

Class Field Theory

A Thesis

submitted to

Indian Institute of Science Education and Research Pune

in partial fulfillment of the requirements for the

BS-MS Dual Degree Programme

by

Shashank Pratap Singh



Indian Institute of Science Education and Research Pune

Dr. Homi Bhabha Road,

Pashan, Pune 411008, INDIA.

May, 2018

Supervisor: Dr. Chandrasheel Bhagwat

© Shashank Pratap Singh 2018

All rights reserved

Certificate

This is to certify that this dissertation entitled *Class Field Theory* towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Shashank Pratap Singh at Indian Institute of Science Education and Research under the supervision of Dr. Chandrasheel Bhagwat, Assistant Professor, Department of Mathematics, IISER Pune, during the academic year 2017-2018.



Dr. Chandrasheel Bhagwat

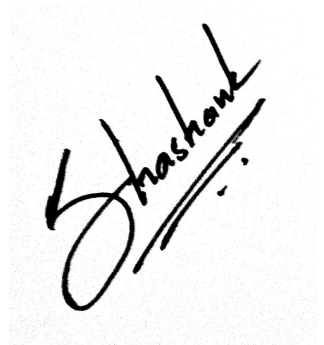
Committee:

Dr. Chandrasheel Bhagwat

Dr. Manish Mishra

Declaration

I hereby declare that the matter embodied in the report entitled Class Field Theory are the results of the work carried out by me at the Department of Mathematics, IISER Pune, Indian Institute of Science Education and Research Pune, under the supervision of Dr. Chandrasheel Bhagwat and the same has not been submitted elsewhere for any other degree.

A handwritten signature in black ink, reading "Shashank", written diagonally on a light gray background.

Shashank Pratap Singh

Acknowledgments

This dissertation reflects the kind and generous support that I received while working on my project.

I would, first and foremost, like to thank my supervisor Dr. Chandrasheel Bhagwat for the opportunity to work with him and also for the wholesome exposure to mathematics through the five years at IISER Pune. My interest in mathematics and inclinations within it are due to the kind encouragement and patient guidance of the department here.

Many thanks are due to my parents for their strong emotional support. And lastly, I would like to thank all my friends for making fifth year a delightful experience.

Shashank Pratap Singh

Abstract

In this thesis, we state and sketch the proofs of main theorems of class field theory. There are many approaches to studying class field theory. We take the cohomological approach to prove the main results for the local case and then using these results establish analogous results for global fields. We briefly discuss John Tate's seminal thesis on meromorphic analytic continuation of L -functions and their functional equations. No claim is made about originality of content and exposition.

Contents

Abstract	ix
1 Introduction	1
2 Number Fields	3
2.1 Kummer Theory	4
2.2 Local Fields	5
2.3 Adèles	8
2.4 Idèles	9
2.5 L -Functions	12
3 Group Cohomology and Galois Cohomology	15
3.1 Group Cohomology	15
3.2 Galois Cohomology	17
4 Local Class Field Theory	21
4.1 Local reciprocity map	21
4.2 Local Existence Theorem	22
4.3 Local Kronecker-Weber Theorem	23
5 Global Class Field Theory	25
5.1 Cohomology of Idèle Group	25
5.2 Idèle Class Group and Reciprocity Law	26
5.3 Cohomology of Idèle Classes	28
5.4 Cohomology of Idèles: First Inequality	29
5.5 Cohomology of Idèles: Second Inequality	30
5.6 The Reciprocity Law	33
5.7 The Existence Theorem	35

Chapter 1

Introduction

We call finite extensions of \mathbb{Q} number fields. As a part of studying algebraic and arithmetic properties we would like to know how all the algebraic extensions of \mathbb{Q} or a number field look like. In other words, we would like to classify all the algebraic extensions in terms of properties of K . Such a classification exists for all abelian extensions of a given number field and is given by class field theory as follows:

1. We associate, to a number field K , a group C_K (called the *class group*) equipped with a homomorphism $\phi : C_K \rightarrow G_K^{ab}$.
2. For a subgroup H of C_K , the fixed field of its image is called the class field associated to H .
3. We then establish a correspondence between certain subgroups of C_K and abelian extensions of K as their class fields.

The homomorphism ϕ in 1 is called the reciprocity law associated to K . The ring of integers R of K is a Dedekind domain which implies every ideal of K can be uniquely factorised into a product of primes. In other words, primes play an important role in the study of algebraic properties of K . In general number fields, prime ideals may not be generated by one element. Local class field theory helps us achieve the above required goals under the assumption that R is a principal ideal domain containing a unique prime ideal, the word local meaning we work locally, that is, at a unique prime of K . The study of local theory facilitates our study of the global one which is concerned with the involvement of all primes of a number field. Localisation of R at a prime \mathfrak{p} gives us a ring $R_{\mathfrak{p}}$ which contains a unique prime ideal corresponding to

\mathfrak{p} . We then study the fields obtained by completing K with respect to the valuation defined by \mathfrak{p} . We construct candidates for the global class group and the global reciprocity map by patching the local components together and therefore classify all abelian extensions of number fields. Good references for local class field theory are [GS97], [CF10] and [Mil13]. For the complete theory; that is, both local and global class field theory, one can refer to [CF10] and [Mil13]. Notes on class field theory by Kiran S. Kedlaya ([Ked17]), freely available at *AMS Open Notes*, is also a nice exposition of the theory.

Another approach to class field theory is Neukirch's abstract class field theory ([NS13] and [Neu86]), which was studied as a part of this project but does not appear in the thesis to avoid repetition of content.

In chapter 2, we develop the relevant notions required to understand the main results of the theory. We briefly discuss Kummer theory, which classifies certain cyclic extensions of number fields containing roots of unity, and also the theory of L -functions and explain the results that John Tate accomplished during his Ph.D., which then appeared in his dissertation, famously known as *Tate's Thesis*.

Chapter 3 includes a description of tools from cohomology theory of finite and profinite groups required to understand and prove the main results. Finally, in chapters 4 and 5, we have the statements and sketches of the main theorems of local and global class field theory respectively.

Chapter 2

Number Fields

In this chapter, we will define and discuss a few properties of algebraic objects related to number fields which are central to the study of class field theory. Any standard text on algebraic number theory includes most of the results displayed in this chapter. Some of the references are [Mil17] and [Neu99].

A Dedekind domain is an integral domain A such that

1. A is Noetherian,
2. A is integrally closed, and
3. every nonzero prime ideal is maximal.

The ring of integers of a number field is a Dedekind domain. In a Dedekind domain every non-zero ideal is generated by at most two elements and can be uniquely factorised into a product of prime ideals. The object of interest for us is the free abelian group generated by the prime ideals of K , denoted by J_K , called the ideal class group.

Let $L|K$ be a finite extension of number fields with number rings O_L and O_K respectively. A prime ideal \mathfrak{p} of O_K , $\mathfrak{p}O_L$ can be factorised as $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ for some prime ideals \mathfrak{P}_i of O_L . Here $\mathfrak{P}_i \cap O_K = \mathfrak{p}$ for all $1 \leq i \leq g$ and we say that the ideals \mathfrak{P}_i lie above \mathfrak{p} . The integer $e_i = e(\mathfrak{P}_i|\mathfrak{p})$ is called the ramification index of $m\mathfrak{P}_i$ over \mathfrak{p} . The field O_L/\mathfrak{P}_i is a finite field containing O_K/\mathfrak{p} and the degree of extension $f_i = f(\mathfrak{P}_i|\mathfrak{p}) = [O_L/\mathfrak{P}_i : O_K/\mathfrak{p}]$ is called the inertia degree of \mathfrak{P}_i over \mathfrak{p} . We have the formula

$$\sum_{1 \leq i \leq g} e_i \cdot f_i = [L : K]$$

Let Σ be the set of all embeddings $L \rightarrow \bar{K}$ fixing K , where \bar{K} is the algebraic closure of K . The norm map $L \rightarrow K$ is defined as $a \mapsto \prod_{\sigma \in \Sigma} \sigma(a)$. To generalise the norm map to the ideals of K we only need to define it for the prime ideals. For a prime ideal \mathfrak{P} of L such that $\mathfrak{P} \cap K = \mathfrak{p}$, we define $N_{L|K}(\mathfrak{P}) = \mathfrak{P}^{f(\mathfrak{P}|\mathfrak{p})}$, where $f(\mathfrak{P}|\mathfrak{p}) = [O_L/\mathfrak{P} : O_K/\mathfrak{p}]$ is the inertia degree of \mathfrak{P} over \mathfrak{p} . The map $N_{L|K}$ is then extended to the whole of J_L .

2.1 Kummer Theory

Reference. [Mil13, p. 222], chapter 2 of [Ked17] and [CF10].

Kummer theory classifies all the cyclic extensions of degree n of a number field K which contains the n -th roots of unity. Throughout this section K is a number field which contains n -th roots of 1. The primitive n -th root of 1 is denoted by ζ_n and the group of these roots by μ_n .

Theorem 2.1.1. *If $\zeta_n \in K$, then the cyclic extensions of K of degree n are of the form $K(\alpha)$, where $\alpha^n \in K$ and no smaller power of α lies in K . Conversely, for such an α , $K(\alpha)$ is Galois with the Galois group $\mathbb{Z}/n\mathbb{Z}$.*

Reference. [CF10, p. 90]

Alternate version of Kummer's theorem says that there is a one-to-one correspondence between extensions of K with Galois group $(\mathbb{Z}/n\mathbb{Z})^r$ and subgroups of $K^\times/(K^\times)^n$ isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$. Let $\Delta \subseteq K^\times/(K^\times)^n$ then for the extension $L = K(\Delta^{1/n})$ we have the isomorphism

$$\Delta \simeq \text{Hom}(G_{L|K}, \mu_n)$$

given by $\bar{x} \mapsto \left(\sigma \mapsto \frac{\sigma \cdot x}{x} \right)$ for some $\bar{x} \in \Delta$ and x some n -th root of \bar{x} in L^\times . The subgroup $\text{Hom}(G_{L|K}, \mu_n)$ is further isomorphic to $G_{L|K}$. Given such an extension L we can retrieve the subgroup Δ as $\frac{K^\times \cap (L^\times)^{1/n}}{(K^\times)^{1/n}}$ which is isomorphic to the Galois group $G_{L|K}$.

2.2 Local Fields

We call a map $\nu : K \rightarrow \mathbb{Z} \cup \{\infty\}$ a discrete valuation on a field K if the following statements hold:

1. The map $\nu : K^\times \rightarrow \mathbb{Z}$ is a group homomorphism.
2. $\nu(0) = \infty$
3. $\nu(x - y) \geq \inf\{\nu(x), \nu(y)\}$

A discrete valuation is called a normalized discrete valuation if the homomorphism $\nu : K^\times \rightarrow \mathbb{Z}$ is surjective. If ν is a discrete valuation defined on a field K and ρ is a real number, $0 < \rho < 1$, then $|x|_\nu = \rho^{\nu(x)}$ is a non-Archimedean valuation often called the discrete multiplicative valuation. Each non-Archimedean valuation on a field K looks like $\rho^{\nu(x)}$ for a real ρ , $0 < \rho < 1$, and a discrete valuation ν . Two non-Archimedean valuations corresponding to the same discrete valuation ν but different ρ are equivalent; that is, they define the same topology on the field K .

The set $\mathcal{O}_K := \{x \in K \mid \nu(x) \geq 0\}$ is a principal ideal domain with field of fractions K and is called the valuation ring of K . The set $\mathfrak{p} := \{x \in K \mid \nu(x) > 0\}$ is a maximal ideal of the ring \mathcal{O}_K called the valuation ideal.

Definition 2.1 (Discrete Valuation Ring). A discrete valuation ring is a principal ideal domain which has a unique non-zero prime ideal.

Proposition 2.2.1. *The valuation ring \mathcal{O}_K of a field K with respect to a discrete valuation ν is a discrete valuation ring. Conversely, for a discrete valuation ring R there is a unique normalized discrete valuation defined on the field of fractions of R .*

Reference. [CF10, p. 4]

The ideal \mathfrak{p} being the unique prime ideal in \mathcal{O}_K is also a maximal ideal and the field $\kappa := \mathcal{O}_K/\mathfrak{p}$ is called the residue class field of K .

We call a field K a local field if K is complete with respect to a non-Archimedean valuation and its residue class field κ is finite.

We shall describe the different kinds of extensions of local fields and explicitly classify all abelian extensions over a local field K only in terms of intrinsic properties of K .

2.2.1 Extensions of Local Fields

We write $[E : F]$ for the dimension of an extension E over a field F and $G_{E|F}$ for the Galois group if $E|F$ is Galois.

Let L be a finite extension of K , \mathcal{O}_L be the valuation ring of L and \mathcal{P} be the maximal ideal of \mathcal{O}_L . We denote the normalized discrete valuations on L and K by $\nu_{\mathfrak{p}}$ and $\nu_{\mathcal{P}}$ respectively.

Proposition 2.2.2. *Any finite extension L of a local field K is likewise local and \mathcal{O}_L , the valuation ring of L is a discrete valuation ring containing K .*

Reference. [CF10, p. 14]

Proposition 2.2.3. *A discrete valuation ν_1 of K can be uniquely extended to a discrete valuation ν_2 of L ; that is, the restriction, $\nu_2|_K = \nu_1$.*

Reference. [CF10, p. 56]

The residue class field $\lambda := \mathcal{O}_L/\mathcal{P}$ of L is an extension of κ . The integer $f(L|K) := [\lambda : \kappa]$ is called the residue class degree. The restriction of $\sigma \in G_{L|K}$ to \mathcal{O}_L , modulo \mathcal{P} gives us an element in $G_{\lambda|\kappa}$.

We define the ramification index, $e(L|K)$ as

$$e(L|K) := \nu_{\mathcal{P}}(\mathfrak{p}\mathcal{O}_L) = \inf_{x \in \mathfrak{p}\mathcal{O}_L} \nu_{\mathcal{P}}(x)$$

which means that $\mathfrak{p}\mathcal{O}_L = \mathcal{P}^{e(L|K)}$. We will write e and f instead of $e(L|K)$ and $f(L|K)$, if the context is clear. The algebra $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is finitely generated over $\mathcal{O}_K/\mathfrak{p}$ of dimension $[L : K]$ and can be written as $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \mathcal{O}_L/\mathcal{P} \oplus \mathcal{P}/\mathcal{P}^2 \oplus \dots \oplus \mathcal{P}^{e-1}/\mathcal{P}^e$. The subspaces $\mathcal{O}_L/\mathcal{P}$ and $\mathcal{P}^{i-1}/\mathcal{P}^i$, each of dimension f , are isomorphic for all $1 \leq i \leq e$. Thus, we have the equation $e \cdot f = [L : K]$.

Unramified Extensions

We call an extension L (possibly infinite) of K unramified if the following statements hold:

1. $e(L|K) = 1$
2. The residue field extension λ is separable over κ .

In the case of unramified extensions, we have $f = [L : K]$.

Theorem 2.2.1. *For every separable extension λ over κ we have a unique unramified extension L over K such that λ is the residue class field of L . The corresponding Galois groups are isomorphic; that is, $G_{L|K} \simeq G_{\lambda|\kappa}$.*

Reference. [CF10, p. 26]

The above theorem establishes a bijection between the collection of all separable extensions of κ and the collection of all unramified extensions of K .

Corollary 2.2.1.1. *For a prescribed degree $n \in \mathbb{Z}$, there exists an unramified extension, denoted by K_n , with Galois group $G_{K_n|K} \simeq \mathbb{Z}/n\mathbb{Z}$.*

Proof. We know from basics of Galois theory that every finite field has an extension of a prescribed degree $n \in \mathbb{N}$ with Galois group isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Hence, the corollary is clear. \square

Corollary 2.2.1.2. *An extension L of K , contains an extension, $K \subseteq F \subseteq L$, such that F is unramified over K and there is no unramified extension of K in L that contains F .*

Proof. The field F is the unramified extension of K corresponding to the separable closure of κ in λ . \square

The field F in Corollary 2.2.1.2 is called the maximal unramified extension of K contained in L and it is the compositum of all unramified extension of K contained in L .

The unramified extension of K corresponding to the separable closure of κ is called the maximal unramified extension of K , denoted by K^{nr} and its Galois group $G_K^{nr} \simeq \hat{\mathbb{Z}}$.

Totally Ramified Extensions

An extension L (possibly infinite) of K is called totally ramified if $e(L|K) = [L : K]$. For a totally ramified extension L , the residue class field λ is the same as κ . If F is the maximal unramified extension of K contained in L , then L is totally ramified over F .

Theorem 2.2.2. 1. An Eisenstein polynomial $E(X)$ is irreducible. If Π is a root of $E(X)$ then the extension $L = K(\Pi)$ is totally ramified.

2. Conversely, a totally ramified extension L of K is of the form $L = K(\Pi)$, where Π is a root of an Eisenstein polynomial.

Reference. [CF10, p. 23]

2.3 Adèles

For a number field K , the set

$$\mathbb{A}_K := \prod'_v K_v$$

where $\prod'_v K_v$ is the restricted product of topological spaces, that is, for all $x \in \mathbb{A}_K$ we have $x_v \in \mathcal{O}_v$ for all but finitely many v . The set \mathbb{A}_K is a topological ring under subspace topology from the product $\prod K_v^\times$ and componentwise addition and multiplication.

Definition 2.2 (Ring of Adèles). The ring \mathbb{A}_K is called the ring of adèles of the number field K .

Other equivalent definitions include $\hat{\mathcal{O}}_K \otimes_{\mathcal{O}_K} K$ and $\varinjlim_{\alpha} \frac{1}{\alpha} \mathcal{O}_K$.

Example (Ring of adèles of \mathbb{Q}). According to the above definitions $\mathbb{A}_{\mathbb{Q}} = \prod'_v \mathbb{Q}_p \simeq \hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \varinjlim_n \frac{1}{n} \hat{\mathbb{Z}}$.

The number field K and its completion K_v embed inside \mathbb{A}_K via the injections $\alpha \mapsto x$ with $x_v = 1$ for all v and $\alpha \mapsto x$ with $x_v = \alpha$ and $x_t = 1$ for $t \neq v$ respectively. We define a valuation on \mathbb{A}_K , using the valuations defined on each completion, by:

$$|\cdot| : (\alpha_v)_v \mapsto \prod_v |\alpha_v|_v$$

which is normalised by choosing the following normalised local valuations:

1. For v real, $|\cdot|_v$ is the usual absolute value on real numbers.
2. For v complex, $|\cdot|_v$ is the square of the usual absolute value on complex numbers.
3. For v nonarchimedean, $|\cdot|_v$ is chosen such that $|p|_v = p^{-1}$ if $v|p$.

Henceforth, the term valuation will be used for normalised valuation.

Proposition 2.3.1 (Product Formula). *For all $\alpha \in K$, we have $|\alpha| = 1$.*

Proof. An element $\alpha \in K$ is divisible by finitely many primes of K and for a normalised valuation $\prod_{v|\alpha} |\alpha_v|_v = 1$. \square

2.4 Idèles

Let S_∞ be the set of infinite places of K and $S \supset S_\infty$ be a finite set of primes of a number field K . The set

$$\mathbb{I}_K^S := \prod_{v \in S} K_v^\times \times \prod_{v \notin S} O_v^\times$$

is a group under componentwise addition and multiplication and is called the group of S -idèles of K . The group $K^S = \mathbb{I}_K^S \cup K^\times$ is called the group of S -unis of K consisting of those elements in K^\times which are coprime to the primes in S .

Definition 2.3 (Group of Idèles). The group

$$\mathbb{I}_K = \bigcup_{\#S < \infty} \mathbb{I}_K^S$$

is called the groups of idèles of K .

Example. $\mathbb{I}_\mathbb{Q} = \mathbb{A}_\mathbb{Q}^\times$.

The topology on \mathbb{I}_K is defined by $\{\mathbb{I}_K^S\}_{(\#S < \infty)}$ as the fundamental system of neighborhoods around 1 and \mathbb{I}_K is locally compact. As groups, $\mathbb{A}_K^\times \simeq \mathbb{I}_K$. But \mathbb{A}_K^\times is not a topological group with subspace topology from \mathbb{A}_K as the map $r \mapsto r^{-1}$ is not continuous.

The map $\mathbb{A}_K \rightarrow \mathbb{A}_K \times \mathbb{A}_K : r \mapsto (r^{-1}, r)$ is a continuous injective ring homomorphism. Under subspace topology from $\mathbb{A}_K \times \mathbb{A}_K$, \mathbb{A}_K^\times becomes a topological group and is isomorphic to \mathbb{I}_K . We may write \mathbb{A}_K^\times or \mathbb{I}_K for the group of idèles of K . The group \mathbb{I}_K is also written as $GL_1(\mathbb{A}_K)$.

The group K^\times naturally embeds inside \mathbb{I}_K via the map $\alpha \mapsto x$ with $x_v = \alpha$ for all v and $K_v^\times \rightarrow \mathbb{I}_K$ mapping α to the element with α as the component at v th place and 1 at the other places. The subgroup K^\times is closed and discrete in \mathbb{I}_K . As a consequence, the group \mathbb{I}_K/K^\times is a locally compact Hausdorff group.

Relation between Idèles and Ideals

We recall that for a number field K , J_K denotes the free abelian group generated by the finite primes of K . The map

$$\begin{aligned} \psi : \mathbb{I}_K &\longrightarrow J_K \\ (\alpha_v)_v &\mapsto \prod_v \mathfrak{p}_v^{v(\alpha_v)} \end{aligned}$$

is a surjective homomorphism. The subgroup \mathbb{I}_{K, S_∞} is contained in the kernel of this map as all the infinite places are ignored by the map. Principal idèles are mapped to the principal ideals one-to-one by ψ . Thus, the map $\psi : \mathbb{I}_K / K^\times \rightarrow J_K / P_K$ is a well-defined surjective homomorphism which is continuous with respect to discrete topology on J_K / P_K .

Valuation on Idèles

In the previous section, we defined valuation on the ring of adèles. This valuation, restricted to the group of idèles, gives a homomorphism from \mathbb{I}_K onto \mathbb{R}_+^\times . Kernel of the homomorphism $|\cdot| : \mathbb{I}_K \rightarrow \mathbb{R}_+^\times$, denoted by \mathbb{I}_K^1 is called the group of norm-1 idèles of K . Similar to the principal adèles, the principal idèles are contained in the kernel of this homomorphism which allows us to define a homomorphism $\mathbb{I}_K / K^\times \rightarrow \mathbb{R}_+^\times$.

The homomorphism $\mathbb{I}_\mathbb{Q} \rightarrow \mathbb{R}_+^\times$ is surjective with kernel equal to $\mathbb{Q}^\times \times \hat{\mathbb{Z}}^\times$, which gives an alternate description $\mathbb{I}_\mathbb{Q} \simeq \mathbb{Q}^\times \times \hat{\mathbb{Z}}^\times \times \mathbb{R}_+^\times$.

Action of the Galois group and Norm map

For a finite extension of number fields $L|K$ and a prime v of K , let w be a prime of L dividing v . For all $w|v$ setting $\alpha_w = \alpha_v$, gives us an embedding of \mathbb{I}_K into \mathbb{I}_L . Let $M|K$ be the normal closure of L . For $\sigma \in G_{M|K}$, the map $\sigma : L \rightarrow \sigma(L)$ is a K -isomorphism leading to a K_v -isomorphism, $\sigma : L_w \rightarrow \sigma(L)_{\sigma w}$. Using these local maps, one can define the action of the Galois group on \mathbb{I}_L by $\sigma(\alpha_w) = (\sigma\alpha)_{\sigma w}$. The action of Galois group enables us to define the norm map $N_{L|K} : \mathbb{I}_L \rightarrow \mathbb{I}_K$ as

$$N_{L|K}(\alpha) = \prod_{\sigma} \sigma\alpha$$

where σ runs over all the representatives of $G_{L|K}/G_{M|L}$.

Proposition 2.4.1. *For a Galois extension $L|K$ of number fields with Galois group G , we have $\mathbb{I}_L^G = \mathbb{I}_K$.*

Proof. If the extension $L|K$ is Galois; that is, the group $G_{L|K}$ acts transitively on the primes. Let $\alpha \in \mathbb{I}_L^G$ then the components $(\alpha_w)_{w|v}$ are equal for all primes w and v , which by definition of the inclusion $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$ belongs to \mathbb{I}_K . Similarly, for some $\alpha \in \mathbb{I}_K \subset \mathbb{I}_L$ the components $(\alpha_w)_{w|v}$ are equal and therefore is fixed by $G_{L|K}$. \square

Proposition 2.4.2. *For a finite extension $L|K$ of number fields and $\alpha \in \mathbb{I}_L$, the local components of $N_{L|K}(\alpha)$ are given by*

$$N_{L|K}(\alpha)_v = \prod_{w|v} N_{L_w|K_v}(\alpha_w)$$

Reference. [Mil13, p. 175]

The above proposition shows that the diagram

$$\begin{array}{ccc} L_w^\times & \xrightarrow{N_{L_w|K_v}} & K_v^\times \\ \downarrow & & \downarrow \\ \mathbb{I}_L & \xrightarrow{N_{L|K}} & \mathbb{I}_K \end{array} \quad \text{and} \quad \begin{array}{ccc} L^\times & \xrightarrow{N_{L|K}} & K^\times \\ \downarrow & & \downarrow \\ \mathbb{I}_L & \xrightarrow{N_{L|K}} & \mathbb{I}_K \end{array}$$

commute, and the map $N_{L|K} : \mathbb{I}_L/L^\times \rightarrow \mathbb{I}_K/K^\times$ is well defined. The norm map is also compatible with the map $\psi : \mathbb{I}_K/K^\times \rightarrow J_K/P_K$; that is, the following diagram

$$\begin{array}{ccc} \mathbb{I}_L/L^\times & \xrightarrow{N_{L|K}} & \mathbb{I}_K/K^\times \\ \downarrow \psi & & \downarrow \psi \\ J_L/P_L & \xrightarrow{N_{L|K}} & J_K/P_K \end{array}$$

commutes. Commutativity of the above diagram helps us translate the results in terms of idèles to ideals.

2.5 L -Functions

Obviously, the best reference is *Tate's Thesis* itself which can be found in [CF10] but one may also refer to the article on Tate's thesis by Stephen S. Kudla which appeared in D. Bump et al., *An Introduction to the Langlands Program*. A Dirichlet character modulo m is a homomorphism $\chi_m : (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$. The trivial Dirichlet character taking value 1 for all elements in $(\mathbb{Z}/m\mathbb{Z})^\times$ is called the primitive Dirichlet character and is denoted by χ_0 . To a Dirichlet character χ we attach a Dirichlet series or an L -series

$$L(s, \chi) = \prod_{p \nmid m} \frac{1}{1 - \chi(p)p^{-s}} = \sum_{n>0} \frac{\chi(n)}{n^s}$$

The expression in the middle is called an Euler product. Note that $L(s, \chi_0)$ is quite similar to the Riemann's zeta function; that is, the factors $\frac{1}{1 - p^{-s}}$ are missing for $p|m$ in $L(\chi_0, s)$.

Given two integers $n|m$ we have the projection map $\pi_n^m : (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ which when composed with a Dirichlet character χ_m gives us a Dirichlet character modulo χ_n . As the Dirichlet characters are compatible with the projection maps and $\{(\mathbb{Z}/m\mathbb{Z})^\times\}_{m \in \mathbb{Z}}$ form an inverse system with the projection maps, every Dirichlet character modulo m can be associated to a continuous character

$$\chi : \hat{\mathbb{Z}}^\times \rightarrow \mathbb{C}^\times.$$

The group $(\mathbb{Z}/m\mathbb{Z})^\times$ decomposes as $\prod_{p|m} (\mathbb{Z}/p\mathbb{Z})^\times$ which gives us a factorisation $\chi_n = \otimes_p \chi_p$ of Dirichlet characters modulo m . Therefore, due to the decomposition $\hat{\mathbb{Z}}^\times = \prod_p \hat{\mathbb{Z}}_p^\times$, we have a factorisation

$$\chi = \otimes_p \chi_p$$

of continuous character $\chi : \hat{\mathbb{Z}}^\times \rightarrow \mathbb{C}^\times$, where each $\chi_p : \hat{\mathbb{Z}}_p^\times \rightarrow \mathbb{C}^\times$ is also a continuous character.

From the decomposition $\mathbb{I}_{\mathbb{Q}} \simeq \mathbb{Q}^\times \times \mathbb{R}_+^\times \times \hat{\mathbb{Z}}^\times$, it is clear that a continuous character χ defines a continuous character

$$\omega : \mathbb{I}_{\mathbb{Q}}/\mathbb{Q}^\times \rightarrow \mathbb{C}^\times$$

by $\omega(x) = \omega(\alpha \cdot t \cdot u) = \chi(t)$ for some $x \in \mathbb{I}_{\mathbb{Q}}$ and corresponding to x , $\alpha \in \mathbb{Q}^\times$, $t \in \mathbb{R}_+^\times$ and $u \in \hat{\mathbb{Z}}^\times$. In general, these characters are of the form $\omega \cdot |\cdot|^s$ for $s \in \mathbb{C}^\times$, where

$|x| = t$ for some $x \in \mathbb{I}_{\mathbb{Q}}$ and the corresponding $t \in \mathbb{R}_+^{\times}$. The embedding $\mathbb{Q}_v^{\times} \hookrightarrow \mathbb{I}_{\mathbb{Q}}$ we have the factorisation of the character

$$\omega = \otimes_v \omega_v$$

where ω_v is a continuous character defined on \mathbb{Q}_v^{\times} .

Note that, for a general number field K , we might not get a simple decomposition for \mathbb{I}_K as we got for $\mathbb{I}_{\mathbb{Q}}$, nontriviality of the class group being one of the reasons. A quasicharacter or Hecke character is a continuous complex character $\mathbb{I}_K \rightarrow \mathbb{C}^{\times}$, trivial on K^{\times} . A quasicharacter ω_v is said to be unramified if it is trivial on \mathcal{O}_v^{\times} . For a quasicharacter $\omega : \mathbb{I}_K \rightarrow \mathbb{C}^{\times}$, let S be a set of all primes such that ω_v is unramified for $v \notin S$. We associate a partial L -function to the quasicharacter ω by the Euler product

$$L^S(s, \omega) = \prod_{v \notin S} \frac{1}{1 - t_v(\omega)q_v^{-s}}$$

where $q_v = \#\mathcal{O}_v/\mathfrak{p}_v$. The factors $L_v(s, \omega_v) = \frac{1}{1 - t_v(\omega)q_v^{-s}}$ are called the local L -factors associated to ω_v 's. By using Fourier analysis on locally compact Hausdorff topological groups, Tate in his thesis completed this partial L -function by adding local L -factors for $v \in S$ and proved that the completed L -function admits a meromorphic analytic continuation and derived a functional equation for the completed L -function.

Chapter 3

Group Cohomology and Galois Cohomology

Reference. [CF10] and [Mil13].

3.1 Group Cohomology

3.1.1 Standard Complex and Tate Groups

Let G be a finite group, and $\mathbb{Z}[G]$ is the group ring generated over G . A G -module is basically a module over the group ring $\mathbb{Z}[G]$. There is an obvious action of the group G over the G -module A given by $(g, a) \mapsto g \cdot a$, for all $g \in G$ and $a \in A$. A standard complex is a sequence of following kind:

$$\begin{array}{ccccccc} \cdots & \longleftarrow & X_{-2} & \xleftarrow{d_{-1}} & X_{-1} & \xleftarrow{d_0} & X_0 & \xleftarrow{d_1} & X_1 & \longleftarrow & \cdots \\ & & & & \swarrow \epsilon & & \searrow \mu & & & & \\ & & & & & \mathbb{Z} & & & & & \\ & & & & \swarrow & & \searrow & & & & \\ & & & & 0 & & 0 & & & & \end{array}$$

where,

1. X_i are G -modules and the maps d_i are G -module homomorphisms, for all $i \in \mathbb{Z}$
2. $d_0 = \mu \circ \epsilon$

3. The sequence is exact at each term.

By construction, there exists a standard complex for a group G where the G -modules. We take q -tuples of the form $(\sigma_1, \dots, \sigma_q)$, where $\sigma_i \in G$. For $q \geq 1$, we define $X_q = X_{-q}$ as the module generated by these q -tuples over $\mathbb{Z}[G]$ and $X_0 = X_{-1} = \mathbb{Z}[G]$. To keep this report concise we do not explicitly describe the maps d_i 's, discussed in **Part I** of [NS13].

Let A be any arbitrary G -module. We apply the functor $\text{Hom}_G(-, A)$ on the above sequence to get the following sequence

$$\cdots \rightarrow \text{Hom}_G(X_{-2}, A) \xrightarrow{\partial_{-1}} \text{Hom}_G(X_{-1}, A) \xrightarrow{\partial_0} \text{Hom}_G(X_0, A) \xrightarrow{\partial_1} \text{Hom}_G(X_1, A) \rightarrow \cdots$$

This new sequence that we get is not exact in general. We define

$$H^q(G, A) := \text{Im}(\partial_{q+1}) / \ker(\partial_q)$$

The group $H^q(G, A)$ is called the q^{th} Tate cohomology group of G with coefficients in A .

Important Tate groups and relevant notation. For a G -module A , we have:

1. $A^G = \{x \in A \mid gx = x \ \forall g \in G\}$, the fixed group of A
2. $N_G A = \{N_G \cdot a = \sum_{g \in G} g \cdot a \mid a \in A\}$, the norm group of A
3. ${}_{N_G} A = \{a \in A \mid N_G \cdot a = 0\}$
4. $I_G A = \{\sum_{g \in G} n_g a_g (g - 1) \mid a_g \in A, n_g \in \mathbb{Z}\}$

Following are some important Tate groups:

1. $H^{-2}(G, A) = G^{ab}$, abelianization of G
2. $H^{-1}(G, A) = {}_{N_G} A / I_G A$
3. $H^0(G, A) = A^G / N_G A$
4. $H^0(G, A) = \frac{\text{crossed homomorphism}}{\text{principal crossed homomorphism}} H^0(G, A) = \text{Hom}(G, A)$ if G acts trivially on A .

3.1.2 Tate's Theorem

Theorem 3.1.1 (Tate). *Let A be a G -module, $a \in H^2(G, A)$. For each prime p let G_p be a p -Sylow subgroup of G , and assume that*

1. $H^1(G_p, A) = 0$
2. $H^2(G_p, A)$ is generated by $\text{Res}(a)$ and has size equal to G_p .

Then for all subgroups H of G and all integers q the cup product with $\text{Res}(a)$ induces an isomorphism

$$H^q(G, \mathbb{Z}) \longrightarrow H^{q+2}(G, A).$$

Reference. [CF10, p. 115] and [Mil13, p. 81]

3.2 Galois Cohomology

3.2.1 Infinite Galois Theory

Let K^s be a separable closure of a field K with Galois group G_K . We consider the family of extensions of K , $\{K_i\}_{i \in I}$, such that $K_i \subset K^s$ and $K_i|K$ is finite and Galois with Galois group G_i , for all $i \in I$. If for two such extensions K_i and K_j we have $K_i \subset K_j$ then we also have a homomorphism $\pi_i^j : G_j \rightarrow G_i$ defined by $\sigma \mapsto \sigma|_{K_i}$. If we allow the finite Galois groups to have a discrete topology then the maps π_i^j are also continuous. Thus, we have an inverse system of finite topological groups, $\{G_i\}_{i \in I}$.

Proposition 3.2.1. *There exists an isomorphism of topological groups*

$$G_K \simeq \varprojlim_{i \in I} G_i.$$

Reference. [CF10, p. 120]

Theorem 3.2.1 (Fundamental Theorem of Galois Theory). *There is a one-to-one correspondence between the set of intermediate fields, $K^s \supset E \supset K$, and the set of closed subgroups $H \subset G_{K^s|K}$, given by*

$$E \mapsto G_{K^s|E} \quad \text{and} \quad H \mapsto (K^s)^H.$$

Reference. [CF10, p. 120]

3.2.2 Galois Cohomology

If $K_i \subset K_j$, then we have an injective homomorphism $K_i \rightarrow K_j$ and a surjective group homomorphism $G_j \rightarrow G_i$, and the two maps together give us the inflation map

$$\lambda_i^j : H^q(G_i, K_i) \longrightarrow H^q(G_j, K_j)$$

which makes the family of abelian groups $\{H^q(G_i, K_i)\}_{i \in I}$ a direct system.

Proposition 3.2.2. *There exists an isomorphism of topological abelian groups*

$$H^q(G_K, K^s) \simeq \varinjlim_{i \in I} H^q(G_i, K_i)$$

Reference. [CF10, p. 123]

Theorem 3.2.2. *The group $H^q(G_K, K^s)$ is trivial, for all $q \geq 1$.*

Reference. [CF10, p. 124]

We denote by F^\times , the multiplicative group of a field F .

Theorem 3.2.3 (Hilbert 90). *The group $H^1(G_K, (K^s)^\times)$ is trivial.*

Reference. [CF10, p. 124]

3.2.3 Brauer Group

Let L_1 and L_2 be Galois extensions of a field K with Galois groups G_1 and G_2 respectively. If $f : L_1 \rightarrow L_2$ is a K -isomorphism then $f(L_1)$ is Galois over K . The restriction $\sigma \mapsto \sigma|_{f(L_1)}$ is a group homomorphism $\bar{f} : G_2 \rightarrow G_1$. Let H be the Galois group of L_2 over $f(L_1)$. Let \tilde{f} be the composition of the maps

$$H^q(G_1, L_1^\times) \xrightarrow{\sim} H^q(G_2/H, f(L_1)^\times) \rightarrow H^q(G_2, L_2^\times).$$

The map \tilde{f} is independent of the choice of K -homomorphism f [CF10, p. 125]. If L_1 and L_2 are two separable closures of K , then there exists a K -isomorphism $L_1 \xrightarrow{\sim} L_2$ and all such isomorphisms yield a unique isomorphism $H^q(G_1, L_1^\times) \xrightarrow{\sim} H^q(G_2, L_2^\times)$.

Definition 3.1 (Brauer Group). The group $H^2(G, (K^s)^\times)$ is called the Brauer group of K and is denoted by $\text{Br}(K)$.

Theorem 3.2.4. *If L and F are Galois extensions of K such that $L \supset F \supset K$, then we have the following inflation-restriction exact sequence*

$$0 \rightarrow H^2(G_{F|K}, F^\times) \rightarrow H^2(G_{L|K}, L^\times) \rightarrow H^2(G_{L|F}, L^\times).$$

Reference. [CF10, p. 126] and [Mil13, p. 101].

The proof follows from theorem 3.2.3 (Hilbert's Theorem 90) and the fact that \varinjlim is an exact functor.

Corollary 3.2.4.1. *If L is the separable closure of K and F then the above exact sequence becomes*

$$0 \rightarrow H^2(G_{F|K}, F^\times) \rightarrow \text{Br}(K) \rightarrow \text{Br}(F).$$

Proof. Clear. □

Chapter 4

Local Class Field Theory

4.1 Local reciprocity map

The Brauer group of a local field K is important to the theory as it helps us prove that $H^2(G_{L|K}, L^\times)$ is cyclic of order n and hence show that the local field case satisfies the hypotheses of Tate's theorem. For a group G acting trivially on \mathbb{Q} and \mathbb{Z} , the exact sequence

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

gives us an isomorphism $\delta^{-1} : H^2(G, \mathbb{Z}) \rightarrow H^1(G, \mathbb{Q}/\mathbb{Z})$. As G acts on \mathbb{Q}/\mathbb{Z} trivially, $H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$ and also $\text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}$. If the group G is G_K , then we have an isomorphism $H^2(G_K, (K^s)^\times) \simeq H^2(G_K, \mathbb{Z})$ induced by the homomorphism $\nu : K^\times \rightarrow \mathbb{Z}$. The composition of the following maps

$$\text{Br}(K) \rightarrow H^2(G_K, \mathbb{Z}) \rightarrow H^1(G_K, \mathbb{Q}/\mathbb{Z}) \rightarrow \mathbb{Q}/\mathbb{Z}$$

is called the invariant map and is denoted by inv_K . If L is a finite extension of K then the following diagram commutes (references)

$$\begin{array}{ccc} \text{Br}(K) & \xrightarrow{\text{Res}} & \text{Br}(L) \\ \downarrow \text{inv}_K & & \downarrow \text{inv}_L \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

We finally arrive at the following commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & \ker(\text{Res}) & \longrightarrow & H^2(G_K^{nr}, (K^{nr})^\times) & \xrightarrow{\text{Res}} & H^2(G_L^{nr}, (L^{nr})^\times) \\
& & \downarrow & & \downarrow \text{inf} & & \downarrow \text{inf} \\
0 & \longrightarrow & H^2(G_{L|K}, L^\times) & \longrightarrow & \text{Br}(K) & \longrightarrow & \text{Br}(L) \\
& & \downarrow & & \downarrow \text{inv}_K & & \downarrow \text{inv}_L \\
0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

Here, the injectivity of the two labelled inflation maps tells us that the map

$$\ker(\text{Res}) \rightarrow H^2(G_{L|K}, L^\times)$$

is injective and similarly we show that the map $H^2(G_{L|K}, L^\times) \rightarrow \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is injective. We then show that $\ker(\text{Res})$ contains an element of order n proving that $H^2(G_{L|K}, L^\times)$ is cyclic of order n .

Now that the hypothesis of theorem 3.1.2 is satisfied, we have an isomorphism $H^{-2}(G_{L|K}, \mathbb{Z}) \rightarrow H^0(G_{L|K}, L^\times)$ which translates to

$$\Phi_{L|K} : K^\times / N(L^\times) \rightarrow G_{L|K}^{ab}$$

It is easy to see that $G_K^{ab} \simeq \varprojlim_L G_{L|K}^{ab}$, and using the universal property of \varprojlim we conclude the existence of the map

$$\Phi_K : K^\times \rightarrow G_K^{ab}$$

4.2 Local Existence Theorem

The local reciprocity map establishes a correspondence between norm subgroups of K^\times and abelian extensions of K . The local existence theorem classifies all the norm subgroups of K^\times .

Theorem 4.2.1. *The norm subgroups of K^\times are precisely the open subgroups of finite index.*

Reference. [CF10, p. 154]

Theorem 4.2.2 (Norm Limitation Theorem). *Let M be the maximal abelian subextension of $L|K$. Then $N_{L|K}L = N_{M|K}M$.*

Reference. [Mil13, p. 157]

4.3 Local Kronecker-Weber Theorem

The local Kronecker-Weber theorem says that every abelian extension of K can be embedded inside a cyclotomic extension. To make sense of the statement of the theorem we discuss a little about formal groups before stating it and sketching the proof.

4.3.1 Lubin-Tate Formal Groups

We know that there exists an extension $\nu : K^s \rightarrow \mathbb{Z} \cup \{\infty\}$ of the valuation $\nu : K \rightarrow \mathbb{Z} \cup \{\infty\}$. The set $\Lambda = \{x \in K^s \mid |x| < 1\}$ is the maximal ideal inside the valuation ring of K^s . The set $1 + \Lambda = \{1 + x \mid x \in \Lambda\}$ is a group under multiplication. The map $x \mapsto 1 + x : \Lambda \rightarrow 1 + \Lambda$ is not a group homomorphism. However, up to the choice of a uniformizer π , we can define a new group structure on Λ using Lubin-Tate formal group laws such that the aforementioned map becomes a group homomorphism. We benefit from this construction as the roots of the polynomial $x^q - 1$ (q is the size of κ) map to the roots of $(1 + x)^q - 1$ which is an Eisenstein polynomial. We discuss the key points in this section and the details of the construction can be found in [references]. Let Λ_f denote the set Λ with this new group operation defined. The polynomial evaluated on Λ_f is a surjective group homomorphism and the following diagram commutes

$$\begin{array}{ccc} \Lambda_f & \xrightarrow{x \mapsto 1+x} & 1 + \Lambda \\ \downarrow f & & \downarrow x \mapsto x^q \\ \Lambda_f & \xrightarrow{x \mapsto 1+x} & 1 + \Lambda \end{array}$$

There exists an injective ring homomorphism $\mathcal{O}_K \hookrightarrow \text{End}(\Lambda_f)$, denoted by $a \mapsto [a]$, such that the uniformiser π maps to f . This makes Λ_f an \mathcal{O}_K -module. Let $f^{(n)}$ denote $f \circ f \cdots \circ f$ (n times) and Λ_n denote the kernel of $f^{(n)}$. Also, let Λ_∞ be the set of points

in Λ_f that are killed by all the powers of π ; that is, they belong to the kernel of $f^{(n)}$, for all n . We now examine the fields $K_{[\pi,n]} := K(\Lambda_n)$ for $n \geq 1$ and $K_\pi := K(\Lambda_\infty)$.

4.3.2 Local Kronecker-Weber Theorem

The fields $K_{[\pi,n]}$ for $n \geq 1$ are totally ramified as they are constructed by adjoining the roots of Eisenstein polynomials. The following theorem concludes that these are precisely all the totally ramified abelian extensions of a local field K .

Theorem 4.3.1 (Local Kronecker-Weber). *For some uniformiser π of the local field K , the maximal abelian extension K^{ab} is of the form*

$$K^{ab} = K_\pi \cdot K^{nr}.$$

We obtain a homomorphism $G_{K_{[\pi,n]}|K} \rightarrow \text{Aut}_{\mathcal{O}_K}(\Lambda_f)$ the above theorem is a corollary to the following

Theorem 4.3.2. *For $K_{[\pi,n]}|K$ and $a = u \cdot \pi^s \in K^\times$, then $a \cdot \lambda = [u^{-1}] \cdot \lambda$ for $\lambda \in \Lambda_f$.*

Reference. [CF10, p. 153]

Chapter 5

Global Class Field Theory

5.1 Cohomology of Idèle Group

Let $L|K$ be a Galois extension with Galois group G and $S \supset S_\infty$ be a finite set of primes of K . We study the cohomology groups $H^q(G, \mathbb{I}_L)$ of the G -module \mathbb{I}_L . To our advantage, these groups can be decomposed into direct product of the cohomology groups of local fields. We define

$$\mathbb{I}_L^S = \prod_{\mathfrak{p}|\mathfrak{p} \in S} L_{\mathfrak{p}}^\times \times \prod_{\mathfrak{p}|\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}^\times = \prod_{\mathfrak{p} \in S} \prod_{\mathfrak{p}|\mathfrak{p}} L_{\mathfrak{p}}^\times \times \prod_{\mathfrak{p} \notin S} \prod_{\mathfrak{p}|\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^\times$$

Set $\mathbb{I}_L^{\mathfrak{p}} = \prod_{\mathfrak{p}|\mathfrak{p}} L_{\mathfrak{p}}^\times$ and $\mathcal{O}_L^{\mathfrak{p}} = \prod_{\mathfrak{p}|\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^\times$. Then

$$\mathbb{I}_L^S = \prod_{\mathfrak{p} \in S} \mathbb{I}_L^{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_L^{\mathfrak{p}}$$

The group G acts transitively on the primes above \mathfrak{p} , $\mathbb{I}_L^{\mathfrak{p}}$ and $\mathcal{O}_L^{\mathfrak{p}}$ are G -modules. We have written \mathbb{I}_L^S as a product of G -modules.

If $\sigma \in G$ runs through the system of representatives of $G/G_{\mathfrak{p}}$, then $\sigma\mathfrak{p}$ runs through all the primes of L above \mathfrak{p} . Hence

$$\mathbb{I}_L^{\mathfrak{p}} = \prod_{\sigma \in G/G_{\mathfrak{p}}} L_{\sigma\mathfrak{p}}^\times \quad \text{and} \quad \mathcal{O}_L^{\mathfrak{p}} = \prod_{\sigma \in G/G_{\mathfrak{p}}} \mathcal{O}_{\sigma\mathfrak{p}}^\times$$

showing that $\mathbb{I}_L^{\mathfrak{p}}$ and $\mathcal{O}_L^{\mathfrak{p}}$ are induced G -modules. Applying Shapiro's lemma we get the following

Proposition 5.1.1. *Let \mathfrak{P} be a prime of L lying above \mathfrak{p} , then, for all $r \in \mathbb{Z}$,*

$$H^r(G, \mathbb{I}_L^{\mathfrak{p}}) = H^r(G_{\mathfrak{P}}, L_{\mathfrak{P}}^{\times}) \text{ and } H^r(G, \mathcal{O}_L^{\mathfrak{p}}) = H^r(G_{\mathfrak{P}}, \mathcal{O}_{\mathfrak{P}}^{\times})$$

where $G_{\mathfrak{P}}$ is the galois group of $L_{\mathfrak{P}}|K_{\mathfrak{p}}$.

From local class field theory, we know that $H^r(G_{\mathfrak{P}}, \mathcal{O}_{\mathfrak{P}}^{\times}) = 1$ if \mathfrak{p} is unramified in L . And, from the above proposition we infer that $H^r(G, \mathcal{O}_L^{\mathfrak{p}}) = 1$ for all unramified primes \mathfrak{p} of K . If S is a finite set of primes of K conatining all the infinite primes, then we can write:

$$H^r(G, \mathbb{I}_L^S) = \bigoplus_{\mathfrak{p} \in S} H^r(G_{\mathfrak{P}}, L_{\mathfrak{P}}^{\times}) \bigoplus_{\mathfrak{p} \notin S} H^r(G_{\mathfrak{P}}, \mathcal{O}_{\mathfrak{P}}^{\times}) = \bigoplus_{\mathfrak{p} \in S} H^r(G_{\mathfrak{P}}, L_{\mathfrak{P}}^{\times})$$

where, \mathfrak{P} varies over a single prime over each \mathfrak{p} . The limit $\varinjlim_S \mathbb{I}_L^S = \mathbb{I}_L$ helps us derive $H^r(G, \mathbb{I}_L) = \varinjlim_S H^r(G, \mathbb{I}_L^S) = \bigoplus_{\mathfrak{p}} H^r(G_{\mathfrak{P}}, L_{\mathfrak{P}}^{\times})$.

5.2 Idèle Class Group and Reciprocity Law

Given a number field K and v a prime in K , each K_v is local field with the reciprocity map $\phi_v : K_v^{\times} \rightarrow G_v$. For a finite extension L of K and w a prime of L dividing v we have the isomorphism $\phi_{L_w|K_v} : K_v^{\times}/N_{L_w|K_v}(L_w^{\times}) \rightarrow G_{L_w|K_v}$. But the group $G_{L_w|K_v}$ sits inside $G_{L|K}$ as the decomposition group of w .

$$\begin{array}{ccccc} L & \longrightarrow & L_w & \longrightarrow & \mathcal{O}_w/\mathfrak{P}_w \\ \Big| f & & \Big| f & & \Big| f \\ L^{G_w} & \longrightarrow & K_v & \longrightarrow & \mathcal{O}_v/\mathfrak{p}_v \\ \Big| g & \Big/ & & & \\ K & & & & \end{array}$$

We now construct a candidate $\Phi_{L|K}$ for the global reciprocity law by taking product of the local ones; that is, $\Phi_{L|K} : \mathbb{I}_K \rightarrow G_{L|K}$ as $\Phi_{L|K}(\alpha) = \prod_{w|v} \phi_{L_w|K_v}(\alpha_w)$. The

following diagram

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & G_{L_w|K_v} \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\Phi_{L|K}} & G_{L|K} \end{array}$$

commutes. We will observe that for abelian extensions of K , K^\times is contained in the kernel of $\Phi_{L|K}$ and the redefined map $\Phi_{L|K} : \mathbb{I}_K/K^\times \rightarrow G_K$ turns out to be the required reciprocity law associated to K . As subgroups of \mathbb{I}_K , K^\times and K_v^\times intersect in the trivial subgroup and the the diagram

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & G_{L_w|K_v} \\ \downarrow & & \downarrow \\ \mathbb{I}_K/K^\times & \xrightarrow{\Phi_{L|K}} & G_{L|K} \end{array}$$

commutes. Hence, the global reciprocity law (once proved) is compatible with the local ones.

Definition 5.1. The group $\mathbb{C}_K = \mathbb{I}_K/K^\times$ is called the idèle class group of K .

The idèle class group plays an important role in the classification of abelian extensions of a number field. In the previous section we discussed that the group \mathbb{C}_K is locally compact and Hausdorff. The norm map $N_{L|K} : \mathbb{C}_L \rightarrow \mathbb{C}_K$ is a well defined homomorphism. Following commutative diagram

$$\begin{array}{ccc} \mathbb{I}_L & \xrightarrow{N_{L|K}} & \mathbb{I}_K \\ \downarrow & & \downarrow \\ \mathbb{C}_L & \xrightarrow{N_{L|K}} & \mathbb{C}_K \end{array}$$

tells us that

$$N_{L|K}(\mathbb{C}_L) = \frac{N_{L|K}(\mathbb{I}_L)}{(N_{L|K}(\mathbb{I}_L) \cap K^\times)} \simeq \frac{N_{L|K}(\mathbb{I}_L) \cdot K^\times}{K^\times}$$

where the latter isomorphism is given by the second isomorphism theorem of groups.

$$\mathbb{C}_K/N_{L|K}(\mathbb{C}_L) \simeq \frac{\mathbb{I}_K/K^\times}{N_{L|K}(\mathbb{I}_L) \cdot K^\times/K^\times} \simeq \frac{\mathbb{I}_K}{K^\times \cdot N_{L|K}(\mathbb{I}_L)}$$

Denote by \mathbb{C}_K^0 the kernel of the map $|\cdot| : \mathbb{C}_K \rightarrow \mathbb{R}_+^\times$. The group \mathbb{C}_K^0 in global class field theory plays a role similar to the group of units in the local theory.

Restriction of the homomorphism $\psi : \mathbb{I}_K/K^\times \rightarrow J_K/P_K$ to \mathbb{C}_K^0 is a surjection onto J_K/P_K because we can always adjust the valuation at the infinite primes as they are ignored by the map.

Proposition 5.2.1. *The Group \mathbb{C}_K^0 is compact.*

Reference. [CF10, p. 70]

Corollary 5.2.0.1. *Class number of K is finite.*

Proof. The map $\psi : \mathbb{C}_K^0 \rightarrow J_K/P_K$ is continuous and surjective implying J_K/P_K is compact. The group J_K/P_K , being discrete and compact, is finite. \square

5.3 Cohomology of Idèle Classes

In order to show that the map $\Phi_{L|K} : \mathbb{C}_K \rightarrow G_{L|K}$ is indeed the required reciprocity law, we shall prove for all abelian extensions $L|K$ that K^\times is contained in the kernel of $\Phi_{L|K} : \mathbb{I}_K \rightarrow G_{L|K}$ and the map

$$\Phi_{L|K} : \mathbb{I}_K/K^\times \cdot N_{L|K}(\mathbb{I}_L) \rightarrow G_{L|K}$$

is an isomorphism. If we show:

1. $\#\mathbb{I}_K/K^\times \cdot N_{L|K}(\mathbb{I}_L) \geq [L : K]$ (first inequality)
2. $\#\mathbb{I}_K/K^\times \cdot N_{L|K}(\mathbb{I}_L) \leq [L : K]$ (second inequality)

then 1 and 2 together will imply that this map is an isomorphism. We will show this isomorphism for cyclic extensions and then extend it to all abelian extensions.

Proposition 5.3.1. *For $S \supset S_\infty$, a large enough finite set of primes of K , we have*

$$\mathbb{I}_K = \mathbb{I}_K^S \cdot K^\times$$

and, therefore,

$$\mathbb{C}_K = \mathbb{I}_K^S \cdot K^\times / K^\times = \mathbb{I}_K^S / K^S$$

Here the set S contains all the ramified primes of K and the primes dividing the generators of ideal class group of K alongside all the infinite primes.

Reference. [Neu86, p. 77]

5.4 Cohomology of Idèles: First Inequality

Theorem 5.4.1. *Let $L|K$ be a cyclic extension of number fields,*

$$\#H^0(G_{L|K}, \mathbb{C}_L) \geq [L : K]$$

As the group $G_{L|K}$ is cyclic, $h(\mathbb{C}_L)$ is defined to be $\frac{\#H^0(G_{L|K}, \mathbb{C}_L)}{\#H^1(G_{L|K}, \mathbb{C}_L)}$. To prove theorem 5.4.1, it is sufficient to show that $h(\mathbb{C}_L) = [L : K]$. For S being a large enough set of primes of K , from proposition 5.3.1 we have the following exact sequence

$$1 \rightarrow L^S \rightarrow \mathbb{I}_L^S \rightarrow \mathbb{C}_L \rightarrow 1$$

and, in case, $L|K$ is cyclic, following identity of Herbrand quotients is true $h(\mathbb{I}_L^S) = \frac{h(\mathbb{C}_L)}{h(L^S)}$. The equality $H^r(G, \mathbb{I}_L^S) = \bigoplus_{v \in S} H^r(G_w, L_w^\times)$, for all $r \in \mathbb{Z}$, implies $h(\mathbb{I}_L^S) = \prod_{v \in S} \#H^0(G_w, L_w^\times) = \prod_{v \in S} [L_w : K_v]$. The proof of theorem 5.4.1, thus, requires $h(L^S) = \frac{1}{[L : K]} \prod_{v \in S} [L_w : K_v]$.

Lemma 5.4.2. *Let G be a finite cyclic group, and let V be a real vector space on which G acts linearly (i.e., V is an $R[G]$ -module). Let M and N be two G -stable full lattices in V . If either $h(M)$ or $h(N)$ is defined, then so is the other, and they are equal.*

Let T be the set of primes of L lying above S . We construct a vector space V over \mathbb{R} with copies of \mathbb{R} indexed by the elements of T . We define the G -action on V by $\sigma \cdot (\alpha_w)_w = (\alpha_{\sigma^{-1}w})_w$. The T -units of L map in to V via the map $\alpha \mapsto (\dots, \log |\alpha|_w, \dots)$ and the image is a lattice of full rank. We construct another lattice by restricting the scalars from \mathbb{R} to \mathbb{Z} , say M . This is an induced module and hence

$$h(M) = \prod_v h(G/G_w, \mathbb{Z}) = \prod_v [L_w : K_v]$$

The herbrand quotient of the image of the T -units of L turns out to be $[L : K] \cdot h(L^S)$ thus proving that $h(L^S) = \frac{1}{[L : K]} \prod_{v \in S} [L_w : K_v]$. Hence, we have our first inequality

$$\#\mathbb{I}_K/K^\times \cdot N_{L|K}(\mathbb{I}_L) \geq [L : K]$$

Proposition 5.4.1. *Let L be a finite solvable extension of K (i.e., a finite Galois extension with solvable Galois group). If there exists a subgroup D of \mathbb{I}_K such that*

1. $D \subseteq N_{L|K}\mathbb{I}_K$ and
2. $K^\times \cdot D$ is dense in \mathbb{I}_K

then $L = K$.

Proof. If $L \neq K$ then there is a cyclic extension K' such that $L \supset K' \supset K$ as by assumption $L|K$ is solvable. Then

$$D \subseteq N_{L|K}(\mathbb{I}_L) = N_{K'|K}(N_{L|K}(\mathbb{I}_L)) \subseteq N_{K'|K}(\mathbb{I}_{K'})$$

As $K^\times \cdot N_{K'|K}(\mathbb{I}_{K'}) = \mathbb{I}_K$, we have $K^\times \cdot N_{K'|K}(\mathbb{I}_{K'}) = \mathbb{I}_K$. Then first inequality implies $L = K$. \square

Proposition 5.4.2. *Let L be a finite solvable extension of K . If $L \neq K$, then there are infinitely many primes of K that do not split completely in L .*

Proof. Suppose not and let $S \supset S_\infty$ be a finite set of primes containing all the primes of K that do not completely split. We take $D = \mathbb{I}_K^S$ and show $D \cdot K^\times$ is dense in \mathbb{I}_K implying $L = K$. \square

Proposition 5.4.3. *For every finite solvable extension $L|K$ with Galois group G , and every finite set of prime ideals T of L including those that ramify from K , the Frobenius elements $(\mathfrak{F}, L/K)$ for $\mathfrak{F} \notin T$ generate G .*

Proof. Let H be the subgroup generated by the Frobenius elements corresponding to the primes $\mathfrak{F} \notin T$ and $E = L^H$. These Frobenius elements restricted to E are identity maps which will imply that all $\mathfrak{p} \in S$ split in E . Therefore $E = K$ and $G = H$. \square

5.5 Cohomology of Idèles: Second Inequality

Theorem 5.5.1. *Let $L|K$ be a Galois extension of degree n with Galois group $G_{L|K} = G$, then the following statements are true:*

- $\#H^0(G, \mathbb{C}_L)$ and $\#H^2(G, \mathbb{C}_L)$ divide n .
- $H^1(G, \mathbb{C}_L) = 1$.

Lemma 5.5.2. *It is sufficient to prove theorem 5.5.1 in the case where $L|K$ is cyclic of prime order p .*

Proof. Let G_p be a p -Sylow subgroup of G for some prime $p \in \mathbb{Z}$. Then we have the injection

$$\text{Res} : H^r(G, \mathbb{C}_L)_p \rightarrow H^r(G_p, \mathbb{C}_L)$$

Because $H^r(G, \mathbb{C}_L)$ is a torsion group, it can be written as the direct sum of its p -primary components, thus, $\#H^r(G_p, \mathbb{C}_L) | n$ implies $\#H^r(G, \mathbb{C}_L) | n$. Therefore, it is sufficient to prove the theorem for p -groups and we can now assume G to be a p -group of size n . To prove that it is sufficient that the result holds for cyclic extensions, we use induction on the degree of p . Being a p -group, G contains a normal subgroup of index p , say H , and we have the restriction inflation exact sequence,

$$0 \rightarrow H^1(G/H, \mathbb{C}_L^H) \rightarrow H^1(G, \mathbb{C}_L) \rightarrow H^1(H, \mathbb{C}_L)$$

Assume that the theorem is true for cyclic extensions $L|K$, then by mathematical induction $\#H^1(G, \mathbb{C}_L) = 0$, which gives rise to another exact sequence,

$$0 \rightarrow H^2(G/H, \mathbb{C}_L^H) \rightarrow H^2(G, \mathbb{C}_L) \rightarrow H^2(H, \mathbb{C}_L)$$

The integer $\#H^2(G, \mathbb{C}_L)$ divides the product $\#H^2(G/H, \mathbb{C}_L^H) \cdot \#H^2(H, \mathbb{C}_L)$ and by our assumption on cyclic extensions $\#H^2(G/H, \mathbb{C}_L^H)$ divides p and if $\#H^2(H, \mathbb{C}_L)$ divides n/p then by mathematical induction $\#H^2(G, \mathbb{C}_L)$ must divide n . It now remains to show that $\#H^0(G, \mathbb{C}_L)$ divides n . Let $K' = L^H$ then $[K' : K] = n/p$ and

$$\#\mathbb{C}_K/N_{L|K}\mathbb{C}_L = \#\mathbb{C}_K/N_{K'|K}\mathbb{C}_{K'} \cdot \#N_{K'|K}\mathbb{C}_{K'}/N_{L|K}\mathbb{C}_L$$

and because $N_{L|K}$ defines a surjection

$$\mathbb{C}_{K'}/N_{L|K'}\mathbb{C}_L \rightarrow N_{K'|K}\mathbb{C}_{K'}/N_{L|K}\mathbb{C}_L$$

$\#\mathbb{C}_K/N_{L|K}\mathbb{C}_L$ divides $p \cdot n/p = n$. □

Lemma 5.5.3. *It is sufficient to prove theorem 5.5.1 for cyclic extensions $L|K$ of degree p such that K contains p^{th} roots of unity.*

Proof. Let ζ be the primitive p^{th} root of 1 in some algebraic closure of the field K . $K' = K[\zeta]$ and $L' = K' \cdot L = L[\zeta]$. The degree $[K' : K] = m$ divides $p - 1$ hence

$L \cap K' = K$ and $G_{L'|K} = G_{L|K} \times G_{K'|K}$ as $[L : K] = p$. The following diagram commutes

$$\begin{array}{ccccccc}
\mathbb{C}_L & \xrightarrow{N_{L|K}} & \mathbb{C}_K & \longrightarrow & \mathbb{C}_K/N_{L|K}\mathbb{C}_L & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
\mathbb{C}_{L'} & \xrightarrow{N_{L'|K'}} & \mathbb{C}_{K'} & \longrightarrow & \mathbb{C}_{K'}/N_{L'|K'}\mathbb{C}_{L'} & \longrightarrow & 0 \\
\downarrow N_{L|L} & & \downarrow N_{K'|K} & & \downarrow & & \\
\mathbb{C}_L & \xrightarrow{N_{L|K}} & \mathbb{C}_K & \longrightarrow & \mathbb{C}_K/N_{L|K}\mathbb{C}_L & \longrightarrow & 0
\end{array}$$

and the maps $\mathbb{C}_L \rightarrow \mathbb{C}_L$ and $\mathbb{C}_K \rightarrow \mathbb{C}_K$ are just multiplication by m implying that the map

$$\mathbb{C}_K/N_{L|K}\mathbb{C}_L \rightarrow \mathbb{C}_K/N_{L|K}\mathbb{C}_L$$

is also multiplication by m which is an automorphism because $(m, p) = 1$. \square

We will now prove the theorem for this case by constructing a subgroup \mathbb{C}' such that $\#\mathbb{C}/\mathbb{C}' = p$ and $\mathbb{C}' \subseteq N_{L|K}\mathbb{C}_L$ which will prove the theorem. Similar to the proof of first inequality, we use a set S of a places of K containing all the infinite places, primes that ramify in L , primes sitting above p and S is large enough so that $\mathbb{I}_K^S \cdot K^\times = \mathbb{I}_K$. Let $M = K((K^S)^{1/p})$. We can now choose a set T disjoint from S such that the Frobenius elements, associated to primes in T , generate $G_{M|K}$. For such a T , we define

$$E = \prod_{v \in S} (K_v^\times)^p \times \prod_{v \in T} K_v^\times \times \prod_{v \in S \cup T} \mathcal{O}_v^\times$$

Let $\Delta = (L^\times)^p \cap K^S$. By Kummer Theory, L is an extension of the form $K(D^{1/p})$ and if $K \neq K(\Delta^{1/p})$ then we can say that $L = K(\Delta^{1/p})$. Choose x such that $L = K(x^{1/p})$. For each $v \notin S$, $K_v(x^{1/p})|K_v$ is an unramified extension, and we can write $x = u_v \cdot y_v^p$ for some unit u_v . Construct an idèle y by setting $y_v = 1$ for $v \in S$. As $\mathbb{I}_K = \mathbb{I}_K^S \cdot K^\times$, write $y = w \cdot z$ for $w \in \mathbb{I}_K^S$ and $z \in K^\times$. Now $x/z^p \in (L^\times)^p \cap K^S$ but $x \notin (K^\times)^p$. Hence, $L = K(\Delta^{1/p})$. It is shown, using Kummer theory and the generalisation of Dirichlet's unit theorem to S -units, that we can choose the set T of $s-1$ primes such that Δ is the kernel of the map $K^S \rightarrow \prod_{v \in T} K_v^\times / (K_v^\times)^p$. Then $E \subset N_{L|K}\mathbb{I}_L$ and $E \cdot K^\times = \mathbb{I}_K$, and set $\mathbb{C}' = E \cdot K^\times / K^\times$. Using the fact that $E \cap K^\times = (K^{S \cup T})^p$ we

obtain the exact sequence

$$1 \rightarrow (\mathbb{I}_K^{S \cup T} \cap K^\times)/(E \cap K^\times) \rightarrow \mathbb{I}_K^{S \cup T}/E \rightarrow \mathbb{I}_K^{S \cup T} \cdot K^\times/E \cdot K^\times \rightarrow 1.$$

The group $\mathbb{I}_K^{S \cup T} \cdot K^\times/E \cdot K^\times = \mathbb{C}_K/\mathbb{C}'$ and $(\mathbb{I}_K^{S \cup T} \cap K^\times)/(E \cap K^\times) = K_{S \cup T}^\times/(K_{S \cup T}^\times)^p$. By Dirichlet's unit theorem, $\#(K_{S \cup T}^\times)^p = p^{2s-1}$ and $\#\mathbb{I}_K^{S \cup T}/E = p^{2s}$ because the group is the product of $K_v^\times/(K_v^\times)^p$ for all $v \in S$ each of which has order p^2 . Therefore, $\#\mathbb{C}_K/\mathbb{C}' = p$.

It remains to show that $\mathbb{C}' \subseteq N_{L|K}\mathbb{C}_L$ for which it is sufficient to show that $E \subseteq N_{L|K}\mathbb{I}_L$. It is obvious for the primes $v \notin S \cup T$, as they are unramified and so every unit is a norm. For primes in S , every element of K_v^\times is a norm form $K(K_v^{1/p})$ and hence also form L_w . Finally, for primes in T , we have $\Delta \subseteq (K_v^\times)^p$ and so K_v^\times consists entirely of norms. We have now proved the second inequality, which is, for all abelian extensions of number fields $L|K$

$$\#\mathbb{I}_K/K^\times \cdot N_{L|K}(\mathbb{I}_L) \leq [L : K]$$

5.6 The Reciprocity Law

We have proved the first and second inequalities and now it remains to show that K^\times is in the kernel of $\Phi_{L|K} : \mathbb{I}_K \rightarrow G_{L|K}$ which we will do with help of following lemmas

Lemma 5.6.1. *If K^\times is in the kernel of $\Phi_{L|K} : \mathbb{I}_K \rightarrow G_{L|K}$ for some extension $L|K$, then the same is true for all subextensions.*

Proof. Let $L \supset K' \supset K$, then $\Phi_{K'|K}$ is the composite of $\Phi_{L|K}$ and the restriction $G_{L|K} \rightarrow G_{K'|K}$. The lemma is now clear. \square

Lemma 5.6.2. *If K^\times is in the kernel of $\Phi_{L|K} : \mathbb{I}_K \rightarrow G_{L|K}$ for some extension $L|K$, then the same is true for $L \cdot K'|K'$ for all number fields $K' \supset K$.*

Proof. Let $L' = L \cdot K'$. For each prime v' of K and $w'|v'$ and $w|v$ we have the commutative diagram

$$\begin{array}{ccc} (K_{v'}^\times) & \xrightarrow{\phi_{v'}} & G_{L'_{w'}|K_{v'}} \\ \downarrow \text{Norm} & & \downarrow \\ K_v^\times & \xrightarrow{\phi_v} & G_{L_w|K_v} \end{array}$$

Which gives us the following commutative diagram

$$\begin{array}{ccc} \mathbb{I}_{K'} & \xrightarrow{\Phi_{L'|K'}} & G_{L'|K'} \\ \downarrow N_{K'|K} & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\Phi_{L|K}} & G_{L|K} \end{array}$$

and hence the lemma holds. \square

Example. We will now show that the \mathbb{Q}^\times is in the kernel of the map $\mathbb{I}_{\mathbb{Q}} \rightarrow G_{K|\mathbb{Q}}$ for some cyclotomic extension $K|\mathbb{Q}$. Let $K = \mathbb{Q}(\zeta_m)$. Identify $G_{K|\mathbb{Q}}$ with $(\mathbb{Z}/m\mathbb{Z})^\times$. It suffices to show the above for m being a prime power, say, $m = l^r$. For the infinite case, $\phi_\infty : \mathbb{R}/N(\mathbb{C}^\times) \rightarrow G_{K|\mathbb{Q}}$, takes a to $[\text{sign}(a)]$. Let $a = u \cdot p^s$ in \mathbb{Q}_p^\times . If $p \neq l$ then $\phi_p(a) = [p^s]$ and if $p = l$ then $\phi_l(a) = [u^{-1}]$, from local theory. It suffices to check the result for $a = -1$, $a = l$ and $a = q$ for some prime $q \neq l$.

$$\phi_p(-1) = \begin{cases} [-1] & \text{if } p = \infty \\ [-1] & \text{if } p = l \\ [1] & \text{if } p \neq l, \infty \end{cases}$$

$$\phi_p(l) = \begin{cases} [1] & \text{if } p = l \\ [1] & \text{if } p \neq l \end{cases}$$

$$\phi_p(q) = \begin{cases} [q] & \text{if } p = q \\ [q^{-1}] & \text{if } p = l \\ [1] & \text{if } p \neq l, q \end{cases}$$

In all the cases $\prod \phi_p(a) = 1$.

This example along with the previous lemmas shows us that K^\times is in the kernel

of the map $\Phi_{L|K} : \mathbb{I}_K \rightarrow G_{L|K}$ for cyclotomic extension of number fields $L|K$. We will use the following lemmas (without providing a proof) to prove that K^\times is in the kernel of the map $\Phi_{L|K} : \mathbb{I}_K \rightarrow G_{L|K}$.

Lemma 5.6.3. *If $L|K$ is cyclic and K^\times is in the kernel of the map $\Phi_{L|K} : \mathbb{I}_K \rightarrow G_{L|K}$ then $\sum \text{inv}_v(\alpha) = 0$ for $\alpha \in H^2(G_{L|K}, L)$. Conversely, if $L|K$ is abelian and $\sum_v \text{inv}_v(\alpha) = 0$ then K^\times is in the kernel of the map $\Phi_{L|K} : \mathbb{I}_K \rightarrow G_{L|K}$.*

Reference. [Mil13, p. 219]

Lemma 5.6.4. *If $L|K$ is cyclic and $\sum \text{inv}_v(\alpha) = 0$ for $\alpha \in H^2(G_{L|K}, L)$ then $\sum \text{inv}_v(\alpha) = 0$ for $\alpha \in H^2(G_{L|K}, L)$ for all Galois extensions.*

Reference. [Mil13, p. 219]

The lemmas and the example above imply that K^\times is in the kernel of the map $\Phi_{L|K} : \mathbb{I}_K \rightarrow G_{L|K}$ defining a homomorphism

$$\Phi_K : \mathbb{I}_K / K^\times \cdot N_{L|K} \mathbb{I}_L \rightarrow G_{L|K}$$

which is surjective because the Galois group is generated by the Frobenius elements corresponding to the unramified primes of K . From the second inequality we can conclude that this map is an isomorphism.

5.7 The Existence Theorem

We have established a one-to-one correspondence between the abelian extensions of a number fields and norm subgroups of the idèle class group with the help of global reciprocity law. It is natural to ask if we can classify all the norm subgroups of the idèle class group. Therefore, we have the following

Theorem 5.7.1. *Every open subgroup of finite index in the idèle class group is a norm group.*

proof of the theorem requires the following lemmas

Lemma 5.7.2. *If $L|K$ is cyclic and $H \subseteq \mathbb{C}_K$ and if $N_{L|K}^{-1}(H) \subseteq \mathbb{C}_L$ is a norm group then H is norm subgroup in \mathbb{C}_K .*

Reference. [CF10, p. 202]

Lemma 5.7.3. *Let p be a prime, and K a number field containing the p -th roots of unity. Then every open subgroup H of index p in \mathbb{C}_K is a norm group.*

Reference. [CF10, p. 201]

We then use induction on the degree of H to prove the existence theorem.

Bibliography

- [Neu86] J. Neukirch. *Class Field Theory*. Grundlehren der mathematischen Wissenschaften. Springer-Verlag Berlin Heidelberg, 1986. ISBN: 9783642824654.
- [GS97] M.J. Greenberg and J.P. Serre. *Local Fields*. Graduate Texts in Mathematics. Springer New York, 1997. ISBN: 9781475756739.
- [Neu99] J. Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer-Verlag Berlin Heidelberg, 1999. ISBN: 9783642084737.
- [CF10] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society (a NATO Advanced Study Institute) with the Support of the International Mathematical Union*. London Mathematical Society, 2010. ISBN: 9780950273426.
- [Mil13] J.S. Milne. *Class Field Theory (v4.02)*. Available at www.jmilne.org/math/. 2013.
- [NS13] J. Neukirch and A. Schmidt. *Class Field Theory: -The Bonn Lectures- Edited by Alexander Schmidt*. Class Field Theory: The Bonn Lectures. Springer Berlin Heidelberg, 2013. ISBN: 9783642354373.
- [Ked17] Kiran S. Kedlaya. *Notes on Class Field Theory*. 2017.
- [Mil17] James S. Milne. *Algebraic Number Theory (v3.07)*. www.jmilne.org/math/. 2017.