*

$$(\bar{a}, \bar{b}) \mapsto \bar{a} \cup \bar{b} = a \bar{\otimes} b, \qquad \bar{a} \in H^0(G,A), \bar{b} \in H^0(G,B)$$

- *If the sequences of G modules*

$$0 \to A \to A^{'} \to A^{''} \to 0$$

$$0 \to A \otimes B \to A^{'} \otimes B \to A^{''} \otimes B \to 0$$

are both exact, then the following diagram commutes:

$$\begin{array}{ccc} H^p(G,A^{''}) \times H^q(G,B) & \xrightarrow{\cup} & H^{p+q}(G, A^{''} \otimes B) \\ \downarrow{\scriptstyle \delta \times 1} & & \downarrow{\scriptstyle \delta} \\ H^{p+1}(G,A) \times H^q(G,B) & \xrightarrow{\cup} & H^{p+q+1}(G, A \otimes B) \end{array}$$

so that

$$\delta(\bar{a}^{''} \cup \bar{b}) = \delta a^{''} \bar{\cup} b, \quad \bar{a}^{''} \in H^p(G,A^{''}), \bar{b} \in H^q(G,B)$$

- *If the sequences of G-modules*

$$0 \to B \to B^{'} \to B^{''} \to 0$$

$$0 \to A \otimes B \to A \otimes B^{'} \to A \otimes B^{''} \to 0$$

are both exact, then the following diagram commutes:

$$\begin{array}{ccc} H^p(G,A) \times H^q(G,B^{''}) & \xrightarrow{\cup} & H^{p+q}(G, A \otimes B^{''}) \\ \downarrow{\scriptstyle 1 \times \delta} & & \downarrow{\scriptstyle (-1)^p \delta} \\ H^p(G,A) \times H^{q+1}(G,B) & \xrightarrow{\cup} & H^{p+q+1}(G, A \otimes B) \end{array}$$

so that

$$\delta(\bar{a} \cup \bar{b}'') = (-1)^p (a \bar{\cup} b'', \quad \bar{a} \in H^p(G, A), \bar{b}'' \in H^q(G, B'')$$

For a fixed element, $a \in H^p(G, A)$, the following map provides a whole family of maps:

$$a\cup : H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

$$b \mapsto a \cup b$$

Theorem 1.6. *Let A be a G-module with the following properties. For each subgroup, $K \subseteq G$, we have*
I. $H^{-1}(K, A) = 0$
II. $H^0(K, A)$ is a cyclic group of order $|K|$
If a generates the group $H^0(G, A)$, then the cup product map

$$a\cup : H^q(G, \mathbb{Z}) \to H^q(G, A)$$

is an isomorphism $\forall q \in \mathbb{Z}$.

Theorem 1.7. ***Tate's theorem:*** *Let A be a G-module with the following properties. For each subgroup K of G,*
I. $H^1(K, A) = 0$, and
II. $H^2(K, A)$ is a cyclic group of order $|K|$.
If a generates the group $H^2(G, A)$, then the cup product map,

$$a\cup : H^q(G, \mathbb{Z}) \to H^{q+2}(G, A)$$

is an isomorphism $\forall q \in \mathbb{Z}$.

Proof. Let A^2 be as defined in Lemma 1.2 for $q = 2$. Shift the cohomology factor group by two dimensions using the method of dimension shifting via the map $\delta^2 : H^q(a, A^2) \to H^{q+2}(K, A)$ from Lemma 1.2. By assumptions I and II, $H^{-1}(K, A^2) = H^1(K, A) = 0$, and that $H^0(g, A^2) = H^2(K, A)$ is cyclic of order $|K|$. Thus, the generator $a \in H^2(G, A)$ can be mapped back from the generator $\delta^{-2}a \in H^0(G, A^2)$. It follows from Definition 1.15 that the diagram

$$\begin{array}{ccc} H^q(G,\mathbb{Z}) & \xrightarrow{\delta^{-2}a\cup} & H^q(G,A^2) \\ \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \delta^2} \\ H^q(G,\mathbb{Z}) & \xrightarrow{a\cup} & H^{q+2}(G,A) \end{array}$$

commutes. Since $\delta^{-2}a\cup$ is bijective by Theorem 1.6, so is $a\cup$. □

For class field theory, the dimension $q = -2$ is of particular interest. By Tate's theorem, we get the canonical isomorphism between $G^{ab} \cong H^{-2}(G,\mathbb{Z})$ and the norm residue group $A^G/N_G A = H^0(G,A)$,

$$G^{ab} \mapsto A^G/N_G A.$$

This canonical isomorphism is the abstract formulation of class field theory, the so called "reciprocity law". For this reason, one can consider Tate's theorem as the foundation of the purely group theoretically formulated abstract version of class field theory. However, this reciprocity map is not canonical as it depends upon the generator of the factor group of dimension 2. To circumvent this, we develop further theory in the next chapters.

Chapter 2

Abstract Class Field Theory

Motivation

The main goal of field theory is to classify all algebraic extensions of a field. The main goal of class field theory is to classify all abelian extensions of a field. Class field theory gives rise to the famous theorem of **Kronecker and Weber**:

> **Theorem.** *Every abelian extension of the field $\mathbb{Q}$ is a cyclotomic field, i.e, a subfield of the cyclotomic extension $\mathbb{Q}(\zeta)$, where ζ is a root of unity.*

At the heart of class field theory lies a canonical one-to-one correspondence between abelian extensions of a field K, and norm subgroups of a module corresponding to this field, say A_K. This correspondence obeys the "reciprocity law", i.e., if a subgroup $I \subseteq A_K$ corresponds to an abelian field extension $L|K$, then there is a canonical isomorphism between the Galois group $G_{L|K}$ and A_K/I. The Galois group is compact and Hausdorff with respect to the Krull toplogy. Thus, to describe class field theory in its abstract form, we consider a profinite group G, and impose certain formal notions to obtain a formal Galois theory.

2.1 Abstract formalism

- We consider G as a profinite group[1]. We may think of G as the Galois group of an infinite Galois extension endowed with Krull topology. The open subgroups are precisely the closed subgroups of finite index. Consider the family $\{G_K | K \in X\}$ of all open subgroups. The indices, K, are called fields.

- We label K_0 with $G_{K_0} = G$ as the base field. If $G_L \subseteq G_K$, we write formally $K \subseteq L$. Define $[L : K] := (G_K : G_L)$.

- A is a G-module on which the G-action is continuous. Such a pair (G, A) is called a **formation**.

- $L|K$ is called a normal extension if G_L is a normal subgroup of G_K. In this case, define $G_{L|K} := G_K/G_L$. For a normal extension $L|K$, A_L becomes a $G_{L|K}$ module. Similarly, $L|K$ is cyclic, abelian or solvable if $G_{L|K}$ is cyclic, abelian or solvable.

- A is assumed to be a multiplicative G-module on which the action of G is captured by:
$$G \times A \to A(\sigma, a) \mapsto a^\sigma.$$
Note that the norm $\sum_{\sigma \in G} \sigma a$ as denoted in the previous section with an abelian group A becomes $\prod_{\sigma \in G} a^\sigma$.

- Once our G and A are fixed, we denote A^{G_K} as A_K, and $H^q(G_{L|K}, A_L)$ by $H^q(L|K)$.

- The intersection of the fields K_i is defined as $K = \cup_{i=1}^n K_i$, if G_K is topologically generated by G_{K_i} in G, and $K = \prod_{i=1}^n K_i$ if $G_K = \cap_{i=1}^n G_{K_i}$.

- L' is said to be conjugate with L if $G_{L'} = \sigma G_L \sigma^{-1}$ for some $\sigma \in G_K$. In this case, we write $L' = \sigma L$.

2.2 Towards the reciprocity map

If $N \supseteq L \supseteq K$ is a tower of normal extensions, then we have $G_{L|K} \trianglelefteq G_{N|K}$. Thus, we have the inflation map $H^q(G_{L|K}, A_N^{G_{N|L}}) \xrightarrow{inf} H^q(G_{N|K}, A_N)$. As, $A_N^{G_{N|L}} = A_L$, we

[1]For theory of infinite Galois extensions and profinite groups, see [Neu99], Chater 4, §1, 2, and 3

write $H^q(G_{L|K}, A_L) \xrightarrow{inf} H^q(G_{N|K}, A_N)$. This induces a map

$$inf_N : H^q(L|K) \to H^q(N|K), \qquad q \geq 1.$$

Similarly, the restriction and corestriction maps,

$$H^q(G_{N|K}, A_N) \xrightarrow{res} H^q(G_{L|K}, A_N) \qquad and \qquad H^q(G_{N|L}, A_N) \xrightarrow{cor} H^q(G_{N|K}, A_N),$$

induce $\forall q \in \mathbb{Z}$ the maps:

$$H^q(N|K) \xrightarrow{res_L} H^q(L|K) \qquad and \qquad H^q(N|L) \xrightarrow{cor_K} H^q(N|K).$$

Also, for $\sigma \in G$ we have the isomorphisms $G_{L|K} \cong G_{\sigma L|\sigma K}$ and $A \cong \sigma A$ defined by the maps $\tau G_L \mapsto \sigma\tau\sigma^{-1} G_{\sigma L}$, and $a \mapsto \sigma a$ respectively. These maps yield the isomorphism

$$H^q(L|K) \xrightarrow{\sigma^*} H^q(\sigma L|\sigma K).$$

This isomorphism commutes with inf_N, res_L, and cor_K.

Definition 2.1. *A formation (G, A) is called a **field formation** if $H^1(L|K) = 1$ for each normal extension $L|K$.*

On a field formation (G, A), imposition of the hypothesis of Tate's theorem yields the isomorphism $G^{ab}_{L|K} \cong A_K / N_{L|K} A_L$. However, this isomorphism is not canonical as it depends upon the generator of $H^2(G_{L|K}, A_L)$. Thus, some extra conditions are required.

Definition 2.2. *A formation (G, A) is called a class formation if it satisfies the following axioms:*
I. $H^1(L|K) = \{1\}$ for every normal extension $L|K$.
II. For every normal extension $L|K$ there exists an isomorphism

$$inv_{L|K} : H^2(L|K) \to \frac{\frac{1}{[L:K]}\mathbb{Z}}{\mathbb{Z}}$$

*called the **invariant map** with the following properties*

- *$K \subseteq L \subseteq N$ is a tower of normal extensions, then $inv_{L|K} = inv_{N|K}\big|_{H^2(L|K)}$.*

- *$K \subseteq L \subseteq N$ is a tower of extensions with $N|K$ normal then*

$$inv_{N|L} \circ res_L = [L : K] \cdot inv_{N|K}$$

.

Definition 2.3. *Let $L|K$ be a normal extension. There exists a uniquely determined element $u_{L|K} \in H^2(L|K)$,*
*s.t. $inv_{L|K}\left(u_{L|K}\right) = \dfrac{1}{[L : K]} + \mathbb{Z}$, called the **fundamental class** of $L|K$.*

Proposition 2.1. *Let $N \supseteq L \supseteq K$ be a tower of extensions with $N|K$ normal. Then*

a. $inv_{N|K}c = inv_{L|K}c$, *if $L|K$ is normal and $c \in H(L|K)$,*

b. $inv_{N|L}(res_L c) = [L : K] \cdot inv_{N|K}c$, *for $c \in H^2(N|K)$,*

c. $inv_{N|K}(cor_K c) = inv_{N|L}c$, *for $c \in H^2(N|L)$,*

d. $inv_{\sigma N|\sigma K}(\sigma^* c) = inv_{N|K}c$, *for $c \in H^2(N|K)$ and $\sigma \in G$.*

From the properties of the invariant map stated in Proposition 2.1, we deduce the following properties of the fundamental classes of different field extensions.

Proposition 2.2. *Let $N \supseteq L \supseteq K$ be a tower of extensions with $N|K$ normal. Then*

a. $u_{L|K} = (u_{N|K})^{[N:L]}$, *if $L|K$ is normal,*

b. $res_L(u_{N|K}) = u_{N|L}$,

c. $cor_K(u_{N|L}) = (u_{N|L})^{[L:K]}$,

d. $\sigma^*(u_{N|K}) = u_{\sigma N|\sigma K}$, *for $\sigma \in G$.*

Theorem 2.1 (**Main Theorem**). *Let $L|K$ be a normal extension. Then the map*

$$u_{L|K} \cup : H^q(G_{L|K}, \mathbb{Z}) \to H^{q+2}(L|K)$$

is an isomorphism for all q.

In particular, for dimension $q = -2$, the canonical isomorphism

$$G_{L|K}^{ab} \cong H^{-2}(G_{L|K}, \mathbb{Z}),$$

and simple computation $H^0(L|K) = A_K/N_{L|K}A_L$, yields the general reciprocity law as stated in the next theorem.

Theorem 2.2 (**General Reciprocity Law**). *Let $L|K$ be a normal extension. Then the map*

$$u_{L|K} \cup : H^{-2}(G_{L|K}, \mathbb{Z}) \to H^0(L|K)$$

yields a canonical isomorphism

$$\Theta_{L|K} : G_{L|K}^{ab} \to A_K/N_{L|K}A_L$$

between the abelianization of the Galois group and the norm residue group of the module.

$\Theta_{L|K}$ is also called the **Nakayama map**.

Definition 2.4. *The inverse of the Nakayama map*

$$A_K/N_{L|K}A_L \to G_{L|K}^{ab},$$

is called the ***reciprocity isomorphism****.*

The reciprocity map is useful in the study of local and global class field theory and has been found to be more accessible than the Nakayama map.

Definition 2.5. *The Nakayama map induces a homomorphism $(\ \ , L|K)$ between A_K and $G_{L|K}^{ab}$, with kernel $N_{L|K}A_L$:*

$$1 \to N_{L|K}A_L \to A_K \xrightarrow{(\ \ ,L|K)} G_{L|K}^{ab} \to 1$$

called the ***norm residue symbol****.*

Definition 2.6. *An element $a \in A_K$ is called a* ***norm*** *if and only if $(a, L|K) = 1$.*

We now go on to obtain a one to one correspondence between abelian extensions and norm subgroups.

Lemma 2.1. *Let $L|K$ be a normal extension and L^{ab} the maximal abelian extension of K contained in L. Then $N_{L|K}A_L = N_{L^{ab}|K^{ab}}A_L^{ab} \subseteq A_K$.*

Theorem 2.3. *Let L_1 and L_2 be abelian extensions of K. The map,*

$$L \mapsto I_L = N_{L|K} A_L$$

gives an inclusion reversing isomorphism between the lattice of abelian extensions $L|K$ and the lattice of norm groups I of A_K. Hence we have,

$$I_{L_1} \supseteq I_{L_2} \Leftrightarrow L_1 \subseteq L_2; \quad I_{L_1 \cdot L_2} = I_{L_1} \cap I_{L_2}; \quad I_{L_1 \cap L_2} = I_{L_1} \cdot I_{L_2}$$

if L_1 and L_2 are abelian extensions.
Moreover, every group $I \subseteq A_K$ containing a norm group is itself a norm group.

Proof. First we show that $I_{L_1 \cdot L_2} \subseteq I_{L_1} \cap I_{L_2}$. Recall that field $L_1 \cdot L_2$ is defined by it's corresponding fixed group $G_{L_1 \cdot L_2} = G_{L1} \cap G_{L_2}$. $I_{L_1 \cdot L_2} = N_{L_1 \cdot L_2|K}(a) = \prod_{\sigma \in G_{L_1} \cap G_{L_2}} (a_1 \cdot a_2)^\sigma$. By multiplicativity of norm, we have $I_{L_1 \cdot L_2} = \prod_\sigma a_1^\sigma \prod_\sigma a_2^\sigma$ where σ varies over the elements of $G_{L_1} \cap G_{L_2}$.

To show the reverse containment, we first note that the following diagram commutes for a tower of normal extensions $N \supseteq L \supseteq K$:

$$\begin{array}{ccc} A_K & \xrightarrow{(\ ,N|K)} & G_{N|K}^{ab} \\ {\scriptstyle id}\downarrow & & \downarrow{\scriptstyle \pi_L} \\ A_K & \xrightarrow{(\ ,L|K)} & G_{L|K}^{ab} \end{array}$$

Let $a \in I_{L_1} \cap I_{L_2}$. Then the element $(a, L_1 \cdot L_2|K)$ has the projections by the map π_{L_1} and π_{L_2} given by $(a, L_1|K) = 1$ and $(a, L_2|K) = 1$ in $G_{L_1|K}$ and $G_{L_2|K}$, respectively. Thus, $(a, L_1 \cdot L_2|K) = 1$ which implies $a \in I_{L_1 \cdot L_2}$. Thus, $I_{L_1 \cdot L_2} = I_{L_1} \cap I_{L_2}$.

Given this, we obtain

$$I_{L_1} \subseteq I_{L_2} \Leftrightarrow I_{L_1} \cap I_{L_2} = I_{L_1 \cdot L_2} \Leftrightarrow [L_1 \cdot L_2 : K] = [L_2 : K] \Leftrightarrow L_1 \subseteq L_2$$

This shows the injectivity of the correspondence $L \mapsto I_L$.
From lemma 2.1, every norm group I is the norm group of an abelian extension. This shows that the correspondence is surjective.

To obtain the equality $I_{L_1 \cap L_2} = I_{L_1} \cdot I_{L_2}$, we proceed as follows.
$L_1 \cap L_2 \subseteq L_i,\ i = 1, 2$. Thus, the inclusion reversing bijective correspondence yields $I_{L_1 \cap L_2} \supseteq I_{L_i}\ i = 1, 2$. This implies $I_{L_1 \cap L_2} \supseteq I_{L_1} \cdot I_{L_2}$. As $I_{L_1} \cdot I_{L_2}$ is open, $I_{L_1} \cdot I_{L_2} = N_L$

for some finite abelian extension $L|K$. But $I_{L_i} \subseteq I_L$ implies $L \subseteq L_1 \cap L_2$, so that

$$I_{L_1} \cdot I_{L_2} = I_L \supseteq I_{L_1} \cap I_{L_2}$$

□

2.3 Galois Cohomology

We state some Galois cohomological results that are crucial for proving results about class formations. In particular, we will use them to prove why certain field formations satisfy Axiom I of class formation.

Theorem 2.4. *$H^q(G, L^+) = 0$, $\forall q \in \mathbb{Z}$.*

Proof. Choose $c \in L$ such that $\{\sigma c \mid \sigma \in G\}$ is a basis of $L|K$. We can do this as L is a finite Galois extension and accommodates a normal basis.

$$L^+ = \bigoplus_{\sigma \in G} K^+ \cdot \sigma c = \bigoplus_{\sigma \in G} \sigma(K^+ \cdot c)$$

This implies that L^+ is a G-induced module.Therefore by 1.2, all of its cohomology groups are trivial. □

Lemma 2.2. *Let $L|K$ be a finite Galois extension with Galois group G. Let $\bar{L}$ be an algebraic closure of L and $G = Hom(\bar{L}, K)$. Then, distinct elements of G are linearly independent.*

Theorem 2.5 (**Hilbert-Noether**)**.** *Let $L|K$ be a finite Galois extension with Galois group G. Then $H^1(G, L^\times) = 1$.*

Proof. Let $\phi : G \to L^\times$ be a 1-cocycle. We show that this is also a 1-coboundary. In order to show that, given $\sigma \in G$, we need to find $c \in L^\times$ such that $\phi(\sigma) = \frac{\sigma(c)}{c}$. This implies $\phi \in R_1(G, L^\times)$, and thus the factor group is trivial.

As ϕ is a crossed homomorphism, we have $\phi(\sigma\tau) = \sigma(\phi(\tau)) \cdot \phi(\sigma)$. Consider the set $\{\phi(\sigma) \cdot \sigma | \sigma \in G\}$ of distinct elements of G. By Lemma 2.3, this is a linearly

independent set. Thus, $\exists\ a \in L^\times$ such that

$$\sum_{\sigma \in G} \phi(\sigma) \cdot \sigma(a) = b \neq 0 \in L^\times.$$

Let $\tau \in G$. Then,

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

This gives $\phi(\tau) = \frac{b}{\tau(b)} = \tau(b^{-1})(b^{-1})^{-1}$. Thus, choose $c = b^{-1}$. □

2.4 Class formation of unramified extensions

Let K be a $\mathfrak{p}$-adic number field, that is, a complete discrete valuation field[2] of characteristic 0 with a finite residue field. We wish to obtain the local reciprocity law with respect to the Galois group $G_{T|K}$ of the maximal unramified field extensions $T|K$ of this field acting on the group of units $T^\times$. For this, we shall prove that $(G_{T|K}, T^\times)$ is a class formation and use Tate's theorem. We start by establishing the following notations:
v is the discrete valuation of K.
$\mathfrak{o} = \{x \in K | v(x) \geq 0\}$ is the valuation ring
$\mathfrak{p} = \{x \in K | v(x) > 0\}$ is the maximal ideal
π is the prime element for $\mathfrak{p}$.
$\bar{K} = \mathfrak{o}/\mathfrak{p}$ is the residue field of K and p is the characteristic and $q = (\mathfrak{o}/\mathfrak{p}$ is the number of elements of $\bar{K}$. If f is the degre of $\bar{K}$ over the prime field of p elements, then $q = p^f$.
$U = \mathfrak{o}\backslash\mathfrak{p}$ is the unit group.

[2]For theory of valuations and ramification of prime ideals, see [Neu99], Chapter 2.

$U^1 = 1 + \mathfrak{p}$ is the group of principal units
$U^n = 1 + \mathfrak{p}^n$ denotes higher unit groups.
We consider finite extensions $L|K$ of $\mathfrak{p}$-adic number fields and append to the notation the relevant field as an index thus writing $v_L, \mathfrak{o}_L, \mathfrak{p}_L, U_L$, etc.
The valuation v_K has a unique extension to L, namely $\frac{1}{e}v_L$ where e is the ramification index of $L|K$.
The extension is unramified when $e = 1$. This means that the prime element $\pi \in K$ of $\mathfrak{p}_K$ is also an element of $\mathfrak{p}_L$. This is equivalent to the statement that $[L : K] = [\bar{L} : \bar{K}]$.

Lemma 2.3. *If m is a positive integer, then the map $x \mapsto x^m$ yields for a sufficiently large n, an isomorphism*

$$U^n \to U^{n+v(m)}.$$

We will skip the proof of this lemma for the sake of brevity.
An unramified extension is normal, and there is a canonical isomorphism

$$G_{L|K} \cong G_{\bar{L}|\bar{K}}.$$

If $\sigma \in G_{L|K}$, we obtain the $\bar{K}$ automorphism

$$\bar{\sigma}(x + \mathfrak{p}_L) = \sigma(x) + \mathfrak{p}_L, \qquad x \in \mathfrak{o}_L$$

The group $G_{\bar{L}|\bar{K}}$ is cyclic as the Galois group of a finite field $\bar{L}$. We have the generating automorphsim

$$\bar{x} \mapsto \bar{x}^{q_K}, \qquad \bar{x} \in \bar{L}$$

where q_K is the number of element in $\bar{K}$. As $G_{L|K} \cong G_{\bar{L}|\bar{K}}$, we also obtain a canonical K-automorphism of L which generates $G_{L|K}$.

Definition 2.7. *The automorphism $\varphi_{L|K} \in G_{L|K}$, which is induced by the automorphism*

$$\bar{x} \mapsto \bar{x}^{q_K}, \qquad \bar{x} \in \bar{L}$$

*of the residue field $\bar{L}$ is called the **Frobenius automorphism** of $L|K$.*

Proposition 2.3. *Let $N \supseteq L \supseteq K$ be a tower of unramified extensions of K. Then,*

$$\varphi_{L|K} = \varphi_{N|K}\big|_L = \varphi_{N|K} G_{N|L} \in G_{L|K} \qquad \& \qquad \varphi_{N|L} = \varphi_{N|K}^{[L:K]}$$

Proof. For all $x \in \mathfrak{o}_L$, we have

$$(\varphi_{L|K}x) \bmod \mathfrak{p}_L = x^{q_K} \bmod \mathfrak{p}_N = (\varphi_{N|K}x) \bmod \mathfrak{p}_N$$

For all $x \in \mathfrak{o}_N$, we have

$$(\varphi_{N|L}x) \bmod \mathfrak{p}_N = x^{q_L^{[L:K]}} \bmod \mathfrak{p}_N = (\varphi_{N|K}^{[L:K]}x) \bmod \mathfrak{p}_N$$

□

Theorem 2.6. *Let $L|K$ be an unramified extension. Then,*

$$H^q(G_{L|K}, U_L) = 1, \qquad \forall q \in \mathbb{Z}.$$

Proof. Consider the exact sequence,

$$1 \to U_L^1 \to U_L \to \bar{L}^\times \to 1 \tag{2.1}$$

of $G_{L|K}$ modules. By Theorem 2.5, $H^q(G_{\bar{L}|\bar{K}}, \bar{L}^\times) = 1\ \forall q \in \mathbb{Z}$. As $G_{L|K} \cong G_{\bar{L}|\bar{K}}$, we may identify the group $G_{\bar{L}|\bar{K}}$ by the group $G_{L|K}$. Thus $H^q(G_{L|K}, \bar{L}^\times) = \{1\}$. As a consequence, if we consider the long exact cohomology sequence for the above exact sequence, we obtain $H^q(G_{L|K}, U_L^1) \cong H^q(G_{L|K}, U_L)$. As the extension is unramified, a prime element $\pi \in K$ of $\mathfrak{p}_K$ is also a prime element of $\mathfrak{p}_L$. Thus the map,

$$\begin{aligned} U_L^{n-1} &\to \bar{L}^+ \\ 1 + a \cdot \pi^{n-1} &\mapsto a \ mod\ \mathfrak{p}_L, \qquad a \in \mathfrak{o}_L, \end{aligned}$$

defines a $G_{L|K}$-homomorphism.
Now consider the exact sequence:

$$1 \to U_L^n \to U_L^{n-1} \to \bar{L}^+ \to 0 \tag{2.2}$$

From Theorem 2.4, we have $H^q(L|K, L^+) = 0,\ \forall q \in \mathbb{Z}$. Again, after obtaining the long exact cohomology sequence from 2.2, we obtain the isomorphism
$H^q(G_{L|K}, U_L^n) \cong H^q(G_{L|K}, U_L^{n-1})$. Thus, it follows that the injection induces an isomorphism $H^q(G_{L|K}, U_L^n) \cong H^q(G_{L|K}, U_L)$.
If $m \in \mathbb{Z}^+$, the map $x \mapsto x^m$ defines a homomorphism $U_L \xrightarrow{m} U_L$, and by 2.3 an

isomorphism $U_L^n \to U_L^{n+v(m)}$, provided n is sufficiently large. Thus, we have a homomorphism $H^q(L|K, U_L) \xrightarrow{m} H^q(L|K, U_L)$, and an isomorphism $H^q(L|K, U_L^n) \xrightarrow{m} H^q(L|K, U_L^{n+v(m)})$. Now, consider the commutative diagram:

$$\begin{array}{ccc} H^q(L|K, U_L^n) & \xrightarrow{\simeq} & H^q(L|K, U_L) \\ \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} \\ H^q(L|K, U_L^{n+v(m)}) & \xrightarrow{\simeq} & H^q(L|K, U_L) \end{array}$$

All maps but the right vertical map are bijections. Thus we have the isomorphism

$$\begin{aligned} H^q(L|K, U_L) &\xrightarrow{m} H^q(L|K, U_L) \\ c &\mapsto c^m \end{aligned}$$

This is true for arbitrary $m \in \mathbb{Z}^+$. However, elements in $H^q(L|K, U_L)$ have finite order from 1.4.1. This forces $H^q(L|K, U_L) = 1$. □

We will now proceed to show that unramified extensions form a class formation. To do this, we have to satisfy the two axioms of class formation. Axiom I is taken care of by Theorem 2.5. We wish to satify the second axiom for which we an invariant map which satifies the requisite properties in Definition 2.2 of class formation. We proceed towards this goal with the following steps.
Consider the long exact cohomology sequence associated to the exact sequence:

$$1 \to U_L \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0.$$

As $H^q(L|K, U_L) = 1 \ \forall q$, in particular we have the isomorphism,
$H^2(L|K, L^\times) \cong H^2(L|K, \mathbb{Z})$, via the map we will call $\bar{v}$.
Now consider the exact sequence of $G_{L|K}$ modules under the trivial action of $G_{L|K}$ on each of them:

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

As $\mathbb{Q}$ is a uniquely divisible $G_{L|K}$ module, by Corollary 1.4.1 it is cohomologically trivial. Thus the long exact cohomology sequence yields the isomorphism for the particular case,

$$H^1(L|K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(L|K, \mathbb{Z})$$

where δ is the connecting homomorphism. Consider the inverse isomorphism:

$$H^2(L|K,\mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(L|K,\mathbb{Q}/\mathbb{Z}) = Hom(G_{L|K},\mathbb{Q}/\mathbb{Z}) = \chi(G_{L|K})$$

If $\chi \in \chi(G_{L|K})$, then $\chi(\varphi_{L|K}) \in \frac{\frac{1}{[L:K]}\mathbb{Z}}{\mathbb{Z}} \subseteq \mathbb{Q}/\mathbb{Z}$. Since $\varphi_{L|K}$ generates $G_{L|K}$, the map

$$H^1(L|K,\mathbb{Q}/\mathbb{Z}) = \chi(G_{L|K}) \xrightarrow{\varphi} \frac{\frac{1}{[L:K]}\mathbb{Z}}{\mathbb{Z}}$$

is also an isomorphism.

Definition 2.8. *If $L|K$ is an unramified extension,*

$$inv_{L|K} : H^2(L|K,L^\times) \to \frac{\frac{1}{[L:K]}\mathbb{Z}}{\mathbb{Z}}$$

is an isomorphism defined as

$$inv_{L|K} = \varphi \circ \delta^{-1} \circ \bar{v}$$

Definition 2.9. *The maximal unramified extension, i.e, the union of all unramified extensions, of a $\mathfrak{p}$-adic number field K is called the **inertia field** over K.*

Before proceeding, we fix K_0 as $\mathfrak{p}$-adic number field and T to be the inertia field over K_0.

Theorem 2.7. *The formation $(G_{T|K_0}, T^\times)$ is a class formation with respect to the invariant map defined in definition 2.8.*

Proof. By Theorem 2.5, Axiom I is satisfied.
Let $N \supseteq L \supseteq K$ be a tower of unramified extensions of K. Consider the commutative diagrams:

$$\begin{array}{ccccccc}
H^2(L|K,L^\times) & \xrightarrow{\bar{v}} & H^2(L|K,\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(L|K,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{\frac{1}{[L:K]}\mathbb{Z}}{\mathbb{Z}} \\
\downarrow{\scriptstyle incl} & & \downarrow{\scriptstyle inf} & & \downarrow{\scriptstyle inf} & & \downarrow{\scriptstyle incl} \\
H^2(N|K,N^\times) & \xrightarrow{\bar{v}} & H^2(N|K,\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(N|K,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{\frac{1}{[N:K]}\mathbb{Z}}{\mathbb{Z}}
\end{array}$$

$$\begin{array}{ccccccc} H^2(N|K,N^\times) & \xrightarrow{\bar{v}} & H^2(N|K,\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(N|K,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{\frac{1}{[N:K]}\mathbb{Z}}{\mathbb{Z}} \\ \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle [L:K]} \\ H^2(N|L,N^\times) & \xrightarrow{\bar{v}} & H^2(N|L,\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(N|L,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{\frac{1}{[N:L]}\mathbb{Z}}{\mathbb{Z}} \end{array}$$

The commutativity of the left squares and the middle squares follows from the commutativity of 2-cocycles with $\bar{v}$, inf and res, and the commutativity of inf and res with the connecting homomorphism respectively.
Now we need to prove the commutativity of the right squares. For the first diagram, let $\chi \in H^1(L|K,\mathbb{Q}/\mathbb{Z})$. Commutativity follows from the formula,

$$inf\chi(\varphi_{N|K}) = \chi(\varphi_{N|K}G_{N|L}) = \chi(\varphi_{L|K}).$$

For the second diagram, commutativity follows from the formula,

$$res\chi(\varphi_{N|L}) = \chi(\varphi_{N|L}) = \chi(\varphi_{N|K}^{[L:K]}) = [L:K]\cdot\chi(\varphi_{N|K}).$$

Thus Axiom IIa and IIb are satisfied which completes the proof. □

As $(G_{T|K_0}, T^\times)$ is a class formation with respect to the invariant map defined in Definition 2.8, we have the general reciprocity law for unramified extensions.

Theorem 2.8. *Let $L|K$ be an unramified extension of a $\mathfrak{p}$-adic number field K. Then the map induced by the invariant map (as defined in 2.8):*

$$inv_{L|K}\cup : H^{-2}(G_{L|K},\mathbb{Z}) \to H^0(L|K)$$

yields a canonical isomorphism

$$G_{L|K}^{ab} \to K^\times/N_{L|K}L^\times$$

between the abelianization of the Galois group and the norm residue group.

An example of an unramified extension of a $\mathfrak{p}$-adic number field is $\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$, where $\zeta = \zeta_{p^n-1}$(denoted for simplicity), is a primitive root of unity. The Galois group is abelian, hence

$$G_{\mathbb{Q}_p(\zeta)|\mathbb{Q}_p}^{ab} = G_{\mathbb{Q}_p(\zeta)|\mathbb{Q}_p} \cong \mathbb{Z}/n\mathbb{Z}.$$

By the general reciprocity law, we have

$$G_{\mathbb{Q}_p(\zeta)|\mathbb{Q}_p} \cong \mathbb{Q}_p^\times / N_{\mathbb{Q}_p(\zeta)|\mathbb{Q}_p}\mathbb{Q}_p(\zeta)^\times$$

We know that $\mathbb{Q}_p^\times \cong \mu_{p-1} \times \mathbb{Z} \times \mathbb{Z}_p$. Thus, the local reciprocity law yields the isomorphism $\mathbb{Q}_p^\times / N_{\mathbb{Q}_p(\zeta)|\mathbb{Q}_p}\mathbb{Q}_p(\zeta)^\times \cong \mathbb{Z}/n\mathbb{Z}$.

ADDENDUM: THE LOCAL CASE

Fix a $\mathfrak{p}$-adic number field K_0 and let Ω denote its algebraic closure. We obtain the field formation $(G, \Omega^\times)$ by setting $G = G_{\Omega|K_0}$ and $A = \Omega$, which turns out to be a class formation with respect to the invariant map $inv_{\Omega|K}$. For every normal extension, $A_L = L^\times$.Then the **local reciprocity law** becomes:

$$u_{L|K} \cup : G_{L|K}^{ab} \to K^\times / N_{L|K} L^\times,$$

where $u_{L|K}$ is the uniquely determined element such that $inv_{L|K}(u_{L|K}) = \frac{1}{[L:K]} + \mathbb{Z}$.

Appendix A

Local fields and unramified extensions

Here we provide a brief synopsis of valuation theory leading upto local fields and ramification of prime ideals. These are the basic number theoretic preliminaries to Chapter 2, §4. Here, we assume K to be a field of characteristic 0 and $K^\times$ to be its group of units.

A.1 Discrete valuation rings

Definition A.1. *A valuation, v, on K is a group homomorphism*

$$v : K^\times \to \mathbb{R}$$

such that the following properties are satisfied:

- $v(x \cdot y) = v(x) + v(y)$. *In other words, this is a homomorphism from the multiplicative group $K^\times$ to the additive group $\mathbb{R}$.*
- $v(x + y) \geq min(v(x), v(y))$.

Definition A.2. *v as defined above is said to be a discrete valuation if $v(K^\times)$ is a discrete subgroup of $\mathbb{R}$, in other words, $v(K^\times) = m\mathbb{Z}$ for $m \neq 0$.*

One can **normalize** a valuation by a rescaling by a suitable m^{-1} such that $v(K^\times) = \mathbb{Z}$.

Definition A.3. *Define the sets*

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

$$A^\times := \{x \in K \mid v(x) = 0\}$$

*A is called the **valuation ring** of K with respect to the valuation v and $A^\times$ is its unit group.*

Note that A is a commutative ring which is also an integral domain. A valuation ring with respect to a discrete valuation is called a **Discrete Valuation Ring (DVR)**. An element $\pi \in A$ is called a uniformizer or a prime element if $v(\pi) = 1$. Note that in general, such a π is not unique as $\pi\times$ a unit will also be prime. However, once a π is fixed, every element x of $K^\times$ can be written as $\pi^n \cdot u$ where $u = \dfrac{x}{\pi^n}$ is a uniquely determined element of $A^\times$. This makes A a UFD. Every ideal of A can we generated by π^n for some n and thus A is a PID.

The ideal,

$$\mathfrak{m} := (\pi) = \{x \in A \mid v(x) > 0\},$$

is the unique maximal ideal of A and thus $A/\mathfrak{m}$ is a field.

Definition A.4. *The field $A/\mathfrak{m}$ is called the residue field of the discrete valuation ring A.*

Absolute values and valuations are related in that one can define one with respect to the other by means of exponentiation or natural logarithms. For instance,

$$|\ \ | : K \to \mathbb{R}$$

$$|x| = c^{-v(x)}$$

is an absolute value.

An absolute value with respect to a discrete valuation is called a discrete absolute value.

A.2 Factorization of prime ideals in extensions

Let K be a perfect field complete with respect to a discrete absolute value and A its valuation ring. We assume that it has a finite residue field k, which is also perfect. Let L be an algebraic extension of K of degree n. We can define

$$B = \{a \in L \mid \ |a| \leq 1\}$$

$$\mathfrak{p} = \{a \in B \mid \ |a| < 1\}$$

Here we call $l = B/\mathfrak{p}$ the residue field of L. Suppose $\mathfrak{p}$ is a prime ideal of A. Then,

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$$

Here e_is are ramification indices. The prime $\mathfrak{p}$ is said to be ramified if $e_i > 1$ for some i. If $e_i = 1$ for all i, the prime is split.

Let $f_i = [B/\mathfrak{P}_\mathfrak{i} : A/\mathfrak{p}]$, then it is well known that

$$n = \sum_{i=1}^{g} e_i f_i,$$

and if $L|K$ is a Galois extension, then all prime ideals are conjugate to each other and we have

$$n = efg.$$

Let K be complete with respect to the absolute value $|\ \ |_K$ and L be a separable extension of degree n. Then $|\ \ |_K$ extends uniquely to an absolute value $|\ \ |_L$.

Consider the factorization of the unique maximal ideal in a discrete valuation ring of $L|K$. Thus $g = 1$ and $n = ef$ where e is the ramification index and f is the degree of the residue field.

The normalized valuations ord_K and ord_L are characterized by the their respective uniformizers π and Π of K and L respectively.

$$ord_K(\pi) = 1 \qquad ord_L(\Pi) = 1$$

$$\pi = \Pi^e \times u$$

where u is a unit in the valuation ring. Thus we have,

$$ord_K = \frac{1}{e} ord_L$$

Also note that $[B/\mathfrak{p}B : A/\mathfrak{p}] = n$. Now if $e = n$, the the extension $L|K$ is said to be **totally ramified**, and if $f = n$, the extension is **unramified** over K.

For a field K complete with respect to an archimidean absolute value, the valuation ring A is compact if and only if $A/\mathfrak{m}$ is finite, where $\mathfrak{m}$ is the unique maximal ideal as defined previously.

Definition A.5. *A local field is a field with a non-trivial absolute value such that it is locally compact with respect to it (and hence complete).*

A.3 Unramified extensions of a local field

Let K be a field with characteristic 0 which is complete with respect to a discrete valuation $|\ \ |$. We assume that it has a finite residue field, k, and that both the K and k are perfect fields.

Let A be the discrete valuation ring in K with respect to $|\ \ |$. Let L be a finite extension of K. We have,

$$B = \{a \in L \mid \quad |a| \leq 1\}$$

$$\mathfrak{p} = \{a \in B \mid \quad |a| < 1\}$$

where B is the valuation ring and $\mathfrak{p}$ the unique maximal ideal.

Theorem A.1. *We have a one to one correspondence between the sets $\{K' \subset L$, finite and unramified over $K\ \}$ and $\{k' \subset l$, finite residue field of K' over $k\ \}$. Moreover,*

- *if $K_1 \leftrightarrow k_1$ and $K_2 \leftrightarrow k_2$ then $K_1 \subset K_2$ if and only if $k_1 \subset k_2$;*
- *if $K_1 \leftrightarrow k_1$, the K_1 is Galois over K if and only if k_1 is Galois over k. In this case, we have the canonical isomorphism*

$$Gal(K_1|K) \cong Gal(k_1|k)$$

Corollary A.1.1. *There exists an unramified extension of $K \subset L$ containing all unramified extensions of K in L. We will call it the maximal unramified extension of K in L. If the residue field k is finite, this extension is obtained by adjoining roots of unity of order coprime to the the charateristic of k.*

Any non-archimedian local field is in fact a finite extension of $\mathbb{Q}_p$ for a prime p. Let q be the order of the finite residue field, k. Recall from field theory that for every finite field $\mathbb{F}_q$, there exists a field extension $\mathbb{F}_{q^n}$ of degree n for every n. This is the splitting field of the polynomial $x^{q^n} - x$. The Galois group of this extension is cyclic of order n with the automorphism $x \mapsto x^q$ as the generator. Thus, it follows that every residue field k has an extension k_n of degree n. By the theorem that describes a one to one correspondence between the category of unramified extensions and finite residue fields, we conclude that there is an unramified extension $K_n|K$ of degree n for every n, with a cyclic Galois group of order n. Let B_n be the discrete valuation ring with respect to the uniquely extended valuation in K_n, and $\mathfrak{p}_n$ be the corresponding maximal ideal. Then the Galois group is generated by the K-automorphism,

$$\beta \mapsto \beta^q \ (mod \ \mathfrak{p}_n)$$

where $\beta \in B_n$. This automorphism is called the **Frobenius automorphism**. An alternate definition of unramfied extensions is given below.

Definition A.6. *An extension $L|K$ is unramified if $[L : K] = [l : k]$, where l and k are the residue fields of L and K respectively.*

For $K = \mathbb{Q}_p$, the residue field is $\mathbb{F}_p$ as the maximal ideal in its valuation ring $\mathbb{Z}_p$ is (p). By Corollary A.1.1, there exists a maximal unramified extension $\mathbb{Q}_p^{ur}$ of $\mathbb{Q}_p$, and every ramified extension of degree n is obtained by adjoining roots of unity of order coprime to p. Thus, there is a unique unramified extension $\mathbb{Q}_p(\zeta_{p^n-1})$ of $\mathbb{Q}_p$ of degree n for every n . Let $K_n = \mathbb{Q}_p(\zeta_{p^n-1})$, then

$$\mathbb{Q}_p^{ur} = \varinjlim_n K_n$$

$$Gal(\mathbb{Q}_p^{ur}|\mathbb{Q}_p) = \varprojlim_n Gal(K_n|\mathbb{Q}_p)$$

We have, $Gal(K_n|\mathbb{Q}_p) \cong Gal(\mathbb{F}_{p^n}|\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$. Thus,

$$Gal(\mathbb{Q}_p^{ur}|\mathbb{Q}_p) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

For every $\sigma \in \hat{\mathbb{Z}}$, we have $\sigma(\zeta_n) = \zeta_n^s$, where $s \equiv \sigma \mod n$.

Bibliography

[Mil] James S Milne, *Algebraic number theory (v3. 01), 2008*, URL http://www.jmilne. org/math/CourseNotes/math676. html. kézirat.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Springer, 1999.

[Sam70] Pierre Samuel, *Algebraic theory of numbers: Translated from the french by allan j. silberger*, Hermann, Paris, 1970.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Springer-Verlag, 1973.

[SN13] Alexander Schmidt and Jürgen Neukirch, *Class field theory. the bonn lectures*, Springer, 2013.